Cisco ASA シリーズ VPN CLI コンフィギュレーション ガイド

ソフトウェア バージョン 9.3

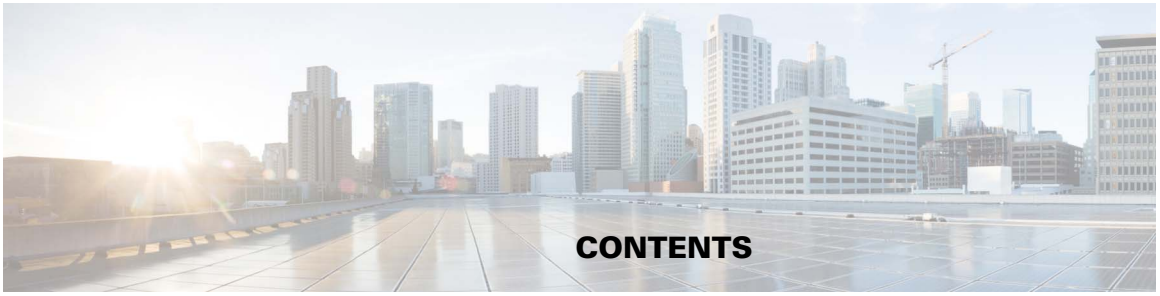
リリース日：2014 年 7 月 24 日

Cisco Systems, Inc.
www.cisco.com

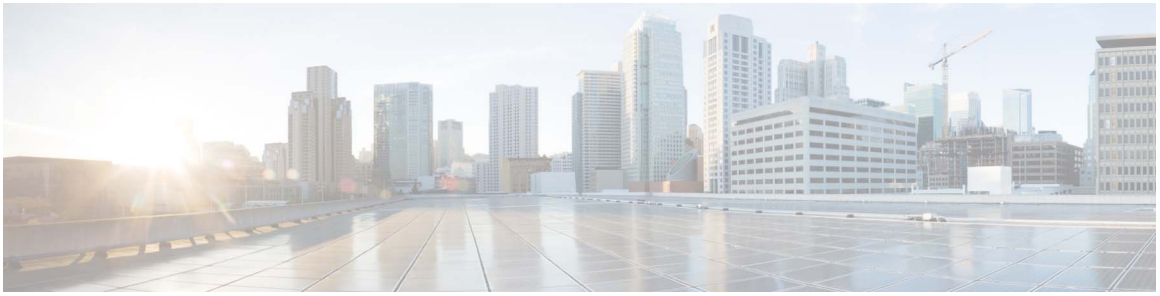
シスコは世界各国 200 箇所にオフィスを開設しています。
住所、電話番号、FAX 番号は
以下のシスコ Web サイトをご覧ください。
www.cisco.com/go/offices

Text Part Number: なし、オンライン専用

Cisco ASA シリーズ VPN CLI コンフィギュレーション ガイド



CONTENTS



このマニュアルについて

マニュアルの目的

このマニュアルの目的は、コマンドライン インターフェイス を使用して適応型セキュリティ アプライアンス（ASA）上で VPN を設定する支援をすることです。このマニュアルは、すべての機能を網羅しているわけではなく、ごく一般的なコンフィギュレーションの事例を紹介しています。

また、Web ベースの GUI アプリケーションである適応型セキュリティ デバイス マネージャ（ASDM）を使用して ASA を設定、監視することもできます。ASDM では、コンフィギュレーション ウィザードを使用して、いくつかの一般的なコンフィギュレーションを設定できます。また、あまり一般的ではない事例には、オンラインのヘルプが用意されています。

このマニュアルは、Cisco ASA シリーズに適用されます。このマニュアルを通じて、「ASA」という語は、特に指定がない限り、サポートされているモデルに一般的に適用されます。

関連資料

詳細については、「*Navigating the Cisco ASA Series Documentation*」（http://www.cisco.com/go/asadocs）を参照してください。

表記法

このマニュアルでは、次の表記法を使用しています。

表記法	説明
太字	コマンド、キーワード、およびユーザが入力するテキストは**太字**で記載されます。
イタリック体	文書のタイトル、新規用語、強調する用語、およびユーザが値を指定する引数は、*イタリック体*で示しています。
[ ]	角カッコの中の要素は、省略可能です。
{x | y | z }	必ずいずれか 1 つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[x | y | z]	いずれか 1 つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
string	引用符を付けない一組の文字。string の前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string とみなされます。
`courier` フォント	システムが表示する端末セッションおよび情報は、`courier` フォントで示しています。
太字の `courier` フォント	コマンド、キーワード、およびユーザが入力したテキストは、**太字の `courier` フォント**で示しています。
イタリック体の `courier` フォント	ユーザが値を指定する引数は、*イタリック体の `courier` フォント*で示しています。
< >	パスワードのように出力されない文字は、山カッコで囲んで示しています。
[ ]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。

（注） 「*注釈*」です。

ヒント 「*問題解決に役立つ情報*」です。

注意 「*要注意*」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『*What's New in Cisco Product Documentation（Cisco 製品資料の更新情報）*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。
http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html

『*What's New in Cisco Product Documentation*』は、シスコの新規および改訂版の技術マニュアルの一覧も示し、RSS フィードとして購読できます。また、リーダー アプリケーションを使用してコンテンツをデスクトップに直接配信することもできます。RSS フィードは無料のサービスです。

PART 1

サイトツーサイトおよびクライアント VPN

IPsec および ISAKMP

リリース：14/07/24

この章では、バーチャル プライベート ネットワーク（VPN）を構築するためにインターネット プロトコル セキュリティ（IPsec）および Internet Security Association and Key Management Protocol（ISAKMP）標準を設定する方法について説明します。

トンネリング、IPsec、および ISAKMP に関する情報

トンネリングは、インターネットなどのパブリック TCP/IP ネットワークを使用して、リモート ユーザとプライベートな企業ネットワークとの間でセキュアな接続を構築することを可能にします。それぞれのセキュアな接続は、トンネルと呼ばれます。

ASA は、ISAKMP と IPsec のトンネリング標準を使用してトンネルの構築と管理を行っています。ISAKMP と IPsec は、次の処理を実行できます。

- トンネル パラメータのネゴシエーション
- トンネルの確立
- ユーザとデータの認証
- セキュリティ キーの管理
- データの暗号化と復号化
- トンネル経由のデータ転送の管理
- トンネル エンドポイントまたはルータとしての着信と発信のデータ転送の管理

ASA は、双方向のトンネル エンドポイントとして機能します。プライベート ネットワークからプレーン パケットを受信してカプセル化し、トンネルを作成して、カプセル化したパケットをトンネルのもう一方の終端に送信します。トンネルの終端では、パケットのカプセル化が解除されて最終的な宛先に送信されます。また、カプセル化されたパケットをパブリック ネットワークから受信してカプセル化を解除し、プライベート ネットワーク上の最終的な宛先に送信します。

IPsec の概要

ASA では、IPsec は LAN-to-LAN VPN 接続に使用され、client-to-LAN VPN 接続にも IPsec を使用できます。IPsec 用語では、*ピア*とは、リモート アクセス クライアントまたは別のセキュアなゲートウェイを意味します。どちらの接続タイプについても、ASA はシスコのピアだけをサポートします。シスコは VPN の業界標準に従っているので、ASA は他ベンダーのピアとの組み合わせでも動作しますが、シスコはこのことをサポートしていません。

トンネルを確立する間に、2 つのピアは、認証、暗号化、カプセル化、キー管理を制御するセキュリティ アソシエーションをネゴシエートします。これらのネゴシエーションには、トンネルの確立（IKE SA）と、トンネル内のトラフィックの制御（IPsec SA）という 2 つのフェーズが含まれます。

LAN-to-LAN VPN は、地理的に異なる場所にあるネットワークを接続します。IPsec LAN-to-LAN 接続では、ASA は発信側または応答側として機能します。IPsec client-to-LAN 接続では、ASA は応答側としてだけ機能します。発信側は SA を提案し、応答側は、設定された SA パラメータに従って、SA の提示を受け入れるか、拒否するか、または対案を提示します。接続を確立するには、両方のエンティティで SA が一致する必要があります。

サイトツーサイト タスクの設定は、シングル コンテキスト モードおよびマルチ コンテキスト モードの両方で実行されます。

（注） マルチ コンテキスト モードが適用されるのは、IKEv2 および IKEv1 のサイトツーサイトのみであり、AnyConnect、クライアントレス SSL VPN、レガシー Cisco VPN クライアント、Apple ネイティブ VPN クライアント、Microsoft ネイティブ VPN クライアント、および IKEv1 IPsec の cTCP には適用されません。

ISAKMP および IKE の概要

ISAKMP は、2 台のホストで IPsec Security Association（SA; セキュリティ アソシエーション）の構築方法を一致させるためのネゴシエーション プロトコルです。これは、SA 属性のフォーマットに合意するための共通のフレームワークを提供します。このセキュリティ アソシエーションには、SA に関するピアとのネゴシエーション、および SA の変更または削除が含まれます。ISAKMP のネゴシエーションは 2 つのフェーズ（フェーズ 1 とフェーズ 2）に分かれています。フェーズ 1 は、以後の ISAKMP ネゴシエーション メッセージを保護する最初のトンネルを作成します。フェーズ 2 では、データを保護するトンネルが作成されます。

IKE は、IPsec を使用するための SA の設定に ISAKMP を使用します。IKE は、ピアの認証に使用される暗号キーを作成します。

ASA は、レガシー Cisco VPN Client から接続するための IKEv1、および AnyConnect VPN クライアントの IKEv2 をサポートしています。

ISAKMP ネゴシエーションの条件を設定するには、IKE ポリシーを作成します。このポリシーには、次のものが含まれます。

- IKEv1 ピアに要求する認証タイプ。証明書を使用する RSA 署名または事前共有キー（PSK）です。
- データを保護しプライバシーを守る暗号化方式。
- 送信者を特定し、搬送中にメッセージが変更されていないことを保証する Hashed Message Authentication Code（HMAC）方式。
- 暗号キー決定アルゴリズムの強度を決定する Diffie-Hellman グループ。このアルゴリズムを使用して、ASA は暗号キーとハッシュ キーを導出します。
- IKEv2 の場合は、別の疑似乱数関数（PRF）。IKEv2 トンネル暗号化などに必要な、キー関連情報とハッシュ操作を導出するためのアルゴリズムとして使用されます。
- この暗号キーを使用する時間の上限。この時間が経過すると ASA は暗号キーを置き換えます。

IKEv1 ポリシーでは、各パラメータに対して 1 個の値を設定します。IKEv2 では、単一のポリシーに対して、複数の暗号化タイプと認証タイプ、および複数の整合性アルゴリズムを設定できます。ASA は、設定をセキュア度が最も高いものから最も低いものに並べ替え、その順序を使用してピアとのネゴシエーションを行います。この並べ替えにより、IKEv1 と同様に、許可される各組み合わせを送信することなく、許可されるすべてのトランスフォームを伝送するために単一のプロポーザルを送信できます。

リモート アクセス IPsec VPN のライセンス要件

次の表に、この機能のライセンス要件を示します。

（注） この機能は、ペイロード暗号化機能のないモデルでは使用できません。

モデル	ライセンス要件[1]
ASA 5505	• IKEv2 を使用した IPsec リモート アクセス VPN（次のいずれかを使用）： – AnyConnect Premium ライセンス： 基本ライセンスと Security Plus ライセンス：2 セッション。 *オプションの永続または時間ベースのライセンス：10 または 25 セッション。* *共有ライセンスはサポートされていません。*[2] – AnyConnect Essentials ライセンス[3]：25 セッション。 • IKEv1 を使用した IPsec リモート アクセス VPN および IKEv1 または IKEv2 を使用した IPsec サイトツーサイト VPN： – 基本ライセンス：10 セッション。 – Security Plus ライセンス：25 セッション。

モデル	ライセンス要件[1]
ASA 5512-X	• IKEv2 を使用した IPsec リモート アクセス VPN（次のいずれかを使用）： – AnyConnect Premium ライセンス： 基本ライセンスと Security Plus ライセンス：2 セッション。 *オプションの永続または時間ベースのライセンス：10、25、50、100、または 250 セッション。* *オプションの共有ライセンス[2]：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。* – AnyConnect Essentials ライセンス[3]：250 セッション。 • IKEv1 を使用した IPsec リモート アクセス VPN および IKEv1 または IKEv2 を使用した IPsec サイトツーサイト VPN： 基本ライセンスと Security Plus ライセンス：250 セッション。
ASA 5515-X	• IKEv2 を使用した IPsec リモート アクセス VPN（次のいずれかを使用）： – AnyConnect Premium ライセンス： 基本ライセンス：2 セッション。 *オプションの永続または時間ベースのライセンス：10、25、50、100、または 250 セッション。* *オプションの共有ライセンス[2]：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。* – AnyConnect Essentials ライセンス[3]：250 セッション。 • IKEv1 を使用した IPsec リモート アクセス VPN および IKEv1 または IKEv2 を使用した IPsec サイトツーサイト VPN： 基本ライセンス：250 セッション。
ASA 5525-X	• IKEv2 を使用した IPsec リモート アクセス VPN（次のいずれかを使用）： – AnyConnect Premium ライセンス： 基本ライセンス：2 セッション。 *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、または 750 セッション。* *オプションの共有ライセンス[2]：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。* – AnyConnect Essentials ライセンス[3]：750 セッション。 • IKEv1 を使用した IPsec リモート アクセス VPN および IKEv1 または IKEv2 を使用した IPsec サイトツーサイト VPN： 基本ライセンス：750 セッション。

モデル	ライセンス要件[1]
ASA 5545-X	• IKEv2 を使用した IPsec リモート アクセス VPN（次のいずれかを使用）： – AnyConnect Premium ライセンス： 基本ライセンス：2 セッション。 *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、750、1000、または 2500 セッション。* *オプションの共有ライセンス[2]：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。* – AnyConnect Essentials ライセンス[3]：2500 セッション。 • IKEv1 を使用した IPsec リモート アクセス VPN および IKEv1 または IKEv2 を使用した IPsec サイトツーサイト VPN： 基本ライセンス：2500 セッション。
ASA 5555-X	• IKEv2 を使用した IPsec リモート アクセス VPN（次のいずれかを使用）： – AnyConnect Premium ライセンス： 基本ライセンス：2 セッション。 *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、750、1000、2500、または 5000 セッション。* *オプションの共有ライセンス[2]：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。* – AnyConnect Essentials ライセンス[3]：5000 セッション。 • IKEv1 を使用した IPsec リモート アクセス VPN および IKEv1 または IKEv2 を使用した IPsec サイトツーサイト VPN： 基本ライセンス：5000 セッション。
ASA 5585-X（SSP-10）	• IKEv2 を使用した IPsec リモート アクセス VPN（次のいずれかを使用）： – AnyConnect Premium ライセンス： 基本ライセンス：2 セッション。 *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、750、1000、2500、または 5000 セッション。* *オプションの共有ライセンス[2]：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。* – AnyConnect Essentials ライセンス[3]：5000 セッション。 • IKEv1 を使用した IPsec リモート アクセス VPN および IKEv1 または IKEv2 を使用した IPsec サイトツーサイト VPN： 基本ライセンス：5000 セッション。

モデル	ライセンス要件[1]
ASA 5585-X（SSP-20、-40、および -60）	• IKEv2 を使用した IPsec リモート アクセス VPN（次のいずれかを使用）： – AnyConnect Premium ライセンス： 基本ライセンス：2 セッション。 *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、750、1000、2500、5000、または 10000 セッション。* *オプションの共有ライセンス[2]：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。* – AnyConnect Essentials ライセンス[3]：10000 セッション。 • IKEv1 を使用した IPsec リモート アクセス VPN および IKEv1 または IKEv2 を使用した IPsec サイトツーサイト VPN： 基本ライセンス：10000 セッション。
ASASM	• IKEv2 を使用した IPsec リモート アクセス VPN（次のいずれかを使用）： – AnyConnect Premium ライセンス： 基本ライセンス：2 セッション。 *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、750、1000、2500、5000、または 10000 セッション。* *オプションの共有ライセンス[2]：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。* – AnyConnect Essentials ライセンス[3]：10000 セッション。 • IKEv1 を使用した IPsec リモート アクセス VPN および IKEv1 または IKEv2 を使用した IPsec サイトツーサイト VPN： 基本ライセンス：10000 セッション。
ASAv（仮想 CPU X 1 を搭載）	• IKEv2 を使用した IPsec リモート アクセス VPN： – 標準ライセンス：2 セッション。 – Premium ライセンス：250 セッション。 • IKEv1 を使用した IPsec リモート アクセス VPN および IKEv1 または IKEv2 を使用した IPsec サイトツーサイト VPN： 標準および Premium ライセンス：250 セッション。
ASAv（仮想 CPU X 4 を搭載）	• IKEv2 を使用した IPsec リモート アクセス VPN： – 標準ライセンス：2 セッション。 – Premium ライセンス：750 セッション。 • IKEv1 を使用した IPsec リモート アクセス VPN および IKEv1 または IKEv2 を使用した IPsec サイトツーサイト VPN： 標準および Premium ライセンス：750 セッション。

1. すべてのタイプの組み合わせ VPN セッションの最大数は、この表に示す最大セッション数を超えることはできません。ASA 5505 では、組み合わせセッションの最大数は 10（基本ライセンスの場合）または 25（Security Plus ライセンスの場合）です。
2. 共有ライセンスによって、ASA は複数のクライアントの ASA の共有ライセンス サーバとして機能します。共有ライセンス プールは大規模ですが、個々の ASA によって使用されるセッションの最大数は、永続的なライセンスで指定される最大数を超えることはできません。

3. AnyConnect Essentials ライセンスにより、AnyConnect VPN クライアントは ASA へのアクセスが可能になります。このライセンスでは、ブラウザベースの SSL VPN アクセスまたは Cisco Secure Desktop はサポートされていません。これらの機能に対しては、AnyConnect Essentials ライセンスの代わりに AnyConnect Premium ライセンスがアクティブ化されます。

   （注）AnyConnect Essentials ライセンスの場合、VPN ユーザは、Web ブラウザを使用してログインし、AnyConnect クライアントのダウンロードと起動（WebLaunch）を実行できます。

   このライセンスと AnyConnect Premium SSL VPN ライセンスのいずれでイネーブル化されたかには関係なく、AnyConnect クライアント ソフトウェアには同じクライアント機能のセットが装備されています。

   特定の ASA では、AnyConnect Premium ライセンス（全タイプ）または Advanced Endpoint Assessment ライセンスを、AnyConnect Essentials ライセンスと同時にアクティブにすることはできません。ただし、同じネットワーク内の異なる ASA で、AnyConnect Essentials ライセンスと AnyConnect Premium ライセンスを実行することは可能です。

   デフォルトでは、ASA は AnyConnect Essentials ライセンスを使用しますが、**webvpn** を使用し、次に **no anyconnect-essentials** コマンド を使用すると、AnyConnect Essentials ライセンスをディセーブルにして他のライセンスを使用できます。

   AnyConnect Essentials ライセンスおよび AnyConnect Premium ライセンスでサポートされている機能の詳細なリストについては、『*AnyConnect Secure Mobility Client Features, Licenses, and OSs*』を参照してください。

   http://www.cisco.com/en/US/products/ps10884/products_feature_guides_list.html

ガイドラインと制限事項

この項では、この機能のガイドラインと制限事項について説明します。

コンテキスト モードのガイドライン

シングルまたはマルチ コンテキスト モードでサポートされます。

ファイアウォール モードのガイドライン

ルーテッド ファイアウォール モードでだけサポートされています。トランスペアレント ファイアウォール モードはサポートされません。

フェールオーバーのガイドライン

IPsec VPN セッションは、アクティブ/スタンバイ フェールオーバー コンフィギュレーションでのみ複製されます。

IPv6 のガイドライン

IPv6 はサポートされません。

ISAKMP の設定

ここでは、Internet Security Association and Key Management Protocol（ISAKMP）とインターネット キー交換（IKE）プロトコルについて説明します。

IKEv1 および IKEv2 のポリシーの設定

IKE ポリシーを作成するには、シングルまたはマルチ コンテキスト モードのグローバル コンフィギュレーション モードで **crypto** ***ikev1*** **|** ***ikev2*** **policy** コマンドを入力します。プロンプトは、IKE ポリシー コンフィギュレーション モードを表示します。次に例を示します。

```
hostname(config)# crypto ikev1 policy 1
hostname(config-ikev1-policy)#
```

ポリシーを作成した後は、そのポリシーの設定を指定できます。

表 1-1 および表 1-2 に、IKEv1 ポリシーと IKEv2 ポリシーのキーワードおよび値を示します。

表 1-1　CLI コマンド用の IKEv1 ポリシー キーワード

コマンド	キーワード	意味	説明
authentication	**rsa-sig**	RSA 署名アルゴリズムによって生成されたキー付きのデジタル証明書	各 IPsec ピアの ID を確立するために ASA が使用する認証方式を指定します。
	crack	Challenge/Response for Authenticated Cryptographic Keys	CRACK は、クライアントが RADIUS などのレガシーな認証方式を使用し、サーバが公開キーによる認証方式を使用している場合に、強力な相互認証を実現します。
	pre-share (デフォルト)	事前共有キー	事前共有キーは、拡大するネットワークに対応した拡張は困難ですが、小規模ネットワークではセットアップが容易です。
encryption	**des**	56 ビット DES-CBC	2 つの IPsec ピア間で伝送されるユーザ データを保護する対称暗号化アルゴリズムを指定します。デフォルトは 168 ビット Triple DES です。
	3des（デフォルト）	168 ビット Triple DES	
hash	**sha**（デフォルト）	SHA-1（HMAC バリアント）	データ整合性の確保のために使用するハッシュ アルゴリズムを指定します。パケットがそのパケットに記されている発信元から発信されたこと、また搬送中に変更されていないことを保証します。
	md5	MD5（HMAC バリアント）	デフォルト値は SHA-1 です。MD5 のダイジェストの方が小さく、SHA-1 よりもやや速いと見なされています。しかし、MD5 に対する攻撃が成功（これは非常に困難）しても、IKE が使用する HMAC バリアントがこの攻撃を防ぎます。

表 1-1　CLI コマンド用の IKEv1 ポリシー キーワード（続き）

コマンド	キーワード	意味	説明
group	**1**	グループ 1（768 ビット）	Diffie-Hellman グループ ID を指定します。この ID は、2 つの IPsec ピアが、相互に共有秘密情報を転送するのではなく、共有秘密情報を取り出すために使用します。 Diffie-Hellman グループ番号が小さいほど、実行に必要な CPU 時間も少なくなります。Diffie-Hellman グループ番号が大きいほど、セキュリティも高くなります。 AES は、VPN-3DES のライセンスがあるセキュリティ アプライアンスに限りサポートされます。AES で必要なより大きいキー長をサポートするには、ISAKMP ネゴシエーションで Diffie-Hellman（DH）のグループ 5 を使用する必要があります。
	2（デフォルト）	グループ 2（1024 ビット）	
	5	グループ 5（1536 ビット）	
lifetime	**整数値** (86400 = デフォルト)	120 ～ 2147483647 秒	SA ライフタイムを指定します。デフォルトは 86,400 秒、つまり 24 時間です。原則として、ライフタイムが短いほど、ISAKMP ネゴシエーションの安全性は（ある程度まで）高くなります。ただし、ライフタイムが短いほど、ASA による IPsec SA のセットアップ機能が高速になります。

表 1-2　CLI コマンド用の IKEv2 ポリシー キーワード

コマンド	キーワード	意味	説明
integrity	**sha**（デフォルト）	SHA-1（HMAC バリアント）	データ整合性の確保のために使用するハッシュ アルゴリズムを指定します。パケットがそのパケットに記されている発信元から発信されたこと、また搬送中に変更されていないことを保証します。
	md5	MD5（HMAC バリアント）	デフォルト値は SHA-1 です。MD5 のダイジェストの方が小さく、SHA-1 よりもやや速いと見なされています。MD5 に対する攻撃の成功例がありますが（これは非常に困難ですが）、IKE が使用する HMAC バリアントがこの攻撃を防ぎます。
	sha256	SHA 2、256 ビットのダイジェスト	256 ビットのダイジェストでセキュア ハッシュ アルゴリズム SHA 2 を指定します。
	sha384	SHA 2、384 ビットのダイジェスト	384 ビットのダイジェストでセキュア ハッシュ アルゴリズム SHA 2 を指定します。
	sha512	SHA 2、512 ビットのダイジェスト	512 ビットのダイジェストでセキュア ハッシュ アルゴリズム SHA 2 を指定します。
	null		AES-GCM が暗号化アルゴリズムとして指定されているときは、IKEv2 整合性アルゴリズムとしてヌルを選択できます。
encryption	**des**	56 ビット DES-CBC	2 つの IPsec ピア間で伝送されるユーザ データを保護する対称暗号化アルゴリズムを指定します。デフォルトは 168 ビット Triple DES です。
	3des（デフォルト）	168 ビット Triple DES	

表 1-2　CLI コマンド用の IKEv2 ポリシー キーワード（続き）

コマンド	キーワード	意味	説明
	aes **aes-192** **aes-256**		Advanced Encryption Standard（AES）は、128 ビット、192 ビット、256 ビットの長さのキーをサポートしています。
	aes-gcm **aes-gcm-192** **aes-gcm-256** **null**	IKEv2 暗号化に使用する AES-GCM アルゴリズムのオプション	Advanced Encryption Standard（AES）は、128 ビット、192 ビット、256 ビットの長さのキーをサポートしています。
policy_index			IKEv2 ポリシー サブモードにアクセスします。
prf	**sha**（デフォルト）	SHA-1（HMAC バリアント）	疑似乱数関数（PRF）を指定します。これは、キー関連情報を生成するために使用されるアルゴリズムです。
	md5	MD5（HMAC バリアント）	デフォルト値は SHA-1 です。MD5 のダイジェストの方が小さく、SHA-1 よりもやや速いと見なされています。しかし、MD5 に対する攻撃が成功（これは非常に困難）しても、IKE が使用する HMAC バリアントがこの攻撃を防ぎます。
	sha256	SHA 2、256 ビットのダイジェスト	256 ビットのダイジェストでセキュア ハッシュ アルゴリズム SHA 2 を指定します。
	sha384	SHA 2、384 ビットのダイジェスト	384 ビットのダイジェストでセキュア ハッシュ アルゴリズム SHA 2 を指定します。
	sha512	SHA 2、512 ビットのダイジェスト	512 ビットのダイジェストでセキュア ハッシュ アルゴリズム SHA 2 を指定します。
priority			ポリシー モードを拡張します。追加の IPsec V3 機能がサポートされ、AES-GCM および ECDH の設定が Suite B サポートに含まれるようになります。
group	1	グループ 1（768 ビット）	Diffie-Hellman グループ ID を指定します。この ID は、2 つの IPsec ピアが、相互に共有秘密情報を転送するのではなく、共有秘密情報を取り出すために使用します。
	2（デフォルト）	グループ 2（1024 ビット）	
	5	グループ 5（1536 ビット）	Diffie-Hellman グループ番号が小さいほど、実行に必要な CPU 時間も少なくなります。Diffie-Hellman グループ番号が大きいほど、セキュリティも高くなります。
	14 **19** **20** **21** **24**		AnyConnect クライアントは、非 FIPS モードで DH グループ 1、2、および 5 をサポートし、FIPS モードではグループ 2 だけをサポートします。
			AES は、VPN-3DES のライセンスがあるセキュリティ アプライアンスに限りサポートされます。AES で必要なより大きいキー長をサポートするには、ISAKMP ネゴシエーションで Diffie-Hellman（DH）のグループ 5 を使用する必要があります。
lifetime	**整数値** (86400 = デフォルト)	120 ～ 2147483647 秒	SA ライフタイムを指定します。デフォルトは 86,400 秒、つまり 24 時間です。原則として、ライフタイムが短いほど、ISAKMP ネゴシエーションの安全性は（ある程度まで）高くなります。ただし、ライフタイムが短いほど、ASA による IPsec SA のセットアップ機能が高速になります。

IKEv1 と IKEv2 はどちらも、最大 20 個の IKE ポリシーをサポートしますが、値のセットはそれぞれ異なります。作成するポリシーのそれぞれに、固有のプライオリティを割り当てます。プライオリティ番号が小さいほど、プライオリティが高くなります。

IKE ネゴシエーションが始まると、ネゴシエーションを開始したピアはそのすべてのポリシーをリモート ピアに送信し、リモート ピアは一致するポリシーを探します。リモート ピアは、一致するポリシーを見つけるまで、設定済みのポリシーに対してピアのすべてのポリシーを 1 つずつプライオリティ順に（最も高いプライオリティから）照合します。

一致と見なされるのは、2 つのピアからの両方のポリシーに、同じ暗号化、ハッシュ、認証、Diffie-Hellman パラメータ値が含まれているときです。IKEv1 では、リモート ピアのポリシーで指定されているライフタイムが、開始側から送信されたポリシーのライフタイム以下であることも必要です。ライフタイムが等しくない場合、ASA は短い方のライフタイムを使用します。IKEv2 では、ライフタイムはネゴシエートされませんが、各ピアの間でローカルに管理されるので、ライフタイムを各ピアで個別に設定できます。一致するポリシーがない場合、IKE はネゴシエーションを拒否し、SA は確立されません。

各パラメータに対して特定の値を選択するときは、セキュリティとパフォーマンスの間に暗黙のトレードオフが発生します。デフォルト値で得られるセキュリティ レベルは、ほとんどの組織のセキュリティ要件に十分に対応します。パラメータに対し 1 つの値だけをサポートしているピアと相互運用する場合は、相手のピアがサポートしている値に選択が制限されます。

（注） 新しい ASA コンフィギュレーションには、デフォルトの IKEv1 や IKEv2 のポリシーはありません。

IKE ポリシーを設定するには、グローバル コンフィギュレーション モードで、**crypto *ikev1* | *ikev2* policy** *priority* コマンドを使用して IKE ポリシー コンフィギュレーション モードを開始します。

ISAKMP コマンドには、それぞれプライオリティを指定する必要があります。プライオリティ番号によってポリシーが一意に識別され、IKE ネゴシエーションにおけるポリシーのプライオリティが決定されます。

IKE をイネーブルにして設定するには、次の手順を実行します。ここでは、IKEv1 の例を示します。

（注） 所定のポリシー パラメータに値を指定しない場合、デフォルト値が適用されます。

ステップ 1　IKEv1 ポリシー コンフィギュレーション モードを開始します。

```
hostname(config)# crypto ikev1 policy 1
hostname(config-ikev1-policy)#
```

ステップ 2　暗号化アルゴリズムを指定します。デフォルトは Triple DES です。この例では、暗号化を DES に設定します。

```
encryption [aes | aes-192 | aes-256 | des | 3des]
```

次に例を示します。

```
hostname(config-ikev1-policy)# encryption des
```

ステップ 3　ハッシュ アルゴリズムを指定します。デフォルト値は SHA-1 です。この例では、MD5 を設定します。

```
hash [md5 | sha]
```

次に例を示します。

```
hostname(config-ikev1-policy)# hash md5
```

ステップ 4　認証方式を指定します。デフォルトは事前共有キーです。この例では、RSA 署名を設定します。

authentication [pre-share | crack | rsa-sig]

次に例を示します。

```
hostname(config-ikev1-policy)# authentication rsa-sig
```

ステップ 5　Diffie-Hellman グループ識別番号を指定します。デフォルトはグループ 2 です。この例では、グループ 5 を設定します。

group [1 | 2 | 5]

次に例を示します。

```
hostname(config-ikev1-policy)# group 5
```

ステップ 6　SA ライフタイムを指定します。この例では、4 時間（14400 秒）のライフタイムを設定します。デフォルトは 86400 秒（24 時間）です。

lifetime *seconds*

次に例を示します。

```
hostname(config-ikev1-policy)# lifetime 14400
```

外部インターフェイスでの IKE のイネーブル化

VPN トンネルの終端となるインターフェイスで、IKE をイネーブルにする必要があります。通常は外部（つまり、パブリック）インターフェイスです。IKEv1 または IKEv2 をイネーブルにするには、**crypto** ***ikev1*** **|** ***ikev2*** **enable** *interface-name* コマンドを、シングルまたはマルチ コンテキスト モードのグローバル コンフィギュレーション モードで実行します。

次に例を示します。

```
hostname(config)# crypto ikev1 enable outside
```

IKEv1 アグレッシブ モードのディセーブル化

フェーズ 1 の IKEv1 ネゴシエーションでは、メイン モードとアグレッシブ モードのどちらも使用できます。どちらのモードも同じサービスを提供しますが、アグレッシブ モードではピア間の交換が 2 回だけ必要で、合計 3 メッセージとなります（交換が 3 回で、合計 6 メッセージではありません）。アグレッシブ モードの方が高速ですが、通信パーティの ID は保護されません。このため、セキュアな SA を確立する前に、ピア間で ID 情報を交換する必要があります。アグレッシブ モードは、デフォルトでイネーブルになっています。

- 交換回数の多いメイン モードは低速ですが、通信しているピアの ID を保護します。
- アグレッシブ モードは高速ですが、ピアの ID を保護しません。

アグレッシブ モードをディセーブルにするには、シングルまたはマルチ コンテキスト モードで次のコマンドを入力します。

crypto ikev1 am-disable

次に例を示します。

```
hostname(config)# crypto ikev1 am-disable
```

アグレッシブ モードをいったんディセーブルにした後でイネーブルに戻すには、**no** 形式でコマンドを使用します。次に例を示します。

```
hostname(config)# no crypto ikev1 am-disable
```

（注）　アグレッシブ モードをディセーブルにすると、Cisco VPN Client は、ASA へのトンネルを確立するための事前共有キー認証を使用できなくなります。ただし、証明書に基づく認証（つまり ASA または RSA）を使用してトンネルを確立できます。

IKEv1 および IKEv2 ISAKMP ピアの識別方式の決定

ISAKMP フェーズ I ネゴシエーション中に、IKEv1 と IKEv2 のどちらの場合も、ピアが互いを識別する必要があります。この識別方式は、次のオプションから選択できます。

アドレス	ISAKMP の識別情報を交換するホストの IP アドレスを使用します。
自動	接続タイプによって ISAKMP ネゴシエーションが決まります。 • 事前共有キーの IP アドレス • 証明書認証の証明書認定者名
ホスト名	ISAKMP の識別情報を交換するホストの完全修飾ドメイン名を使用します（デフォルト）。この名前は、ホスト名とドメイン名で構成されます。
キー ID *key_id_string*	リモート ピアが事前共有キーを検索するために使用するストリングを指定します。

ASA は、ピアに送信するフェーズ I の ID を使用します。これは、事前共有キーで認証を行うメイン モードでの LAN-to-LAN IKEv1 接続を除いて、すべての VPN シナリオで行われます。

デフォルトの設定は「自動」です。

ピア識別方式を変更するには、シングルまたはマルチ コンテキスト モードで次のコマンドを入力します。

```
crypto isakmp identity {address | hostname | key-id id-string | auto}
```

たとえば、次のコマンドはピア識別方式を「ホスト名」に設定します。

```
hostname(config)# crypto isakmp identity hostname
```

IPsec over NAT-T のイネーブル化

NAT-T を使用すると、IPsec ピアは NAT デバイスを介した接続を確立できます。このことを実現するために、IPsec トラフィックが UDP データグラムとしてカプセル化されます。これにはポート 4500 が使用されるので、これによって、NAT デバイスにポート情報が提供されます。NAT-T は NAT デバイスを自動検出し、必要な場合だけ IPsec トラフィックをカプセル化します。この機能はデフォルトで無効に設定されています。

（注）　AnyConnect クライアントの制限により、AnyConnect クライアントが IKEv2 を使用して接続できるようにするには NAT-T のイネーブル化が必要になります。この要件は、クライアントが NAT-T デバイスの背後になくても適用されます。

ASA は、データ交換を行うクライアントに応じて、標準の IPSec、IPSec over TCP、NAT-T、および IPSec over UDP を同時にサポートできます。

各オプションがイネーブルのときの接続の状態を次に示します。

オプション	イネーブルの機能	クライアントの位置	使用する機能
オプション 1	NAT-T がイネーブル	およびクライアントが NAT の背後にある場合は	NAT-T が使用される
		および NAT が存在しない場合は	ネイティブ IPsec（ESP）が使用される
オプション 2	IPsec over UDP がイネーブル	およびクライアントが NAT の背後にある場合は、	IPsec over UDP が使用される
		および NAT が存在しない場合は	IPsec over UDP が使用される
オプション 3	NAT-T と IPsec over UDP の両方がイネーブル	およびクライアントが NAT の背後にある場合は	NAT-T が使用される
		および NAT が存在しない場合は	IPsec over UDP が使用される

（注） IPsec over TCP がイネーブルになっている場合は、その他のすべての接続方式よりも優先されます。

NAT-T をイネーブルにすると、ASA は自動的に、IPsec がイネーブルになっているすべてのインターフェイス上でポート 4500 を開きます。

ASA は、次の両方のネットワークではなく、どちらか一方のネットワークで動作する単一の NAT/PAT デバイスの背後にある複数の IPsec ピアをサポートします。

- LAN-to-LAN
- リモート アクセス

混合環境では、リモート アクセス トンネルのネゴシエーションに失敗します。これは、すべてのピアが同じパブリック IP アドレス、つまり NAT デバイスのアドレスから発信されたように見えるためです。また、リモート アクセス トンネルは、LAN-to-LAN トンネル グループ（つまり NAT デバイスの IP アドレス）と同じ名前を使用することが多いため、混合環境では失敗します。この名前の一致により、NAT デバイスの背後にあるピアの LAN-to-LAN とリモート アクセスの混合ネットワークでは、複数のピア間のネゴシエーションが失敗する場合があります。

NAT-T の使用

NAT-T を使用するには、次のサイトツーサイトの手順をシングルまたはマルチ コンテキスト モードで実行する必要があります。

ステップ 1　次のコマンドを入力して、ASA 上でグローバルに IPsec over NAT-T をイネーブルにします。

crypto isakmp nat-traversal *natkeepalive*

natkeepalive 引数の範囲は 10 ～ 3600 秒です。デフォルトは 20 秒です。

たとえば、次のコマンドを入力して、NAT-T をイネーブルにし、キープアライブ値を 1 時間に設定します。

```
hostname(config)# crypto isakmp nat-traversal 3600
```

ステップ 2　IPsec フラグメンテーション ポリシーに対して暗号化前オプションを選択するために、次のコマンドを入力します。

```
hostname(config)# crypto ipsec fragmentation before-encryption
```

このオプションは、IP フラグメンテーションをサポートしていない NAT デバイス間をトラフィックが通過できるようにします。このオプションを使用しても、IP フラグメンテーションをサポートしていない NAT デバイスの動作を妨げることはありません。

IPsec with IKEv1 over TCP のイネーブル化

IPsec/IKEv1 over TCP を使用すると、標準の ESP や IKEv1 が機能できない環境や、既存のファイアウォール ルールを変更した場合に限って機能できる環境で、Cisco VPN クライアントが動作できるようになります。IPsec over TCP は、IKEv1 と IPsec の両方のプロトコルを TCP に似たパケットの中にカプセル化するものであり、NAT と PAT の両方のデバイスとファイアウォールを通過するセキュアなトンネリングを実現します。この機能はデフォルトで無効に設定されています。

（注）　この機能は、プロキシベースのファイアウォールでは動作しません。

IPsec over TCP は、リモート アクセス クライアントで動作します。イネーブル化はグローバルに行います。IKEv1 がイネーブルになっているすべてのインターフェイスで動作します。これは、ASA の機能に対するクライアントにすぎません。LAN-to-LAN 接続では機能しません。

ASA は、データ交換を行うクライアントに応じて、標準の IPsec、IPsec over TCP、NAT-Traversal、および IPsec over UDP を同時にサポートできます。IPsec over TCP は、イネーブルになっている場合、その他のすべての接続方式よりも優先されます。

1 度に 1 つのトンネルをサポートする VPN 3002 ハードウェア クライアントは、標準の IPsec、IPsec over TCP、NAT-Traversal、または IPsec over UDP を使用して接続できます。

ASA とその接続先のクライアントの両方で IPsec over TCP をイネーブルにします。

最大 10 個のポートを指定して、それらのポートに対して IPsec over TCP をイネーブルにできます。ポート 80（HTTP）やポート 443（HTTPS）などの周知のポートを入力すると、そのポートに関連付けられているプロトコルがパブリック インターフェイスで機能しなくなることを示すアラートが表示されます。その結果、パブリック インターフェイスを介して ASA を管理するためにブラウザを使用することができなくなります。この問題を解決するには、HTTP/HTTPS 管理を別のポートに再設定します。

デフォルトのポートは 10000 です。

ASA だけでなく、クライアントでも TCP ポートを設定する必要があります。クライアントの設定には、ASA 用に設定したポートを少なくとも 1 つ含める必要があります。

IKEv1 の IPsec over TCP を ASA でグローバルにイネーブルにするには、次のコマンドをシングルまたはマルチ コンテキスト モードで実行します。

```
crypto ikev1 ipsec-over-tcp [port port 1...port0]
```

次の例では、IPsec over TCP をポート 45 でイネーブルにしています。

```
hostname(config)# crypto ikev1 ipsec-over-tcp port 45
```

リブートの前にアクティブ セッションの終了を待機

すべてのアクティブ セッションが自発的に終了したら ASA をリブートするように、スケジュールを設定できます。この機能はデフォルトで無効に設定されています。

すべてのアクティブ セッションが自発的に終了するのを待って ASA をリブートする機能をイネーブルにするには、次のサイトツーサイト タスクをシングルまたはマルチ コンテキスト モードで実行します。

crypto isakmp reload-wait

次に例を示します。

```
hostname(config)# crypto isakmp reload-wait
```

reload コマンドを使用して、ASA をリブートします。**reload-wait** コマンドを設定する場合、**reload quick** コマンドを使用して **reload-wait** 設定を無効にできます。**reload** コマンドと **reload-wait** コマンドは特権 EXEC モードで使用できます。どちらにも **isakmp** プレフィックスは付けません。

接続解除の前にピアに警告

リモート アクセスや LAN-to-LAN のセッションがドロップする理由には、さまざまなものがあります。たとえば、ASA のシャットダウンまたはリブート、セッション アイドル タイムアウト、最大接続時間の超過、管理者による停止です。

ASA は、限定されたピア、つまり Cisco VPN Client と VPN 3002 ハードウェア クライアントに対して、セッションが接続解除される直前に通知できます（LAN-to-LAN コンフィギュレーションの場合）。アラートを受信したピアまたはクライアントは、その理由を復号化してイベント ログまたはポップアップ ペインに表示します。この機能はデフォルトで無効に設定されています。

限定されたクライアントとピアには次のものが含まれます。

- アラートがイネーブルになっているセキュリティ アプライアンス
- Cisco VPN Client のうち、バージョン 4.0 以降のソフトウェアを実行しているもの（コンフィギュレーションは不要）
- VPN 3002 ハードウェア クライアントのうち、バージョン 4.0 以降のソフトウェアを実行し、アラートがイネーブルになっているもの
- VPN 3000 シリーズ コンセントレータのうち、バージョン 4.0 以降のソフトウェアを実行し、アラートがイネーブルになっているもの

IPsec ピアへの切断通知をイネーブルにするには、**crypto isakmp disconnect-notify** コマンドをシングルまたはマルチ コンテキスト モードで入力します。

次に例を示します。

```
hostname(config)# crypto isakmp disconnect-notify
```

IKEv1 の証明書グループ照合の設定

トンネル グループは、ユーザの接続条件とアクセス権を定義します。証明書グループ照合では、ユーザ証明書のサブジェクト DN または発行者 DN を使用して、ユーザとトンネル グループを照合します。

（注）　証明書グループ照合は IKEv1 と IKEv2 LAN-to-LAN 接続だけに適用されます。IKEv2 リモート アクセス接続は、トンネルグループの webvpn 属性および certificate-group-map の webvpn コンフィギュレーション モードなどに設定されるグループ選択のプルダウンをサポートしています。

証明書のこれらのフィールドに基づいてユーザをトンネル グループと照合するには、まず照合基準を定義したルールを作成し、次に各ルールを目的のトンネル グループに関連付ける必要があります。

証明書マップを作成するには、**crypto ca certificate map** コマンドを使用します。トンネル グループを定義するには、**tunnel-group** コマンドを使用します。

また、証明書グループ照合ポリシーも設定する必要があります。これには、ルールからグループを照合する、組織ユニット（OU）フィールドからグループを照合する、すべての証明書ユーザにデフォルトのグループを使用する、という方式があります。これらの方式のいずれかまたはすべてを使用できます。

次の項でさらに詳しく説明します。

- 「証明書グループ照合のルールとポリシーの作成」（P.1-17）
- 「tunnel-group-map default-group コマンドの使用」（P.1-18）

証明書グループ照合のルールとポリシーの作成

証明書ベースの ISAKMP セッションをトンネル グループにマッピングするためのポリシーとルールを設定し、証明書マップ エントリをトンネル グループに関連付けるには、**tunnel-group-map** コマンドをシングルまたはマルチ コンテキスト モードで入力します。

このコマンドの構文は次のとおりです。

tunnel-group-map enable {*rules* | *ou* | *ike-id* | *peer ip*}

tunnel-group-map [*rule-index*] **enable** *policy*

policy	証明書からトンネル グループ名を取得するためのポリシーを指定します。*policy* は次のいずれかです。 *ike-id*：トンネル グループがルール検索に基づいて特定されず、OU からも取得されない場合に、証明書ベースの ISAKMP セッションをフェーズ 1 ISAKMP ID の内容に基づいてトンネル グループにマッピングすることを示します。 *ou*：トンネル グループをルール検索によって決定しない場合、サブジェクト認定者名（DN）の OU の値を使用することを示します。 *peer-ip*：トンネル グループをルール検索によって決定しない場合や OU または ike-id 方式で取得しない場合、ピアの IP アドレスを使用することを示します。 *rules*：証明書ベースの ISAKMP セッションが、このコマンドによって設定された証明書マップの関連付けに基づいて、トンネル グループにマッピングされることを示します。

rule index	（オプション）**crypto ca certificate map** コマンドで指定したパラメータを参照します。有効な値は 1 ～ 65535 です。

次のことに注意してください。

- 各呼び出しが一意であり、マップ インデックスを 2 回以上参照しない限り、このコマンドを複数回実行できます。
- ルールは 255 文字以下です。
- 1 つのグループに複数のルールを割り当てられます。複数のルールを割り当てるには、まずルールのプライオリティを追加し、グループ化します。次に、各グループに必要な数だけ基準文を定義します。1 つのグループに複数のルールを割り当てた場合、テストされる最初のルールの照合結果は一致します。
- ルールを 1 つだけ作成すると、すべての条件に一致したときにのみユーザを特定のトンネル グループに割り当てることができるようになります。すべての照合基準が必要であることは、論理 AND 操作に相当します。または、ユーザを特定のトンネル グループに割り当てる前に 1 つだけの照合基準が必要な場合は、基準ごとに 1 つのルールを作成します。照合基準が 1 つだけ必要であることは、論理 OR 操作に相当します。

次の例では、フェーズ 1 の ISAKMP ID の内容に基づいて、証明書ベースの ISAKMP セッションをトンネル グループにマッピングする機能をイネーブルにします。

```
hostname(config)# tunnel-group-map enable ike-id
hostname(config)#
```

次の例では、ピアの IP アドレスに基づいて、証明書ベースの ISAKMP セッションをトンネル グループにマッピングする機能をイネーブルにします。

```
hostname(config)# tunnel-group-map enable peer-ip
hostname(config)#
```

次の例では、サブジェクト認定者名（DN）の組織ユニット（OU）に基づいて、証明書ベースの ISAKMP セッションをマッピングする機能をイネーブルにします。

```
hostname(config)# tunnel-group-map enable ou
hostname(config)#
```

次の例では、設定されたルールに基づいて、証明書ベースの ISAKMP セッションをマッピングする機能をイネーブルにします。

```
hostname(config)# tunnel-group-map enable rules
hostname(config)#
```

tunnel-group-map default-group コマンドの使用

このコマンドは、コンフィギュレーションにトンネル グループが指定されていない場合に使用する、デフォルトのトンネル グループを指定します。

コマンドの構文は、**tunnel-group-map** [*rule-index*] **default-group** *tunnel-group-name* です。*rule-index* はルールのプライオリティで、*tunnel-group name* は既存のトンネル グループ名である必要があります。

IPsec の設定

この項では、IPsec に関する背景情報と、IPsec を使用して VPN を実装するときに ASA を設定する手順について説明します。

IPsec トンネルの概要

IPsec トンネルとは、ASA がピア間に確立する SA のセットのことです。SA とは、機密データに適用するプロトコルとアルゴリズムを指定するものであり、ピアが使用するキー関連情報も指定します。IPsec SA は、ユーザ トラフィックの実際の伝送を制御します。SA は単方向ですが、通常ペア（着信と発信）で確立されます。

ピアは SA ごとに使用する設定をネゴシエートします。各 SA は次のもので構成されます。

- IKEv1 トランスフォーム セットまたは IKEv2 プロポーザル
- クリプト マップ
- ACL
- トンネル グループ
- 事前フラグメンテーション ポリシー

IKEv1 トランスフォーム セットおよび IKEv2 プロポーザルの概要

IKEv1 トランスフォーム セットや IKEv2 プロポーザルは、ASA によるデータ保護の方法を定義するセキュリティ プロトコルとアルゴリズムの組み合わせです。IPsec SA のネゴシエート時に、ピアはそれぞれトランスフォーム セットまたはプロポーザルを指定しますが、これは両ピアで同一であることが必要です。ASA は、この一致しているトランスフォーム セットまたはプロポーザルを使用して SA を作成し、この SA によってクリプト マップに対する ACL のデータ フローが保護されます。

IKEv1 トランスフォーム セットでは、各パラメータに対して 1 個の値を設定します。IKEv2 プロポーザルでは、単一のプロポーザルに対して、複数の暗号化および認証のタイプ、および複数の整合性アルゴリズムを設定できます。ASA は、設定をセキュア度が最も高いものから最も低いものに並べ替え、その順序を使用してピアとのネゴシエーションを行います。これによって、IKEv1 と同様に、許可される各組み合わせを個別に送信することなく、許可されるすべての組み合わせを伝送するために単一のプロポーザルを送信できます。

SA の作成に使用されたトランスフォーム セットまたはプロポーザルの定義が変更された場合は、ASA はトンネルを切断します。詳細については、「セキュリティ アソシエーションのクリア」（P.1-39）を参照してください。

（注）　トランスフォーム セットまたはプロポーザルの唯一の要素が消去または削除された場合は、ASA はそのトランスフォーム セットまたはプロポーザルを参照するクリプト マップを自動的に削除します。

クリプト マップの定義

*クリプト マップ*は、IPsec SA でネゴシエートされる IPsec ポリシーを定義します。これには次のものが含まれます。

- IPsec 接続が許可および保護するパケットを識別するための ACL。
- ピア ID。
- IPsec トラフィックのローカル アドレス （詳細については、「クリプト マップのインターフェイスへの適用」（P.1-29）を参照してください）。
- 最大 11 個の IKEv1 トランスフォーム セットまたは IKEv2 プロポーザル。ピアのセキュリティ設定の照合に使用されます。

*クリプト マップ セット*は、同じマップ名を持つ 1 つまたは複数のクリプト マップで構成されます。最初のクリプト マップを作成したときに、クリプト マップ セットを作成します。次のサイトツーサイト タスクでは、シングルまたはマルチ コンテキスト モードでクリプト マップを作成またはクリプト マップに追加します。

crypto map *map-name seq-num* **match address** *access-list-name*

access-list-name では、ACL ID を、最大 241 文字の文字列または整数として指定します。

ヒント　すべて大文字にすると、ACL ID がコンフィギュレーション内で見つけやすくなります。

このコマンドを続けて入力すると、クリプト マップをクリプト マップ セットに追加できます。次の例では、クリプト マップを追加するクリプト マップ セットの名前は *mymap* です。

```
crypto map mymap 10 match address 101
```

上記の構文に含まれる*シーケンス番号*（*seq-num*）によって、同じ名前を持つクリプト マップがそれぞれ区別されます。クリプト マップに割り当てられているシーケンス番号によって、クリプト マップ セット内のクリプト マップ間のプライオリティが決まります。シーケンス番号が小さいほど、プライオリティが高くなります。クリプト マップ セットをインターフェイスに割り当てると、ASA は、そのインターフェイスを通過するすべての IP トラフィックとクリプト マップ セット内のクリプト マップを、シーケンス番号が低い順に照合して評価します。

[no] crypto map *map_name map_index* **set pfs [group1 | group2 | group5 | group14 | group19 | group20 | group21 | group24]**

暗号化マップの完全転送秘密（FCS）に使用する ECDH グループを指定します。暗号化マップに対して group14 および group24 オプションを設定することはできなくなります（IKEv1 ポリシーを使用するとき）。

[no]crypto map *name priority* **set validate-icmp-errors**
または
[no]crypto dynamic-map *name priority* **set validate-icmp-errors**

着信 ICMP エラー メッセージを、暗号化マップとダイナミック暗号化マップのどちらに対して検証するかを指定します。

```
[no] crypto map <name> <priority> set df-bit [clear-df | copy-df | set-df}
または
[no] crypto map dynamic-map <name> <priority> set df-bit [clear-df | copy-df | set-df]
```

暗号化マップまたはダイナミック暗号化マップの、既存の Do Not Fragment（DF）ポリシー（セキュリティ アソシエーション レベル）を設定します。

- *clear-df* : DF ビットを無視します。
- *copy-df* : DF ビットを維持します。
- *set-df* : DF ビットを設定して使用します。

```
[no] crypto map <name> <priority> set tfc-packets [burst <length | auto] [payload-size
<bytes | auto> [timeout <seconds | auto>
または
[no] crypto dynamic-map <name> <priority> set tfc-packets [burst <length | auto]
[payload-size <bytes | auto> [timeout <seconds | auto>
```

管理者は、IPsec セキュリティ アソシエーションにおける、ランダムな長さおよび間隔のダミーのトラフィック フローの機密性（TFC）パケットをイネーブルにできます。TFC をイネーブルにするには、IKEv2 IPsec プロポーザルが設定されている必要があります。

クリプト マップに割り当てられている ACL は、同じ ACL 名を持つすべての ACE で構成されます。コマンドの構文は次のとおりです。

```
access-list access-list-name {deny | permit} ip source source-netmask destination
destination-netmask
```

各 ACL は、同じ ACL 名を持つ 1 つまたは複数の ACE で構成されます。最初の ACE を作成したときに、ACL を作成します。ACL を作成または追加するコマンドの構文は次のとおりです。

```
access-list access-list-name {deny | permit} ip source source-netmask destination
destination-netmask
```

次の例では、ASA は 10.0.0.0 サブネットから 10.1.1.0 サブネットへのすべてのトラフィックに対して、クリプト マップに割り当てられている IPsec 保護を適用します。

```
access-list 101 permit ip 10.0.0.0 255.255.255.0 10.1.1.0 255.255.255.0
```

パケットが一致するクリプト マップによって、SA ネゴシエーションで使用されるセキュリティ設定が決定します。ローカルの ASA がネゴシエーションを開始する場合は、スタティック クリプト マップで指定されたポリシーを使用して、指定のピアに送信するオファーを作成します。ピアがネゴシエーションを開始する場合は、ASA はポリシーに一致するスタティック クリプト マップを探しますが、見つからない場合は、クリプト マップ セット内のダイナミック クリプト マップの中で見つかるものを探します。これは、ピアのオファーを受け入れるか拒否するかを決定するためです。

2 つのピアが SA の確立に成功するには、両方のピアが互換性のあるクリプト マップを少なくとも 1 つ持っている必要があります。互換性が成立するには、クリプト マップが次の条件を満たす必要があります。

- クリプト マップに、互換性を持つ暗号 ACL（たとえば、ミラー イメージ ACL）が含まれている。応答側ピアがダイナミック クリプト マップを使用している場合は、ASA 側でも互換性のある暗号 ACL が含まれていることが、IPsec を適用するための要件の 1 つです。
- 各クリプト マップが他のピアを識別する（応答するピアがダイナミック クリプト マップを使用していない場合）。
- クリプト マップに、共通のトランスフォーム セットまたはプロポーザルが少なくとも 1 つある。

1 つのインターフェイスに適用できるクリプト マップ セットは 1 つだけです。次の条件のいずれかが当てはまる場合は、ASA 上の特定のインターフェイスに対して複数のクリプト マップを作成します。

- 特定のピアに異なるデータ フローを処理させる。
- さまざまなタイプのトラフィックにさまざまな IPsec セキュリティを適用する。

たとえば、クリプト マップを 1 つ作成し、2 つのサブネット間のトラフィックを識別する ACL を割り当て、IKEv1 トランスフォーム セットまたは IKEv2 プロポーザルを 1 つ割り当てます。別のクリプト マップを作成し、別の 2 つのサブネット間のトラフィックを識別する ACL を割り当て、VPN パラメータが異なるトランスフォーム セットまたはプロポーザルを適用します。

1 つのインターフェイスに複数のクリプト マップを作成する場合は、クリプト マップ セット内のプライオリティを決めるシーケンス番号（seq-num）を各クリプト マップ エントリに指定します。

各 ACE には permit 文または deny 文が含まれます。表 1-3 に、クリプト マップに適用される ACL での許可 ACE と拒否 ACE の特別な意味を示します。

表 1-3　　発信トラフィックに適用される暗号 ACL における許可と拒否の特別な意味

クリプト マップ評価の結果	応答
permit 文が含まれている ACE の基準と一致	パケットをクリプト マップ セットの残りの ACE と照合して評価することを停止し、パケット セキュリティ設定を、クリプト マップに割り当てられている IKEv1 トランスフォーム セットまたは IKEv2 プロポーザルの中の設定と照合して評価します。セキュリティ設定がトランスフォーム セットまたはプロポーザルのセキュリティ設定と一致したら、ASA は関連付けられた IPsec 設定を適用します。一般に発信トラフィックの場合、IPsec 設定の適用とはパケットの復号化、認証、ルーティングを行うことを意味します。
deny 文が含まれている ACE の基準と一致	パケットを評価中のクリプト マップの残りの ACE と照合して評価することを中断し、次のクリプト マップ（クリプト マップに割り当てられているシーケンス番号で判断する）の ACE との照合と評価を再開します。
クリプト マップ セット内のテスト済みのすべての許可 ACE と不一致	パケットを暗号化せずにルーティングします。

deny 文が含まれている ACE は、IPsec 保護が不要な発信トラフィック（たとえば、ルーティング プロトコル トラフィックなど）をフィルタリングして除外します。したがって、暗号 ACL の permit 文と照合して評価する必要のない発信トラフィックをフィルタリングするために、最初の deny 文を挿入します。

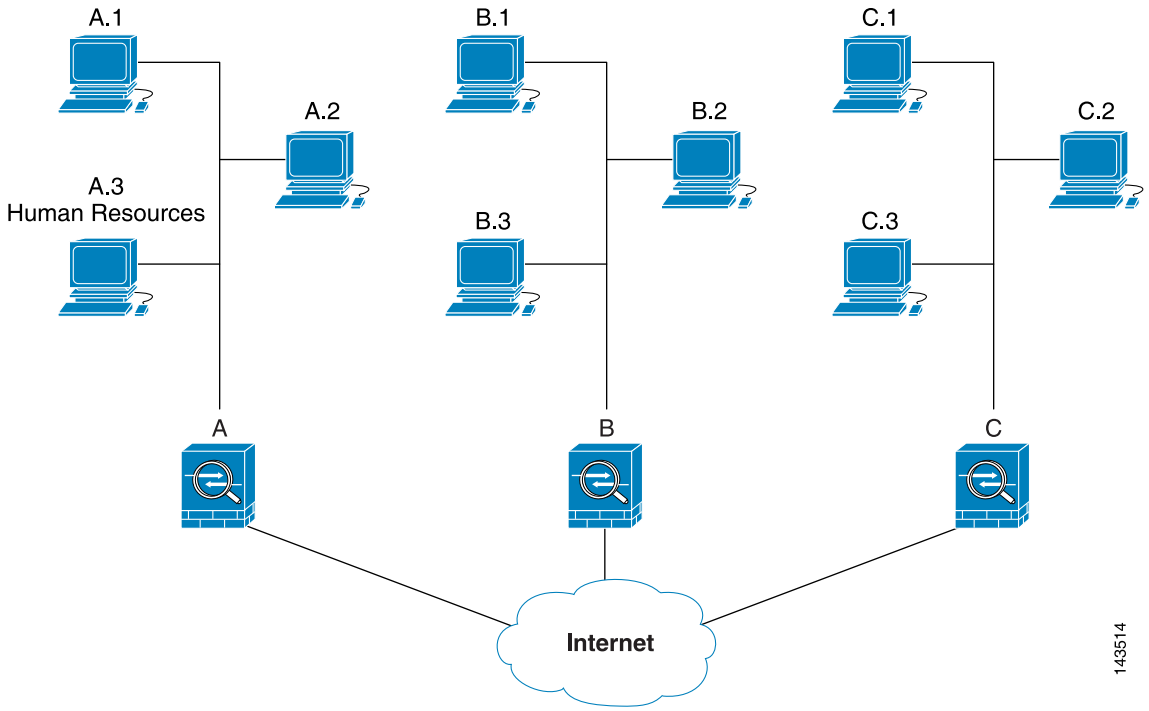
暗号化された着信パケットに対しては、セキュリティ アプライアンスは送信元アドレスと ESP SPI を使用して、パラメータの復号化を決定します。セキュリティ アプライアンスは、パケットを復号化した後で、復号化されたパケットの内部ヘッダーを、そのパケットの SA に関連付けられている ACL の許可 ACE と比較します。内部ヘッダーがプロキシと一致しない場合、セキュリティ アプライアンスはそのパケットをドロップします。内部ヘッダーがプロキシと一致する場合、セキュリティ アプライアンスはそのパケットをルーティングします。

暗号化されていない着信パケットの内部ヘッダーを比較する場合は、セキュリティ アプライアンスはすべての拒否ルールを無視します。これは、拒否ルールによってフェーズ 2 の SA の確立が妨げられるためです。

（注）　暗号化されていない着信トラフィックをクリア テキストとしてルーティングするには、許可 ACE の前に拒否 ACE を挿入します。

図 1-1 に、ASA の LAN-to-LAN ネットワークの例を示します。

図 1-1　許可 ACE と拒否 ACE がトラフィックに及ぼす影響（概念上のアドレス）



この図に示され、また以下の説明で使用されている単純なアドレス表記は、抽象化したものです。実際の IP アドレスを使用した例は、この説明の後に示します。

この LAN-to-LAN ネットワーク例において、セキュリティ アプライアンス A、B、および C を設定する目的は、図 1-1 に示したホストのいずれか 1 台から発信され、別のホストを宛先とするすべてのトラフィックのトンネリングを許可することです。ただし、ホスト A.3 から発信されるトラフィックには人事部の機密データが含まれるため、他のトラフィックよりも強固な暗号化と頻繁なキー再生が必要です。そのため、ホスト A.3 から発信されるトラフィックには特別なトランスフォーム セットを割り当てます。

セキュリティ アプライアンス A を発信トラフィック用に設定するには、2 つのクリプト マップを作成します。1 つはホスト A.3 からのトラフィック用で、もう 1 つはネットワーク A の他のホストからのトラフィック用です。次に例を示します。

```
Crypto Map Seq_No_1
    deny packets from A.3 to B
    deny packets from A.3 to C
    permit packets from A to B
    permit packets from A to C
Crypto Map Seq_No_2
    permit packets from A.3 to B
    permit packets from A.3 to C
```

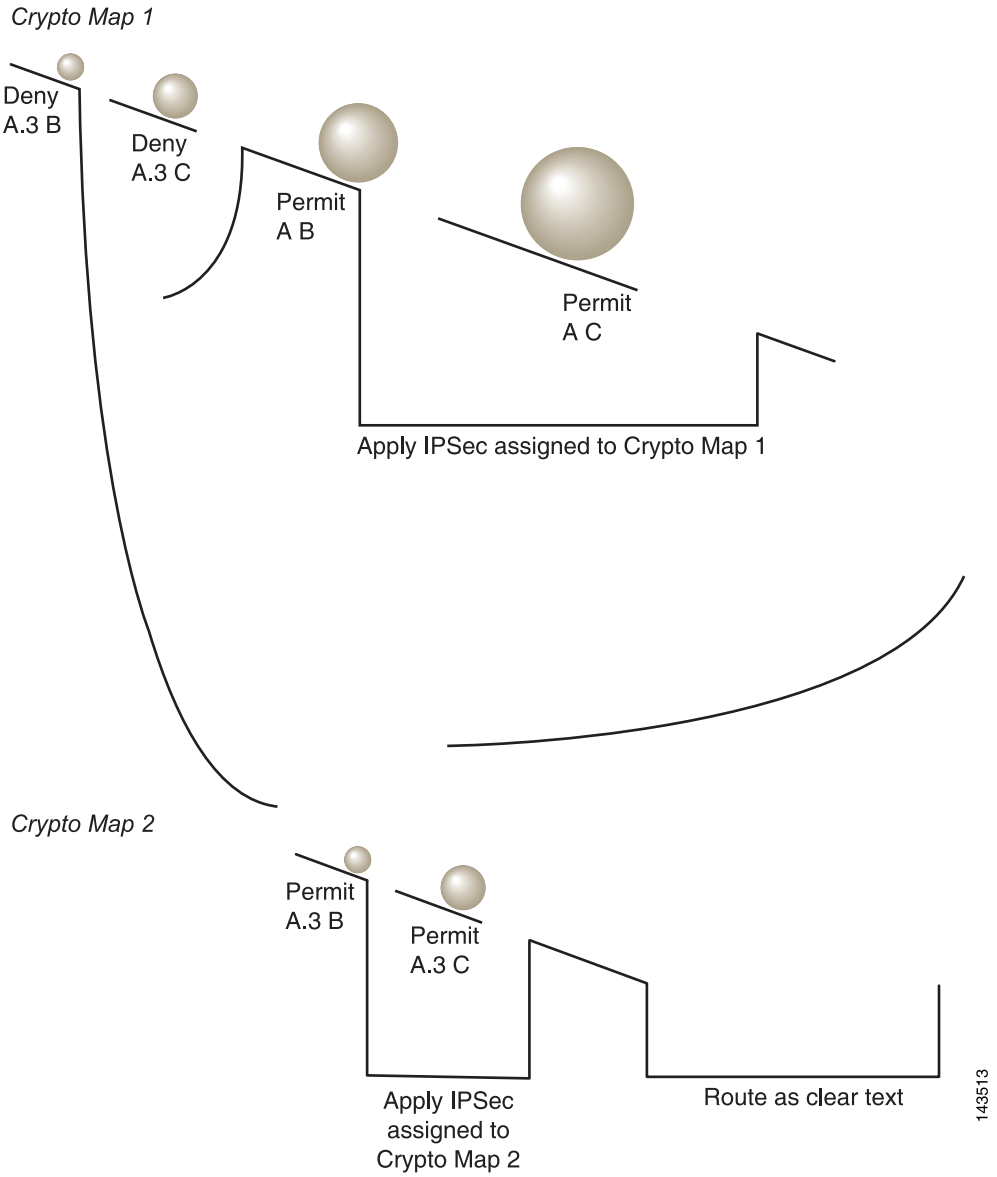
ACL を作成したら、一致するパケットごとに必要な IPsec を適用するためのトランスフォーム セットを各クリプト マップに割り当てます。

カスケード ACL とは、拒否 ACE を挿入することで、ACL の評価をバイパスし、クリプト マップ セット内の次の ACL の評価を再開するものです。クリプト マップごとに異なる IPsec 設定を関連付けることができるため、拒否 ACE を使用することで、特別なトラフィックを対応するクリプト マップでの以後の評価から除外し、異なるセキュリティを提供する別のクリプト マップ、または異なるセキュリティを必要とする別のクリプト マップの permit 文と特別なトラフィックを照合することができます。暗号 ACL に割り当てられているシーケンス番号によって、クリプト マップ セット内の評価の順序が決まります。

図 1-2 に、この例の概念的な ACE から作成されたカスケード ACL を示します。この図で使用されている各記号の意味は、次のとおりです。

	クリプト マップ セット内のクリプト マップ。
	（すき間がある直線）パケットが ACE に一致した時点でクリプト マップの照合を終了します。
	1 つの ACE の説明と一致したパケット。それぞれの大きさのボールは、図中の別々の ACE に一致する異なるパケットを表しています。大きさの違いは、各パケットの発信元と宛先が異なることを示しています。
	クリプト マップ セット内での次のクリプト マップへのリダイレクション。
	パケットが ACE に一致するか、またはクリプト マップ セット内のすべての許可 ACE に一致しない場合の応答。

図 1-2　クリプト マップ セット内のカスケード ACL



セキュリティ アプライアンス A は、ホスト A.3 から発信されたパケットが許可 ACE と一致するまで評価し、クリプト マップに関連付けられている IPsec セキュリティの割り当てを試行します。このパケットが拒否 ACE と一致すると、ASA はこのクリプト マップの残りの ACE を無視し、次のクリプト マップ（クリプト マップに割り当てられているシーケンス番号で判断する）との照合と評価を再開します。この例では、セキュリティ アプライアンス A がホスト A.3 から発信されたパケットを受信すると、このパケットを最初のクリプト マップの拒否 ACE と照合し、次のクリプト マップでの照合と評価を再開します。パケットが 2 番目のクリプト マップの許可 ACE と一致すると、関連付けられた IPsec セキュリティ（強固な暗号化と頻繁なキー再生）がパケットに適用されます。

このネットワーク例における ASA の設定を完了するために、ミラー クリプト マップを ASA B と C に割り当てます。しかし、ASA は、暗号化された着信トラフィックの評価では拒否 ACE を無視するため、deny A.3 B と deny A.3 C の ACE のミラーに相当するものを無視できます。したがって、クリプト マップ 2 のミラーに相当するものを無視できます。このため、ASA B と C のカスケード ACL の設定は不要です。

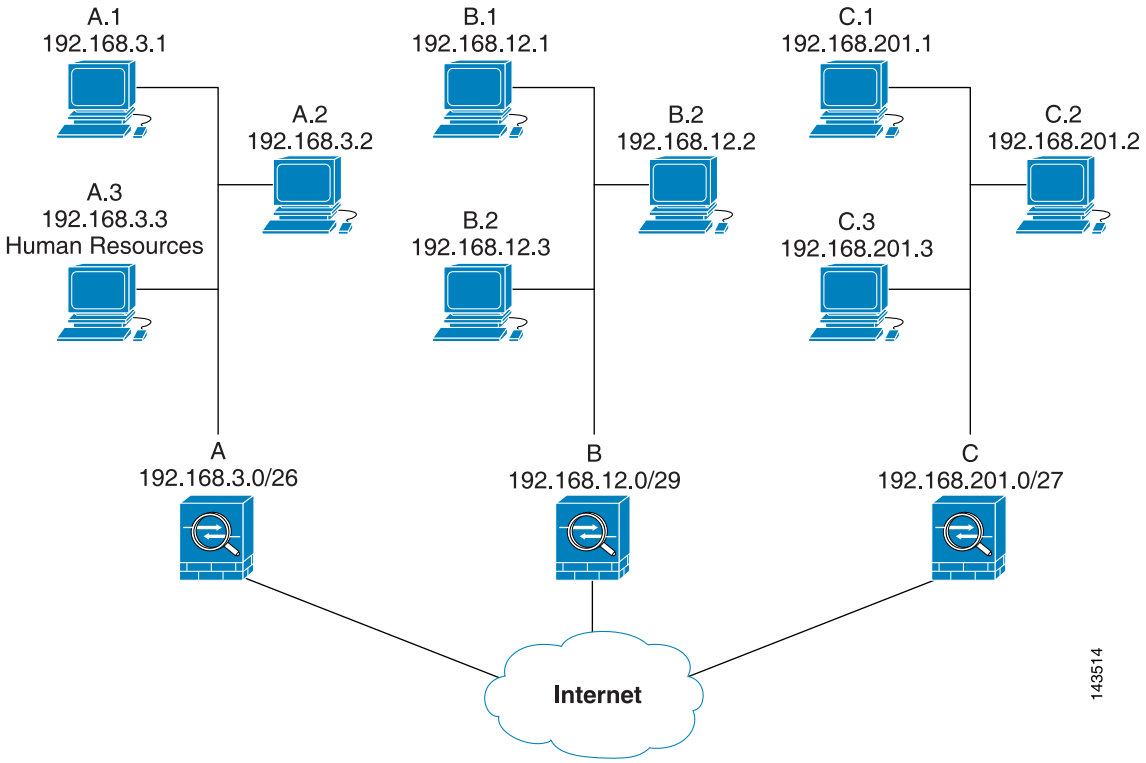
表 1-4 に、図 1-1 の 3 台の ASA 用に設定されたクリプト マップに割り当てられている ACL を示します。

表 1-4　　許可文と拒否文の例（概念図）

セキュリティ アプライアンス A		セキュリティ アプライアンス B		セキュリティ アプライアンス C	
クリプト マップ シーケンス番号	**ACE パターン**	**クリプト マップ シーケンス番号**	**ACE パターン**	**クリプト マップ シーケンス番号**	**ACE パターン**
1	A.3 B を拒否	1	B A を許可	1	C A を許可
	A.3 C を拒否				
	A B を許可				
	A C を許可		B C を許可		C B を許可
2	A.3 B を許可				
	A.3 C を許可				

図 1-3 では、図 1-1 の概念アドレスを実際の IP アドレスにマッピングしています。

図 1-3　　許可 ACE と拒否 ACE がトラフィックに及ぼす影響（実際のアドレス）



次の表は、図 1-3 の IP アドレスを表 1-4 の概念と結合したものです。これらの表に示されている実際の ACE によって、このネットワーク内で評価を受けたすべての IPsec パケットに適切な IPsec 設定が適用されます。

表 1-5　ASA A の許可文と拒否文の例

セキュリティ アプライアンス	クリプト マップ シーケンス番号	ACE パターン	実際の ACE
A	1	A.3 B を拒否	deny 192.168.3.3 255.255.255.192 192.168.12.0 255.255.255.248
		A.3 C を拒否	deny 192.168.3.3 255.255.255.192 192.168.201.0 255.255.255.224
		A B を許可	permit 192.168.3.0 255.255.255.192 192.168.12.0 255.255.255.248
		A C を許可	permit 192.168.3.0 255.255.255.192 192.168.201.0 255.255.255.224
	2	A.3 B を許可	permit 192.168.3.3 255.255.255.192 192.168.12.0 255.255.255.248
		A.3 C を許可	permit 192.168.3.3 255.255.255.192 192.168.201.0 255.255.255.224
B	必要なし	B A を許可	permit 192.168.12.0 255.255.255.248 192.168.3.0 255.255.255.192
		B C を許可	permit 192.168.12.0 255.255.255.248 192.168.201.0 255.255.255.224
C	必要なし	C A を許可	permit 192.168.201.0 255.255.255.224 192.168.3.0 255.255.255.192
		C B を許可	permit 192.168.201.0 255.255.255.224 192.168.12.0 255.255.255.248

この例のネットワークで示した論法を応用すると、カスケード ACL を使用して、1 台の ASA で保護されているさまざまなホストまたはサブネットにそれぞれ異なるセキュリティ設定を割り当てることができます。

（注） デフォルトでは、ASA は、IPsec トラフィックが入ってきたインターフェイスと同じインターフェイスを宛先とする IPsec トラフィックはサポートしません このタイプのトラフィックには、U ターン、ハブアンドスポーク、ヘアピニングなどの名称があります。ただし、U ターン トラフィックをサポートするように IPsec を設定できます。それには、そのネットワークとの間のトラフィックを許可する ACE を挿入します。たとえば、セキュリティ アプライアンス B で U ターン トラフィックをサポートするには、概念上の「B B を許可」ACE を ACL1 に追加します。実際の ACE は次のようになります。

```
permit 192.168.12.0 255.255.255.248 192.168.12.0 255.255.255.248
```

公開キー インフラストラクチャ（PKI）キーの管理

キー ペアを生成またはゼロ化するときに Suite-B ECDSA アルゴリズムを選択できるようにするには、公開キー インフラストラクチャ（PKI）を設定する必要があります。

前提条件

RSA または ECDSA のトラストポイントを認証に使用するように暗号化マップを設定する場合は、最初にキー セットを生成する必要があります。これで、そのトラストポイントを作成して、トンネル グループ コンフィギュレーションの中で参照できるようになります。

手順の詳細

ステップ 1　キー ペアを生成するときに Suite-B ECDSA アルゴリズムを選択します。

```
crypto key generate [rsa [general-keys | label <name> | modules [512 | 768 | 1024 | 2048 |
4096] | noconfirm | usage-keys] | ecdsa [label <name> | elliptic-curve [256 | 384 | 521] |
noconfirm]]
```

ステップ 2　キー ペアをゼロ化するときに Suite-B ECDSA アルゴリズムを選択します。

```
crypto key zeroize [rsa | ecdsa] [default | label <name> | noconfirm]
```

暗号化コアのプールの設定

AnyConnect TLS/DTLS トラフィックに対してより適切なスループット パフォーマンスが得られるように、対称型マルチプロセッシング（SMP）プラットフォーム上での暗号化コアの割り当てを変更することができます。この変更によって、SSL VPN データパスが高速化され、AnyConnect、スマート トンネル、およびポート転送において、ユーザが認識できるパフォーマンス向上が実現します。暗号化コアのプールを設定するには、次の手順を実行します。

制限事項

- 暗号化コア再分散ができるのは、次のプラットフォームです。
  - 5585-X
  - 5545-X/5555-X
  - ASASM

手順の詳細

ステップ 1　次の 3 つの相互排他的オプションの 1 つを指定して暗号化コアのプールを設定します。

- balanced：暗号化ハードウェア リソースを均等に分散します（Admin/SSL および IPsec コア）。
- ipsec：IPsec を優先するように暗号化ハードウェア リソースを割り当てます（SRTP 暗号化音声トラフィックを含む）。
- ssl：Admin/SSL を優先するように暗号化ハードウェア リソースを割り当てます。

```
hostname(config)# crypto engine ?

configure mode commands/options:
accelerator-bias
Specify how to allocate crypto accelerator processors

hostname(config)# crypto engine accelerator-bias ?
configure mode commands/options
balanced - Equally distribute crypto hardware resources
ipsec - Allocate crypto hardware resources to favor IPsec/Encrypted Voice (SRTP)
ssl - Allocate crypto hardware resources to favor SSL

hostname(config)# crypto engine accelerator-bias ssl
```

クリプト マップのインターフェイスへの適用

クリプト マップ セットは、IPsec トラフィックが通過する各インターフェイスに割り当てる必要があります。ASA は、すべてのインターフェイスで IPsec をサポートします。クリプト マップ セットをインターフェイスに割り当てると、ASA は、すべてのトラフィックをクリプト マップ セットと照合して評価し、接続中またはネゴシエーション中は指定されたポリシーを使用します。

クリプト マップをインターフェイスに割り当てると、SA データベースやセキュリティ ポリシー データベースなどのランタイム データ構造も初期化されます。クリプト マップを修正してインターフェイスに再割り当てすると、ランタイム データ構造はクリプト マップ設定と再同期化されます。また、新しいシーケンス番号を使用して新しいピアを追加し、クリプト マップを再割り当てしても、既存の接続が切断されることはありません。

インターフェイス ACL の使用

ASA では、デフォルトで IPsec パケットがインターフェイス ACL をバイパスするようになっています。インターフェイス ACL を IPsec トラフィックに適用する場合は、**no** 形式の **sysopt connection permit-vpn** コマンドを使用します。

発信インターフェイスにバインドされているクリプト マップ ACL は、VPN トンネルを通過する IPsec パケットの許可と拒否を行います。IPsec は、IPsec トンネルから来たパケットの認証と解読を行い、トンネルに関連付けられている ACL とパケットを照合して評価します。

ACL は、どの IP トラフィックを保護するかを定義します。たとえば、2 つのサブネット間または 2 台のホスト間のすべての IP トラフィックを保護するための ACL を作成できます （これらの ACL は、**access-group** コマンドで使用される ACL とよく似ています。ただし、**access-group** コマンドでは、ACL がインターフェイスで転送するトラフィックと阻止するトラフィックを決めます）。

クリプト マップを割り当てるまで、ACL は IPsec の使用に限定されません。各クリプト マップは ACL を参照し、パケットが ACL のいずれか 1 つで permit と一致した場合に適用する IPsec プロパティを決めます。

IPsec クリプト マップに割り当てられている ACL には、次の 4 つの主要機能があります。

- IPSec で保護する発信トラフィックを選択する（permit に一致したものが保護の対象）。
- 確立された SA がない状態で移動するデータに対して ISAKMP ネゴシエーションをトリガーする。
- 着信トラフィックを処理して、IPSec で保護すべきであったトラフィックをフィルタリングして廃棄する。
- ピアからの IKE ネゴシエーションを処理するときに、IPsec SA の要求を受け入れるかどうかを決定する （ネゴシエーションは **ipsec-isakmp crypto map** エントリだけに適用されます）。ピアは、**ipsec-isakmp crypto map** コマンド エントリが関連付けられているデータ フローを許可する必要があります。これは、ネゴシエーション中に確実に受け入れられるようにするためです。

トラフィックが着信か発信かに関係なく、ASA は、インターフェイスに割り当てられている ACL とトラフィックを照合して評価します。インターフェイスに IPsec を割り当てるには、次の手順を実行します。

ステップ 1　IPsec に使用する ACL を作成します。

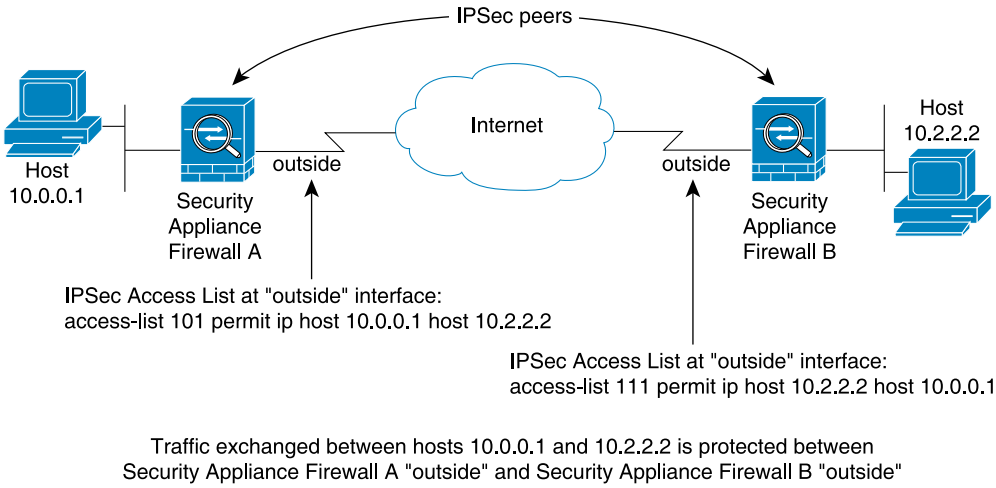
ステップ 2　作成したアクセス リストを、同じクリプト マップ名を使用して 1 つまたは複数のクリプト マップにマッピングします。

ステップ 3　データ フローに IPsec を適用するために、クリプト マップに IKEv1 トランスフォーム セットまたは IKEv2 プロポーザルをマッピングします。

ステップ 4　共有するクリプト マップ名を割り当てて、クリプト マップを一括してクリプト マップ セットとしてインターフェイスに適用します。

図 1-4 では、データが ASA A 上の外部インターフェイスを出てホスト 10.2.2.2 に向かうときに、ホスト 10.0.0.1 とホスト 10.2.2.2 の間のトラフィックに IPsec 保護が適用されます。

図 1-4　暗号 ACL を IPsec に適用する方法



ASA A は、ホスト 10.0.0.1 からホスト 10.2.2.2 へのトラフィックを次のように評価します。

- 送信元 = ホスト 10.0.0.1
- 宛先 = ホスト 10.2.2.2

また ASA A は、ホスト 10.2.2.2 からホスト 10.0.0.1 へのトラフィックを次のように評価します。

- 送信元 = ホスト 10.2.2.2
- 宛先 = ホスト 10.0.0.1

評価中のパケットと最初に一致した permit 文によって、IPsec SA のスコープが決まります。

（注）　ACL の要素を 1 つだけ削除すると、ASA は関連付けられているクリプト マップも削除します。

現在 1 つまたは複数のクリプト マップが参照している ACL を修正する場合は、**crypto map interface** コマンドを使用してランタイム SA データベースを再初期化します。詳細については、**crypto map** コマンドを参照してください。

ローカル ピアで定義するスタティック クリプト マップに対して指定するすべての暗号 ACL について、リモート ピアで「ミラー イメージ」暗号 ACL を定義することを推奨します。また、クリプト マップは共通トランスフォームをサポートし、他のシステムをピアとして参照する必要があります。これにより、両方のピアで IPsec が正しく処理されます。

（注）　すべてのスタティック クリプト マップで ACL と IPsec ピアを定義する必要があります。どちらかが定義されていないと、クリプト マップは不完全なものになり、ASA は、前の完全なクリプト マップにまだ一致していないトラフィックをドロップします。**show conf** コマンドを使用して、すべてのクリプト マップが完全なものになるようにします。不完全なクリプト マップを修正するには、クリプト マップを削除し、欠けているエントリを追加してからクリプト マップを再適用します。

暗号 ACL で送信元アドレスまたは宛先アドレスの指定に **any** キーワードを使用すると問題が発生するため、このキーワードの使用は避けてください。**permit any any** コマンド文を使用すると次の現象が発生するため、使用は極力避けてください。

- すべての発信トラフィックが保護されます。これには、対応するクリプト マップで指定されているピアに送信される保護済みのトラフィックも含まれます。
- すべての着信トラフィックに対する保護が必要になります。

  このシナリオでは、ASA は IPsec 保護されていないすべての着信パケットを通知なしでドロップします。

保護するパケットを定義したことを必ず確認してください。**permit** 文に **any** キーワードを使用する場合は、その文の前に一連の **deny** 文をおき、保護対象外のトラフィックをすべてフィルタリングして排除します。これを行わないと、その **permit** 文に保護対象外のトラフィックが含まれることになります。

（注）　**no sysopt connection permit-vpn** が設定されているときに、外部インターフェイスのアクセス グループが deny ip any any アクセス リストを呼び出すように設定されていたとしても、クライアントからの復号化された通過トラフィックは許可されます。

保護されたネットワークへの、サイトツーサイトまたはリモート アクセス VPN 経由でのアクセスをコントロールするために、**no sysopt permit** コマンドを外部インターフェイス上のアクセス コントロール リスト（ACL）と組み合わせて使用しようとしても、うまくいきません。

このような状況では、内部の管理アクセスがイネーブルになっていると、ACL は適用されず、ユーザはまだセキュリティ アプライアンスへの SSH を使用して接続できます。内部ネットワーク上のホストへのトラフィックは ACL によって正しくブロックされますが、内部インターフェイスへの復号化された通過トラフィックはブロックできません。

ssh および **http** コマンドは、ACL よりもプライオリティが高くなります。つまり、VPN セッションからデバイスへの SSH、Telnet、または ICMP トラフィックを拒否するには、IP ローカル プールを拒否する **ssh**、**telnet**、および **icmp** コマンドを追加する必要があります。

IPsec SA のライフタイムの変更

ASA が新しい IPSec SA とネゴシエートするときに使用する、グローバル ライフタイム値を変更できます。特定のクリプト マップのグローバル ライフタイム値を上書きできます。

IPsec SA では、取得された共有秘密キーが使用されます。このキーは SA に不可欠な要素です。キーは同時にタイムアウトするので、キーのリフレッシュが必要です。各 SA には、「指定時刻」と「トラフィック量」の 2 種類のライフタイムがあります。それぞれのライフタイムを過ぎると SA は失効し、新しい SA のためのネゴシエーションが開始します。デフォルトのライフタイムは、28,800 秒（8 時間）および 4,608,000 キロバイト（10 メガバイト/秒で 1 時間）です。

グローバル ライフタイムを変更すると、ASA はトンネルをドロップします。変更後に確立された SA のネゴシエーションでは、新しい値が使用されます。

クリプト マップに設定されたライフタイム値がなく、ASA から新しい SA を要求された場合、クリプト マップは、ピアに送信される新しい SA 要求に、既存の SA で使用されているグローバル ライフタイム値を挿入します。ピアがネゴシエーション要求を受け取ると、このピアが提案するライフタイム値とローカルに設定されているライフタイム値のうち小さい方の値を、新しい SA のライフタイム値として使用します。

既存 SA のライフタイムのしきい値を超える前に、ピアは新しい SA をネゴシエートします。このようにして、既存 SA の有効期限が切れる前に、新しい SA の準備が整います。既存 SA の残りのライフタイムが約 5 ～ 15% になると、ピアは新しい SA をネゴシエートします。

基本的な IPsec コンフィギュレーションの作成

スタティックまたはダイナミック クリプト マップを使用する基本的な IPsec コンフィギュレーションを作成できます。

スタティック クリプト マップを使用する基本的な IPsec コンフィギュレーションを作成するには、次の手順を実行します。

ステップ 1　次のコマンドを入力して、保護するトラフィックを定義する ACL を作成します。

access-list *access-list-name* **{deny | permit} ip** *source source-netmask destination destination-netmask*

次に例を示します。

```
hostname(config)# access-list 101 permit ip 10.0.0.0 255.255.255.0 10.1.1.0 255.255.255.0
```

access-list-name では、ACL ID を、最大 241 文字の文字列または整数として指定します。*destination-netmask* と *source-netmask* では、IPv4 ネットワーク アドレスおよびサブネット マスクを指定します。この例では、**permit** キーワードによって、指定の条件に一致するトラフィックすべてが暗号で保護されます。

ステップ 2　トラフィックを保護する方法を定義する IKEv1 トランスフォーム セットを設定するには、次のコマンドを入力します。

crypto ipsec ikev1 transform-set *transform-set-name encryption* [*authentication*]

encryption では、IPsec データ フローを保護するための暗号化方式を指定します。

- esp-aes：AES と 128 ビット キーを使用します。
- esp-aes-192：AES と 192 ビット キーを使用します。
- esp-aes-256：AES と 256 ビット キーを使用します。
- esp-des：56 ビット DES-CBC を使用します。
- esp-3des：トリプル DES アルゴリズムを使用します。
- esp-null：暗号化なし。

authentication では、IPsec データ フローを保護するための暗号化方式を指定します

- esp-md5-hmac：ハッシュ アルゴリズムとして MD5/HMAC-128 を使用します。
- esp-sha-hmac：ハッシュ アルゴリズムとして SHA/HMAC-160 を使用します。
- esp-none：HMAC 認証なし。

次に例を示します。

```
hostname(config)# crypto ipsec ikev1 transform-set myset1 esp-des esp-sha-hmac
hostname(config)# crypto ipsec ikev1 transform-set myset2 esp-3des esp-sha-hmac
hostname(config)# crypto ipsec ikev1 transform-set aes_set esp-md5-hmac esp-aes-256
```

この例では、myset1、myset2、aes_set がトランスフォーム セットの名前です。

IKEv2 プロポーザルを設定するとともに、トラフィックを保護する方法も定義するには、**crypto ipsec ikev2 ipsec-proposal** コマンドを入力すると、プロポーザルが作成され、IPsec プロポーザル コンフィギュレーション モードが開始します。ここで、プロポーザルの暗号化と整合性のタイプを複数指定することができます。

crypto ipsec ikev2 ipsec-proposal [*proposal tag*]

proposal tag は IKEv2 IPsec プロポーザルの名前で、1 ～ 64 文字の文字列です。

次に例を示します。

```
hostname(config)# crypto ipsec ikev2 ipsec-proposal secure
```

この例では、secure がプロポーザルの名前です。プロトコルおよび暗号化タイプを入力します。

```
hostname(config-ipsec-proposal)# protocol esp encryption 3des aes des
```

逆に、次のコマンドでは、どの AES-GCM または AES-GMAC アルゴリズムを使用するかを選択します。

```
hostname(config-ipsec-proposal)# [no] protocol esp encryption [3des | aes | aes-192 |
aes-256 | aes-gcm | aes-gcm-192 | aes-gcm-256 | aes-gmac | aes-gmac-192 | aes-gmac-256 |
des | null]
```

SHA-2 またはヌルが選択されている場合は、どのアルゴリズムを IPsec 整合性アルゴリズムとして使用するかを選択する必要があります。AES-GCM/GMAC が暗号化アルゴリズムとして設定されている場合は、ヌル整合性アルゴリズムを選択する必要があります。

```
hostname(config-ipsec-proposal)# [no] protocol esp integrity [md5 | sha-1 | sha-256 |
sha-384 | sha-512 | null]
```

（注） AES-GCM/GMAC が暗号化アルゴリズムとして設定されている場合は、ヌル整合性アルゴリズムを選択する必要があります。SHA-256 は IKEv2 トンネルを確立するために整合性や PRF に使用できますが、ESP 整合性保護にも使用できます。

ステップ 3　（オプション）管理者はパス最大伝送単位（PMTU）エージングをイネーブルにして、PMTU 値を元の値にリセットする間隔を設定することができます。

```
hostname(config-ipsec-proposal)# [no] crypto ipsec security-association pmtu-aging
<reset-interval>
```

ステップ 4　クリプト マップを作成するには、シングルまたはマルチ コンテキスト モードを使用して、次のサイトツーサイト手順を実行します。

a. ACL をクリプト マップに割り当てます。

```
crypto map map-name seq-num match address access-list-name
```

クリプト マップ セットとは、クリプト マップ エントリの集合です。エントリはそれぞれ異なるシーケンス番号（*seq-num*）を持ちますが、*map name* が同じです。*access-list-name* では、ACL ID を、最大 241 文字の文字列または整数として指定します。次の例では、mymap がクリプト マップ セットの名前です。マップ セットのシーケンス番号は 10 です。シーケンス番号は、1 つのクリプト マップ セット内の複数のエントリにランクを付けるために使用します。シーケンス番号が小さいほど、プライオリティが高くなります。

```
crypto map mymap 10 match address 101
```

この例では、ACL 101 がクリプト マップ mymap に割り当てられます。

b. IPsec で保護されたトラフィックの転送先となるピアを指定します。

```
crypto map map-name seq-num set peer ip-address
```

次に例を示します。

```
crypto map mymap 10 set peer 192.168.1.100
```

ASA は、ピアに IP アドレス 192.168.1.100 が割り当てられている SA をセットアップします。このコマンドを繰り返して、複数のピアを指定します。

c. このクリプト マップに対して、IKEv1 トランスフォーム セットと IKEv2 プロポーザルのどちらを許可するかを指定します。複数のトランスフォーム セットまたはプロポーザルを、プライオリティ順（最高のプライオリティのものが最初）に列挙します。1 つのクリプト マップに最大 11 個のトランスフォーム セットまたはプロポーザルを指定できます。次の 2 つのいずれかのコマンドを使用します。

```
crypto map map-name seq-num set ikev1 transform-set transform-set-name1
[transform-set-name2, …transform-set-name11]
```

```
crypto map map-name seq-num set ikev2 ipsec-proposal proposal-name1
[proposal-name2, … proposal-name11]
```

proposal-name1 と *proposal-name11* では、IKEv2 の IPsec プロポーザルを 1 つ以上指定します。各クリプト マップ エントリは、最大 11 個のプロポーザルをサポートします。

例（IKEv1 の場合）：

```
crypto map mymap 10 set ikev1 transform-set myset1 myset2
```

この例では、トラフィックが ACL 101 に一致したときに、SA は、どのトランスフォーム セットがピアのトランスフォーム セットに一致するかによって、myset1（第 1 プライオリティ）と myset2（第 2 プライオリティ）のいずれかを使用できます。

d. （オプション）グローバル ライフタイムを上書きする場合は、クリプト マップの SA ライフタイムを指定します。

```
crypto map map-name seq-num set security-association lifetime {seconds seconds |
kilobytes kilobytes}
```

map-name では、クリプト マップ セットの名前を指定します。*seq-num* では、クリプト マップ エントリに割り当てる番号を指定します。

次に例を示します。

```
crypto map mymap 10 set security-association lifetime seconds 2700
```

この例では、クリプト マップ mymap 10 の指定時刻ライフタイムを 2700 秒（45 分）に短縮します。トラフィック量ライフタイムは変更されません。

e. （オプション）IPsec がこのクリプト マップに対して新しい SA を要求するときに完全転送秘密（PFS）を要求するか、または IPsec ピアから受け取る要求に PFS を要求するかを指定します。

```
crypto map map-name seq-num set pfs [group1 | group2 | group5]
```

次に例を示します。

```
crypto map mymap 10 set pfs group2
```

この例では、クリプト マップ mymap 10 に対して新しい SA をネゴシエートするときに PFS が必要です。ASA は、1024 ビット Diffie-Hellman プライム モジュラス グループを新しい SA で使用します。

ステップ 5　IPsec トラフィックを評価するために、クリプト マップ セットをインターフェイスに適用します。

```
crypto map map-name interface interface-name
```

map-name では、クリプト マップ セットの名前を指定します。*interface-name* では、ISAKMP IKEv1 ネゴシエーションをイネーブルまたはディセーブルにするインターフェイスの名前を指定します。

次に例を示します。

```
crypto map mymap interface outside
```

この例では、ASA は外部インターフェイスを通過するトラフィックをクリプト マップ mymap と照合して評価し、保護が必要かどうかを判断します。

ダイナミック クリプト マップの使用

ダイナミック クリプト マップは、いずれのパラメータも設定されていないクリプト マップです。ダイナミック クリプト マップは、不 足しているパラメータが、ピアの要件に合うように後でダイナミックに取得される（IPsec ネゴシエーションの結果として）ポリシー テンプレートの役割を果たします。ASA は、スタティック クリプト マップでピアの IP アドレスがまだ指定されていない場合、ピアでトンネルをネゴシエートさせるためにダイナミック クリプト マップを適用します。これは、次のタイプのピアで発生します。

- パブリック IP アドレスがダイナミックに割り当てられるピア。

  LAN-to-LAN のピア、およびリモート アクセスするピアは、両方とも DHCP を使用してパブリック IP アドレスを取得できます。ASA は、トンネルを開始するときだけこのアドレスを使用します。

- プライベート IP アドレスがダイナミックに割り当てられるピア。

  通常、リモート アクセスのトンネルを要求するピアは、ヘッドエンドによって割り当てられたプライベート IP アドレスを持っています 一般に、LAN-to-LAN トンネルには事前に決定されたプライベート ネットワークのセットがあります。これがスタティック マップの設定に使用されるので、結果として IPsec SA の確立にも使用されます。

管理者がスタティック クリプト マップを設定するため、（DHCP または別の方法で）ダイナミックに割り当てられた IP アドレスがわからない場合や、割り当て方法には関係なく他のクライアントのプライベート IP アドレスがわからない場合があります。通常、VPN クライアントには、スタティック IP アドレスがなく、IPsec ネゴシエーションを発生させるためのダイナミック クリプト マップが必要です。たとえば、ヘッドエンドは IKE ネゴシエーション中に IP アドレスを Cisco VPN Client に割り当て、クライアントはこのアドレスを使用して IPsec SA をネゴシエートします。

（注） ダイナミック クリプト マップには **transform-set** パラメータだけが必要です。

ダイナミック クリプト マップを使用すると、IPsec のコンフィギュレーションが簡単になります。ピアが常に事前に決定されるとは限らないネットワークで使用することを推奨します。ダイナミック クリプト マップは、Cisco VPN Client（モバイル ユーザなど）、およびダイナミックに割り当てられた IP アドレスを取得するルータに対して使用してください。

ヒント ダイナミック クリプト マップの **permit** エントリに **any** キーワードを使用する場合は、注意が必要です。このような **permit** エントリの対象となるトラフィックにマルチキャストやブロードキャストのトラフィックが含まれる場合、該当するアドレス範囲について **deny** エントリを ACL に挿入します。ネットワークとサブネット ブロードキャスト トラフィックに対して、また IPsec で保護しないその他のトラフィックに対しては、必ず **deny** エントリを挿入してください。

ダイナミック クリプト マップは、接続を開始したリモートのピアと SA をネゴシエートするときだけ機能します。ASA は、ダイナミック クリプト マップを使用してリモート ピアとの接続を開始することはできません。ダイナミック クリプト マップ エントリでは、発信トラフィックが ACL の permit エントリと一致しても、対応する SA がまだ存在しない場合、ASA はそのトラフィックをドロップします。

クリプト マップ セットには、ダイナミック クリプト マップを含めることができます。ダイナミック クリプト マップのセットには、クリプト マップ セットで一番低いプライオリティ（つまり、一番大きいシーケンス番号）を設定し、ASA が他のクリプト マップを先に評価するようにする必要があります。セキュリティ アプライアンスは、他の（スタティック）マップのエントリが一致しない場合にだけ、ダイナミック クリプト マップのセットを調べます。

スタティック クリプト マップ セットと同様に、ダイナミック クリプト マップ セットにも、同じ dynamic-map-name を持つすべてのダイナミック クリプト マップを含めます。dynamic-seq-num によって、セット内のダイナミック クリプト マップが区別されます。ダイナミック クリプト マップを設定する場合は、IPsec ピアのデータ フローを暗号 ACL で識別するために、ACL の許可を挿入します。このように設定しないと、ASA は、ピアが提示するあらゆるデータ フロー ID を受け入れることになります。

注意 ダイナミック クリプト マップ セットを使用して設定された、ASA インターフェイスにトンネリングされるトラフィックに対して、モジュールのデフォルト ルートを割り当てないでください。トンネリングされるトラフィックを指定するには、ダイナミック クリプト マップに ACL を追加します。リモート アクセス トンネルに関連付けられた ACL を設定する場合は、適切なアドレス プールを指定してください。逆ルート注入を使用してルートをインストールするのは、必ずトンネルがアップ状態になった後にしてください。

ダイナミック クリプト マップ エントリを使用するための手順は、スタティック クリプト マップを作成する代わりにダイナミック クリプト マップ エントリを作成するという点を除いて、「基本的な IPsec コンフィギュレーションの作成」で説明した基本的なコンフィギュレーションと同じです。1 つのクリプト マップ セットの中でスタティック マップ エントリとダイナミック マップ エントリを組み合わせることもできます。

次の手順に従って、ダイナミック クリプト マップ エントリを、シングルまたはマルチ コンテキスト モードを使用して作成します。

ステップ 1　（オプション）ACL をダイナミック クリプト マップに割り当てます。

```
crypto dynamic-map dynamic-map-name dynamic-seq-num match address access-list-name
```

これによって、保護するトラフィックと保護しないトラフィックが決まります。*dynamic-map-name* では、既存のダイナミック クリプト マップを参照するクリプト マップ エントリの名前を指定します。*dynamic-seq-num* では、ダイナミック クリプト マップ エントリに対応するシーケンス番号を指定します。

次に例を示します。

```
crypto dynamic-map dyn1 10 match address 101
```

この例では、ACL 101 がダイナミック クリプト マップ dyn1 に割り当てられます。マップのシーケンス番号は 10 です。

ステップ 2　このダイナミック クリプト マップに対して、どの IKEv1 トランスフォーム セットまたは IKEv2 プロポーザルを許可するかを指定します。複数のトランスフォーム セットまたはプロポーザルをプライオリティ順に（最高のプライオリティのものが最初）指定します。IKEv1 トランスフォーム セットまたは IKEv2 プロポーザルに応じたコマンドを使用してください。

```
crypto dynamic-map dynamic-map-name dynamic-seq-num set ikev1 transform-set
transform-set-name1, [transform-set-name2, …transform-set-name9]

crypto dynamic-map dynamic-map-name dynamic-seq-num set ikev2 ipsec-proposal
proposal-name1
[proposal-name2, … proposal-name11]
```

dynamic-map-name では、既存のダイナミック クリプト マップを参照するクリプト マップ エントリの名前を指定します。*dynamic-seq-num* では、ダイナミック クリプト マップ エントリに対応するシーケンス番号を指定します。*transform-set-name* は、作成または変更するトランスフォーム セットの名前です。*proposal-name* では、IKEv2 の IPsec プロポーザルの名前を 1 つ以上指定します。

例（IKEv1 の場合）：

```
crypto dynamic-map dyn 10 set ikev1 transform-set myset1 myset2
```

この例では、トラフィックが ACL 101 に一致したときに、SA は、どのトランスフォーム セットがピアのトランスフォーム セットに一致するかによって、myset1（第 1 プライオリティ）と myset2（第 2 プライオリティ）のいずれかを使用できます。

ステップ 3　（オプション）グローバル ライフタイムを無効にする場合は、ダイナミック クリプト マップの SA ライフタイムを指定します。

```
crypto dynamic-map dynamic-map-name dynamic-seq-num set security-association lifetime
{seconds seconds | kilobytes kilobytes}
```

dynamic-map-name では、既存のダイナミック クリプト マップを参照するクリプト マップ エントリの名前を指定します。*dynamic-seq-num* では、ダイナミック クリプト マップ エントリに対応するシーケンス番号を指定します。

次に例を示します。

```
crypto dynamic-map dyn1 10 set security-association lifetime seconds 2700
```

この例では、ダイナミック クリプト マップ dyn1 10 の指定時刻ライフタイムを 2700 秒（45 分）に短縮します。トラフィック量ライフタイムは変更されません。

ステップ 4　（オプション）IPsec がこのダイナミック クリプト マップに対して新しい SA を要求するときに PFS を要求するか、または IPsec ピアから受け取る要求に PFS を要求するかを指定します。

```
crypto dynamic-map dynamic-map-name dynamic-seq-num set pfs [group1 | group2 | group5 |
group7]
```

dynamic-map-name では、既存のダイナミック クリプト マップを参照するクリプト マップ エントリの名前を指定します。*dynamic-seq-num* では、ダイナミック クリプト マップ エントリに対応するシーケンス番号を指定します。

次に例を示します。

```
crypto dynamic-map dyn1 10 set pfs group5
```

ステップ 5　ダイナミック クリプト マップ セットをスタティック クリプト マップ セットに追加します。

ダイナミック マップを参照するクリプト マップは、必ずクリプト マップ セットの中でプライオリティ エントリを最低（シーケンス番号が最大）に設定してください。

```
crypto map map-name seq-num ipsec-isakmp dynamic dynamic-map-name
```

map-name では、クリプト マップ セットの名前を指定します。*dynamic-map-name* では、既存のダイナミック クリプト マップを参照するクリプト マップ エントリの名前を指定します。

次に例を示します。

```
crypto map mymap 200 ipsec-isakmp dynamic dyn1
```

サイトツーサイト冗長性の定義

クリプト マップを使用して複数の IKEv1 ピアを定義すると、冗長性を持たせることができます。このコンフィギュレーションはサイトツーサイト VPN に便利です。この機能は、IKEv2 ではサポートされません。

あるピアが失敗すると、ASA は、クリプト マップに関連付けられている次のピアへのトンネルを確立します。ネゴシエーションが成功したピアにデータが送信され、そのピアがアクティブ ピアになります。アクティブ ピアとは、後続のネゴシエーションのときに、ASA が常に最初に試みるピアのことです。これは、ネゴシエーションが失敗するまで続きます。ネゴシエーションが失敗した時点で、ASA は次のピアに移ります。クリプト マップに関連付けられているすべてのピアが失敗すると、ASA のサイクルは最初のピアに戻ります。

IPsec コンフィギュレーションの表示

表 1-6 に示すコマンドをシングルまたはマルチ コンテキスト モードで入力すると、IPsec コンフィギュレーションに関する情報を表示できます。

表 1-6　IPsec コンフィギュレーション情報を表示するためのコマンド

コマンド	目的
show running-configuration crypto	IPsec、クリプト マップ、ダイナミック クリプト マップ、ISAKMP など、暗号コンフィギュレーション全体を表示します。
show running-config crypto ipsec	IPsec コンフィギュレーション全体を表示します。
show running-config crypto isakmp	ISAKMP コンフィギュレーション全体を表示します。
show running-config crypto map	クリプト マップ コンフィギュレーション全体を表示します。
show running-config crypto dynamic-map	ダイナミック クリプト マップのコンフィギュレーションを表示します。
show all crypto map	すべてのコンフィギュレーション パラメータ（デフォルト値を持つパラメータも含む）を表示します。
show crypto ikev2 sa detail	暗号化統計情報での Suite-B アルゴリズム サポートを表示します。
show crypto ipsec sa	シングルまたはマルチ コンテキスト モードでの Suite-B アルゴリズム サポートおよび ESPv3 IPsec 出力を表示します。
show ipsec stats	シングルまたはマルチ コンテキスト モードでの IPsec サブシステムに関する情報を表示します。ESPv3 統計情報は、受信した TFC パケットおよび有効および無効な ICMP エラーに表示されます。

セキュリティ アソシエーションのクリア

一部のコンフィギュレーション変更は、後続の SA をネゴシエートしている間だけ有効になります。新しい設定をただちに有効にするには、既存の SA をクリアして、変更後のコンフィギュレーションで SA を再確立します。ASA がアクティブに IPsec トラフィックを処理している場合は、SA データベースのうち、コンフィギュレーション変更の影響を受ける部分だけをクリアします。SA データベースを完全にクリアするのは、大規模な変更の場合や、ASA が処理している IPsec トラフィック量が少ない場合に限定するようにしてください。

表 1-7 に示すコマンドを入力すると、シングルまたはマルチ コンテキスト モードで IPsec SA をクリアして再初期化することができます。

表 1-7　IPsec SA のクリアおよび再初期化用のコマンド

コマンド	目的
clear configure crypto	IPsec、クリプト マップ、ダイナミック クリプト マップ、ISAKMP など、暗号コンフィギュレーション全体を削除します。
clear configure crypto ca trustpoint	すべてのトラストポイントを削除します。
clear configure crypto dynamic-map	すべてのダイナミック クリプト マップを削除します。特定のダイナミック クリプト マップを削除できるキーワードもあります。
clear configure crypto map	すべてのクリプト マップを削除します。特定のクリプト マップを削除できるキーワードもあります。
clear configure crypto isakmp	ISAKMP コンフィギュレーション全体を削除します。
clear configure crypto isakmp policy	すべての ISAKMP ポリシーまたは特定のポリシーを削除します。
clear crypto isakmp sa	ISAKMP SA データベース全体を削除します。

クリプト マップ コンフィギュレーションのクリア

clear configure crypto コマンドには、IPsec、クリプト マップ、ダイナミック クリプト マップ、CA トラストポイント、すべての証明書、証明書マップ コンフィギュレーション、ISAKMP など、暗号コンフィギュレーションの要素を削除できる引数が含まれます。

引数を指定しないで **clear configure crypto** コマンドを入力すると、暗号コンフィギュレーション全体（すべての認証も含む）が削除されることに注意してください。

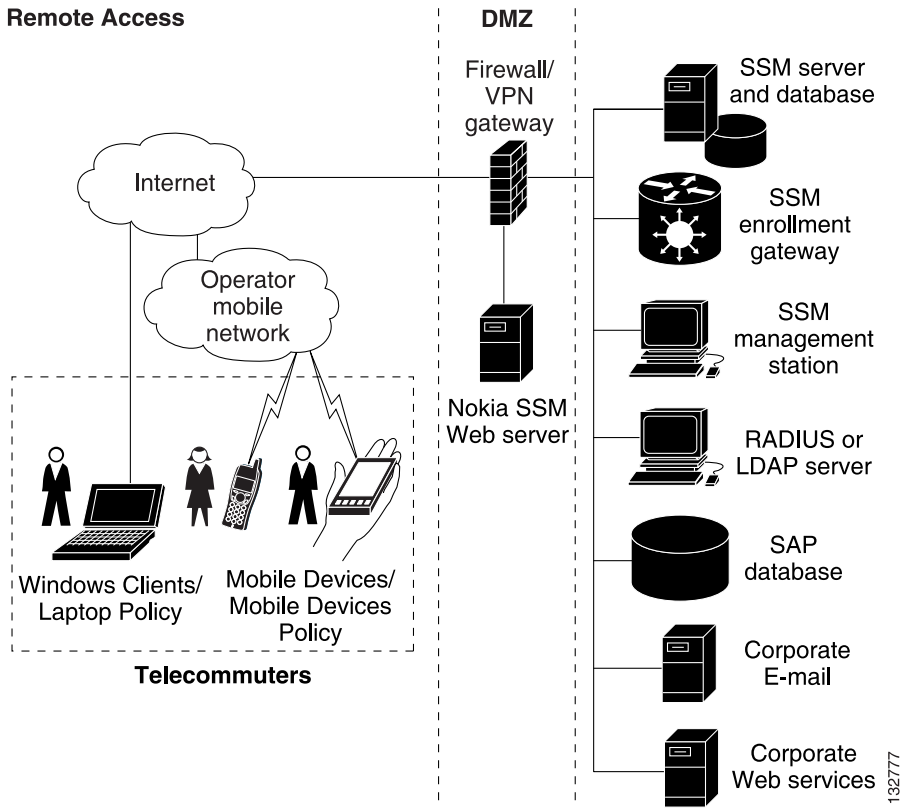
詳細については、『*Cisco ASA Series Command Reference*』の **clear configure crypto** コマンドを参照してください。

Nokia VPN クライアントのサポート

ASA は、Nokia 92xx Communicator シリーズ電話機上の Nokia VPN クライアントからの接続をサポートするために、Challenge/Response for Authenticated Cryptographic Keys（CRACK）プロトコルを使用します。CRACK は、デジタル証明書ではなくレガシーな認証技術を使用している、IPsec に対応したモバイル クライアントに最も適しています。クライアントがレガシーな方式に基づいた秘密キー認証技術（RADIUS など）を使用し、ゲートウェイが公開キー認証を使用している場合に、このプロトコルは相互認証を提供します。

Nokia のクライアントと CRACK プロトコルの両方をサポートするには、Nokia バックエンド サービスが稼働している必要があります。この要件には、図 1-5 に示すように、Nokia Security Services Manager（NSSM）と Nokia のデータベースが含まれます。

図 1-5　Nokia 92xx Communicator サービスの要件



Nokia VPN クライアントをサポートするには、ASA で次の手順を実行します。

- グローバル コンフィギュレーション モードで、**crypto isakmp policy** *priority* **authentication** コマンドに **crack** キーワードを指定して使用し、CRACK 認証をイネーブルにします。次に例を示します。

```
hostname(config)# crypto isakmp policy 2
hostname(config-isakmp-policy)# authentication crack
```

クライアント認証にデジタル証明書を使用する場合は、さらに次の手順を実行します。

ステップ 1　トラストポイントを設定し、完全修飾ドメイン名を不要にします。トラストポイントは、NSSM やその他の CA の場合があります。次の例では、トラストポイントには CompanyVPNCA という名前が付いています。

```
hostname(config)# crypto ca trustpoint CompanyVPNCA
hostname(config-ca-trustpoint)# fqdn none
```

ステップ 2　ISAKMP ピアの ID を設定するには、次のいずれかの手順を実行します。

- **crypto isakmp identity** コマンドに **hostname** キーワードを指定して使用します。次に例を示します。

```
hostname(config)# crypto isakmp identity hostname
```

- **crypto isakmp identity** コマンドに **auto** キーワードを指定して使用し、接続タイプから ID が自動的に判定されるように設定します。次に例を示します。

```
hostname(config)# crypto isakmp identity auto
```

（注）　**crypto isakmp identity auto** コマンドを使用する場合は、クライアント証明書に含まれる DN 属性が CN、OU、O、C、St、L の順になっていることを確認します。

Nokia クライアントで CRACK プロトコルをサポートするために必要な Nokia サービスの詳細、およびこれらのサービスのインストールと設定については、Nokia の代理店にお問い合わせください。

L2TP over IPsec

この章では、ASA での L2TP over IPsec/IKEv1 の設定方法について説明します。この章では、次の事項について説明します。

L2TP over IPsec/IKEv1 に関する情報

Layer 2 Tunneling Protocol（L2TP; レイヤ 2 トンネリング プロトコル）は、リモート クライアントがパブリック IP ネットワークを使用して、企業のプライベート ネットワーク サーバと安全に通信できるようにする VPN トンネリング プロトコルです。L2TP は、データのトンネリングに PPP over UDP（ポート 1701）を使用します。

L2TP プロトコルは、クライアント / サーバ モデルを基本にしています。機能は L2TP ネットワーク サーバ（LNS）と L2TP アクセス コンセントレータ（LAC）に分かれています。LNS は、通常、ルータなどのネットワーク ゲートウェイで実行されます。一方、LAC は、ダイヤルアップの Network Access Server（NAS; ネットワーク アクセス サーバ）や、Microsoft Windows、Apple iPhone、または Android などの L2TP クライアントが搭載されたエンドポイント デバイスで実行されます。

リモート アクセスのシナリオで、IPsec/IKEv1 を使用する L2TP を設定する最大の利点は、リモート ユーザがゲートウェイや専用回線を使わずにパブリック IP ネットワークを介して VPN にアクセスできることです。これにより、実質的にどの場所からでも POTS を使用してリモート アクセスが可能になります。この他に、Cisco VPN Client ソフトウェアなどの追加のクライアント ソフトウェアが必要ないという利点もあります。

（注） L2TP over IPsec は、IKEv1 だけをサポートしています。IKEv2 はサポートされていません。

IPsec/IKEv1 を使用する L2TP の設定では、事前共有キーまたは RSA シグニチャ方式を使用する証明書、および（スタティックではなく）ダイナミック クリプト マップの使用がサポートされます。ただし、ここで説明する概要手順では、IKEv1、および事前共有キーまたは RSA 署名の設定が完了していることを前提にしています。事前共有キー、RSA、およびダイナミック クリプト マップの設定手順については、一般的な操作のコンフィギュレーション ガイドの第 41 章「Digital Certificates」を参照してください。

（注）　ASA で IPsec を使用する L2TP を設定すると、Windows、MAC OS X、Android および Cisco IOS などのオペレーティング システムに統合されたネイティブ VPN クライアントと LNS が相互運用できるようになります。サポートされているのは、IPsec を使用する L2TP だけで、ネイティブの L2TP そのものは、ASA ではサポートされていません。
Windows クライアントがサポートしている IPsec セキュリティ アソシエーションの最短ライフタイムは 300 秒です。ASA でライフタイムを 300 秒未満に設定している場合、Windows クライアントはこの設定を無視して、300 秒のライフタイムに置き換えます。

IPsec の転送モードとトンネル モード

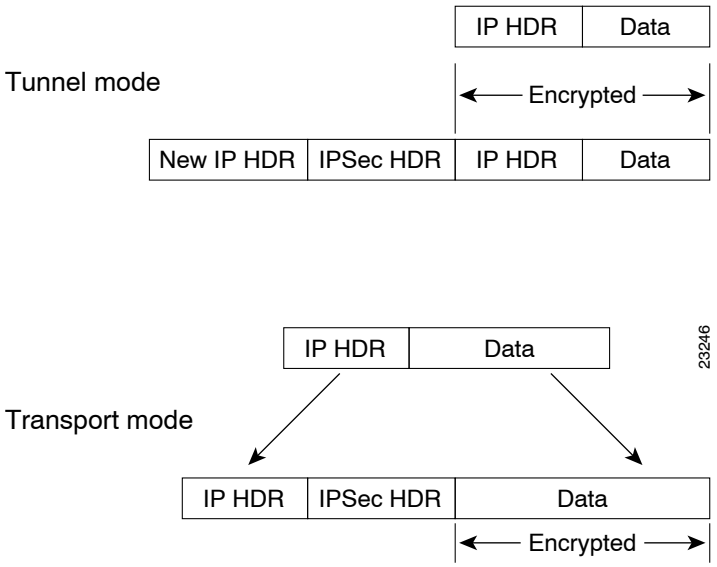
ASA は、デフォルトで IPsec トンネル モードを使用します。このモードでは、元の IP データグラム全体が暗号化され、新しい IP パケットのペイロードになります。このモードでは、ルータなどのネットワーク デバイスが IPsec のプロキシとして動作できます。つまり、ルータがホストに代わって暗号化を行います。送信元ルータがパケットを暗号化し、IPsec トンネルを使用して転送します。宛先ルータは元の IP データグラムを復号化し、宛先システムに転送します。トンネル モードの大きな利点は、エンド システムを変更しなくても IPsec を利用できるということです。また、トラフィック分析から保護することもできます。トンネル モードを使用すると、攻撃者にはトンネルのエンドポイントしかわからず、トンネリングされたパケットの本来の送信元と宛先はわかりません（これらがトンネルのエンドポイントと同じ場合でも同様）。

ただし、Windows の L2TP/IPsec クライアントは、IPsec 転送モードを使用します。このモードでは IP ペイロードだけが暗号化され、元の IP ヘッダーは暗号化されません。このモードには、各パケットに数バイトしか追加されず、パブリック ネットワーク上のデバイスに、パケットの最終的な送信元と宛先を認識できるという利点があります。図 2-1 に、IPsec のトンネル モードと転送モードの違いを示します。

Windows の L2TP および IPsec クライアントから ASA に接続するには、**crypto ipsec transform-set *trans_name* mode transport** コマンドを使用してトランスフォーム セット用に IPsec 転送モードを設定する必要があります。このコマンドは、設定手順で使用されます。

このような転送が可能になると、中間ネットワークでの特別な処理（たとえば QoS）を、IP ヘッダーの情報に基づいて実行できるようになります。ただし、レイヤ 4 ヘッダーが暗号化されるため、パケットの検査が制限されます。転送モードでは、IP ヘッダーがクリア テキストで送信されると、攻撃者に何らかのトラフィック分析を許すことになります。

図 2-1　IPsec のトンネル モードと転送モード



L2TP over IPsec のライセンス要件

次の表に、この機能のライセンス要件を示します。

（注）　この機能は、ペイロード暗号化機能のないモデルでは使用できません。

モデル	ライセンス要件[1]
ASA 5505	• IKEv2 を使用した IPsec リモート アクセス VPN（次のいずれかを使用）： – AnyConnect Premium ライセンス： 基本ライセンスと Security Plus ライセンス：2 セッション。 *オプションの永続または時間ベースのライセンス：10 または 25 セッション。* *共有ライセンスはサポートされていません。*[2] – AnyConnect Essentials ライセンス[3]：25 セッション。 • IKEv1 を使用した IPsec リモート アクセス VPN および IKEv1 または IKEv2 を使用した IPsec サイトツーサイト VPN： – 基本ライセンス：10 セッション。 – Security Plus ライセンス：25 セッション。

モデル	ライセンス要件[1]
ASA 5512-X	• IKEv2 を使用した IPsec リモート アクセス VPN（次のいずれかを使用）： – AnyConnect Premium ライセンス： 基本ライセンスと Security Plus ライセンス：2 セッション。 *オプションの永続または時間ベースのライセンス：10、25、50、100、または 250 セッション。* *オプションの共有ライセンス[2]：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。* – AnyConnect Essentials ライセンス[3]：250 セッション。 • IKEv1 を使用した IPsec リモート アクセス VPN および IKEv1 または IKEv2 を使用した IPsec サイトツーサイト VPN： 基本ライセンスと Security Plus ライセンス：250 セッション。
ASA 5515-X	• IKEv2 を使用した IPsec リモート アクセス VPN（次のいずれかを使用）： – AnyConnect Premium ライセンス： 基本ライセンス：2 セッション。 *オプションの永続または時間ベースのライセンス：10、25、50、100、または 250 セッション。* *オプションの共有ライセンス[2]：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。* – AnyConnect Essentials ライセンス[3]：250 セッション。 • IKEv1 を使用した IPsec リモート アクセス VPN および IKEv1 または IKEv2 を使用した IPsec サイトツーサイト VPN： 基本ライセンス：250 セッション。
ASA 5525-X	• IKEv2 を使用した IPsec リモート アクセス VPN（次のいずれかを使用）： – AnyConnect Premium ライセンス： 基本ライセンス：2 セッション。 *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、または 750 セッション。* *オプションの共有ライセンス[2]：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。* – AnyConnect Essentials ライセンス[3]：750 セッション。 • IKEv1 を使用した IPsec リモート アクセス VPN および IKEv1 または IKEv2 を使用した IPsec サイトツーサイト VPN： 基本ライセンス：750 セッション。

モデル	ライセンス要件[1]
ASA 5545-X	• IKEv2 を使用した IPsec リモート アクセス VPN（次のいずれかを使用）： – AnyConnect Premium ライセンス： 基本ライセンス：2 セッション。 *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、750、1000、または 2500 セッション。* *オプションの共有ライセンス[2]：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。* – AnyConnect Essentials ライセンス[3]：2500 セッション。 • IKEv1 を使用した IPsec リモート アクセス VPN および IKEv1 または IKEv2 を使用した IPsec サイトツーサイト VPN： 基本ライセンス：2500 セッション。
ASA 5555-X	• IKEv2 を使用した IPsec リモート アクセス VPN（次のいずれかを使用）： – AnyConnect Premium ライセンス： 基本ライセンス：2 セッション。 *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、750、1000、2500、または 5000 セッション。* *オプションの共有ライセンス[2]：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。* – AnyConnect Essentials ライセンス[3]：5000 セッション。 • IKEv1 を使用した IPsec リモート アクセス VPN および IKEv1 または IKEv2 を使用した IPsec サイトツーサイト VPN： 基本ライセンス：5000 セッション。
ASA 5585-X（SSP-10）	• IKEv2 を使用した IPsec リモート アクセス VPN（次のいずれかを使用）： – AnyConnect Premium ライセンス： 基本ライセンス：2 セッション。 *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、750、1000、2500、または 5000 セッション。* *オプションの共有ライセンス[2]：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。* – AnyConnect Essentials ライセンス[3]：5000 セッション。 • IKEv1 を使用した IPsec リモート アクセス VPN および IKEv1 または IKEv2 を使用した IPsec サイトツーサイト VPN： 基本ライセンス：5000 セッション。

モデル	ライセンス要件[1]
ASA 5585-X（SSP-20、-40、および -60）	• IKEv2 を使用した IPsec リモート アクセス VPN（次のいずれかを使用）： – AnyConnect Premium ライセンス： 基本ライセンス：2 セッション。 *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、750、1000、2500、5000、または 10000 セッション。* *オプションの共有ライセンス[2]：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。* – AnyConnect Essentials ライセンス[3]：10000 セッション。 • IKEv1 を使用した IPsec リモート アクセス VPN および IKEv1 または IKEv2 を使用した IPsec サイトツーサイト VPN： 基本ライセンス：10000 セッション。
ASASM	• IKEv2 を使用した IPsec リモート アクセス VPN（次のいずれかを使用）： – AnyConnect Premium ライセンス： 基本ライセンス：2 セッション。 *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、750、1000、2500、5000、または 10000 セッション。* *オプションの共有ライセンス[2]：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。* – AnyConnect Essentials ライセンス[3]：10000 セッション。 • IKEv1 を使用した IPsec リモート アクセス VPN および IKEv1 または IKEv2 を使用した IPsec サイトツーサイト VPN： 基本ライセンス：10000 セッション。
ASAv（仮想 CPU X 1 を搭載）	• IKEv2 を使用した IPsec リモート アクセス VPN： – 標準ライセンス：2 セッション。 – Premium ライセンス：250 セッション。 • IKEv1 を使用した IPsec リモート アクセス VPN および IKEv1 または IKEv2 を使用した IPsec サイトツーサイト VPN： 標準および Premium ライセンス：250 セッション。
ASAv（仮想 CPU X 4 を搭載）	• IKEv2 を使用した IPsec リモート アクセス VPN： – 標準ライセンス：2 セッション。 – Premium ライセンス：750 セッション。 • IKEv1 を使用した IPsec リモート アクセス VPN および IKEv1 または IKEv2 を使用した IPsec サイトツーサイト VPN： 標準および Premium ライセンス：750 セッション。

1. すべてのタイプの組み合わせ VPN セッションの最大数は、この表に示す最大セッション数を超えることはできません。ASA 5505 では、組み合わせセッションの最大数は 10（基本ライセンスの場合）または 25（Security Plus ライセンスの場合）です。
2. 共有ライセンスによって、ASA は複数のクライアントの ASA の共有ライセンス サーバとして機能します。共有ライセンス プールは大規模ですが、個々の ASA によって使用されるセッションの最大数は、永続的なライセンスで指定される最大数を超えることはできません。

3. AnyConnect Essentials ライセンスにより、AnyConnect VPN クライアントは ASA へのアクセスが可能になります。このライセンスでは、ブラウザベースの SSL VPN アクセスまたは Cisco Secure Desktop はサポートされていません。これらの機能に対しては、AnyConnect Essentials ライセンスの代わりに AnyConnect Premium ライセンスがアクティブ化されます。

   （注）AnyConnect Essentials ライセンスの場合、VPN ユーザは、Web ブラウザを使用してログインし、AnyConnect クライアントのダウンロードと起動（WebLaunch）を実行できます。

   このライセンスと AnyConnect Premium SSL VPN ライセンスのいずれでイネーブル化されたかには関係なく、AnyConnect クライアント ソフトウェアには同じクライアント機能のセットが装備されています。

   特定の ASA では、AnyConnect Premium ライセンス（全タイプ）または Advanced Endpoint Assessment ライセンスを、AnyConnect Essentials ライセンスと同時にアクティブにすることはできません。ただし、同じネットワーク内の異なる ASA で、AnyConnect Essentials ライセンスと AnyConnect Premium ライセンスを実行することは可能です。

   デフォルトでは、ASA は AnyConnect Essentials ライセンスを使用しますが、**webvpn** を使用し、次に **no anyconnect-essentials** コマンド を使用すると、AnyConnect Essentials ライセンスをディセーブルにして他のライセンスを使用できます。

   AnyConnect Essentials ライセンスおよび AnyConnect Premium ライセンスでサポートされている機能の詳細なリストについては、『*AnyConnect Secure Mobility Client Features, Licenses, and OSs*』を参照してください。

   http://www.cisco.com/en/US/products/ps10884/products_feature_guides_list.html

L2TP over IPsec を設定するための前提条件

L2TP over IPsec の設定については、次の前提条件があります。

- デフォルト グループ ポリシー（DfltGrpPolicy）またはユーザ定義グループ ポリシーを L2TP/IPsec 接続に対して設定できます。どちらの場合も、L2TP/IPsec トンネリング プロトコルを使用するには、グループ ポリシーを設定する必要があります。L2TP/IPsec トンネリング プロトコルがユーザ定義グループ ポリシーに対して設定されていない場合は、DfltGrpPolicy を L2TP/IPsec トンネリング プロトコルに対して設定し、ユーザ定義グループ ポリシーにこの属性を継承させます。
- 「事前共有キー」認証を実行する場合は、デフォルトの接続プロファイル（トンネル グループ）、DefaultRAGroup を設定する必要があります。証明書ベースの認証を実行する場合は、証明書 ID に基づいて選択できるユーザ定義接続プロファイルを使用できます。
- IP 接続性をピア間で確立する必要があります。接続性をテストするには、エンドポイントから ASA への IP アドレスの ping と、ASA からエンドポイントへの IP アドレスの ping を実行します。
- 接続パス上のどの場所でも、UDP ポート 1701 がブロックされていないことを確認してください。
- Windows 7 のエンドポイント デバイスが、SHA のシグニチャ タイプを指定する証明書を使用して認証を実行する場合、シグニチャ タイプは、ASA のシグニチャ タイプと SHA1 または SHA2 のいずれかが一致している必要があります。

ガイドラインと制限事項

この項では、この機能のガイドラインと制限事項について説明します。

コンテキスト モードのガイドライン

シングル コンテキスト モードでサポートされています。マルチ コンテキスト モードはサポートされていません。

ファイアウォール モードのガイドライン

ルーテッド ファイアウォール モードでだけサポートされています。トランスペアレント モードはサポートされていません。

フェールオーバーのガイドライン

L2TP over IPsec セッションはステートフル フェールオーバーではサポートされていません。

IPv6 のガイドライン

L2TP over IPsec に対してネイティブの IPv6 トンネル セットアップのサポートはありません。

認証のガイドライン

ローカル データベースの場合、ASA は、PPP 認証方式として PAP および Microsoft CHAP のバージョン 1 と 2 だけをサポートします。EAP と CHAP は、プロキシ認証サーバによって実行されます。そのため、リモート ユーザが **authentication eap-proxy** または **authentication chap** コマンドで設定したトンネル グループに所属している場合、ASA でローカル データベースを使用するように設定すると、このユーザは接続できなくなります。

サポートされている PPP 認証タイプ

ASA の L2TP over IPsec 接続は表 2-1 に示す PPP 認証タイプだけをサポートします。

表 2-1　AAA サーバ サポートと PPP 認証タイプ

AAA サーバ タイプ	サポートされている PPP 認証タイプ
LOCAL	PAP、MSCHAPv1、MSCHAPv2
RADIUS	PAP、CHAP、MSCHAPv1、MSCHAPv2、EAP-Proxy
TACACS+	PAP、CHAP、MSCHAPv1
LDAP	PAP
NT	PAP
Kerberos	PAP
SDI	SDI

表 2-2　PPP 認証タイプの特性

キーワード	認証タイプ	特性
chap	CHAP	サーバのチャレンジに対する応答で、クライアントは暗号化された「チャレンジとパスワード」およびクリアテキストのユーザ名を返します。このプロトコルは、PAP より安全ですが、データは暗号化されません。
eap-proxy	EAP	EAP をイネーブルにします。これによってセキュリティ アプライアンスは、PPP 認証プロセスを外部の RADIUS 認証サーバにプロキシします。
ms-chap-v1 **ms-chap-v2**	Microsoft CHAP、バージョン 1 Microsoft CHAP、バージョン 2	CHAP と似ていますが、サーバは、CHAP のようなクリアテキストのパスワードではなく、暗号化されたパスワードだけを保存および比較するのでよりセキュアです。また、このプロトコルはデータ暗号化のためのキーを MPPE によって生成します。
pap	PAP	認証中にクリアテキストのユーザ名とパスワードを渡すので、セキュアではありません。

L2TP over IPsec の設定

この項では、ASA IKEv1（ISAKMP）ポリシーの設定について説明します。これは、エンドポイント上のオペレーティング システムと統合されたネイティブ VPN クライアントが、L2TP over IPsec プロトコルを使用して ASA への VPN 接続を行う場合に必要です。

- IKEv1 フェーズ 1：SHA1 ハッシュ方式を使用する 3DES 暗号化
- IPsec フェーズ 2：MD5 または SHA ハッシュ方式を使用する 3DES または AES 暗号化
- PPP 認証：PAP、MS-CHAPv1、または MSCHAPv2（推奨）
- 事前共有キー（iPhone の場合に限る）

ASA 8.2.5 の詳細な CLI 設定手順

	コマンド	目的
ステップ 1	`crypto ipsec transform-set` *`transform_name ESP_Encryption_Type ESP_Authentication_Type`* **例：** `hostname(config)# crypto ipsec transform-set my-transform-set esp-des esp-sha-hmac`	特定の ESP 暗号化タイプおよび認証タイプで、トランスフォーム セットを作成します。
ステップ 2	`crypto ipsec transform-set` *`trans_name`* `mode transport` **例：** `hostname(config)# crypto ipsec transform-set my-transform-set mode transport`	IPsec にトンネル モードではなく転送モードを使用するように指示します。

	コマンド	目的
ステップ 3	**vpn-tunnel-protocol** *tunneling_protocol* **例：** hostname(config)# group-policy DfltGrpPolicy attributes hostname(config-group-policy)# vpn-tunnel-protocol l2tp-ipsec	L2TP/IPsec を vpn トンネリング プロトコルとして指定します。
ステップ 4	**dns value** [**none** | *IP_primary* [*IP_secondary*] **例：** hostname(config)# **group-policy** DfltGrpPolicy **attributes** hostname(config-group-policy)# **dns value** 209.165.201.1 209.165.201.2	（オプション）適応型セキュリティ アプライアンスに DNS サーバ IP アドレスをグループ ポリシーのクライアントに送信するように指示します。
ステップ 5	**wins-server value** [**none** | *IP_primary* [*IP_secondary*]] **例：** hostname(config)# **group-policy** DfltGrpPolicy **attributes** hostname (config-group-policy)# wins-server value 209.165.201.3 209.165.201.4	（オプション）適応型セキュリティ アプライアンスに WINS サーバ IP アドレスをグループ ポリシーのクライアントに送信するように指示します。
ステップ 6	**tunnel-group** *name* **type remote-access** **例：** hostname(config)# tunnel-group sales-tunnel type remote-access	接続プロファイル（トンネル グループ）を作成します。
ステップ 7	**default-group-policy** *name* **例：** hostname(config)# tunnel-group DefaultRAGroup general-attributes hostname(config-tunnel-general)# default-group-policy DfltGrpPolicy	グループ ポリシーの名前を接続プロファイル（トンネル グループ）にリンクします。
ステップ 8	**ip local pool** *pool_name starting_address-ending_address* **mask** *subnet_mask* **例：** hostname(config)# ip local pool sales_addresses 10.4.5.10-10.4.5.20 mask 255.255.255.0	（オプション）IP アドレス プールを作成します。
ステップ 9	**address-pool** *pool_name* **例：** hostname(config)# tunnel-group DefaultRAGroup general-attributes hostname(config-tunnel-general)# address-pool sales_addresses	（オプション）IP アドレス プールを接続プロファイル（トンネル グループ）と関連付けます。

	コマンド	目的
ステップ 10	**authentication-server-group** *server_group* **例：** hostname(config)# tunnel-group DefaultRAGroup general-attributes hostname(config-tunnel-general)# authentication-server-group sales_server LOCAL	L2TP over IPsec 接続を試行するユーザの認証方式を、接続プロファイル（トンネル グループ）に対して指定します。ローカル認証の実行に ASA を使用していない場合や、ローカル認証にフォールバックする場合は、コマンドの末尾に LOCAL を追加します。
ステップ 11	authentication *auth_type* **例：** hostname(config)# tunnel-group name ppp-attributes hostname(config-ppp)# authentication ms-chap-v1	トンネル グループに対して PPP 認証プロトコルを指定します。PPP 認証のタイプとその特性については、表 2-2 を参照してください。
ステップ 12	**tunnel-group** *tunnel group name* **ipsec-attributes** **例：** hostname(config)# tunnel-group DefaultRAGroup ipsec-attributes hostname(config-tunnel-ipsec)# pre-shared-key *cisco123*	接続プロファイル（トンネル グループ）の事前共有キーを設定します。
ステップ 13	**accounting-server-group** *aaa_server_group* **例：** hostname(config)# tunnel-group sales_tunnel general-attributes hostname(config-tunnel-general)# accounting-server-group sales_aaa_server	（オプション）接続プロファイル（トンネル グループ）に対して、L2TP セッション用に AAA アカウンティングの開始レコードと終了レコードを生成します。
ステップ 14	**l2tp tunnel hello** *seconds* **例：** hostname(config)# l2tp tunnel hello 100	hello メッセージの間隔を（秒単位で）設定します。範囲は 10 ～ 300 秒です。デフォルトは 60 秒です。
ステップ 15	**crypto isakmp nat-traversal** *seconds* **例：** hostname(config)# crypto isakmp enable hostname(config)# crypto isakmp nat-traversal 1500	（オプション）ESP パケットが 1 つ以上の NAT デバイスを通過できるように、NAT-Traversal をイネーブルにします。 NAT デバイスの背後に適応型セキュリティ アプライアンスへの L2TP over IPsec 接続を試行する L2TP クライアントが複数あると予想される場合、NAT-Traversal をイネーブルにする必要があります。 グローバルに NAT-Traversal をイネーブルにするには、グローバル コンフィギュレーション モードで ISAKMP がイネーブルになっていることをチェックし（**crypto isakmp enable** コマンドでイネーブルにできます）、次に **crypto isakmp nat-traversal** コマンドを使用します。

	コマンド	目的
ステップ 16	`strip-group` `strip-realm` **例：** `hostname(config)# tunnel-group DefaultRAGroup general-attributes` `hostname(config-tunnel-general)# strip-group` `hostname(config-tunnel-general)# strip-realm`	（オプション）トンネル グループのスイッチングを設定します。トンネル グループのスイッチングにより、ユーザがプロキシ認証サーバを使用して認証する場合に、VPN 接続の確立が容易になります。トンネル グループは、接続プロファイルと同義語です。
ステップ 17	**username** *name* **password** *password* **mschap** **例：** hostname`(config)# username xxxx password j!doe1 mschap`	次に、ユーザ名 `xxxx`、パスワード `j!doe1` でユーザを作成する例を示します。mschap オプションは、パスワードを入力した後に、そのパスワードが Unicode に変換され、MD4 を使用してハッシュされることを示します。 この手順が必要になるのは、ローカル ユーザ データベースを使用する場合だけです。
ステップ 18	**crypto isakmp policy** *priority* **例：** hostname(config)# crypto isakmp policy 5	crypto isakmp policy コマンドは、フェーズ 1 の IKE ポリシーを作成し、番号を割り当てます。IKE ポリシーの設定可能なパラメータは数種類あります。 ASA が IKE ネゴシエーションを完了するためには、isakamp ポリシーが必要です。 Windows 7 のネイティブ VPN クライアントの設定例については、「Windows 7 のプロポーザルに応答するための IKE ポリシーの作成」（P.2-12）を参照してください。

Windows 7 のプロポーザルに応答するための IKE ポリシーの作成

Windows 7 の L2TP/IPsec クライアントは、ASA との VPN 接続を確立するために、数種類の IKE ポリシーのプロポーザルを送信します。Windows 7 の VPN ネイティブ クライアントからの接続を容易にするために、次の IKE ポリシーのいずれかを定義します。

	コマンド	目的
ステップ 1	「ASA 8.2.5 の詳細な CLI 設定手順」（P.2-9）	「ASA 8.2.5 の詳細な CLI 設定手順」の手順に従ってください（ステップ 18 まで）。Windows 7 のネイティブ VPN クライアントの IKE ポリシーを設定するには、この表の追加の手順を実行します。
ステップ 2	**show run crypto isakmp** **例：** `hostname(config)# show run crypto isakmp`	既存の IKE ポリシーの属性と番号をすべて表示します。

	コマンド	目的
ステップ 3	**crypto isakmp policy** number **例：** hostname(config)# crypto isakmp policy *number* hostname(config-isakmp-policy)#	IKE ポリシーを設定できます。number 引数には、設定する IKE ポリシーの番号を指定します。この番号は、show run crypto isakmp コマンドの出力で表示されたものです。
ステップ 4	**authentication** **例：** hostname(config-isakmp-policy)# authentication pre-share	各 IPsec ピアの ID を確立し、事前共有キーを使用するために、ASA が使用する認証方式を設定します。
ステップ 5	**encryption** *type* **例：** hostname(config-isakmp-policy)# encryption {3des|aes|aes-256}	2 つの IPsec ピア間で伝送されるユーザ データを保護する対称暗号化方式を選択します。Windows 7 の場合は、**3des**、**aes**（128 ビット AES の場合）、または **aes-256** を選択します。
ステップ 6	**hash** **例：** hostname(config-isakmp-policy)# hash sha	データの整合性を保証するハッシュ アルゴリズムを選択します。Windows 7 の場合は、SHA-1 アルゴリズムに **sha** を指定します。
ステップ 7	group **例：** hostname(config-isakmp-policy)# group 5	Diffie-Hellman グループ識別番号を選択します。Windows 7 の場合は、1536 ビット Diffie-Hellman グループを表す 5 を指定します。
ステップ 8	lifetime **例：** hostname(config-isakmp-policy)# lifetime 86400	SA ライフタイム（秒）を指定します。Windows 7 の場合は、86400 秒（24 時間）を指定します。

ASA 8.4.1 以降の詳細な CLI 設定手順

	コマンド	目的
ステップ 1	crypto ipsec *ike_version* transform-set *transform_name ESP_Encryption_Type ESP_Authentication_Type* **例：** crypto ipsec ikev1 transform-set my-transform-set-ikev1 esp-des esp-sha-hmac	特定の ESP 暗号化タイプおよび認証タイプで、トランスフォーム セットを作成します。
ステップ 2	crypto ipsec *ike_version* transform-set *trans_name* mode transport **例：** crypto ipsec ikev1 transform-set my-transform-set-ikev1 mode transport	IPsec にトンネル モードではなく転送モードを使用するように指示します。

	コマンド	目的
ステップ 3	**vpn-tunnel-protocol** *tunneling_protocol* **例：** hostname(config)# group-policy DfltGrpPolicy attributes hostname(config-group-policy)# vpn-tunnel-protocol l2tp-ipsec	L2TP/IPsec を vpn トンネリング プロトコルとして指定します。
ステップ 4	**dns value** [**none** | *IP_primary* [*IP_secondary*] **例：** hostname(config)# **group-policy** DfltGrpPolicy **attributes** hostname(config-group-policy)# **dns value** 209.165.201.1 209.165.201.2	（オプション）適応型セキュリティ アプライアンスに DNS サーバ IP アドレスをグループ ポリシーのクライアントに送信するように指示します。
ステップ 5	**wins-server value** [**none** | *IP_primary* [*IP_secondary*]] **例：** hostname(config)# **group-policy** DfltGrpPolicy **attributes** hostname (config-group-policy)# wins-server value 209.165.201.3 209.165.201.4	（オプション）適応型セキュリティ アプライアンスに WINS サーバ IP アドレスをグループ ポリシーのクライアントに送信するように指示します。
ステップ 6	**ip local pool** *pool_name starting_address-ending_address* **mask** *subnet_mask* **例：** hostname(config)# ip local pool sales_addresses 10.4.5.10-10.4.5.20 mask 255.255.255.0	（オプション）IP アドレス プールを作成します。
ステップ 7	**address-pool** *pool_name* **例：** hostname(config)# tunnel-group DefaultRAGroup general-attributes hostname(config-tunnel-general)# address-pool sales_addresses	（オプション）IP アドレス プールを接続プロファイル（トンネル グループ）と関連付けます。
ステップ 8	**tunnel-group** *name* **type remote-access** **例：** hostname(config)# tunnel-group sales-tunnel type remote-access	接続プロファイル（トンネル グループ）を作成します。
ステップ 9	**default-group-policy** *name* **例：** hostname(config)# tunnel-group DefaultRAGroup general-attributes hostname(config-tunnel-general)# default-group-policy DfltGrpPolicy	グループ ポリシーの名前を接続プロファイル（トンネル グループ）にリンクします。

	コマンド	目的
ステップ 10	**authentication-server-group** *server_group* [local] **例：** hostname(config)# tunnel-group DefaultRAGroup general-attributes hostname(config-tunnel-general)# authentication-server-group sales_server LOCAL	L2TP over IPsec 接続を試行するユーザの認証方式を、接続プロファイル（トンネル グループ）に対して指定します。ローカル認証の実行に ASA を使用していない場合や、ローカル認証にフォールバックする場合は、コマンドの末尾に LOCAL を追加します。
ステップ 11	**authentication** *auth_type* **例：** hostname(config)# tunnel-group *name* ppp-attributes hostname(config-ppp)# authentication ms-chap-v1	トンネル グループに対して PPP 認証プロトコルを指定します。PPP 認証のタイプとその特性については、表 2-2 を参照してください。
ステップ 12	**tunnel-group** *tunnel group name* **ipsec-attributes** **例：** hostname(config)# tunnel-group DefaultRAGroup ipsec-attributes hostname(config-tunnel-ipsec)# ikev1 pre-shared-key *cisco123*	接続プロファイル（トンネル グループ）の事前共有キーを設定します。
ステップ 13	**accounting-server-group** *aaa_server_group* **例：** hostname(config)# tunnel-group sales_tunnel general-attributes hostname(config-tunnel-general)# accounting-server-group sales_aaa_server	（オプション）接続プロファイル（トンネル グループ）に対して、L2TP セッション用に AAA アカウンティングの開始レコードと終了レコードを生成します。
ステップ 14	**l2tp tunnel hello** *seconds* **例：** hostname(config)# l2tp tunnel hello 100	hello メッセージの間隔を（秒単位で）設定します。範囲は 10 ～ 300 秒です。デフォルト インターバルは 60 秒です。
ステップ 15	**crypto isakmp nat-traversal** *seconds* **例：** hostname(config)# crypto isakmp enable hostname(config)# crypto isakmp nat-traversal 1500	（オプション）ESP パケットが 1 つ以上の NAT デバイスを通過できるように、NAT-Traversal をイネーブルにします。 NAT デバイスの背後に適応型セキュリティ アプライアンスへの L2TP over IPsec 接続を試行する L2TP クライアントが複数あると予想される場合、NAT-Traversal をイネーブルにする必要があります。 グローバルに NAT-Traversal をイネーブルにするには、グローバル コンフィギュレーション モードで ISAKMP がイネーブルになっていることをチェックし（**crypto isakmp enable** コマンドでイネーブルにできます）、次に **crypto isakmp nat-traversal** コマンドを使用します。

	コマンド	目的
ステップ 16	`strip-group` `strip-realm` **例：** `hostname(config)# tunnel-group DefaultRAGroup general-attributes` `hostname(config-tunnel-general)# strip-group` `hostname(config-tunnel-general)# strip-realm`	（オプション）トンネル グループのスイッチングを設定します。トンネル グループのスイッチングにより、ユーザがプロキシ認証サーバを使用して認証する場合に、VPN 接続の確立が容易になります。トンネル グループは、接続プロファイルと同義語です。
ステップ 17	**username** *name* **password** *password* **mschap** **例：** `asa2(config)# username jdoe password j!doe1 mschap`	次に、ユーザ名 `jdoe`、パスワード `j!doe1` でユーザを作成する例を示します。mschap オプションは、パスワードを入力した後に、そのパスワードが Unicode に変換され、MD4 を使用してハッシュされることを示します。 この手順が必要になるのは、ローカル ユーザ データベースを使用する場合だけです。
ステップ 18	**crypto ikev1 policy** *priority* **group** *Diffie-Hellman Group* **例：** `hostname(config)# crypto ikev1 policy 5` `hostname(config-ikev1-policy)# group 5`	crypto isakmp policy コマンドは、フェーズ 1 の IKE ポリシーを作成し、番号を割り当てます。IKE ポリシーの設定可能なパラメータは数種類あります。 ポリシーの Diffie-Hellman グループも指定できます。 ASA が IKE ネゴシエーションを完了するためには、isakamp ポリシーが必要です。 Windows 7 のネイティブ VPN クライアントの設定例については、「Windows 7 のプロポーザルに応答するための IKE ポリシーの作成」（P.2-16）を参照してください。

Windows 7 のプロポーザルに応答するための IKE ポリシーの作成

Windows 7 の L2TP/IPsec クライアントは、ASA との VPN 接続を確立するために、数種類の IKE ポリシーのプロポーザルを送信します。Windows 7 の VPN ネイティブ クライアントからの接続を容易にするために、次の IKE ポリシーのいずれかを定義します。

	コマンド	目的
ステップ 1	「ASA 8.4.1 以降の詳細な CLI 設定手順」（P.2-13）	「ASA 8.4.1 以降の詳細な CLI 設定手順」の手順に従ってください（ステップ 18 まで）。Windows 7 のネイティブ VPN クライアントの IKE ポリシーを設定するには、この表の追加の手順を実行します。
ステップ 2	**show run crypto ikev1** **例：** `hostname(config)# show run crypto ikev1`	既存の IKE ポリシーの属性と番号をすべて表示します。

	コマンド	目的
ステップ 3	**crypto ikev1 policy** number **例：** hostname(config)# crypto ikev1 policy *number* hostname(config-ikev1-policy)#	IKE ポリシーを設定できます。number 引数には、設定する IKE ポリシーの番号を指定します。この番号は、`show run crypto ikev1` コマンドの出力で表示されたものです。
ステップ 4	**authentication** **例：** hostname(config-ikev1-policy)# authentication pre-share	各 IPsec ピアの ID を確立し、事前共有キーを使用するために、ASA が使用する認証方式を設定します。
ステップ 5	**encryption** *type* **例：** hostname(config-ikev1-policy)# encryption {3des|aes|aes-256}	2 つの IPsec ピア間で伝送されるユーザ データを保護する対称暗号化方式を選択します。Windows 7 の場合は、**3des**、**aes**（128 ビット AES の場合）、または **aes-256** を選択します。
ステップ 6	**hash** **例：** hostname(config-ikev1-policy)# hash sha	データの整合性を保証するハッシュ アルゴリズムを選択します。Windows 7 の場合は、SHA-1 アルゴリズムに **sha** を指定します。
ステップ 7	group **例：** hostname(config-ikev1-policy)# group 5	Diffie-Hellman グループ識別番号を選択します。aes、aes-256、または 3des 暗号化タイプには 5 を指定できます。2 は 3des 暗号化タイプだけに指定できます。
ステップ 8	lifetime **例：** hostname(config-ikev1-policy)# lifetime 86400	SA ライフタイム（秒）を指定します。Windows 7 の場合は、86400 秒（24 時間）を指定します。

ASA 8.2.5 を使用する L2TP over IPsec の設定例

次に、任意のオペレーティング システム上のネイティブ VPN クライアントと ASA との互換性を保持するコンフィギュレーション ファイルのコマンドの例を示します。

```
ip local pool sales_addresses 209.165.202.129-209.165.202.158
group-policy sales_policy internal
group-policy sales_policy attributes
    wins-server value 209.165.201.3 209.165.201.4
    dns-server value 209.165.201.1 209.165.201.2
    vpn-tunnel-protocol l2tp-ipsec
tunnel-group DefaultRAGroup general-attributes
    default-group-policy sales_policy
    address-pool sales_addresses
tunnel-group DefaultRAGroup ipsec-attributes
    pre-shared-key *
tunnel-group DefaultRAGroup ppp-attributes
    no authentication pap
    authentication chap
    authentication ms-chap-v1
    authentication ms-chap-v2
crypto ipsec transform-set trans esp-3des esp-sha-hmac
crypto ipsec transform-set trans mode transport
```

```
crypto dynamic-map dyno 10 set transform-set set trans
crypto map vpn 20 ipsec-isakmp dynamic dyno
crypto map vpn interface outside
crypto isakmp enable outside
crypto isakmp policy 10
    authentication pre-share
    encryption 3des
    hash sha
    group 2
    lifetime 86400
```

ASA 8.4.1 以降を使用する L2TP over IPsec の設定例

次に、任意のオペレーティング システム上のネイティブ VPN クライアントと ASA との互換性を保持するコンフィギュレーション ファイルのコマンドの例を示します。

```
ip local pool sales_addresses 209.165.202.129-209.165.202.158
group-policy sales_policy internal
group-policy sales_policy attributes
    wins-server value 209.165.201.3 209.165.201.4
    dns-server value 209.165.201.1 209.165.201.2
    vpn-tunnel-protocol l2tp-ipsec
tunnel-group DefaultRAGroup general-attributes
    default-group-policy sales_policy
    address-pool sales_addresses
tunnel-group DefaultRAGroup ipsec-attributes
    pre-shared-key *
tunnel-group DefaultRAGroup ppp-attributes
    no authentication pap
    authentication chap
    authentication ms-chap-v1
    authentication ms-chap-v2
crypto ipsec ikev1 transform-set my-transform-set-ikev1 esp-des esp-sha-hmac
crypto ipsec ikev1 transform-set my-transform-set-ikev1 mode transport
crypto dynamic-map dyno 10 set ikev1 transform-set trans
crypto map vpn 20 ipsec-isakmp dynamic dyno
crypto map vpn interface outside
crypto ikev1 enable outside
crypto ikev1 policy 10
    authentication pre-share
    encryption 3des
    hash sha
    group 2
    lifetime 86400
```

L2TP over IPsec の機能履歴

表 2-3 に、この機能のリリース履歴を示します。

表 2-3　L2TP over IPsec の機能履歴

機能名	リリース	機能情報
L2TP over IPsec	7.2(1)	L2TP over IPsec は、単一のプラットフォームで IPsec VPN サービスとファイアウォール サービスとともに L2TP VPN ソリューションを展開および管理する機能を提供します。 リモート アクセスのシナリオで、L2TP over IPsec を設定する最大の利点は、リモート ユーザがゲートウェイや専用回線を使わずにパブリック IP ネットワークを介して VPN にアクセスできることです。これにより、実質的にどの場所からでも POTS を使用してリモート アクセスが可能になります。この他に、VPN にアクセスするクライアントは Windows で Microsoft Dial-Up Networking（DUN; ダイヤルアップ ネットワーク）を使用するだけでよいという利点もあります。Cisco VPN Client ソフトウェアなど、追加のクライアント ソフトウェアは必要ありません。 **authentication eap-proxy**、**authentication ms-chap-v1**、**authentication ms-chap-v2**、**authentication pap**、**l2tp tunnel hello**、および **vpn-tunnel-protocol l2tp-ipsec** コマンドが導入または変更されました。

全般 VPN パラメータ

バーチャル プライベート ネットワークの ASA の実装には、カテゴリの枠を越えた便利な機能があります。この章では、これらの機能のいくつかについて説明します。内容は次のとおりです。

ACL をバイパスするための IPsec の設定

この章の SSL VPN は、クライアントレス（ブラウザベース）SSL VPN が指定されていない限り、SSL VPN クライアント（AnyConnect 2.x またはその前身である SVC 1.x）を指します。IPsec トンネルから送信されるすべてのパケットに対して、ACL で発信元インターフェイスと宛先インターフェイスをチェックせずに許可するには、グローバル コンフィギュレーション モードで **sysopt connection permit-vpn** コマンドを入力します。

IPsec トラフィックのインターフェイス ACL をバイパスする必要があるのは、ASA の背後で別の VPN コンセントレータを使用し、なおかつ ASA のパフォーマンスを最大限にする場合などです。通常、IPsec パケットを許可する ACL を **access-list** コマンドを使用して作成し、これを発信元インターフェイスに適用します。ACL を使用すると、ASA を通過できるトラフィックを正確に指定できるため、セキュリティが向上します。

構文は、**sysopt connection permit-vpn** です。このコマンドには、キーワードも引数もありません。

次の例では、ACL をチェックせずに ASA を通過する IPsec トラフィックをイネーブルにします。

```
hostname(config)# sysopt connection permit-vpn
```

（注）　**no sysopt connection permit-vpn** が設定されている間は、外部インターフェイスで access-group が設定されていたとしても、クライアントからの復号化された通過トラフィックが許可されます。これは、**deny ip any any** ACL を呼び出します。

外部インターフェイスのアクセス コントロール リスト（ACL）と共に **no sysopt permit-vpn** コマンドを使用して、サイトツーサイト VPN またはリモート アクセス VPN 経由での保護されたネットワークへのアクセスを制御しようとしても、うまくいきません。

このような状況では、内部の管理アクセスがイネーブルになっていると、ACL は適用されず、ユーザは SSH を使用して ASA に引き続き接続できます。内部ネットワーク上のホストへのトラフィックは ACL によって正しくブロックされますが、内部インターフェイスへの復号化された通過トラフィックはブロックされません。

ssh および **http** コマンドは、ACL よりもプライオリティが高くなります。つまり、VPN セッションからボックスへの SSH、Telnet、または ICMP トラフィックを拒否するには、**ssh**、**telnet**、および **icmp** コマンドを使用します。

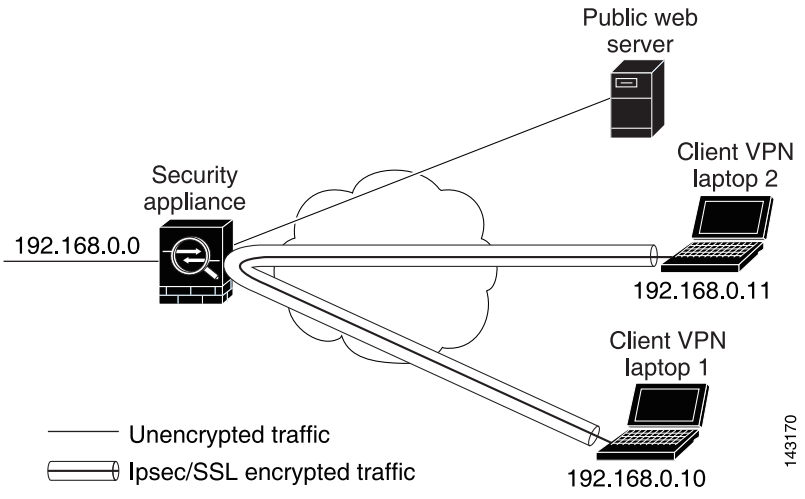
インターフェイス内トラフィックの許可（ヘアピニング）

ASA には、IPsec で保護されたトラフィックに対して、同じインターフェイスの出入りを許可することにより、VPN クライアントが別の VPN ユーザに IPsec で保護されたトラフィックを送信できる機能があります。「ヘアピニング」とも呼ばれるこの機能は、VPN ハブ（ASA）を介して接続している VPN スポーク（クライアント）と見なすことができます。

別のアプリケーションでは、ヘアピニングにより、着信 VPN トラフィックを同じインターフェイスを介して暗号化されていないトラフィックとしてリダイレクトできます。この機能は、たとえば、スプリット トンネリングがない状態で、VPN へのアクセスと Web のブラウズの両方を行う必要がある VPN クライアントに役立ちます。

図 3-1 では、VPN クライアント 1 が VPN クライアント 2 に対してセキュアな IPsec トラフィックを送信し、パブリック Web サーバに対しては暗号化されていないトラフィックを送信していることを示しています。

図 3-1　　ヘアピニングにインターフェイス内機能を使用する VPN クライアント



この機能を設定するには、グローバル コンフィギュレーション モードで **intra-interface** 引数を指定して **same-security-traffic** コマンドを実行します。

コマンドの構文は、**same-security-traffic permit** {**inter-interface** | **intra-interface**} です。

次の例では、インターフェイス内トラフィックをイネーブルにする方法を示しています。

```
hostname(config)# same-security-traffic permit intra-interface
hostname(config)#
```

（注）　**same-security-traffic** コマンドに **inter-interface** 引数を指定すると、セキュリティ レベルが同一のインターフェイス間の通信を許可します。この機能は、IPsec 接続に固有のものではありません。詳細については、このマニュアルの「インターフェイス パラメータの設定」の章を参照してください。

ヘアピニングを使用するには、次の項で説明するように、適切な NAT ルールを ASA インターフェイスに適用する必要があります。

インターフェイス内トラフィックにおける NAT の注意事項

ASA がインターフェイスを介して暗号化されていないトラフィックを送信するには、そのインターフェイスに対する NAT をイネーブルにし、プライベート IP アドレスをパブリックにルーティング可能なアドレスに変換する必要があります（ただし、ローカル IP アドレス プールですでにパブリック IP アドレスを使用している場合は除きます）。次の例では、クライアント IP プールから発信されたトラフィックに、インターフェイス PAT ルールを適用しています。

```
hostname(config)# ip local pool clientpool 192.168.0.10-192.168.0.100
hostname(config)# object network vpn_nat
hostname(config-network-object)# subnet 192.168.0.0 255.255.255.0
hostname(config-network-object)# nat (outside,outside) interface
```

ただし、ASA がこの同じインターフェイスから暗号化された VPN トラフィックを送信する場合、NAT は任意です。VPN 間ヘアピニングは、NAT を使用してもしなくても機能します。すべての発信トラフィックに NAT を適用するには、上記のコマンドを実装するだけです。VPN 間トラフィックを NAT から免除するには、次のように、VPN 間トラフィックの NAT 免除を実装するコマンドを（上記のコマンドに）追加します。

```
hostname(config)# nat (outside,outside) source static vpn_nat vpn_nat destination static
vpn_nat vpn_nat
```

NAT ルールの詳細については、このマニュアルの「NAT の適用」の章を参照してください。

アクティブな IPsec セッションまたは SSL VPN セッションの最大数の設定

VPN セッションの数を ASA が許可する数よりも小さい値に制限するには、グローバル コンフィギュレーション モードで **vpn-sessiondb** コマンドを入力します。

vpn-sessiondb {**max-anyconnect-premium-or-essentials-limit** <*number*> |
max-other-vpn-limit <*number*>}

max-anyconnect-premium-or-essentials-limit キーワードは、ライセンスで許可される AnyConnect セッションの数を 1 から最大数まで指定します。

max-other-vpn-limit キーワードは、ライセンスで許可される（AnyConnect クライアント セッション以外の）VPN セッションの数を 1 から最大数まで指定します。これには、Cisco VPN Client（IPsec IKEv1）、LAN-to-LAN VPN、およびクライアントレス SSL VPN セッションが含まれます。

このセッション数の制限は、VPN ロード バランシング用に算出されたロード率に影響します。

次に、最大 Anyconnect VPN セッション数の制限を 450 に設定する例を示します。

```
hostname(config)# vpn-sessiondb max-anyconnect-premium-or-essentials-limit 450
hostname(config)#
```

許可される IPsec クライアント リビジョン レベル確認のためのクライアント アップデートの使用

（注）　この項の情報は、IPsec 接続にのみ適用されます。

クライアント アップデート機能を使用すると、中央にいる管理者は、VPN クライアント ソフトウェアをアップデートする時期と VPN 3002 ハードウェア クライアント イメージを、VPN クライアント ユーザに自動的に通知できます。

リモート ユーザは、旧式の VPN ソフトウェア バージョンまたはハードウェア クライアント バージョンを使用している可能性があります。**client-update** コマンドを使用すると、いつでもクライアント リビジョンのアップデートをイネーブルにして、アップデートを適用するクライアントのタイプおよびリビジョン番号を指定し、アップデートを取得する URL または IP アドレスを提供できます。また、Windows クライアントの場合は、オプションで、VPN クライアント バージョンをアップデートする必要があることをユーザに通知できます。Windows クライアントに対しては、アップデートを実行するメカニズムをユーザに提供できます。VPN 3002 ハードウェア クライアント ユーザの場合、アップデートは通知せずに自動的に行われます。このコマンドは、IPsec リモート アクセス トンネル グループ タイプにのみ適用されます。

クライアント アップデートを実行するには、一般コンフィギュレーション モードまたはトンネル グループ ipsec 属性コンフィギュレーション モードで **client-update** コマンドを入力します。リビジョン番号のリストにあるソフトウェア バージョンをすでに実行しているクライアントの場合は、ソフトウェアをアップデートする必要はありません。リストにあるソフトウェア バージョンを実行していないクライアントの場合は、ソフトウェアをアップデートする必要があります。次の手順は、クライアント アップデートの実行方法を示しています。

ステップ 1　グローバル コンフィギュレーション モードで、次のコマンドを入力してクライアント アップデートをイネーブルにします。

```
hostname(config)# client-update enable
hostname(config)#
```

ステップ 2　グローバル コンフィギュレーション モードで、特定のタイプのすべてのクライアントに適用するクライアント アップデートのパラメータを指定します。つまり、クライアントのタイプ、アップデート イメージを取得する URL または IP アドレス、および許可されるリビジョン番号または対象クライアントの番号を指定します。最大 4 つのリビジョン番号をカンマで区切って指定できます。

ユーザのクライアント リビジョン番号が、指定したリビジョン番号のいずれかと一致する場合、そのクライアントをアップデートする必要はありません。このコマンドは、ASA 全体にわたって指定されているタイプのすべてのクライアントのクライアント アップデート値を指定します。

次の構文を使用します。

```
hostname(config)# client-update type type url url-string rev-nums rev-numbers
hostname(config)#
```

使用可能なクライアント タイプは、**win9X**（Windows 95、Windows 98、および Windows ME プラットフォーム）、**winnt**（Windows NT 4.0、Windows 2000、および Windows XP プラットフォーム）、**windows**（すべての Windows ベースのプラットフォーム）、および **vpn3002**（VPN 3002 ハードウェア クライアント）です。

リビジョン番号のリストにあるソフトウェア バージョンをすでに実行しているクライアントの場合は、ソフトウェアをアップデートする必要はありません。リストにあるソフトウェア バージョンを実行していないクライアントの場合は、ソフトウェアをアップデートする必要があります。これらのクライアント アップデート エントリから 3 つまで指定することができます。キーワード **windows** を指定すると、許可されるすべての Windows プラットフォームがカバーされます。**windows** を指定する場合は、個々の Windows クライアント タイプは指定しないでください。

（注）　すべての Windows クライアントでは、URL のプレフィックスとしてプロトコル http:// または https:// を使用する必要があります。VPN 3002 ハードウェア クライアントの場合、代わりにプロトコル tftp:// を指定する必要があります。

次の例では、リモート アクセス トンネル グループのクライアント アップデート パラメータを設定しています。リビジョン番号 4.6.1 とアップデートを取得するための URL（https://support/updates）を指定します。

```
hostname(config)# client-update type windows url https://support/updates/ rev-nums 4.6.1
hostname(config)#
```

あるいは、特定のタイプのすべてのクライアントではなく、個々のトンネル グループだけのためのクライアント アップデートを設定できます （ステップ 3 を参照）。

VPN 3002 クライアントはユーザの介入なしでアップデートされ、ユーザは通知メッセージを受信しません。次の例は、VPN 3002 ハードウェア クライアントだけに適用されます。トンネル グループ ipsec 属性コンフィギュレーション モードを開始すると、このコマンドによって、IPsec リモート アクセス トンネル グループ **salesgrp** 用のクライアント アップデート パラメータが設定されます。次の例では、リビジョン番号 4.7 を指定し、TFTP プロトコルを使用して、アップデートされたソフトウェアを IP アドレス 192.168.1.1 のサイトから取得します。

```
hostname(config)# tunnel-group salesgrp type ipsec-ra
hostname(config)# tunnel-group salesgrp ipsec-attributes
hostname(config-tunnel-ipsec)# client-update type vpn3002 url tftp:192.168.1.1 rev-nums
4.7
```

```
hostname(config-tunnel-ipsec)#
```

（注）　URL の末尾にアプリケーション名を含めることで（例：**https://support/updates/vpnclient.exe**）、アプリケーションを自動的に起動するようにブラウザを設定できます。

ステップ 3　特定の ipsec-ra トンネル グループの client-update パラメータのセットを定義します。

トンネル グループ ipsec 属性モードで、トンネル グループ名とそのタイプ、アップデートされたイメージを取得する URL または IP アドレス、およびリビジョン番号を指定します。ユーザのクライアントのリビジョン番号が、指定されているリビジョン番号のいずれかと一致している場合、クライアントをアップデートする必要はありません。たとえば、Windows クライアントの場合、次のコマンドを入力します。

```
hostname(config)# tunnel-group remotegrp type ipsec-ra
hostname(config)# tunnel-group remotegrp ipsec-attributes
hostname(config-tunnel-ipsec)# client-update type windows url https://support/updates/
rev-nums 4.6.1
hostname(config-tunnel-ipsec)#
```

ステップ 4　（オプション）クライアントのアップデートが必要な旧式の Windows クライアントを使用しているアクティブなユーザに通知を送信します。これらのユーザにはポップアップ ウィンドウが表示され、ブラウザを起動して、URL で指定したサイトからアップデートされたソフトウェアをダウンロードする機会が提供されます。このメッセージで設定可能な部分は URL だけです （ステップ 2 または 3 を参照）。アクティブでないユーザは、次回ログイン時に通知メッセージを受信します。この通知は、すべてのトンネル グループのすべてのアクティブ クライアントに送信するか、または特定のトンネル グループのクライアントに送信できます。たとえば、すべてのトンネル グループのすべてのアクティブ クライアントに通知する場合は、特権 EXEC モードで次のコマンドを入力します。

```
hostname# client-update all
hostname#
```

ユーザのクライアントのリビジョン番号が指定されているリビジョン番号のいずれかと一致している場合、そのクライアントをアップデートする必要はなく、通知メッセージはユーザに送信されません。VPN 3002 クライアントはユーザの介入なしでアップデートされ、ユーザは通知メッセージを受信しません。

（注）　クライアント アップデート タイプを **windows**（Windows ベースのすべてのプラットフォーム）に指定し、その後、同じエンティティに **win9x** または **winnt** のクライアント アップデート タイプを入力する必要が生じた場合は、まずこのコマンドの **no** 形式で windows クライアント タイプを削除してから、新しい client-update コマンドを使用して新しいクライアント タイプを指定します。

パブリック IP 接続への NAT 割り当てによる IP アドレスの実装

まれに、内部ネットワークで、割り当てられたローカル IP アドレスではなく、VPN ピアの実際の IP アドレスを使用する場合があります。VPN では通常、内部ネットワークにアクセスするために、割り当てられたローカル IP アドレスがピアに指定されます。ただし、内部サーバおよびネットワーク セキュリティがピアの実際の IP アドレスに基づく場合などに、ローカル IP アドレスを変換してピアの実際のパブリック アドレスに戻す場合があります。

Cisco ASA 55xx では、内部/保護対象ネットワークの VPN クライアントの割り当てられた IP アドレスをパブリック（送信元）IP アドレスに変換する方法が導入されました。この機能は、内部ネットワークおよびネットワーク セキュリティ ポリシーのターゲット サーバ/サービスが、社内ネットワークの割り当てられた IP ではなく、VPN クライアントのパブリック/送信元 IP との通信を必要とするシナリオをサポートします。

この機能は、トンネル グループごとに 1 つのインターフェイスでイネーブルにすることができます。VPN セッションが確立または切断されると、オブジェクト NAT ルールが動的に追加および削除されます。

制限事項

ルーティングの問題のため、この機能が必要でない場合は、この機能の使用は推奨しません。

- レガシー Cisco VPN Client（IKEv1）と AnyConnect クライアントだけをサポートします。
- NAT ポリシーおよび VPN ポリシーが適用されるように、パブリック IP アドレスへのリターン トラフィックは ASA にルーティングされる必要があります。
- 割り当てられた IPv4 およびパブリック アドレスだけをサポートします。
- NAT/PAT デバイスの背後にある複数のピアはサポートされません。
- ロード バランシングはサポートされません（ルーティングの問題のため）。
- ローミングはサポートされません。

手順の詳細

ステップ 1　グローバル コンフィギュレーション モードで、**tunnel general** を入力します。

ステップ 2　アドレス変換をイネーブルにするには、次の構文を使用します。

```
hostname(config-tunnel-general)# nat-assigned-to-public-ip interface
```

このコマンドは、送信元のパブリック IP アドレスに、割り当てられた IP アドレスの NAT ポリシーをダイナミックにインストールします。*interface* は、NAT の適用先を決定します。

ステップ 3　アドレス変換をディセーブルにするには、次の構文を使用します。

```
hostname(config-tunnel-general)# no nat-assigned-to-public-ip
```

VPN NAT ポリシーの表示

アドレス変換は、基礎となるオブジェクト NAT メカニズムを使用します。そのため、VPN NAT ポリシーは、手動設定されたオブジェクト NAT ポリシーと同様に表示されます。次の例では、割り当てられた IP として 95.1.226.4 を使用して、ピアのパブリック IP として 75.1.224.21 を使用します。

```
hostname# show nat
Auto NAT Policies (Section 2)
1 (outside) to (inside) source static _vpn_nat_95.1.226.4 75.1.224.21
    translate_hits = 315, untranslate_hits = 315

prompt# show nat detail

Auto NAT Policies (Section 2)
1 (outside) to (inside) source static _vpn_nat_95.1.226.4 75.1.224.21
    translate_hits = 315, untranslate_hits = 315
    Source - Origin: 95.1.226.4/32, Translated: 75.1.224.21/32
```

outside は AnyConnect クライアントが接続するインターフェイスであり、*inside* は新しいトンネルグループに固有のインターフェイスです。

（注） VPN NAT ポリシーがダイナミックであり、設定に追加されないため、VPN NAT オブジェクトおよび NAT ポリシーは、show run object レポートおよび show run nat レポートから非表示になります。

ロード バランシングの概要

同じネットワークに接続されている 2 つ以上の ASA または VPN コンセントレータを使用しているリモート アクセス コンフィギュレーションがある場合、それぞれのセッションの負荷を共有するようにこれらのデバイスを設定できます。この機能は、*ロード バランシング*と呼ばれます。ロード バランシングを実装するには、同じプライベート LAN-to-LAN ネットワーク、プライベート サブネット、およびパブリック サブネット上の 2 つ以上のデバイスを論理的に*仮想クラスタ*にグループ化します。

セッションの負荷は、仮想クラスタ内のすべてのデバイスに分散されます。ロード バランシングにより、セッションのトラフィックはクラスタ内の最も負荷の少ないデバイスに転送され、負荷はすべてのデバイス間に分散されます。これにより、システム リソースが効率的に使用され、パフォーマンスが向上し、ハイ アベイラビリティが実現されます。

仮想クラスタ内の 1 つのデバイスである*仮想クラスタ マスター*は、着信トラフィックを*バックアップ デバイス*と呼ばれる他のデバイスに転送します。仮想クラスタ マスターは、クラスタ内のすべてのデバイスをモニタし、各デバイスの負荷を追跡して、その負荷に基づいてセッションの負荷を分散します。仮想クラスタ マスターの役割は、1 つの物理デバイスに結び付けられるものではなく、デバイス間でシフトできます。たとえば、現在の仮想クラスタ マスターで障害が発生すると、クラスタ内のバックアップ デバイスの 1 つがその役割を引き継いで、すぐに新しい仮想クラスタ マスターになります。

仮想クラスタは、外部のクライアントには 1 つの*仮想クラスタ IP アドレス*として表示されます。この IP アドレスは、特定の物理デバイスに結び付けられていません。現在の仮想クラスタ マスターに属しているため、仮想のアドレスです。接続の確立を試みている VPN クライアントは、最初にこの仮想クラスタ IP アドレスに接続します。仮想クラスタ マスターは、クラスタ内で使用できるホストのうち、最も負荷の低いホストのパブリック IP アドレスをクライアントに返します。2 回めのトランザクション（ユーザに対しては透過的）になると、クライアントはホストに直接接続します。仮想クラスタ マスターは、このようにしてリソース全体に均等かつ効率的にトラフィックを転送します。

（注） Cisco VPN Client または Cisco 3002 ハードウェア クライアント以外のすべてのクライアントは、通常どおり ASA に直接接続する必要があります。これらのクライアントは、仮想クラスタ IP アドレスを使用しません。

クラスタ内のマシンで障害が発生すると、終了されたセッションはただちに仮想クラスタ IP アドレスに再接続できます。次に、仮想クラスタ マスターは、クラスタ内の別のアクティブ デバイスにこれらの接続を転送します。仮想クラスタ マスター自体に障害が発生した場合、クラスタ内のバックアップ デバイスが、ただちに新しい仮想セッション マスターを自動的に引き継ぎます。クラスタ内の複数のデバイスで障害が発生しても、クラスタ内のデバイスが 1 つ稼働していて使用可能である限り、ユーザはクラスタに引き続き接続できます。

ロード バランシングとフェールオーバーの比較

ロード バランシングとフェールオーバーはどちらもハイ アベイラビリティ機能ですが、これらは機能も要件も異なります。場合によっては、ロード バランシングとフェールオーバーの両方を使用できます。次の項では、これらの機能の違いについて説明します。

ロード バランシング

ロード バランシングとは、リモート アクセス VPN トラフィックを、仮想クラスタ内のデバイス間で均等に分配するメカニズムのことです。この機能は、スループットまたはその他の要因を考慮しない単純なトラフィックの分散に基づいています。ロードバランシング クラスタは 2 つ以上のデバイスで構成され、そのうちの 1 つが仮想マスターとなり、それ以外のデバイスはバックアップとなります。これらのデバイスは、完全に同じタイプである必要はなく、同じソフトウェア バージョンやコンフィギュレーションを使用する必要もありません。

仮想クラスタ内のすべてのアクティブなデバイスがセッションの負荷を分散します。ロード バランシングにより、トラフィックはクラスタ内の最も負荷の少ないデバイスに転送され、負荷はすべてのデバイス間に分散されます。これにより、システム リソースが効率的に使用され、パフォーマンスが向上し、ハイ アベイラビリティが実現されます。

フェールオーバー

フェールオーバー設定には、同じ ASA が 2 台、専用のフェールオーバー リンク（オプションで、ステートフル フェールオーバー リンク）で相互に接続されている必要があります。アクティブ インターフェイスおよび装置のヘルスがモニタされて、所定のフェールオーバー条件に一致しているかどうかが判断されます。これらの条件に一致した場合は、フェールオーバーが行われます。フェールオーバーは、VPN とファイアウォールの両方のコンフィギュレーションをサポートします。

ASA は、アクティブ/アクティブ フェールオーバーとアクティブ/スタンバイ フェールオーバーの 2 つのフェールオーバーをサポートします。

アクティブ/アクティブ フェールオーバーでは、両方の装置がネットワーク トラフィックを通過させることができます。これは、同じ結果になる可能性がありますが、真のロード バランシングではありません。フェールオーバーが行われると、残りのアクティブ装置が、設定されたパラメータに基づいて結合されたトラフィックの通過を引き継ぎます。したがって、アクティブ/アクティブ フェールオーバーを構成する場合は、両方の装置の合計トラフィックが各装置の容量以内になるようにする必要があります。

アクティブ/スタンバイ フェールオーバーでは、1 つの装置だけがトラフィックを通過させることができ、もう 1 つの装置はスタンバイ状態で待機して、トラフィックを通過させません。アクティブ/スタンバイ フェールオーバーでは、2 番目の ASA を使用して、障害の発生した装置の機能を引き継ぎます。アクティブ装置が故障すると、スタンバイ状態に変わり、そしてスタンバイ装置がアクティブ状態に変わります。アクティブになる装置が、障害の発生した装置の IP アドレス（または、トランスペアレント ファイアウォールの場合は管理 IP アドレス）および MAC アドレスを引き継いで、トラフィックの転送を開始します。現在スタンバイになっている装置が、アクティブ装置のスタンバイの IP アドレスを引き継ぎます。アクティブ装置で障害が発生すると、スタンバイ装置は、クライアント VPN トンネルを中断することなく引き継ぎます。

ロード バランシングの実装

説明　ロード バランシングをイネーブルにするには、次の手順を実行します。

- 共通仮想クラスタ IP アドレス、UDP ポート（必要に応じて）、およびクラスタの IPsec 共有秘密情報を確立することによりロードバランシング クラスタを設定する。クラスタ内のすべてのデバイスに対してこれらの値を同一に設定します。
- デバイスでロード バランシングをイネーブルにし、デバイス固有のプロパティを定義することにより、参加デバイスを設定する。これらの値はデバイスによって異なります。

（注）　VPN ロード バランシングには、アクティブな 3DES または AES ライセンスが必要です。ASA は、ロード バランシングをイネーブルにする前に、この暗号化ライセンスの存在をチェックします。アクティブな 3DES または AES ライセンスを検出できない場合、ASA は、ロード バランシングのイネーブル化を回避し、さらにライセンスがこの使用を許可していない限り、ロード バランシング システムによる 3DES の内部コンフィギュレーションも回避します。

前提条件

ロード バランシングはデフォルトではディセーブルになっています。ロード バランシングは明示的にイネーブルにする必要があります。

まず、パブリック（outside）インターフェイスおよびプライベート（inside）インターフェイスを設定し、さらに仮想クラスタ IP アドレスが参照するインターフェイスを事前に設定しておく必要があります。これらのインターフェイスに異なる名前を設定するには、**interface** コマンドと **nameif** コマンドを使用します。この項では、これ以降の参照に outside および inside という名前を使用します。

クラスタに参加するすべてのデバイスは、同じクラスタ固有の値（IP アドレス、暗号化設定、暗号キー、およびポート）を共有する必要があります。

適格なプラットフォーム

ロードバランシング クラスタには、ASA モデルの ASA 5512-X（Security Plus ライセンスあり）および Model 5515-X 以降を含めることができます。クラスタには Cisco VPN 3000 シリーズのコンセントレータも含めることができます。混合コンフィギュレーションは可能ですが、通常は、同種クラスタにする方が容易に管理できます。

適格なクライアント

ロード バランシングは、次のクライアントで開始されるリモート セッションでのみ有効です。

- Cisco AnyConnect VPN Client（Release 2.0 以降）
- Cisco VPN Client（Release 3.0 以降）
- Cisco ASA 5505 ASA（Easy VPN クライアントとして動作している場合）
- Cisco VPN 3002 Hardware Client（Release 3.5 以降）
- Easy VPN クライアントとして動作している場合、Cisco PIX 501/506E
- IKE リダイレクトをサポートする Cisco IOS EZVPN クライアント デバイス（IOS 831/871）
- クライアントレス SSL VPN（クライアントではない）

ロード バランシングは、IPsec クライアント セッションと SSL VPN クライアントおよびクライアントレス セッションで機能します。LAN-to-LAN を含む他のすべての VPN 接続タイプ（L2TP、PPTP、L2TP/IPsec）は、ロード バランシングがイネーブルになっている ASA に接続できますが、これらの接続タイプはロード バランシングには参加できません。

VPN ロードバランシングのアルゴリズム

マスター デバイスには、バックアップ クラスタ メンバーを IP アドレスの昇順にソートしたリストが保持されます。各バックアップ クラスタ メンバーの負荷は、整数の割合（アクティブ セッション数）として計算されます。AnyConnect の非アクティブ セッションは、ロード バランシングの SSL VPN 負荷に数えられません。マスター デバイスは、IPsec トンネルと SSL VPN トンネルを負荷が最も低いデバイスに、その他のデバイスより負荷が 1% 高くなるまでリダイレクトします。すべてのバックアップ クラスタ メンバーの負荷がマスターより 1% 高くなると、マスター デバイスは自分自身に対してリダイレクトします。

たとえば、1 つのマスターと 2 つのバックアップ クラスタ メンバーがある場合に、次のサイクルが当てはまります。

（注） すべてのノードは 0% から始まり、すべての割合は四捨五入されます。

1. マスター デバイスは、すべてのメンバーにマスターよりも 1% 高い負荷がある場合に、接続を使用します。
2. マスターが接続を使用しない場合、セッションは、最もロード率が低いバックアップ デバイスが処理します。
3. すべてのメンバーに同じ割合の負荷がかかっている場合、セッション数が最も少ないバックアップ デバイスがセッションを取得します。
4. すべてのメンバーに同じ割合の負荷と同じ数のセッションがある場合、IP アドレス数が最も少ないデバイスがセッションを取得します。

VPN ロードバランシング クラスタ コンフィギュレーション

ロードバランシング クラスタは、次の制限に従って、同じリリース、または混在リリースの ASA と、VPN 3000 コンセントレータ、あるいはこれらの組み合わせで構成できます。

- 同じリリースの ASA、またはすべて VPN 3000 コンセントレータで構成されるロードバランシング クラスタは、IPsec、AnyConnect、およびクライアントレス SSL VPN セッションの組み合わせに対してロード バランシングを実行できます。
- 同じリリースの ASA および VPN 3000 コンセントレータの両方で構成されるロードバランシング クラスタは、IPsec、AnyConnect、およびクライアントレス SSL VPN クライアントとクライアントレス セッションの組み合わせに対してロード バランシングを実行できます。
- 混在リリースの ASA または同じリリースの ASA および VPN 3000 コンセントレータあるいはこれら両方で構成されるロードバランシング クラスタは、IPsec セッションのみをサポートできます。ただし、このようなコンフィギュレーションでは、ASA は、それぞれの IPsec のキャパシティに完全に到達しない可能性があります。「シナリオ 1：SSL VPN 接続のない混在クラスタ」は、この状況を示しています。

Release 7.1(1) 以降、IPsec セッションと SSL VPN セッションは、クラスタ内の各デバイスに分散される負荷を決定するときに均等にカウントまたは重み付けします。これは、ASA Release 7.0(x) ソフトウェアと VPN 3000 コンセントレータのロードバランシング計算からの変更です。両方のプラットフォームで、一部のハードウェア プラットフォームが SSL VPN セッションの負荷を IPSec セッションの負荷とは異なる方法で計算する重み付けアルゴリズムが使用されます。

クラスタの仮想マスターは、クラスタのメンバーにセッション要求を割り当てます。ASA は、すべてのセッション、SSL VPN または IPsec を同等と見なし、それらを同等に割り当てます。許可する IPsec セッションと SSL VPN セッションの数は、コンフィギュレーションおよびライセンスで許可されている最大数まで設定できます。これらの制限の設定方法については、「VPN セッション制限の設定」を参照してください。

ロードバランシング クラスタで最大 10 のノードはテスト済みです。これよりクラスタが多くても機能しますが、そのようなトポロジは正式にはサポートされていません。

一部の一般的な混在クラスタのシナリオ

混在コンフィギュレーション、つまりロードバランシング クラスタにさまざまな ASA ソフトウェア リリースを実行しているデバイスが含まれている、または ASA Release 7.1(1) 以降および VPN 3000 コンセントレータを実行している ASA が少なくとも 1 つ含まれる場合、最初のクラスタ マスターで障害が発生し、別のデバイスがマスターを引き継ぐときに、重み付けアルゴリズムの違いが問題になります。

次のシナリオは、ASA Release 7.1(1)、ASA Release 7.0(x) ソフトウェアを実行している ASA と VPN 3000 シリーズ コンセントレータの混在で構成されているクラスタでの VPN ロード バランシングの使用を示しています。

シナリオ 1：SSL VPN 接続のない混在クラスタ

このシナリオでは、クラスタは ASA と VPN 3000 コンセントレータの混在で構成されています。ASA クラスタ ピアには、ASA Release 7.0(x) を実行しているものも、Release 7.1(1) を実行しているものもあります。7.1(1) 以前のピアおよび VPN 3000 ピアには、SSL VPN 接続はなく、7.1(1) クラスタ ピアには、SSL VPN の基本ライセンスのみあり、2 つの SSL VPN セッションは許可されますが、SSL VPN 接続はありません。この場合、すべての接続は IPsec であり、ロード バランシングは良好に機能します。

2 つの SSL VPN ライセンスは、ユーザの最大 IPsec セッション制限の活用にはほとんど影響を及ぼしません。また、これは VPN 3000 コンセントレータがクラスタ マスターの場合に限られます。一般に、混在クラスタ内の ASA の SSL VPN ライセンスの数が少なければ少ないほど、IPsec セッションしかないシナリオで IPsec セッションの制限に達することができる ASA 7.1(1) デバイスへの影響も小さくなります。

シナリオ 2：SSL VPN 接続を処理する混在クラスタ

たとえば、ASA Release 7.1(1) ソフトウェアを実行している ASA が最初のクラスタ マスターで、そのデバイスに障害が発生したとします。クラスタ内の別のデバイスが自動的にマスターを引き継ぎ、そのクラスタ内のプロセッサの負荷を決定するためにそのデバイス独自のロードバランシング アルゴリズムを適用します。ASA Release 7.1(1) ソフトウェアを実行しているクラスタ マスターは、そのソフトウェアが提供する方法以外では、セッションの負荷を重み付けすることはできません。そのため、IPsec および SSL VPN セッションの負荷の組み合わせを、以前のバージョンを実行する ASA デバイスにも、VPN 3000 コンセントレータにも適切に割り当てることができません。これとは逆に、クラスタ マスターとして動作している VPN 3000 コンセントレータは、ASA Release 7.1(1) ASA に負荷を適切に割り当てることができません。次のシナリオは、このジレンマを示しています。

このシナリオは、クラスタが ASA と VPN 3000 コンセントレータの混在で構成されているという点において、前述のシナリオと似ています。ASA クラスタ ピアには ASA Release 7.0(x) を実行しているものも、Release 7.1(1) を実行しているものもあります。ただし、この場合は、クラスタは IPsec 接続だけでなく SSL VPN 接続も処理されます。

ASA Release 7.1(1) 以前のソフトウェアを実行しているデバイスがクラスタ マスターである場合、マスターは実質的に Release 7.1(1) 以前のプロトコルとロジックを適用します。つまり、セッションはそのセッション制限を超えているロードバランシング ピアに転送される場合もあります。その場合、ユーザはアクセスを拒否されます。

クラスタ マスターが ASA Release 7.0(x) ソフトウェアを実行しているデバイスである場合、古いセッション重み付けアルゴリズムは、クラスタ内の 7.1(1) 以前のピアにのみ適用されます。この場合、アクセスが拒否されることはありません。7.1(1) 以前のピアは、セッション重み付けアルゴリズムを使用するため、負荷がより軽くなっています。

ただし、7.1(1) ピアが常にクラスタ マスターであることは保証できないため、問題が発生します。クラスタ マスターで障害が発生すると、別のピアがマスターの役割を引き継ぎます。新しいマスターは、適格なピアのいずれかになります。結果を予測することは不可能であるため、このタイプのクラスタを構成しないことを推奨します。

ロード バランシングの設定

ロード バランシングを使用するには、クラスタに参加する各デバイスに対して次の要素を設定します。

- パブリック インターフェイスとプライベート インターフェイス
- VPN ロードバランシング クラスタ属性

（注） クラスタに参加するすべてのデバイスには、クラスタ内でのデバイス プライオリティを除き、同一のクラスタ コンフィギュレーションを設定する必要があります。

（注） アクティブ/アクティブステートフル フェールオーバー、または VPN ロードバランシングを使用している場合、ローカル CA 機能はサポートされません。ローカル CA を別の CA の下位に置くことはできません。ローカル CA はルート CA にしかなれません。

ロード バランシング用のパブリック インターフェイスとプライベート インターフェイスの設定

ロードバランシング クラスタ デバイス用のパブリック（外部）インターフェイスとプライベート（内部）インターフェイスを設定するには、次の手順を実行します。

ステップ 1　vpn-load-balancing コンフィギュレーション モードで、**lbpublic** キーワードを指定して **interface** コマンドを入力し、ASA にパブリック インターフェイスを設定します。このコマンドは、このデバイスのロード バランシングのためのパブリック インターフェイスの名前または IP アドレスを指定します。

```
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# interface lbpublic outside
hostname(config-load-balancing)#
```

ステップ 2　vpn-load-balancing コンフィギュレーション モードで、**lbprivate** キーワードを指定して **interface** コマンドを入力し、ASA にプライベート インターフェイスを設定します。このコマンドで、このデバイスのロード バランシングのためのプライベート インターフェイスの名前または IP アドレスを指定します。

```
hostname(config-load-balancing)# interface lbprivate inside
hostname(config-load-balancing)#
```

ステップ 3　このデバイスを割り当てるためのクラスタ内でのプライオリティを設定します。指定できる範囲は 1 ～ 10 です。プライオリティは、起動時または既存のマスターで障害が発生したときに、このデバイスが仮想クラスタ マスターになる可能性を表します。プライオリティを高く設定すると（たとえば 10）、このデバイスが仮想クラスタ マスターになる可能性が高くなります。

```
hostname(config-load-balancing)# priority number
hostname(config-load-balancing)#
```

たとえば、このデバイスにクラスタ内でのプライオリティ 6 を割り当てるには、次のコマンドを入力します。

```
hostname(config-load-balancing)# priority 6
hostname(config-load-balancing)#
```

ステップ 4　このデバイスにネットワーク アドレス変換を適用する場合は、デバイスに割り当てられた NAT アドレスを指定して **nat** コマンドを入力します。IPv4 および IPv6 アドレスを定義するか、デバイスのホスト名を指定できます。

```
hostname(config-load-balancing)# nat ipv4_address ipv_address
hostname(config-load-balancing)#
```

たとえば、このデバイスに NAT アドレス 192.168.30.3 および 2001:DB8::1 を割り当てるには、次のコマンドを入力します。

```
hostname(config-load-balancing)# nat 192.168.30.3 2001:DB8::1
hostname(config-load-balancing)#
```

ロード バランシング クラスタ属性の設定

クラスタ内の各デバイスのロードバランシング クラスタ属性を設定するには、次の手順を実行します。

ステップ 1　グローバル コンフィギュレーション モードで **vpn load-balancing** コマンドを入力して、VPN ロード バランシングをセットアップします。

```
hostname(config)# vpn load-balancing
hostname(config-load-balancing)#
```

これで vpn-load-balancing コンフィギュレーション モードに入るため、ここで残りのロードバランシング属性を設定できます。

ステップ 2　このデバイスが属しているクラスタの IP アドレスまたは完全修飾ドメイン名を設定します。このコマンドは、仮想クラスタ全体を表す単一の IP アドレスまたは FQDN を指定します。仮想クラスタ内のすべての ASA が共有するパブリック サブネットのアドレス範囲内で、IP アドレスを選択します。IPv4 アドレスまたは IPv6 アドレスを指定できます。

```
hostname(config-load-balancing)# cluster ip address ip_address
hostname(config-load-balancing)#
```

たとえば、クラスタ IP アドレスを IPv6 アドレス 2001:DB8::1 に設定するには、次のコマンドを入力します。

```
hostname(config-load-balancing)# cluster ip address 2001:DB8::1
hostname(config-load-balancing)#
```

ステップ 3　クラスタ ポートを設定します。次のコマンドは、このデバイスが参加する仮想クラスタの UDP ポートを指定します。デフォルト値は 9023 です。別のアプリケーションでこのポートが使用されている場合は、ロード バランシングに使用する UDP の宛先ポート番号を入力します。

```
hostname(config-load-balancing)# cluster port port_number
hostname(config-load-balancing)#
```

たとえば、クラスタ ポートを 4444 に設定するには、次のコマンドを入力します。

```
hostname(config-load-balancing)# cluster port 4444
hostname(config-load-balancing)#
```

ステップ 4　（オプション）クラスタに対する IPsec 暗号化をイネーブルにします。デフォルトでは暗号化は使用されません。このコマンドは、IPsec 暗号化をイネーブルまたはディセーブルにします。このチェック属性を設定する場合は、まず共有秘密情報を指定して検証する必要があります。仮想クラスタ内の ASA は、IPsec を使用して LAN-to-LAN トンネル経由で通信します。デバイス間で通信されるすべてのロードバランシング情報が暗号化されるようにするには、この属性をイネーブルにします。

```
hostname(config-load-balancing)# cluster encryption
hostname(config-load-balancing)#
```

（注）　暗号化を使用する場合、事前にロードバランシング内部インターフェイスを設定しておく必要があります。そのインターフェイスがロードバランシング内部インターフェイスでイネーブルになっていない場合、クラスタの暗号化を設定しようとするとエラー メッセージが表示されます。

クラスタの暗号化を設定したときにロードバランシング内部インターフェイスがイネーブルになっており、仮想クラスタ内の参加デバイスを設定する前にディセーブルになった場合、**participate** コマンドを入力する（または、ASDM で、[Participate in Load Balancing Cluster] チェックボックスをオンにする）と、エラー メッセージが表示され、そのクラスタに対する暗号化はイネーブルになりません。

クラスタの暗号化を使用するには、内部インターフェイスを指定して **crypto isakmp enable** コマンドを使用し、内部インターフェイス上の ISAKMP をイネーブルにする必要があります。

ステップ 5　クラスタの暗号化をイネーブルにする場合、**cluster key** コマンドを入力して IPsec 共有秘密情報も指定する必要があります。このコマンドは、IPsec 暗号化をイネーブルにしてある場合、IPsec ピア間に共有秘密を指定します。ボックスに入力する値は、連続するアスタリスク文字として表示されます。

```
hostname(config-load-balancing)# cluster key shared_secret
hostname(config-load-balancing)#
```

たとえば、共有秘密情報を 123456789 に設定するには、次のコマンドを入力します。

```
hostname(config-load-balancing)# cluster key 123456789
hostname(config-load-balancing)#
```

ステップ 6　participate コマンドを入力して、クラスタへのこのデバイスの参加をイネーブルにします。

```
hostname(config-load-balancing)# participate
hostname(config-load-balancing)#
```

完全修飾ドメイン名を使用したリダイレクションのイネーブル化

VPN ロードバランシング モードで完全修飾ドメイン名を使用したリダイレクトをイネーブルまたはディセーブルにするには、グローバル コンフィギュレーション モードで **redirect-fqdn enable** コマンドを使用します。この動作は、デフォルトではディセーブルになっています。

デフォルトで、ASA はロードバランシング リダイレクトの IP アドレスだけをクライアントに送信します。DNS 名に基づく証明書が使用されている場合、その証明書はバックアップ デバイスにリダイレクトされたときに無効になります。

VPN クラスタ マスターとして、ASA は、VPN クライアント接続を別のクラスタ デバイスにリダイレクトする場合に、DNS 逆ルックアップを使用して、そのクラスタ デバイス（クラスタ内の別の ASA）の外部 IP アドレスではなく Fully Qualified Domain Name（FQDN; 完全修飾ドメイン名）を送信できます。

クラスタ内のロードバランシング デバイスのすべての外部および内部ネットワーク インターフェイスは、同じ IP ネットワーク上に存在する必要があります。

IP アドレスではなく、FQDN を使用して SSL 接続または IPsec/IKEv2 接続のロード バランシングを実行するには、次の設定手順を実行します。

ステップ 1　**redirect-fqdn enable** コマンドを使用して、ロード バランシングのための FQDN の使用をイネーブルにします。

redirect-fqdn {enable | disable}
no redirect-fqdn {enable | disable}

次に例を示します。

```
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# redirect-fqdn enable
hostname(config-load-balancing)#
```

ステップ 2　DNS サーバに、各 ASA 外部インターフェイスのエントリを追加します（エントリが存在しない場合）。それぞれの ASA 外部 IP アドレスに、ルックアップ用にそのアドレスに関連付けられた DNS エントリが設定されている必要があります。これらの DNS エントリに対しては、逆ルックアップもイネーブルにする必要があります。

ステップ 3　**dns domain-lookup inside** コマンドを使用して、ASA で DNS ルックアップをイネーブルにします。inside の部分には、DNS サーバへのルートを持つ任意のインターフェイスを指定します。

ステップ 4　ASA 上の DNS サーバ IP アドレスを定義します。たとえば、**dns name-server 10.2.3.4**（DNS サーバの IP アドレス）。

次に、完全修飾ドメイン名のリダイレクトをイネーブルにし、クラスタのパブリック インターフェイスを **test** と指定し、クラスタのプライベート インターフェイスを **foo** と指定するインターフェイス コマンドを含む、VPN ロードバランシング コマンド シーケンスの例を示します。

```
hostname(config)# interface GigabitEthernet 0/1
hostname(config-if)# ip address 209.165.202.159 255.255.255.0
hostname(config)# nameif test
hostname(config)# interface GigabitEthernet 0/2
hostname(config-if)# ip address 209.165.201.30 255.255.255.0
hostname(config)# nameif foo
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# nat 192.168.10.10
hostname(config-load-balancing)# priority 9
hostname(config-load-balancing)# interface lbpublic test
hostname(config-load-balancing)# interface lbprivate foo
hostname(config-load-balancing)# cluster ip address 209.165.202.224
hostname(config-load-balancing)# cluster key 123456789
hostname(config-load-balancing)# cluster encryption
```

```
hostname(config-load-balancing)# cluster port 9023
hostname(config-load-balancing)# redirect-fqdn enable
hostname(config-load-balancing)# participate
```

ロード バランシングについての FAQ

IP アドレス プールの枯渇

Q. ASA は、IP アドレス プールの枯渇をその VPN ロードバランシング方式の一部と見なしますか。

A. いいえ。リモート アクセス VPN セッションが、IP アドレス プールが枯渇したデバイスに転送された場合、セッションは確立されません。ロードバランシング アルゴリズムは、負荷に基づき、各バックアップ クラスタ メンバーが提供する整数の割合（アクティブ セッション数および最大セッション数）として計算されます。

固有の IP アドレス プール

Q. VPN ロード バランシングを実装するには、異なる ASA 上の AnyConnect クライアントまたは IPsec クライアントの IP アドレス プールを固有にする必要がありますか。

A. はい。IP アドレス プールはデバイスごとに固有にする必要があります。

同じデバイスでのロード バランシングとフェールオーバーの使用

Q. 単一のデバイスで、ロード バランシングとフェールオーバーの両方を使用できますか。

A. はい。この設定では、クライアントはクラスタの IP アドレスに接続し、クラスタ内で最も負荷の少ない ASA にリダイレクトされます。そのデバイスで障害が発生すると、スタンバイ装置がすぐに引き継ぎ、VPN トンネルにも影響を及ぼしません。

複数のインターフェイスでのロード バランシング

Q. 複数のインターフェイスで SSL VPN をイネーブルにする場合、両方のインターフェイスにロード バランシングを実装することはできますか。

A. パブリック インターフェイスとしてクラスタに参加するインターフェイスは 1 つしか定義できません。これは、CPU 負荷のバランスをとることを目的としています。複数のインターフェイスは、同じ CPU に集中するため、複数のインターフェイスにおけるロード バランシングの概念には意味がありません。

ロード バランシング クラスタの最大同時セッション

Q. それぞれが 100 ユーザの SSL VPN ライセンスを持つ 2 つの ASA 5525-X が構成されているとします。この場合、ロードバランシング クラスタで許可されるユーザの最大合計数は、200 同時セッションでしょうか。または 100 同時セッションだけでしょうか。さらに 100 ユーザ ライセンスを持つ 3 台目のデバイスを追加した場合、300 の同時セッションをサポートできますか。

A. VPN ロード バランシングを使用すると、すべてのデバイスがアクティブになるため、クラスタでサポートできる最大セッション数は、クラスタ内の各デバイスのセッション数の合計になります。この例の場合は、300 になります。

ロード バランシングの表示

ロードバランシング クラスタのマスターは、アクティブな AnyConnect セッション、クライアントレス セッション、そして設定された制限またはライセンス数制限に基づく最大許可セッションがあるクラスタ内の各 ASA からメッセージを定期的に受信します。クラスタ内のある ASA の容量が 100% いっぱいであると示される場合、クラスタ マスターはこれに対してさらに接続をリダイレクトすることはできません。ASA がいっぱいであると示されても、ユーザによっては非アクティブまたは再開待ち状態となり、ライセンスを消費する可能性があります。回避策として、セッション合計数ではなく、セッション合計数から非アクティブ状態のセッション数を引いた数が各 ASA によって提供されます（コマンド リファレンスの **-sessiondb summary** コマンドを参照してください）。つまり、非アクティブなセッションはクラスタ マスターに報告されません。ASA が（非アクティブなセッションによって）いっぱいになっている場合でも、クラスタ マスターは必要に応じて接続を ASA に引き続きリダイレクトします。ASA が新しい接続を受信すると、最も長く非アクティブになっていたセッションがログオフされ、新しい接続がそのライセンスを引き継ぎます。

次の例は、100 個の SSL セッション（アクティブのみ）と 2% の SSL 負荷を示しています。これらの数字には、非アクティブなセッションは含まれていません。つまり、非アクティブなセッションはロード バランシングの負荷に数えられません。

```
hostname# load-balancing
    Status :        enabled
    Role :          Master
    Failover :      Active
    Encryption :    enabled
    Cluster IP :    192.168.1.100
    Peers :         1

                                                Load %
Sessions
    Public IP       Role    Pri     Model           IPsec   SSL     IPsec SSL
    192.168.1.9     Master  7       ASA-5540        4       2       216     100
    192.168.1.19    Backup  9       ASA-5520        0       0       0       0
```

VPN セッション制限の設定

IPsec セッションと SSL VPN セッションは、プラットフォームと ASA ライセンスがサポートする限り、いくつでも実行できます。ASA の最大セッション数を含むライセンス情報を表示するには、グローバル コンフィギュレーション モードで **show version** コマンドを入力します。次の例は、このコマンドの出力からのコマンドとライセンス情報を示しています。

```
hostname(config)# show version

Cisco Adaptive Security Appliance Software Version 8.4(1)
Device Manager Version 6.4(1)

Compiled on Sun 02-Jan-11 03:45 by builders
System image file is "disk0:/cdisk.bin"
Config file at boot was "startup-config"
asa4 up 9 days 3 hours

Hardware:   ASA5510, 256 MB RAM, CPU Pentium 4 Celeron 1600 MHz
Internal ATA Compact Flash, 256MB
BIOS Flash M50FW080 @ 0xfff00000, 1024KB

Encryption hardware device : Cisco ASA-55x0 on-board accelerator (revision 0x0)
                             Boot microcode        : CN1000-MC-BOOT-2.00
                             SSL/IKE microcode     : CNLite-MC-SSLm-PLUS-2.03
                             IPsec microcode       : CNlite-MC-IPSECm-MAIN-2.06
                             Number of accelerators: 1

 0: Ext: Ethernet0/0         : address is 001e.f75e.8b84, irq 9
 1: Ext: Ethernet0/1         : address is 001e.f75e.8b85, irq 9
 2: Ext: Ethernet0/2         : address is 001e.f75e.8b86, irq 9
 3: Ext: Ethernet0/3         : address is 001e.f75e.8b87, irq 9
 4: Ext: Management0/0       : address is 001e.f75e.8b83, irq 11
 5: Int: Internal-Data0/0    : address is 0000.0001.0002, irq 11
 6: Int: Internal-Control0/0 : address is 0000.0001.0001, irq 5

Licensed features for this platform:
Maximum Physical Interfaces       : Unlimited      perpetual
Maximum VLANs                     : 100            perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Active  perpetual
VPN-DES                           : Enabled        perpetual
VPN-3DES-AES                      : Enabled        perpetual
Security Contexts                 : 2              perpetual
GTP/GPRS                          : Disabled       perpetual
AnyConnect Premium Peers          : 250            perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 250            perpetual
Total VPN Peers                   : 250            perpetual
Shared License                    : Disabled       perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Enabled        perpetual
UC Phone Proxy Sessions           : 2              perpetual
Total UC Proxy Sessions           : 2              perpetual
Botnet Traffic Filter             : Disabled       perpetual
Intercompany Media Engine         : Disabled       perpetual

This platform has an ASA 5510 Security Plus license.

hostname#
```

AnyConnect VPN セッション（IPsec/IKEv2 または SSL）を ASA で許可されているよりも小さい値に制限するには、グローバル コンフィギュレーション モードで **vpn-sessiondb max-anyconnect-premium-or-essentials-limit** コマンドを使用します。セッションの制限を削除するには、このコマンドの **no** バージョンを使用します。

たとえば、ASA のライセンスで 500 の AnyConnect VPN セッションが許可されていて、SSL VPN セッション数を 250 に制限する場合は、次のコマンドを入力します。

```
hostname(config)# vpn-sessiondb max-anyconnect-premium-or-essentials-limit 250
hostname(config)#
```

セッションの制限を削除するには、このコマンドの **no** バージョンを使用します。

```
hostname(config)# no vpn-sessiondb max-anyconnect-premium-or-essentials-limit 250
hostname(config)#
```

Cisco VPN Client（IPsec IKEv1）、LAN-to-LAN VPN、およびクライアントレス SSL VPN のセッション数を ASA が許可している数よりも小さい値に制限するには、グローバル コンフィギュレーション モードで **vpn-sessiondb max-other-vpn-limit** コマンドを入力します。

たとえば、ASA のライセンスが 750 の IPsec セッションを許可していて、IPsec セッション数を 500 に制限する場合は、次のコマンドを入力します。

```
hostname(config)# vpn-sessiondb max-other-vpn-limit 500
hostname(config)#
```

セッションの制限を削除するには、このコマンドの **no** バージョンを使用します。

```
hostname(config)# no vpn-sessiondb max-other-vpn-limit 500
hostname(config)#
```

ID 証明書のネゴシエート時の使用

IKEv2 トンネルを AnyConnect クライアントとネゴシエートする場合、ASA は ID 証明書を使用する必要があります。ikev2 リモート アクセス トラストポイント コンフィギュレーションの場合、次のコマンドを使用します。

```
crypto ikev2 remote-access trustpoint <name> [line<number>]
```

このコマンドを使用すると、AnyConnect クライアントは、エンド ユーザのグループ選択をサポートできます。2 つのトラストポイントを同時に設定できます。RSA を 2 つ、ECDSA を 2 つ、またはそれぞれ 1 つずつ設定できます。ASA は、設定したトラストポイント リストをスキャンし、クライアントがサポートする最初の 1 つを選択します。ECDSA を使用する場合は、RSA トラストポイントの前に、このトラストポイントを設定する必要があります。

行番号オプションは、トラストポイントを挿入する行番号の場所を指定します。通常、このオプションは、別の行を削除および再追加しないで一番上にトラストポイントを挿入するために使用されます。行が指定されていない場合、ASA はリストの末尾にトラストポイントを追加します。

すでに存在するトラストポイントを追加しようとすると、エラーが表示されます。削除するトラストポイント名を指定しないで *no crypto ikev2 remote-access trustpoint* コマンドを使用すると、すべてのトラストポイント コンフィギュレーションが削除されます。

暗号化コアのプールの設定

AnyConnect TLS/DTLS トラフィックに対してより適切なスループット パフォーマンスが得られるように、対称型マルチプロセッシング（SMP）プラットフォーム上での暗号化コアの割り当てを変更することができます。この変更によって、SSL VPN データパスが高速化され、AnyConnect、スマート トンネル、およびポート転送において、ユーザが認識できるパフォーマンス向上が実現します。次の手順では、シングル コンテキスト モードまたはマルチ コンテキスト モードで暗号化コアのプールを設定します。

（注） マルチ コンテキスト モードが適用されるのは、IKEv2 および IKEv1 のサイトツーサイトのみであり、AnyConnect、クライアントレス SSL VPN、レガシー Cisco VPN クライアント、Apple ネイティブ VPN クライアント、Microsoft ネイティブ VPN クライアント、および IKEv1 IPsec の cTCP には適用されません。

制限事項

- 暗号化コア再分散ができるのは、次のプラットフォームです。
  - 5585-X
  - 5545-X
  - 5555-X
  - ASASM

手順の詳細

	コマンド	目的
ステップ 1	`hostname(config)# crypto engine ?` `hostname(config)# crypto engine accelerator-bias ?`	暗号アクセラレータ プロセッサの割り当てを指定します。 • **balanced**：暗号化ハードウェア リソースを均等に分散します。 • **ipsec**：IPsec/暗号化音声（SRTP）を優先するように暗号化ハードウェア リソースを割り当てます。 • **ssl**：SSL を優先するように暗号化ハードウェア リソースを割り当てます。

アクティブな VPN セッションの表示

IP アドレス タイプ別のアクティブな AnyConnect セッションの表示

コマンドライン インターフェイスを使用して、アクティブな AnyConnect セッションを表示するには、特権 EXEC モードで **show vpn-sessiondb anyconnect filter p-ipversion** または **show vpn-sessiondb anyconnect filter a-ipversion** コマンドを入力します。

コマンド	目的
show vpn-sessiondb anyconnect filter p-ipversion {v4 | v6}	このコマンドは、エンドポイントのパブリック IPv4 アドレスまたはパブリック IPv6 アドレスでフィルタリングされたアクティブな AnyConnect セッションを表示します。 パブリック アドレスは、企業によってエンドポイントに割り当てられたアドレスです。
show vpn-sessiondb anyconnect filter a-ipversion {v4 | v6}	このコマンドは、エンドポイントの割り当て済み IPv4 または IPv6 アドレスでフィルタリングされたアクティブな AnyConnect セッションを表示します。 割り当て済みアドレスは、ASA によって AnyConnect Secure Mobility Client に割り当てられたアドレスです。

例

例 3-1　show vpn-sessiondb anyconnect filter p-ipversion [v4 | v6] コマンドの出力

```
hostname(config)# show vpn-sessiondb anyconnect filter p-ipversion v4

Session Type: AnyConnect

Username     : user1                  Index        : 40
Assigned IP  : 192.168.17.10          Public IP    : 198.51.100.1
Protocol     : AnyConnect-Parent SSL-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)RC4
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA1
Bytes Tx     : 10570                  Bytes Rx     : 8085
Group Policy : GroupPolicy_SSLACCLIENT
Tunnel Group : SSLACCLIENT
Login Time   : 15:17:12 UTC Mon Oct 22 2012
Duration     : 0h:00m:09s
Inactivity   : 0h:00m:00s
NAC Result   : Unknown
VLAN Mapping : N/A                    VLAN         : none
```

例 3-2　show vpn-sessiondb anyconnect filter a-ipversion [v4 | v6] コマンドの出力

```
hostname(config)# show vpn-sessiondb anyconnect filter a-ipversion v6

Session Type: AnyConnect

Username     : user1                  Index        : 45
Assigned IP  : 192.168.17.10
Public IP    : 2001:DB8:8:1:90eb:3fe5:9eea:fb29
Assigned IPv6: 2001:DB8:9:1::24
Protocol     : AnyConnect-Parent SSL-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)RC4
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA1
Bytes Tx     : 10662                  Bytes Rx     : 17248
Group Policy : GroupPolicy_SSL_IPv6   Tunnel Group : SSL_IPv6
Login Time   : 17:42:42 UTC Mon Oct 22 2012
Duration     : 0h:00m:33s
Inactivity   : 0h:00m:00s
NAC Result   : Unknown
VLAN Mapping : N/A                    VLAN         : none
```

IP アドレス タイプ別のアクティブなクライアントレス SSL VPN セッションの表示

コマンドライン インターフェイスを使用して、アクティブなクライアントレス SSL VPN セッションを表示するには、特権 EXEC モードで **show vpn-sessiondb webvpn filter ipversion** コマンドを入力します。

コマンド	目的
show vpn-sessiondb webvpn filter ipversion {v4 | v6}	このコマンドは、エンドポイントのパブリック IPv4 アドレスまたはパブリック IPv6 アドレスでフィルタリングされたアクティブなクライアントレス SSL VPN セッションを表示します。 パブリック アドレスは、企業によってエンドポイントに割り当てられたアドレスです。

例

例 3-3　show vpn-sessiondb webvpn filter ipversion [v4 | v6] コマンドの出力

```
hostname# sh vpn-sessiondb webvpn filter ipversion v4

Session Type: WebVPN

Username     : user1                  Index        : 63
Public IP    : 171.16.17.6
Protocol     : Clientless
License      : AnyConnect Premium
Encryption   : Clientless: (1)RC4     Hashing      : Clientless: (1)SHA1
Bytes Tx     : 62454                  Bytes Rx     : 13082
Group Policy : SSLv6                  Tunnel Group : SSL_IPv6
Login Time   : 18:07:48 UTC Mon Oct 22 2012
Duration     : 0h:00m:16s
```

```
Inactivity   : 0h:00m:00s
NAC Result   : Unknown
VLAN Mapping : N/A                    VLAN         : none
```

IP アドレス タイプ別のアクティブな LAN-to-LAN VPN セッションの表示

コマンドライン インターフェイスを使用して、アクティブなクライアントレス SSL VPN セッションを表示するには、特権 EXEC モードで **show vpn-sessiondb l2l filter ipversion** コマンドを入力します。

コマンド	目的
show vpn-sessiondb l2l filter ipversion {v4 | v6}	このコマンドは、接続のパブリック IPv4 アドレスまたはパブリック IPv6 アドレスでフィルタリングされたアクティブな LAN-to-LAN VPN セッションを表示します。 パブリック アドレスは、企業によってエンドポイントに割り当てられたアドレスです。

ISE ポリシー実施の設定

Cisco Identity Services Engine（ISE）は、セキュリティ ポリシー管理および制御プラットフォームです。有線、ワイヤレス、VPN 接続のアクセス制御とセキュリティ コンプライアンスを自動化し、シンプルにします。Cisco ISE は主に、Cisco TrustSec と連携してセキュアなアクセスおよびゲスト アクセスを提供し、BYOD に対する取り組みをサポートし、使用ポリシーを適用するために使用されます。

ISE Change of Authorization（CoA）機能は、認証、認可、およびアカウンティング（AAA）セッションの属性を、セッション確立後に変更するためのメカニズムを提供します。AAA のユーザまたはユーザ グループのポリシーを変更すると、ISE から ASA へ CoA パケットを直接送信して認証を再初期化し、新しいポリシーを適用できます。インライン ポスチャ実施ポイント（IPEP）で、ASA と確立された各 VPN セッションのアクセス コントロール リスト（ACL）を適用する必要がなくなりました。

ISE ポリシーの実施は、次の VPN クライアントでサポートされています。

- IPSec
- AnyConnect
- L2TP/IPSec

システム フローは次のとおりです。

1. エンド ユーザが VPN 接続を要求します。
2. ASA は、ISE に対してユーザを認証し、ネットワークへの限定アクセスを提供するユーザ ACL を受け取ります。
3. アカウンティング開始メッセージが ISE に送信され、セッションが登録されます。
4. ポスチャ アセスメントが NAC エージェントと ISE 間で直接行われます。このプロセスは、ASA に透過的です。

5. ISE が CoA の「ポリシー プッシュ」を介して ASA にポリシーのアップデートを送信します。これにより、ネットワーク アクセス権限を引き上げる新しいユーザ ACL が識別されます。

（注）　後続の CoA アップデートを介し、接続のライフタイム中に追加のポリシー評価が ASA に透過的に行われる場合があります。

RADIUS サーバ グループの設定

認証、許可、またはアカウンティングに外部 RADIUS サーバを使用する場合は、まず AAA プロトコルあたり少なくとも 1 つの RADIUS サーバ グループを作成して、各グループに 1 つ以上のサーバを追加する必要があります。AAA サーバ グループは名前で識別されます。

RADIUS サーバ グループを追加するには、次の手順を実行します。

手順の詳細

	コマンド	目的
ステップ 1	**aaa-server** *server_tag* **protocol radius** **例：** `hostname(config)# aaa-server servergroup1 protocol radius` `hostname(config-aaa-server-group)#`	サーバ グループ名とプロトコルを識別します。 **aaa-server protocol** コマンドを入力する場合は、コンフィギュレーション モードを開始します。
ステップ 2	**merge-dacl {before-avpair | after-avpair}** **例：** `hostname(config)# aaa-server servergroup1 protocol radius` `hostname(config-aaa-server-group)# merge-dacl before-avpair`	ダウンロード可能 ACL と、RADIUS パケットから Cisco AV ペアで受信した ACL を結合します。デフォルト設定は **no merge dacl** で、ダウンロード可能な ACL は Cisco AV ペア ACL と結合されません。AV ペアおよびダウンロード可能な ACL の両方を受信した場合は、AV ペアが優先し、使用されます。 **before-avpair** オプションは、ダウンロード可能な ACL エントリが Cisco-AV-Pair エントリの前に配置されるように指定します。 **after-avpair** オプションは、ダウンロード可能な ACL エントリが Cisco-AV-Pair エントリの後に配置されるように指定します。このオプションは、VPN 接続にのみ適用されます。VPN ユーザの場合は、ACL は Cisco AV ペア ACL、ダウンロード可能 ACL、および ASA で設定される ACL の形式になります。このオプションでは、ダウンロード可能 ACL と AV ペア ACL が結合されているどうかを判断します。ASA で設定される ACL には適用されません。

	コマンド	目的
ステップ 3	**max-failed-attempts** *number* **例：** hostname(config-aaa-server-group)# max-failed-attempts 2	次のサーバを試す前にグループ内の RADIUS サーバに送信する要求の最大数を指定します。*number* 引数の範囲は 1 ～ 5 です。デフォルト値は 3 です。 ローカル データベースを使用してフォールバック方式（管理アクセス専用）を設定している場合で、グループ内のすべてのサーバが応答しないとき、グループは応答なしと見なされ、フォールバック方式が試行されます。サーバ グループで、追加の AAA 要求によるアクセスがない、非応答と見なされる時間が 10 分間（デフォルト）続くと、ただちにフォールバック方式が使用されます。非応答時間をデフォルトから変更するには、次のステップの **reactivation-mode** コマンドを参照してください。 フォールバック方式が設定されていない場合、ASA は引き続きグループ内のサーバにアクセスしようとします。
ステップ 4	**reactivation-mode** {**depletion** [**deadtime** *minutes*] | **timed**} **例：** hostname(config-aaa-server-group)# reactivation-mode deadtime 20	グループ内で障害の発生したサーバを再度アクティブ化する方法（再アクティブ化ポリシー）を指定します。 **depletion** キーワードを指定すると、グループ内のすべてのサーバが非アクティブになった後に、障害の発生したサーバが再度アクティブ化されます。 **deadtime** *minutes* キーワード引数のペアには、グループ内の最後のサーバをディセーブルにしてから、次にすべてのサーバを再度イネーブルにするまでの経過時間を分単位で 0 ～ 1440 から指定します。デフォルトは 10 分です。 **timed** キーワードは、30 秒間のダウンタイムの後に障害が発生したサーバを再度アクティブ化します。
ステップ 5	**accounting-mode simultaneous** **例：** hostname(config-aaa-server-group)# accounting-mode simultaneous	グループ内のすべてのサーバにアカウンティング メッセージを送信します。 アクティブ サーバだけ送信メッセージをデフォルトに戻すには、**accounting-mode single** コマンドを入力します。
ステップ 6	**aaa-server** *server_group* [*interface_name*] **host** *server_ip* **例：** hostname(config)# aaa-server servergroup1 outside host 10.10.1.1	サーバと、そのサーバが属する AAA サーバ グループを識別します。 **aaa-server host** コマンドを入力すると、AAA サーバのホスト コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 7	**dynamic-authorization** {port *port-number*} **例：** hostname(config-aaa-server-group)# dynamic-authorization port 1700	AAA サーバ グループの RADIUS の動的認可（CoA）サービスをイネーブルにします。 定義されると、対応する RADIUS サーバ グループが CoA 通知用に登録され、ASA は ISE からの CoA ポリシー アップデート用ポートをリッスンします。 CoA のリスニング *ポート番号*の有効な範囲は、1 ～ 65535 です。 このコマンドの「no」形式で指定されたポート番号またはインターフェイスが現在のコンフィギュレーションの行に一致しない場合は、エラー メッセージが表示されます。
ステップ 8	**authorize-only** **例：** hostname(config-aaa-server-group)# authorize-only	RADIUS サーバ グループ用の認可専用モードをイネーブルにします。これで、このサーバ グループが認可に使用されている場合に RADIUS アクセス要求メッセージが現在利用可能になっている設定済みのパスワード方式ではなく、「認可専用」要求として構築されることが示されます。認可専用要求には値 Authorize-Only（17）を持つサービス タイプ属性と、アクセス要求内のメッセージ認証子が含まれます。 認可専用モードのサポートにより、アクセス要求に RADIUS 共通パスワードを含める必要がなくなります。したがって、AAA サーバ ホスト モードで radius Common pw CLI を使用して共通パスワードを設定する必要はありません。 **（注）** 認可専用モードはサーバ グループに対して設定されますが、共通パスワードはホストに固有です。したがって、認可専用モードを設定すると、個々の AAA サーバに設定された共通パスワードは無視されるようになります。
ステップ 9	**without-csd** {**anyconnect**} **例：** hostname(config-tunnel-webvpn)# without-csd anyconnect	特定のトンネル グループに行われる接続のホスト スキャン処理をオフに切り替えます。この設定は現在、クライアントレスおよび L3 接続に適用されます。このコマンドは、この設定を AnyConnect 接続にのみ適用するように変更されています。

	コマンド	目的
ステップ 10	**interim-accounting-update** {periodic *interval*} **例：** hostname(config-aaa-server-group)# interim-accounting-update periodic 12	RADIUS 中間アカウンティング アップデート メッセージの生成をイネーブルにします。現在、これらのメッセージは、VPN トンネル接続がクライアントレス VPN セッションに追加された場合にだけ生成されます。これが発生した場合、新たに割り当てられた IP アドレスを RADIUS に通知するためのアカウンティング アップデートが生成されます。現在の機能を許可する、またはアカウンティング メッセージを指示されたサーバ グループに送信するように設定されたすべてのセッションに対して定期的な中間アカウンティング アップデートの生成を許可する設定ができるように、このコマンドにキーワードが追加されています。 *periodic*：このオプションのキーワードは、対象のサーバ グループにアカウンティング レコードを送信するように設定されたすべての VPN セッションのアカウンティング レコードの定期的な生成と伝送をイネーブルにします。 *interval*：定期的なアカウンティング アップデート間の間隔の長さを時間単位で表す数値です。有効な範囲は 1 ～ 120 で、デフォルト値は 24 です。

構成例

次に、単一サーバで 1 つの RADIUS グループを追加する例を示します。

```
hostname(config)# aaa-server AuthOutbound protocol radius
hostname(config-aaa-server-group)# exit
hostname(config)# aaa-server AuthOutbound (inside) host 10.1.1.3
hostname(config-aaa-server-host)# key RadUauthKey
hostname(config-aaa-server-host)# exit
```

次に、認可専用の動的認可（CoA）のアップデートと時間ごとの定期的なアカウンティングの ISE サーバ オブジェクトを設定する例を示します。

```
hostname(config)# aaa-server ise protocol radius
hostname(config-aaa-server-group)# authorize-only
hostname(config-aaa-server-group)# interim-accounting-update periodic 1
hostname(config-aaa-server-group)# dynamic-authorization
hostname(config-aaa-server-group)# exit
hostname(config-aaa-server-group)# authorize-only
hostname(config)# aaa-server ise (inside) host 10.1.1.3
hostname(config-aaa-server-host)# key sharedsecret
hostname(config-aaa-server-host)# exit
```

次に、ISE によるパスワード認証用のトンネル グループを設定する例を示します。

```
hostname(config)# tunnel-group aaa-coa general-attributes
hostname(config-tunnel-general)# address-pool vpn
hostname(config-tunnel-general)# authentication-server-group ise
hostname(config-tunnel-general)# accounting-server-group ise
hostname(config-tunnel-general)# exit
```

次に、ISE によるローカル証明書の検証と認可用のトンネル グループを設定する例を示します。

```
hostname(config)# tunnel-group aaa-coa general-attributes
hostname(config-tunnel-general)# address-pool vpn
hostname(config-tunnel-general)# authentication certificate
hostname(config-tunnel-general)# authorization-server-group ise
hostname(config-tunnel-general)# accounting-server-group ise
hostname(config-tunnel-general)# exit
```

CoA をイネーブルにする方法の詳細については、『*Cisco ASA Series General Operations CLI Configuration Guide*』の「*Configuring RADIUS Servers for AAA*」を参照してください。

コマンドの概要

コマンド	目的
hostname(config-aaa-server-group)# **dynamic-authorization {port *port-number*}**	AAA サーバ グループの RADIUS の動的認可（CoA）サービスをイネーブルにします。 定義されると、対応する RADIUS サーバ グループが CoA 通知用に登録され、ASA は ISE からの CoA ポリシー アップデート用ポートをリッスンします。 CoA のリスニング *ポート番号*の有効な範囲は、1 ～ 65535 です。 このコマンドの「no」形式で指定されたポート番号またはインターフェイスが現在のコンフィギュレーションの行に一致しない場合は、エラー メッセージが表示されます。
hostname(config-aaa-server-group)# **authorize-only**	RADIUS サーバ グループ用の認可専用モードをイネーブルにします。これで、このサーバ グループが認可に使用されている場合に RADIUS アクセス要求メッセージが現在利用可能になっている設定済みのパスワード方式ではなく、「認可専用」要求として構築されることが示されます。認可専用要求には値 Authorize-Only（17）を持つサービス タイプ属性と、アクセス要求内のメッセージ認証子が含まれます。 認可専用モードのサポートにより、アクセス要求に RADIUS 共通パスワードを含める必要がなくなります。したがって、AAA サーバ ホスト モードで radius Common pw CLI を使用して共通パスワードを設定する必要はありません。 **（注）** 認可専用モードはサーバ グループに対して設定されますが、共通パスワードはホストに固有です。したがって、認可専用モードを設定すると、個々の AAA サーバに設定された共通パスワードは無視されるようになります。

コマンド	目的
hostname(config-tunnel-webvpn)# **without-csd {anyconnect}**	特定のトンネル グループに行われる接続のホストスキャン処理をオフに切り替えます。この設定は現在、クライアントレスおよび L3 接続に適用されます。このコマンドは、この設定を AnyConnect 接続にのみ適用するように変更されています。
hostname(config-aaa-server-group)# **interim-accounting-update {periodic *interval*}**	RADIUS 中間アカウンティング アップデート メッセージの生成をイネーブルにします。現在、これらのメッセージは、VPN トンネル接続がクライアントレス VPN セッションに追加された場合にだけ生成されます。これが発生した場合、新たに割り当てられた IP アドレスを RADIUS に通知するためのアカウンティング アップデートが生成されます。現在の機能を許可する、またはアカウンティング メッセージを指示されたサーバ グループに送信するように設定されたすべてのセッションに対して定期的な中間アカウンティング アップデートの生成を許可する設定ができるように、このコマンドにキーワードが追加されています。 *periodic*：このオプションのキーワードは、対象のサーバ グループにアカウンティング レコードを送信するように設定されたすべての VPN セッションのアカウンティング レコードの定期的な生成と伝送をイネーブルにします。 *interval*：定期的なアカウンティング アップデート間の間隔の長さを時間単位で表す数値です。有効な範囲は 1 ～ 120 で、デフォルト値は 24 です。

トラブルシューティング

次のコマンドは、デバッグに使用できます。

CoA のアクティビティを追跡するには：

debug radius dynamic-authorization

リダイレクト URL 機能を追跡するには：

debug aaa url-redirect

URL リダイレクト機能に対応する NP 分類ルールを表示するには：

show asp table classify domain url-redirect

接続プロファイル、グループ ポリシー、およびユーザ

この章では、VPN 接続プロファイル（以前は「トンネル グループ」と呼ばれていました）、グループ ポリシー、およびユーザの設定方法について説明します。この章は、次の項で構成されています。

要約すると、最初に接続プロファイルを設定して、接続用の値を設定します。次に、グループ ポリシーを設定します。グループ ポリシーでは、ユーザの集合に関する値が設定されます。その後、ユーザを設定します。ユーザはグループの値を継承でき、さらに個別のユーザ単位に特定の値を設定することができます。この章では、これらのエンティティを設定する方法と理由について説明します。

接続プロファイル、グループ ポリシー、およびユーザの概要

グループとユーザは、バーチャル プライベート ネットワーク（VPN）のセキュリティ管理と ASA の設定における中核的な概念です。グループとユーザで指定される属性によって、VPN へのユーザ アクセスと VPN の使用方法が決定されます。*グループ*は、ユーザの集合を 1 つのエンティティとして扱うものです。*ユーザ*の属性は、*グループ ポリシー*から取得されます。*接続プロファイル*では、特定の接続用のグループ ポリシーを指定します。ユーザに対して特定のグループ ポリシーを割り当てない場合は、接続のデフォルト グループ ポリシーが適用されます。

（注） 接続プロファイルは、**tunnel-group** コマンドを使用して設定します。この章では、「接続プロファイル」と「トンネル グループ」は頻繁にほとんど同じ意味で使用されています。

接続プロファイルとグループ ポリシーを使用すると、システム管理が簡略化されます。コンフィギュレーション タスクを効率化するために、ASA にはデフォルトの LAN-to-LAN 接続プロファイル、デフォルトのリモート アクセス接続プロファイル、SSL/IKEv2 VPN 用のデフォルトの接続プロファイル、およびデフォルトのグループ ポリシー（DfltGrpPolicy）が用意されています。デフォルトの接続プロファイルとグループ ポリシーでは、多くのユーザに共通すると考えられる設定が提供されます。ユーザを追加するときに、グループ ポリシーからパラメータを「継承」するように指定できます。これにより、数多くのユーザに対して迅速に VPN アクセスを設定できます。

すべての VPN ユーザに同一の権限を許可する場合は、特定の接続プロファイルやグループ ポリシーを設定する必要はありませんが、VPN がそのように使用されることはほとんどありません。たとえば、経理グループ、カスタマー サポート グループ、および MIS（経営情報システム）グループが、プライベート ネットワークのそれぞれ異なる部分にアクセスできるようにする場合が考えられます。また、MIS に所属する特定のユーザには、他の MIS ユーザにはアクセスできないシステムにアクセスを許可する場合があります。接続プロファイルとグループ ポリシーにより、このような柔軟な設定を安全に実行することができます。

（注） ASA には、オブジェクト グループという概念もあります。これは、ネットワーク リストのスーパーセットです。オブジェクト グループを使用すると、ポートやネットワークに対する VPN アクセスを定義することができます。オブジェクト グループは、グループ ポリシーや接続プロファイルよりも、ACL と関連があります。オブジェクト グループの使用方法の詳細については、一般的な操作のコンフィギュレーション ガイドの第 20 章「オブジェクト」を参照してください。

セキュリティ アプライアンスでは、さまざまなソースから属性値を適用できます。次の階層に従って、属性値を適用します。

1. ダイナミック アクセス ポリシー（DAP）レコード
2. ユーザ名
3. グループ ポリシー
4. 接続プロファイル用のグループ ポリシー
5. デフォルトのグループ ポリシー

そのため、属性の DAP 値は、ユーザ、グループ ポリシー、または接続プロファイル用に設定された値よりもプライオリティが高くなっています。

DAP レコードの属性をイネーブルまたはディセーブルにすると、ASA はその値を適用して実行します。たとえば、DAP webvpn コンフィギュレーション モードで HTTP プロキシをディセーブルにすると、ASA はそれ以上値を検索しません。代わりに、**http-proxy** コマンドの **no** 値を使用すると、属性は DAP レコードに存在しないため、適用する値を検索するために、セキュリティ アプライアンスはユーザ名の AAA 属性、および必要に応じてグループ ポリシーに移動して適用する値を検出します。ASA クライアントレス SSL VPN コンフィギュレーションは、それぞれ 1 つの **http-proxy** コマンドと 1 つの **https-proxy** コマンドのみサポートしています。ASDM を使用して DAP を設定することをお勧めします。

接続プロファイル

接続プロファイルは、トンネル接続ポリシーを決定するレコードのセットで構成されます。これらのレコードは、トンネル ユーザが認証先サーバ、および接続情報の送信先となるアカウンティング サーバ（存在する場合）を特定します。また、これらのレコードには、接続用のデフォルト グループ ポリシーも指定され、さらにプロトコル固有の接続パラメータも含まれています。接続プロファイルには、トンネル自体の作成に関連する少数の属性が含まれます。接続プロファイルには、ユーザ関連の属性を定義するグループ ポリシーへのポインタも含まれます。

ASA には、LAN-to-LAN 接続用の DefaultL2Lgroup、リモート アクセス用の DefaultRAgroup、および SSL VPN（ブラウザベース）接続用の DefaultWEBVPNGroup という、デフォルト接続プロファイルがあります。これらのデフォルト接続プロファイルは変更できますが、削除はできません。また、環境に固有の接続プロファイルを 1 つ以上作成することもできます。接続プロファイルは、ASA のローカルな設定であり、外部サーバでは設定できません。

接続プロファイルでは、次の属性が指定されます。

- 「接続プロファイルの一般接続パラメータ」（P.4-3）
- 「IPSec トンネルグループ接続パラメータ」（P.4-4）
- 「接続プロファイルの SSL VPN セッション接続パラメータ」（P.4-6）

接続プロファイルの一般接続パラメータ

一般パラメータは、すべての VPN 接続に共通です。一般パラメータには、次のものがあります。

- 接続プロファイル名：接続プロファイル名は、接続プロファイルを追加または編集するときに指定します。次の注意事項があります。
  - 認証に事前共有キーを使用するクライアントの場合、接続プロファイル名はクライアントが ASA に渡すグループ名と同じです。
  - 認証に証明書を使用するクライアントはこの名前を証明書の一部として渡し、ASA が証明書からこの名前を抽出します。
- 接続タイプ：接続タイプには、IKEv1 リモート アクセス、IPsec Lan-to-LAN、および Anyconnect（SSL/IKEv2）が含まれます。接続プロファイルでは、1 つの接続タイプだけ指定できます。
- 認証、認可、アカウンティング サーバ：これらのパラメータでは、ASA が次の目的で使用するサーバのグループまたはリストを指定します。
  - ユーザの認証
  - ユーザがアクセスを認可されたサービスに関する情報の取得
  - アカウンティング レコードの保存

  サーバ グループは、1 つ以上のサーバで構成されます。
- 接続用のデフォルト グループ ポリシー：グループ ポリシーは、ユーザ関連の属性のセットです。デフォルト グループ ポリシーは、ASA がトンネル ユーザを認証または認可する際にデフォルトで使用する属性を含んだグループ ポリシーです。
- クライアント アドレスの割り当て方式：この方式には、ASA がクライアントに割り当てる 1 つ以上の DHCP サーバまたはアドレス プールの値が含まれます。
- アカウント無効の上書き：このパラメータを使用すると、AAA サーバから受信した「account-disabled」インジケータを上書きできます。

- パスワード管理：このパラメータを使用すると、現在のパスワードが指定日数（デフォルトは 14 日）で期限切れになることをユーザに警告して、パスワードを変更する機会をユーザに提供できます。
- グループ除去およびレルム除去：これらのパラメータにより、ASA が受信するユーザ名を処理する方法が決まります。これらは、user@realm の形式で受信するユーザ名にだけ適用されます。

  レルムは @ デリミタ付きでユーザ名に付加される管理ドメインです（user@abc）。レルムを除去する場合、ASA は認証にユーザ名およびグループ（ある場合）を使用します。グループを除去すると、ASA は認証にユーザ名およびレルム（ある場合）を使用します。

  レルム修飾子を除去するには strip-realm コマンドを入力し、認証中にユーザ名からグループ修飾子を削除するには strip-group コマンドを入力します。両方の修飾子を削除すると、認証は *username* だけに基づいて行われます。それ以外の場合、認証は *username@realm* 文字列全体または *username<delimiter> group* 文字列に基づいて行われます。サーバでデリミタを解析できない場合は、strip-realm を指定する必要があります。

  さらに、L2TP/IPsec クライアントの場合に strip-group コマンドを指定すると、ASA は VPN クライアントが提示したユーザ名からグループ名を取得してユーザ接続の接続プロファイル（トンネル グループ）を選択します。
- 認可の要求：このパラメータを使用すると、ユーザ接続の前に認可を要求したり、またはその要求を取り下げたりできます。
- 認可 DN 属性:このパラメータは､認可を実行するときに使用する認定者名属性を指定します。

IPSec トンネルグループ接続パラメータ

IPSec パラメータには、次のものがあります。

- クライアント認証方式：事前共有キー、証明書、または両方。
  - 事前共有キーに基づいた IKE 接続の場合、接続ポリシーに関連付けられた英数字のキー自体です（最大 128 文字）。
  - ピア ID 確認の要求：このパラメータでは、ピアの証明書を使用してピア ID の確認を要求するかどうかを指定します。
  - 認証方式に証明書または両方を指定する場合、エンド ユーザは認証のために有効な証明書を指定する必要があります。
- 拡張ハイブリッド認証方式：XAUTH およびハイブリッド XAUTH。

  isakmp ikev1-user-authentication コマンドは、ASA 認証にデジタル証明書を使用する必要があり、かつリモート VPN ユーザ認証に RADIUS、TACACS+、または SecurID などのレガシーな方式を別途使用する必要がある場合に、ハイブリッド XAUTH 認証を実装するために使用します。
- ISAKMP（IKE）キープアライブの設定：この機能により、ASA はリモート ピアの継続的な存在をモニタし、自分自身の存在をピアに報告します。ピアが応答しなくなると、ASA は接続を削除します。IKE キープアライブをイネーブルにすると、IKE ピアが接続を失ったときに接続がハングしません。

IKE キープアライブにはさまざまな形式があります。この機能が動作するには、ASA とリモート ピアが共通の形式をサポートしている必要があります。この機能は、次のピアに対して動作します。

- Cisco AnyConnet VPN Client
- Cisco VPN Client（Release 3.0 以上）
- Cisco VPN 3000 Client（Release 2.x）
- Cisco VPN 3002 Hardware Client
- Cisco VPN 3000 シリーズ Concentrator
- Cisco IOS ソフトウェア
- Cisco Secure PIX Firewall

シスコ以外の VPN クライアントは IKE キープアライブをサポートしません。

IKE キープアライブをサポートするピアとサポートしないピアが混在するグループを設定する場合は、グループ全体に対して IKE キープアライブをイネーブルにします。この機能をサポートしないピアに影響はありません。

IKE キープアライブをディセーブルにすると、応答しないピアとの接続はタイムアウトになるまでアクティブのままになるため、アイドル タイムアウトを短くすることを推奨します。アイドル タイムアウトを変更するには、「グループ ポリシーの設定」（P.4-42）を参照してください。

（注） ISDN 回線経由で接続するクライアントがグループに含まれる場合は、接続コストを削減するために IKE キープアライブをディセーブルにしてください。通常、ISDN 接続はアイドルになると切断されますが、IKE キープアライブのメカニズムによって接続がアイドル状態にならないため、切断されなくなります。

IKE キープアライブをディセーブルにすると、クライアントは IKE キーと IPSec キーのどちらかの期限が満了した場合にだけ切断されます。IKE キープアライブがイネーブルになっている場合とは異なり、障害が発生したトラフィックは Peer Timeout Profile 値を持つトンネルから切断されません。

（注） IKE メイン モードを使用する LAN-to-LAN コンフィギュレーションの場合は、2 つのピアの IKE キープアライブのコンフィギュレーションが同じであることを確認してください。両方のピアで IKE キープアライブがイネーブルになっているか、または両方のピアで IKE キープアライブがディセーブルになっている必要があります。

- デジタル証明書を使用して認証を設定する場合、証明書チェーン全体を送信する（ID 証明書と発行するすべての証明書をピアに送信する）か、証明書だけを発行する（ルート証明書とすべての下位 CA 証明書を含む）かを指定できます。
- Windows クライアント ソフトウェアの古いバージョンを使用しているユーザに、クライアントをアップデートする必要があることを通知し、アップデートされたクライアント バージョンをユーザが取得するためのメカニズムを提供できます。VPN 3002 ハードウェア クライアント ユーザの場合は、自動アップデートをトリガーできます。すべての接続プロファイルまたは特定の接続プロファイルに対して、client-update を設定および変更できます。
- デジタル証明書を使用して認証を設定する場合は、IKE ピアに送信する証明書を識別するトラストポイントの名前を指定できます。

接続プロファイルの SSL VPN セッション接続パラメータ

表 4-1 は、SSL VPN（AnyConnect クライアントおよびクライアントレス）接続に固有の接続プロファイルの属性のリストです。これらの属性に加えて、すべての VPN 接続に共通の一般接続プロファイルの属性を設定します。接続プロファイルの設定に関する手順ごとの情報については、「クライアントレス SSL VPN セッションの接続プロファイルの設定」（P.4-22）を参照してください。

（注）　以前のリリースでは、「接続プロファイル」は「トンネル グループ」と呼ばれていました。tunnel-group コマンドを使用して接続プロファイルを設定します。この章では、この 2 つの用語が同義的によく使用されています。

表 4-1　SSL VPN 用接続プロファイルの属性

コマンド	機能
authentication	認証方式、AAA または証明書を設定します。
customization	適用するすでに定義済みのカスタマイゼーションの名前を指定します。カスタマイゼーションによって、ログイン時にユーザに表示されるウィンドウの外観が決まります。カスタマイゼーション パラメータは、クライアントレス SSL VPN の設定の一部として設定します。
nbns-server	CIFS 名前解決に使用する NetBIOS ネーム サービス サーバ（nbns-server）の名前を指定します。
group-alias	サーバから接続プロファイルを参照できる 1 つ以上の代替名を指定します。ログイン時に、ユーザはドロップダウン メニューからグループ名を選択します。
group-url	1 つ以上のグループ URL を指定します。この属性を設定する場合、指定した URL にアクセスするユーザは、ログイン時にグループを選択する必要はありません。
dns-group	DNS サーバ名、ドメイン名、ネーム サーバ、リトライ回数、および接続ファイルで使用される DNS サーバのタイムアウト値を指定する DNS サーバ グループを指定します。
hic-fail-group-policy	Cisco Secure Desktop Manager を使用して、グループベース ポリシー属性を「Use Failure Group-Policy」または「Use Success Group-Policy, if criteria match」に設定する場合は、VPN 機能ポリシーを指定します。
override-svc-download	AnyConnect VPN クライアントをリモート ユーザにダウンロードするために、設定されているグループ ポリシー属性またはユーザ名属性のダウンロードが上書きされます。
radius-reject-message	認証が拒否されたときに、ログイン画面に RADIUS 拒否メッセージを表示します。

接続プロファイルの設定

ここでは、シングル コンテキスト モードまたはマルチ コンテキスト モードの両方での接続プロファイルの内容および設定について説明します。

（注）　マルチ コンテキスト モードは IKEv1 および IKEv2 サイトツーサイトにのみ適用され、IKEv1 IPSec の AnyConnect、クライアントレス SSL VPN、レガシー Cisco VPN クライアント、Apple ネイティブ VPN クライアント、Microsoft ネイティブ VPN クライアント、または cTCP には適用されません。

デフォルトの接続プロファイルを変更し、3 つのトンネルグループ タイプのいずれかで新しい接続プロファイルを設定できます。接続プロファイル内で明示的に設定しない属性に対しては、その値がデフォルトの接続プロファイルから取得されます。デフォルトの接続プロファイル タイプはリモート アクセスです。その後のパラメータは、選択したトンネル タイプによって異なります。デフォルト接続プロファイルも含めて、すべての接続プロファイルの現在のコンフィギュレーションとデフォルトのコンフィギュレーションを確認するには、**show running-config all tunnel-group** コマンドを入力します。

接続プロファイルの最大数

1 つの ASA がサポートできる接続プロファイル（トンネル グループ）の最大数は、プラットフォームの同時 VPN セッションの最大数 + 5 の関数です。制限を超えるトンネル グループを追加しようとすると、「ERROR: The limit of 30 configured tunnel groups has been reached」メッセージが表示されます。

デフォルトの IPsec リモート アクセス接続プロファイルの設定

デフォルトのリモート アクセス接続プロファイルの内容は、次のとおりです。

```
tunnel-group DefaultRAGroup type remote-access
tunnel-group DefaultRAGroup general-attributes
 no address-pool
 no ipv6-address-pool
 authentication-server-group LOCAL
 accounting-server-group RADIUS
 default-group-policy DfltGrpPolicy
 no dhcp-server
 no strip-realm
 no password-management
 no override-account-disable
 no strip-group
 no authorization-required
 authorization-dn-attributes CN OU
tunnel-group DefaultRAGroup webvpn-attributes
 hic-fail-group-policy DfltGrpPolicy
 customization DfltCustomization
 authentication aaa
 no override-svc-download
 no radius-reject-message
 dns-group DefaultDNS
tunnel-group DefaultRAGroup ipsec-attributes
 no pre-shared-key
 peer-id-validate req
 no chain
 no trust-point
 isakmp keepalive threshold 1500 retry 2
 no radius-sdi-xauth
 isakmp ikev1-user-authentication xauth
tunnel-group DefaultRAGroup ppp-attributes
 no authentication pap
 authentication chap
 authentication ms-chap-v1
 no authentication ms-chap-v2
 no authentication eap-proxy
```

IPSec トンネルグループの一般属性の設定

一般属性は、複数のトンネルグループ タイプに共通です。IPSec リモート アクセス トンネルとクライアントレス SSL VPN トンネルでは、同じ一般属性の大部分を共有しています。IPSec LAN-to-LAN トンネルは、サブセットを使用します。すべてのコマンドの詳細については、『*Cisco ASA Series Command Reference*』を参照してください。ここでは、リモート アクセス接続プロファイルおよび LAN-to-LAN 接続プロファイルを設定する方法について順に説明します。

リモート アクセス接続プロファイルの設定

次のリモート クライアントと中央サイトの ASA の間に接続を設定する場合は、リモート アクセス接続プロファイルを使用します。

- レガシー Cisco VPN Client（IPsec/IKEv1 と接続）
- AnyConnect Secure Mobility Client（SSL または IPsec/IKEv2 と接続）
- クライアントレス SSL VPN（SSL とのブラウザベースの接続）
- Cisco ASA 5500 Easy VPN ハードウェア クライアント（IPsec/IKEv1 と接続）
- Cisco VPM 3002 ハードウェア クライアント（IPsec/IKEv1 と接続）

また、*DfltGrpPolicy* という名前のデフォルト グループ ポリシーも提供します。

リモート アクセス接続プロファイルを設定するには、最初にトンネル グループ一般属性を設定し、次にリモート アクセス属性を設定します。次の項を参照してください。

- 「リモート アクセス接続プロファイルの名前とタイプの指定」（P.4-9）
- 「リモート アクセス接続プロファイルの一般属性の設定」（P.4-9）
- 「二重認証の設定」（P.4-13）
- 「リモート アクセス接続プロファイルの IPSec IKEv1 属性の設定」（P.4-15）
- 「IPSec リモート アクセス接続プロファイルの PPP 属性の設定」（P.4-17）

リモート アクセス接続プロファイルの名前とタイプの指定

tunnel-group コマンドを入力し、名前とタイプを指定して、接続プロファイルを作成します。リモート アクセス トンネルの場合、タイプは **remote-access** です。

```
hostname(config)# tunnel-group tunnel_group_name type remote-access
hostname(config)#
```

たとえば、TunnelGroup1 という名前のリモート アクセス接続プロファイルを作成するには、次のコマンドを入力します。

```
hostname(config)# tunnel-group TunnelGroup1 type remote-access
hostname(config)#
```

リモート アクセス接続プロファイルの一般属性の設定

接続プロファイルの一般属性を設定または変更するには、次の手順でパラメータを指定します。

ステップ 1　一般属性を設定するには、シングル コンテキスト モードまたはマルチ コンテキスト モードで **tunnel-group general-attributes** タスクを入力します。これで、トンネルグループ一般属性コンフィギュレーション モードが開始されます。プロンプトが変化して、モードが変更されたことがわかります。

```
hostname(config)# tunnel-group tunnel_group_name general-attributes
hostname(config-tunnel-general)#
```

ステップ 2　認証サーバ グループがある場合、使用するグループの名前を指定します。指定したサーバ グループに障害が発生したときにローカル データベースを認証に使用する場合は、キーワード **LOCAL** を追加します。

```
hostname(config-tunnel-general)# authentication-server-group [(interface_name)] groupname
[LOCAL]
hostname(config-tunnel-general)#
```

認証サーバ グループの名前は、最大 16 文字です。

オプションで、グループ名の後ろにインターフェイス名を指定することにより、インターフェイス固有の認証を設定することもできます。トンネルの終了場所を指定するインターフェイス名は、丸カッコで囲む必要があります。次のコマンドでは、認証にサーバ servergroup1 を使用する test という名前のインターフェイスのインターフェイス固有の認証が設定されます。

```
hostname(config-tunnel-general)# authentication-server-group (test) servergroup1
hostname(config-tunnel-general)#
```

ステップ 3　使用する認可サーバ グループの名前を指定します（存在する場合）。この値を設定する場合、ユーザは接続する認可データベースに存在する必要があります。

```
hostname(config-tunnel-general)# authorization-server-group groupname
hostname(config-tunnel-general)#
```

認可サーバ グループの名前は、最大 16 文字です。たとえば、次のコマンドは、認可サーバ グループ FinGroup を使用することを指定しています。

```
hostname(config-tunnel-general)# authorization-server-group FinGroup
hostname(config-tunnel-general)#
```

ステップ 4　アカウンティングサーバ グループがある場合、使用するグループの名前を指定します。

```
hostname(config-tunnel-general)# accounting-server-group groupname
hostname(config-tunnel-general)#
```

アカウンティング サーバ グループの名前は、最大 16 文字です。たとえば、次のコマンドは、アカウンティングサーバ グループ comptroller を使用することを指定しています。

```
hostname(config-tunnel-general)# accounting-server-group comptroller
hostname(config-tunnel-general)#
```

ステップ 5　デフォルト グループ ポリシーの名前を指定します。

```
hostname(config-tunnel-general)# default-group-policy policyname
hostname(config-tunnel-general)#
```

グループ ポリシーの名前は、最大 64 文字です。次の例では、デフォルト グループ ポリシーの名前として DfltGrpPolicy を設定しています。

```
hostname(config-tunnel-general)# default-group-policy DfltGrpPolicy
hostname(config-tunnel-general)#
```

ステップ 6　DHCP サーバ（最大 10 サーバ）の名前または IP アドレス、および DHCP アドレス プール（最大 6 プール）の名前を指定します。デフォルトでは、DHCP サーバとアドレス プールは使用されません。**dhcp-server** コマンドにより、VPN クライアントの IP アドレスを取得しようとするときに、指定の DHCP サーバに追加オプションを送信するように ASA を設定できるようになります。詳細については、『*Cisco ASA Series Command Reference*』の **dhcp-server** コマンドを参照してください。

```
hostname(config-tunnel-general)# dhcp-server server1 [...server10]
hostname(config-tunnel-general)# address-pool [(interface name)] address_pool1
[...address_pool6]
hostname(config-tunnel-general)#
```

（注）　インターフェイス名を指定する場合は、丸カッコで囲む必要があります。

アドレス プールは、グローバル コンフィギュレーション モードで **ip local pool** コマンドを使用して設定します。

ステップ 7　ネットワーク アドミッション コントロールを使用している場合は、ネットワーク アドミッション コントロール ポスチャ検証で使用される認証サーバのグループを特定するために、NAC 認証サーバ グループの名前を指定します。NAC をサポートするように、少なくとも 1 つの Access Control Server を設定します。ACS グループの名前を指定するには、**aaa-server** コマンドを使用します。次に、その同じ名前をサーバ グループに使用して、**nac-authentication-server-group** コマンドを使用します。

次に、NAC ポスチャ検証に使用される認証サーバ グループとして acs-group1 を識別する例を示します。

```
hostname(config-group-policy)# nac-authentication-server-group acs-group1
hostname(config-group-policy)
```

次に、デフォルトのリモート アクセス グループから認証サーバ グループを継承する例を示します。

```
hostname(config-group-policy)# no nac-authentication-server-group
hostname(config-group-policy)
```

（注）　NAC を使用するには、リモート ホスト上に Cisco Trust Agent が存在する必要があります。

ステップ 8　ユーザ名を AAA サーバに渡す前に、ユーザ名からグループまたはレルムを除去するかどうかを指定します。デフォルトでは、グループ名もレルムも除去されません。

```
hostname(config-tunnel-general)# strip-group
hostname(config-tunnel-general)# strip-realm
hostname(config-tunnel-general)#
```

レルムとは管理ドメインのことです。レルムを除去する場合、ASA はユーザ名およびグループ（ある場合）認証を使用します。グループを除去すると、ASA は認証にユーザ名およびレルム（ある場合）を使用します。レルム修飾子を削除するには **strip-realm** コマンドを入力し、認証中にユーザ名からグループ修飾子を削除するには strip-group コマンドを使用します。両方の修飾子を削除すると、認証は *username* だけに基づいて行われます。それ以外の場合、認証は *username@realm* 文字列全体または *username<delimiter> group* 文字列に基づいて行われます。サーバでデリミタを解析できない場合は、**strip-realm** を指定する必要があります。

ステップ 9　サーバが RADIUS、RADIUS with NT、または LDAP サーバの場合、オプションで、パスワード管理をイネーブルにできます。

（注）　認証に LDAP ディレクトリ サーバを使用している場合、パスワード管理は Sun Microsystems JAVA System Directory Server（旧名称は Sun ONE Directory Server）および Microsoft Active Directory を使用してサポートされます。

Sun：Sun ディレクトリ サーバにアクセスするために ASA に設定されている DN は、そのサーバ上のデフォルト パスワード ポリシーにアクセスできる必要があります。DN として、ディレクトリ管理者、またはディレクトリ管理者権限を持つユーザを使用することを推奨します。または、デフォルト パスワード ポリシーに ACI を設定できます。

Microsoft：Microsoft Active Directory を使用したパスワード管理をイネーブルにするには、LDAP over SSL を設定する必要があります。

この機能はデフォルトでディセーブルになっており、現在のパスワードの有効期限が近づくとユーザに警告を表示します。デフォルトでは、期限切れの 14 日前に警告が開始されます。

```
hostname(config-tunnel-general)# password-management
hostname(config-tunnel-general)#
```

サーバが LDAP サーバの場合、有効期限が近いことに関する警告が開始されるまでの日数（0 ～ 180）を指定できます。

```
hostname(config-tunnel-general)# password-management [password-expire in days n]
hostname(config-tunnel-general)#
```

（注）　トンネルグループ一般属性コンフィギュレーション モードで入力した **password-management** コマンドによって、トンネルグループ ipsec 属性モードで事前に入力された非推奨の **radius-with-expiry** コマンドが置き換えられます。

password-management コマンドを設定すると、ASA は、リモート ユーザがログインするときに、そのユーザの現在のパスワードの期限切れが迫っている、または期限が切れたことを通知します。それから ASA は、ユーザがパスワードを変更できるようにします。現行のパスワードが失効していない場合、ユーザはそのパスワードを使用してログインし続けることができます。RADIUS または LDAP 認証が設定されていない場合、ASA ではこのコマンドが無視されます。

これによってパスワードが期限切れになるまでの日数が変更されるわけではなく、ASA がパスワードが期限切れになる何日前にユーザへの警告を開始するかが変更されるという点に注意してください。

password-expire-in-days キーワードを指定する場合は、日数も指定する必要があります。

このコマンドで日数に 0 を指定すると、このコマンドはディセーブルになります。ASA は、ユーザに対して失効が迫っていることを通知しませんが、失効後にユーザはパスワードを変更できます。

詳細については、「パスワード管理用の Microsoft Active Directory の設定」（P.4-31）を参照してください。

（注）　ASA Version 7.1 以降では、LDAP または MS-CHAPv2 をサポートする RADIUS 接続で認証を行うときに、AnyConnect VPN Client 接続、Cisco IPSec VPN Client 接続、SSL VPN 完全トンネリング クライアント接続、およびクライアントレス接続に対するパスワード管理が一般的にサポートされています。Kerberos/AD（Windows パスワード）または NT 4.0 ドメインに対するこれらの接続タイプのいずれでも、パスワード管理はサポートされて*いません*。

MS-CHAP をサポートしている一部の RADIUS サーバは、現在 MS-CHAPv2 をサポートしていません。**password-management** コマンドを使用するには、MS-CHAPv2 が必要なため、ベンダーに確認してください。

RADIUS サーバ（Cisco ACS など）は、認証要求を別の認証サーバにプロキシする場合があります。ただし、ASA からは RADIUS サーバのみに対して通信しているように見えます。

LDAP でパスワードを変更するには、市販の LDAP サーバごとに独自の方法が使用されています。現在、ASA では Microsoft Active Directory および Sun LDAP サーバに対してのみ、独自のパスワード管理ロジックを実装しています。ネイティブ LDAP には、SSL 接続が必要です。LDAP のパスワード管理を実行する前に、SSL 上での LDAP をイネーブルにする必要があります。デフォルトでは、LDAP はポート 636 を使用します。

ステップ 10　オプションで、**override-account-disable** コマンドを入力して、AAA サーバからの account-disabled インジケータを上書きする機能を設定できます。

```
hostname(config-tunnel-general)# override-account-disable
hostname(config-tunnel-general)#
```

（注）　override-account-disable を許可することは、潜在的なセキュリティ リスクとなります。

ステップ 11　証明書から認可クエリー用の名前を得るために使用する 1 つまたは複数の属性を指定します。この属性により、サブジェクト DN フィールドのどの部分を認可用のユーザ名として使用するかが指定されます。

```
hostname(config-tunnel-general)# authorization-dn-attributes {primary-attribute
[secondary-attribute] | use-entire-name}
```

たとえば、次のコマンドは、CN 属性を認可用のユーザ名として使用することを指定しています。

```
hostname(config-tunnel-general)# authorization-dn-attributes CN
hostname(config-tunnel-general)#
```

authorization-dn-attributes は、**C**（国）、**CN**（通常名）、**DNQ**（DN 修飾子）、**EA**（電子メール アドレス）、**GENQ**（世代修飾子）、**GN**（名）、**I**（イニシャル）、**L**（地名）、**N**（名前）、**O**（組織）、**OU**（組織ユニット）、**SER**（シリアル番号）、**SN**（姓）、**SP**（州または都道府県）、**T**（役職）、**UID**（ユーザ ID）、および **UPN**（ユーザ プリンシパル ネーム）があります。

ステップ 12　ユーザに接続を許可する前に、そのユーザが正常に認可されている必要があるかどうかを指定します。デフォルトでは認可は要求されません。

```
hostname(config-tunnel-general)# authorization-required
hostname(config-tunnel-general)#
```

二重認証の設定

二重認証は、ユーザがログイン画面に追加の認証クレデンシャル（2 つ目のユーザ名とパスワードなど）を入力するよう要求するオプションの機能です。二重認証を設定するには、次のコマンドを指定します。

ステップ 1　セカンダリ認証サーバ グループを指定します。このコマンドはセカンダリ AAA サーバとして使用する AAA サーバ グループを指定します。

（注）　このコマンドは、AnyConnect クライアント VPN 接続にだけ適用されます。

セカンダリのサーバ グループでは SDI サーバ グループを指定できません。デフォルトでは、セカンダリ認証は必要ありません。

```
hostname(config-tunnel-general)# secondary-authentication-server-group [interface_name]
{none | LOCAL | groupname [LOCAL]} [use-primary-name]
```

none キーワードを指定すると、セカンダリ認証は要求されません。*groupname* 値は AAA サーバ グループ名を示します。ローカルは内部サーバ データベースを使用することを示し、groupname 値と併用すると、LOCAL はフォールバックを示します。たとえば、プライマリ認証サーバ グループを sdi_group に、セカンダリ認証サーバ グループを ldap_server に設定するには、次のコマンドを入力します。

```
hostname(config-tunnel-general)# authentication-server-group
hostname(config-tunnel-general)# secondary-authentication-server-group
```

（注）　**use-primary-name** キーワードを使用する場合、ログイン ダイアログは 1 つのユーザ名だけ要求します。また、ユーザ名をデジタル証明書から抽出する場合、プライマリ ユーザ名だけが認証に使用されます。

ステップ 2　セカンダリ ユーザ名を証明書から取得する場合は、**secondary-username-from-certificate** を入力します。

```
hostname(config-tunnel-general)# secondary-username-from-certificate C | CN | ... |
use-script
```

セカンダリ ユーザ名として使用するために証明書から抽出する DN フィールドの値は、プライマリの **username-from-certificate** コマンドと同じです。または、use-script キーワードを指定して、ASDM によって生成されたスクリプト ファイルを使用するよう ASA に指示します。

たとえば、プライマリ ユーザ名フィールドとして通常名を、セカンダリ ユーザ名フィールドとして組織ユニットを指定するには、次のコマンドを入力します。

```
hostname(config-tunnel-general)# tunnel-group test1 general-attributes
hostname(config-tunnel-general)# username-from-certificate cn
hostname(config-tunnel-general)# secondary-username-from-certificate ou
```

ステップ 3　認証で使用するためにクライアント証明書からセカンダリ ユーザ名を抽出できるようにするには、トンネルグループ webvpn 属性モードで **secondary-pre-fill-username** コマンドを使用します。このコマンドをクライアントレス接続または SSL VPN（AnyConnect）クライアント接続に適用するかどうか、抽出されたユーザ名をエンド ユーザに非表示にするかどうかを指定するキーワードを使用します。この機能はデフォルトで無効に設定されています。クライアントレス オプションと SSL クライアント オプションは同時に使用できますが、それぞれ別個のコマンドで設定する必要があります。

```
hostname(config-tunnel-general)# secondary-pre-fill-username-from-certificate {clientless
| ssl-client} [hide]
```

たとえば、接続のプライマリとセカンダリの両方の認証に pre-fill-username を使用するには、次のコマンドを入力します。

```
hostname(config-tunnel-general)# tunnel-group test1 general-attributes
hostname(config-tunnel-general)# pre-fill-username ssl-client
hostname(config-tunnel-general)# secondary-pre-fill-username ssl-client
```

ステップ 4　接続に適用する認可属性を取得するために使用する認証サーバを指定します。デフォルトの選択は、プライマリ認証サーバです。このコマンドは二重認証でのみ意味を持ちます。

```
hostname(config-tunnel-general)# authentication-attr-from-server {primary | secondary}
```

たとえば、セカンダリ認証サーバを指定するには、次のコマンドを入力します。

```
hostname(config-tunnel-general)# tunnel-group test1 general-attributes
hostname(config-tunnel-general)# authentication-attr-from-server secondary
```

ステップ 5　セッションと関連付ける認証ユーザ名（プライマリまたはセカンダリ）を指定します。デフォルト値は primary です。二重認証をイネーブルにすると、2 つの別のユーザ名でセッションを認証できます。管理者はセッションのユーザ名として認証されたユーザ名のいずれかを指定する必要があります。セッションのユーザ名は、アカウンティング、セッション データベース、syslog、デバッグ出力に提供されるユーザ名です。

```
hostname(config-tunnel-general)# authenticated-session-username {primary | secondary}
```

たとえば、セッションと関連付ける認証ユーザ名をセカンダリ認証サーバから取得するよう指定するには、次のコマンドを入力します。

```
hostname(config-tunnel-general)# tunnel-group test1 general-attributes
hostname(config-tunnel-general)# authenticated-session-username secondary
```

リモート アクセス接続プロファイルの IPSec IKEv1 属性の設定

リモート アクセス接続プロファイルの IPSec IKEv1 属性を設定するには、次の手順を実行します。次の説明は、リモート アクセス接続プロファイルをすでに作成していることを前提としています。リモート アクセス接続プロファイルには、LAN-to-LAN 接続プロファイルよりも多くの属性があります。

ステップ 1　リモート アクセス トンネル グループの IPSec 属性を指定するには、シングル コンテキスト モードまたはマルチ コンテキスト モードで次のコマンドを入力してトンネルグループ ipsec 属性モードを開始します。プロンプトが変化して、モードが変更されたことがわかります。

```
hostname(config)# tunnel-group tunnel-group-name ipsec-attributes
hostname(config-tunnel-ipsec)#
```

このコマンドにより、トンネル グループ ipsec 属性コンフィギュレーション モードが開始されます。このモードでは、シングル コンテキスト モードまたはマルチ コンテキスト モードでリモート アクセス トンネルグループの IPSec 属性を設定します。

たとえば、次のコマンドは、TG1 という名前の接続プロファイルに関係するトンネルグループ ipsec 属性モードのコマンドが続くことを指定しています。プロンプトが変化して、トンネルグループ ipsec 属性モードに入ったことがわかります。

```
hostname(config)# tunnel-group TG1 type remote-access
hostname(config)# tunnel-group TG1 ipsec-attributes
hostname(config-tunnel-ipsec)#
```

ステップ 2　事前共有キーに基づく IKEv1 接続をサポートするために、事前共有キーを指定します。たとえば、次のコマンドは、IPsec IKEv1 リモート アクセス接続プロファイルの IKEv1 接続をサポートするために、事前共有キー xyzx を指定しています。

```
hostname(config-tunnel-ipsec)# ikev1 pre-shared-key xyzx
hostname(config-tunnel-ipsec)#
```

ステップ 3　ピアの証明書を使用してピアの ID を検証するかどうかを指定します。

```
hostname(config-tunnel-ipsec)# peer-id-validate option
hostname(config-tunnel-ipsec)#
```

使用できる*オプション*値は、**req**（必須）、**cert**（証明書でサポートされている場合）、**nocheck**（調べない）です。デフォルトは **req** です。

たとえば、次のコマンドは peer-id 検証が必要なことを指定しています。

```
hostname(config-tunnel-ipsec)# peer-id-validate req
```

```
hostname(config-tunnel-ipsec)#
```

ステップ 4　証明書チェーンを送信できるかどうかを指定します。次のコマンドは、ルート証明書とすべての下位 CA 証明書を送信しています。

```
hostname(config-tunnel-ipsec)# chain
hostname(config-tunnel-ipsec)#
```

この属性は、すべての IPsec トンネルグループ タイプに適用されます。

ステップ 5　IKE ピアに送信する証明書を識別するトラストポイントの名前を指定します。

```
hostname(config-tunnel-ipsec)# ikev1 trust-point trust-point-name
hostname(config-tunnel-ipsec)#
```

次のコマンドは、IKE ピアに送信する証明書の名前として mytrustpoint を指定しています。

```
hostname(config-ipsec)# ikev1 trust-point mytrustpoint
```

ステップ 6　ISAKMP キープアライブのしきい値と許可されるリトライ回数を指定します。

```
hostname(config-tunnel-ipsec)# isakmp keepalive threshold <number> retry <number>
hostname(config-tunnel-ipsec)#
```

threshold パラメータでは、ピアがキープアライブ モニタリングを開始するまでの最長アイドル時間を秒数（10 ～ 3600）で指定します。**retry** パラメータは、キープアライブ応答が受信されなくなった後のリトライ間の間隔です（2 ～ 10 秒）。IKE キープアライブは、デフォルトでイネーブルです。ISAKMP キープアライブをディセーブルにするには、**isakmp keepalive disable** と入力します。

たとえば、次のコマンドは、IKE キープアライブのしきい値を 15 秒に設定し、リトライ インターバルを 10 秒に設定します。

```
hostname(config-tunnel-ipsec)# isakmp keepalive threshold 15 retry 10
hostname(config-tunnel-ipsec)#
```

threshold パラメータのデフォルト値は、リモート アクセスの場合は 300、LAN-to-LAN の場合は 10 です。また、retry パラメータのデフォルト値は 2 です。

中央サイト（セキュア ゲートウェイ）で、ISAKMP モニタリングを決して開始しないように指定する場合は、次のコマンドを入力します。

```
hostname(config-tunnel-ipsec)# isakmp keepalive threshold infinite
hostname(config-tunnel-ipsec)#
```

ステップ 7　ISAKMP ハイブリッド認証方式、XAUTH またはハイブリッド XAUTH を指定します。

isakmp ikev1-user-authentication コマンドは、ASA 認証にデジタル証明書を使用する必要があり、かつリモート VPN ユーザ認証に RADIUS、TACACS+、または SecurID などのレガシーな方式を別途使用する必要がある場合に、ハイブリッド XAUTH 認証を実装するために使用します。ハイブリッド XAUTH によって、IKE のフェーズ 1 が次の 2 つの手順に分割されます。2 つ合わせてハイブリッド認証と呼ばれます。

a. ASA は、標準の公開キー技術を使用して、リモート VPN ユーザに対して認証します。これにより、単方向に認証する IKE セキュリティ アソシエーションが確立されます。

b. 次に、XAUTH 交換がリモート VPN ユーザを認証します。この拡張認証では、サポートされている従来のいずれかの認証方式を使用できます。

（注）　認証タイプをハイブリッドに設定するには、事前に認証サーバを設定し、事前共有キーを作成し、トラストポイントを設定する必要があります。

isakmp ikev1-user-authentication コマンドとオプションの **interface** パラメータを使用して、特定のインターフェイスを指定できます。**interface** パラメータを省略すると、このコマンドはすべてのインターフェイスに適用され、インターフェイスごとにコマンドが指定されていない場合のバックアップとして機能します。接続プロファイルに 2 つの **isakmp ikev1-user-authentication** コマンドを指定していて、1 つで **interface** パラメータを使用し、もう 1 つで使用しない場合、インターフェイスを指定するコマンドはその特定のインターフェイスを優先します。

たとえば、次のコマンドは、example-group と呼ばれる接続プロファイルの内部インターフェイスでハイブリッド XAUTH をイネーブルにします。

```
hostname(config)# tunnel-group example-group type remote-access
hostname(config)# tunnel-group example-group ipsec-attributes
hostname(config-tunnel-ipsec)# isakmp ikev1-user-authentication (inside) hybrid
hostname(config-tunnel-ipsec)#
```

IPSec リモート アクセス接続プロファイルの PPP 属性の設定

リモート アクセス接続プロファイルのポイントツーポイント プロトコル属性を設定するには、次の手順を実行します。PPP 属性は、IPSec リモート アクセスの接続プロファイルに*だけ*適用されます。次の説明は、IPSec リモート アクセス接続プロファイルをすでに作成していることを前提としています。

ステップ 1　トンネルグループ ppp 属性コンフィギュレーション モードに入ります。このモードで、次のコマンドを入力して、リモート アクセス トンネルグループ PPP 属性を設定します。プロンプトが変化して、モードが変更されたことがわかります。

```
hostname(config)# tunnel-group tunnel-group-name type remote-access
hostname(config)# tunnel-group tunnel-group-name ppp-attributes
hostname(config-tunnel-ppp)#
```

たとえば、次のコマンドは、TG1 という名前の接続プロファイルに関係するトンネルグループ ppp 属性モードのコマンドが続くことを指定しています。プロンプトが変化して、トンネルグループ ppp 属性モードに入ったことがわかります。

```
hostname(config)# tunnel-group TG1 type remote-access
hostname(config)# tunnel-group TG1 ppp-attributes
hostname(config-tunnel-ppp)#
```

ステップ 2　PPP 接続に対する固有のプロトコルを使用する認証をイネーブルにするかどうかを指定します。プロトコルの値は次のいずれかになります。

- pap：PPP 接続で Password Authentication Protocol（パスワード認証プロトコル）の使用をイネーブルにします。
- chap：PPP 接続で Challenge Handshake Authentication Protocol（チャレンジ ハンドシェイク認証プロトコル）の使用をイネーブルにします。
- ms-chap-v1 または ms-chap-v2：PPP 接続で Microsoft Challenge Handshake Authentication Protocol（Microsoft チャレンジ ハンドシェイク認証プロトコル）のバージョン 1 またはバージョン 2 の使用をイネーブルにします。
- eap：PPP 接続で Extensible Authentication Protocol（拡張認証プロトコル）の使用をイネーブルにします。

CHAP と MSCHAPv1 は、デフォルトでイネーブルになっています。

このコマンドの構文は次のとおりです。

```
hostname(config-tunnel-ppp)# authentication protocol
hostname(config-tunnel-ppp)#
```

特定のプロトコルの認証をディセーブルにするには、このコマンドの **no** 形式を使用します。

```
hostname(config-tunnel-ppp)# no authentication protocol
hostname(config-tunnel-ppp)#
```

たとえば、次のコマンドは PPP 接続で PAP プロトコルの使用をイネーブルにします。

```
hostname(config-tunnel-ppp)# authentication pap
hostname(config-tunnel-ppp)#
```

次のコマンドは、PPP 接続で MS-CHAP バージョン 2 プロトコルの使用をイネーブルにします。

```
hostname(config-tunnel-ppp)# authentication ms-chap-v2
hostname(config-tunnel-ppp)#
```

次のコマンドは、PPP 接続で EAP-PROXY プロトコルの使用をイネーブルにします。

```
hostname(config-tunnel-ppp)# authentication pap
hostname(config-tunnel-ppp)#
```

次のコマンドは、PPP 接続で MS-CHAP バージョン 1 プロトコルの使用をディセーブルにします。

```
hostname(config-tunnel-ppp)# no authentication ms-chap-v1
hostname(config-tunnel-ppp)#
```

LAN-to-LAN 接続プロファイルの設定

IPSec LAN-to-LAN VPN 接続プロファイルは、LAN-to-LAN IPSec クライアント接続にだけ適用されます。設定するパラメータの多くは IPSec リモート アクセスの接続プロファイルのものと同じですが、LAN-to-LAN トンネルの方がパラメータの数は少なくなります。ここでは、LAN-to-LAN 接続プロファイルを設定する方法について説明します。

- 「LAN-to-LAN 接続プロファイルの名前とタイプの指定」（P.4-19）
- 「LAN-to-LAN 接続プロファイルの一般属性の設定」（P.4-19）
- 「LAN-to-LAN IPSec IKEv1 属性の設定」（P.4-20）

デフォルトの LAN-to-LAN 接続プロファイルのコンフィギュレーション

デフォルトの LAN-to-LAN 接続プロファイルの内容は、次のとおりです。

```
tunnel-group DefaultL2LGroup type ipsec-l2l
tunnel-group DefaultL2LGroup general-attributes
 no accounting-server-group
 default-group-policy DfltGrpPolicy
tunnel-group DefaultL2LGroup ipsec-attributes
 no ikev1 pre-shared-key
 peer-id-validate req
 no chain
 no ikev1 trust-point
 isakmp keepalive threshold 10 retry 2
```

LAN-to-LAN 接続プロファイルのパラメータはリモート アクセス接続プロファイルのパラメータより少なく、そのほとんどはどちらのグループでも同じです。実際に接続を設定する場合の利便性を考え、ここではこのグループのパラメータを個別に説明します。明示的に設定しないパラメータはすべて、デフォルトの接続プロファイルからその値を継承します。

LAN-to-LAN 接続プロファイルの名前とタイプの指定

接続プロファイルの名前とタイプを指定するには、次のように **tunnel-group** コマンドを入力します。

```
hostname(config)# tunnel-group tunnel_group_name type tunnel_type
```

LAN-to-LAN トンネルの場合、タイプは **ipsec-l2l** になります。たとえば、docs という名前の LAN-to-LAN 接続プロファイルを作成するには、次のコマンドを入力します。

```
hostname(config)# tunnel-group docs type ipsec-l2l
hostname(config)#
```

LAN-to-LAN 接続プロファイルの一般属性の設定

接続プロファイルの一般属性を設定するには、次の手順を実行します。

ステップ 1　シングル コンテキスト モードまたはマルチ コンテキスト モードで general-attributes キーワードを指定して、トンネルグループ一般属性モードを開始します。

```
hostname(config)# tunnel-group_tunnel-group-name general-attributes
hostname(config-tunnel-general)#
```

プロンプトが変化して、config-general モードに入ったことがわかります。トンネルグループの一般属性は、このモードで設定します。

たとえば、docs という名前の接続プロファイルの場合は、次のコマンドを入力します。

```
hostname(config)# tunnel-group_docs general-attributes
hostname(config-tunnel-general)#
```

ステップ 2　アカウンティングサーバ グループがある場合、使用するグループの名前を指定します。

```
hostname(config-tunnel-general)# accounting-server-group groupname
hostname(config-tunnel-general)#
```

たとえば、次のコマンドはアカウンティングサーバ グループ acctgserv1 の使用を指定しています。

```
hostname(config-tunnel-general)# accounting-server-group acctgserv1
hostname(config-tunnel-general)#
```

ステップ 3　デフォルト グループ ポリシーの名前を指定します。

```
hostname(config-tunnel-general)# default-group-policy policyname
hostname(config-tunnel-general)#
```

たとえば、次のコマンドは、デフォルト グループ ポリシーの名前に MyPolicy を指定しています。

```
hostname(config-tunnel-general)# default-group-policy MyPolicy
hostname(config-tunnel-general)#
```

LAN-to-LAN IPSec IKEv1 属性の設定

IPsec IKEv1 属性を設定するには、次の手順を実行します。

ステップ 1　トンネルグループ IPSec IKEv1 属性を設定するには、シングル コンテキスト モードまたはマルチ コンテキスト モードで IPSec-attributes キーワードを指定して tunnel-group コマンドを入力し、トンネルグループ ipsec 属性コンフィギュレーション モードを開始します。

```
hostname(config)# tunnel-group tunnel-group-name ipsec-attributes
hostname(config-tunnel-ipsec)#
```

たとえば、次のコマンドでは、config-ipsec モードを開始し、TG1 という名前の接続プロファイルのパラメータを設定できます。

```
hostname(config)# tunnel-group TG1 ipsec-attributes
hostname(config-tunnel-ipsec)#
```

プロンプトが変化して、トンネルグループ ipsec 属性コンフィギュレーション モードに入ったことがわかります。

ステップ 2　事前共有キーに基づく IKEv1 接続をサポートするために、事前共有キーを指定します。

```
hostname(config-tunnel-ipsec)# ikev1 pre-shared-key key
hostname(config-tunnel-ipsec)#
```

たとえば、次のコマンドは、LAN-to-LAN 接続プロファイルの IKEv1 接続をサポートするために、事前共有キー XYZX を指定しています。

```
hostname(config-tunnel-ipsec)# ikev1 pre-shared-key xyzx
hostname(config-tunnel-general)#
```

ステップ 3　ピアの証明書を使用してピアの ID を検証するかどうかを指定します。

```
hostname(config-tunnel-ipsec)# peer-id-validate option
hostname(config-tunnel-ipsec)#
```

使用できるオプションは、**req**（必須）、**cert**（証明書でサポートされている場合）、**nocheck**（調べない）です。デフォルトは **req** です。たとえば、次のコマンドは、peer-id-validate オプションを **nocheck** に設定しています。

```
hostname(config-tunnel-ipsec)# peer-id-validate nocheck
hostname(config-tunnel-ipsec)#
```

ステップ 4　証明書チェーンを送信できるかどうかを指定します。次のアクションは、ルート証明書とすべての下位 CA 証明書を送信しています。

```
hostname(config-tunnel-ipsec)# chain
hostname(config-tunnel-ipsec)#
```

この属性は、すべてのトンネル グループ タイプに適用できます。

ステップ 5　IKE ピアに送信する証明書を識別するトラストポイントの名前を指定します。

```
hostname(config-tunnel-ipsec)# trust-point trust-point-name
hostname(config-tunnel-ipsec)#
```

たとえば、次のコマンドは、トラストポイント名を mytrustpoint に設定しています。

```
hostname(config-tunnel-ipsec)# trust-point mytrustpoint
hostname(config-tunnel-ipsec)#
```

この属性は、すべてのトンネル グループ タイプに適用できます。

ステップ 6　ISAKMP（IKE）キープアライブのしきい値と許可されるリトライ回数を指定します。**threshold** パラメータでは、ピアがキープアライブ モニタリングを開始するまでの最長アイドル時間を秒数（10 ～ 3600）で指定します。**retry** パラメータは、キープアライブ応答が受信されなくなった後のリトライ間の間隔です（2 ～ 10 秒）。IKE キープアライブは、デフォルトでイネーブルです。IKE キープアライブをディセーブルにするには、**isakmp** コマンドの **no** 形式を入力します。

```
hostname(config)# isakmp keepalive threshold <number> retry <number>
hostname(config-tunnel-ipsec)#
```

たとえば、次のコマンドは、ISAKMP キープアライブのしきい値を 15 秒に設定し、リトライ インターバルを 10 秒に設定します。

```
hostname(config-tunnel-ipsec)# isakmp keepalive threshold 15 retry 10
hostname(config-tunnel-ipsec)#
```

threshold パラメータのデフォルト値は、LAN-to-LAN の場合は 10 です。retry パラメータのデフォルト値は 2 です。

中央サイト（セキュア ゲートウェイ）で、ISAKMP モニタリングを決して開始しないように指定する場合は、次のコマンドを入力します。

```
hostname(config-tunnel-ipsec)# isakmp keepalive threshold infinite
hostname(config-tunnel-ipsec)#
```

ステップ 7　ISAKMP ハイブリッド認証方式、XAUTH またはハイブリッド XAUTH を指定します。

isakmp ikev1-user-authentication コマンドは、ASA 認証にデジタル証明書を使用する必要があり、かつリモート VPN ユーザ認証に RADIUS、TACACS+、または SecurID などのレガシーな方式を別途使用する必要がある場合に、ハイブリッド XAUTH 認証を実装するために使用します。ハイブリッド XAUTH によって、IKE のフェーズ 1 が次の 2 つの手順に分割されます。2 つ合わせてハイブリッド認証と呼ばれます。

a. ASA は、標準の公開キー技術を使用して、リモート VPN ユーザに対して認証します。これにより、単方向に認証する IKE セキュリティ アソシエーションが確立されます。

b. 次に、XAUTH 交換がリモート VPN ユーザを認証します。この拡張認証では、サポートされている従来のいずれかの認証方式を使用できます。

（注）　認証タイプをハイブリッドに設定するには、事前に認証サーバを設定し、事前共有キーを作成し、トラストポイントを設定する必要があります。

たとえば、次のコマンドは、example-group と呼ばれる接続プロファイルのハイブリッド XAUTH をイネーブルにします。

```
hostname(config)# tunnel-group example-group type remote-access
hostname(config)# tunnel-group example-group ipsec-attributes
hostname(config-tunnel-ipsec)# isakmp ikev1-user-authentication hybrid
hostname(config-tunnel-ipsec)#
```

クライアントレス SSL VPN セッションの接続プロファイルの設定

クライアントレス SSL VPN 接続プロファイル用のトンネルグループ一般属性は、トンネルグループのタイプが webvpn で、**strip-group** コマンドと **strip-realm** コマンドが適用されない点を除いて、IPSec リモート アクセスの接続プロファイルのものと同じです。クライアントレス SSL VPN に固有の属性は別々に定義します。次の項では、クライアントレス SSL VPN 接続プロファイルを設定する方法について説明します。

- 「クライアントレス SSL VPN セッションの一般トンネルグループ属性の設定」（P.4-22）
- 「クライアントレス SSL VPN セッションのトンネルグループ属性の設定」（P.4-25）

クライアントレス SSL VPN セッションの一般トンネルグループ属性の設定

接続プロファイルの一般属性を設定または変更するには、次の手順でパラメータを指定します。

ステップ 1　一般属性を設定するには、シングル コンテキスト モードまたはマルチ コンテキスト モードで **tunnel-group general-attributes** コマンドを入力します。これで、トンネルグループ一般属性コンフィギュレーション モードが開始されます。プロンプトが変化することに注意してください。

```
hostname(config)# tunnel-group tunnel_group_name general-attributes
hostname(config-tunnel-general)#
```

前の項で作成した TunnelGroup3 の一般属性を設定するには、次のコマンドを入力します。

```
hostname(config)# tunnel-group TunnelGroup3 general-attributes
hostname(config-tunnel-general)#
```

ステップ 2　認証サーバ グループがある場合、使用するグループの名前を指定します。指定したサーバ グループに障害が発生したときにローカル データベースを認証に使用する場合は、キーワード LOCAL を追加します。

```
hostname(config-tunnel-general)# authentication-server-group groupname [LOCAL]
hostname(config-tunnel-general)#
```

たとえば、test という名前の認証サーバ グループを設定し、認証サーバ グループで障害が発生したときにローカル サーバにフォールバックするようにするには、次のコマンドを入力します。

```
hostname(config-tunnel-general)# authentication-server-group test LOCAL
hostname(config-tunnel-general)#
```

authentication-server-group 名で、事前に設定した認証サーバまたはサーバのグループを指定します。認証サーバを設定するには、**aaa-server** コマンドを使用します。グループ タグの最大長は 16 文字です。

グループ名の前にある丸カッコ内にインターフェイス名を指定することにより、インターフェイス固有の認証を設定することもできます。次のインターフェイスはデフォルトで使用可能になっています。

- inside：インターフェイス GigabitEthernet0/1 の名前
- outside：インターフェイス GigabitEthernet0/0 の名前

（注）　ASA の外部インターフェイス アドレス（IPv4 と IPv6 の両方）は、プライベート側のアドレス空間と重複していてはなりません。

interface コマンドを使用して設定したその他のインターフェイスも使用可能です。次のコマンドは、認証にサーバ servergroup1 を使用する outside という名前のインターフェイスのインターフェイス固有の認証を設定しています。

```
hostname(config-tunnel-general)# authentication-server-group (outside) servergroup1
hostname(config-tunnel-general)#
```

ステップ 3　オプションで、使用する認可サーバ グループの名前を指定します（存在する場合）。認可を使用していない場合は、ステップ 6 に進んでください。この値を設定する場合、ユーザは接続する認可データベースに存在する必要があります。

```
hostname(config-tunnel-general)# authorization-server-group groupname
hostname(config-tunnel-general)#
```

認可サーバを設定するには、**aaa-server** コマンドを使用します。グループ タグの最大長は 16 文字です。

たとえば、次のコマンドは、認可サーバ グループ FinGroup を使用することを指定しています。

```
hostname(config-tunnel-general)# authorization-server-group FinGroup
hostname(config-tunnel-general)#
```

ステップ 4　ユーザに接続を許可する前に、そのユーザが正常に認可されている必要があるかどうかを指定します。デフォルトでは認可は要求されません。

```
hostname(config-tunnel-general)# authorization-required
hostname(config-tunnel-general)#
```

ステップ 5　証明書から認可クエリー用の名前を得るために使用する 1 つまたは複数の属性を指定します。この属性により、サブジェクト DN フィールドのどの部分を認可用のユーザ名として使用するかが指定されます。

```
hostname(config-tunnel-general)# authorization-dn-attributes {primary-attribute
[secondary-attribute] | use-entire-name}
```

たとえば、次のコマンドは、CN 属性を認可用のユーザ名として使用することを指定しています。

```
hostname(config-tunnel-general)# authorization-dn-attributes CN
hostname(config-tunnel-general)#
```

authorization-dn-attributes は、**C**（国）、**CN**（通常名）、**DNQ**（DN 修飾子）、**EA**（電子メール アドレス）、**GENQ**（世代修飾子）、**GN**（名）、**I**（イニシャル）、**L**（地名）、**N**（名前）、**O**（組織）、**OU**（組織ユニット）、**SER**（シリアル番号）、**SN**（姓）、**SP**（州または都道府県）、**T**（役職）、**UID**（ユーザ ID）、および **UPN**（ユーザ プリンシパル ネーム）があります。

ステップ 6　オプションで、使用するアカウンティング サーバ グループの名前を指定します（存在する場合）。アカウンティングを使用していない場合は、ステップ 7 に進んでください。アカウンティング サーバを設定するには、**aaa-server** コマンドを使用します。グループ タグの最大長は 16 文字です。

```
hostname(config-tunnel-general)# accounting-server-group groupname
hostname(config-tunnel-general)#
```

たとえば、次のコマンドは、アカウンティング サーバ グループ comptroller を使用することを指定しています。

```
hostname(config-tunnel-general)# accounting-server-group comptroller
hostname(config-tunnel-general)#
```

ステップ 7　オプションで、デフォルト グループ ポリシーの名前を指定します。デフォルト値は DfltGrpPolicy です。

```
hostname(config-tunnel-general)# default-group-policy policyname
hostname(config-tunnel-general)#
```

次の例では、デフォルト グループ ポリシーの名前として MyDfltGrpPolicy を設定しています。

```
hostname(config-tunnel-general)# default-group-policy MyDfltGrpPolicy
hostname(config-tunnel-general)#
```

ステップ 8　オプションで、DHCP サーバ（最大 10 サーバ）の名前または IP アドレス、および DHCP アドレス プール（最大 6 プール）の名前を指定します。リスト項目はスペースで区切ります。デフォルトでは、DHCP サーバとアドレス プールは使用されません。

```
hostname(config-tunnel-general)# dhcp-server server1 [...server10]
hostname(config-tunnel-general)# address-pool [(interface name)] address_pool1
[...address_pool6]
hostname(config-tunnel-general)#
```

（注）　インターフェイス名は丸カッコで囲む必要があります。

アドレス プールは、グローバル コンフィギュレーション モードで **ip local pool** コマンドを使用して設定します。アドレス プールの設定の詳細については、第 5 章「VPN の IP アドレス」を参照してください。

ステップ 9　サーバが RADIUS、RADIUS with NT、または LDAP サーバの場合、オプションで、パスワード管理をイネーブルにできます。

（注）　認証に LDAP ディレクトリ サーバを使用している場合、パスワード管理は Sun Microsystems JAVA System Directory Server（旧名称は Sun ONE Directory Server）および Microsoft Active Directory を使用してサポートされます。

- Sun：Sun ディレクトリ サーバにアクセスするために ASA に設定されている DN は、そのサーバ上のデフォルト パスワード ポリシーにアクセスできる必要があります。DN として、ディレクトリ管理者、またはディレクトリ管理者権限を持つユーザを使用することを推奨します。または、デフォルト パスワード ポリシーに ACI を設定できます。
- Microsoft：Microsoft Active Directory を使用したパスワード管理をイネーブルにするには、LDAP over SSL を設定する必要があります。

この機能はデフォルトでイネーブルになっており、現在のパスワードの有効期限が近づくとユーザに警告を表示します。デフォルトでは、期限切れの 14 日前に警告が開始されます。

```
hostname(config-tunnel-general)# password-management
hostname(config-tunnel-general)#
```

サーバが LDAP サーバの場合、有効期限が近いことに関する警告が開始されるまでの日数（0 ～ 180）を指定できます。

```
hostname(config-tunnel-general)# password-management [password-expire in days n]
hostname(config-tunnel-general)#
```

（注）　トンネルグループ一般属性コンフィギュレーション モードで入力した **password-management** コマンドによって、トンネルグループ ipsec 属性モードで事前に入力された非推奨の **radius-with-expiry** コマンドが置き換えられます。

このコマンドを設定すると、リモート ユーザがログインするときに、ASA は、ユーザの現在のパスワードの有効期限が近づいていること、または期限が切れていることを通知します。それから ASA は、ユーザがパスワードを変更できるようにします。現行のパスワードが失効していない場合、ユーザはそのパスワードを使用してログインし続けることができます。RADIUS または LDAP 認証が設定されていない場合、ASA ではこのコマンドが無視されます。

これによってパスワードが期限切れになるまでの日数が変更されるわけではなく、ASA がパスワードが期限切れになる何日前にユーザへの警告を開始するかが変更されるという点に注意してください。

password-expire-in-days キーワードを指定する場合は、日数も指定する必要があります。

詳細については、「パスワード管理用の Microsoft Active Directory の設定」（P.4-31）を参照してください。

ステップ 10　このコマンドで日数に 0 を指定すると、このコマンドはディセーブルになります。ASA は、期限切れが近いことをユーザに通知しませんが、ユーザは期限切れ後にパスワードを変更できます。オプションで、**override-account-disable** コマンドを入力して、AAA サーバからの account-disabled インジケータを上書きする機能を設定できます。

```
hostname(config-tunnel-general)# override-account-disable
hostname(config-tunnel-general)#
```

（注）　override account-disabled を許可することは、潜在的なセキュリティ リスクとなります。

クライアントレス SSL VPN セッションのトンネルグループ属性の設定

クライアントレス SSL VPN 接続プロファイルに固有のパラメータを設定するには、この項の次の手順を実行します。クライアントレス SSL VPN は、以前は WebVPN として知られていました。これらの属性は、トンネルグループ webvpn 属性モードで設定します。

ステップ 1　クライアントレス SSL VPN トンネルグループの属性を指定するには、次のコマンドを入力してトンネルグループ webvpn 属性モードに入ります。プロンプトが変化して、モードが変更されたことがわかります。

```
hostname(config)# tunnel-group tunnel-group-name webvpn-attributes
hostname(config-tunnel-ipsec)#
```

たとえば、sales という名前のクライアントレス SSL VPN トンネルグループの webvpn 属性を指定するには、次のコマンドを入力します。

```
hostname(config)# tunnel-group sales webvpn-attributes
hostname(config-tunnel-webvpn)#
```

ステップ 2　AAA、デジタル証明書、または両方を使用するための認証方式を指定するには、**authentication** コマンドを入力します。AAA、証明書、または両方を任意の順序で指定できます。

```
hostname(config-tunnel-webvpn)# authentication authentication_method
hostname(config-tunnel-webvpn)#
```

たとえば、次のコマンドは AAA と証明書の両方の認証を許可します。

```
hostname(config-tunnel-webvpn)# authentication aaa certificate
hostname(config-tunnel-webvpn)#
```

カスタマイゼーションの適用

カスタマイゼーションによって、ログイン時にユーザに表示されるウィンドウの外観が決まります。カスタマイゼーション パラメータは、クライアントレス SSL VPN の設定の一部として設定します。

ログイン時にユーザに表示される Web ページのルックアンドフィールを変更するために、事前に定義した Web ページ カスタマイゼーションを適用するには、ユーザ名 webvpn コンフィギュレーション モードで customization コマンドを入力します。

```
hostname(config-username-webvpn)# customization {none | value customization_name}
hostname(config-username-webvpn)#
```

たとえば、blueborder という名前のカスタマイゼーションを使用するには、次のコマンドを入力します。

```
hostname(config-username-webvpn)# customization value blueborder
hostname(config-username-webvpn)#
```

カスタマイゼーション自体は、webvpn モードで **customization** コマンドを入力して設定します。

次の例は、「123」という名前のカスタマイゼーションを最初に確立するコマンド シーケンスを示しています。このコマンド シーケンスによって、パスワード プロンプトが定義されます。この例では、「test」という名前のクライアントレス SSL VPN トンネルグループを定義して、**customization** コマンドを使用し、「123」という名前のカスタマイゼーションを使用することを指定しています。

```
hostname(config)# webvpn
hostname(config-webvpn)# customization 123
hostname(config-webvpn-custom)# password-prompt Enter password
hostname(config-webvpn)# exit
hostname(config)# tunnel-group test type webvpn
hostname(config)# tunnel-group test webvpn-attributes
hostname(config-tunnel-webvpn)# customization value 123
hostname(config-tunnel-webvpn)#
```

ステップ 3　ASA は、NetBIOS 名を IP アドレスにマップするために NetBIOS ネーム サーバにクエリーを送信します。クライアントレス SSL VPN では、リモート システムのファイルをアクセスまたは共有するための NetBIOS が必要です。クライアントレス SSL VPN では、NetBIOS と CIFS プロトコルを使用して、リモート システムのファイルをアクセスまたは共有します。Windows コンピュータにそのコンピュータ名を使用してファイル共有接続をしようとすると、指定されたファイル サーバはネットワーク上のリソースを識別する特定の NetBIOS 名と対応します。

NBNS 機能を動作させるには、少なくとも 1 台の NetBIOS サーバ（ホスト）を設定する必要があります。冗長性を実現するために NBNS サーバを 3 つまで設定できます。ASA は、リストの最初のサーバを NetBIOS/CIFS 名前解決に使用します。クエリーが失敗すると、次のサーバが使用されます。

CIFS 名前解決に使用する NBNS（NetBIOS ネーム サービス）サーバの名前を指定するには、**nbns-server** コマンドを使用します。サーバ エントリは 3 つまで入力できます。冗長性のために、設定する最初のサーバはプライマリ サーバで、その他のサーバはバックアップです。これが（ただの WINS サーバではなく）マスター ブラウザであるかどうか、タイムアウト間隔、およびリトライ回数も指定できます。WINS サーバまたはマスター ブラウザは、通常、ASA と同じネットワーク上か、そのネットワークから到達可能な場所に設定されます。タイムアウト間隔はリトライ回数の前に指定する必要があります。

```
hostname(config-tunnel-webvpn)# nbns-server {host-name | IP_address} [master]
[timeout seconds] [retry number]
hostname(config-tunnel-webvpn)#
```

たとえば、nbnsprimary という名前のサーバをプライマリ サーバとして設定し、サーバ 192.168.2.2 をセカンダリ サーバとして設定し、それぞれに 3 回のリトライを許可し、5 秒のタイムアウトを設定するには、次のコマンドを入力します。

```
hostname(config)# name 192.168.2.1 nbnsprimary
hostname(config-tunnel-webvpn)# nbns-server nbnsprimary master timeout 5 retry 3
hostname(config-tunnel-webvpn)# nbns-server 192.168.2.2 timeout 5 retry 3
hostname(config-tunnel-webvpn)#
```

タイムアウト間隔の範囲は 1 ～ 30 秒（デフォルトは 2）、リトライ回数は 0 ～ 10（デフォルトは 2）です。

トンネルグループ webvpn 属性コンフィギュレーション モードで **nbns-server** コマンドを使用すると、webvpn コンフィギュレーション モードで非推奨の **nbns-server** コマンドが置き換えられます。

ステップ 4　グループの代替名を指定するには、**group-alias** コマンドを使用します。グループ エイリアスを指定すると、ユーザがトンネルグループを参照できる 1 つ以上の代替名が作成されます。ここで指定するグループ エイリアスは、ユーザのログイン ページにあるドロップダウン リストに表示されます。各グループに対して複数のエイリアスを指定することも、エイリアスを指定しないこともできます。それぞれを別のコマンドで指定します。この機能は、同じグループが「Devtest」や「QA」などの複数の通常名で指定されている場合に便利です。

各グループ エイリアスに対して、**group-alias** コマンドを入力します。各エイリアスはデフォルトでイネーブルになっています。各エイリアスは、オプションで明示的にイネーブルまたはディセーブルにできます。

```
hostname(config-tunnel-webvpn)# group-alias alias [enable | disable]
hostname(config-tunnel-webvpn)#
```

たとえば、QA という名前のトンネルグループのエイリアスの QA と Devtest をイネーブルにするには、次のコマンドを入力します。

```
hostname(config-tunnel-webvpn)# group-alias QA enable
hostname(config-tunnel-webvpn)# group-alias Devtest enable
hostname(config-tunnel-webvpn)#
```

（注）　webvpn tunnel-group-list は、表示する（ドロップダウン）グループ リストに対してイネーブルにする必要があります。

ステップ 5　グループの着信 URL または IP アドレスを指定するには、**group-url** コマンドを使用します。グループの URL または IP アドレスを指定すると、ユーザがログイン時にグループを選択する必要がなくなります。ユーザがログインすると、ASA は、tunnel-group-policy テーブル内のユーザの着信 URL またはアドレスを検索します。URL またはアドレスが見つかり、group-url が接続プロファイル内でイネーブルになっている場合、ASA は、関連の接続プロファイルを自動的に選択して、ログイン ウィンドウにユーザ名フィールドとパスワード フィールドだけを表示します。これによりユーザ インターフェイスが簡素化され、グループ リストがユーザに表示されなくなるという利点が追加されます。ユーザに表示するログイン ウィンドウには、その接続プロファイル用に設定されたカスタマイゼーションが使用されます。

URL またはアドレスがディセーブルになっており、group-alias が設定されている場合、グループのドロップダウン リストも表示され、ユーザは選択を行う必要があります。

1 つのグループに対して複数の URL またはアドレスを設定できます（何も設定しないこともできます）。各 URL またはアドレスは、個別にイネーブルまたはディセーブルにできます。指定した各 URL またはアドレスに対しては、別々の **group-url** コマンドを使用する必要があります。http または https プロトコルを含め、URL またはアドレス全体を指定する必要があります。

同じ URL またはアドレスを複数のグループに関連付けることはできません。ASA は、接続プロファイルの URL またはアドレスを受け入れる前にその URL またはアドレスの固有性を検証します。

各グループ URL またはアドレスに対して、**group-url** コマンドを入力します。各 URL またはエイリアスは、オプションで明示的にイネーブル（デフォルト）またはディセーブルにできます。

```
hostname(config-tunnel-webvpn)# group-url url [enable | disable]
hostname(config-tunnel-webvpn)#
```

url は、このトンネル グループの URL または IP アドレスを指定します。

たとえば、RadiusServer という名前のトンネルグループに対してグループ URL http://www.example.com と http://192.168.10.10 をイネーブルにするには、次のコマンドを入力します。

```
hostname(config)# tunnel-group RadiusServer type webvpn
hostname(config)# tunnel-group RadiusServer general-attributes
hostname(config-tunnel-general)# authentication server-group RADIUS
hostname(config-tunnel-general)# accounting-server-group RADIUS
hostname(config-tunnel-general)# tunnel-group RadiusServer webvpn-attributes
hostname(config-tunnel-webvpn)# group-alias “Cisco Remote Access” enable
hostname(config-tunnel-webvpn)# group-url http://www.example.com enable
hostname(config-tunnel-webvpn)# group-url http://192.168.10.10 enable
hostname(config-tunnel-webvpn)#
```

多数の例については、「クライアントレス SSL VPN セッションのユーザ用ログイン ウィンドウのカスタマイズ」（P.4-30）を参照してください。

ステップ 6　グループ URL のいずれかを入力した場合に、接続プロファイルごとに実行中の Cisco Secure Desktop から特定のユーザを免除するには、次のコマンドを入力します。

```
hostname(config-tunnel-webvpn)# without-csd
hostname(config-tunnel-webvpn)#
```

（注）　このコマンドを入力すると、これらのセッションのエンドポイント状態が検出されないため、ダイナミック アクセス ポリシー（DAP）コンフィギュレーションを調整する必要があります。

ステップ 7　クライアントレス SSL VPN セッションの接続プロファイルに使用する DNS サーバ グループを指定するには、**dns-group** コマンドを使用します。指定するグループは、グローバル コンフィギュレーション モードで（**dns server-group** コマンドおよび **name-server** コマンドを使用して）設定済みのグループである必要があります。

デフォルトでは、接続プロファイルは DNS サーバ グループ *DefaultDNS* を使用します。ただし、セキュリティ アプライアンスで DNS 要求を解決する前にこのグループを設定する必要があります。

次の例は、*corp_dns* という名前の新規 DNS サーバ グループを設定し、接続プロファイル *telecommuters* のサーバ グループを指定します。

```
hostname(config)# dns server-group corp_dns
hostname(config-dns-server-group)# domain-name cisco.com
hostname(config-dns-server-group)# name-server 209.165.200.224

hostname(config)# tunnel-group telecommuters webvpn-attributes
hostname(config-tunnel-webvpn)# dns-group corp_dns
hostname(config-tunnel-webvpn)#
```

ステップ 8　（オプション）認証および認可で使用するためにクライアント証明書からユーザ名を抽出するには、トンネルグループ webvpn 属性モードで **pre-fill-username** コマンドを使用します。デフォルト値はありません。

```
hostname(config)# pre-fill-username {ssl-client | clientless}
```

pre-fill-username コマンドは、ユーザ名 / パスワードの認証および認可のユーザ名として、**username-from-certificate** コマンド（トンネルグループ一般属性モード）で指定した証明書フィールドから抽出されるユーザ名の使用をイネーブルにします。この、証明書からユーザ名を事前に入力する機能を使用するには、両方のコマンドを設定する必要があります。

（注）　バージョン 8.0.4 では、ユーザ名は事前に入力されません。ユーザ名フィールド内の送信されたデータは無視されます。

次の例では、グローバル コンフィギュレーション モードで入力された、remotegrp という名前の IPSec リモート アクセス トンネル グループを作成し、証明書からのユーザ名の取得をイネーブルにして、SSL VPN クライアント認証または許可のクエリーのための名前がデジタル証明書から派生している必要があることを指定します。

```
hostname(config)# tunnel-group remotegrp type ipsec_ra
hostname(config)# tunnel-group remotegrp general-attributes
hostname(config-tunnel-general)# username-from-certificate CN OU
hostname(config)# tunnel-group remotegrp webvpn-attributes
hostname(config-tunnel-webvpn)# pre-fill-username ssl-client
hostname(config-tunnel-webvpn)#
```

ステップ 9　（オプション）AnyConnect または SSL VPN クライアントをダウンロードするためにグループ ポリシーまたはユーザ名属性コンフィギュレーションを上書きするかどうかを指定するには、**override-svc-download** コマンドを使用します。この機能はデフォルトで無効に設定されています。

セキュリティ アプライアンスは、**vpn-tunnel-protocol** コマンドによってグループ ポリシーまたはユーザ名属性でクライアントレスや SSL VPN がイネーブルになっているかどうかに基づいて、リモート ユーザに対してクライアントレス接続または AnyConnect クライアント接続を許可します。**anyconnect ask** コマンドはさらに、クライアントをダウンロードするか、または WebVPN ホームページに戻るようにユーザに要求して、クライアントのユーザ エクスペリエンスを変更します。

ただし、特定のトンネルグループでログインしているクライアントレス ユーザには、ダウンロード プロンプトが終了するまで待たせることなく、クライアントレス SSL VPN ホームページを表示することができます。**override-svc-download** コマンドを使用すると、接続プロファイル レベルでこのようなユーザに対する遅延を防止できます。このコマンドにより、接続プロファイル経由でログインするユーザには、**vpn-tunnel-protocol** コマンドまたは **anyconnect ask** コマンドの設定に関係なく、ただちにクライアントレス SSL VPN ホームページが表示されるようになります。

次の例では、接続プロファイル *engineering* のトンネルグループ webvpn 属性コンフィギュレーション モードに入り、クライアント ダウンロード プロンプトのグループ ポリシーとユーザ名属性設定を上書きする接続プロファイルをイネーブルにします。

```
hostname(config)# tunnel-group engineering webvpn-attributes
hostname(config-tunnel-webvpn)# override-svc-download
```

ステップ 10　（オプション）認証が拒否されたときのログイン画面への RADIUS 拒否メッセージの表示をイネーブルにするには、**radius-eject-message** コマンドを使用します。

次に、engineering という名前の接続プロファイルに対して RADIUS 拒否メッセージの表示をイネーブルにする例を示します。

```
hostname(config)# tunnel-group engineering webvpn-attributes
hostname(config-tunnel-webvpn)# radius-reject-message
```

クライアントレス SSL VPN セッションのユーザ用ログイン ウィンドウのカスタマイズ

カスタマイゼーション プロファイルと接続プロファイルの組み合わせを使用することで、さまざまなグループに対して異なるログイン ウィンドウをセットアップできます。たとえば、salesgui と呼ばれるカスタマイゼーション プロファイルを作成してある場合、そのカスタマイゼーション プロファイルを使用する sales と呼ばれるクライアントレス SSL VPN セッション用の接続プロファイルを、次のように作成できます。

ステップ 1　webvpn モードで、クライアントレス SSL VPN アクセスのカスタマイゼーションを定義します。この場合は、salesgui という名前で、デフォルトのロゴを mycompanylogo.gif に変更します。mycompanylogo.gif を ASA のフラッシュ メモリに事前にロードし、設定を保存している必要があります。詳細については、第 13 章「クライアントレス SSL VPN の概要」を参照してください。

```
hostname# webvpn
hostname (config-webvpn)# customization value salesgui
hostname(config-webvpn-custom)# logo file disk0:\mycompanylogo.gif
hostname(config-webvpn-custom)#
```

ステップ 2　グローバル コンフィギュレーション モードで、ユーザ名をセットアップし、先ほど定義したクライアントレス SSL VPN 用のカスタマイゼーションと関連付けます。

```
hostname# username seller attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# customization value salesgui
hostname(config-username-webvpn)# exit
hostname(config-username)# exit
hostname#
```

ステップ 3　グローバル コンフィギュレーション モードで、sales という名前のクライアントレス SSL VPN セッションのトンネルグループを作成します。

```
hostname# tunnel-group sales type webvpn
hostname(config-tunnel-webvpn)#
```

ステップ 4　この接続プロファイルに対して salesgui カスタマイゼーションを使用することを指定します。

```
hostname# tunnel-group sales webvpn-attributes
hostname(config-tunnel-webvpn)# customization salesgui
```

ステップ 5　ASA にログインするためにユーザがブラウザに入力するアドレスに対するグループ URL を設定します。たとえば、ASA に IP アドレス 192.168.3.3 が設定されている場合は、グループ URL を https://192.168.3.3 に設定します。

```
hostname(config-tunnel-webvpn)# group-url https://192.168.3.3.
hostname(config-tunnel-webvpn)#
```

ログインを成功させるためにポート番号が必要な場合は、コロンに続けてポート番号を指定します。ASA は、この URL を sales 接続プロファイルにマッピングし、ユーザが https://192.168.3.3 にログインしたときに表示されるログイン画面に salesgui カスタマイゼーション プロファイルを適用します。

パスワード管理用の Microsoft Active Directory の設定

（注）　認証に LDAP ディレクトリ サーバを使用している場合、パスワード管理は Sun Microsystems JAVA System Directory Server（旧名称は Sun ONE Directory Server）および Microsoft Active Directory を使用してサポートされます。

- Sun：Sun ディレクトリ サーバにアクセスするために ASA に設定されている DN は、そのサーバ上のデフォルト パスワード ポリシーにアクセスできる必要があります。DN として、ディレクトリ管理者、またはディレクトリ管理者権限を持つユーザを使用することを推奨します。または、デフォルト パスワード ポリシーに ACI を設定できます。
- Microsoft：Microsoft Active Directory を使用したパスワード管理をイネーブルにするには、LDAP over SSL を設定する必要があります。

Microsoft Active Directory でパスワード管理を使用するには、一定の Active Directory パラメータを設定し、ASA でパスワード管理を設定する必要があります。この項では、さまざまなパスワード管理アクションに関連する Active Directory の設定について説明します。これらの説明は、ASA でのパスワード管理がイネーブルになっていて、対応するパスワード管理属性が設定されていることを前提としています。この項の特定の手順では、Windows 2000 における Active Directory の用語に言及し、次の項目を取り上げます。

- 「次回ログイン時にパスワードの変更をユーザに強制するための Active Directory の使用」（P.4-32）
- 「Active Directory を使用したパスワードの最大有効日数の指定」（P.4-33）
- 「Active Directory を使用した Account Disabled AAA インジケータの上書き」（P.4-34）
- 「Active Directory を使用したパスワードの複雑性の強制」（P.4-36）

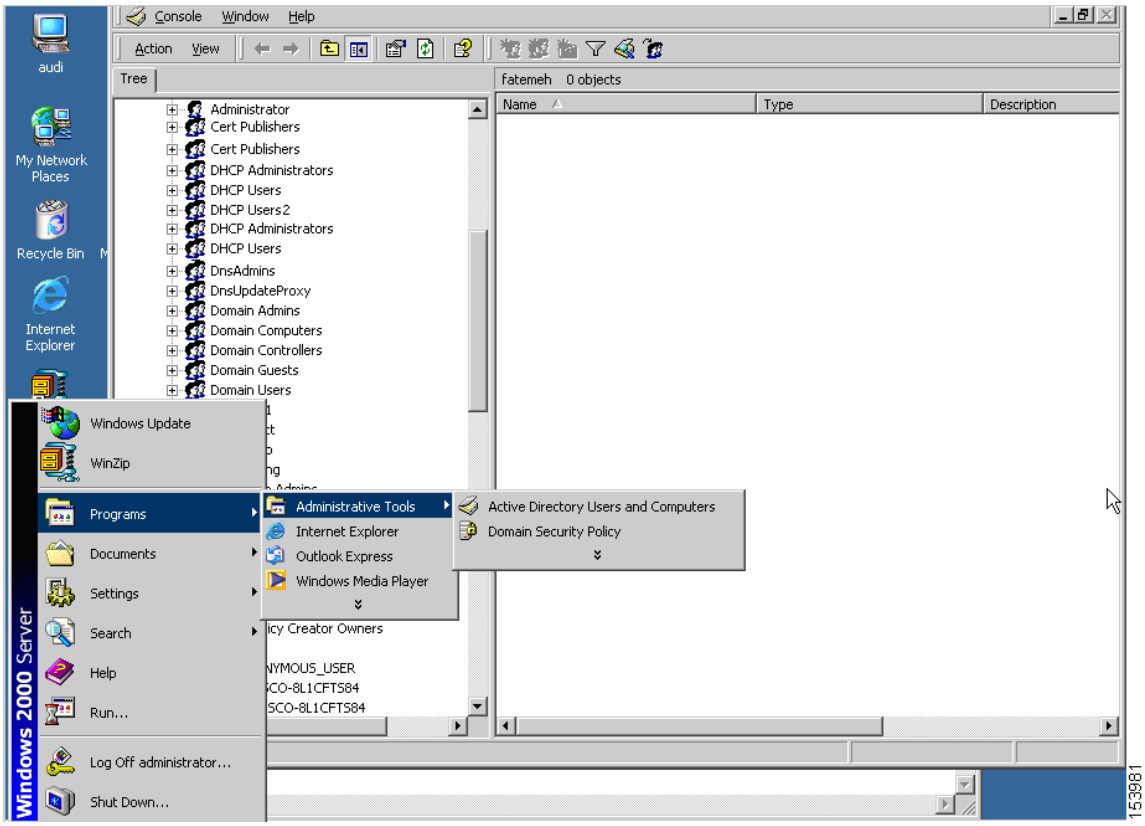
この項では、認証に LDAP ディレクトリ サーバを使用していることを前提としています。

次回ログイン時にパスワードの変更をユーザに強制するための Active Directory の使用

次回ログイン時にユーザ パスワードの変更をユーザに強制するには、ASA のトンネルグループ一般属性コンフィギュレーション モードで **password-management** コマンドを指定して、Active Directory で次の手順を実行します。

ステップ 1　[Start] > [Programs] > [Administrative Tools] > [Active Directory Users and Computers] を選択します（図 4-1）。

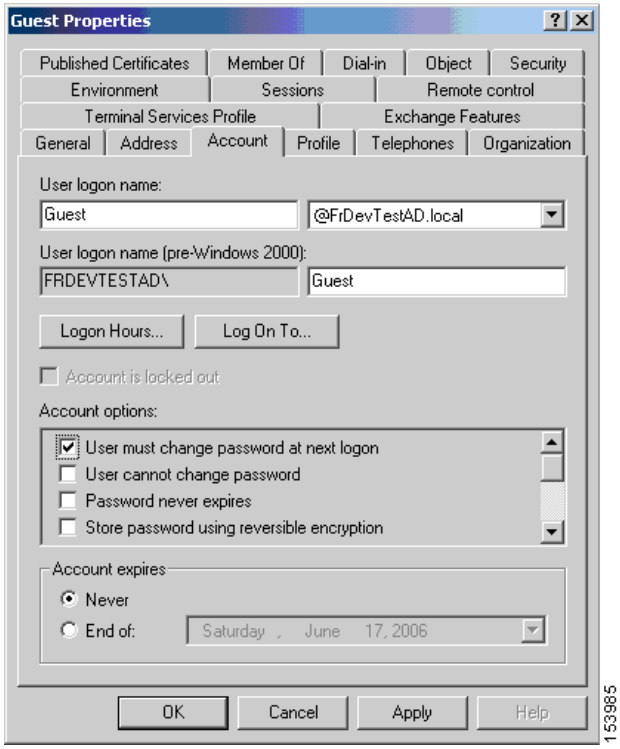
図 4-1　Active Directory：[Administrative Tools] メニュー



ステップ 2　右クリックして、[Username] > [Properties] > [Account] を選択します。

ステップ 3　[User must change password at next logon] チェックボックスをオンにします（図 4-2）。

図 4-2　　Active Directory：ログイン時のパスワード変更要求



このユーザが次回ログインするときに、ASA で「New password required.Password change required. You must enter a new password with a minimum length *n* to continue.」というプロンプトが表示されます。[Start] > [Programs] > [Administrative Tools] > [Domain Security Policy] > [Windows Settings] > [Security Settings] > [Account Policies] > [Password Policy] を選択し、Active Directory 設定の一部として、パスワードの最小の長さ *n* を設定できます。[Minimum password length] パスワードの最小の長さを選択します。

Active Directory を使用したパスワードの最大有効日数の指定

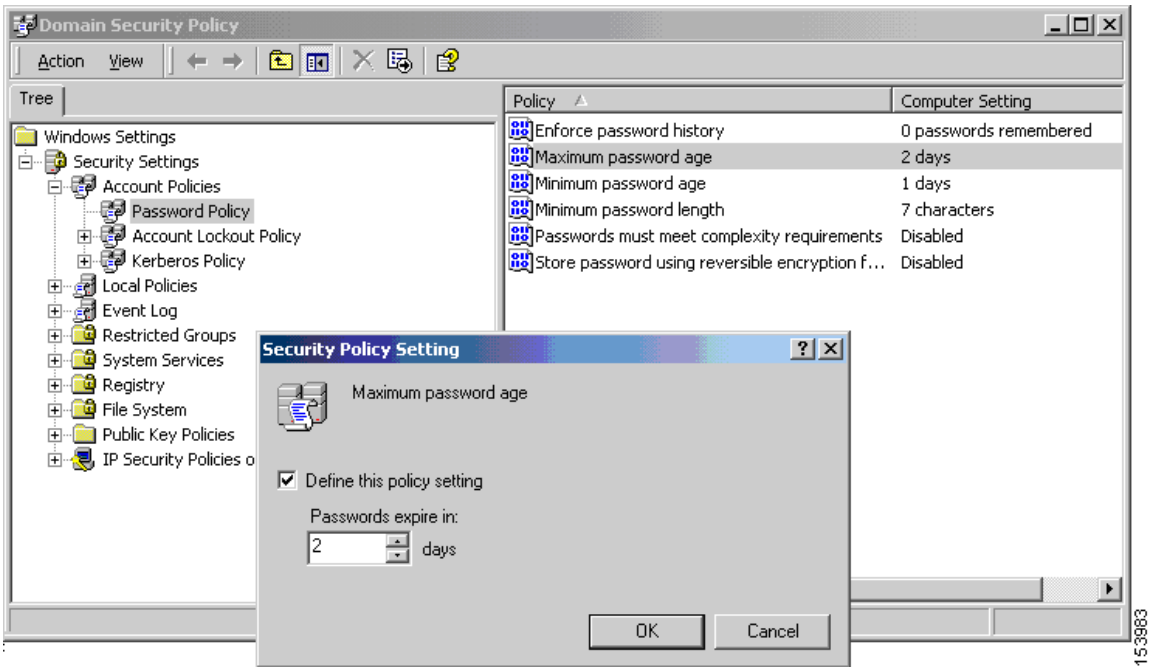
セキュリティを強化するために、一定の日数経過後パスワードが期限切れになるように指定できます。ユーザ パスワードの最大有効日数を指定するには、ASA のトンネルグループ一般属性コンフィギュレーション モードで **password-management** コマンドを指定し、Active Directory で次の手順を実行します。

ステップ 1　[Start] > [Programs] > [Administrative Tools] > [Domain Security Policy] > [Windows Settings] > [Security Settings] > [Account Policies] > [Password Policy] を選択します。

ステップ 2　[Maximum password age] をダブルクリックします。[Security Policy Setting] ダイアログボックスが表示されます。

ステップ 3　[Define this policy setting] チェックボックスをオンにして、許可する [Maximum password age] を日単位で指定します。

図 4-3　　Active Directory：パスワードの最大有効日数



（注）　以前、パスワードの有効日数の設定機能を実行するためにトンネルグループ リモート アクセス コンフィギュレーションの一部として設定されていた **radius-with-expiry** コマンドは非推奨になっています。このコマンドは、トンネルグループ一般属性モードで入力される **password-management** コマンドに置き換えられます。

Active Directory を使用した Account Disabled AAA インジケータの上書き

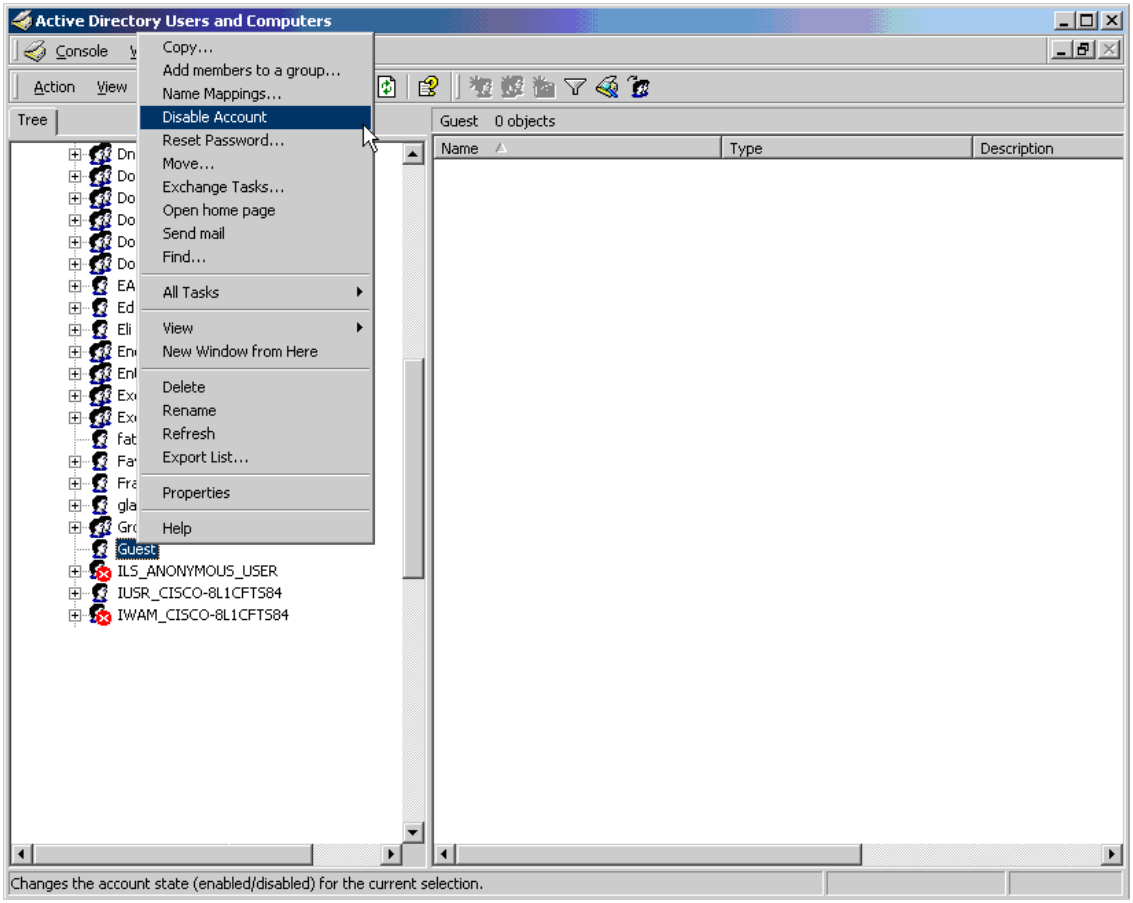
AAA サーバからの account-disabled 表示を上書きするには、ASA のトンネルグループ一般属性コンフィギュレーション モードで **override-account-disable** コマンドを使用し、Active Directory で次の手順を実行します。

（注）　override account-disabled を許可することは、潜在的なセキュリティ リスクとなります。

ステップ 1　[Start] > [Programs] > [Administrative Tools] > [Active Directory Users and Computers] を選択します。

ステップ 2　[Username] > [Properties] > [Account] を右クリックして、メニューから [Disable Account] を選択します。

図 4-4　　Active Directory：アカウント無効の上書き



AAA サーバを介して account-disabled インジケータが表示されていても、ユーザは正常にログインできます。

Active Directory を使用した最小パスワード長の強制

パスワードの最小長を強制するには、ASA のトンネルグループ一般属性コンフィギュレーション モードで **password-management** コマンドを指定し、Active Directory で次の手順を実行します。

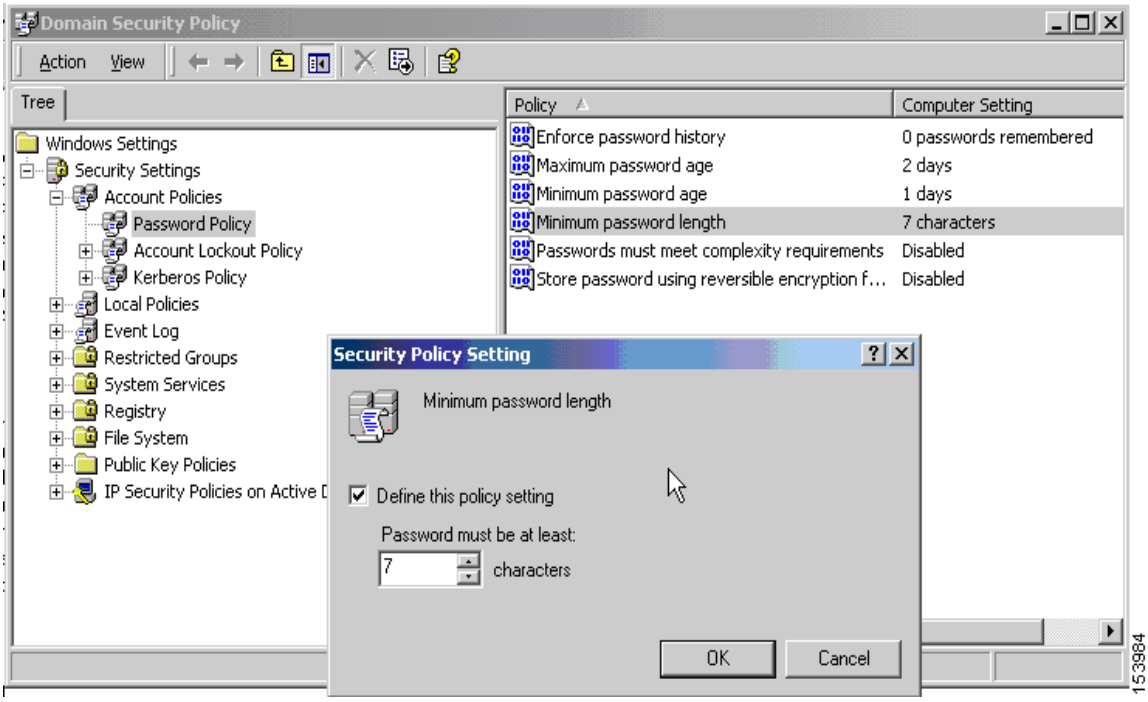
ステップ 1　[Start] > [Programs] > [Administrative Tools] > [Domain Security Policy] を選択します。

ステップ 2　[Windows Settings] > [Security Settings] > [Account Policies] > [Password Policy] を選択します。

ステップ 3　[Minimum Password Length] をダブルクリックします。[Security Policy Setting] ダイアログボックスが表示されます。

ステップ 4　[Define this policy setting] チェックボックスをオンにして、パスワードに含める必要がある最小文字数を指定します。

図 4-5　　Active Directory：最小パスワード長



Active Directory を使用したパスワードの複雑性の強制

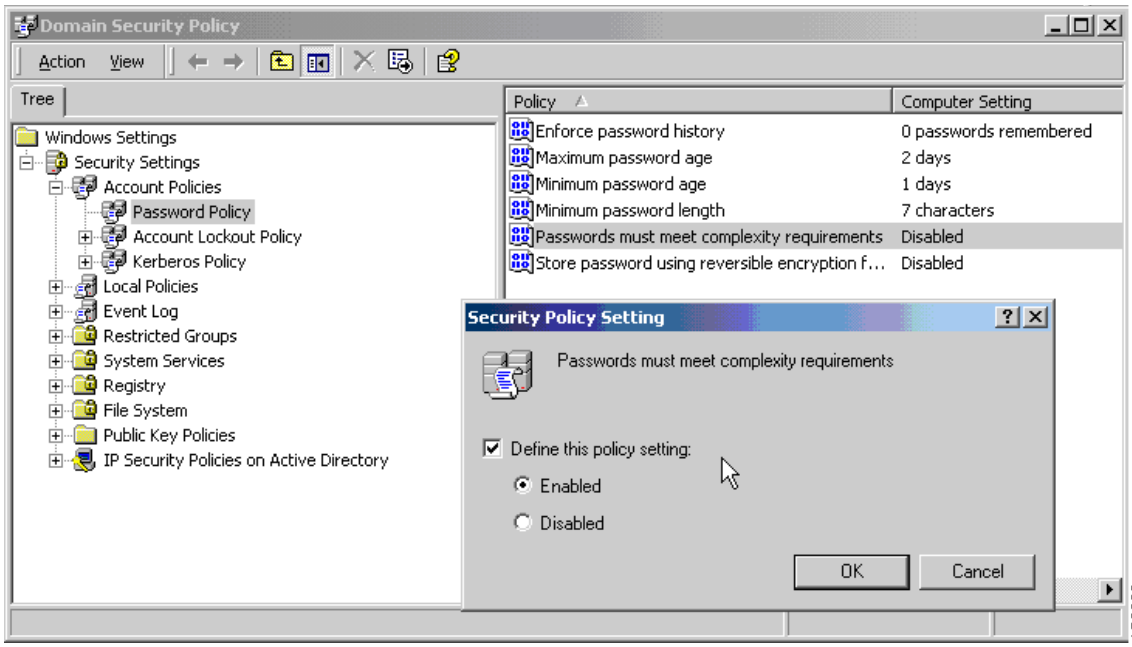
複雑なパスワード、たとえば、大文字と小文字、数字、および特殊文字を含むパスワードを要求するには、ASA のトンネルグループ一般属性コンフィギュレーション モードで **password-management** コマンドを入力し、Active Directory で次の手順を実行します。

ステップ 1　[Start] > [Programs] > [Administrative Tools] > [Domain Security Policy] を選択します。[Windows Settings] > [Security Settings] > [Account Policies] > [Password Policy] を選択します。

ステップ 2　[Password must meet complexity requirements] をダブルクリックして、[Security Policy Setting] ダイアログボックスを開きます。

ステップ 3　[Define this policy setting] チェックボックスをオンにして、[Enabled] を選択します。

図 4-6　　Active Directory：パスワードの複雑性の強制



パスワードの複雑性の強制は、ユーザがパスワードを変更するときにだけ有効になります。たとえば、次回ログイン時にパスワード変更を強制する、または *n* 日後にパスワードが期限切れになるように設定した場合です。ログイン時に、新しいパスワードの入力を求めるプロンプトが表示され、システムは複雑なパスワードだけを受け入れます。

AnyConnect クライアントをサポートする RADIUS/SDI メッセージの接続プロファイルの設定

この項では、RSA SecureID ソフトウェア トークンを使用する AnyConnect VPN クライアントが、SDI サーバにプロキシする RADIUS サーバ経由でクライアントに配信されるユーザ プロンプトに正しく応答できるようにする手順について説明します。ここでは、次の内容について説明します。

- AnyConnect クライアントと RADIUS/SDI サーバのインタラクション
- RADIUS/SDI メッセージをサポートするためのセキュリティ アプライアンスの設定

（注）　二重認証機能を設定した場合、SDI 認証はプライマリ認証サーバでだけサポートされます。

AnyConnect クライアントと RADIUS/SDI サーバのインタラクション

リモート ユーザが AnyConnect VPN クライアントで ASA に接続し、RSA SecurID トークンを使用して認証を試みると、ASA は RADIUS サーバと通信を行い、次に、RADIUS サーバは認証について SDI サーバと通信を行います。

認証の間に、RADIUS サーバは ASA にアクセス チャレンジ メッセージを提示します。これらのチャレンジ メッセージ内に、SDI サーバからのテキストを含む応答メッセージがあります。メッセージ テキストは、ASA が SDI サーバと直接通信している場合と、RADIUS プロキシ経由で通信している場合とでは異なります。そのため、AnyConnect クライアントにネイティブ SDI サーバとして認識させるために、ASA は RADIUS サーバからのメッセージを解釈する必要があります。

また、SDI メッセージは SDI サーバで設定可能であるため、ASA のメッセージ テキストの全体または一部が、SDI サーバのメッセージ テキストと一致する必要があります。一致しない場合、リモート クライアント ユーザに表示されるプロンプトは、認証中に必要とされるアクションに対して適切でない場合があります。そのため、AnyConnect クライアントが応答できずに、認証が失敗する可能性があります。

「RADIUS/SDI メッセージをサポートするためのセキュリティ アプライアンスの設定」（P.4-38）では、クライアントと SDI サーバ間の認証を確実に成功させるように ASA を設定する方法について説明します。

RADIUS/SDI メッセージをサポートするためのセキュリティ アプライアンスの設定

SDI 固有の RADIUS 応答メッセージを解釈し、AnyConnect ユーザに適切なアクションを求めるプロンプトを表示するように ASA を設定するには、次の手順を実行します。

ステップ 1　トンネルグループ webvpn コンフィギュレーション モードで **proxy-auth sdi** コマンドを使用して、SDI サーバとの直接通信をシミュレートする方法で、RADIUS 応答メッセージを転送するための接続プロファイル（トンネルグループ）を設定します。SDI サーバに認証されるユーザは、この接続プロファイルを介して接続する必要があります。

次に例を示します。

```
hostname(config)# tunnel-group sales webvpn attributes
hostname(tunnel-group-webvpn)# proxy-auth sdi
```

ステップ 2　トンネルグループ webvpn コンフィギュレーション モードで **proxy-auth_map sdi** コマンドを使用して、RADIUS サーバによって送信されるメッセージ テキストと全体または一部が一致する RADIUS 応答メッセージ テキストを ASA で設定します。

ASA が使用するデフォルトのメッセージ テキストは、Cisco Secure Access Control Server（ACS）で使用されるデフォルトのメッセージ テキストです。Cisco Secure ACS を使用していて、デフォルトのメッセージ テキストを使用している場合、ASA でメッセージ テキストを設定する必要はありません。それ以外の場合は、**proxy-auth_map sdi** コマンドを使用して、メッセージ テキストが一致するようにします。

表 4-2 は、メッセージ コード、デフォルトの RADIUS 応答メッセージ テキスト、および各メッセージの機能を示しています。セキュリティ アプライアンスは、テーブルに表示される順番に文字列を検索するため、メッセージ テキストに使用する文字列は別の文字列のサブセットではないようにする必要があります。

たとえば、「new PIN」が new-pin-sup と next-ccode-and-reauth の両方に対するデフォルトのメッセージ テキストのサブセットだとします。new-pin-sup を「new PIN」として設定した場合、セキュリティ アプライアンスは RADIUS サーバから「new PIN with the next card code」を受信すると、next-ccode-and-reauth コードではなく new-pin-sup コードとテキストを一致させます。

表 4-2　SDI 操作コード、デフォルトのメッセージ テキスト、およびメッセージの機能

メッセージ コード	デフォルトの RADIUS 応答メッセージ テキスト	機能
next-code	Enter Next PASSCODE	ユーザは PIN を入力せずに次のトークンコードを入力する必要があることを示します。
new-pin-sup	Please remember your new PIN	新しいシステムの PIN が提供されており、ユーザにその PIN を表示することを示します。
new-pin-meth	Do you want to enter your own pin	新しい PIN の作成にどの新しい PIN 方式を使用するかをユーザに尋ねます。
new-pin-req	Enter your new Alpha-Numerical PIN	ユーザ生成の PIN を入力することを要求することを示します。
new-pin-reenter	Reenter PIN:	ユーザが提供した PIN の確認のために ASA が内部的に使用します。ユーザにプロンプトを表示せずに、クライアントが PIN を確認します。
new-pin-sys-ok	New PIN Accepted	ユーザが提供した PIN が受け入れられたことを示します。
next-ccode-and-reauth	new PIN with the next card code	PIN 操作後、次のトークンコードを待ってから、認証のために新しい PIN と次のトークンコードの両方を入力する必要があることをユーザに示します。
ready-for-sys-pin	ACCEPT A SYSTEM GENERATED PIN	ユーザがシステム生成の PIN に対する準備ができていることを示すために ASA が内部的に使用します。

次の例では、aaa-server-host モードに入り、RADIUS 応答メッセージ new-pin-sup のテキストが変更します。

```
hostname(config)# aaa-server radius_sales host 10.10.10.1
hostname(config-aaa-server-host)# proxy-auth_map sdi new-pin-sup “This is your new PIN”
```

グループ ポリシー

この項では、グループ ポリシーとその設定方法について説明します。

グループ ポリシーは、IPSec 接続用のユーザ関連の属性と値のペアがセットになったもので、デバイスに内部的（ローカル）に保存されるか、外部の RADIUS サーバに保存されます。接続プロファイルでは、トンネル確立後、ユーザ接続の条件を設定するグループ ポリシーが使用されます。グループ ポリシーを使用すると、ユーザまたはユーザのグループに属性セット全体を適用できるので、ユーザごとに各属性を個別に指定する必要がありません。

ユーザにグループ ポリシーを割り当てたり、特定のユーザのグループ ポリシーを変更したりするには、グローバル コンフィギュレーション モードで **group-policy** コマンドを入力します。

ASA には、デフォルトのグループ ポリシーが含まれています。変更はできても削除はできないデフォルトのグループ ポリシーに加え、自分の環境に固有の 1 つ以上のグループ ポリシーを作成することもできます。

内部グループ ポリシーと外部グループ ポリシーを設定できます。内部グループは ASA の内部データベースで設定されます。外部グループは RADIUS などの外部認証サーバに設定されます。グループ ポリシーには、次の属性があります。

- アイデンティティ
- サーバの定義
- クライアント ファイアウォールの設定
- トンネリング プロトコル
- IPsec の設定
- ハードウェア クライアントの設定
- フィルタ
- クライアント コンフィギュレーションの設定
- 接続の設定

デフォルトのグループ ポリシー

ASA では、デフォルトのグループ ポリシーが提供されます。このデフォルト グループ ポリシーは変更できますが、削除はできません。デフォルトのグループ ポリシーは、DfltGrpPolicy という名前で ASA に常に存在していますが、このデフォルトのグループ ポリシーは、ASA でそれを使用するように設定しない限り有効にはなりません。その他のグループ ポリシーを設定する場合、明示的に指定しない属性の値はデフォルトのグループ ポリシーから取得されます。デフォルトのグループ ポリシーを表示するには、次のコマンドを入力します。

```
hostname(config)# show running-config all group-policy DfltGrpPolicy
hostname(config)#
```

デフォルトのグループ ポリシーを設定するには、次のコマンドを入力します。

```
hostname(config)# group-policy DfltGrpPolicy internal
hostname(config)#
```

（注） デフォルトのグループ ポリシーは、常に内部（internal）です。コマンド構文は、hostname(config)# group-policy DfltGrpPolicy {internal | external} ですが、タイプを外部（external）に変更することはできません。

デフォルトのグループ ポリシーの任意の属性を変更する場合は、**group-policy attributes** コマンドを使用して属性モードに入り、その後、変更対象の属性を変更するためのコマンドを指定します。

```
hostname(config)# group-policy DfltGrpPolicy attributes
```

（注） 属性モードは内部グループ ポリシーにだけ適用されます。

ASA で提供されるデフォルトのグループ ポリシー DfltGrpPolicy は、次のとおりです。

```
hostname# show run all group-policy DfltGrpPolicy
group-policy DfltGrpPolicy internal
group-policy DfltGrpPolicy attributes
 banner none
 wins-server none
```

```
dns-server value 10.10.10.1.1
dhcp-network-scope none
vpn-access-hours none
vpn-simultaneous-logins 3
vpn-idle-timeout 30
vpn-idle-timeout alert-interval 1
vpn-session-timeout none
vpn-session-timeout alert-interval 1
vpn-filter none
vpn-tunnel-protocol ikev1 ikev2 l2tp-ipsec ssl-client ssl-clientless
password-storage disable
ip-comp disable
re-xauth disable
group-lock none
pfs disable
ipsec-udp disable
ipsec-udp-port 10000
split-tunnel-policy tunnelall
ipv6-split-tunnel-policy tunnelall
split-tunnel-network-list none
default-domain value cisco.com
split-dns none
split-tunnel-all-dns disable
intercept-dhcp 255.255.255.255 disable
secure-unit-authentication disable
user-authentication disable
user-authentication-idle-timeout 30
ip-phone-bypass disable
client-bypass-protocol disable
gateway-fqdn none
leap-bypass disable
nem disable
backup-servers keep-client-config
msie-proxy server none
msie-proxy method no-modify
msie-proxy except-list none
msie-proxy local-bypass disable
msie-proxy pac-url none
msie-proxy lockdown enable
vlan none
nac-settings none
address-pools none
ipv6-address-pools none
smartcard-removal-disconnect enable
scep-forwarding-url none
client-firewall none
client-access-rule none
webvpn
 url-list none
 filter none
 homepage none
 html-content-filter none
 port-forward name Application Access
 port-forward disable
 http-proxy disable
 sso-server none
 anyconnect ssl dtls enable
 anyconnect mtu 1406
 anyconnect firewall-rule client-interface private none
 anyconnect firewall-rule client-interface public none
 anyconnect keep-installer installed
 anyconnect ssl keepalive 20
 anyconnect ssl rekey time none
 anyconnect ssl rekey method none
```

```
  anyconnect dpd-interval client 30
  anyconnect dpd-interval gateway 30
  anyconnect ssl compression none
  anyconnect dtls compression lzs
  anyconnect modules none
  anyconnect profiles none
  anyconnect ask none
  customization none
  keep-alive-ignore 4
  http-comp gzip
  download-max-size 2147483647
  upload-max-size 2147483647
  post-max-size 2147483647
  user-storage none
  storage-objects value cookies,credentials
  storage-key none
  hidden-shares none
  smart-tunnel disable
  activex-relay enable
  unix-auth-uid 65534
  unix-auth-gid 65534
  file-entry enable
  file-browsing enable
  url-entry enable
  deny-message value Login was successful, but because certain criteria have not been met
or due to some specific group policy, you do not have permission to use any of the VPN
features.Contact your IT administrator for more information
  smart-tunnel auto-signon disable
  anyconnect ssl df-bit-ignore disable
  anyconnect routing-filtering-ignore disable
  smart-tunnel tunnel-policy tunnelall
  always-on-vpn profile-setting
```

デフォルト グループ ポリシーは変更可能です。また、環境に固有の 1 つ以上のグループ ポリシーを作成することもできます。

グループ ポリシーの設定

グループ ポリシーは、すべての種類のトンネルに適用できます。どちらの場合も、パラメータが明示的に指定されていなければ、そのグループはデフォルト グループ ポリシーの値を使用します。

設定タスクは、シングル コンテキスト モードまたはマルチ コンテキスト モードの両方で実行できます。

（注） マルチ コンテキスト モードは IKEv1 および IKEv2 サイトツーサイトにのみ適用され、IKEv1 IPSec の AnyConnect、クライアントレス SSL VPN、レガシー Cisco VPN クライアント、Apple ネイティブ VPN クライアント、Microsoft ネイティブ VPN クライアント、または cTCP には適用されません。

外部グループ ポリシーの設定

外部グループ ポリシーの属性値には、指定する外部サーバの値が取得されます。外部グループ ポリシーの場合は、ASA が属性のクエリーを実行できる AAA サーバ グループを特定し、その外部 AAA サーバ グループから属性を取得するときに使用するパスワードを指定する必要があります。外部認証サーバを使用していて、外部グループ ポリシー属性が、認証する予定のユーザと同じ RADIUS サーバにある場合、それらの間で名前が重複しないようにする必要があります。

（注） ASA の外部グループ名は、RADIUS サーバのユーザ名を参照しています。つまり、ASA に外部グループ X を設定する場合、RADIUS サーバはクエリーをユーザ X に対する認証要求と見なします。そのため、外部グループは実際には、ASA にとって特別な意味を持つ、RADIUS サーバ上のユーザ アカウントということになります。外部グループ属性が認証する予定のユーザと同じ RADIUS サーバに存在する場合、それらの間で名前を重複させることはできません。

ASA は、外部 LDAP または RADIUS サーバでのユーザ認証をサポートしています。外部サーバを使用するように ASA を設定する前に、正しい ASA 認可属性でサーバを設定し、それらの属性のサブセットから個々のユーザに対する個別の許可を割り当てる必要があります。外部サーバを設定するには、第 12 章「認可および認証用の外部サーバ」の説明に従ってください。

外部グループ ポリシーを設定するには、次の手順を実行して、server-group 名と password とともにグループ ポリシーの名前とタイプを指定します。

```
hostname(config)# group-policy group_policy_name type server-group server_group_name
password server_password
hostname(config)#
```

（注） 外部グループ ポリシーの場合、サポートされる AAA サーバ タイプは RADIUS だけです。

たとえば、次のコマンドは、ExtGroup という名前の外部グループ ポリシーを作成します。このグループ ポリシーの属性は、ExtRAD という名前の外部 RADIUS サーバから取得され、属性を取得するときに使用されるパスワードが newpassword に指定されます。

```
hostname(config)# group-policy ExtGroup external server-group ExtRAD password newpassword
hostname(config)#
```

（注） 第 12 章「認可および認証用の外部サーバ」に説明されているように、いくつかのベンダー固有属性（VSA）を設定できます。RADIUS サーバが Class 属性（#25）を返すように設定されている場合、ASA は、グループ名の認証にその属性を使用します。RADIUS サーバでは、属性は次の形式で指定する必要があります。OU=*groupname*。ここで、*groupname* は、ASA で設定されたグループ名と同一です。例、OU=Finance。

内部グループ ポリシーの作成

内部グループ ポリシーを設定するには、コンフィギュレーション モードを開始します。group-policy コマンドを使用して、グループ ポリシーの名前と **internal** タイプを指定します。

```
hostname(config)# group-policy group_policy_name internal
hostname(config)#
```

たとえば、次のコマンドは GroupPolicy1 という名前の内部グループ ポリシーを作成します。

```
hostname(config)# group-policy GroupPolicy1 internal
hostname(config)#
```

（注）　いったん作成したグループ ポリシーの名前は変更できません。

キーワード **from** を追加して既存のポリシーの名前を指定することにより、既存のグループ ポリシーの値をコピーして、内部グループ ポリシーの属性を設定できます。

```
hostname(config)# group-policy group_policy_name internal from group_policy_name
hostname(config-group-policy)#
```

たとえば、次のコマンドは GroupPolicy1 の属性をコピーして、GroupPolicy2 という名前の内部グループ ポリシーを作成します。

```
hostname(config)# group-policy GroupPolicy2 internal from GroupPolicy1
hostname(config-group-policy)#
```

一般的な内部グループ ポリシー属性の設定

グループ ポリシー名

グループ ポリシーの名前は内部グループ ポリシーの作成時に選択されています。いったん作成されたグループ ポリシーの名前は変更できません。詳細については、「内部グループ ポリシーの作成」（P.4-43）を参照してください。

グループ ポリシーのバナー メッセージの設定

表示するバナーまたは初期メッセージ（ある場合）を指定します。デフォルトでは、バナーは表示されません。指定したメッセージは、リモート クライアントが接続したときに、そのクライアントに表示されます。バナーを指定するには、グループ ポリシー コンフィギュレーション モードで **banner** コマンドを入力します。バナー テキストの長さは 510 文字までです。復帰改行を挿入する場合は、「\n」シーケンスを入力します。

（注）　バナー内の復帰改行は、2 文字として数えられます。

バナーを削除するには、このコマンドの **no** 形式を入力します。このコマンドの **no** バージョンを使用すると、グループ ポリシーのすべてのバナーが削除されることに注意してください。

グループ ポリシーは、別のグループ ポリシーからこの値を継承できます。値を継承しないようにするには、次のように、バナー文字列の値を指定する代わりに **none** キーワードを入力します。

```
hostname(config-group-policy)# banner {value banner_string | none}
```

次の例は、FirstGroup という名前のグループ ポリシーにバナーを作成する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# banner value Welcome to Cisco Systems ASA 9.0.
```

リモート アクセス接続のアドレス プールの指定

リモート アクセス クライアントが ASA に接続する場合、ASA は、接続に指定されたグループ ポリシーに基づいて IPv4 または IPv6 アドレスをクライアントに割り当てることができます。

ローカル アドレスの割り当てに使用する最大 6 個のローカル アドレス プールのリストを指定できます。プールの指定順序は重要です。ASA では、このコマンドでプールを指定した順序に従って、それらのプールからアドレスが割り当てられます。

内部グループ ポリシーへの IPv4 アドレス プールの割り当て

前提条件

IPv4 アドレス プールを作成します。第 5 章「VPN の IP アドレス」を参照してください。

手順の詳細

	コマンド	目的
ステップ 1	`group-policy value attributes` **例：** `hostname> en` `hostname# config t` `hostname(config)# group-policy FirstGroup attributes` `hostname(config-group-policy)#`	グループ ポリシー コンフィギュレーション モードを開始します。
ステップ 2	**address-pools value** *pool-name1 pool-name2 pool-name6* **例：** `asa4(config-group-policy)# address-pools value ipv4-pool1 ipv4-pool2 ipv4-pool3` `asa4(config-group-policy)#`	ipv4-pool1、ipv4-pool2、および ipv4-pool3 という名前のアドレス プールを FirstGroup グループ ポリシーに割り当てます。 グループ ポリシーには、最大 6 個のアドレス プールを指定できます。
ステップ 3	（オプション） **no address-pools value pool-name1 pool-name2 pool-name6** **例：** `hostname(config-group-policy)# no address-pools value ipv4-pool1 ipv4-pool2 ipv4-pool3` `hostname(config-group-policy)#`	グループ ポリシー設定からアドレス プールを削除し、アドレス プール設定を戻して DefltGroupPolicy などの他のソースからのアドレス プール情報を継承するには、**no address-pools value pool-name** コマンドを使用します。
ステップ 4	（オプション） **address-pools none** **例：** `hostname(config-group-policy)# address-pools none` `hostname(config-group-policy)#`	**address-pools none** コマンドは、ポリシーの別のソース（DefltGrpPolicy など）からこの属性を継承することをディセーブルにします。
ステップ 5	（オプション） **no address-pools none** **例：** `hostname(config-group-policy)# no address-pools none` `hostname(config-group-policy)#`	**no address pools none** コマンドは、**address-pools none** コマンドをグループ ポリシーから削除して、デフォルト値（継承の許可）に戻します。

内部グループ ポリシーへの IPv6 アドレス プールの割り当て

前提条件

IPv6 アドレス プールを作成します。第 5 章「VPN の IP アドレス」を参照してください。

手順の詳細

	コマンド	目的
ステップ 1	`group-policy value attributes` **例：** `hostname> en` `hostname# config t` `hostname(config)# group-policy FirstGroup attributes` `hostname(config-group-policy)#`	グループ ポリシー コンフィギュレーション モードを開始します。
ステップ 2	**ipv6-address-pools value** *pool-name1 pool-name2 pool-name6* **例：** hostname(config-group-policy)# **ipv6-address-pools value ipv6-pool1 ipv6-pool2 ipv6-pool3** hostname(config-group-policy)#	ipv6-pool という名前のアドレス プールを FirstGroup グループ ポリシーに割り当てます。 グループ ポリシーには、最大 6 個の IPv6 アドレス プールを割り当てることができます。 この例では、ipv6-pool1、ipv6-pool2、および ipv6-pool3 が FirstGroup グループ ポリシーに割り当てられています。
ステップ 3	（オプション） **no ipv6-address-pools value pool-name1 pool-name2 pool-name6** **例：** `hostname(config-group-policy)# no ipv6-address-pools value ipv6-pool1 ipv6-pool2 ipv6-pool3` `hostname(config-group-policy)#`	グループ ポリシー設定からアドレス プールを削除し、アドレス プール設定を戻して DfltGroupPolicy などの他のソースからのアドレス プール情報を継承するには、**no ipv6-address-pools value pool-name** コマンドを使用します。
ステップ 4	（オプション） **ipv6-address-pools none** **例：** `hostname(config-group-policy)# ipv6-address-pools none` `hostname(config-group-policy)#`	**ipv6-address-pools none** コマンドは、この属性が DfltGrpPolicy など他のポリシーから継承されないようにします。
ステップ 5	（オプション） **no ipv6-address-pools none** **例：** `hostname(config-group-policy)# no ipv6-address-pools none` `hostname(config-group-policy)#`	**no ipv6-address pools none** コマンドは、**ipv6-address-pools none** コマンドをグループ ポリシーから削除して、デフォルト値（継承の許可）に戻します。

グループ ポリシーのトンネリング プロトコルの指定

グループ ポリシー コンフィギュレーション モードで **vpn-tunnel-protocol {ikev1 | ikev2 | l2tp-ipsec | ssl-client | ssl-clientless}** コマンドを入力して、このグループ ポリシーの VPN トンネル タイプを指定します。

デフォルト値は、デフォルト グループ ポリシーの属性を継承することです。この属性を実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を入力します。

このコマンドのパラメータの値は、次のとおりです。

- **ikev1**：2 つのピア（Cisco VPN Client または別のセキュア ゲートウェイ）間の IPsec IKEv1 トンネルをネゴシエートします。認証、暗号化、カプセル化、およびキー管理を制御するセキュリティ アソシエーションを作成します。
- **ikev2**：2 つのピア（AnyConnect Secure Mobility Client または別のセキュア ゲートウェイ）間の IPsec IKEv2 トンネルをネゴシエートします。認証、暗号化、カプセル化、およびキー管理を制御するセキュリティ アソシエーションを作成します。
- **l2tp-ipsec**：L2TP 接続用の IPsec トンネルをネゴシエートします。
- **ssl-client**：AnyConnect Secure Mobility Client で TLS または DTLS を使用して、SSL トンネルをネゴシエートします。
- **ssl-clientless**：HTTPS 対応の Web ブラウザ経由でリモート ユーザに VPN サービスを提供します。クライアントは必要ありません。

このコマンドを入力して、1 つ以上のトンネリング モードを設定します。VPN トンネルを介して接続するユーザには、少なくとも 1 つのトンネリング モードを設定する必要があります。

次の例は、FirstGroup という名前のグループ ポリシーに IPsec IKEv1 トンネリング モードを設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-tunnel-protocol ikev1
hostname(config-group-policy)#
```

リモート アクセスの VLAN の指定またはグループ ポリシーへの統合アクセス コントロール ルール

フィルタは、ASA を経由して着信したトンネリングされたデータ パケットを、送信元アドレス、宛先アドレス、プロトコルなどの基準によって、許可するか拒否するかを決定するルールで構成されます。グループ ポリシーの IPv4 または IPv6 統合アクセス コントロール リストを指定するか、またはデフォルト グループ ポリシーで指定された ACL を継承するようにできます。

次のオプションのいずれかを選択して、リモート アクセス用の出力 VLAN（「VLAN マッピング」とも呼ばれる）、またはトラフィックをフィルタリングする ACL を指定します。

- グループ ポリシー コンフィギュレーション モードで次のコマンドを入力して、このグループ ポリシーまたはこのグループ ポリシーを継承するグループ ポリシーに割り当てられているリモート アクセス VPN セッション用の出力 VLAN を指定します。

  ```
  hostname(config-group-policy)# [no] vlan {vlan_id |none}
  ```

  no vlan は、グループ ポリシーから *vlan_id* を削除します。グループ ポリシーは、デフォルトのグループ ポリシーから vlan 値を継承します。

  none は、グループ ポリシーから *vlan_id* を削除し、このグループ ポリシーに対する VLAN マッピングをディセーブルにします。グループ ポリシーは、デフォルトのグループ ポリシーから vlan 値を継承しません。

vlan_id は、このグループ ポリシーを使用するリモート アクセス VPN セッションに割り当てる VLAN の番号（10 進表記）です。VLAN は一般的な操作のコンフィギュレーション ガイドの「Configuring VLAN Subinterfaces and 802.1Q Trunking」の手順に従って、この ASA で設定する必要があります。

（注） 出力 VLAN は、HTTP 接続では機能しますが、FTP と CIFS では機能しません。

- グループ ポリシー モードで **vpn-filter** コマンドを使用して、VPN セッションに適用するアクセス コントロール ルール（ACL）の名前を指定します vpn-filter コマンドを使用して、IPv4 または IPv6 ACL を指定できます。

（注） 以前のリリースでは、vpn-filter で指定された IPv6 エントリが存在しない場合に IPv6 ACL を指定するには、非推奨の ipv6-vpn-filter コマンドを使用できました。ASA 9.1(4) 以降、ipv6-vpn-filter は無効になっているため、IPv6 ACL エントリは、vpn-filter コマンドを使用して指定する必要があります。ipv6-vpn-filter が設定されている場合は、VPN 接続は終了します。

（注） この属性はユーザ名モードで設定することもできます。その場合、ユーザ名の下で設定された値がグループ ポリシーの値よりも優先されます。

```
hostname(config-group-policy)# vpn-filter {value ACL name | none}
hostname(config-group-policy)#
```

ACL を設定して、このグループ ポリシーについて、さまざまなタイプのトラフィックを許可または拒否します。次に、**vpn-filter** コマンドを入力して、これらの ACL を適用します。

vpn-filter none コマンドを入力して作成したヌル値を含めて、ACL を削除するには、このコマンドの **no** 形式を入力します。**no** オプションを使用すると、値を別のグループ ポリシーから継承できるようになります。

グループ ポリシーは、別のグループ ポリシーからこの値を継承できます。値を継承しないようにするには、ACL 名を指定する代わりに、**none** キーワードを入力します。**none** キーワードは、ACL がないことを示します。このキーワードにより、ヌル値が設定され、ACL が拒否されます。

次に、FirstGroup という名前のグループ ポリシーの、acl_vpn という ACL を呼び出すフィルタを設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-filter acl_vpn
hostname(config-group-policy)#
```

vpn-filter コマンドは、トンネルから出た後の、復号化後のトラフィックとトンネルに入る前の、暗号化前のトラフィックに適用されます。vpn-filter に使用される ACL を interface access-group にも使用することはできません。**vpn-filter** コマンドを、リモート アクセス VPN クライアント接続を制御するグループ ポリシーに適用する場合は、ACL の **src_ip** の位置のクライアント割り当て IP アドレスおよび ACL の **dest_ip** の位置のローカル ネットワークに対して ACL を設定する必要があります。

vpn-filter コマンドを、LAN-to-LAN VPN 接続を制御するグループ ポリシーに適用する場合は、ACL の **src_ip** の位置のリモート ネットワークおよび ACL の **dest_ip** の位置のローカル ネットワークに対して ACL を設定する必要があります。

vpn-filter 機能で使用するために ACL を設定する場合は、注意する必要があります。ACL は、復号化後のトラフィックに対して構築されていることに留意してください。ただし、ACL は反対方向のトラフィックに対しても適用されます。トンネル宛ての、暗号化前のこのトラフィックについては、ACL は **src_ip** の位置と **dest_ip** の位置を入れ替えたものに対して構築されています。

次の例では、vpn-filter をリモート アクセス VPN クライアントと共に使用します。
この例では、クライアント割り当て IP アドレスを 10.10.10.1/24、ローカル ネットワークを 192.168.1.0/24 としています。

次の ACE によって、リモート アクセス VPN クライアントがローカル ネットワークに Telnet を使用することが許可されます。

```
hostname(config-group-policy)# access-list vpnfilt-ra permit 10.10.10.1 255.255.255.255
192.168.1.0 255.255.255.0 eq 23
```

次の ACE によって、ローカル ネットワークがリモート アクセス クライアントに Telnet を使用することが許可されます。

```
hostname(config-group-policy)# access-list vpnfilt-ra permit 10.10.10.1 255.255.255.255 eq
23 192.168.1.0 255.255.255.0
```

（注）　ACE の **access-list vpnfilt-ra permit 10.10.10.1 255.255.255.255 192.168.1.0 255.255.255.0 eq 23** によって、ローカル ネットワークは、送信元ポート 23 を使用している場合に任意の TCP ポートでのリモート アクセス クライアントへの接続開始が許可されます。ACE の **access-list vpnfilt-ra permit 10.10.10.1 255.255.255.255 eq 23 192.168.1.0 255.255.255.0** によって、リモート アクセス クライアントは、送信元ポート 23 を使用している場合に任意の TCP ポートでのローカル ネットワークへの接続開始が許可されます。

次の例では、vpn-filter を LAN-to-LAN VPN 接続と共に使用します。この例では、リモート ネットワークを 10.0.0.0/24、ローカル ネットワークを 192.168.1.0/24 としています。
次の ACE によって、リモート ネットワークがローカル ネットワークに Telnet を使用することが許可されます。

```
hostname(config-group-policy)# access-list vpnfilt-l2l permit 10.0.0.0 255.255.255.0
192.168.1.0 255.255.255.0 eq 23
```

次の ACE によって、ローカル ネットワークがリモート ネットワークに Telnet を使用することが許可されます。

```
hostname(config-group-policy)# access-list vpnfilt-l2l permit 10.0.0.0 255.255.255.0 eq 23
192.168.1.0 255.255.255.0
```

（注）　ACE の **access-list vpnfilt-l2l permit 10.0.0.0 255.255.255.0 192.168.1.0 255.255.255.0 eq 23** によって、ローカル ネットワークは、送信元ポート 23 を使用している場合に任意の TCP ポートでのリモート ネットワークへの接続開始が許可されます。ACE の **access-list vpnfilt-l2l permit 10.0.0.0 255.255.255.0 eq 23 192.168.1.0 255.255.255.0** によって、リモート ネットワークは、送信元ポート 23 を使用している場合に任意の TCP ポートでのローカル ネットワークへの接続開始が許可されます。

グループ ポリシーに対する NAC ポリシーの指定

このコマンドでは、このグループ ポリシーに適用するネットワーク アドミッション コントロール ポリシーの名前を選択します。オプションの NAC ポリシーを各グループ ポリシーに割り当てることができます。デフォルト値は --None-- です。

前提条件

NAC ポリシーを作成します。「ネットワーク アドミッション コントロール」（P.7-1）を参照してください。

手順の詳細

	コマンド	目的
ステップ 1	`group-policy value attributes` **例：** `hostname> en` `hostname# config t` `hostname(config)# group-policy FirstGroup attributes` `hostname(config-group-policy)#`	グループ ポリシー コンフィギュレーション モードを開始します。
ステップ 2	**nac-settings value** *nac-policy-name* **例：** hostname(config-group-policy)# **nac-settings value nac-policy-1** hostname(config-group-policy)#	nac-policy-1 という名前の NAC ポリシーを FirstGroup グループ ポリシーに割り当てます。

グループ ポリシーの VPN アクセス時間の指定

前提条件

時間の範囲を作成します。一般的な操作のコンフィギュレーション ガイドの「Configuring Time Ranges」を参照してください。

手順の詳細

	コマンド	目的
ステップ 1	`group-policy value attributes` **例：** `hostname> en` `hostname# config t` `hostname(config)# group-policy FirstGroup attributes` `hostname(config-group-policy)#`	グループ ポリシー コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 2	hostname(config-group-policy)# **vpn-access-hours value** {*time-range-name* | **none**} **例：** hostname(config-group-policy)# **vpn-access-hours value business-hours** hostname(config-group-policy)#	グループ ポリシー コンフィギュレーション モードで **vpn-access-hours** コマンドを使用して、グループ ポリシーと設定済みの time-range ポリシーを関連付けることによって、VPN アクセス時間を設定できます。 このコマンドは、business-hours という名前の VPN アクセス時間範囲を FirstGroup という名前のグループ ポリシーに割り当てます。 グループ ポリシーは、デフォルトまたは指定されたグループ ポリシーの time-range の値を継承することができます。この継承が発生しないようにするには、このコマンドで time-range の名前ではなく **none** キーワードを入力します。このキーワードにより、VPN アクセス時間がヌル値に設定され、time-range ポリシーは許可されなくなります。

グループ ポリシーの同時 VPN ログインの指定

グループ ポリシー コンフィギュレーション モードで **vpn-simultaneous-logins** コマンドを使用して、任意のユーザに許可される同時ログイン数を指定します。

```
hostname(config-group-policy)# vpn-simultaneous-logins integer
```

デフォルト値は 3 です。値の範囲は 0 ～ 2147483647 の整数です。グループ ポリシーは、別のグループ ポリシーからこの値を継承できます。ログインをディセーブルにしてユーザのアクセスを禁止するには、0 を入力します。次に、FirstGroup という名前のグループ ポリシーに対して最大 4 つの同時ログインを許可する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-simultaneous-logins 4
hostname(config-group-policy)#
```

（注） 同時ログイン数の最大制限は非常に大きい値ですが、複数の同時ログインを許可すると、セキュリティが侵害されたり、パフォーマンスが低下したりすることがあります。

失効した AnyConnect、IPsec クライアント、またはクライアントレス セッション（異常終了したセッション）は、同じユーザ名で「新しい」セッションが確立されても、セッション データベースに残る場合があります。

vpn-simultaneous-logins の値が 1 の場合は、異常終了後に同じユーザが再度ログインすると、失効したセッションはデータベースから削除され、新しいセッションが確立されます。ただし、既存のセッションがまだアクティブな接続である場合は、同じユーザが別の PC などから再度ログインすると、最初のセッションがログオフし、データベースから削除されて、新しいセッションが確立されます。

同時ログイン数が 1 より大きい値の場合、その最大数に達した状態で再度ログインしようとすると、最もアイドル時間の長いセッションがログオフします。現在のすべてのセッションが同じくらい長い間アイドル状態の場合は、最も古いセッションがログオフします。このアクションにより、セッションが解放されて新しいログインが可能になります。

特定の接続プロファイルへのアクセスの制限

グループ ポリシー コンフィギュレーション モードで **group-lock** コマンドを使用して、接続プロファイルを介してだけアクセスするようにリモート ユーザを制限するかどうかを指定します。

```
hostname(config-group-policy)# group-lock {value tunnel-grp-name | none}
hostname(config-group-policy)# no group-lock
hostname(config-group-policy)#
```

tunnel-grp-name 変数は、ASA がユーザの接続に関して要求する既存の接続プロファイルの名前を指定します。group-lock は、VPN クライアントで設定されたグループが、そのユーザが割り当てられている接続プロファイルと同じかどうかをチェックすることによって、ユーザを制限します。同一ではなかった場合、ASA はユーザによる接続を禁止します。group-lock を設定しなかった場合、ASA は、割り当てられているグループに関係なくユーザを認証します。グループのロックは、デフォルトではディセーブルになっています。

group-lock 属性を実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。このオプションを使用すると、別のグループ ポリシーの値を継承できます。

group-lock をディセーブルにするには、**none** キーワードを指定して **group-lock** コマンドを入力します。none キーワードにより、group-lock はヌル値に設定され、group-lock の制限が拒否されます。また、デフォルトまたは指定されたグループ ポリシーから group-lock の値が継承されなくなります。

グループ ポリシーの VPN の最大接続時間の指定

ステップ 1　グループ ポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで **vpn-session-timeout** コマンドを使用して、VPN 接続の最大時間を設定します。

```
hostname(config-group-policy)# vpn-session-timeout {minutes | none}
hostname(config-group-policy)#
```

最小時間は 1 分で、最大時間は 35791394 分です。デフォルト値はありません。この期間が終了すると、ASA は接続を終了します。

グループ ポリシーは、別のグループ ポリシーからこの値を継承できます。値を継承しないようにするには、分を指定する代わりに **none** キーワードを指定して、このコマンドを入力します。**none** キーワードを指定すると、無制限のセッション タイムアウト期間が許可されます。セッション タイムアウトにはヌル値が設定され、セッション タイムアウトが拒否されます。

次に、FirstGroup という名前のグループ ポリシーに対して 180 分の VPN セッション タイムアウトを設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-session-timeout 180
hostname(config-group-policy)#
```

ステップ 2　**vpn-session-timeout alert-interval** {minutes | none} コマンドを使用して、セッション タイムアウトのアラート メッセージがユーザに表示される時間を設定します。このアラート メッセージは、VPN セッションが自動的に切断されるまでに何分あるかをユーザに伝えます。

次に、VPN セッションが切断される 20 分前にユーザに通知されるよう **vpn-session-timeout alert-interval** を設定する例を示します。1 ～ 30 分の範囲を指定できます。

```
hostname(config-webvpn)# vpn-session-timeout alert-interval 20
```

none パラメータは、ユーザが通知を受信しないことを示します。

VPN セッション タイムアウト アラート間隔属性がデフォルト グループ ポリシーから継承されることを示すには、このコマンドの no 形式を使用します。

```
no vpn-session-timeout alert-interval
```

グループ ポリシーの VPN セッション アイドル タイムアウトの指定

ステップ 1　グループ ポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで **vpn-idle-timeout** コマンドを入力して、ユーザ タイムアウト期間を設定します。

```
hostname(config-group-policy)# vpn-idle-timeout {minutes | none}
hostname(config-group-policy)#
```

AnyConnect（SSL IPsec/IKEv2）：次のコマンドで設定されたグローバル WebVPN default-idle-timeout 値（秒単位）を使用します。**hostname(config-webvpn)# default-idle-timeout**

WebVPN **default-idle-timeout** コマンドにおけるこの値の範囲は、60 ～ 86400 秒です。デフォルトのグローバル WebVPN アイドル タイムアウト（秒単位）は、1800 秒（30 分）です。

（注）　すべての AnyConnect 接続では、ASA によってゼロ以外のアイドル タイムアウト値が要求されます。

WebVPN ユーザの場合、**default-idle-timeout** 値は、vpn-idle-timeout none がグループ ポリシー / ユーザ名属性に設定されている場合にのみ有効です。

サイト間（IKEv1、IKEv2）および IKEv1 リモート アクセス：タイムアウトをディセーブルにし、無制限のアイドル期間を許可します。

次の例は、FirstGroup という名前のグループ ポリシーに 15 分の VPN アイドル タイムアウトを設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-idle-timeout 15
hostname(config-group-policy)#
```

ステップ 2　**vpn-idle-timeout alert-interval {minutes | none}** コマンドを使用して、アイドルタイムアウトのアラート メッセージがユーザに表示される時間を設定します。このアラート メッセージは、VPN セッションが非アクティブ状態のため切断されるまでに何分あるかをユーザに伝えます。

次に、VPN セッションが非アクティブ状態のため切断される 20 分前にユーザに通知されるよう vpn-idle-timeout alert-interval を設定する例を示します。1 ～ 30 分の範囲を指定できます。

```
hostname(config-webvpn)# vpn-idle-timeout alert-interval 20
```

none パラメータは、ユーザが通知を受信しないことを示します。

VPN アイドル タイムアウト アラート間隔属性がデフォルト グループ ポリシーから継承されることを示すには、このコマンドの no 形式を使用します。

```
no vpn-idle-timeout alert-interval
```

グループ ポリシーの WINS サーバと DNS サーバの設定

プライマリおよびセカンダリの WINS サーバと DNS サーバを指定できます。それぞれのデフォルト値は none です。これらのサーバを指定するには、次の手順を実行します。

ステップ 1　プライマリとセカンダリの WINS サーバを指定します。

```
hostname(config-group-policy)# wins-server value {ip_address [ip_address] | none}
hostname(config-group-policy)#
```

最初に指定する IP アドレスがプライマリ WINS サーバの IP アドレスです。2 番目（オプション）の IP アドレスはセカンダリ WINS サーバの IP アドレスです。IP アドレスではなく **none** キーワードを指定すると、WINS サーバにヌル値が設定されます。この設定により、WINS サーバは許可されず、デフォルトまたは指定のグループ ポリシーから値が継承されなくなります。

wins-server コマンドを入力するたびに、既存の設定が上書きされます。たとえば、WINS サーバ x.x.x.x を設定してから WINS サーバ y.y.y.y を設定すると、2 番めのコマンドによって最初の設定が上書きされ、y.y.y.y が唯一の WINS サーバになります。サーバを複数設定する場合も同様です。設定済みのサーバを上書きするのではなく、WINS サーバを追加するには、このコマンドを入力するときに、すべての WINS サーバの IP アドレスを含めます。

次の例は、FirstGroup という名前のグループ ポリシーに、IP アドレスが 10.10.10.15 と 10.10.10.30 である WINS サーバを設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# wins-server value 10.10.10.15 10.10.10.30
hostname(config-group-policy)#
```

ステップ 2　プライマリとセカンダリの DNS サーバを指定します。

```
hostname(config-group-policy)# dns-server value {ip_address [ip_address] | none}
hostname(config-group-policy)#
```

最初に指定する IP アドレスがプライマリ DNS サーバの IP アドレスです。2 番目（オプション）の IP アドレスはセカンダリ DNS サーバの IP アドレスです。IP アドレスではなく **none** キーワードを指定すると、DNS サーバにヌル値が設定されます。この設定により、DNS サーバは許可されず、デフォルトまたは指定のグループ ポリシーから値が継承されなくなります。最大 4 つの DNS サーバ アドレス、2 つの IPv4 アドレス、および 2 つの IPv6 アドレスを指定できます。

dns-server コマンドを入力するたびに、既存の設定が上書きされます。たとえば、DNS サーバ x.x.x.x を設定し、次に DNS サーバ y.y.y.y を設定した場合、2 番めのコマンドは最初のコマンドを上書きし、y.y.y.y が唯一の DNS サーバになります。サーバを複数設定する場合も同様です。以前に設定された DNS サーバを上書きする代わりにサーバを追加するには、このコマンドを入力するときにすべての DNS サーバの IP アドレスを含めます。

次に、FirstGroup という名前のグループ ポリシーで、IP アドレスが 10.10.10.15、10.10.10.30、2001:DB8::1、および 2001:DB8::2 の DNS サーバを設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# dns-server value 10.10.10.15 10.10.10.30 2001:DB8::1
2001:DB8::2
hostname(config-group-policy)#
```

ステップ 3　**DeafultDNS DNS サーバ グループ**にデフォルトのドメイン名が指定されていない場合は、デフォルト ドメインを指定する必要があります。たとえば、**example.com** というドメイン名およびトップ レベル ドメインを使用します。

```
asa4(config)# group-policy FirstGroup attributes
asa4(config-group-policy)# default-domain value example.com
asa4(config-group-policy)#
```

ステップ 4　DHCP ネットワーク スコープを次のように設定します。

```
hostname(config-group-policy)# dhcp-network-scope {ip_address | none}
hostname(config-group-policy)#
```

DHCP スコープでは、ASA DHCP サーバがこのグループ ポリシーのユーザにアドレスを割り当てるために使用する IP アドレスの範囲（つまり、サブネットワーク）を指定します。

次の例は、First Group という名前のグループ ポリシーに IP サブネットワーク 10.10.85.0（アドレス範囲 10.10.85.0 ～ 10.10.85.255 を指定）を設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# dhcp-network-scope 10.10.85.0
```

AnyConnect トラフィックに対するスプリット トンネリングの設定

スプリット トンネリングは、VPN トンネル（暗号化）と VPN トンネル外の他のネットワーク トラフィック（非暗号化、つまり「クリア テキスト」）を介して一部の AnyConnect ネットワーク トラフィックを誘導します。

スプリット トンネリングを設定するには、スプリット トンネリング ポリシーを作成し、そのポリシーにアクセス コントロール リストを設定し、グループ ポリシーにスプリット トンネル ポリシーを追加します。グループ ポリシーをクライアントに送信する際に、クライアントはスプリット トンネリング ポリシーの ACL を使用してどこにネットワーク トラフィックを送信するかを決定します。

アクセス リストを作成する場合：

- アクセス コントロール リストには IPv4 および IPv6 両方のアドレスを指定できます。
- 標準 ACL を使用すると、1 つのアドレスまたはネットワークのみが使用されます。
- 拡張 ACL を使用すると、ソース ネットワークがスプリット トンネリング ネットワークになります。この場合、宛先ネットワークは無視されます。
- any として設定したアクセス リストや、アドレス 0.0.0.0/0.0.0.0 または ::/0 で設定したアクセス リストは、クライアントに送信されません。トンネル上のすべてのトラフィックを送信するには、スプリット トンネル ポリシーを作成するときに「tunnelall」を指定します。
- アドレス 0.0.0.0/255.255.255.255 または ::/128 は、スプリット トンネル ポリシーが **excludespecified** の場合にのみクライアントに送信されます。この設定は、トンネル トラフィックがローカル サブネット宛でないことをクライアントに通知します。
- AnyConnect では、スプリット トンネリング ポリシーで指定されたすべてのサイト、**および** ASA によって割り当てられた IP アドレスと同じサブネット内に含まれるすべてのサイトにトラフィックを渡します。たとえば、ASA によって割り当てられた IP アドレスが 10.1.1.1、マスクが 255.0.0.0 の場合、エンドポイント デバイスは、スプリット トンネリング ポリシーに関係なく、10.0.0.0/8 を宛先とするすべてのトラフィックを渡します。そのため、割り当てられた IP アドレスが、期待されるローカル サブネットを適切に参照するように、ネットマスクを使用します。

スプリット トンネル トラフィックを送信するようにドメインのリストを指定することもできます。クライアントは、split-dns リストのドメインへのトラフィックを VPN に送信します。また、その他のトラフィックはクリア テキストです。

前提条件

- ACL および ACE でアクセス リストを作成する必要があります。
- IPv4 ネットワークのスプリット トンネル ポリシーを作成し、IPv6 ネットワークに別のスプリット トンネル ポリシーを作成した場合は、split-tunnel-network-list コマンドで指定したネットワーク リストが両方のプロトコルに使用されます。このため、ネットワーク リストには、IPv4 および IPv6 の両方のトラフィックのアクセス コントロール エントリ（ACE）が含まれている必要があります。

スプリット トンネリング ポリシーの設定

IPv4 トラフィックのスプリット トンネリング ポリシーを指定して、トラフィックのトンネリング ルールを設定します。

```
hostname(config-group-policy)# split-tunnel-policy {tunnelall | tunnelspecified |
excludespecified}
hostname(config-group-policy)# no split-tunnel-policy
```

IPv6 トラフィックのスプリット トンネリング ポリシーを指定して、トラフィックのトンネリング ルールを設定します。

```
hostname(config-group-policy)# ipv6-split-tunnel-policy {tunnelall | tunnelspecified |
excludespecified}
hostname(config-group-policy)# no ipv6-split-tunnel-policy
```

ポリシー オプションは次のとおりです。

- **tunnelspecified**：トンネルを通じてネットワーク リストに指定されているネットワークに対するすべてのトラフィックをトンネリングします。その他すべてのアドレスに対するデータは、クリア テキストで送信され、リモート ユーザのインターネット サービス プロバイダーによってルーティングされます。

  ASA 9.1.4 以降のバージョンでは、インクルード リストを指定するときに、インクルード範囲内のサブネットにエクスクルード リストも指定できます。除外されたサブネットのアドレスは、トンネリングされず、インクルード リストの残りの部分がトンネリングされます。エクスクルージョン リストのネットワークはトンネルを介して送信されません。エクスクルージョン リストは拒否エントリを使用して指定され、インクルージョン リストは許可エントリを使用して指定されます。

（注） インクルード リストのサブネットではないエクスクルージョン リストのネットワークは、クライアントに無視されます。

- **excludespecified**：ネットワーク リストに指定されているネットワークとの双方向のトラフィックをトンネリングしません。その他すべてのアドレスに対するトラフィックはトンネリングされます。クライアント上でアクティブになっている VPN クライアント プロファイルは、ローカル LAN アクセスを有効にしておく必要があります。
- **tunnelall**：すべてのトラフィックがトンネルを通過するよう指定します。このポリシーは、スプリット トンネリングをディセーブルにします。リモート ユーザは企業ネットワークにアクセスできますが、ローカル ネットワークへはアクセスできません。これがデフォルトのオプションです。

（注） スプリット トンネリングはセキュリティ機能ではなく、トラフィック管理機能です。最大限のセキュリティを確保するには、スプリット トンネリングをイネーブルにしないことを推奨します。

次に、IPv4 と IPv6 の FirstGroup という名前のグループ ポリシーに対して、指定したネットワークのみをトンネリングするスプリット トンネリング ポリシーを設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# split-tunnel-policy tunnelspecified

hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# ipv6-split-tunnel-policy tunnelspecified
```

スプリット トンネリング用のネットワーク リストの指定

スプリット トンネリングでは、どのネットワーク トラフィックがトンネルを通過するかはネットワーク リストによって決まります。AnyConnect は、ACL であるネットワーク リストに基づいてスプリット トンネリングの判断を行います。

手順

```
hostname(config-group-policy)# split-tunnel-network-list {value access-list_name | none}
hostname(config-group-policy)# no split-tunnel-network-list value [access-list_name]
```

- **value** *access-list name* : トンネリングを実行する、または実行しないネットワークを列挙した ACL を指定します。ACL には、IPv4 と IPv6 の両方のアドレスを指定する ACE が含まれている統合 ACL を指定できます。
- **none** : スプリット トンネリング用のネットワーク リストが存在しないことを示し、ASA はすべてのトラフィックをトンネリングします。**none** キーワードを指定すると、スプリット トンネリングのネットワーク リストにヌル値が設定され、スプリット トンネリングが拒否されます。また、これにより、デフォルトまたは指定されたグループ ポリシーから、デフォルトのスプリット トンネリング ネットワーク リストが継承されなくなります。

ネットワーク リストを削除するには、このコマンドの **no** 形式を入力します。すべてのスプリット トンネリング ネットワーク リストを削除するには、引数を指定せずに **no split-tunnel-network-list** コマンドを入力します。このコマンドにより、**none** キーワードを入力して作成したヌル リストがあればそれも含めて、設定済みのすべてのネットワーク リストが削除されます。

スプリット トンネリング ネットワーク リストがない場合、ユーザはデフォルトのグループ ポリシーまたは指定したグループ ポリシー内に存在するネットワーク リストを継承します。ユーザがこのようなネットワーク リストを継承しないようにするには、**split-tunnel-network-list none** コマンドを入力します。

例

次に、FirstList という名前のネットワーク リストを作成し、FirstGroup という名前のグループ ポリシーに追加する例を示します。FistList はエクスクルージョン リストであり、エクスクルージョン リストのサブネットであるインクルージョン リストです。

```
hostname(config)# split-tunnel-policy tunnelspecified
hostname(config)# access-list FirstList deny ip 10.10.10.0 255.255.255.0 any
hostname(config)# access-list FirstList permit ip 10.0.0.0 255.0.0.0 any

hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# split-tunnel-network-list value FirstList
```

次に、v6 という名前のネットワーク リストを作成し、GroupPolicy_ipv6-ikev2 という名前のグループ ポリシーに v6 スプリット トンネル ポリシーを追加する例を示します。v6 はエクスクルージョン リストであり、エクスクルージョン リストのサブネットであるインクルージョン リストです。

```
hostname(config)# access-list v6 extended permit ip fd90:5000::/32 any6
hostname(config)# access-list v6 extended deny ip fd90:5000:3000:2880::/64 any6

hostname(config)# group-policy GroupPolicy_ipv6-ikev2 internal
hostname(config)# group-policy GroupPolicy_ipv6-ikev2 attributes
hostname(config-group-policy)# vpn-tunnel-protocol ikev2 ssl-client
hostname(config-group-policy)# ipv6-split-tunnel-policy tunnelspecified
hostname(config-group-policy)# split-tunnel-network-list value v6
```

スプリット トンネル設定の確認

show runn group-policy attributes コマンドを実行して、設定を確認します。次の例は、管理者が IPv4 と IPv6 の両方のネットワーク ポリシーを設定し、両方のポリシーに対してネットワーク リスト（統合 ACL）**FirstList** を使用したことを示しています。

```
hostname(config-group-policy)# show runn group-policy FirstGroup attributes
group-policy FirstGroup attributes
 split-tunnel-policy tunnelspecified
 ipv6-split-tunnel-policy tunnelspecified
 split-tunnel-network-list value FirstList
```

スプリット トンネリング用のドメイン属性の設定

デフォルト ドメイン名、またはスプリット トンネルを介して解決する、スプリット DNS と呼ばれるドメインのリストを指定できます。

AnyConnect 3.1 は、Windows および Mac OS X のプラットフォームのトゥルー スプリット DNS 機能をサポートします。セキュリティ アプライアンスのグループ ポリシーにより Split-Include トンネリングがイネーブルになっており、トンネリング対象の DNS 名が指定されている場合、AnyConnect は、この名前に一致するすべての DNS クエリーをプライベート DNS サーバにトンネリングします。トゥルー スプリット DNS を使用すると、ASA によってクライアントにプッシュダウンされたドメインに一致する DNS 要求へのトンネル アクセスのみが許可されます。これらの要求は、クリア テキストでは送信されません。一方、DNS 要求が ASA によってプッシュダウンされたドメインに一致しない場合は、AnyConnect は、クライアントのオペレーティング システムにある DNS リゾルバから、DNS 解決に使用されるホスト名を暗号化せずに送信させます。

スプリット DNS は、標準クエリーおよび更新クエリー（A、AAAA、NS、TXT、MX、SOA、ANY、SRV、PTR、CNAME など）をサポートしています。トンネリングされたネットワークのいずれかに一致する PTR クエリーは、トンネル経由で許可されます。

Mac OS X の場合、AnyConnect は、次のいずれかの条件を満たす場合のみ、ある IP プロトコルのトゥルー スプリット DNS を使用できます。

- グループ ポリシーで、スプリット DNS が 1 つの IP プロトコル（IPv4 など）に設定されており、クライアント バイパス プロトコルがもう片方の IP プロトコル（IPv6 など）に設定されている（後者の IP プロトコルにはアドレス プールは設定されていない）。
- スプリット DNS が両方の IP プロトコルに設定されている。

デフォルトのドメイン名の定義

ASA は AnyConnect クライアントにデフォルトのドメイン名を渡します。クライアントは、ドメイン フィールドを省略した DNS クエリーにドメイン名を追加します。このドメイン名は、トンネル パケットにだけ適用されます。デフォルトのドメイン名がない場合、ユーザはデフォルト グループ ポリシーのデフォルト ドメイン名を継承します。

グループ ポリシーのユーザのデフォルト ドメイン名を指定するには、グループ ポリシー コンフィギュレーション モードで **default-domain** コマンドを入力します。ドメイン名を削除するには、このコマンドの **no** 形式を入力します。

```
hostname(config-group-policy)# default-domain {value domain-name | none}
hostname(config-group-policy)# no default-domain [domain-name]
```

value *domain-name* パラメータは、グループのデフォルト ドメイン名を指定します。デフォルト ドメイン名が存在しないことを指定するには、**none** キーワードを入力します。このコマンドにより、デフォルト ドメイン名にヌル値が設定され、デフォルト ドメイン名が拒否されます。また、デフォルトまたは指定されたグループ ポリシーからデフォルト ドメイン名が継承されなくなります。

すべてのデフォルト ドメイン名を削除するには、引数を指定せずに **no default-domain** コマンドを入力します。このコマンドにより、**none** キーワードを指定して **default-domain** コマンドを入力して作成したヌル リストがあればそれも含めて、設定済みのすべてのデフォルト ドメイン名が削除されます。**no** 形式を使用すると、ドメイン名の継承が許可されます。

次に、FirstGroup という名前のグループ ポリシーに対して、FirstDomain のデフォルト ドメイン名を設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# default-domain value FirstDomain
```

スプリット トンネリング用のドメイン リストの定義

デフォルトのドメイン名のほかに、スプリット トンネルを介して解決されるドメインのリストを入力します。グループ ポリシー コンフィギュレーション モードで **split-dns** コマンドを入力します。リストを削除するには、このコマンドの **no** 形式を入力します。

スプリット トンネリング ドメインのリストがない場合、ユーザはデフォルトのグループ ポリシー内に存在するリストを継承します。ユーザがこのようなスプリット トンネリング ドメイン リストを継承しないようにするには、**none** キーワードを指定して **split-dns** コマンドを入力します。

すべてのスプリット トンネリング ドメイン リストを削除するには、引数を指定せずに **no split-dns** コマンドを入力します。これにより、**none** キーワードを指定して **split-dns** コマンドを発行して作成したヌル リストを含めて、設定済みのすべてのスプリット トンネリング ドメイン リストが削除されます。

パラメータ **value** *domain-name* では、ASA がスプリット トンネルを介して解決するドメイン名を指定します。**none** キーワードは、スプリット DNS リストが存在しないことを示します。また、このキーワードにより、スプリット DNS リストにヌル値が設定されます。そのため、スプリット DNS リストは拒否され、デフォルトまたは指定されたグループ ポリシーのスプリット DNS リストが継承されなくなります。このコマンドの構文は次のとおりです。

```
hostname(config-group-policy)# split-dns {value domain-name1 [domain-name2...
domain-nameN] | none}
hostname(config-group-policy)# no split-dns [domain-name domain-name2 domain-nameN]
```

ドメインのリスト内で各エントリを区切るには、スペースを 1 つ入力します。エントリ数に制限はありませんが、ストリング全体の長さは 255 文字以下にします。英数字、ハイフン（-）、およびピリオド（.）のみを使用できます。デフォルト ドメイン名がトンネルを介して解決される場合は、そのドメイン名をこのリストに明示的に含める必要があります。

次の例は、FirstGroup という名前のグループ ポリシーで、Domain1、Domain2、Domain3、Domain4 の各ドメインがスプリット トンネリングを介して解決されるように設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# split-dns value Domain1 Domain2 Domain3 Domain4
```

（注）　スプリット DNS を設定する場合、指定したプライベート DNS サーバが、クライアント プラットフォームに設定されている DNS サーバと重複していないことを確認します。重複していると、名前解決が正しく動作せず、クエリーがドロップされる可能性があります。

Windows XP およびスプリット トンネリング用の DHCP 代行受信の設定

スプリット トンネル オプションが 255 バイトを超えていると、Microsoft XP で異常が発生し、ドメイン名が破損します。この問題を回避するには、ASA で送信ルートの数を 27 ～ 40 に制限します。ルートの数はルートのクラスによって異なります。

DHCP 代行受信を使用することにより、Microsoft Windows XP クライアントで ASA とともにスプリット トンネリングを使用できます。ASA は、Microsoft Windows XP クライアント DHCP Inform メッセージに直接応答して、クライアントにトンネル IP アドレス用のサブネット マスク、ドメイン名、およびクラスレス スタティック ルートを提供します。Windows XP 以前の Windows クライアントの場合、DHCP 代行受信によってドメイン名とサブネット マスクが提供されます。これは、DHCP サーバを使用するのが効果的でない環境で役立ちます。

intercept-dhcp コマンドは、DHCP 代行受信をイネーブルまたはディセーブルにします。

```
hostname(config-group-policy)# intercept-dhcp netmask {enable | disable}
hostname(config-group-policy)#
```

netmask 変数で、トンネル IP アドレスのサブネット マスクを提供します。このコマンドの **no** 形式は、コンフィギュレーションから DHCP 代行受信を削除します。

```
[no] intercept-dhcp
```

次に、FirstGroup というグループ ポリシーに DHCP 代行受信を設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# intercept-dhcp enable
```

Web Security のスプリット除外ポリシーの設定

Cloud Web Security に関する情報

AnyConnect Web Security モジュールとは、Cisco Cloud Web Security が HTTP トラフィックを評価する Cisco Cloud Web Security スキャニング プロキシに、そのトラフィックをルーティングするエンドポイント コンポーネントのことです。同時に各要素を分析できるように、Cisco Cloud Web Security は Web ページの要素を分解します。これにより、潜在的に危険なコンテンツがブロックされ、問題のないコンテンツが通過します。

多数の Cisco Cloud Web Security スキャニング プロキシが世界各国に普及することで、AnyConnect Web Security を活用するユーザは、遅延を最小限に抑えるために、応答時間が最も早い Cisco Cloud Web Security スキャニング プロキシにトラフィックをルーティングできます。

ユーザが VPN セッションを確立すると、すべてのネットワーク トラフィックが VPN トンネルを介して送信されます。ただし、AnyConnect ユーザが Web Security を使用している場合は、エンドポイントから送信される HTTP トラフィックをトンネルから除外し、Cloud Web Security スキャニング プロキシに直接送信する必要があります。

Cisco Cloud Web Security スキャニング プロキシのためのトラフィックのスプリット トンネル除外を設定するには、グループ ポリシーの **[Set up split exclusion for Web Security]** ボタンを使用します。

前提条件

- ASDM を使用して ASA にアクセスできる必要があります。この手順は、コマンドライン インターフェイスを使用して実行できません。
- AnyConnect クライアントで使用するために Web Security を設定する必要があります。『*AnyConnect Secure Mobility Client Administrator Guide*』の「Configuring Web Security」を参照してください。
- グループ ポリシーを作成し、Web Security を使用して設定された AnyConnect クライアント用の接続プロファイルにそれを割り当てている必要があります。

手順の詳細

ステップ 1　設定するヘッド エンドの ASDM セッションを開始し、[Remote Access VPN] > [Configuration] > [Group Policies] の順に選択します。

ステップ 2　設定するグループ ポリシーを選択し、[Edit] をクリックします。

ステップ 3　[Advanced] > [Split Tunneling] を選択します。

ステップ 4　[Set up split exclusion for Web Security] を選択します。

ステップ 5　Web Security のスプリット除外に使用される新しい ACL を入力するか、既存のアクセス リストを選択します。ASDM は、ネットワーク リストで使用する ACL を設定します。

ステップ 6　新しいリストには [Create Access List for a new list] をクリックし、既存のリストには [Update Access List for an existing list] をクリックします。

ステップ 7　**[OK]** をクリックします。

次の実施手順

追加スキャニング プロキシを追加した場合は、この手順で作成した統合 ACL を新しい情報で更新します。

リモート アクセス クライアントで使用するためのブラウザ プロキシ設定の設定

クライアントのプロキシ サーバ パラメータを設定するには、次の手順を実行します。

ステップ 1　グループ ポリシー コンフィギュレーション モードで **msie-proxy server** コマンドを入力し、クライアント デバイスのブラウザのプロキシ サーバとポート番号を設定します。

```
hostname(config-group-policy)# msie-proxy server {value server[:port] | none}
hostname(config-group-policy)#
```

デフォルト値は **none** です。コンフィギュレーションから属性を削除するには、このコマンドの **no** 形式を使用します。

```
hostname(config-group-policy)# no msie-proxy server
hostname(config-group-policy)#
```

プロキシ サーバの IP アドレスまたはホスト名およびポート番号が含まれている行の長さは、100 文字未満である必要があります。

次に、ブラウザ プロキシ サーバとして IP アドレス 192.168.10.1 を設定し、ポート 880 を使用し、FirstGroup というグループ ポリシーを対象にする例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# msie-proxy server value 192.168.21.1:880
hostname(config-group-policy)#
```

ステップ 2　グループ ポリシー コンフィギュレーション モードで **msie-proxy method** コマンドを入力して、クライアント デバイスのブラウザ プロキシ アクション（「メソッド」）を設定します。

```
hostname(config-group-policy)# msie-proxy method [auto-detect | no-modify | no-proxy |
use-server]
hostname(config-group-policy)#
```

デフォルト値は **use-server** です。コンフィギュレーションから属性を削除するには、このコマンドの **no** 形式を使用します。

```
hostname(config-group-policy)# no msie-proxy method [auto-detect | no-modify | no-proxy |
use-server]
hostname(config-group-policy)#
```

使用できるメソッドは、次のとおりです。

- **auto-detect**：クライアント デバイスのブラウザでプロキシ サーバの自動検出の使用をイネーブルにします。
- **no-modify**：このクライアント デバイスで使用しているブラウザの HTTP ブラウザ プロキシ サーバの設定をそのままにします。
- **no-proxy**：クライアント デバイスで使用しているブラウザの HTTP プロキシの設定をディセーブルにします。
- **use-server**：**msie-proxy server** コマンドに設定された値を使用するように、ブラウザの HTTP プロキシ サーバ設定を設定します。

プロキシ サーバの IP アドレスまたはホスト名およびポート番号が含まれている行の長さは、100 文字未満である必要があります。

次に、FirstGroup というグループ ポリシーのブラウザ プロキシ設定として自動検出を設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# msie-proxy method auto-detect
hostname(config-group-policy)#
```

次に、クライアント デバイスのサーバとしてサーバ QASERVER、ポート 1001 を使用するように、FirstGroup というグループ ポリシーのブラウザ プロキシ設定を設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# msie-proxy server QAserver:port 1001
hostname(config-group-policy)# msie-proxy method use-server
hostname(config-group-policy)#
```

ステップ 3　グループ ポリシー コンフィギュレーション モードで **msie-proxy except-list** コマンドを入力して、クライアント デバイスのブラウザがローカルでプロキシをバイパスするために使用するプロキシの例外リストを設定します。これらのアドレスは、プロキシ サーバによってアクセスされません。このリストは、[Proxy Stteings] ダイアログボックスにある [Exceptions] ボックスに相当します。

```
hostname(config-group-policy)# msie-proxy except-list {value server[:port] | none}
hostname(config-group-policy)#
```

コンフィギュレーションから属性を削除するには、このコマンドの **no** 形式を使用します。

```
hostname(config-group-policy)# no msie-proxy except-list
hostname(config-group-policy)#
```

- **value** *server:port* : このクライアント デバイスに適用する MSIE サーバの IP アドレスまたは名前、およびポートを指定します。ポート番号は任意です。
- **none** : IP アドレスまたはホスト名とポートがないことを示し、例外リストを継承しません。

デフォルトでは、msie-proxy except-list はディセーブルになっています。

プロキシ サーバの IP アドレスまたはホスト名およびポート番号が含まれている行の長さは、100 文字未満である必要があります。

次に、ブラウザのプロキシ例外リストを設定する例を示します。IP アドレス 192.168.20.1 のサーバで構成され、ポート 880 を使用し、FirstGroup というグループ ポリシーを対象とします。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# msie-proxy except-list value 192.168.20.1:880
hostname(config-group-policy)#
```

ステップ 4　グループ ポリシー コンフィギュレーション モードで **msie-proxy local-bypass** コマンドを入力し、クライアント デバイスで使用するブラウザが、プロキシをローカルでバイパスする設定をイネーブルまたはディセーブルにします。

```
hostname(config-group-policy)# msie-proxy local-bypass {enable | disable}
hostname(config-group-policy)#
```

コンフィギュレーションから属性を削除するには、このコマンドの **no** 形式を使用します。

```
hostname(config-group-policy)# no msie-proxy local-bypass {enable | disable}
hostname(config-group-policy)#
```

デフォルトでは、msie-proxy local-bypass はディセーブルになっています。

次に、FirstGroup というグループ ポリシーのブラウザのプロキシ ローカル バイパスをイネーブルにする例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# msie-proxy local-bypass enable
hostname(config-group-policy)#
```

AnyConnect Secure Mobility Client 接続のグループ ポリシー属性の設定

第 10 章「AnyConnect VPN Client 接続」に示すように、AnyConnect クライアント接続をイネーブルにした後は、グループ ポリシーの AnyConnect 機能をイネーブルまたは必須にできます。グループ ポリシー webvpn コンフィギュレーション モードで次の手順を実行します。

ステップ 1　グループ ポリシー webvpn コンフィギュレーション モードを開始します。次に例を示します。

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
```

ステップ 2　エンドポイント コンピュータ上で AnyConnect クライアントの永続的なインストールをディセーブルにするには、**none** キーワードで **anyconnect keep-installer** コマンドを使用します。次に例を示します。

```
hostname(config-group-webvpn)# anyconnect keep-installer none
hostname(config-group-webvpn)#
```

デフォルトでは、クライアントの永続的なインストールはイネーブルになっています。クライアントは、AnyConnect セッションの終了時にエンドポイントにインストールされたままになります。

ステップ 3　グループ ポリシーの AnyConnect SSL 接続経由で HTTP データの圧縮をイネーブルにするには、**anyconnect ssl compression** コマンドを入力します。デフォルトでは、圧縮は **none**（ディセーブル）に設定されています。圧縮をイネーブルにするには、**deflate** キーワードを使用します。次に例を示します。

```
hostname(config-group-webvpn)# anyconnect compression deflate
hostname(config-group-webvpn)#
```

ステップ 4　ASA で Dead Peer Detection（DPD; デッド ピア検出）をイネーブルにし、AnyConnect または ASA が DPD を実行する頻度を設定するには、**anyconnect dpd-interval** コマンドを使用します。

anyconnect dpd-interval {[**gateway** {*seconds* | **none**}] | [**client** {*seconds* | **none**}]}

デフォルトでは、ASA と AnyConnect クライアントの両方が 30 秒間隔で DPD を実行します。

gateway は、ASA のことです。ASA が DPD テストを実行する頻度を、30 ～ 3600 秒（1 時間）の範囲で指定できます。**none** を指定すると、ASA が実行する DPD テストはディセーブルになります。値 300 が推奨されます。

client は、AnyConnect クライアントのことです。クライアントが DPD テストを実行する頻度は、30 ～ 3600 秒（1 時間）の範囲で指定できます。**none** を指定すると、クライアントが実行する DPD テストはディセーブルになります。値 30 が推奨されます。

次の例では、ASA（ゲートウェイ）で実行される DPD の頻度を 300 秒に設定し、クライアントで実行される DPD の頻度を 30 秒に設定します。

```
hostname(config-group-webvpn)# anyconnect dpd-interval gateway 300
hostname(config-group-webvpn)# anyconnect dpd-interval client 30
hostname(config-group-webvpn)#
```

ステップ 5　デバイスが接続のアイドル状態を維持する時間を制限する場合でも、**anyconnect ssl keepalive** コマンドを使用してキープアライブ メッセージの頻度を調整することで、プロキシ、ファイアウォール、または NAT デバイス経由の AnyConnect 接続を開いたままにすることができます。

anyconnect ssl keepalive {none | *seconds***}**

また、キープアライブを調整すると、リモート ユーザが Microsoft Outlook または Microsoft Internet Explorer などのソケットベース アプリケーションをアクティブに実行していない場合でも、AnyConnect クライアントは切断および再接続されません。

次の例では、AnyConnect クライアントがキープアライブ メッセージを 300 秒（5 分）の頻度で送信できるようにセキュリティ アプライアンスを設定します。

```
hostname(config-group-webvpn)# anyconnect ssl keepalive 300
hostname(config-group-webvpn)#
```

ステップ 6　AnyConnect クライアントが SSL セッションでキーを再生成できるようにするには、**anyconnect ssl rekey** コマンドを使用します。

anyconnect ssl rekey {**method** {**ssl** | **new-tunnel**} | **time** *minutes* | **none**}}

デフォルトでは、キー再生成はディセーブルになっています。

method を new-tunnel に指定すると、SSL キーの再生成中に AnyConnect クライアントが新しいトンネルを確立することが指定されます。method を **none** に指定すると、キー再生成はディセーブルになります。method を **ssl** に指定すると、SSL の再ネゴシエーションはキー再生成中に行われます。method を指定する代わりに、セッションの開始からキー再生成が行われるまでの時間を 1 ～ 10080（1 週間）の分数で指定できます。

次の例では、キー再生成中に AnyConnect クライアントが SSL と再ネゴシエートするように設定し、キー再生成がセッション開始の 30 分後に発生するように設定しています。

```
hostname(config-group-webvpn)# anyconnect ssl rekey method ssl
hostname(config-group-webvpn)# anyconnect ssl rekey time 30
hostname(config-group-webvpn)#
```

ステップ 7　クライアント プロトコル バイパス機能を使用すると、ASA が IPv6 トラフィックだけを予期しているときの IPv4 トラフィックの管理方法や、IPv4 トラフィックだけを予期しているときの IPv6 トラフィックの管理方法を設定することができます。

AnyConnect クライアントが ASA に VPN 接続するときに、ASA は IPv4 と IPv6 の一方または両方のアドレスを割り当てます。ASA が AnyConnect 接続に IPv4 アドレスまたは IPv6 アドレスだけを割り当てた場合に、ASA が IP アドレスを割り当てなかったネットワーク トラフィックについて、クライアント プロトコル バイパスによってそのトラフィックをドロップさせるか、または ASA をバイパスしてクライアントからの暗号化なし、つまり「クリア テキスト」としての送信を許可するかを設定できるようになりました。

たとえば、IPv4 アドレスのみ AnyConnect 接続に割り当てられ、エンドポイントがデュアル スタックされていると想定してください。このエンドポイントが IPv6 アドレスへの到達を試みたときに、クライアント バイパス プロトコル機能がディセーブルの場合は、IPv6 トラフィックがドロップされますが、クライアント バイパス プロトコルがイネーブルの場合は、IPv6 トラフィックはクライアントからクリア テキストとして送信されます。

client-bypass-protocol コマンドを使用して、クライアント バイパス プロトコル機能をイネーブルまたはディセーブルにします。コマンド構文は次のとおりです。

client-bypass-protocol {enable | disable}

次に、クライアント バイパス プロトコルをイネーブルにする例を示します。

```
hostname(config-group-policy)# client-bypass-protocol enable
hostname(config-group-policy)#
```

次に、クライアント バイパス プロトコルをデイセーブルにする例を示します。

```
hostname(config-group-policy)# client-bypass-protocol disable
hostname(config-group-policy)#
```

次に、イネーブルまたはディセーブルになっているクライアント バイパス プロトコル設定を削除する例を示します。

```
hostname(config-group-policy)# no client-bypass-protocol enable
hostname(config-group-policy)#
```

ステップ 8　ASA 間にロード バランシングを設定した場合は、VPN セッションの再確立に使用される ASA IP アドレスを解決するために、ASA の FQDN を指定します。この設定は、さまざまな IP プロトコルのネットワーク間のクライアント ローミングをサポートするうえで重要です（IPv4 から IPv6 など）。

AnyConnect プロファイルにある ASA FQDN を使用してローミング後に ASA IP アドレスを取得することはできません。アドレスがロード バランシング シナリオの正しいデバイス（トンネルが確立されているデバイス）と一致しない場合があります。

デバイスの FQDN がクライアントに配信されない場合、クライアントは、以前にトンネルが確立されている IP アドレスへの再接続を試みます。異なる IP プロトコル（IPv4 から IPv6）のネットワーク間のローミングをサポートするには、AnyConnect は、トンネルの再確立に使用する ASA アドレスを決定できるように、ローミング後にデバイス FQDN の名前解決を行う必要があります。クライアントは、初期接続中にプロファイルに存在する ASA FQDN を使用します。以後のセッション再接続では、常に、ASA によってプッシュされた（また、グループ ポリシーで管理者が設定した）デバイス FQDN を使用します（使用可能な場合）。FQDN が設定されていない場合、ASA は、[Device Setup] > [Device Name/Password and Domain Name] の設定内容からデバイス FQDN を取得（およびクライアントに送信）します。

デバイス FQDN が ASA によってプッシュされていない場合、クライアントは、異なる IP プロトコルのネットワーク間のローミング後に VPN セッションを再確立できません。

gateway-fqdn コマンドを使用して、ASA の FQDN を設定します。コマンド構文は次のとおりです。

```
gateway-fqdn value {FQDN_Name | none}
no gateway-fqdn
```

次に、ASA の FQDN を ASAName.example.cisco.com として定義する例を示します。

```
hostname(config-group-policy)# gateway-fqdn value ASAName.example.cisco.com
hostname(config-group-policy)#
```

次に、グループ ポリシーから ASA の FQDN を削除する例を示します。グループ ポリシーは、デフォルト グループ ポリシーからこの値を継承します。

```
hostname(config-group-policy)# no gateway-fqdn
hostname(config-group-policy)#
```

次に、FQDN を空の値として定義する例を示します。hostname コマンドおよび domain-name コマンドを使用して設定されたグローバル FQDN が使用されます（使用可能な場合）。

```
hostname(config-group-policy)# gateway-fqdn none
hostname(config-group-policy)#
```

IPSec（IKEv1）クライアントのグループ ポリシー属性の設定

IPSec（IKEv1）クライアントのセキュリティ属性の設定

グループのセキュリティ設定を指定するには、次の手順を実行します。

ステップ 1　グループ ポリシー コンフィギュレーション モードで、**enable** キーワードを指定して **password-storage** コマンドを使用し、ユーザがログイン パスワードをクライアント システムに保存できるようにするかどうかを指定します。パスワード保存をディセーブルにするには、**disable** キーワードを指定して **password-storage** コマンドを使用します。

```
hostname(config-group-policy)# password-storage {enable | disable}
hostname(config-group-policy)#
```

セキュリティ上の理由から、パスワード保存はデフォルトでディセーブルになっています。セキュア サイトにあることがわかっているシステム上でのみ、パスワード保存をイネーブルにしてください。

password-storage 属性を実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を入力します。

```
hostname(config-group-policy)# no password-storage
hostname(config-group-policy)#
```

no 形式を指定すると、password-storage の値を別のグループ ポリシーから継承することができます。

このコマンドは、ハードウェア クライアントのインタラクティブ ハードウェア クライアント認証または個別ユーザ認証には関係ありません。

次に、FirstGroup という名前のグループ ポリシーに対してパスワード保存をイネーブルにする例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# password-storage enable
hostname(config-group-policy)#
```

ステップ 2　デフォルトではディセーブルになっている IP 圧縮をイネーブルにするかどうかを指定します。

（注）　IPSec IKEv2 接続では、IP 圧縮はサポートされていません。

```
hostname(config-group-policy)# ip-comp {enable | disable}
hostname(config-group-policy)#
```

LZS IP 圧縮をイネーブルにするには、グループ ポリシー コンフィギュレーション モードで、**enable** キーワードを指定して **ip-comp** コマンドを入力します。IP 圧縮をディセーブルにするには、**disable** キーワードを指定して **ip-comp** コマンドを入力します。

ip-comp 属性を実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を入力します。これにより、別のグループ ポリシーの値を継承できます。

```
hostname(config-group-policy)# no ip-comp
hostname(config-group-policy)#
```

データ圧縮をイネーブルにすると、モデムで接続するリモート ダイヤルイン ユーザのデータ伝送レートが向上する場合があります。

注意　データ圧縮を使用すると、ユーザ セッションごとのメモリ要求と CPU 使用率が増加し、結果として ASA のスループット全体が低下します。そのため、データ圧縮はモデムで接続しているリモート ユーザに対してだけイネーブルにすることを推奨します。モデム ユーザに固有のグループ ポリシーを設計し、それらのユーザに対してだけ圧縮をイネーブルにします。

ステップ 3　グループ ポリシー コンフィギュレーション モードで、**enable** キーワードを指定して **re-xauth** コマンドを使用し、IKE キーが再生成される際にユーザが再認証を受ける必要があるかどうかを指定します。

（注）　IKEv2 接続では、IKE キー再生成はサポートされていません。

IKE キー再生成時の再認証をイネーブルにすると、ASA では、最初のフェーズ 1 IKE ネゴシエーションにおいてユーザに対してユーザ名とパスワードの入力が求められ、その後 IKE キー再生成が行われるたびにユーザ認証が求められます。再認証によって、セキュリティが強化されます。

設定されているキー再生成間隔が極端に短い場合、ユーザは認証を繰り返し求められることに不便を感じることがあります。認可要求が何度も繰り返されないようにするには、再認証をディセーブルにします。設定されているキー再生成インターバルを確認するには、モニタリング モードで **show crypto ipsec sa** コマンドを入力して、セキュリティ アソシエーションの秒単位のライフタイム、およびデータのキロバイト単位のライフタイムを表示します。IKE キーが再生成される際のユーザの再認証をディセーブルにするには、**disable** キーワードを入力します。IKE キーが再生成される際の再認証は、デフォルトではディセーブルになっています。

```
hostname(config-group-policy)# re-xauth {enable | disable}
hostname(config-group-policy)#
```

IKE キーが再生成される際の再認証用の値を別のグループ ポリシーから継承することをイネーブルにするには、このコマンドの **no** 形式を入力して、実行コンフィギュレーションから re-xauth 属性を削除します。

```
hostname(config-group-policy)# no re-xauth
hostname(config-group-policy)#
```

（注）　接続先にユーザが存在しない場合、再認証は失敗します。

ステップ 4　完全転送秘密をイネーブルにするかどうかを指定します。IPsec ネゴシエーションでは、完全転送秘密により、新しい各暗号キーは以前のどのキーとも関連性がないことが保証されます。グループ ポリシーは、別のグループ ポリシーから完全転送秘密の値を継承できます。完全転送秘密は、デフォルトではディセーブルになっています。完全転送秘密をイネーブルにするには、グループ ポリシー コンフィギュレーション モードで、**enable** キーワードを指定して **pfs** コマンドを使用します。

```
hostname(config-group-policy)# pfs {enable | disable}
hostname(config-group-policy)#
```

完全転送秘密をディセーブルにするには、**disable** キーワードを指定して **pfs** コマンドを入力します。

完全転送秘密属性を実行コンフィギュレーションから削除して、値を継承しないようにするには、このコマンドの **no** 形式を入力します。

```
hostname(config-group-policy)# no pfs
hostname(config-group-policy)#
```

IKEv1 クライアントの IPsec-UDP 属性の設定

IPsec over UDP（IPsec through NAT と呼ばれることもあります）を使用すると、Cisco VPN Client またはハードウェア クライアントは、NAT を実行している ASA に UDP 経由で接続できます。この機能はデフォルトではディセーブルになっています。IPsec over UDP は、リモート アクセス接続だけに適用される専用の機能で、モード コンフィギュレーションが必要です。ASA は、SA のネゴシエート時にクライアントとの間でコンフィギュレーション パラメータをやり取りします。IPSec over UDP を使用すると、システム パフォーマンスが若干低下します。

IPsec over UDP をイネーブルにするには、グループ ポリシー コンフィギュレーション モードで、次のように **enable** キーワードを指定して **ipsec-udp** コマンドを設定します。

```
hostname(config-group-policy)# ipsec-udp {enable | disable}
hostname(config-group-policy)# no ipsec-udp
```

IPsec over UDP を使用するには、この項の説明に従って、**ipsec-udp-port** コマンドも設定する必要があります。

IPsec over UDP をディセーブルにするには、**disable** キーワードを入力します。IPSec over UDP 属性を実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を入力します。これにより、別のグループ ポリシーから IPSec over UDP の値を継承できるようになります。

また、IPsec over UDP を使用するように Cisco VPN Client を設定しておく必要があります（Cisco VPN Client は、デフォルトで IPsec over UDP を使用するように設定されています）。VPN 3002 では、IPsec over UDP を使用するためのコンフィギュレーションが必要ありません。

次に、FirstGroup というグループ ポリシーの IPSec over UDP を設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# ipsec-udp enable
```

IPsec over UDP をイネーブルにした場合は､グループ ポリシー コンフィギュレーション モードで **ipsec-udp-port** コマンドも設定する必要があります。このコマンドにより、IPSec over UDP 用の UDP ポート番号が設定されます。IPSec ネゴシエーションでは、ASA は設定されたポートでリッスンし、他のフィルタ ルールで UDP トラフィックがドロップされていても、そのポート宛ての UDP トラフィックを転送します。ポート番号の範囲は 4001 ～ 49151 です。デフォルトのポート値は 10000 です。

UDP ポートをディセーブルにするには、このコマンドの **no** 形を入力します。これにより、別のグループ ポリシーから IPsec over UDP ポートの値を継承できるようになります。

```
hostname(config-group-policy)# ipsec-udp-port port
```

次に、FirstGroup というグループ ポリシーの IPsec UDP ポートをポート 4025 に設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# ipsec-udp-port 4025
```

VPN ハードウェア クライアントの属性の設定

この項では、セキュア ユニット認証およびユーザ認証をイネーブルまたはディセーブルにし、VPN ハードウェア クライアントのユーザ認証タイムアウト値を設定する方法について説明します。これらのコマンドは、Cisco IP Phone および LEAP パケットで個別のユーザ認証をバイパスすることを許可し、ネットワーク拡張モードを使用するハードウェア クライアントの接続を許可することもできます。

セキュア ユニット認証の設定

セキュア ユニット認証では、VPN ハードウェア クライアントがトンネルを開始するたびにユーザ名とパスワードを使用した認証を要求することで、セキュリティが強化されます。この機能をイネーブルにすると、ハードウェア クライアントではユーザ名とパスワードが保存されません。セキュア ユニット認証はデフォルトでディセーブルになっています。

（注） この機能をイネーブルにした場合に VPN トンネルを確立するには、ユーザがユーザ名とパスワードを入力する必要があります。

セキュア ユニット認証では、ハードウェア クライアントが使用する接続プロファイルに対して認証サーバ グループが設定されている必要があります。プライマリ ASA でセキュア ユニット認証が必要な場合は、すべてのバックアップ サーバに対してもセキュア ユニット認証を設定する必要があります。

グループ ポリシー コンフィギュレーション モードで、**enable** キーワードを指定して **secure-unit-authentication** コマンドを入力し、セキュア ユニット認証をイネーブルにするかどうかを指定します。

```
hostname(config-group-policy)# secure-unit-authentication {enable | disable}
hostname(config-group-policy)# no secure-unit-authentication
```

セキュア ユニット認証をディセーブルにするには、**disable** キーワードを入力します。セキュア ユニット認証の属性を実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を入力します。このオプションを指定すると、他のグループ ポリシーからセキュア ユニット認証の値を継承できます。

次に、FirstGroup という名前のグループ ポリシーに対して、セキュア ユニット認証をイネーブルにする例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# secure-unit-authentication enable
```

ユーザ認証の設定

ユーザ認証はデフォルトでディセーブルになっています。ユーザ認証をイネーブルにすると、ハードウェア クライアントの背後にいる個々のユーザは、トンネルを介してネットワークにアクセスするために認証を受けることが必要となります。個々のユーザは、設定した認証サーバの順序に従って認証されます。

グループ ポリシー コンフィギュレーション モードで、**enable** キーワードを指定して **user-authentication** コマンドを入力し、ユーザ認証をイネーブルにするかどうかを指定します。

```
hostname(config-group-policy)# user-authentication {enable | disable}
hostname(config-group-policy)# no user-authentication
```

ユーザ認証をディセーブルにするには、**disable** キーワードを入力します。ユーザ認証属性を実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を入力します。このオプションを使用すると、別のグループ ポリシーからユーザ認証の値を継承できます。

プライマリ ASA でユーザ認証が必要な場合は、バックアップ サーバでも同様にユーザ認証を設定する必要があります。

次の例は、FirstGroup という名前のグループ ポリシーのユーザ認証をイネーブルにする方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# user-authentication enable
```

アイドル タイムアウトの設定

グループ ポリシー コンフィギュレーション モードで **user-authentication-idle-timeout** コマンドを入力して、ハードウェア クライアントの背後の個々のユーザにアイドル タイムアウトを設定します。アイドル タイムアウト期間中にハードウェア クライアントの背後のユーザによる通信アクティビティがない場合、ASA はそのクライアントのアクセスを終了します。

```
hostname(config-group-policy)# user-authentication-idle-timeout {minutes | none}
hostname(config-group-policy)# no user-authentication-idle-timeout
```

（注） このタイマーは、VPN トンネル自体ではなく、VPN トンネルを通過するクライアントのアクセスだけを終了します。

show uauth コマンドへの応答で示されるアイドル タイムアウトは、常に Cisco Easy VPN リモート デバイスのトンネルを認証したユーザのアイドル タイムアウト値になります。

minutes パラメータで、アイドル タイムアウト時間（分単位）を指定します。最短時間は 1 分、デフォルトは 30 分、最長時間は 35791394 分です。

アイドル タイムアウト値を削除するには、このコマンドの **no** 形式を入力します。このオプションを使用すると、他のグループ ポリシーからアイドル タイムアウト値を継承できます。

アイドル タイムアウト値を継承しないようにするには、**none** キーワードを指定して **user-authentication-idle-timeout** コマンドを入力します。このコマンドにより、アイドル タイムアウトにヌル値が設定されます。この設定によってアイドル タイムアウトが拒否され、デフォルトまたは指定されたグループ ポリシーからユーザ認証のアイドル タイムアウト値が継承されなくなります。

次の例は、FirstGroup という名前のグループ ポリシーに 45 分のアイドル タイムアウト値を設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# user-authentication-idle-timeout 45
```

IP Phone Bypass の設定

Cisco IP Phone は、ハードウェア クライアントの背後の個別のユーザ認証をバイパスさせることができます。IP Phone Bypass をイネーブルにするには、グループ ポリシー コンフィギュレーション モードで、**enable** キーワードを指定して **ip-phone-bypass** コマンドを入力します。IP Phone Bypass を使用すると、ハードウェア クライアントの背後にある IP フォンが、ユーザ認証プロセスなしで接続できます。IP Phone Bypass は、デフォルトでディセーブルになっています。イネーブルの場合、セキュア ユニット認証は有効のままになります。

IP Phone Bypass をディセーブルにするには、**disable** キーワードを入力します。IP Phone Bypass 属性を実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を入力します。このオプションを使用すると、IP Phone Bypass の値を別のグループ ポリシーから継承できます。

```
hostname(config-group-policy)# ip-phone-bypass {enable | disable}
hostname(config-group-policy)# no ip-phone-bypass
```

（注） mac-exempt を設定してクライアントの認証を免除する必要があります。

LEAP Bypass の設定

LEAP Bypass がイネーブルの場合、VPN 3002 ハードウェア クライアントの背後の無線デバイスからの LEAP パケットは、ユーザ認証の前に VPN トンネルを通過します。このアクションによって、Cisco ワイヤレス アクセス ポイント デバイスを使用するワークステーションは、LEAP 認証を確立し、その後ユーザ認証ごとに認証を再度実行できます。LEAP Bypass は、デフォルトでディセーブルになっています。

シスコ ワイヤレス アクセス ポイントからの LEAP パケットが個々のユーザ認証をバイパスできるようにするには、グループ ポリシー コンフィギュレーション モードで **enable** キーワードを指定して **leap-bypass** コマンドを入力します。LEAP Bypass をディセーブルにするには、**disable** キーワードを入力します。LEAP Bypass の属性を実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を入力します。このオプションを使用すると、LEAP Bypass の値を別のグループ ポリシーから継承できます。

```
hostname(config-group-policy)# leap-bypass {enable | disable}
hostname(config-group-policy)# no leap-bypass
```

（注） IEEE 802.1X は、有線および無線ネットワークにおける認証規格です。この規格では、クライアントと認証サーバの間で強力な相互認証を実現し、ユーザ単位およびセッション単位のダイナミックな無線暗号化秘密（WEP）キーの使用を可能にして、スタティックな WEP キーの場合に介在する面倒な管理作業やセキュリティ上の問題を軽減することができます。

シスコは、Cisco LEAP と呼ばれる 802.1X 無線認証タイプを開発しました。LEAP（Lightweight Extensible Authentication Protocol）は、無線クライアントと RADIUS サーバの間の接続における相互認証を実装します。パスワードなど、認証に使用されるクレデンシャルは、ワイヤレス媒体を経由して送信される前に必ず暗号化されます。

Cisco LEAP では、無線クライアントを RADIUS サーバに対して認証します。RADIUS アカウンティング サービスは提供されません。

インタラクティブ ハードウェア クライアント認証をイネーブルにした場合、この機能は正常に動作しません。

注意 認証されていないトラフィックがトンネルを通過できるようにすると、ネットワークにセキュリティ リスクを招くおそれがあります。

次の例は、FirstGroup という名前のグループ ポリシーに LEAP Bypass を設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# leap-bypass enable
```

ネットワーク拡張モードのイネーブル化

ネットワーク拡張モードを使用すると、ハードウェア クライアントは、単一のルーティング可能なネットワークを VPN トンネルを介してリモート プライベート ネットワークに提供できます。IPSec は、ハードウェア クライアントの背後にあるプライベート ネットワークから ASA の背後にあるネットワークへのトラフィックをすべてカプセル化します。PAT は適用されません。したがって、ASA の背後にあるデバイスは、ハードウェア クライアントの背後にある、トンネルを介したプライベート ネットワーク上のデバイスに直接アクセスできます。これはトンネルを介した場合に限ります。逆の場合も同様です。トンネルはハードウェア クライアントによって開始される必要がありますが、トンネルがアップ状態になったあとは、いずれの側もデータ交換を開始できます。

グループ ポリシー コンフィギュレーション モードで、**enable** キーワードを指定して **nem** コマンドを入力し、ハードウェア クライアントのネットワーク拡張モード（NEM）をイネーブルにします。

```
hostname(config-group-policy)# nem {enable | disable}
hostname(config-group-policy)# no nem
```

NEM をディセーブルにするには、**disable** キーワードを入力します。この NEM の属性を実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を入力します。このオプションを使用すると、別のグループ ポリシーの値を継承できます。

次に、FirstGroup というグループ ポリシーの NEM を設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# nem enable
```

バックアップ サーバ属性の設定

バックアップ サーバを設定します（使用する予定がある場合）。IPsec バックアップ サーバを使用すると、VPN クライアントはプライマリ ASA が使用不可の場合も中央サイトに接続することができます。バックアップ サーバを設定すると、ASA は、IPsec トンネルを確立するときにクライアントにサーバ リストを渡します。クライアント上またはプライマリ ASA 上にバックアップ サーバを設定しない限り、バックアップ サーバは存在しません。

バックアップ サーバは、クライアント上またはプライマリ ASA 上に設定します。ASA 上にバックアップ サーバを設定すると、適応型セキュリティ アプライアンスは、バックアップ サーバ ポリシーをグループ内のクライアントにプッシュして、クライアント上にバックアップ サーバ リストが設定されている場合、そのリストを置き換えます。

（注） ホスト名を使用する場合は、バックアップ DNS サーバおよびバックアップ WINS サーバを、プライマリ DNS サーバおよびプライマリ WINS サーバとは別のネットワーク上に配置することを推奨します。このようにしないと、ハードウェア クライアントの背後のクライアントが DHCP を介してハードウェア クライアントから DNS 情報および WINS 情報を取得している場合、プライマリ サーバとの接続が失われ、バックアップ サーバに異なる DNS 情報と WINS 情報があると、DHCP リースが期限切れになるまでクライアントを更新できなくなります。また、ホスト名を使用している場合に DNS サーバが使用不可になると、大幅な遅延が発生するおそれがあります。

バックアップ サーバを設定するには、グループ ポリシー コンフィギュレーション モードで **backup-servers** コマンドを入力します。

```
hostname(config-group-policy)# backup-servers {server1 server2... server10 |
clear-client-config | keep-client-config}
```

バックアップ サーバを削除するには、バックアップ サーバを指定してこのコマンドの **no** 形式を入力します。backup-servers 属性を実行コンフィギュレーションから削除し、backup-servers の値を他のグループ ポリシーから継承できるようにするには、引数を指定せずにこのコマンドの **no** 形式を入力します。

```
hostname(config-group-policy)# no backup-servers [server1 server2... server10 |
clear-client-config | keep-client-config]
```

clear-client-config キーワードは、クライアントでバックアップ サーバを使用しないことを指定します。ASA は、ヌルのサーバ リストをプッシュします。

keep-client-config キーワードは、ASA がバックアップ サーバ情報をクライアントに送信しないことを指定します。クライアントは、独自のバックアップ サーバ リストを使用します（設定されている場合）。これはデフォルトです。

server1 server 2....server10 パラメータ リストは、プライマリの ASA が使用不可の場合に VPN クライアントが使用するサーバをプライオリティ順にスペースで区切ったリストです。このリストには、サーバを IP アドレスまたはホスト名で指定します。このリストの長さは 500 文字までで、格納できるエントリは最大 10 個までです。

次の例は、FirstGroup という名前のグループ ポリシーに、IP アドレスが 10.10.10.1 と 192.168.10.14 であるバックアップ サーバを設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# backup-servers 10.10.10.1 192.168.10.14
```

ネットワーク アドミッション コントロールのパラメータの設定

この項で説明するグループ ポリシー NAC コマンドには、すべてデフォルトの値があります。どうしても必要な場合を除き、これらのパラメータのデフォルト値は変更しないでください。

ASA は、拡張認証プロトコル（EAP）over UDP（EAPoUDP）のメッセージを使用して、リモート ホストのポスチャを確認します。ポスチャ検証では、リモート ホストにネットワーク アクセス ポリシーを割り当てる前に、そのホストがセキュリティの必要条件を満たしているかどうかが調べられます。セキュリティ アプライアンスでネットワーク アドミッション コントロールを設定する前に、NAC 用に Access Control Server を設定しておく必要があります。

Access Control Server は、システムのモニタリング、レポートの作成、デバッグ、およびロギングに役立つ情報を示すポスチャ トークン（ACS で設定可能な文字列）をセキュリティ アプライアンスにダウンロードします。一般的なポスチャ トークンは、Healthy、Checkup、Quarantine、Infected、または Unknown です。ポスチャ検証またはクライアントレス認証が終わると、ACS はセッション用のアクセス ポリシーをセキュリティ アプライアンスにダウンロードします。

デフォルトのグループ ポリシーまたは代替グループ ポリシーのネットワーク アドミッション コントロールを設定するには、次の手順を実行します。

ステップ 1　（オプション）ステータス クエリー タイマーの期間を設定します。セキュリティ アプライアンスは、ポスチャ検証が問題なく終わり、ステータス クエリーの応答を受け取るたびに、ステータス クエリーのタイマーを始動させます。このタイマーが切れると、ホスト ポスチャの変化を調べるクエリー（ステータス クエリーと呼ばれる）がトリガーされます。タイマーの期限を 30 ～ 1800 の秒数で入力します。デフォルトの設定は 300 秒です。

ネットワーク アドミッション コントロールのセッションで、ポスチャ検証が問題なく終わり、ポスチャの変更を調べる次のクエリーが発行されるまでの間隔を指定するには、グループ ポリシー コンフィギュレーション モードで **nac-sq-period** コマンドを使用します。

```
hostname(config-group-policy)# nac-sq-period seconds
hostname(config-group-policy)#
```

デフォルトのグループ ポリシーからステータス クエリー タイマーの値を継承するには、継承先の代替グループ ポリシーにアクセスして、このコマンドの **no** 形式を使用します。

```
hostname(config-group-policy)# no nac-sq-period [seconds]
hostname(config-group-policy)#
```

次に、ステータス クエリー タイマーの値を 1800 秒に変更する例を示します。

```
hostname(config-group-policy)# nac-sq-period 1800
hostname(config-group-policy)
```

次の例では、デフォルト グループ ポリシーからステータス クエリー タイマーの値を継承しています。

```
hostname(config-group-policy)# no nac-sq-period
hostname(config-group-policy)#
```

ステップ 2　（*任意*）NAC の再検証の期間を設定します。セキュリティ アプライアンスは、ポスチャ検証が問題なく終わるたびに、再検証タイマーを始動させます。このタイマーが期限切れになると、次の無条件のポスチャ検証がトリガーされます。セキュリティ アプライアンスは、それまでと同じ方法でポスチャを再検証します。ポスチャ検証または再検証中に Access Control Server が使用できない場合、デフォルトのグループ ポリシーが有効になります。ポスチャを検証する間隔を秒数で入力します。範囲は 300 ～ 86400 秒です。デフォルトの設定は 36000 秒です。

ネットワーク アドミッション コントロールのセッションでポスチャを検証する間隔を指定するには、グループ ポリシー コンフィギュレーション モードで **nac-reval-period** コマンドを使用します。

```
hostname(config-group-policy)# nac-reval-period seconds
hostname(config-group-policy)#
```

再検証タイマーの値をデフォルト グループ ポリシーから継承するには、継承先の代替グループ ポリシーにアクセスして、このコマンドの **no** 形式を使用します。

```
hostname(config-group-policy)# no nac-reval-period [seconds]
hostname(config-group-policy)#
```

次に、再検証タイマーを 86400 秒に変更する例を示します。

```
hostname(config-group-policy)# nac-reval-period 86400
hostname(config-group-policy)
```

次の例では、デフォルトのグループ ポリシーから再検証タイマーの値を継承しています。

```
hostname(config-group-policy)# no nac-reval-period
hostname(config-group-policy)#
```

ステップ 3　（*任意*）NAC のデフォルト ACL を設定します。セキュリティ アプライアンスは、ポスチャを検証できない場合に、選択された ACL に関連付けられているセキュリティ ポリシーを適用します。**none** または拡張 ACL を指定します。デフォルト設定は **none** です。**none** に設定すると、セキュリティ アプライアンスは、ポスチャを検証できなかったときにデフォルトのグループ ポリシーを適用します。

ポスチャを検証できなかったネットワーク アドミッション コントロール セッションのデフォルト ACL として使用される ACL を指定するには、グループ ポリシー コンフィギュレーション モードで **nac-default-acl** コマンドを使用します。

```
hostname(config-group-policy)# nac-default-acl {acl-name | none}
hostname(config-group-policy)#
```

デフォルトのグループ ポリシーから ACL を継承するには、継承先の代替グループ ポリシーにアクセスして、このコマンドの **no** 形式を使用します。

```
hostname(config-group-policy)# no nac-default-acl [acl-name | none]
hostname(config-group-policy)#
```

このコマンドの要素は次のとおりです。

- *acl-name*：**aaa-server host** コマンドを使用して ASA に設定されている、ポスチャを検証するサーバ グループの名前を指定します。この名前は、そのコマンドに指定された server-tag 変数に一致する必要があります。
- **none**：デフォルト グループ ポリシーからの ACL の継承をディセーブルにし、NAC セッションでポスチャ検証ができなかったときに ACL を適用しません。

NAC はデフォルトでディセーブルになっているため、ASA を通過する VPN トラフィックは、NAC がイネーブルになるまで、NAC デフォルトの ACL の影響は受けません。

次の例では、ポスチャを検証できなかったときに、acl-1 という ACL を適用するように指定しています。

```
hostname(config-group-policy)# nac-default-acl acl-1
hostname(config-group-policy)
```

次の例では、デフォルト グループ ポリシーから ACL を継承しています。

```
hostname(config-group-policy)# no nac-default-acl
hostname(config-group-policy)
```

次の例では、デフォルト グループ ポリシーからの ACL の継承をディセーブルにし、NAC セッションでポスチャを検証できなかったときに ACL を適用しません。

```
hostname(config-group-policy)# nac-default-acl none
hostname(config-group-policy)#
```

ステップ 4　VPN の NAC 免除を設定します。デフォルトでは、免除リストは空になっています。フィルタ属性のデフォルト値は **none** です。ポスチャ検証を免除するリモート ホストのオペレーティング システム（および ACL）ごとに **vpn-nac-exempt** コマンドを 1 回入力します。

ポスチャ検証を免除するリモート コンピュータのタイプのリストにエントリを追加するには、グループ ポリシー コンフィギュレーション モードで **vpn-nac-exempt** コマンドを使用します。

```
hostname(config-group-policy)# vpn-nac-exempt os "os name" [filter {acl-name | none}]
[disable]
hostname(config-group-policy)#
```

継承をディセーブルにし、すべてのホストをポスチャ検証の対象にするには、**vpn-nac-exempt** のすぐ後ろに **none** キーワードを入力します。

```
hostname(config-group-policy)# vpn-nac-exempt none
hostname(config-group-policy)#
```

免除リストのエントリを削除するには、このコマンドの **no** 形式を使用し、削除するオペレーティング システム（および ACL）を指定します。

```
hostname(config-group-policy)# no vpn-nac-exempt [os "os name"] [filter {acl-name | none}]
[disable]
hostname(config-group-policy)#
```

このグループ ポリシーに関連付けられている免除リストにある全エントリを削除し、デフォルト グループ ポリシーの免除リストを継承するには、キーワードを指定せずにこのコマンドの **no** 形式を使用します。

```
hostname(config-group-policy)# no vpn-nac-exempt
hostname(config-group-policy)#
```

このコマンドの構文要素は次のとおりです。

- *acl-name*：ASA のコンフィギュレーションに存在する ACL の名前。
- **disable**：免除リストのエントリを削除せずにディセーブルにします。
- **filter**：（オプション）コンピュータのオペレーティング システムの名前が一致したときにトラフィックをフィルタリングするために ACL に適用するフィルタ。
- **none**：このキーワードを **vpn-nac-exempt** のすぐ後ろに入力した場合は、継承がディセーブルになり、すべてのホストがポスチャ検証の対象になります。このキーワードを **filter** のすぐ後ろに入力した場合は、エントリで ACL を指定しないことを示します。
- **OS**：オペレーティング システムをポスチャ検証から免除します。
- *os name*：オペレーティング システムの名前です。名前にスペースが含まれている場合にのみ引用符が必要です（たとえば "Windows XP"）。

次に、ポスチャ検証を免除するコンピュータのリストに Windows XP を実行するすべてのホストを追加する例を示します。

```
hostname(config-group-policy)# vpn-nac-exempt os "Windows XP"
hostname(config-group-policy)
```

次の例では、Windows 98 を実行しているホストのうち、acl-1 という名前の ACL にある ACE に一致するものがすべて免除されます。

```
hostname(config-group-policy)# vpn-nac-exempt os "Windows 98" filter acl-1
hostname(config-group-policy)
```

次の例では、上と同じエントリが免除リストに追加されますが、ディセーブルにされます。

```
hostname(config-group-policy)# vpn-nac-exempt os "Windows 98" filter acl-1 disable
hostname(config-group-policy)
```

次の例では、同じエントリが、ディセーブルかどうかにかかわらず、免除リストから削除されます。

```
hostname(config-group-policy)# no vpn-nac-exempt os "Windows 98" filter acl-1
hostname(config-group-policy)
```

次の例では、継承がディセーブルにされ、すべてのホストがポスチャ検証の対象にされます。

```
hostname(config-group-policy)# no vpn-nac-exempt none
hostname(config-group-policy)
```

次に、免除リストからすべてのエントリを削除する例を示します。

```
hostname(config-group-policy)# no vpn-nac-exempt
hostname(config-group-policy)
```

ステップ 5　次のコマンドを入力して、ネットワーク アドミッション コントロールをイネーブルまたはディセーブルにします。

```
hostname(config-group-policy)# nac {enable | disable}
hostname(config-group-policy)#
```

デフォルト グループ ポリシーから NAC の設定を継承するには、継承先の代替グループ ポリシーにアクセスして、このコマンドの **no** 形式を使用します。

```
hostname(config-group-policy)# no nac [enable | disable]
hostname(config-group-policy)#
```

デフォルトでは、NAC はディセーブルになっています。NAC をイネーブルにすると、リモート アクセスでポスチャ検証が必要になります。リモート コンピュータのポスチャが正しいことが確認されると、ACS サーバが ASA で使用するアクセス ポリシーをダウンロードします。NAC は、デフォルトではディセーブルになっています。

Access Control Server はネットワーク上に存在する必要があります。

次の例では、グループ ポリシーに対して NAC をイネーブルにします。

```
hostname(config-group-policy)# nac enable
hostname(config-group-policy)#
```

VPN クライアント ファイアウォール ポリシーの設定

*ファイアウォール*は、データの着信パケットと発信パケットをそれぞれ検査して、パケットのファイアウォール通過を許可するか、またはパケットをドロップするかどうかを決定することにより、コンピュータをインターネットから分離して保護します。ファイアウォールは、グループのリモート ユーザがスプリット トンネリングを設定している場合、セキュリティの向上をもたらします。この場合、ファイアウォールが、インターネットまたはユーザのローカル LAN を経由する不正侵入からユーザのコンピュータを保護し、ひいては企業ネットワークも保護します。VPN クライアントを使用して ASA に接続しているリモート ユーザは、適切なファイアウォール オプションを選択できます。

グループ ポリシー コンフィギュレーション モードで **client-firewall** コマンドを使用して、ASA が IKE トンネル ネゴシエーション中に VPN クライアントに配信するパーソナル ファイアウォール ポリシーを設定します。ファイアウォール ポリシーを削除するには、このコマンドの **no** 形式を入力します。

すべてのファイアウォール ポリシーを削除するには、引数を指定せずに **no client-firewall** コマンドを入力します。このコマンドにより、**none** キーワードを指定して **client-firewall** コマンドを入力して作成したヌル ポリシーがあればそれも含めて、設定済みのすべてのファイアウォール ポリシーが削除されます。

ファイアウォール ポリシーがなくなると、ユーザはデフォルトまたはその他のグループ ポリシー内に存在するファイアウォール ポリシーを継承します。ユーザがこのようなファイアウォール ポリシーを継承しないようにするには、**none** キーワードを指定して **client-firewall** コマンドを入力します。

[Add or Edit Group Policy] ダイアログボックスの [Client Firewall] タブでは、追加または変更するグループ ポリシーに対して VPN クライアントのファイアウォール設定を指定できます。

（注） これらのファイアウォール機能を使用できるのは、Microsoft Windows を実行する VPN クライアントだけです。現在、ハードウェア クライアントまたは他（Windows 以外）のソフトウェア クライアントでは、これらの機能は使用できません。

最初のシナリオでは、リモート ユーザの PC 上にパーソナル ファイアウォールがインストールされています。VPN クライアントは、ローカル ファイアウォールで定義されているファイアウォール ポリシーを適用し、そのファイアウォールが実行されていることを確認するためにモニタします。ファイアウォールの実行が停止すると、VPN クライアントは ASA への通信をドロップします（このファイアウォール適用メカニズムは *Are You There（AYT）*と呼ばれます。VPN クライアントが定期的に「are you there?」メッセージを送信することによってファイアウォールをモニタするからです。応答が返されない場合、VPN クライアントは、ファイアウォールがダウンしたため ASA への接続が終了したことを認識します）。ネットワーク管理者がこれらの PC ファイアウォールを独自に設定する場合もありますが、この方法を使用すれば、ユーザは各自の設定をカスタマイズできます。

第 2 のシナリオでは、VPN クライアント PC のパーソナル ファイアウォールに中央集中型ファイアウォール ポリシーを適用することが選択されることがあります。一般的な例としては、スプリット トンネリングを使用してグループのリモート PC へのインターネット トラフィックをブロックすることが挙げられます。この方法は、トンネルが確立されている間、インターネット経由の侵入から PC を保護するので、中央サイトも保護されます。このファイアウォールのシナリオは、*プッシュ ポリシー*または *Central Protection Policy（CPP）*と呼ばれます。ASA では、VPN クライアントに適用するトラフィック管理ルールのセットを作成し、これらのルールをフィルタに関連付けて、そのフィルタをファイアウォール ポリシーに指定します。ASA は、このポリシーを VPN クライアントまで配信します。その後、VPN クライアントはポリシーをローカル ファイアウォールに渡し、そこでポリシーが適用されます。

AnyConnect クライアント ファイアウォール ポリシーの設定

AnyConnect クライアントのファイアウォール ルールでは、IPv4 および IPv6 のアドレスを指定できます。

前提条件

IPv6 アドレスが指定された統合アクセス ルールを作成します。

	コマンド	説明
ステップ 1	**webvpn** **例：** `hostname(config)# group-policy ac-client-group attributes` `hostname(config-group-policy)# webvpn` `hostname(config-group-webvpn)#`	webvpn グループ ポリシー コンフィギュレーション モードを開始します。
ステップ 2	**anyconnect firewall-rule client-interface {private | public} value** *[RuleName]* **例：** `hostname(config-group-webvpn)# anyconnect fireall-rule client-iterface private value ClientFWRule`	プライベートまたはパブリック ネットワーク ルールのアクセス コントロール ルールを指定します。プライベート ネットワーク ルールが、クライアントの VPN 仮想アダプタに適用されるルールです。
ステップ 3	**show runn group-policy** [value] **例：** `hostname(config-group-webvpn)# show runn group-policy FirstGroup` `group-policy FirstGroup internal` `group-policy FirstGroup attributes` `webvpn` `  anyconnect firewall-rule client-interface private value ClientFWRule`	グループ ポリシーのグループ ポリシー属性と webvpn ポリシー属性を表示します。

	コマンド	説明
ステップ 4	（オプション） **no anyconnect firewall-rule client-ineterface private value** [*RuleName*] **例：** hostname(config-group-webvpn)**#no anyconnect firewall-rule client-ineterface private value** hostname(config-group-webvpn)#	プライベート ネットワーク ルールからクライアント ファイアウォール ルールが削除されます。

Zone Labs Integrity サーバのサポート

この項では Zone Labs Integrity サーバ（Check Point Integrity サーバとも呼ばれる）について説明し、Zone Labs Integrity サーバをサポートするように ASA を設定する手順の例を示します。Integrity サーバは、リモート PC 上でセキュリティ ポリシーを設定および実行するための中央管理ステーションです。リモート PC が Integrity サーバによって指定されたセキュリティ ポリシーと適合しない場合、Integrity サーバおよび ASA が保護するプライベート ネットワークへのアクセス権が与えられません。

この項では、次のトピックについて取り上げます。

- 「Integrity サーバと ASA とのインタラクションの概要」（P.4-80）
- 「Integrity サーバのサポートの設定」（P.4-81）

Integrity サーバと ASA とのインタラクションの概要

VPN クライアント ソフトウェアと Integrity クライアント ソフトウェアは、リモート PC 上に共に常駐しています。次の手順では、リモート PC と企業のプライベート ネットワーク間にセッションを確立する際のリモート PC、ASA、および Integrity サーバのアクションをまとめます。

1. VPN クライアント ソフトウェア（Integrity クライアント ソフトウェアと同じリモート PC に常駐）は、ASA に接続し、それがどのタイプのファイアウォール クライアントであるかを ASA に知らせます。
2. ASA でクライアント ファイアウォールのタイプが承認されると、ASA から Integrity クライアントに Integrity サーバのアドレス情報が返されます。
3. ASA はプロキシとして動作し、Integrity クライアントは Integrity サーバとの制限付き接続を確立します。制限付き接続は、Integrity クライアントと Integrity サーバの間だけで確立されます。
4. Integrity サーバは、Integrity クライアントが指定されたセキュリティ ポリシーに準拠しているかどうかを特定します。Integrity クライアントがセキュリティ ポリシーに準拠している場合、Integrity サーバから ASA に対して、接続を開いて接続の詳細をクライアントに提供するように指示されます。
5. リモート PC では、VPN クライアントから Integrity クライアントに接続の詳細が渡され、ポリシーの実施がただちに開始されること、また、Integrity クライアントがプライベート ネットワークに接続できることが知らされます。
6. VPN 接続が確立すると、Integrity サーバは、クライアント ハートビート メッセージを使用して Integrity クライアントの状態のモニタを続けます。

（注）　ユーザ インターフェイスが最大 5 つの Integrity サーバのコンフィギュレーションをサポートしている場合でも、現在のリリースの ASA が一度にサポートする Integrity サーバは 1 つです。アクティブな Integrity サーバに障害が発生した場合は、ASA 上に別の Integrity サーバを設定してから、VPN クライアント セッションを再度確立します。

Integrity サーバのサポートの設定

この項では、Zone Labs Integrity サーバをサポートするように ASA を設定するための手順の例を示します。この手順には、アドレス、ポート、接続障害タイムアウトおよび障害の状態、および SSL 証明書パラメータの設定が含まれます。

Integrity サーバを設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	**zonelabs-Integrity server-address** {*hostname1* | *ip-address1*} **例：** `hostname(config)# zonelabs-Integrity server-address 10.0.0.5`	IP アドレス 10.0.0.5 を使用して Integrity サーバを設定します。
ステップ 2	**zonelabs-integrity port** *port-number* **例：** `hostname(config)# zonelabs-integrity port 300`	ポート 300 を指定します（デフォルト ポートは 5054 です）。
ステップ 3	**zonelabs-integrity interface** *interface* **例：** `hostname(config)# zonelabs-integrity interface inside`	Integrity サーバとの通信用に内部インターフェイスを指定します。
ステップ 4	**zonelabs-integrity fail-timeout** *timeout* **例：** `hostname(config)# zonelabs-integrity fail-timeout 12`	Integrity サーバに障害があることを宣言して VPN クライアント接続を閉じる前に、ASA がアクティブまたはスタンバイ Integrity サーバからの応答を 12 秒間待つようにします。 （注）　ASA と Integrity サーバの間の接続で障害が発生した場合、エンタープライズ VPN が Integrity サーバの障害によって中断されないように、デフォルトで VPN クライアント接続は開いたままになります。ただし、Zone Labs Integrity サーバに障害が発生した場合、必要に応じて VPN 接続を閉じることができます。
ステップ 5	**zonelabs-integrity fail-close** **例：** `hostname(config)# zonelabs-integrity fail-close`	ASA と Zone Labs Integrity サーバとの接続に障害が発生した場合に VPN クライアントとの接続が閉じるよう、ASA を設定します。

	コマンド	目的
ステップ 6	**zonelabs-integrity fail-open** **例：** hostname(config)# zonelabs-integrity fail-open	設定された VPN クライアント接続の障害状態をデフォルトに戻して、クライアント接続が開いたままになるようにします。
ステップ 7	**zonelabs-integrity ssl-certificate-port** *cert-port-number* **例：** hostname(config)# zonelabs-integrity ssl-certificate-port 300	Integrity サーバが ASA のポート 300（デフォルトはポート 80）に接続して、サーバ SSL 証明書を要求するように指定します。
ステップ 8	**zonelabs-integrity ssl-client-authentication {enable | disable}** **例：** hostname(config)# zonelabs-integrity ssl-client-authentication enable	サーバの SSL 証明書は常に認証されますが、Integrity サーバのクライアント SSL 証明書も認証されるように指定します。

ファイアウォール クライアント タイプを Zone Labs Integrity タイプに設定するには、次のコマンドを入力します。

コマンド	目的
client-firewall {opt | req} zonelabs-integrity **例：** hostname(config)# client-firewall req zonelabs-integrity	詳細については、「VPN クライアント ファイアウォール ポリシーの設定」（P.4-78）を参照してください。ファイアウォールのタイプが **zonelabs-integrity** の場合、Integrity サーバによってこれらのポリシーが決定されるため、ファイアウォール ポリシーを指定するコマンド引数は使用されません。

クライアント ファイアウォールのパラメータの設定

次のコマンドを入力して、適切なクライアント ファイアウォールのパラメータを設定します。各コマンドに設定できるインスタンスは 1 つだけです。詳細については、「VPN クライアント ファイアウォール ポリシーの設定」（P.4-78）を参照してください。

Cisco Integrated ファイアウォール

```
hostname(config-group-policy)# client-firewall {opt | req} cisco-integrated acl-in ACL
acl-out ACL
```

Cisco Security Agent

```
hostname(config-group-policy)# client-firewall {opt | req} cisco-security-agent
```

ファイアウォールなし

```
hostname(config-group-policy)# client-firewall none
```

カスタム ファイアウォール

```
hostname(config-group-policy)# client-firewall {opt | req} custom vendor-id num product-id
num policy {AYT | CPP acl-in ACL acl-out ACL} [description string]
```

Zone Labs ファイアウォール

```
hostname(config-group-policy)# client-firewall {opt | req} zonelabs-integrity
```

（注）　ファイアウォールのタイプを **zonelabs-integrity** にする場合は、引数を指定しないでください。ポリシーは、Zone Labs Integrity サーバによって決められます。

```
hostname(config-group-policy)# client-firewall {opt | req} zonelabs-zonealarm policy {AYT
| CPP acl-in ACL acl-out ACL}

hostname(config-group-policy)# client-firewall {opt | req} zonelabs-zonealarmorpro policy
{AYT | CPP acl-in ACL acl-out ACL}

client-firewall {opt | req} zonelabs-zonealarmpro policy {AYT | CPP acl-in ACL acl-out
ACL}
```

Sygate Personal ファイアウォール

```
hostname(config-group-policy)# client-firewall {opt | req} sygate-personal

hostname(config-group-policy)# client-firewall {opt | req} sygate-personal-pro

hostname(config-group-policy)# client-firewall {opt | req} sygate-security-agent
```

Network Ice、Black Ice ファイアウォール：

```
hostname(config-group-policy)# client-firewall {opt | req} networkice-blackice
```

表 4-1　client-firewall コマンドのキーワードと変数

パラメータ	説明
acl-in *ACL*	クライアントが着信トラフィックに使用するポリシーを指定します。
acl-out *ACL*	クライアントが発信トラフィックに使用するポリシーを指定します。
AYT	クライアント PC のファイアウォール アプリケーションがファイアウォール ポリシーを制御することを指定します。ASA はファイアウォールが実行されていることを確認します。「Are You There?」の送信に対して応答がない場合は、ASA によりトンネルが切断されます。
cisco-integrated	Cisco Integrated ファイアウォール タイプを指定します。
cisco-security-agent	Cisco Intrusion Prevention Security Agent ファイアウォール タイプを指定します。
CPP	VPN クライアントのファイアウォール ポリシーのソースとして Policy Pushed を指定します。

表 4-1　client-firewall コマンドのキーワードと変数

custom	カスタム ファイアウォール タイプを指定します。
description *string*	ファイアウォールの説明を示します。
networkice-blackice	Network ICE Black ICE ファイアウォール タイプを指定します。
none	クライアント ファイアウォール ポリシーがないことを指定します。ファイアウォール ポリシーにヌル値を設定して、ファイアウォール ポリシーを拒否します。デフォルトのグループ ポリシーまたは指定されているグループ ポリシーからファイアウォール ポリシーを継承しないようにします。
opt	オプションのファイアウォール タイプを指定します。
product-id	ファイアウォール製品を指定します。
req	必要なファイアウォール タイプを指定します。
sygate-personal	Sygate Personal ファイアウォール タイプを指定します。
sygate-personal-pro	Sygate Personal Pro ファイアウォール タイプを指定します。
sygate-security-agent	Sygate Security Agent ファイアウォール タイプを指定します。
vendor-id	ファイアウォールのベンダーを指定します。
zonelabs-integrity	Zone Labs Integrity サーバ ファイアウォール タイプを指定します。
zonelabs-zonealarm	Zone Labs Zone Alarm ファイアウォール タイプを指定します。
zonelabs-zonealarmorpro policy	Zone Labs Zone Alarm または Pro ファイアウォール タイプを指定します。
zonelabs-zonealarmpro policy	Zone Labs Zone Alarm Pro ファイアウォール タイプを指定します。

次に、FirstGroup という名前のグループ ポリシーについて、Cisco Intrusion Prevention Security Agent を必要とするクライアント ファイアウォール ポリシーを設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# client-firewall req cisco-security-agent
hostname(config-group-policy)#
```

クライアント アクセス ルールの設定

グループ ポリシー コンフィギュレーション モードで **client-access-rule** コマンドを使用して、ASA を介して IPsec で接続できるリモート アクセス クライアントのタイプとバージョンを制限するルールを設定します。次のガイドラインに従ってルールを作成します。

- ルールを定義しない場合、ASA はすべての接続タイプを許可します。
- クライアントがいずれのルールにも一致しない場合、ASA は接続を拒否します。拒否ルールを定義する場合は、許可ルールも 1 つ以上定義する必要があります。定義しない場合、ASA はすべての接続を拒否します。
- ソフトウェア クライアントとハードウェア クライアントのどちらでも、タイプとバージョンは **show vpn-sessiondb remote** で表示される内容と完全に一致している必要があります。
- ***** 文字はワイルドカードです。ワイルドカードは各ルールで複数回入力することができます。たとえば、**client-access rule 3 deny type * version 3.*** では、バージョン 3.x のソフトウェア リリースを実行しているすべてのクライアント タイプを拒否する、プライオリティ 3 のクライアント アクセス ルールが作成されます。

- 1 つのグループ ポリシーにつき最大 25 のルールを作成できます。
- ルール セット全体に対して 255 文字の制限があります。
- クライアントのタイプまたはバージョン（あるいはその両方）を送信しないクライアントには、n/a を入力できます。

ルールを削除するには、このコマンドの **no** 形式を入力します。このコマンドは、次のコマンドと同等です。

```
hostname(config-group-policy)# client-access-rule 1 deny type "Cisco VPN Client" version
4.0
```

すべてのルールを削除するには、引数を指定せずに **no client-access-rule** コマンドを入力します。これにより、**none** キーワードを指定して **client-access-rule** コマンドを発行して作成したヌル ルールがあればそれも含めて、設定済みのすべてのルールが削除されます。

デフォルトでは、アクセス ルールはありません。クライアント アクセス ルールがない場合、ユーザはデフォルトのグループ ポリシー内に存在するすべてのルールを継承します。

ユーザがクライアント アクセス ルールを継承しないようにするには、**none** キーワードを指定して **client-access-rule** コマンドを入力します。このコマンドの結果、すべてのタイプとバージョンのクライアントが接続できるようになります。

```
hostname(config-group-policy)# client-access rule priority {permit | deny} type type
version {version | none}

hostname(config-group-policy)# no client-access rule [priority {permit | deny} type type
version version]
```

表 4-2 に、これらのコマンドのキーワードとパラメータの意味を示します。

表 4-2　client-access rule コマンドのキーワードと変数

パラメータ	説明
deny	特定のタイプとバージョンのデバイスの接続を拒否します。
none	クライアント アクセス ルールを許可しません。client-access-rule をヌル値に設定します。これにより制限が許可されなくなります。デフォルトのグループ ポリシーまたは指定されているグループ ポリシーから値を継承しないようにします。
permit	特定のタイプとバージョンのデバイスの接続を許可します。
priority	ルールのプライオリティを決定します。最小の整数値を持つルールは、プライオリティが最も高くなります。したがって、クライアントのタイプとバージョン（またはこのいずれか）に一致する最も小さい整数のルールが、適用されるルールとなります。プライオリティの低いルールに矛盾がある場合、ASA はそのルールを無視します。
type *type*	VPN 3002 などの自由形式のストリングを使用して、デバイス タイプを指定します。文字列は、**show vpn-sessiondb remote** で表示される内容と完全に一致している必要があります。ただし、ワイルドカードとして * 文字を入力できます。
version *version*	7.0 などの自由形式のストリングを使用して、デバイス バージョンを指定します。文字列は、**show vpn-sessiondb remote** で表示される内容と完全に一致している必要があります。ただし、ワイルドカードとして * 文字を入力できます。

次に、FirstGroup という名前のグループ ポリシーのクライアント アクセス ルールを作成する例を示します。これらのルールは、バージョン 4.x のソフトウェアを実行する Cisco VPN Client を許可し、すべての Windows NT クライアントを拒否します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# client-access-rule 1 deny type WinNT version *
hostname(config-group-policy)# client-access-rule 2 permit “Cisco VPN Client” version 4.*
```

（注）　「type」フィールドは、任意の値が許可される自由形式の文字列ですが、その値は、接続時にクライアントから ASA に送信される固定値と一致している必要があります。

グループ ポリシーのクライアントレス SSL VPN セッションの属性の設定

クライアントレス SSL VPN によってユーザは、Web ブラウザを使用して ASA へのセキュアなリモート アクセス VPN トンネルを確立できます。ソフトウェアまたはハードウェア クライアントは必要ありません。クライアントレス SSL VPN を使用することで、HTTPS インターネット サイトにアクセスできるほとんどすべてのコンピュータから、幅広い Web リソースおよび Web 対応アプリケーションに簡単にアクセスできます。クライアントレス SSL VPN は SSL およびその後継である TLS1 を使用して、リモート ユーザと、中央サイトで設定した特定のサポートされている内部リソースとの間のセキュアな接続を提供します。ASA はプロキシで処理する必要がある接続を認識し、HTTP サーバは認証サブシステムと対話してユーザを認証します。デフォルトでは、クライアントレス SSL VPN はディセーブルになっています。

特定の内部グループ ポリシー用のクライアントレス SSL VPN のコンフィギュレーションをカスタマイズできます。

（注）　グローバル コンフィギュレーション モードから入る webvpn モードでは、クライアントレス SSL VPN セッションのグローバル設定を構成できます。この項で説明する webvpn モード（グループ ポリシー コンフィギュレーション モードから入ります）を使用すると、クライアントレス SSL VPN セッションに固有のグループ ポリシーのコンフィギュレーションをカスタマイズできます。

グループ ポリシー webvpn コンフィギュレーション モードでは、すべての機能の設定を継承するか、または次のパラメータをカスタマイズするかどうかを指定できます。各パラメータについては、後述の項で説明します。

- customizations
- html-content-filter
- homepage
- filter
- url-list
- port-forward
- port-forward-name
- sso server（シングル サインオン サーバ）
- auto-signon
- deny message
- AnyConnect Secure Mobility Client
- keep-alive ignore
- HTTP compression

多くの場合、クライアントレス SSL VPN の設定の一部として webvpn 属性を定義した後、グループ ポリシーの webvpn 属性を設定するときにこれらの定義を特定のグループに適用します。グループ ポリシー コンフィギュレーション モードで **webvpn** コマンドを使用して、グループ ポリシー webvpn コンフィギュレーション モードに入ります。グループ ポリシー用の webvpn コマンドは、ファイル、URL、および TCP アプリケーションへのクライアントレス SSL VPN セッション経由のアクセスを定義します。ACL およびフィルタリングするトラフィックのタイプも指定します。クライアントレス SSL VPN は、デフォルトではディセーブルになっています。クライアントレス SSL VPN セッションの属性の設定の詳細については、*第 13 章「クライアントレス SSL VPN の概要」*の説明を参照してください。

グループ ポリシー webvpn コンフィギュレーション モードで入力されたすべてのコマンドを削除するには、このコマンドの **no** 形式を入力します。これらの webvpn コマンドは、設定元のユーザ名またはグループ ポリシーに適用されます。

```
hostname(config-group-policy)# webvpn
hostname(config-group-policy)# no webvpn
```

次の例は、FirstGroup という名前のグループ ポリシーのグループ ポリシー webvpn コンフィギュレーション モードに入る方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)#
```

カスタマイゼーションの適用

カスタマイゼーションによって、ログイン時にユーザに表示されるウィンドウの外観が決まります。カスタマイゼーション パラメータは、クライアントレス SSL VPN の設定の一部として設定します。定義済みの Web ページ カスタマイゼーションを適用して、ログイン時にユーザに表示される Web ページのルックアンドフィールを変更するには、グループ ポリシー webvpn コンフィギュレーション モードで customization コマンドを入力します。

```
hostname(config-group-webvpn)# customization customization_name
hostname(config-group-webvpn)#
```

たとえば、blueborder という名前のカスタマイゼーションを使用するには、次のコマンドを入力します。

```
hostname(config-group-webvpn)# customization blueborder
hostname(config-group-webvpn)#
```

カスタマイゼーション自体は、webvpn モードで **customization** コマンドを入力して設定します。

次の例は、123 という名前のカスタマイゼーションを最初に確立するコマンド シーケンスを示しています。このコマンド シーケンスによって、パスワード プロンプトが定義されます。次の例は、testpolicy という名前のグループ ポリシーを定義し、**customization** コマンドを使用して、クライアントレス SSL VPN セッションに 123 という名前のカスタマイゼーションを使用することを指定しています。

```
hostname(config)# webvpn
hostname(config-webvpn)# customization 123
hostname(config-webvpn-custom)# password-prompt Enter password
hostname(config-webvpn)# exit
hostname(config)# group-policy testpolicy nopassword
hostname(config)# group-policy testpolicy attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# customization value 123
hostname(config-group-webvpn)#
```

「Deny」メッセージの指定

グループ ポリシー webvpn コンフィギュレーション モードで、**deny-message** コマンドを入力すると、クライアントレス SSL VPN セッションに正常にログインできるが VPN 特権を持たないリモート ユーザに送信されるメッセージを指定できます。

```
hostname(config-group-webvpn)# deny-message value "message"
hostname(config-group-webvpn)# no deny-message value "message"
hostname(config-group-webvpn)# deny-message none
```

no deny-message value コマンドは、リモート ユーザがメッセージを受信しないように、メッセージ文字列を削除します。

no deny-message none コマンドは、接続プロファイル ポリシーのコンフィギュレーションから属性を削除します。ポリシーは属性値を継承します。

メッセージは、特殊文字、スペース、および句読点を含む英数字で最大 491 文字まで指定できますが、囲みの引用符はカウントされません。テキストは、ログイン時にリモート ユーザのブラウザに表示されます。**deny-message value** コマンドへのストリングの入力時は、コマンドがラップしている場合でも引き続き入力します。

デフォルトの拒否メッセージは次のとおりです。「Login was successful, but because certain criteria have not been met or due to some specific group policy, you do not have permission to use any of the VPN features. Contact your IT administrator for more information.」

次の例の最初のコマンドは、group2 という名前の内部グループ ポリシーを作成します。後続のコマンドは、そのポリシーに関連付けられている webvpn 拒否メッセージが含まれた属性を変更します。

```
hostname(config)# group-policy group2 internal
hostname(config)# group-policy group2 attributes
hostname(config-group)# webvpn
hostname(config-group-webvpn)# deny-message value "Your login credentials are OK.However,
you have not been granted rights to use the VPN features.Contact your administrator for
more information."
hostname(config-group-webvpn)
```

グループ ポリシーのクライアントレス SSL VPN セッションのフィルタ属性の設定

webvpn モードで **html-content-filter** コマンドを使用して、このグループ ポリシーのクライアントレス SSL VPN セッションの Java、ActiveX、イメージ、スクリプト、およびクッキーをフィルタリングするかどうかを指定します。HTML フィルタリングは、デフォルトでディセーブルです。

コンテンツ フィルタを削除するには、このコマンドの **no** 形式を入力します。**none** キーワードを指定して **html-content-filter** コマンドを発行して作成したヌル値を含めて、すべてのコンテンツ フィルタを削除するには、引数を指定せずにこのコマンドの **no** 形式を入力します。**no** オプションを使用すると、値を別のグループ ポリシーから継承できるようになります。HTML コンテンツ フィルタを継承しないようにするには、**none** キーワードを指定して **html-content-filter** コマンドを入力します。

次回このコマンドを使用すると、前回までの設定が上書きされます。

```
hostname(config-group-webvpn)# html-content-filter {java | images | scripts | cookies |
none}

hostname(config-group-webvpn)# no html-content-filter [java | images | scripts | cookies |
none]
```

表 4-3 に、このコマンドで使用するキーワードの意味を示します。

表 4-3　　filter コマンドのキーワード

キーワード	意味
cookies	イメージからクッキーを削除して、限定的な広告フィルタリングとプライバシーを提供します。
images	イメージへの参照を削除します（<IMG> タグを削除します）。
java	Java および ActiveX への参照を削除します（<EMBED>、<APPLET>、および <OBJECT> の各タグを削除）。
none	フィルタリングを行わないことを指定します。ヌル値を設定して、フィルタリングを拒否します。フィルタリング値を継承しないようにします。
scripts	スクリプトへの参照を削除します（<SCRIPT> タグを削除します）。

次に、FirstGroup という名前のグループ ポリシーに対して JAVA と ActiveX、クッキー、およびイメージのフィルタリングを設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# html-content-filter java cookies images
hostname(config-group-webvpn)#
```

ユーザ ホームページの指定

グループ ポリシー webvpn コンフィギュレーション モードで **homepage** コマンドを使用して、このグループのユーザのログイン時に表示される Web ページの URL を指定します。デフォルトのホームページはありません。

homepage none コマンドを発行して作成したヌル値を含めて、設定されているホームページを削除するには、このコマンドの **no** 形式を入力します。**no** オプションを使用すると、値を別のグループ ポリシーから継承できるようになります。ホームページを継承しないようにするには、**homepage none** コマンドを入力します。

none キーワードは、クライアントレス SSL VPN セッションのホームページがないことを示します。これにより、ヌル値が設定されてホームページが拒否され、ホームページが継承されなくなります。

キーワード *value* の後ろの **url-string** 変数で、ホームページの URL を指定します。http:// または https:// のいずれかで始まるストリングにする必要があります。

```
hostname(config-group-webvpn)# homepage {value url-string | none}
hostname(config-group-webvpn)# no homepage
hostname(config-group-webvpn)#
```

自動サインオンの設定

auto-signon コマンドは、クライアントレス SSL VPN セッションのユーザ用のシングル サインオン方式です。NTLM 認証、基本認証、またはその両方を使用する認証のためにログイン クレデンシャル（ユーザ名とパスワード）を内部サーバに渡します。複数の auto-signon コマンドを入力でき、それらのコマンドは入力順に処理されます（先に入力したコマンドが優先されます）。

自動サインオン機能は、webvpn コンフィギュレーション、webvpn グループ コンフィギュレーション、または webvpn ユーザ名コンフィギュレーション モードの 3 つのモードで使用できます。ユーザ名がグループに優先し、グループがグローバルに優先するという標準的な優先動作が適用されます。選択するモードは、使用する認証の対象範囲によって異なります。

特定のサーバへの特定のユーザの自動サインオンをディセーブルにするには、元の IP ブロックまたは URL を指定してこのコマンドの **no** 形式を使用します。すべてのサーバへの認証をディセーブルにするには、引数を指定しないで **no** 形式を使用します。**no** オプションを使用すると、値をグループ ポリシーから継承できます。

次の例では、グループ ポリシー webvpn コンフィギュレーション モードで入力し、基本認証を使用して、10.1.1.0 から 10.1.1.255 の範囲の IP アドレスを持つサーバへの anyuser という名前のユーザの自動サインオンを設定します。

次のコマンド例では、基本認証または NTLM 認証を使用して、クライアントレス SSL VPN セッションのユーザに対し、URI マスク https://*.example.com/* で定義されたサーバへのアクセスに自動サインオンを設定します。

```
hostname(config)# group-policy ExamplePolicy attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# auto-signon allow uri https://*.example.com/* auth-type all
hostname(config-group-webvpn)#
```

次のコマンド例では、基本認証または NTLM 認証を使用して、クライアントレス SSL VPN セッションのユーザに対し、サブネット マスク 255.255.255.0 を使用する IP アドレス 10.1.1.0 のサーバへのアクセスに自動サインオンを設定します。

```
hostname(config)# group-policy ExamplePolicy attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# auto-signon allow ip 10.1.1.0 255.255.255.0 auth-type all
hostname(config-group-webvpn)#
```

クライアントレス SSL VPN セッションに使用する ACL の指定

webvpn モードで **filter** コマンドを使用して、このグループ ポリシーまたはユーザ名でクライアントレス SSL VPN セッションに使用する ACL の名前を指定します。**filter** コマンドを入力して指定するまで、クライアントレス SSL VPN ACL は適用されません。

filter none コマンドを発行して作成したヌル値を含めて、ACL を削除するには、このコマンドの **no** 形式を入力します。**no** オプションを使用すると、値を別のグループ ポリシーから継承できるようになります。フィルタの値を継承しないようにするには、**filter value none** コマンドを入力します。

filter コマンドを入力して指定するまで、クライアントレス SSL VPN セッションの ACL は適用されません。

ACL を設定して、このグループ ポリシーについて、さまざまなタイプのトラフィックを許可または拒否します。次に、**filter** コマンドを入力して、これらの ACL をクライアントレス SSL VPN トラフィックに適用します。

```
hostname(config-group-webvpn)# filter {value ACLname | none}
hostname(config-group-webvpn)# no filter
```

none キーワードは、**webvpntype** ACL がないことを示します。これにより、ヌル値が設定されて ACL が拒否され、別のグループ ポリシーから ACL が継承されなくなります。

キーワード **value** の後ろの *ACLname* 文字列で、事前に設定されている ACL の名前を指定します。

（注） クライアントレス SSL VPN セッションは、**vpn-filter** コマンドで定義されている ACL を使用しません。

次に、FirstGroup という名前のグループ ポリシーの、*acl_in* という ACL を呼び出すフィルタを設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# filter acl_in
hostname(config-group-webvpn)#
```

URL リストの適用

グループ ポリシーのクライアントレス SSL VPN ホームページに URL のリストを表示するように指定できます。最初に、グローバル コンフィギュレーション モードで **url-list** コマンドを入力して、1 つ以上の名前付きリストを作成する必要があります。特定のグループ ポリシーにクライアントレス SSL VPN セッションのサーバと URL のリストを適用して、特定のグループ ポリシーのリストにある URL にアクセスできるようにするには、グループ ポリシー webvpn コンフィギュレーション モードで **url-list** コマンドを実行する際に、作成するリスト（複数可）の名前を使用します。デフォルトの URL リストはありません。

url-list none コマンドを使用して作成したヌル値を含めて、リストを削除するには、このコマンドの **no** 形式を使用します。**no** オプションを使用すると、値を別のグループ ポリシーから継承できるようになります。URL リストを継承しないようにするには、**url-list none** コマンドを入力します。コマンドを 2 回使用すると、先行する設定が上書きされます。

```
hostname(config-group-webvpn)# url-list {value name | none} [index]
hostname(config-group-webvpn)# no url-list
```

表 4-4 に、**url-list** コマンドのパラメータとその意味を示します。

表 4-4　　url-list コマンドのキーワードと変数

パラメータ	意味
index	ホームページ上の表示のプライオリティを指定します。
none	URL リストにヌル値を設定します。デフォルトまたは指定したグループ ポリシーからリストが継承されないようにします。
value *name*	設定済み URL リストの名前を指定します。このようなリストを設定するには、グローバル コンフィギュレーション モードで **url-list** コマンドを使用します。

次の例では、FirstGroup という名前のグループ ポリシーに FirstGroupURLs という名前の URL リストを設定し、これがホームページに表示される最初の URL リストになるように指定します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# url-list value FirstGroupURLs 1
hostname(config-group-webvpn)#
```

グループ ポリシーの ActiveX Relay のイネーブル化

ActiveX Relay を使用すると、クライアントレス SSL VPN セッションを確立したユーザが、ブラウザを使用して Microsoft Office アプリケーションを起動できるようになります。アプリケーションは、セッションを使用して Microsoft Office ドキュメントのダウンロードとアップロードを行います。ActiveX のリレーは、クライアントレス SSL VPN セッションを終了するまで有効なままです。

クライアントレス SSL VPN セッションで ActiveX コントロールをイネーブルまたはディセーブルにするには、グループ ポリシー webvpn コンフィギュレーション モードで次のコマンドを入力します。

activex-relay {**enable** | **disable**}

デフォルト グループ ポリシーから **activex-relay** コマンドを継承するには、次のコマンドを入力します。

no activex-relay

次のコマンドは、特定のグループ ポリシーに関連付けられているクライアントレス SSL VPN セッションの ActiveX コントロールをイネーブルにします。

```
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# activex-relay enable
hostname(config-group-webvpn)
```

グループ ポリシーのクライアントレス SSL VPN セッションのアプリケーション アクセスのイネーブル化

このグループ ポリシーのアプリケーション アクセスをイネーブルにするには、グループ ポリシー webvpn コンフィギュレーション モードで **port-forward** コマンドを入力します。ポート転送は、デフォルトではディセーブルになっています。

グループ ポリシー webvpn コンフィギュレーション モードで **port-forward** コマンドを入力し、アプリケーション アクセスをイネーブルにする前に、クライアントレス SSL VPN セッションでユーザが使用できるアプリケーションのリストを定義する必要があります。グローバル コンフィギュレーション モードで **port-forward** コマンドを入力して、このリストを定義します。

port-forward none コマンドを発行して作成したヌル値を含めて、グループ ポリシー コンフィギュレーションからポート転送属性を削除するには、このコマンドの **no** 形式を入力します。**no** オプションを使用すると、リストを別のグループ ポリシーから継承できます。ポート転送リストを継承しないようにするには、**none** キーワードを指定して **port-forward** コマンドを入力します。**none** キーワードは、フィルタリングが実行されないことを示します。これにより、ヌル値が設定されてフィルタリングが拒否され、フィルタリング値が継承されなくなります。

このコマンドの構文は次のとおりです。

```
hostname(config-group-webvpn)# port-forward {value listname | none}
hostname(config-group-webvpn)# no port-forward
```

キーワード *value* の後ろの **listname** 文字列で、クライアントレス SSL VPN セッションのユーザがアクセスできるアプリケーションのリストを指定します。webvpn コンフィギュレーション モードで port-forward コマンドを入力し、このリストを定義します。

次回このコマンドを使用すると、前回までの設定が上書きされます。

次の例は、FirstGroup という名前の内部グループ ポリシーに *ports1* というポート転送リストを設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup internal attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# port-forward value ports1
hostname(config-group-webvpn)#
```

ポート転送表示名の設定

グループ ポリシー webvpn コンフィギュレーション モードで **port-forward-name** コマンドを使用して、特定のユーザまたはグループ ポリシーでエンド ユーザへの TCP ポート転送を識別する表示名を設定します。**port-forward-name none** コマンドを使用して作成したヌル値を含めて、表示名を削除するには、このコマンドの **no** 形式を入力します。**no** オプションは、デフォルト名の、Application Access を復元します。表示名を使用しないようにするには、**port-forward none** コマンドを入力します。このコマンドの構文は次のとおりです。

```
hostname(config-group-webvpn)# port-forward-name {value name | none}
hostname(config-group-webvpn)# no port-forward-name
```

次の例は、*FirstGroup* という名前の内部グループ ポリシーに Remote Access TCP Applications という名前を設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup internal attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# port-forward-name value Remote Access TCP Applications
hostname(config-group-webvpn)#
```

セッション タイマー更新のために無視する最大オブジェクト サイズの設定

ネットワーク デバイスは、短いキープアライブ メッセージを交換して、デバイス間の仮想回路が引き続きアクティブであることを確認します。これらのメッセージの長さは異なる可能性があります。**keep-alive-ignore** コマンドを使用すると、指定したサイズ以下のすべてのメッセージをキープアライブ メッセージと見なし、セッション タイマーの更新時にトラフィックと見なさないよう ASA に指示できます。範囲は 0 ～ 900 KB です。デフォルトは 4 KB です。

トランザクションごとに無視する HTTP/HTTPS トラフィックの上限を指定するには、グループ ポリシー属性 webvpn コンフィギュレーション モードで **keep-alive-ignore** コマンドを使用します。

```
hostname(config-group-webvpn)# keep-alive-ignore size
hostname(config-group-webvpn)#
```

このコマンドの **no** 形式は、この指定をコンフィギュレーションから削除します。

```
hostname(config-group-webvpn)# no keep-alive-ignore
hostname(config-group-webvpn)#
```

次の例では、無視するオブジェクトの最大サイズを 5 KB に設定します。

```
hostname(config-group-webvpn)# keep-alive-ignore 5
hostname(config-group-webvpn)#
```

HTTP 圧縮の指定

グループ ポリシー webvpn モードで、**http-comp** コマンドを入力して、特定のグループまたはユーザのクライアントレス SSL VPN セッションで HTTP データの圧縮をイネーブルにします。

```
hostname(config-group-webvpn)# http-comp {gzip | none}
hostname(config-group-webvpn)#
```

コンフィギュレーションからコマンドを削除し、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

```
hostname(config-group-webvpn)# no http-comp {gzip | none}
hostname(config-group-webvpn)#
```

このコマンドの構文は次のとおりです。

- **gzip**：圧縮がグループまたはユーザに対してイネーブルになることを指定します。これはデフォルト値です。
- **none**：圧縮がグループまたはユーザに対してディセーブルになることを指定します。

クライアントレス SSL VPN セッションの場合、グローバル コンフィギュレーション モードで設定された **compression** コマンドは、グループ ポリシー webvpn モードおよびユーザ名 webvpn モードで設定された **http-comp** コマンドを上書きします。

次に、グローバル ポリシー sales の圧縮をディセーブルにする例を示します。

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# http-comp none
hostname(config-group-webvpn)#
```

SSO サーバの指定

クライアントレス SSL VPN セッションだけに使用できるシングル サインオンのサポートを使用すると、ユーザはユーザ名とパスワードを複数回入力しなくても、さまざまなサーバのセキュアな各種のサービスにアクセスできます。グループ ポリシー webvpn モードで **sso-server value** コマンドを入力すると、SSO サーバをグループ ポリシーに割り当てることができます。

グループ ポリシーに SSO サーバを割り当てるには、グループ ポリシーの webvpn コンフィギュレーション モードで **sso-server value** コマンドを使用します。このコマンドでは、コンフィギュレーションに CA SiteMinder コマンドが含まれている必要があります。

```
hostname(config-group-webvpn)# sso-server value server_name
hostname(config-group-webvpn)#
```

割り当てを削除してデフォルト ポリシーを使用するには、このコマンドの **no** 形式を使用します。デフォルト ポリシーが継承されないようにするには、**sso-server none** コマンドを使用します。

```
hostname(config-group-webvpn)# sso-server {value server_name | none}
hostname(config-group-webvpn)# [no] sso-server value server_name
```

SSO サーバに割り当てられているデフォルト ポリシーは DfltGrpPolicy です。

次の例では、グループ ポリシー「my-sso-grp-pol」を作成し、「example」という名前の SSO サーバに割り当てます。

```
hostname(config)# group-policy my-sso-grp-pol internal
hostname(config)# group-policy my-sso-grp-pol attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# sso-server value example
hostname(config-group-webvpn)#
```

ユーザ属性の設定

この項では、ユーザ属性とその設定方法について説明します。内容は次のとおりです。

デフォルトでは、ユーザは、割り当てられているグループ ポリシーからすべてのユーザ属性を継承します。また、ASA では、ユーザ レベルで個別に属性を割り当て、そのユーザに適用されるグループ ポリシーの値を上書きすることができます。たとえば、すべてのユーザに営業時間内のアクセスを許可し、特定のユーザに 24 時間のアクセスを許可するグループ ポリシーを指定することができます。

ユーザ名のコンフィギュレーションの表示

グループ ポリシーから継承したデフォルト値も含めて、すべてのユーザ名のコンフィギュレーションを表示するには、次のように、**all** キーワードを指定して **show running-config username** コマンドを入力します。

```
hostname# show running-config all username
hostname#
```

このコマンドは、すべてのユーザまたは特定のユーザ（ユーザ名を指定した場合）の 暗号化されたパスワードと特権レベルを表示します。**all** キーワードを省略すると、明示的に設定された値だけがこのリストに表示されます。次の例は、このコマンドで testuser というユーザを指定した場合の出力を示します。

```
hostname# show running-config all username testuser
username testuser password 12RsxXQnphyr/I9Z encrypted privilege 15
```

個々のユーザの属性の設定

特定のユーザを設定するには、**username** コマンドを使用してユーザ名モードに入り、ユーザにパスワード（パスワードなしも可）と属性を割り当てます。指定しなかったすべての属性は、グループ ポリシーから継承されます。

内部ユーザ認証データベースは、**username** コマンドを使用して入力されたユーザで構成されています。**login** コマンドでは、このデータベースを認証用に使用します。ユーザを ASA データベースに追加するには、グローバル コンフィギュレーション モードで **username** コマンドを入力します。ユーザを削除するには、削除するユーザ名を指定して、このコマンドの **no** バージョンを使用します。すべてのユーザ名を削除するには、ユーザ名を指定せずに **clear configure username** コマンドを使用します。

ユーザのパスワードと特権レベルの設定

ユーザにパスワードと特権レベルを割り当てるには、**username** コマンドを入力します。**nopassword** キーワードを入力すると、このユーザにパスワードが不要であることを指定できます。パスワードを指定する場合は、そのパスワードを暗号化形式で保存するかどうかを指定できます。

オプションの **privilege** キーワードにより、このユーザの特権レベルを設定できます。特権レベルの範囲は 0（最低）～ 15 です。一般に、システム管理者は最高の特権レベルを持ちます。デフォルトのレベルは 2 です。

```
hostname(config)# username name {nopassword | password password [encrypted]} [privilege
priv_level]}

hostname(config)# no username [name]
```

表 4-5 に、このコマンドで使用するキーワードと変数の意味を示します。

表 4-5　username コマンドのキーワードと変数

キーワード / 変数	意味
encrypted	パスワードの暗号化を指定します。
name	ユーザの名前を指定します。
nopassword	このユーザにパスワードが必要ないことを示します。
password *password*	このユーザにパスワードが存在することを示し、パスワードを指定します。
privilege *priv_level*	このユーザの特権レベルを設定します。範囲は 0 ～ 15 です。この数値が低いほど、コマンドの使用や ASA の管理に関する機能が限定されます。デフォルトの特権レベルは 2 です。システム管理者の通常の特権レベルは 15 です。

デフォルトでは、このコマンドで追加した VPN ユーザには属性またはグループ ポリシーが関連付けられません。すべての値を明示的に設定する必要があります。

次の例は、暗号化されたパスワードが pw_12345678 で、特権レベルが 12 の anyuser という名前のユーザを設定する方法を示しています。

```
hostname(config)# username anyuser password pw_12345678 encrypted privilege 12
hostname(config)#
```

ユーザ属性の設定

ユーザのパスワード（存在する場合）と特権レベルの設定後は、その他の属性を設定します。これらは任意の順序で設定できます。任意の属性と値のペアを削除するには、このコマンドの **no** 形式を入力します。

attributes キーワードを指定して **username** コマンドを入力して、ユーザ名モードに入ります。

```
hostname(config)# username name attributes
hostname(config-username)#
```

プロンプトが変化し、新しいモードになったことが示されます。これで属性を設定できます。

VPN ユーザ属性の設定

VPN ユーザ属性は、次の項で説明するように、VPN 接続に固有の値を設定します。

継承の設定

ユーザが、それまでにユーザ名レベルで設定されていない属性の値をグループ ポリシーから継承するようにできます。このユーザが属性を継承するグループ ポリシーの名前を指定するには、**vpn-group-policy** コマンドを入力します。デフォルトでは、VPN ユーザにはグループ ポリシーが関連付けられていません。

```
hostname(config-username)# vpn-group-policy group-policy-name
hostname(config-username)# no vpn-group-policy group-policy-name
```

ユーザ名モードで使用できる属性の場合、ユーザ名モードで設定すると、特定のユーザに関してグループ ポリシーにおける属性の値を上書きできます。

次に、FirstGroup という名前のグループ ポリシーから属性を使用するように anyuser という名前のユーザを設定する例を示します。

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-group-policy FirstGroup
hostname(config-username)#
```

アクセス時間の設定

設定済みの time-range ポリシーの名前を指定して、このユーザがシステムへのアクセスを許可される時間を関連付けます。

この属性を実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を入力します。このオプションを使用すると、他のグループ ポリシーから time-range 値を継承できます。値を継承しないようにするには、**vpn-access-hours none** コマンドを入力します。デフォルトでは、アクセスは無制限です。

```
hostname(config-username)# vpn-access-hours value {time-range | none}
hostname(config-username)# vpn-access-hours value none
hostname(config)#
```

次の例は、anyuser という名前のユーザを 824 と呼ばれる time-range ポリシーに関連付ける方法を示しています。

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-access-hours 824
hostname(config-username)#
```

最大同時ログイン数の設定

このユーザに許可される同時ログインの最大数を指定します。指定できる範囲は 0 ～ 2147483647 です。デフォルトの同時ログイン数は、3 です。この属性を実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を入力します。ログインをディセーブルにしてユーザのアクセスを禁止するには、0 を入力します。

```
hostname(config-username)# vpn-simultaneous-logins integer
hostname(config-username)# no vpn-simultaneous-logins
hostname(config-username)# vpn-session-timeout alert-interval none
```

（注） 同時ログインの最大数の制限は非常に大きなものですが、複数の同時ログインを許可すると、セキュリティが低下し、パフォーマンスに影響を及ぼすことがあります。

次の例は、anyuser という名前のユーザに最大 4 つの同時ログインを許可する方法を示しています。

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-simultaneous-logins 4
hostname(config-username)#
```

アイドル タイムアウトの設定

アイドル タイムアウト期間を分単位で指定するか、**none** を入力してアイドル タイムアウトをディセーブルにします。この期間中に接続上で通信アクティビティがない場合、ASA は接続を終了します。任意でアラート間隔を設定することも、1 分のデフォルト設定のままにすることもできます。

範囲は 1 ～ 35791394 分です。デフォルトは 30 分です。無制限のタイムアウト期間を許可し、タイムアウト値を継承しないようにするには、**none** キーワードを指定して **vpn-idle-timeout** コマンドを入力します。この属性を実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を入力します。

```
hostname(config-username)# vpn-idle-timeout {minutes | none} alert-interval {minutes}
hostname(config-username)# no vpn-idle-timeout alert-interval
hostname(config-username)# vpn-idle-timeout alert-interval none
```

次の例は、anyuser という名前のユーザに 15 分の VPN アイドル タイムアウトおよび 3 分のアラート間隔を設定する方法を示しています。

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-idle-timeout 30 alert-interval 3
hostname(config-username)#
```

最大接続時間の設定

ユーザの最大接続時間を分単位で指定するか、**none** を入力して無制限の接続時間を許可し、この属性の値を継承しないようにします。この期間が終了すると、ASA は接続を終了します。任意でアラート間隔を設定することも、1 分のデフォルト設定のままにすることもできます。

範囲は 1 ～ 35791394 分です。デフォルトのタイムアウトはありません。無制限のタイムアウト期間を許可し、タイムアウト値を継承しないようにするには、**none** キーワードを指定して **vpn-session-timeout** コマンドを入力します。この属性を実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を入力します。

```
hostname(config-username)# vpn-session-timeout {minutes | none} alert-interval {minutes}
hostname(config-username)# no vpn-session-timeout alert-interval
hostname(config-username)#
```

次の例は、anyuser という名前のユーザに 180 分の VPN セッション タイムアウトを設定する方法を示しています。

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-session-timeout 180 alert-interval {minutes}
hostname(config-username)#
```

ACL フィルタの適用

VPN 接続用のフィルタとして使用する、事前に設定されたユーザ固有の ACL の名前を指定します。ACL を拒否し、グループ ポリシーから ACL を継承しないようにするには、none キーワードを指定して **vpn-filter** コマンドを入力します。**vpn-filter none** コマンドを発行して作成したヌル値を含めて、ACL を削除するには、このコマンドの **no** 形式を入力します。**no** オプションを使用すると、値をグループ ポリシーから継承できます。このコマンドには、デフォルトの動作や値はありません。

ACL を設定して、このユーザについて、さまざまなタイプのトラフィックを許可または拒否します。次に、**vpn-filter** コマンドを使用して、それらの ACL を適用します。

```
hostname(config-username)# vpn-filter {value ACL_name | none}
hostname(config-username)# no vpn-filter
hostname(config-username)#
```

（注） クライアントレス SSL VPN は、**vpn-filter** コマンドで定義されている ACL を使用しません。

次に、anyuser という名前のユーザの、acl_vpn という ACL を呼び出すフィルタを設定する例を示します。

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-filter value acl_vpn
hostname(config-username)#
```

IPv4 アドレスとネットマスクの指定

特定のユーザに割り当てる IP アドレスとネットマスクを指定します。IP アドレスを削除するには、このコマンドの **no** 形式を入力します。

```
hostname(config-username)# vpn-framed-ip-address {ip_address}
hostname(config-username)# no vpn-framed-ip-address
hostname(config-username)
```

次に、anyuser という名前のユーザに IP アドレス 10.92.166.7 を設定する例を示します。

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-framed-ip-address 10.92.166.7
hostname(config-username)
```

前の手順で指定した IP アドレスに使用するネットワーク マスクを指定します。**no vpn-framed-ip-address** コマンドを使用した場合は、ネットワーク マスクを指定しないでください。サブネット マスクを削除するには、このコマンドの **no** 形式を入力します。デフォルトの動作や値はありません。

```
hostname(config-username)# vpn-framed-ip-netmask {netmask}
hostname(config-username)# no vpn-framed-ip-netmask
hostname(config-username)
```

次の例は、anyuser という名前のユーザに、サブネット マスク 255.255.255.254 を設定する方法を示しています。

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-framed-ip-netmask 255.255.255.254
hostname(config-username)
```

IPv6 アドレスとネットマスクの指定

特定のユーザに割り当てる IPv6 アドレスとネットマスクを指定します。IP アドレスを削除するには、このコマンドの **no** 形式を入力します。

```
hostname(config-username)# vpn-framed-ipv6-address {ip_address}
hostname(config-username)# no vpn-framed-ipv6-address
hostname(config-username)
```

次に、anyuser という名前のユーザに IP アドレスとネットマスク 2001::3000:1000:2000:1/64 を設定する例を示します。このアドレスは、プレフィックス値 2001:0000:0000:0000 およびインターフェイス ID 3000:1000:2000:1 を示しています。

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-framed-ipv6-address 2001::3000:1000:2000:1/64
hostname(config-username)
```

トンネル プロトコルの指定

このユーザが使用できる VPN トンネルのタイプ（IPsec またはクライアントレス SSL VPN）を指定します。デフォルトは、デフォルト グループ ポリシーから取得される値で、IPsec になります。この属性を実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を入力します。

```
hostname(config-username)# vpn-tunnel-protocol {webvpn | IPsec}
hostname(config-username)# no vpn-tunnel-protocol [webvpn | IPsec]
hostname(config-username)
```

このコマンドのパラメータの値は、次のとおりです。

- **IPsec**：2 つのピア（リモート アクセス クライアントまたは別のセキュア ゲートウェイ）間の IPsec トンネルをネゴシエートします。認証、暗号化、カプセル化、およびキー管理を制御するセキュリティ アソシエーションを作成します。
- **webvpn**：HTTPS 対応 Web ブラウザ経由でリモート ユーザにクライアントレス SSL VPN アクセスを提供します。クライアントは不要です。

このコマンドを入力して、1 つ以上のトンネリング モードを設定します。VPN トンネルを介して接続するユーザには、少なくとも 1 つのトンネリング モードを設定する必要があります。

次の例は、anyuser という名前のユーザにクライアントレス SSL VPN および IPsec トンネリング モードを設定する方法を示しています。

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-tunnel-protocol webvpn
hostname(config-username)# vpn-tunnel-protocol IPsec
hostname(config-username)
```

リモート ユーザ アクセスの制限

value キーワードを指定して **group-lock** 属性を設定することにより、指定した既存の接続プロファイルだけを介してアクセスするようにリモート ユーザを制限します。group-lock は、VPN クライアントで設定されたグループが、そのユーザが割り当てられている接続プロファイルと同じかどうかをチェックすることによって、ユーザを制限します。同一ではなかった場合、ASA はユーザによる接続を禁止します。group-lock を設定しなかった場合、ASA は、割り当てられているグループに関係なくユーザを認証します。

group-lock 属性を実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。このオプションを使用すると、値をグループ ポリシーから継承できます。group-lock をディセーブルにし、デフォルトまたは指定されたグループ ポリシーから group-lock の値を継承しないようにするには、**none** キーワードを指定して **group-lock** コマンドを入力します。

```
hostname(config-username)# group-lock {value tunnel-grp-name | none}
hostname(config-username)# no group-lock
hostname(config-username)
```

次の例は、anyuser という名前のユーザにグループ ロックを設定する方法を示しています。

```
hostname(config)# username anyuser attributes
hostname(config-username)# group-lock value tunnel-group-name
hostname(config-username)
```

ソフトウェア クライアント ユーザのパスワード保存のイネーブル化

ユーザがログイン パスワードをクライアント システム上に保存するかどうかを指定します。パスワード保存は、デフォルトでディセーブルになっています。パスワード保存は、セキュアなサイトにあることがわかっているシステムでのみイネーブルにします。パスワード保存をディセーブルにするには、**disable** キーワードを指定して **password-storage** コマンドを入力します。password-storage 属性を実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を入力します。これにより、password-storage の値をグループ ポリシーから継承できます。

```
hostname(config-username)# password-storage {enable | disable}
hostname(config-username)# no password-storage
hostname(config-username)
```

このコマンドは、ハードウェア クライアントのインタラクティブ ハードウェア クライアント認証または個別ユーザ認証には関係ありません。

次の例は、anyuser という名前のユーザでパスワード保存をイネーブルにする方法を示しています。

```
hostname(config)# username anyuser attributes
hostname(config-username)# password-storage enable
hostname(config-username)
```

特定ユーザのクライアントレス SSL VPN アクセスの設定

次の各項では、特定のユーザのクライアントレス SSL VPN セッションの設定をカスタマイズする方法について説明します。ユーザ名コンフィギュレーション モードで **webvpn** コマンドを使用して、ユーザ名 webvpn コンフィギュレーション モードに入ります。クライアントレス SSL VPN によってユーザは、Web ブラウザを使用して ASA へのセキュアなリモート アクセス VPN トンネルを確立できます。ソフトウェアまたはハードウェア クライアントは必要ありません。クライアントレス SSL VPN を使用することで、HTTPS インターネット サイトにアクセスできるほとんどすべてのコンピュータから、幅広い Web リソースおよび Web 対応アプリケーションに簡単にアクセスできます。クライアントレス SSL VPN は SSL およびその後継である TLS1 を使用して、リモート ユーザと、中央サイトで設定した特定のサポートされている内部リソースとの間のセキュアな接続を提供します。ASA はプロキシで処理する必要がある接続を認識し、HTTP サーバは認証サブシステムと対話してユーザを認証します。

ユーザ名 webvpn コンフィギュレーション モードのコマンドは、ファイル、URL、および TCP アプリケーションへのクライアントレス SSL VPN セッション経由のアクセスを定義します。ACL およびフィルタリングするトラフィックのタイプも指定します。クライアントレス SSL VPN は、デフォルトではディセーブルになっています。これらの **webvpn** コマンドは、設定を行ったユーザ名にだけ適用されます。プロンプトが変化して、ユーザ名 webvpn コンフィギュレーション モードに入ったことがわかります。

```
hostname(config-username)# webvpn
hostname(config-username-webvpn)#
```

ユーザ名 webvpn コンフィギュレーション モードで入力したすべてのコマンドを削除するには、このコマンドの **no** 形式を使用します。

```
hostname(config-username)# no webvpn
hostname(config-username)#
```

電子メール プロキシを使用するためにクライアントレス SSL VPN を設定する必要はありません。

（注） グローバル コンフィギュレーション モードから入る webvpn モードでは、クライアントレス SSL VPN セッションのグローバル設定を構成できます。この項で説明した、ユーザ名モードから入ったユーザ名 webvpn コンフィギュレーション モードを使用すると、特定のユーザのクライアントレス SSL VPN セッションのコンフィギュレーションをカスタマイズできます。

ユーザ名 webvpn コンフィギュレーション モードでは、次のパラメータをカスタマイズできます。各パラメータについては、後続の手順で説明します。

- customizations
- deny message
- html-content-filter
- homepage
- filter
- url-list
- port-forward
- port-forward-name
- sso server（シングル サインオン サーバ）
- auto-signon
- AnyConnect Secure Mobility Client
- keep-alive ignore
- HTTP compression

次の例は、ユーザ名 anyuser の属性のユーザ名 webvpn コンフィギュレーション モードに入る方法を示しています。

```
hostname(config)# username anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)#
```

HTML からフィルタリングするコンテンツとオブジェクトの指定

このユーザのクライアントレス SSL VPN セッションの Java、ActiveX、イメージ、スクリプト、およびクッキーをフィルタリングするには、ユーザ名 webvpn コンフィギュレーション モードで **html-content-filter** コマンドを入力します。コンテンツ フィルタを削除するには、このコマンドの **no** 形式を入力します。**html-content-filter none** コマンドを発行して作成したヌル値を含めて、すべてのコンテンツ フィルタを削除するには、引数を指定せずにこのコマンドの **no** 形式を入力します。**no** オプションを使用すると、値をグループ ポリシーから継承できます。HTML コンテンツ フィルタを継承しないようにするには、**html-content-filter none** コマンドを入力します。HTML フィルタリングは、デフォルトでディセーブルです。

次回このコマンドを使用すると、前回までの設定が上書きされます。

```
hostname(config-username-webvpn)# html-content-filter {java | images | scripts | cookies |
none}

hostname(config-username-webvpn)# no html-content-filter [java | images | scripts |
cookies | none]
```

このコマンドで使用するキーワードは、次のとおりです。

- **cookies**：イメージからクッキーを削除して、限定的な広告フィルタリングとプライバシーを提供します。
- **images**：イメージへの参照を削除します（<IMG> タグを削除）。
- **java**：Java および ActiveX への参照を削除します（<EMBED>、<APPLET>、および <OBJECT> の各タグを削除）。
- **none**：フィルタリングを実行しないことを指定します。ヌル値を設定して、フィルタリングを拒否します。フィルタリング値を継承しないようにします。
- **scripts**：スクリプトへの参照を削除します（<SCRIPT> タグを削除）。

次の例は、anyuser という名前のユーザに、Java と ActiveX、クッキー、およびイメージのフィルタリングを設定する方法を示しています。

```
hostname(config)# username anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# html-content-filter java cookies images
hostname(config-username-webvpn)#
```

ユーザ ホームページの指定

このユーザがクライアントレス SSL VPN セッションにログインするときに表示される Web ページの URL を指定するには、ユーザ名 webvpn コンフィギュレーション モードで **homepage** コマンドを入力します。**homepage none** コマンドを発行して作成したヌル値を含めて、設定されているホームページを削除するには、このコマンドの **no** 形式を入力します。**no** オプションを使用すると、値をグループ ポリシーから継承できます。ホームページを継承しないようにするには、**homepage none** コマンドを入力します。

none キーワードは、クライアントレス SSL VPN ホームページがないことを示します。これにより、ヌル値が設定されてホームページが拒否され、ホームページが継承されなくなります。

キーワード *value* の後ろの **url-string** 変数で、ホームページの URL を指定します。http:// または https:// のいずれかで始まるストリングにする必要があります。

デフォルトのホームページはありません。

```
hostname(config-username-webvpn)# homepage {value url-string | none}
hostname(config-username-webvpn)# no homepage
hostname(config-username-webvpn)#
```

次の例は、anyuser という名前のユーザのホームページとして www.example.com を指定する方法を示しています。

```
hostname(config)# username anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# homepage value www.example.com
hostname(config-username-webvpn)#
```

カスタマイゼーションの適用

カスタマイゼーションによって、ログイン時にユーザに表示されるウィンドウの外観が決まります。カスタマイゼーション パラメータは、クライアントレス SSL VPN の設定の一部として設定します。ログイン時にユーザに表示される Web ページのルックアンドフィールを変更するために、事前に定義した Web ページ カスタマイゼーションを適用するには、ユーザ名 webvpn コンフィギュレーション モードで customization コマンドを入力します。

```
hostname(config-username-webvpn)# customization {none | value customization_name}
hostname(config-username-webvpn)#
```

たとえば、blueborder という名前のカスタマイゼーションを使用するには、次のコマンドを入力します。

```
hostname(config-username-webvpn)# customization value blueborder
hostname(config-username-webvpn)#
```

カスタマイゼーション自体は、webvpn モードで **customization** コマンドを入力して設定します。

次の例は、123 という名前のカスタマイゼーションを最初に確立するコマンド シーケンスを示しています。このコマンド シーケンスによって、パスワード プロンプトが定義されます。次に test という名前のトンネルグループを定義し、**customization** コマンドを使用して、123 という名前のカスタマイゼーションを使用することを指定しています。

```
hostname(config)# webvpn
hostname(config-webvpn)# customization 123
hostname(config-webvpn-custom)# password-prompt Enter password
hostname(config-webvpn)# exit
hostname(config)# username testuser nopassword
hostname(config)# username testuser attributes
hostname(config-username-webvpn)# webvpn
hostname(config-username-webvpn)# customization value 123
hostname(config-username-webvpn)#
```

「Deny」メッセージの指定

ユーザ名 webvpn コンフィギュレーション モードで、**deny-message** コマンドを入力すると、クライアントレス SSL VPN セッションに正常にログインできるが VPN 特権を持たないリモート ユーザに送信されるメッセージを指定できます。

```
hostname(config-username-webvpn)# deny-message value "message"
hostname(config-username-webvpn)# no deny-message value "message"
hostname(config-username-webvpn)# deny-message none
```

no deny-message value コマンドは、リモート ユーザがメッセージを受信しないように、メッセージ文字列を削除します。

no deny-message none コマンドは、接続プロファイル ポリシーのコンフィギュレーションから属性を削除します。ポリシーは属性値を継承します。

メッセージは、特殊文字、スペース、および句読点を含む英数字で最大 491 文字まで指定できますが、囲みの引用符はカウントされません。テキストは、ログイン時にリモート ユーザのブラウザに表示されます。**deny-message value** コマンドへのストリングの入力時は、コマンドがラップしている場合でも引き続き入力します。

デフォルトの拒否メッセージは次のとおりです。「Login was successful, but because certain criteria have not been met or due to some specific group policy, you do not have permission to use any of the VPN features. Contact your IT administrator for more information.」

次の例の最初のコマンドは、ユーザ名モードに入り、anyuser という名前のユーザに属性を設定します。後続のコマンドは、ユーザ名 webvpn コンフィギュレーション モードに入り、そのユーザに関連付けられている拒否メッセージを変更します。

```
hostname(config)# username anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# deny-message value "Your login credentials are
OK.However, you have not been granted rights to use the VPN features.Contact your
administrator for more information."
hostname(config-username-webvpn)
```

クライアントレス SSL VPN セッションに使用する ACL の指定

このユーザのクライアントレス SSL VPN セッションに使用する ACL の名前を指定するには、ユーザ名 webvpn コンフィギュレーション モードで **filter** コマンドを入力します。**filter none** コマンドを発行して作成したヌル値を含めて、ACL を削除するには、このコマンドの **no** 形式を入力します。**no** オプションを使用すると、値をグループ ポリシーから継承できます。フィルタの値を継承しないようにするには、**filter value none** コマンドを入力します。

filter コマンドを入力して指定するまで、クライアントレス SSL VPN ACL は適用されません。

ACL を設定して、このユーザについて、さまざまなタイプのトラフィックを許可または拒否します。次に、**filter** コマンドを入力して、これらの ACL をクライアントレス SSL VPN トラフィックに適用します。

```
hostname(config-username-webvpn)# filter {value ACLname | none}
hostname(config-username-webvpn)# no filter
hostname(config-username-webvpn)#
```

none キーワードは、**webvpntype** ACL がないことを示します。これにより、ヌル値が設定されて ACL が拒否され、別のグループ ポリシーから ACL が継承されなくなります。

キーワード **value** の後ろの *ACLname* 文字列で、事前に設定されている ACL の名前を指定します。

（注） クライアントレス SSL VPN は、**vpn-filter** コマンドで定義されている ACL を使用しません。

次に、anyuser という名前のユーザの、*acl_in* という ACL を呼び出すフィルタを設定する例を示します。

```
hostname(config)# username anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# filter acl_in
hostname(config-username-webvpn)#
```

URL リストの適用

クライアントレス SSL VPN セッションを確立したユーザのホームページに URL のリストを表示するように指定できます。最初に、グローバル コンフィギュレーション モードで **url-list** コマンドを入力して、1 つ以上の名前付きリストを作成する必要があります。クライアントレス SSL VPN の特定のユーザにサーバと URL のリストを適用するには、ユーザ名 webvpn コンフィギュレーション モードで **url-list** コマンドを入力します。

url-list none コマンドを使用して作成したヌル値を含めて、リストを削除するには、このコマンドの **no** 形式を入力します。**no** オプションを使用すると、値をグループ ポリシーから継承できます。URL リストを継承しないようにするには、**url-list none** コマンドを入力します。

```
hostname(config-username-webvpn)# url-list {listname displayname url | none}
hostname(config-username-webvpn)# no url-list
```

このコマンドで使用するキーワードと変数は、次のとおりです。

- *displayname*：URL の名前を指定します。この名前は、クライアントレス SSL VPN セッションのポータル ページに表示されます。
- *listname*：URL をグループ化する名前を指定します。
- **none**：URL のリストが存在しないことを示します。ヌル値を設定して、URL リストを拒否します。URL リストの値を継承しないようにします。
- *url*：クライアントレス SSL VPN のユーザがアクセスできる URL を指定します。

デフォルトの URL リストはありません。

次回このコマンドを使用すると、前回までの設定が上書きされます。

次の例は、anyuser という名前のユーザに AnyuserURLs という URL リストを設定する方法を示しています。

```
hostname(config)# username anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# url-list value AnyuserURLs
hostname(config-username-webvpn)#
```

ユーザの ActiveX Relay のイネーブル化

ActiveX Relay を使用すると、クライアントレス SSL VPN セッションを確立したユーザが、ブラウザを使用して Microsoft Office アプリケーションを起動できるようになります。アプリケーションは、セッションを使用して Microsoft Office ドキュメントのダウンロードとアップロードを行います。ActiveX のリレーは、クライアントレス SSL VPN セッションを終了するまで有効なままです。

クライアントレス SSL VPN セッションの ActiveX コントロールをイネーブルまたはディセーブルにするには、ユーザ名 webvpn コンフィギュレーション モードで次のコマンドを入力します。

activex-relay {**enable** | **disable**}

グループ ポリシーから **activex-relay** コマンドを継承するには、次のコマンドを入力します。

no activex-relay

次のコマンドは、特定のユーザ名に関連付けられているクライアントレス SSL VPN セッションの ActiveX コントロールをイネーブルにします。

```
hostname(config-username-policy)# webvpn
hostname(config-username-webvpn)# activex-relay enable
hostname(config-username-webvpn)
```

クライアントレス SSL VPN セッションのアプリケーション アクセスのイネーブル化

このユーザのアプリケーション アクセスをイネーブルにするには、ユーザ名 webvpn コンフィギュレーション モードで **port-forward** コマンドを入力します。ポート転送は、デフォルトではディセーブルになっています。

port-forward none コマンドを発行して作成したヌル値を含めて、コンフィギュレーションからポート転送属性を削除するには、このコマンドの **no** 形式を入力します。**no** オプションを使用すると、リストをグループ ポリシーから継承できます。フィルタリングを拒否してポート転送リストを継承しないようにするには、**none** キーワードを指定して **port-forward** コマンドを入力します。

```
hostname(config-username-webvpn)# port-forward {value listname | none}
hostname(config-username-webvpn)# no port-forward
hostname(config-username-webvpn)#
```

キーワード **value** の後ろの *listname* 文字列で、クライアントレス SSL VPN のユーザがアクセスできるアプリケーションのリストを指定します。コンフィギュレーション モードで **port-forward** コマンドを入力して、このリストを定義します。

次回このコマンドを使用すると、前回までの設定が上書きされます。

ユーザ名 webvpn コンフィギュレーション モードで **port-forward** コマンドを入力し、アプリケーション アクセスをイネーブルにする前に、クライアントレス SSL VPN セッションでユーザが使用できるアプリケーションのリストを定義する必要があります。グローバル コンフィギュレーション モードで **port-forward** コマンドを入力して、このリストを定義します。

次の例は、ports1 というポート転送リストを設定する方法を示しています。

```
hostname(config-group-policy)# webvpn
hostname(config-username-webvpn)# port-forward value ports1
hostname(config-username-webvpn)#
```

ポート転送表示名の設定

ユーザ名 webvpn コンフィギュレーション モードで **port-forward-name** コマンドを使用して、特定のユーザでエンド ユーザへの TCP ポート転送を識別する表示名を設定します。**port-forward-name none** コマンドを使用して作成したヌル値を含めて、表示名を削除するには、このコマンドの **no** 形式を入力します。**no** オプションは、デフォルト名の、Application Access を復元します。表示名を使用しないようにするには、**port-forward none** コマンドを入力します。

```
hostname(config-username-webvpn)# port-forward-name {value name | none}
hostname(config-username-webvpn)# no port-forward-name
```

次の例は、ポート転送名 test を設定する方法を示しています。

```
hostname(config-group-policy)# webvpn
hostname(config-username-webvpn)# port-forward-name value test
hostname(config-username-webvpn)#
```

セッション タイマー更新のために無視する最大オブジェクト サイズの設定

ネットワーク デバイスは、短いキープアライブ メッセージを交換して、デバイス間の仮想回路が引き続きアクティブであることを確認します。これらのメッセージの長さは異なる可能性があります。**keep-alive-ignore** コマンドを使用すると、指定したサイズ以下のすべてのメッセージをキープアライブ メッセージと見なし、セッション タイマーの更新時にトラフィックと見なさないよう ASA に指示できます。範囲は 0 ～ 900 KB です。デフォルトは 4 KB です。

トランザクションごとに無視する HTTP/HTTPS トラフィックの上限を指定するには、グループ ポリシー属性 webvpn コンフィギュレーション モードで **keep-alive-ignore** コマンドを使用します。

```
hostname(config-group-webvpn)# keep-alive-ignore size
hostname(config-group-webvpn)#
```

このコマンドの **no** 形式は、この指定をコンフィギュレーションから削除します。

```
hostname(config-group-webvpn)# no keep-alive-ignore
hostname(config-group-webvpn)#
```

次の例では、無視するオブジェクトの最大サイズを 5 KB に設定します。

```
hostname(config-group-webvpn)# keep-alive-ignore 5
hostname(config-group-webvpn)#
```

自動サインオンの設定

NTLM、基本 HTTP 認証、またはその両方を使用する内部サーバに、特定のクライアントレス SSL VPN のユーザのログイン クレデンシャルを自動的に渡すには、ユーザ名 webvpn コンフィギュレーション モードで **auto-signon** コマンドを使用します。

auto-signon コマンドは、クライアントレス SSL VPN セッションのユーザ用のシングル サインオン方式です。NTLM 認証、基本認証、またはその両方を使用する認証のためにログイン クレデンシャル（ユーザ名とパスワード）を内部サーバに渡します。複数の auto-signon コマンドを入力でき、それらのコマンドは入力順に処理されます（先に入力したコマンドが優先されます）。

自動サインオン機能は、webvpn コンフィギュレーション、webvpn グループ コンフィギュレーション、または webvpn ユーザ名コンフィギュレーション モードの 3 つのモードで使用できます。ユーザ名がグループに優先し、グループがグローバルに優先するという標準的な優先動作が適用されます。選択するモードは、使用する認証の対象範囲によって異なります。

特定のサーバへの特定のユーザの自動サインオンをディセーブルにするには、元の IP ブロックまたは URL を指定してこのコマンドの **no** 形式を使用します。すべてのサーバへの認証をディセーブルにするには、引数を指定しないで **no** 形式を使用します。**no** オプションを使用すると、値をグループ ポリシーから継承できます。

次のコマンド例では、基本認証または NTLM 認証を使用して、anyuser という名前のクライアントレス SSL VPN のユーザに対し、URI マスク https://*.example.com/* で定義されたサーバへのアクセスに自動サインオンを設定します。

```
hostname(config)# username anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# auto-signon allow uri https://*.example.com/* auth-type
all
```

次のコマンド例では、基本認証または NTLM 認証を使用して、anyuser という名前のクライアントレス SSL VPN のユーザに対し、サブネット マスク 255.255.255.0 を使用する IP アドレス 10.1.1.0 のサーバへの自動サインオンを設定します。

```
hostname(config)# username anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# auto-signon allow ip 10.1.1.0 255.255.255.0 auth-type
all
hostname(config-username-webvpn)#
```

HTTP 圧縮の指定

ユーザ名 webvpn コンフィギュレーション モードで、**http-comp** コマンドを入力し、特定のユーザのクライアントレス SSL VPN セッションで HTTP データの圧縮をイネーブルにします。

```
hostname(config-username-webvpn)# http-comp {gzip | none}
hostname(config-username-webvpn)#
```

コンフィギュレーションからコマンドを削除し、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

```
hostname(config-username-webvpn)# no http-comp {gzip | none}
hostname(config-username-webvpn)#
```

このコマンドの構文は次のとおりです。

- **gzip**：圧縮がグループまたはユーザに対してイネーブルになることを指定します。これはデフォルト値です。
- **none**：圧縮がグループまたはユーザに対してディセーブルになることを指定します。

クライアントレス SSL VPN セッションの場合、グローバル コンフィギュレーション モードで設定された **compression** コマンドは、グループ ポリシー webvpn モードおよびユーザ名 webvpn モードで設定された **http-comp** コマンドを上書きします。

次の例は、testuser というユーザ名で圧縮をディセーブルにしています。

```
hostname(config)# username testuser internal
hostname(config)# username testuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# http-comp none
hostname(config-username-webvpn)#
```

SSO サーバの指定

クライアントレス SSL VPN セッションだけに使用できるシングル サインオンのサポートを使用すると、ユーザはユーザ名とパスワードを複数回入力しなくても、さまざまなサーバのセキュアな各種のサービスにアクセスできます。**sso-server value** コマンドをユーザ名 webvpn モードで入力すると、SSO サーバをユーザに割り当てることができます。

SSO サーバをユーザに割り当てるには、ユーザ名 webvpn コンフィギュレーション モードで **sso-server value** コマンドを使用します。このコマンドでは、コンフィギュレーションに CA SiteMinder コマンドが含まれている必要があります。

```
hostname(config-username-webvpn)# sso-server value server_name
hostname(config-username-webvpn)#
```

割り当てを削除してデフォルト ポリシーを使用するには、このコマンドの **no** 形式を使用します。デフォルト ポリシーが継承されないようにするには、**sso-server none** コマンドを使用します。

```
hostname(config-username-webvpn)# sso-server {value server_name | none}
hostname(config-username-webvpn)# [no] sso-server value server_name
```

SSO サーバに割り当てられているデフォルト ポリシーは DfltGrpPolicy です。

次の例は、example という名前の SSO サーバを anyuser という名前のユーザに割り当てます。

```
hostname(config)# username anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# sso-server value example
hostname(config-username-webvpn)#
```

CHAPTER 5

VPN の IP アドレス

この章では、IP アドレスの割り当て方式について説明します。

インターネットワーク接続は、IP アドレスによって可能になります。IP アドレスは、送信者と受信者の両方に接続用の番号が割り当てられている必要があるという点で、電話番号に似ています。ただし、VPN では、実際には 2 セットのアドレスが存在します。最初のセットは、パブリック ネットワーク上でクライアントとサーバを接続します。この接続が確立されると、2 番目のセットが VPN トンネル経由でクライアントとサーバを接続します。

ASA のアドレス管理では、この IP アドレスの 2 番目のセットを扱います。これらのプライベート IP アドレスは、クライアントをトンネル経由でプライベート ネットワーク上のリソースに接続し、プライベート ネットワークに直接接続されているかのようなクライアント機能を提供します。また、ここでは、クライアントに割り当てられたプライベート IP アドレスのみを扱います。プライベート ネットワーク上のその他のリソースに割り当てられた IP アドレスは、VPN 管理ではなく、ネットワーク管理業務の一部に位置づけられます。したがって、ここで IP アドレスに言及する場合は、クライアントをトンネルのエンドポイントとして機能させる、プライベート ネットワークのアドレッシング方式で取得される IP アドレスを意味します。

IP アドレスの割り当てポリシーの設定

ASA では、リモート アクセス クライアントに IP アドレスを割り当てる際に、次の 1 つ以上の方式を使用することができます。複数のアドレス割り当て方式を設定すると、ASA は IP アドレスが見つかるまで各オプションを検索します。デフォルトでは、すべての方式がイネーブルになっています。

- aaa：ユーザ単位で外部認証、認可、アカウンティング サーバからアドレスを取得します。IP アドレスが設定された認証サーバを使用している場合は、この方式を使用することをお勧めします。[Configuration] >[AAA Setup] ペインで AAA サーバを設定できます。この方法は IPv4 および IPv6 の割り当てポリシーに使用できます。
- dhcp：DHCP サーバから IP アドレスを取得します。DHCP を使用する場合は、DHCP サーバを設定する必要があります。また、DHCP サーバで使用可能な IP アドレスの範囲も定義する必要があります。この方法は IPv4 の割り当てポリシーに使用できます。

- **local**：内部的に設定されたアドレス プールは、最も設定が簡単なアドレス プール割り当て方式です。ローカルを選択する場合は、**ip-local-pool** コマンドを使用して、使用する IP アドレスの範囲を定義する必要があります。この方法は IPv4 および IPv6 の割り当てポリシーに使用できます。
  - [Allow the reuse of an IP address so many minutes after it is released]：IP アドレスがアドレス プールに戻された後に、IP アドレスを再利用するまでの時間を指定します。遅延時間を設けることにより、IP アドレスがすぐに再割り当てされることによって発生する問題がファイアウォールで生じないようにできます。デフォルトでは、つまり、ASA は遅延時間を課しません。この設定要素は IPv4 の割り当てポリシーに使用できます。

次の方法のいずれかを使用して、IP アドレスをリモート アクセス クライアントに割り当てる方法を指定します。

- コマンドラインでの IPv4 アドレス割り当ての設定
- コマンドラインでの IPv6 アドレス割り当ての設定

コマンドラインでの IPv4 アドレス割り当ての設定

コマンド	目的
vpn-addr-assign {aaa | dhcp | local [reuse-delay *minutes*]**}** **例：** hostname(config)# **vpn-addr-assign aaa** **例：** hostname(config)# **vpn-addr-assign local reuse-delay 180** **例：** hostname(config)# **no vpn-addr-assign dhcp**	ASA のアドレス割り当て方式をイネーブルにして、IPv4 アドレスを VPN 接続に割り当てるときに使用します。IP アドレスを取得する使用可能な方式は、AAA サーバ、DHCP サーバ、またはローカル アドレス プールからの取得です。これらの方式はすべてデフォルトでイネーブルになっています。 ローカル IP アドレス プールの場合、IP アドレスが解放された後に 0 ～ 480 分間の IP アドレスの再使用を設定できます。 アドレス割り当て方式をディセーブルにするには、コマンドの no 形式を使用します。

コマンドラインでの IPv6 アドレス割り当ての設定

コマンド	目的
ipv6-vpn-addr-assign {aaa | local} **例：** hostname(config)# **ipv6-vpn-addr-assign aaa** **例：** hostname(config)# **no ipv6-vpn-addr-assign local**	ASA のアドレス割り当て方式をイネーブルにして、IPv6 アドレスを VPN 接続に割り当てるときに使用します。IP アドレスを取得する使用可能な方式は、AAA サーバまたはローカル アドレス プールからの取得です。これら両方の方式はデフォルトでイネーブルになっています。 アドレス割り当て方式をディセーブルにするには、コマンドの no 形式を使用します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	トランスペアレント	シングル	コンテキスト	システム
•	—	•	—	—

アドレス割り当て方式の表示

ASA で設定されているアドレス割り当て方式を表示するには、次のいずれかの方式を使用します。

コマンドラインからの IPv4 アドレス割り当ての表示

コマンド	目的
show running-config all vpn-addr-assign **例：** hostname(config)# show running-config all vpn-addr-assign	設定されているアドレス割り当て方式を示します。設定されているアドレス方式は、aaa、dhcp、または local となります。 vpn-addr-assign aaa vpn-addr-assign dhcp vpn-addr-assign local

コマンドラインからの IPv6 アドレス割り当ての表示

コマンド	目的
show running-config all ipv6-vpn-addr-assign **例：** hostname(config)# show running-config all ipv6-vpn-addr-assign	設定されているアドレス割り当て方式を示します。設定されているアドレス方式は、aaa または local となります。 ipv6-vpn-addr-assign aaa ipv6-vpn-addr-assign local reuse-delay 0

ローカル IP アドレス プールの設定

VPN リモート アクセス トンネルに使用する IPv4 アドレス プールを設定するには、グローバル コンフィギュレーション モードで **ip local pool** コマンドを入力します。アドレス プールを削除するには、このコマンドの **no** 形式を入力します。

VPN リモート アクセス トンネルに使用する IPv6 アドレス プールを設定するには、グローバル コンフィギュレーション モードで **ipv6 local pool** コマンドを入力します。アドレス プールを削除するには、このコマンドの **no** 形式を入力します。

ASA は、接続の接続プロファイルまたはグループ ポリシーに基づいてアドレス プールを使用します。プールの指定順序は重要です。接続プロファイルまたはグループ ポリシーに複数のアドレス プールを設定する場合、ASA はそれらを ASA に追加した順序で使用します。

ローカルでないサブネットのアドレスを割り当てる場合は、そのようなネットワーク用のルートの追加が容易になるように、サブネットの境界を担当するプールを追加することをお勧めします。

ローカル IP アドレス プールを設定するには、次のいずれかの方法を使用します。

- 「CLI を使用したローカル IPv4 アドレス プールの設定」（P.5-4）
- 「CLI を使用したローカル IPv6 アドレス プールの設定」（P.5-5）

CLI を使用したローカル IPv4 アドレス プールの設定

	コマンド	目的
ステップ 1	**vpn-addr-assign local** **例：** hostname(config)# **vpn-addr-assign local**	**local** 引数を指定して **vpn-addr-assign** コマンドを入力し、アドレス割り当て方式として IP アドレス プールを設定します。「コマンドラインでの IPv4 アドレス割り当ての設定」（P.5-2）も参照してください。
ステップ 2	**ip local pool** *poolname first_address–last_address* **mask** *mask* **例：** hostname(config)# ip local pool **firstpool** **10.20.30.40-10.20.30.50** mask **255.255.255.0** **例：** hostname(config)# no ip local pool **firstpool**	アドレス プールを設定します。このコマンドは、プールの名前を指定し、IPv4 アドレスとサブネット マスクの範囲を指定します。 最初の例では、**firstpool** という名前で IP アドレス プールを設定しています。開始アドレスは **10.20.30.40** で、最終アドレスは **10.20.30.50** です。ネットワーク マスクは **255.255.255.0** です。 2 番目の例では、**firstpool** という名前の IP アドレス プールを削除しています。

CLI を使用したローカル IPv6 アドレス プールの設定

	コマンド	目的
ステップ 1	**ipv6-vpn-addr-assign local** **例：** hostname(config)# **ipv6-vpn-addr-assign local**	**local** 引数を指定して **ipv6-vpn-addr-assign** コマンドを入力し、アドレス割り当て方式として IP アドレス プールを設定します。「コマンドラインでの IPv6 アドレス割り当ての設定」（P.5-2）も参照してください。
ステップ 2	**ipv6 local pool** *pool_name starting_address prefix_length number_of_addresses* **例：** hostname(config)# **ipv6 local pool** *ipv6pool 2001:DB8::1/32 100* **例：** hostname(config)# **no ipv6 local pool** *ipv6pool*	アドレス プールを設定します。このコマンドは、プールに名前を指定し、開始 IPv6 アドレス、ビット単位のプレフィックス長、および範囲内で使用するアドレスの数を特定します。 最初の例では、**ipv6pool** という名前で IP アドレス プールを設定しています。開始アドレスは **2001:DB8::1**、プレフィックス長は **32** ビット、プールで使用するアドレス数は **100** です。 2 番目の例では、**ipv6pool** という名前の IP アドレス プールを削除しています。

ASDM で内部アドレス プールをグループ ポリシーに割り当てる

[Add or Edit Group Policy] ダイアログボックスでは、追加または編集している内部ネットワーク（クライアント）アクセス グループ ポリシーのアドレス プール、トンネリング プロトコル、フィルタ、接続設定、およびサーバを指定できます。このダイアログボックスの各フィールドで、[Inherit] チェックボックスを選択すると、対応する設定の値をデフォルト グループ ポリシーから取得できます。[Inherit] は、このダイアログボックスの属性すべてのデフォルト値です。

同じグループ ポリシーで IPv4 と IPv6 両方のアドレス プールを設定できます。同じグループ ポリシーに両方のバージョンの IP アドレスが設定されている場合、IPv4 に設定されたクライアントは IPv4 アドレス、IPv6 に設定されたクライアントは IPv6 アドレスを取得し、IPv4 アドレスと IPv6 アドレス両方に設定されたクライアントは IPv4 アドレスと IPv6 アドレス両方を取得します。

ステップ 1　ASDM を使用して ASA に接続し、**[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies]** を選択します。

ステップ 2　新しいグループ ポリシーまたは内部アドレス プールで設定するグループ ポリシーを作成し、[**Edit**] をクリックします。

[General attributes] ペインは [group policy] ダイアログで、デフォルトで選択されています。

ステップ 3　[Address Pools] フィールドを使用して、このグループ ポリシーの IPv4 アドレス プールを指定します。[Select] をクリックし、IPv4 アドレス プールを追加または編集します。

ステップ 4　[IPv6 Address Pools] フィールドを使用して、このグループ ポリシーに使用する IPv6 アドレス プールを指定します。[Select] をクリックし、IPv6 アドレス プールを追加または編集します。

ステップ 5　[**OK**] をクリックします。

ステップ 6　[**Apply**] をクリックします。

AAA アドレッシングの設定

AAA サーバを使用して VPN リモート アクセス クライアントにアドレスを割り当てるには、まず AAA サーバまたは AAA サーバ グループを設定する必要があります。コマンド リファレンスで **aaa-server protocol** コマンドを参照してください。

また、ユーザは RADIUS 認証用に設定された接続プロファイルと一致している必要があります。

次の例は、firstgroup という名前のトンネル グループに、RAD2 という AAA サーバ グループを定義する方法を示しています。例の中に 1 つ余分な手順が入っていますが、これは以前にそのトンネル グループに名前を付け、トンネル グループ タイプを定義していた場合のためです。この手順が次の例に記載されているのは、これらの値を設定しない限り、後続の tunnel-group コマンドにアクセスできないので、注意を促すためです。

この例で作成されるコンフィギュレーションの概要は、次のとおりです。

```
hostname(config)# vpn-addr-assign aaa
hostname(config)# tunnel-group firstgroup type ipsec-ra
hostname(config)# tunnel-group firstgroup general-attributes
hostname(config-general)# authentication-server-group RAD2
```

IP アドレッシング用に AAA を設定するには、次の手順を実行します。

ステップ 1　アドレス割り当て方式として AAA を設定するには、**aaa** 引数を指定して **vpn-addr-assign** コマンドを入力します。

```
hostname(config)# vpn-addr-assign aaa
hostname(config)#
```

ステップ 2　firstgroup というトンネル グループをリモート アクセスまたは LAN-to-LAN トンネル グループとして確立するには、**type** キーワードを指定して **tunnel-group** コマンドを入力します。次の例では、リモート アクセス トンネル グループを設定しています。

```
hostname(config)# tunnel-group firstgroup type ipsec-ra
hostname(config)#
```

ステップ 3　一般属性コンフィギュレーション モードに入り、firstgroup というトンネル グループの AAA サーバ グループを定義するには、**general-attributes** 引数を指定して **tunnel-group** コマンドを入力します。

```
hostname(config)# tunnel-group firstgroup general-attributes
hostname(config-general)#
```

ステップ 4　認証に使用する AAA サーバ グループを指定するには、**authentication-server-group** コマンドを入力します。

```
hostname(config-general)# authentication-server-group RAD2
hostname(config-general)#
```

このコマンドには、この例で示すより多くの引数があります。詳細については、コマンド リファレンスを参照してください。

DHCP アドレッシングの設定

DHCP を使用して VPN クライアントのアドレスを割り当てるには、まず DHCP サーバ、およびその DHCP サーバで使用可能な IP アドレスの範囲を設定する必要があります。その後、接続プロファイル単位で DHCP サーバを定義します。また、オプションとして、該当の接続プロファイルまたはユーザ名に関連付けられたグループ ポリシー内に、DHCP ネットワーク スコープも定義できます。このスコープは、使用する IP アドレス プールを DHCP サーバに指定するための、IP ネットワーク番号または IP アドレスです。

次の例では、**firstgroup** という名前の接続プロファイルに、IP アドレス 172.33.44.19 の DHCP サーバを定義しています。また、この例では、**remotegroup** というグループ ポリシーに対して、192.86.0.0 という DHCP ネットワーク スコープも定義しています（remotegroup というグループ ポリシーは、firstgroup という接続プロファイルに関連付けられています）。ネットワーク スコープを定義しない場合、DHCP サーバはアドレス プールの設定順にプール内を探して IP アドレスを割り当てます。未割り当てのアドレスが見つかるまで、プールが順に検索されます。

次のコンフィギュレーションには、本来不要な手順が含まれています。これらは、以前にその接続プロファイルに名前を付け、接続プロファイル タイプをリモート アクセスとして定義していたり、グループ ポリシーに名前を付け、内部または外部として指定していた場合のためです。これらの手順が次の例に記載されているのは、これらの値を設定しない限り、後続の tunnel-group コマンドおよび group-policy コマンドにアクセスできないので、注意を促すためです。

ガイドラインと制限事項

クライアント アドレスを割り当てる DHCP サーバの識別には IPv4 のみ使用できます。

CLI を使用した DHCP アドレッシングの設定

	コマンド	目的
ステップ 1	`vpn-addr-assign dhcp`	アドレス割り当て方式として IP アドレス プールを設定します。**dhcp** 引数を指定して **vpn-addr-assign** コマンドを入力します。「コマンドラインでの IPv4 アドレス割り当ての設定」（P.5-2）も参照してください。
ステップ 2	`tunnel-group firstgroup type remote-access`	リモート アクセス接続プロファイルとして firstgroup という接続プロファイルを確立します。 **type** キーワードおよび **remote-access** 引数を指定して **tunnel-group** コマンドを入力します。
ステップ 3	`tunnel-group firstgroup general-attributes`	DHCP サーバを設定できるように、接続プロファイルの一般属性コンフィギュレーション モードを開始します。 **general-attributes** 引数を指定して **tunnel-group** コマンドを入力します。

	コマンド	目的
ステップ 4	dhcp-server *IPv4_address_of_DHCP_server* 例： hostname(config-general)# dhcp-server **172.33.44.19** hostname(config-general)#	IPv4 アドレスで DHCP サーバを定義します。IPv6 アドレスで DHCP サーバを定義することはできません。接続プロファイルに複数の DHCP サーバ アドレスを指定できます。 **dhcp-server** コマンドを入力します。このコマンドを使用すると、VPN クライアントの IP アドレスを取得しようとしているときに指定した DHCP サーバに追加のオプションを送信するように ASA を設定できます。詳細については、『*Cisco Security Appliance Command Reference*』の **dhcp-server** コマンドを参照してください。 この例では、IP アドレス 172.33.44.19 の DHCP サーバを設定しています。
ステップ 5	hostname(config-general)# **exit** hostname(config)#	トンネル グループ モードを終了します。
ステップ 6	hostname(config)# group-policy remotegroup **internal**	**remotegroup** という内部グループ ポリシーを作成します。 内部グループ ポリシーを作成するには、**internal** 引数を指定して **group-policy** コマンドを入力します。 この例では、内部グループを設定しています。
ステップ 7	hostname(config)# group-policy remotegroup **attributes** 例： hostname(config)# group-policy remotegroup **attributes** hostname(config-group-policy)#	（オプション）グループ ポリシー属性コンフィギュレーション モードを開始し、DHCP サーバで使用する IP アドレスのサブネットワークを設定します。 **attributes** キーワードを指定して **group-policy** コマンドを入力します。 この例では、**remotegroup** グループ ポリシーのグループ ポリシー属性コンフィギュレーション モードを開始しています。

	コマンド	目的
ステップ 8	`hostname(config-group-policy)# dhcp-network-scope 192.86.0.0` `hostname(config-group-policy)#`	（オプション）**remotegroup** というグループ ポリシーのユーザにアドレスを割り当てるために DHCP サーバで使用する IP アドレスの範囲を指定するには、**dhcp-network-scope** コマンドを入力します。 この例では、192.86.0.0 というネットワーク スコープを設定しています。 **（注）** dhcp-network-scope は、DHCP プールのサブセットではなく、ルーティング可能な IP アドレスである必要があります。DHCP サーバは、この IP アドレスが属するサブネットを判別し、そのプールからの IP アドレスを割り当てます。ルーティングの理由により、ASA のインターフェイスを dhcp-network-scope として使用することをお勧めします。任意の IP アドレスを dhcp-network-scope として使用できますが、ネットワークにスタティック ルートを追加する必要がある場合があります。

例

この例で作成されるコンフィギュレーションの概要は、次のとおりです。

```
hostname(config)# vpn-addr-assign dhcp
hostname(config)# tunnel-group firstgroup type remote-access
hostname(config)# tunnel-group firstgroup general-attributes
hostname(config-general)# dhcp-server 172.33.44.19
hostname(config-general)# exit
hostname(config)# group-policy remotegroup internal
hostname(config)# group-policy remotegroup attributes
hostname(config-group-policy)# dhcp-network-scope 192.86.0.0
```

ローカル ユーザへの IP アドレスの割り当て

グループ ポリシーを使用するようにローカル ユーザ アカウントを設定し、また AnyConnect 属性を設定することもできます。IP アドレスの他のソースに障害が発生した場合に、これらのユーザ アカウントがフォールバックを提供するので、管理者は引き続きアクセスできます。

ここでは、ローカル ユーザのすべての属性を設定する方法について説明します。

前提条件

この手順では、既存のユーザを編集する方法について説明します。ユーザを追加するには、**[Configuration] > [Remote Access VPN] > [AAA/Local Users] > [Local Users]** を選択し、**[Add]** をクリックします。詳細については、一般的な操作のコンフィギュレーション ガイドを参照してください。

ユーザの編集

デフォルトでは、[Edit User Account] 画面の設定ごとに **[Inherit]** チェックボックスがオンになっています。つまり、ユーザ アカウントは、デフォルト グループ ポリシー DfltGrpPolicy のその設定の値を継承するということです。

各設定内容を上書きする場合は、**[Inherit]** チェックボックスをオフにし、新しい値を入力します。次の「手順の詳細」で、[Edit User Account] 画面の各設定について説明しています。

手順の詳細

ステップ 1　ASDM を開始し、**[Configuration] > [Remote Access VPN] > [AAA/Local Users] > [Local Users]** を選択します。

ステップ 2　設定するユーザを選択し、**[Edit]** をクリックします。

[Edit User Account] 画面が開きます。

ステップ 3　左側のペインで、**[VPN Policy]** をクリックします。

ステップ 4　ユーザのグループ ポリシーを指定します。ユーザ ポリシーは、このグループ ポリシーの属性を継承します。この画面にデフォルト グループ ポリシーの設定を継承するよう設定されている他のフィールドがある場合、このグループ ポリシーで指定された属性がデフォルト グループ ポリシーの属性より優先されます。

ステップ 5　ユーザが使用できるトンネリング プロトコルを指定するか、グループ ポリシーから値を継承するかどうかを指定します。目的の **[Tunneling Protocols]** チェックボックスをオンにし、使用できる VPN トンネリング プロトコルを選択します。選択されたプロトコルのみが使用可能になります。次の選択肢があります。

- （SSL/TLS を利用する VPN）クライアントレス SSL VPN では、Web ブラウザを使用して VPN コンセントレータへのセキュアなリモート アクセス トンネルを確立し、ソフトウェア クライアントもハードウェア クライアントも必要としません。クライアントレス SSL VPN を使用すると、HTTPS インターネット サイトを利用できるほとんどすべてのコンピュータから、企業の Web サイト、Web 対応アプリケーション、NT/AD ファイル共有（Web 対応）、電子メール、およびその他の TCP ベース アプリケーションなど、幅広い企業リソースに簡単にアクセスできるようになります。
- SSL VPN クライアントは、Cisco AnyConnect Client アプリケーションのダウンロード後にユーザが接続できるようにします。ユーザは、最初にクライアントレス SSL VPN 接続を使用してこのアプリケーションをダウンロードします。ユーザが接続するたびに、必要に応じてクライアント アップデートが自動的に行われます。
- [IPsec IKEv1]：IP セキュリティ プロトコル。IPsec は最もセキュアなプロトコルとされており、VPN トンネルのほぼ完全なアーキテクチャを提供します。Site-to-Site（ピアツーピア）接続、および Cisco VPN Client と LAN 間の接続の両方で IPsec IKEv1 を使用できます。
- [IPsec IKEv2]：AnyConnect Secure Mobility Client 対応の IPsec IKEv2。IKEv2 を使用した IPsec による AnyConnect 接続では、SSL VPN 接続が使用できる同じ機能セットを利用できます。
- L2TP over IPSec では、複数の PC やモバイル PC に採用されている一般的なオペレーティング システムに付属の VPN クライアントを使用するリモート ユーザが、パブリック IP ネットワークを介して ASA およびプライベート企業ネットワークへのセキュアな接続を確立できるようにします。

（注）　プロトコルを選択しなかった場合は、エラー メッセージが表示されます。

ステップ 6　使用するフィルタ（IPv4 または IPv6）を指定するか、またはグループ ポリシーの値を継承するかどうかを指定します。フィルタは、ASA を経由して着信したトンネリングされたデータ パケットを、送信元アドレス、宛先アドレス、プロトコルなどの基準によって、許可するか拒否するかを決定するルールで構成されます。フィルタおよびルールを設定するには、**[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] > [Add/Edit] > [General] > [More Options] > [Filter]** を選択します。

[Manage] をクリックして、ACL と ACE を追加、編集、および削除できる [ACL Manager] ペインを表示します。

ステップ 7　接続プロファイル（トンネル グループ）ロックを継承するかどうか、または選択したトンネル グループ ロックがあればそれを使用するかどうかを指定します。特定のロックを選択すると、ユーザのリモート アクセスはこのグループだけに制限されます。[Tunnel Group Lock] では、VPN クライアントで設定されたグループと、そのユーザが割り当てられているグループが同じかどうかをチェックすることによって、ユーザが制限されます。同一ではなかった場合、ASA はユーザによる接続を禁止します。[Inherit] チェックボックスがオフの場合、デフォルト値は [None] です。

ステップ 8　[Store Password on Client System] 設定をグループから継承するかどうかを指定します。**[Inherit]** チェックボックスをオフにすると、[Yes] および [No] のオプション ボタンが有効になります。**[Yes]** をクリックすると、ログオン パスワードがクライアント システムに保存されます（セキュリティが低下するおそれのあるオプションです）。接続ごとにユーザにパスワードの入力を求めるようにするには、**[No]** をクリックします（デフォルト）。セキュリティを最大限に確保するためにも、パスワードの保存は*許可しない*ことを推奨します。

ステップ 9　このユーザに適用するアクセス時間ポリシーを指定する、そのユーザの新しいアクセス時間ポリシーを作成する、または [Inherit] チェックボックスをオンのままにします。デフォルトは [Inherit] です。また、[Inherit] チェックボックスがオフの場合のデフォルトは [Unrestricted] です。

[Manage] をクリックして、[Add Time Range] ダイアログボックスを開きます。このダイアログボックスでアクセス時間の新規セットを指定できます。

ステップ 10　ユーザによる同時ログオン数を指定します。Simultaneous Logons パラメータは、このユーザに指定できる最大同時ログオン数を指定します。デフォルト値は 3 です。最小値は 0 で、この場合ログオンが無効になり、ユーザ アクセスを禁止します。

（注）　最大値を設定で制限しておかないと、同時に多数の接続が許可されるため、セキュリティとパフォーマンスの低下を招くおそれがあります。

ステップ 11　ユーザ接続時間の**最大接続時間**を分で指定します。ここで指定した時間が経過すると、システムは接続を終了します。最短時間は 1 分、最長時間は 2147483647 分（4000 年超）です。接続時間を無制限にするには、**[Unlimited]** チェックボックスをオンにします（デフォルト）。

ステップ 12　ユーザのアイドル タイムアウトを分で指定します。この期間、このユーザの接続に通信アクティビティがなかった場合、システムは接続を終了します。最短時間は 1 分で、最長時間は 10080 分です。この値は、クライアントレス SSL VPN 接続のユーザには適用されません。

ステップ 13　セッション アラート間隔を設定します。[Inherit] チェックボックスをオフにすると、自動的に [Default] チェックボックスがオンになります。これにより、セッション アラート間隔が 30 分に設定されます。新しい値を指定する場合は、[Default] チェックボックスをオフにして、セッション アラート間隔（1 ～ 30 分）を分数ボックスで指定します。

ステップ 14　アイドル アラート間隔を設定します。[Inherit] チェックボックスをオフにすると、自動的に [Default] チェックボックスがオンになります。これにより、アイドル アラート間隔が 30 分に設定されます。新しい値を指定する場合は、[Default] チェックボックスをオフにして、セッション アラート間隔（1 ～ 30 分）を分数ボックスで指定します。

ステップ 15　このユーザに対して専用の IPv4 アドレスを設定する場合は、[Dedicated IPv4 Address] 領域（オプション）で、IPv4 アドレスおよびサブネット マスクを入力します。

ステップ 16　このユーザに対して専用の IPv6 アドレスを設定する場合は、[Dedicated IPv6 Address] フィールド（オプション）で、IPv6 アドレスを IPv6 プレフィックスとともに入力します。IPv6 プレフィックスは、IPv6 アドレスが常駐するサブネットを示します。

ステップ 17　クライアントレス SSL の設定を行う場合は、左側のペインで、**[Clientless SSL VPN]** をクリックします。各設定内容を上書きする場合は、**[Inherit]** チェックボックスをオフにし、新しい値を入力します。

ステップ 18　**[Apply]** をクリックします。

変更内容が実行コンフィギュレーションに保存されます。

リモート アクセス IPSec VPN

この章では、リモート アクセス IPsec VPN の設定方法について説明します。次の項目を取り上げます。

リモート アクセス IPsec VPN に関する情報

リモート アクセス VPN を使用すると、インターネットなどの TCP/IP ネットワーク上のセキュアな接続を介して、ユーザを中央サイトに接続することができます。Internet Security Association and Key Management Protocol は IKE とも呼ばれ、リモート PC の IPsec クライアントと ASA で、IPsec セキュリティ アソシエーションの構築方法を一致させるためのネゴシエーション プロトコルです。各 ISAKMP ネゴシエーションは、フェーズ 1 とフェーズ 2 と呼ばれる 2 つの部分に分かれます。

フェーズ 1 は、以後の ISAKMP ネゴシエーション メッセージを保護する最初のトンネルを作成します。フェーズ 2 は、セキュアな接続を移動するデータを保護するトンネルを作成します。

ISAKMP ネゴシエーションの条件を設定するには、ISAKMP ポリシーを作成します。内容は次のとおりです。

- ピアの ID を確認する認証方式。
- データを保護し、プライバシーを守る暗号化方式。
- 送信者を特定し、搬送中にメッセージが変更されていないことを保証する Hashed Message Authentication Code（HMAC）方式。
- 暗号キーのサイズを設定する Diffie-Hellman グループ。
- ASA が暗号キーを置き換える前に、この暗号キーを使用する最長時間の制限。

トランスフォーム セットは、暗号化方式と認証方式を組み合わせたものです。ピアは、ISAKMP との IPsec セキュリティ アソシエーションのネゴシエート中に、特定のデータ フローを保護する特定のトランスフォーム セットの使用に同意します。トランスフォーム セットは、両方のピアで同じである必要があります。

トランスフォーム セットにより、関連付けられたクリプト マップ エントリで指定された ACL のデータ フローが保護されます。ASA 設定でトランスフォーム セットを作成して、クリプト マップまたはダイナミック クリプト マップ エントリでトランスフォーム セットの最大数 11 を指定できます。有効な暗号化方式と認証方式をリストしたテーブルなど、さらに詳細な情報については、このマニュアルの第 9 章「LAN-to-LAN IPsec VPN」の「IKEv1 トランスフォーム セットの作成」（P.9-6）を参照してください。

AnyConnect クライアントに IPv4 アドレスと IPv6 アドレスの一方または両方を割り当てるように ASA を設定できます。このようにするには、ASA 上で内部的なアドレス プールを作成するか、ASA 上のローカル ユーザに専用アドレスを割り当てます。

エンドポイントに両方のタイプのアドレスを割り当てるには、エンドポイントのオペレーティング システムの中でデュアル スタック プロトコルが実装されている必要があります。どちらのシナリオでも、IPv6 アドレス プールは残っていないが IPv4 アドレスが使用できる場合や、IPv4 アドレス プールは残っていないが IPv6 アドレスが使用できる場合は、接続は行われます。ただし、クライアントには通知されないので、管理者は ASA ログで詳細を確認する必要があります。

クライアントへの IPv6 アドレスの割り当ては、SSL プロトコルに対してサポートされます。この機能は、IKEv2/IPsec プロトコルに対してはサポートされません。

リモート アクセス IPsec VPN のライセンス要件

次の表に、この機能のライセンス要件を示します。

（注）　この機能は、ペイロード暗号化機能のないモデルでは使用できません。

モデル	ライセンス要件[1]
ASA 5505	• IKEv2 を使用した IPsec リモート アクセス VPN（次のいずれかを使用）： – AnyConnect Premium ライセンス： 基本ライセンスと Security Plus ライセンス：2 セッション。 *オプションの永続または時間ベースのライセンス：10 または 25 セッション。* *共有ライセンスはサポートされていません。*[2] – AnyConnect Essentials ライセンス[3]：25 セッション。 • IKEv1 を使用した IPsec リモート アクセス VPN および IKEv1 または IKEv2 を使用した IPsec サイトツーサイト VPN： – 基本ライセンス：10 セッション。 – Security Plus ライセンス：25 セッション。

モデル	ライセンス要件[1]
ASA 5512-X	• IKEv2 を使用した IPsec リモート アクセス VPN（次のいずれかを使用）： – AnyConnect Premium ライセンス： 基本ライセンスと Security Plus ライセンス：2 セッション。 *オプションの永続または時間ベースのライセンス：10、25、50、100、または 250 セッション。* *オプションの共有ライセンス[2]：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。* – AnyConnect Essentials ライセンス[3]：250 セッション。 • IKEv1 を使用した IPsec リモート アクセス VPN および IKEv1 または IKEv2 を使用した IPsec サイトツーサイト VPN： 基本ライセンスと Security Plus ライセンス：250 セッション。
ASA 5515-X	• IKEv2 を使用した IPsec リモート アクセス VPN（次のいずれかを使用）： – AnyConnect Premium ライセンス： 基本ライセンス：2 セッション。 *オプションの永続または時間ベースのライセンス：10、25、50、100、または 250 セッション。* *オプションの共有ライセンス[2]：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。* – AnyConnect Essentials ライセンス[3]：250 セッション。 • IKEv1 を使用した IPsec リモート アクセス VPN および IKEv1 または IKEv2 を使用した IPsec サイトツーサイト VPN： 基本ライセンス：250 セッション。
ASA 5525-X	• IKEv2 を使用した IPsec リモート アクセス VPN（次のいずれかを使用）： – AnyConnect Premium ライセンス： 基本ライセンス：2 セッション。 *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、または 750 セッション。* *オプションの共有ライセンス[2]：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。* – AnyConnect Essentials ライセンス[3]：750 セッション。 • IKEv1 を使用した IPsec リモート アクセス VPN および IKEv1 または IKEv2 を使用した IPsec サイトツーサイト VPN： 基本ライセンス：750 セッション。

モデル	ライセンス要件[1]
ASA 5545-X	• IKEv2 を使用した IPsec リモート アクセス VPN（次のいずれかを使用）： – AnyConnect Premium ライセンス： 基本ライセンス：2 セッション。 *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、750、1000、または 2500 セッション。* *オプションの共有ライセンス[2]：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。* – AnyConnect Essentials ライセンス[3]：2500 セッション。 • IKEv1 を使用した IPsec リモート アクセス VPN および IKEv1 または IKEv2 を使用した IPsec サイトツーサイト VPN： 基本ライセンス：2500 セッション。
ASA 5555-X	• IKEv2 を使用した IPsec リモート アクセス VPN（次のいずれかを使用）： – AnyConnect Premium ライセンス： 基本ライセンス：2 セッション。 *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、750、1000、2500、または 5000 セッション。* *オプションの共有ライセンス[2]：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。* – AnyConnect Essentials ライセンス[3]：5000 セッション。 • IKEv1 を使用した IPsec リモート アクセス VPN および IKEv1 または IKEv2 を使用した IPsec サイトツーサイト VPN： 基本ライセンス：5000 セッション。
ASA 5585-X（SSP-10）	• IKEv2 を使用した IPsec リモート アクセス VPN（次のいずれかを使用）： – AnyConnect Premium ライセンス： 基本ライセンス：2 セッション。 *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、750、1000、2500、または 5000 セッション。* *オプションの共有ライセンス[2]：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。* – AnyConnect Essentials ライセンス[3]：5000 セッション。 • IKEv1 を使用した IPsec リモート アクセス VPN および IKEv1 または IKEv2 を使用した IPsec サイトツーサイト VPN： 基本ライセンス：5000 セッション。

モデル	ライセンス要件[1]
ASA 5585-X（SSP-20、-40、および -60）	• IKEv2 を使用した IPsec リモート アクセス VPN（次のいずれかを使用）： – AnyConnect Premium ライセンス： 基本ライセンス：2 セッション。 *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、750、1000、2500、5000、または 10000 セッション。* *オプションの共有ライセンス[2]：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。* – AnyConnect Essentials ライセンス[3]：10000 セッション。 • IKEv1 を使用した IPsec リモート アクセス VPN および IKEv1 または IKEv2 を使用した IPsec サイトツーサイト VPN： 基本ライセンス：10000 セッション。
ASASM	• IKEv2 を使用した IPsec リモート アクセス VPN（次のいずれかを使用）： – AnyConnect Premium ライセンス： 基本ライセンス：2 セッション。 *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、750、1000、2500、5000、または 10000 セッション。* *オプションの共有ライセンス[2]：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。* – AnyConnect Essentials ライセンス[3]：10000 セッション。 • IKEv1 を使用した IPsec リモート アクセス VPN および IKEv1 または IKEv2 を使用した IPsec サイトツーサイト VPN： 基本ライセンス：10000 セッション。
ASAv（仮想 CPU X 1 を搭載）	• IKEv2 を使用した IPsec リモート アクセス VPN： – 標準ライセンス：2 セッション。 – Premium ライセンス：250 セッション。 • IKEv1 を使用した IPsec リモート アクセス VPN および IKEv1 または IKEv2 を使用した IPsec サイトツーサイト VPN： 標準および Premium ライセンス：250 セッション。
ASAv（仮想 CPU X 4 を搭載）	• IKEv2 を使用した IPsec リモート アクセス VPN： – 標準ライセンス：2 セッション。 – Premium ライセンス：750 セッション。 • IKEv1 を使用した IPsec リモート アクセス VPN および IKEv1 または IKEv2 を使用した IPsec サイトツーサイト VPN： 標準および Premium ライセンス：750 セッション。

1. すべてのタイプの組み合わせ VPN セッションの最大数は、この表に示す最大セッション数を超えることはできません。ASA 5505 では、組み合わせセッションの最大数は 10（基本ライセンスの場合）または 25（Security Plus ライセンスの場合）です。
2. 共有ライセンスによって、ASA は複数のクライアントの ASA の共有ライセンス サーバとして機能します。共有ライセンス プールは大規模ですが、個々の ASA によって使用されるセッションの最大数は、永続的なライセンスで指定される最大数を超えることはできません。

3. AnyConnect Essentials ライセンスにより、AnyConnect VPN クライアントは ASA へのアクセスが可能になります。このライセンスでは、ブラウザベースの SSL VPN アクセスまたは Cisco Secure Desktop はサポートされていません。これらの機能に対しては、AnyConnect Essentials ライセンスの代わりに AnyConnect Premium ライセンスがアクティブ化されます。

   （注）AnyConnect Essentials ライセンスの場合、VPN ユーザは、Web ブラウザを使用してログインし、AnyConnect クライアントのダウンロードと起動（WebLaunch）を実行できます。

   このライセンスと AnyConnect Premium SSL VPN ライセンスのいずれでイネーブル化されたかには関係なく、AnyConnect クライアント ソフトウェアには同じクライアント機能のセットが装備されています。

   特定の ASA では、AnyConnect Premium ライセンス（全タイプ）または Advanced Endpoint Assessment ライセンスを、AnyConnect Essentials ライセンスと同時にアクティブにすることはできません。ただし、同じネットワーク内の異なる ASA で、AnyConnect Essentials ライセンスと AnyConnect Premium ライセンスを実行することは可能です。

   デフォルトでは、ASA は AnyConnect Essentials ライセンスを使用しますが、**webvpn** を使用し、次に **no anyconnect-essentials** コマンド を使用すると、AnyConnect Essentials ライセンスをディセーブルにして他のライセンスを使用できます。

   AnyConnect Essentials ライセンスおよび AnyConnect Premium ライセンスでサポートされている機能の詳細なリストについては、『*AnyConnect Secure Mobility Client Features, Licenses, and OSs*』を参照してください。

   http://www.cisco.com/en/US/products/ps10884/products_feature_guides_list.html

ガイドラインと制限事項

この項では、この機能のガイドラインと制限事項について説明します。

コンテキスト モードのガイドライン

シングル コンテキスト モードだけでサポートされます。マルチ コンテキスト モードをサポートしません。

ファイアウォール モードのガイドライン

ルーテッド ファイアウォール モードでだけサポートされています。トランスペアレント モードはサポートされていません。

フェールオーバーのガイドライン

IPsec VPN セッションは、アクティブ/スタンバイ フェールオーバー コンフィギュレーションでのみ複製されます。アクティブ/アクティブ フェールオーバー コンフィギュレーションはサポートされません。

リモート アクセス IPsec VPN の設定

この項では、リモート アクセス VPN を設定する方法について説明します。次の項目を取り上げます。

- 「ダイナミック クリプト マップの作成」（P.6-12）
- 「ダイナミック クリプト マップを使用するためのクリプト マップ エントリの作成」（P.6-13）
- 「セキュリティ アプライアンスのコンフィギュレーションの保存」（P.6-14）

インターフェイスの設定

ASA には、少なくとも 2 つのインターフェイスがあり、これらをここでは外部と内部と言います。一般に、外部インターフェイスはパブリック インターネットに接続されます。一方、内部インターフェイスは、プライベート ネットワークに接続され、一般のアクセスから保護されます。

最初に、ASA の 2 つのインターフェイスを設定し、イネーブルにします。次に、名前、IP アドレス、およびサブネット マスクを割り当てます。オプションで、セキュリティ レベル、速度、およびセキュリティ アプライアンスでの二重操作を設定します。

インターフェイスを設定するには、例に示すコマンド構文を使用して、次の手順を実行します。

手順の詳細

	コマンド	目的
ステップ 1	**interface** {*interface*} 例： hostname(config)# interface ethernet0 hostname(config-if)#	グローバル コンフィギュレーション モードからインターフェイス コンフィギュレーション モードに入ります。
ステップ 2	**ip address** *ip_address* [*mask*] [**standby** *ip_address*] 例： hostname(config)# interface ethernet0 hostname(config-if)# hostname(config-if)# ip address 10.10.4.200 255.255.0.0	インターフェイスに IP アドレスとサブネット マスクを設定します。
ステップ 3	**nameif** *name* 例： hostname(config-if)# nameif outside hostname(config-if)#	インターフェイスの名前（最大 48 文字）を指定します。この名前は、設定した後での変更はできません。
ステップ 4	shutdown 例： hostname(config-if)# no shutdown hostname(config-if)#	インターフェイスをイネーブルにします。デフォルトでは、インターフェイスはディセーブルです。

ISAKMP ポリシーの設定と外部インターフェイスでの ISAKMP のイネーブル化

この項では、外部インターフェイスに ISAKMP ポリシーを設定する手順と、ポリシーをイネーブルにする方法について説明します。

手順の詳細

次のコマンドを実行します。

	コマンド	目的
ステップ 1	`crypto ikev1 policy priority authentication {crack | pre-share | rsa-sig}` 例： `hostname(config)# crypto ikev1 policy 1 authentication pre-share` `hostname(config)#`	IKEv1 ネゴシエーション中に使用する認証方式とパラメータのセットを指定します。 *Priority* は、インターネット キー交換（IKE）ポリシーを一意に識別し、ポリシーにプライオリティを割り当てます。1 ～ 65,534 の整数を使用します。1 はプライオリティが最も高く、65,534 が最も低くなります。 この例およびその後に続く手順では、プライオリティは 1 に設定されます。
ステップ 2	`crypto ikev1 policy priority encryption {aes | aes-192 | aes-256 | des | 3des}` 例： `hostname(config)# crypto ikev1 policy 1 encryption 3des` `hostname(config)#`	IKE ポリシー内で使用する暗号化方式を指定します。
ステップ 3	`crypto ikev1 policy priority hash {md5 | sha}` 例： `hostname(config)# crypto ikev1 policy 1 hash sha` `hostname(config)#`	IKE ポリシーのハッシュ アルゴリズム（HMAC バリアントとも呼ばれます）を指定します。
ステップ 4	`crypto ikev1 policy priority group {1 | 2 | 5}` 例： `hostname(config)# crypto ikev1 policy 1 group 2` `hostname(config)#`	IKE ポリシーの Diffie-Hellman グループ（IPsec クライアントと ASA が共有秘密キーを確立できる暗号化プロトコル）を指定します。
ステップ 5	`crypto ikev1 policy priority lifetime {seconds}` 例： `hostname(config)# crypto ikev1 policy 1 lifetime 43200` `hostname(config)#`	暗号キーのライフタイム（各セキュリティ アソシエーションが有効期限まで存在する秒数）を指定します。 限定されたライフタイムの範囲は、120 ～ 2147483647 秒です。 無制限のライフタイムの場合は、0 秒を使用します。

	コマンド	目的
ステップ 6	**crypto ikev1** enable *interface-name* 例： hostname(config)# **crypto ikev1** enable outside hostname(config)#	*outside* というインターフェイス上の ISAKMP をイネーブルにします。
ステップ 7	write memory 例： hostname(config-if)# write memory Building configuration... Cryptochecksum: 0f80bf71 1623a231 63f27ccf 8700ca6d 11679 bytes copied in 3.390 secs (3893 bytes/sec) [OK] hostname(config-if)#	変更をコンフィギュレーションに保存します。

アドレス プールの設定

ASA では、ユーザに IP アドレスを割り当てる方式が必要です。この項では、例としてアドレス プールを使用します。ガイドとして次の例で示すコマンド構文を使用します。

コマンド	目的
ip local pool *poolname* *first-address–last-address* [mask *mask*] 例： hostname(config)# **ip local pool testpool 192.168.0.10-192.168.0.15** hostname(config)#	IP アドレスの範囲を使用してアドレス プールを作成します。ASA は、このアドレス プールのアドレスをクライアントに割り当てます。 アドレス マスクはオプションです。ただし、VPN クライアントに割り当てられた IP アドレスが非標準のネットワークに属し、デフォルトのマスクを使用するとデータが誤ってルーティングされる可能性があるときは、マスク値を指定する必要があります。典型的な例が、IP ローカル プールに 10.10.10.0/255.255.255.0 アドレスが含まれている場合で、これはデフォルトではクラス A ネットワークです。これによって、VPN クライアントがさまざまなインターフェイスで 10 のネットワーク内の異なるサブネットにアクセスする必要がある場合、ルーティングの問題が生じる可能性があります。

ユーザの追加

この項では、ユーザ名とパスワードを設定する方法について説明します。ガイドとして次の例で示すコマンド構文を使用します。

コマンド	目的
`username` *name* {`nopassword` | `password` *password* [`mschap` | `encrypted` | `nt-encrypted`]} [`privilege` *priv_level*] 例： `hostname(config)# username testuser password 12345678` `hostname(config)#`	ユーザ、パスワード、および特権レベルを作成します。

IKEv1 トランスフォーム セットまたは IKEv2 プロポーザルの作成

この項では、トランスフォーム セット（IKEv1）およびプロポーザル（IKEv2）を設定する方法について説明します。トランスフォーム セットは、暗号化方式と認証方式を組み合わせたものです。

次の作業を実行します。

コマンド	目的
IKEv1 トランスフォーム セットの設定手順 `crypto ipsec ikev1 transform-set` *transform-set-name encryption-method* [*authentication*] 例： `hostname(config)# crypto ipsec transform set FirstSet esp-3des esp-md5-hmac` `hostname(config)#`	データ整合性を確保するために使用される IPsec IKEv1 暗号化とハッシュ アルゴリズムを指定する IKEv1 トランスフォーム セットを設定します。 *encryption* には、次のいずれかの値を指定します。 • **esp-aes**：128 ビット キーで AES を使用する場合。 • **esp-aes-192**：192 ビット キーで AES を使用する場合。 • **esp-aes-256**：256 ビット キーで AES を使用する場合。 • **esp-des**：56 ビットの DES-CBC を使用する場合。 • **esp-3des**：トリプル DES アルゴリズムを使用する場合。 • **esp-null**：暗号化を使用しない場合。 *authentication* には、次のいずれかの値を指定します。 • **esp-md5-hmac**：ハッシュ アルゴリズムとして MD5/HMAC-128 を使用する場合。 • **esp-sha-hmac**：ハッシュ アルゴリズムとして SHA/HMAC-160 を使用する場合。 • **esp-none**：HMAC 認証を使用しない場合。

コマンド	目的
IKEv2 プロポーザルの設定手順 **crypto ipsec ikev2 ipsec-proposal** *proposal_name* 次に実行するコマンド **protocol {esp} {encryption {des | 3des | aes | aes-192 | aes-256 | null} | integrity {md5 | sha-1}** **例：** hostname(config)# **crypto ipsec ikev2 ipsec-proposal secure_proposal** hostname(config-ipsec-proposal)# **protocol esp encryption des integrity md5**	IKEv2 プロポーザル セットを設定し、使用される IPsec IKEv2 プロトコル、暗号化、および整合性アルゴリズムを指定します。 **esp** は、Encapsulating Security Payload（ESP; カプセル化セキュリティ ペイロード）IPsec プロトコルを指定します（現在、唯一サポートされている IPsec のプロトコルです）。 *encryption* には、次のいずれかの値を指定します。 • **des**：ESP に 56 ビットの DES-CBC 暗号化を使用する場合。 • **3des**：（デフォルト）ESP にトリプル DES 暗号化アルゴリズムを使用する場合。 • **aes**：ESP に 128 ビット キー暗号化で AES を使用する場合。 • **aes-192**：ESP に 192 ビット キー暗号化で AES を使用する場合。 • **aes-256**：ESP に 256 ビット キー暗号化で AES を使用する場合。 • **null**：ESP に暗号化を使用しない場合。 *integrity* には、次のいずれかの値を指定します。 • **md5**：ESP の整合性保護のための md5 アルゴリズムを指定。 • **sha-1**（デフォルト）は、セキュア ハッシュ アルゴリズム（SHA）SHA-1 を指定します。このアルゴリズムは、ESP の整合性保護のための米国連邦情報処理標準（FIPS）で定義されています。

トンネル グループの定義

この項では、トンネル グループを設定する方法について説明します。トンネル グループは、トンネル接続ポリシーを格納したレコードのセットです。AAA サーバを識別するトンネル グループを設定し、接続パラメータを指定し、デフォルトのグループ ポリシーを定義します。ASA は、トンネル グループを内部的に保存します。

ASA システムには、2 つのデフォルト トンネル グループがあります。1 つはデフォルトのリモート アクセス トンネル グループである DefaultRAGroup で、もう 1 つはデフォルトの LAN-to-LAN トンネル グループである DefaultL2Lgroup です。これらは変更可能ですが、削除はできません。トンネル ネゴシエーションで識別された特定のトンネル グループがない場合は、ASA は、これらのグループを使用して、リモート アクセスおよび LAN-to-LAN トンネル グループのデフォルト トンネル パラメータを設定します。

次の作業を実行します。

手順の詳細

	コマンド	目的
ステップ 1	`tunnel-group` *name* `type` *type* 例： `hostname(config)# tunnel-group testgroup type ipsec-ra` `hostname(config)#`	IPsec リモート アクセス トンネル グループ（接続プロファイルとも呼ばれます）を作成します。
ステップ 2	**tunnel-group** *name* **general-attributes** 例： `hostname(config)# tunnel-group testgroup general-attributes` `hostname(config-tunnel-general)#`	トンネル グループ一般属性モードに入ります。このモードでは、認証方式を入力できます。
ステップ 3	**address-pool** [(*interface name*)] **address_pool1** [...address_pool6] 例： `hostname(config-general)# address-pool testpool`	トンネル グループに使用するアドレス プールを指定します。
ステップ 4	**tunnel-group** *name* **ipsec-attributes** 例： `hostname(config)# tunnel-group testgroup ipsec-attributes` `hostname(config-tunnel-ipsec)#`	トンネル グループ ipsec 属性モードに入ります。このモードでは、IKEv1 接続のための IPsec 固有の属性を入力できます。
ステップ 5	**ikev1 pre-shared-key** *key* 例： `hostname(config-tunnel-ipsec)# pre-shared-key 44kkaol59636jnfx`	（オプション）事前共有キー（IKEv1 のみ）を設定します。キーには、1 ～ 128 文字の英数字文字列を指定できます。 適応型セキュリティ アプライアンスとクライアントのキーは同じである必要があります。事前共有キーのサイズが異なる Cisco VPN Client が接続しようとすると、ピアの認証に失敗したことを示すエラー メッセージがクライアントによってログに記録されます。 **（注）** トンネル グループ webvpn 属性の証明書を使用して、IKEv2 の AAA 認証を設定します。

ダイナミック クリプト マップの作成

この項では、ダイナミック クリプト マップを設定する方法について説明します。ダイナミック クリプト マップは、すべてのパラメータを設定する必要のないポリシー テンプレートを定義します。このようなダイナミック クリプト マップにより、ASA は IP アドレスが不明なピアからの接続を受信することができます。リモート アクセス クライアントは、このカテゴリに入ります。

ダイナミック クリプト マップのエントリは、接続のトランスフォーム セットを指定します。また、逆ルーティングもイネーブルにします。これにより、ASA は接続されたクライアントのルーティング情報を取得し、それを RIP または OSPF 経由でアドバタイズします。

次の作業を実行します。

手順の詳細

	コマンド	目的
ステップ 1	IKEv1 の場合は、このコマンドを使用します。 `crypto dynamic-map dynamic-map-name seq-num set ikev1 transform-set transform-set-name` 例： `hostname(config)# crypto dynamic-map dyn1 1 set ikev1 transform-set FirstSet` `hostname(config)#` IKEv2 の場合は、このコマンドを使用します。 `crypto dynamic-map dynamic-map-name seq-num set ikev2 ipsec-proposal proposal-name` 例： `hostname(config)# crypto dynamic-map dyn1 1 set ikev2 ipsec-proposal FirstSet` `hostname(config)#`	ダイナミック クリプト マップを作成し、マップの IKEv1 トランスフォーム セットまたは IKEv2 プロポーザルを指定します。
ステップ 2	**crypto dynamic-map *dynamic-map-name dynamic-seq-num* set reverse-route** 例： `hostname(config)# crypto dynamic-map dyn1 1 set reverse route` `hostname(config)#`	（オプション）このクリプト マップ エントリに基づく接続に対して逆ルート注入をイネーブルにします。

ダイナミック クリプト マップを使用するためのクリプト マップ エントリの作成

この項では、クリプト マップ エントリを作成する方法について説明します。クリプト マップを作成すると、ASA は、ダイナミック クリプト マップを使用して IPsec セキュリティ アソシエーションのパラメータを設定することができます。

このコマンドに関する次の例では、クリプト マップ名は *mymap*、シーケンス番号は 1、ダイナミック クリプト マップ名は *dyn1* です。この名前は、前の項の「ダイナミック クリプト マップの作成」で作成したものです。

次の作業を実行します。

手順の詳細

	コマンド	目的
ステップ 1	crypto map *map-name seq-num* ipsec-isakmp dynamic *dynamic-map-name* 例： hostname(config)# crypto map mymap 1 ipsec-isakmp dynamic dyn1 hostname(config)#	ダイナミック クリプト マップを使用するクリプト マップ エントリを作成します。
ステップ 2	**crypto map** *map-name* **interface** *interface-name* 例： hostname(config)# crypto map mymap interface outside hostname(config)#	クリプト マップを外部インターフェイスに適用します。

セキュリティ アプライアンスのコンフィギュレーションの保存

上記の設定タスクを実行したら、この例に示すようにコンフィギュレーションの変更を必ず保存します。

コマンド	目的
write memory 例： hostname(config-if)# write memory Building configuration... Cryptochecksum: 0f80bf71 1623a231 63f27ccf 8700ca6d 11679 bytes copied in 3.390 secs (3893 bytes/sec) [OK] hostname(config-if)#	変更をコンフィギュレーションに保存します。

リモート アクセス IPsec VPN の設定例

次の例は、リモート アクセス IPsec/IKEv1 VPN を設定する方法を示しています。

```
hostname(config)# interface ethernet0
hostname(config-if)# ip address 10.10.4.200 255.255.0.0
hostname(config-if)# nameif outside
hostname(config-if)# no shutdown
hostname(config)# crypto ikev1 policy 1
hostname(config-ikev1-policy)# authentication pre-share
hostname(config-ikev1-policy)# encryption 3des
hostname(config-ikev1-policy)# hash sha
hostname(config-ikev1-policy)# group 2
hostname(config-ikev1-policy)# lifetime 43200
hostname(config)# crypto ikev1 outside
hostname(config)# ip local pool testpool 192.168.0.10-192.168.0.15
hostname(config)# username testuser password 12345678
```

```
hostname(config)# crypto ipsec ikev1 transform set FirstSet esp-3des esp-md5-hmac
hostname(config)# tunnel-group testgroup type remote-access
hostname(config)# tunnel-group testgroup general-attributes
hostname(config-general)# address-pool testpool
hostname(config)# tunnel-group testgroup ipsec-attributes
hostname(config-ipsec)# ikev1 pre-shared-key 44kkaol59636jnfx
hostname(config)# crypto dynamic-map dyn1 1 set ikev1 transform-set FirstSet
hostname(config)# crypto dynamic-map dyn1 1 set reverse-route
hostname(config)# crypto map mymap 1 ipsec-isakmp dynamic dyn1
hostname(config)# crypto map mymap interface outside
hostname(config)# write memory
```

次の例は、リモート アクセス IPsec/IKEv2 VPN を設定する方法を示しています。

```
hostname(config)# interface ethernet0
hostname(config-if)# ip address 10.10.4.200 255.255.0.0
hostname(config-if)# nameif outside
hostname(config-if)# no shutdown
hostname(config)# crypto ikev2 policy 1
hostname(config-ikev2-policy)# group 2
hostname(config-ikev2-policy)# integrity sha
hostname(config-ikev2-policy)# lifetime 43200
hostname(config-ikev2-policy)# prf sha
hostname(config)# crypto ikev2 outside
hostname(config)# ip local pool testpool 192.168.0.10-192.168.0.15
hostname(config)# username testuser password 12345678
hostname(config)# crypto ipsec ikev2 ipsec-proposal FirstSet
hostname(config-ipsec-proposal)# protocol esp encryption 3des aes
hostname(config)# tunnel-group testgroup type remote-access
hostname(config)# tunnel-group testgroup general-attributes
hostname(config-general)# address-pool testpool
hostname(config)# tunnel-group testgroup webvpn-attributes
hostname(config-webvpn)# authentication aaa certificate
hostname(config)# crypto dynamic-map dyn1 1 set ikev2 ipsec-proposal FirstSet
hostname(config)# crypto dynamic-map dyn1 1 set reverse-route
hostname(config)# crypto map mymap 1 ipsec-isakmp dynamic dyn1
hostname(config)# crypto map mymap interface outside
hostname(config)# write memory
```

リモート アクセス VPN の機能履歴

表 6-1 に、この機能のリリース履歴を示します。

表 6-1　　機能 1 の機能履歴

機能名	リリース	機能情報
IPsec IKEv1 および SSL のリモート アクセス VPN	7.0	リモート アクセス VPN を使用すると、インターネットなどの TCP/IP ネットワーク上のセキュアな接続を介して、ユーザを中央サイトに接続することができます。
IPsec IKEv2 のリモート アクセス VPN	8.4(1)	AnyConnect Secure Mobility Client に対する IPSec IKEv2 サポートが追加されました。

CHAPTER 7

ネットワーク アドミッション コントロール

この章は、次の項で構成されています。

ネットワーク アドミッション コントロールに関する情報

ネットワーク アドミッション コントロールは、実働状態でのネットワーク アクセスの条件として、エンドポイントにおける準拠性チェックと脆弱性チェックを実行することで、ワーム、ウイルス、および危険なアプリケーションの侵入や感染から企業ネットワークを保護します。これらのチェックは、*ポスチャ検証* と呼ばれます。ポスチャ検証を設定して、イントラネット上の脆弱なホストへのアクセスを提供する前に、IPsec セッションまたは WebVPN セッションを行っているホスト上のアンチウイルス ファイル、パーソナル ファイアウォール ルール、または侵入予防ソフトウェアが最新の状態であることを確認できます。ポスチャ検証の一部として、リモート ホストで実行されているアプリケーションが最新のパッチで更新されているか検証することもできます。NAC は、ユーザ認証およびトンネルの設定の完了後に行われます。自動ネットワーク ポリシー実施が適用されないホスト（ホーム PC など）からエンタープライズ ネットワークを保護する場合は、NAC が特に有用です。

エンドポイントと ASA 間でトンネルを確立すると、ポスチャ検証がトリガーされます。

クライアントがポスチャ検証の要求に応答しない場合は、ASA を設定して、そのクライアントの IP アドレスをオプションの監査サーバに渡すことができます。監査サーバ（Trend サーバなど）では、ホスト IP アドレスを使用して、ホストに対して直接チャレンジを行い、ホストのヘルスを評価します。たとえば、ホストに対してチャレンジを行い、そのウイルス チェック ソフトウェアがアクティブで最新の状態かどうかを判断します。監査サーバは、リモート ホストとの対話を完了すると、リモート ホストのヘルスを示すトークンをポスチャ検証サーバに渡します。

ポスチャ検証が成功する、またはリモート ホストが正常であることを示すトークンを受信すると、ポスチャ検証サーバは、トンネル上のトラフィックに対するアプリケーション用のネットワーク アクセス ポリシーを ASA に送信します。

ASA を含む *NAC Framework* のコンフィギュレーションには、クライアントで実行されている Cisco Trust Agent だけがポスチャ エージェントの役割を果たすことができ、Cisco Access Control Server（ACS）だけがポスチャ検証サーバの役割を果たすことができます。ACS はダイナミック ACL を使用して、各クライアントのアクセス ポリシーを決定します。

RADIUS サーバである ACS は、ポスチャ検証サーバとしての役割を果たすことに加え、トンネルの確立に必要なログイン クレデンシャルを認証できます。

（注） ASA に設定されている NAC Framework ポリシーだけが、監査サーバの使用をサポートしています。

ACS はそのポスチャ検証サーバとしての役割において、アクセス コントロール リストを使用します。ポスチャ検証が成功し、ACS によって、ASA に送信するアクセス ポリシーの一部としてリダイレクト URL が指定されると、ASA は、リモート ホストからのすべての HTTP 要求と HTTPS 要求をリダイレクト URL にリダイレクトします。ポスチャ検証サーバによってアクセス ポリシーが ASA にアップロードされると、関連するすべてのトラフィックはその宛先に到達するためにセキュリティ アプライアンスと ACS（またはその逆も同じ）の両方を通過する必要があります。

IPsec または WebVPN クライアントと ASA 間のトンネルが確立されると、NAC Framework ポリシーがグループ ポリシーに割り当てられている場合、ポスチャ検証がトリガーされます。ただし、NAC Framework ポリシーでは、ポスチャ検証を免除されているオペレーティング システムを特定し、そのようなトラフィックをフィルタリングするためにオプションの ACL を指定できます。

ライセンス要件

次の表に、この機能のライセンス要件を示します。

（注） この機能は、ペイロード暗号化機能のないモデルでは使用できません。

モデル	ライセンス要件
ASA 5512-X	AnyConnect Premium ライセンス： • 基本ライセンス：2 セッション。 • *オプションの永続または時間ベースのライセンス：10、25、50、100、または 250 セッション。* • *オプションの共有ライセンス：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。*

モデル	ライセンス要件
ASA 5515-X	AnyConnect Premium ライセンス： • 基本ライセンス：2 セッション。 • *オプションの永続または時間ベースのライセンス：10、25、50、100、または 250 セッション。* • *オプションの共有ライセンス：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。*
ASA 5525-X	AnyConnect Premium ライセンス： • 基本ライセンス：2 セッション。 • *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、または 750 セッション。* • *オプションの共有ライセンス：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。*
ASA 5545-X	AnyConnect Premium ライセンス： • 基本ライセンス：2 セッション。 • *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、750、1000、または 2500 セッション。* • *オプションの共有ライセンス：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。*
ASA 5555-X	AnyConnect Premium ライセンス： • 基本ライセンス：2 セッション。 • *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、750、1000、2500、または 5000 セッション。* • *オプションの共有ライセンス：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。*
ASA 5585-X（SSP-10）	AnyConnect Premium ライセンス： • 基本ライセンス：2 セッション。 • *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、750、1000、2500、または 5000 セッション。* • *オプションの共有ライセンス：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。*
ASA 5585-X（SSP-20、-40、および -60）	AnyConnect Premium ライセンス： • 基本ライセンス：2 セッション。 • *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、750、1000、2500、5000、または 10000 セッション。* • *オプションの共有ライセンス：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。*

モデル	ライセンス要件
ASASM	AnyConnect Premium ライセンス： • 基本ライセンス：2 セッション。 • *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、750、1000、2500、5000、または 10000 セッション。* • *オプションの共有ライセンス：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。*
ASAv（仮想 CPU X 1 を搭載）	• 標準ライセンス：2 セッション。 • Premium ライセンス：250 セッション。
ASAv（仮想 CPU X 4 を搭載）	• 標準ライセンス：2 セッション。 • Premium ライセンス：750 セッション。

（注）　クライアントレス SSL VPN セッションを開始した後、ポータルから AnyConnect クライアント セッションを開始した場合は、合計 1 つのセッションが使用されています。これに対して、最初に AnyConnect クライアントを（スタンドアロン クライアントなどから）開始した後、クライアントレス SSL VPN ポータルにログインした場合は、2 つのセッションが使用されています。

すべてのタイプの組み合わせ VPN セッションの最大数は、この表に示す最大セッション数を超えることはできません。

共有ライセンスによって、ASA は複数のクライアントの ASA の共有ライセンス サーバとして機能します。共有ライセンス プールは大規模ですが、個々の ASA によって使用されるセッションの最大数は、永続的なライセンスで指定される最大数を超えることはできません。

NAC の前提条件

NAC をサポートするように設定すると、ASA は、Cisco Secure Access Control Server のクライアントとして機能します。そのため、NAC 認証サービスを提供するために、ネットワーク上に少なくとも 1 台の Access Control Server をインストールする必要があります。

ガイドラインと制限事項

ネットワークに 1 つまたは複数の Access Control Server を設定した後で、**aaa-server** コマンドを使用して Access Control Server グループに名前を付ける必要があります。次に、「NAC ポリシーの設定」（P.7-8）の手順の説明に従ってください。

NAC Framework に対する ASA サポートは、リモート アクセス IPsec セッションおよび WebVPN クライアント セッションに限定されます。NAC Framework コンフィギュレーションは、シングル モードだけをサポートしています。

ASA 上の NAC は、レイヤ 3（非 VPN）トラフィックと IPv6 トラフィックはサポートしていません。

セキュリティ アプライアンスの NAC ポリシーの表示

グループ ポリシーに割り当てる NAC ポリシーを設定する前に、ASA にすでに設定されている可能性があるポリシーを確認することをお勧めします。デフォルト コンフィギュレーションには NAC ポリシーは含まれていませんが、このコマンドを入力すると、他のユーザによってすでにポリシーが追加されているかどうかを手軽に判断できます。設定済みのポリシーがある場合に、そのポリシーが適切であると判断できる場合は、NAC ポリシーの設定に関する項を無視してもかまいません。

手順の詳細

	コマンド	目的
ステップ 1	**show running-config nac-policy** **例：** `hostname# show running-config nac-policy` `nac-policy nacframework1 nac-framework` `default-acl acl-1` `reval-period 36000` `sq-period 300` `exempt-list os "Windows XP" filter acl-2` `hostname#`	ASA 上ですでに設定されている NAC ポリシーを表示します。 nac-framework1 という名前の NAC ポリシーのコンフィギュレーションを表示します。
ステップ 2	• default-acl：NAC デフォルト ACL がポスチャ検証の前に適用されます。セキュリティ アプライアンスは、ポスチャ検証の後、リモート ホストの Access Control Server から取得した ACL でデフォルト ACL を置き換えます。ポスチャ検証が失敗した場合、ASA にはデフォルト ACL が残ります。 • reval-period：NAC Framework セッション内でのポスチャ検証が正常に完了してから次回の検証までの間隔（秒）。 • sq-period：NAC Framework セッション内でのポスチャ検証が正常に完了してから、ホスト ポスチャの変化を調べる次回のクエリーまでの間隔（秒）。 • exempt-list：ポスチャ検証を免除されるオペレーティング システム名。リモート コンピュータのオペレーティング システムがこの名前に一致する場合は、トラフィックをフィルタリングするオプションの ACL も表示されます。 • authentication-server-group：NAC ポスチャ検証に使用される認証サーバ グループの名前。	nac-framework の属性を表示します。

	コマンド	目的
ステップ 3	`show nac-policy` **例：** `asa2(config)# show nac-policy` `nac-policy framework1 nac-framework` `  applied session count = 0` `  applied group-policy count = 2` `  group-policy list:  GroupPolicy2  GroupPolicy1` `nac-policy framework2 nac-framework is not in use.` `asa2(config)#`	グループ ポリシーへの NAC ポリシーの割り当てを表示します。 どの NAC ポリシーが未割り当てであるかと、各 NAC ポリシーの使用回数を表示します。
ステップ 4	• applied session count：この ASA が NAC ポリシーを適用した VPN セッションの累積数。 • applied group-policy count：この ASA が NAC ポリシーを適用したグループ ポリシーの累積数。 • group-policy list：この NAC ポリシーが割り当てられているグループ ポリシーのリスト。この場合、グループ ポリシーの使用状況によってこのリストに表示されるかどうかは決まりません。NAC ポリシーが実行コンフィギュレーションのグループ ポリシーに割り当てられている場合は、このリストにグループ ポリシーが表示されます。	show nac-policy コマンドのフィールドの説明です。 **（注）** どのグループ ポリシーにも割り当てられていないポリシーについては、「is not in use」がポリシー タイプの隣に表示されます。

NAC ポリシーを作成する、またはすでに存在するポリシーを変更するには、次の項を参照してください。

NAC ポリシーの追加、アクセス、または削除

NAC ポリシーを追加または変更するには、次のコマンドを入力します。

手順の詳細

	コマンド	目的
ステップ 1	**global**	グローバル コンフィギュレーション モードに切り替えます。
ステップ 2	**nac-policy** *nac-policy-name* **nac-framework** **例：** hostname(config)# **nac-policy nac-framework1 nac-framework** hostname(config-nac-policy-nac-framework)	NAC ポリシーを追加または変更します。 *nac-policy-name* は、新しい NAC ポリシーまたはすでに存在するポリシーの名前です。名前は最大 64 文字の文字列です。 **nac-framework** は、NAC Framework コンフィギュレーションで、リモート ホスト用のネットワーク アクセス ポリシーを提供することを指定します。ASA の NAC Framework サービスを提供するには、Cisco Access Control Server がネットワークに存在している必要があります。このタイプを指定すると、プロンプトは nac-policy-nac-framework コンフィギュレーション モードにいることを示します。このモードでは、NAC Framework ポリシーを設定できます。 **（注）** NAC Framework ポリシーは複数作成できますが、1 つのグループ ポリシーに 1 つしか割り当てることはできません。 NAC Framework ポリシーを nac-framework1 という名前で作成し、アクセスします。
ステップ 3	（オプション） [**no**] **nac-policy** *nac-policy-name* **nac-framework**	NAC ポリシーをコンフィギュレーションから削除します。ポリシーの名前とタイプの両方を指定する必要があります。
ステップ 4	（オプション） **clear configure nac-policy**	グループ ポリシーに割り当てられているものを除き、すべての NAC ポリシーをコンフィギュレーションから削除します。
ステップ 5	**show running-config nac-policy**	セキュリティ アプライアンスにすでに存在する各 NAC ポリシーの名前およびコンフィギュレーションを表示します。

NAC ポリシーの設定

nac-policy コマンドを使用して NAC Framework ポリシーに名前を付けたら、そのポリシーをグループ ポリシーに割り当てる前に、次の項の手順に従ってポリシーの属性に値を割り当てます。

Access Control Server グループの指定

NAC をサポートするためには、少なくとも 1 つの Cisco Access Control Server を設定する必要があります。

手順の詳細

	コマンド	目的
ステップ 1	**aaa-server host**	Access Control Server グループに名前を付けます（グループに含まれているサーバが 1 つだけであっても）。
ステップ 2	（オプション） **show running-config aaa-server** **例：** hostname(config)# **show running-config aaa-server** aaa-server acs-group1 protocol radius aaa-server acs-group1 (outside) host 192.168.22.44 key secret radius-common-pw secret hostname(config)#	AAA サーバの設定を表示します。
ステップ 3	**nac-policy-nac-framework**	nac-policy-nac-framework コンフィギュレーション モードに切り替えます。
ステップ 4	**authentication-server-group** *server-group* **例：** hostname(config-nac-policy-nac-framework)# **authentication-server-group acs-group1** hostname(config-nac-policy-nac-framework)	NAC ポスチャ検証に使用されるグループを指定します。 *server-group* は、**aaa-server host** コマンドで指定した server-tag 変数と一致する必要があります。このコマンドの **no** バージョンを使用している場合は、一致していなくてもかまいません。 NAC ポスチャ検証に使用される認証サーバ グループとして acs-group1 を指定します。
ステップ 5	（オプション） [**no**] **authentication-server-group** *server-group*	コマンドを NAC ポリシーから削除します。

ポスチャ変更確認のクエリーのタイマーの設定

ポスチャ検証が成功するたびに、ASA はステータス クエリー タイマーを起動します。このタイマーの期限が切れると、直前のポスチャ検証以降のポスチャ変更を確認するクエリーがリモート ホストにトリガーされます。変更がないことを応答が示している場合、ステータス クエリー タイマーがリセットされます。ポスチャに変更があったことを応答が示している場合、無条件のポスチャ再検証がトリガーされます。ASA は、再検証中、現在のアクセス ポリシーを保持します。

デフォルトでは、成功した各ポスチャ検証、ステータス クエリー、および以降の各ステータス クエリーの間隔は 300 秒（5 分）です。ステータス クエリーの間隔を変更するには、次の手順を実行します。

手順の詳細

	コマンド	目的
ステップ 1	**nac-policy-nac-framework**	nac-policy-nac-framework コンフィギュレーション モードに切り替えます。
ステップ 2	**sq-period seconds** **例：** `hostname(config-group-policy)# sq-period 1800` `hostname(config-group-policy)`	ステータス クエリーの間隔を変更します。 *seconds* は、30 ～ 1800 秒（5 ～ 30 分）の範囲で指定する必要があります。 クエリー タイマーを 1800 秒に変更します。
ステップ 3	（オプション） **[no] sq-period** *seconds*	ステータス クエリー タイマーをオフにします。
ステップ 4	**show running-config nac-policy**	sq-period 属性の隣に 0 が表示されます。これは、タイマーがオフであることを意味します。

再検証タイマーの設定

ポスチャ検証が成功するたびに、ASA は再検証タイマーを起動します。このタイマーが期限切れになると、次の無条件のポスチャ検証がトリガーされます。ASA は、再検証中、現在のアクセス ポリシーを保持します。

デフォルトでは、成功した各ポスチャ検証間の間隔は 36000 秒（10 時間）です。この間隔を変更するには、nac-policy-nac-framework コンフィギュレーション モードで次のコマンドを入力します。

手順の詳細

	コマンド	目的
ステップ 1	**nac-policy-nac-framework**	nac-policy-nac-framework に切り替えます。
ステップ 2	**reval-period** ***seconds*** **例：** `hostname(config-nac-policy-nac-framework)#` `reval-period 86400` `hostname(config-nac-policy-nac-framework)`	ポスチャ検証が正常に完了してから次回の検証までの間隔を変更します。 *seconds* は、300 ～ 86400 秒（5 分～ 24 時間）の範囲で指定する必要があります。

	コマンド	目的
ステップ 3	（オプション） **[no] reval-period** *seconds*	ステータス クエリー タイマーをオフにします。
ステップ 4	**show running-config nac-policy**	sq-period 属性の隣に 0 が表示されます。これは、タイマーがオフであることを意味します。

NAC 用デフォルト ACL の設定

各グループ ポリシーは、ポリシーに一致し、NAC に対して適格なホストに適用されるデフォルト ACL を指しています。ASA は、ポスチャ検証の前に NAC のデフォルト ACL を適用します。ポスチャ検証の後、ASA はデフォルト ACL をリモート ホストの Access Control Server から取得した ACL に置き換えます。ポスチャ検証が失敗した場合、ASA にはデフォルト ACL が残ります。

また、ASA は、クライアントレス認証がイネーブルになっている（デフォルト設定）場合にも、NAC のデフォルト ACL を適用します。

手順の詳細

	コマンド	目的
ステップ 1	**nac-policy-nac-framework**	nac-policy-nac-framework コンフィギュレーション モードに切り替えます。
ステップ 2	**default-acl** *acl-name* **例：** hostname(config-nac-policy-nac-framework)# **default-acl acl-2** hostname(config-nac-policy-nac-framework)	NAC セッションのデフォルト ACL として使用される ACL を指定します。 *acl-name* は、セッションに適用されるアクセス コントロール リストの名前です。 ポスチャ検証成功の前に適用される ACL として ac1-2 を指定します。
ステップ 3	（オプション） **[no] default-acl** *acl-name*	コマンドを NAC Framework ポリシーから削除します。*acl-name* の指定は任意です。

NAC 免除の設定

ASA のコンフィギュレーションには、NAC ポスチャ検証免除のリストが保存されます。免除されるオペレーティング システムを指定できます。ACL を指定すると、指定したオペレーティング システムを実行しているクライアントは、ポスチャ検証が免除され、クライアントのトラフィックは ACL の対象になります。

NAC ポスチャ検証を免除されるリモート コンピュータ タイプのリストにエントリを追加するには、nac-policy-nac-framework コンフィギュレーション モードで次のコマンドを入力します。

手順の詳細

	コマンド	目的
ステップ 1	nac-policy-nac-framework	nac-policy-nac-framework コンフィギュレーション モードに切り替えます。

	コマンド	目的
ステップ 2	**exempt-list os** "*os-name*" [**disable** | **filter** *acl-name* [**disable**]	NAC ポスチャ検証を免除されるリモート コンピュータ タイプのリストにエントリを追加します。 • *os-name* は、オペレーティング システムの名前です。引用符は、名前にスペースが含まれている場合に使用します（たとえば "Windows XP"）。 • **filter** を指定すると、コンピュータのオペレーティング システムが *os name* と一致する場合、トラフィックをフィルタリングするために ACL が適用されます。**filter**/*acl-name* のペアはオプションです。 • **disable** を指定すると、次の 2 つの機能のいずれかが実行されます。 – "os-name" の後に入力した場合、ASA は、指定したオペレーティング システムを実行するリモート ホストで免除を行わず、NAC ポスチャ検証を適用します。 – このキーワードを *acl-name* の後に入力すると、ASA はそのオペレーティング システムを免除しますが、関連のトラフィックには ACL を適用しません。 • *acl-name* は、ASA コンフィギュレーションにある ACL の名前です。指定する場合は、**filter** キーワードの後に指定する必要があります。
	例： hostname(config-group-policy)# **exempt-list os "Windows XP"** hostname(config-group-policy)	ポスチャ検証を免除するコンピュータのリストに、Windows XP を実行するすべてのホストを追加します。
	hostname(config-nac-policy-nac-framework)# **exempt-list os "Windows XP" filter acl-2** hostname(config-nac-policy-nac-framework)	Windows XP を実行するすべてのホストを免除し、そのホストからのトラフィックに ACL acl-2 を適用します。
	hostname(config-nac-policy-nac-framework)# **no exempt-list os "Windows XP" filter acl-2** hostname(config-nac-policy-nac-framework)	同じエントリを免除リストから削除します。
ステップ 3	（オプション） [**no**] **exempt-list os** "*os-name*" [**disable** | **filter** *acl-name* [**disable**]]	NAC Framework ポリシーからすべての免除を削除します。エントリを指定してこのコマンドの no 形式を発行すると、そのエントリが免除リストから削除されます。
	例： hostname(config-nac-policy-nac-framework)# **no exempt-list** hostname(config-nac-policy-nac-framework)	免除リストからすべてのエントリを削除します。

（注）　コマンドでオペレーティング システムを指定しても、例外リストに追加済みのエントリは上書きされません。免除する各オペレーティング システムおよび ACL に対して 1 つずつコマンドを入力します。

グループ ポリシーへの NAC ポリシーの割り当て

各トンネルのセットアップを完了すると、グループ ポリシーに割り当てられている場合、ASA は NAC ポリシーをセッションに適用します。デフォルトでは、**nac-settings** コマンドは、各グループ ポリシーのコンフィギュレーションには存在しません。ASA は、NAC ポリシーが割り当てられると、グループ ポリシーの NAC を自動的にイネーブルにします。

手順の詳細

	コマンド	目的
ステップ 1	**group-policy**	グループ ポリシー コンフィギュレーション モードに切り替えます。
ステップ 2	**nac-settings** { **value** *nac-policy-name* | **none** } **例：** hostname(config-group-policy)# **nac-settings value framework1** hostname(config-group-policy)	NAC ポリシーをグループ ポリシーに割り当てます。 • **nac-settings none** は、グループ ポリシーから *nac-policy-name* を削除し、このグループ ポリシーに対する NAC ポリシーの使用をディセーブルにします。グループ ポリシーは、デフォルト グループ ポリシーから nac-settings 値を継承しません。 • **nac-settings value** は、指定した NAC ポリシーをグループ ポリシーに割り当てます。 framework1 という名前の NAC ポリシーをグループ ポリシーに割り当てます。
ステップ 3	（オプション） [**no**] **nac-settings** { **value** *nac-policy-name* | **none** }	nac-policy-name をグループ ポリシーから削除します。グループ ポリシーは、デフォルト グループ ポリシーから nac-settings 値を継承します。
ステップ 4	（オプション） **show running-config nac-policy**	各 NAC ポリシーの名前およびコンフィギュレーションを表示します。

グローバルな NAC Framework 設定の変更

ASA では、NAC Framework コンフィギュレーションがデフォルトで設定されています。この項の手順に従って、ネットワークの強制ポリシーを順守するようにこれらの設定を調整します。

クライアントレス認証設定の変更

クライアントレス認証に対する NAC Framework のサポートは設定可能です。これは、ポスチャ エージェントの役割を果たす Cisco Trust Agent を持たないホストに適用されます。ASA は、デフォルト アクセス ポリシーを適用し、ポスチャ検証用に Extensible Authentication Protocol（EAP）over User Datagram Protocol（UDP）要求を送信して、その要求がタイムアウトします。ASA が、Access Control Server からのクライアントレス ホストに対するポリシーを要求するように設定されていない場合、クライアントレス ホストにすでに使用されているデフォルト アクセス ポリシーを保持します。ASA が、Access Control Server からのクライアントレス ホストに対するポリシーを要求するように設定されている場合、そのように要求して、Access Control Server は ASA が実施するアクセス ポリシーをダウンロードします。

クライアントレス認証のイネーブル化とディセーブル化

クライアントレス認証は、デフォルトでイネーブルになっています。デフォルトのコンフィギュレーションには、**eou allow clientless** コンフィギュレーションが含まれています。

制限

eou コマンドは、NAC Framework セッションに*だけ*適用されます。

手順の詳細

NAC Framework コンフィギュレーションに対してクライアントレス認証をイネーブルにするには、次の手順を実行します。

	コマンド	目的
ステップ 1	**global**	グローバル コンフィギュレーション モードに切り替えます。
ステップ 2	**eou allow {audit | clientless | none}** **例：** hostname(config)# **eou allow audit** hostname(config)#	NAC Framework コンフィギュレーションに対してクライアントレス認証をイネーブルにします。 • **audit** を指定すると、クライアントレス認証の実行に監査サーバを使用します。 • **clientless** を指定すると、クライアントレス認証の実行に Cisco Access Control Server を使用します。 • **none** は、クライアントレス認証をディセーブルにします。 監査サーバを使用してクライアントレス認証を実行するように ASA を設定する方法を示します。

	コマンド	目的
ステップ 3	[no] eou allow {audit | clientless | none} 例： hostname(config)# no eou allow audit hostname(config)#	コマンドをコンフィギュレーションから削除します。 監査サーバの使用をディセーブルにします。

クライアントレス認証に使用するログイン クレデンシャルの変更

クライアントレス認証がイネーブルで、ASA がリモート ホストからの検証要求に対する応答を受信できなかった場合、リモート ホストの代わりに、セキュリティ アプライアンスはクライアントレス認証要求を Access Control Server に送信します。この要求には、Access Control Server でのクライアントレス認証用に設定されたクレデンシャルに一致するログイン クレデンシャルが含まれます。ASA のクライアントレス認証用のデフォルト ユーザ名とパスワードは、Access Control Server のデフォルト ユーザ名とパスワードと一致します。デフォルト ユーザ名とパスワードはいずれも「clientless」です。

前提条件

Access Control Server でこれらの値を変更する場合は、ASA でも変更する必要があります。

手順の詳細

クライアントレス認証に使用するユーザ名を変更するには、次のとおりに入力します。

	コマンド	目的
ステップ 1	global	グローバル コンフィギュレーション モードに切り替えます。
ステップ 2	eou clientless username *username* 例： hostname(config)# eou clientless username sherlock hostname(config)# eou clientless password 221B-baker hostname(config)#	クライアントレス認証に使用するユーザ名を変更します。 *username* は、クライアントレス ホストをサポートする Access Control Server に設定されているユーザ名に一致する必要があります。先頭および末尾のスペース、シャープ記号（#）、疑問符（?）、引用符（"）、アスタリスク（*）、山カッコ（< および >）を除く、1 ～ 64 文字の ASCII 文字を入力します。 クライアントレス認証のユーザ名を sherlock に、パスワードを 221B-baker に変更します。ユーザ名だけ、パスワードだけ、または両方を指定できます。

	コマンド	目的
ステップ 3	**eou clientless password** *password*	クライアントレス認証に使用するパスワードを変更します。 *password* は、クライアントレス ホストをサポートする Access Control Server に設定されているパスワードに一致する必要があります。4 ～ 32 文字の ASCII 文字を入力します。
ステップ 4	（オプション） **no eou clientless username** **例：** hostname(config)# **no eou clientless username** hostname(config)#	ユーザ名をデフォルト値に変更します。
ステップ 5	（オプション） **no eou clientless password** **例：** hostname(config)# **no eou clientless password** hostname(config)#	パスワードをデフォルト値に変更します。

NAC Framework セッション属性の変更

ASA には、ASA とリモート ホスト間の通信を指定する属性のデフォルト設定があります。これらの属性で、リモート ホストのポスチャ エージェントと通信するポート番号、およびポスチャ エージェントとの通信を制限する有効制限カウンタを指定します。これらの属性、デフォルト設定、およびそれらを変更するために入力できるコマンドは次のとおりです。

手順の詳細

	コマンド	目的
ステップ 1	global	グローバル コンフィギュレーション モードに切り替えます。
ステップ 2	**eou port** *port_number* **例：** hostname(config)# **eou port 62445** hostname(config)#	デフォルトのポート番号は 21862 です。このコマンドは、ポスチャ エージェントとの EAP over UDP 通信に使用されるポート番号（クライアント エンドポイントの）を変更します。 *port_number* は、CTA で設定されているポート番号に一致する必要があります。値は 1024 ～ 65535 の範囲で入力します。 EAP over UDP 通信用のポート番号を 62445 に変更します。

	コマンド	目的
ステップ 3	（オプション） **no** eou port **例：** hostname(config)# **no eou port** hostname(config)#	ポート番号をデフォルト値に変更します。
ステップ 4	**eou timeout retransmit** *seconds* **例：** hostname(config)# **eou timeout retransmit 6** hostname(config)#	再送信リトライ タイマーを変更します。ASA は EAP over UDP メッセージをリモート ホストに送信する場合、応答を待ちます。*n* 秒以内に応答を受信できない場合、EAP over UDP メッセージを再送信します。デフォルトでは、再送信タイマーは 3 秒です。 *seconds* は、1 ～ 60 の範囲の値です。 再送信タイマーを 6 秒に変更します。
ステップ 5	（オプション） no eou timeout **retransmit** **例：** hostname(config)# **no eou timeout retransmit** hostname(config)#	再送信リトライ タイマーをデフォルト値に変更します。
ステップ 6	**eou max-retry** *retries* **例：** hostname(config)# **eou max-retry 1** hostname(config)#	再送信リトライ回数を変更します。ASA は EAP over UDP メッセージをリモート ホストに送信する場合、応答を待ちます。応答を受信できない場合、EAP over UDP メッセージを再送信します。デフォルトでは、3 回まで再送信されます。 *retries* は、1 ～ 3 の範囲の値です。 EAP over UDP 再送回数の上限を 1 に設定します。
ステップ 7	（オプション） **no eou max-retry** **例：** hostname(config)# **no eou max-retry** hostname(config)#	再送信リトライの最大回数をデフォルト値に変更します。

	コマンド	目的
ステップ 8	**eou timeout hold-period** *seconds* **例：** hostname(config)# **eou timeout hold-period 120** hostname(config)#	セッション再初期化タイマーを変更します。再送信リトライ カウンタと max-retry 値が一致すると、ASA はリモート ホストとの EAP over UDP セッションを終了し、保持タイマーを起動します。保持タイマーが *n* 秒になると、ASA は、リモート ホストとの新しい EAP over UDP セッションを確立します。デフォルトでは、新規セッションを確立するまでの最大待機秒数は 180 秒です。 *seconds* は、60 ～ 86400 の範囲の値です。 新しい EAP over UDP アソシエーションを開始する前の待機期間を 120 秒に変更します
ステップ 9	(オプション) **no** eou timeout hold-period **例：** hostname(config)# **no eou timeout hold-period** hostname(config)#	セッション再初期化をデフォルト値に変更します。

PPPoE クライアント

この項では、ASA が提供する PPPoE クライアントの設定方法について説明します。説明する項目は次のとおりです。

PPPoE クライアントの概要

PPPoE は、イーサネットと PPP という広く受け入れられている 2 つの標準を結合して、IP アドレスをクライアント システムに割り当てる認証方式を提供します。一般的な PPPoE クライアントは、DSL やケーブル サービスなどのリモート ブロードバンド接続によって ISP に接続されているパーソナル コンピュータです。ISP は、既存のリモート アクセス インフラストラクチャを使用して高速ブロードバンド アクセスをサポートするためと、顧客の使い勝手向上のために、PPPoE を配置します。

PPPoE は、イーサネット ネットワーク上でポイントツーポイント プロトコル PPP による認証方式を使用するための標準方式です。ISP が使用する場合は、PPPoE で IP アドレスを割り当ててから認証できます。このタイプの実装では、PPPoE クライアントとサーバが、DSL または他のブロードバンド接続上で実行されているレイヤ 2 ブリッジング プロトコルによって相互に接続されます。

PPPoE は、次の 2 つの主要フェーズで構成されています。

- アクティブ ディスカバリ フェーズ：このフェーズでは、PPPoE クライアントが、アクセス コンセントレータと呼ばれる PPPoE サーバの場所を探索します。このフェーズの期間にセッション ID が割り当てられ、PPPoE レイヤが確立されます。
- PPP セッション フェーズ：このフェーズでは、PPP オプションがネゴシエートされ、認証処理が実行されます。リンクのセットアップが完了すると、PPPoE がレイヤ 2 カプセル化方式としての機能を開始し、PPPoE ヘッダーにデータを入れて PPP リンク経由で転送できるようになります。

PPPoE クライアントは、システムの初期化時に一連のパケットを交換して、アクセス コンセントレータとのセッションを確立します。セッションが確立されると PPP リンクがセットアップされます。これにはパスワード認証プロトコル（PAP）による認証が含まれます。PPP セッションが確立されると、各パケットは PPPoE ヘッダーと PPP ヘッダーでカプセル化されます。

（注） PPPoE は、ASA でフェールオーバーを設定している場合、またはマルチ コンテキスト モードやトランスペアレント モードではサポートされません。PPPoE がサポートされるのは、フェールオーバーを設定していない、シングル モード、ルーテッド モードの場合だけです。

PPPoE クライアントのユーザ名とパスワードの設定

ASA がアクセス コンセントレータにアクセスするときの認証で使用されるユーザ名とパスワードを設定するには、**vpdn** コマンドを使用します。**vpdn** コマンドを使用するには、まず VPDN グループを定義し、次にグループ内で個々のユーザを作成します。

PPPoE ユーザ名とパスワードを設定するには、次の手順を実行します。

ステップ 1　次のコマンドを使用して、PPPoE で使用される VPDN グループを定義します。

```
hostname(config)# vpdn group group_name request dialout pppoe
```

このコマンド例では、*group_name* の部分を、「pppoe-sbc」などのわかりやすいグループ名で置き換えます。

ステップ 2　利用する ISP が認証を要求する場合は、次のコマンドを入力して認証プロトコルを選択します。

```
hostname(config)# vpdn group group_name ppp authentication {chap | mschap | pap}
```

group_name の部分を、前のステップで定義したグループ名と同じ名前で置き換えます。ISP で使用する認証方式に応じた適切なキーワードを入力します。

- CHAP：Challenge Handshake Authentication Protocol（チャレンジ ハンドシェイク認証プロトコル）
- MS-CHAP：Microsoft Challenge Handshake Authentication Protocol Version 1（Microsoft チャレンジ ハンドシェイク認証プロトコル バージョン 1）
- PAP：Password Authentication Protocol（パスワード認証プロトコル）

（注） CHAP または MS-CHAP を使用する場合は、ユーザ名がリモート システム名として参照され、パスワードが CHAP シークレットとして参照されます。

ステップ 3　次のコマンドを入力して、ISP で割り当てられたユーザ名を VPDN グループに関連付けます。

```
hostname(config)# vpdn group group_name localname username
```

group_name の部分を VPDN グループ名で置き換え、*username* の部分を ISP によって割り当てられたユーザ名で置き換えます。

ステップ 4　次のコマンドを入力して、PPPoE 接続用のユーザ名とパスワードのペアを 1 組作成します。

```
hostname(config)# vpdn username username password password [store-local]
```

username の部分をユーザ名で置き換え、*password* の部分を ISP によって割り当てられたパスワードで置き換えます。

（注）　**store-local** オプションを指定すると、ユーザ名とパスワードが ASA の NVRAM の特別な場所に保存されます。Auto Update Server が **clear config** コマンドを ASA に送信し、その後に接続が中断された場合、ASA は、ユーザ名とパスワードを NVRAM から読み取り、アクセス コンセントレータに対して再認証できます。

PPPoE のイネーブル化

（注）　「PPPoE クライアントのユーザ名とパスワードの設定」の説明に従い、PPPoE をイネーブルにする前に、**vpdn** コマンドを使用してコンフィギュレーションを完了する必要があります。

PPPoE クライアント機能は、デフォルトでオフになっています。PPPoE をイネーブルにするには、次の手順を実行します。

ステップ 1　インターフェイス コンフィギュレーション モードで次のコマンドを入力して、PPPoE クライアントをイネーブルにします。

```
hostname(config-if)# ip address pppoe [setroute]
```

setroute オプションを指定すると、PPPoE クライアントが接続をまだ確立していない場合に、デフォルト ルートが設定されます。**setroute** オプションを使用する場合は、スタティックに定義されたルートをコンフィギュレーションに含めることはできません。

PPPoE では IP アドレスが PPP によって割り当てられるため、PPPoE は DHCP と併用できません。**setroute** オプションを指定すると、デフォルト ルートが存在しない場合にデフォルト ルートが作成されます。デフォルト ルータは、アクセス コンセントレータのアドレスです。最大伝送単位（MTU）サイズは、自動的に 1492 バイトに設定されます。これは、イーサネット フレーム内で PPPoE 伝送を許可する正しい値です。

DHCP リースをリセットし、新規リースを要求するには、このコマンドを再入力します。

（注）　2 つのインターフェイス（プライマリ インターフェイスとバックアップ インターフェイスなど）で PPPoE がイネーブルになっているときに、デュアル ISP サポートを設定しない場合（一般的な操作のコンフィギュレーション ガイドの「Monitoring a Static or Default Route」）を参照）、ASA では、最初のインターフェイスに限り、IP アドレスを取得するためにトラフィックを送信できます。

次に例を示します。

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# ip address pppoe
```

ステップ 2　インターフェイス コンフィギュレーション モードで次のコマンドを入力して、使用する PPPoE クライアントの VPDN グループを指定します（オプション）。

```
hostname(config-if)# pppoe client vpdn group grpname
```

grpname は、VPDN *グループ*の名前です。

（注）　複数の VPDN グループが設定されているときに、**pppoe client vpdn group** コマンドでグループを指定しないと、ASA は VPDN グループをランダムに選択します。これを避けるには、VPDN グループを指定してください。

固定 IP アドレスによる PPPoE の使用

インターフェイス コンフィギュレーション モードで次の形式の ip address コマンドを使用し、IP アドレスを手動で入力することで、PPPoE をイネーブルにすることもできます。

```
hostname(config-if)# ip address ipaddress mask pppoe
```

このコマンドを入力すると、ASA は、PPPoE サーバとネゴシエートしてアドレスをダイナミックに割り当てる代わりに、指定されたアドレスを使用します。*ipaddress* と *mask* の部分を、ASA に割り当てられた IP アドレスとサブネット マスクで置き換えます。

次に例を示します。

```
hostname(config-if)# ip address outside 201.n.n.n 255.255.255.0 pppoe
```

（注）　**setroute** オプションは **ip address** コマンドのオプションで、PPPoE クライアントがまだ接続を確立していない場合に、アクセス コンセントレータでデフォルト ルートを設定できるようにするために使用できます。**setroute** オプションを使用する場合は、スタティックに定義されたルートをコンフィギュレーションに含めることはできません。

PPPoE クライアントのモニタリングとデバッグ

次のコマンドを使用して、現在の PPPoE クライアント コンフィギュレーション情報を表示します。

```
hostname# show ip address outside pppoe
```

次のコマンドを使用して、PPPoE クライアントでのデバッグをイネーブルまたはディセーブルにします。

```
hostname# [no] debug pppoe {event | error | packet}
```

次に、各キーワードの機能をまとめます。

- **event**：プロトコル イベント情報を表示します。
- **error**：エラー メッセージを表示します。
- **packet**：パケット情報を表示します。

次のコマンドを使用して、PPPoE セッションのステータスを表示します。

```
hostname# show vpdn session [l2tp | pppoe] [id sess_id | packets | state | window]
```

次の例は、このコマンドで提供される情報のサンプルです。

```
hostname# show vpdn

Tunnel id 0, 1 active sessions
     time since change 65862 secs
     Remote Internet Address 10.0.0.1
    Local Internet Address 199.99.99.3
     6 packets sent, 6 received, 84 bytes sent, 0 received
Remote Internet Address is 10.0.0.1
     Session state is SESSION_UP
       Time since event change 65865 secs, interface outside
       PPP interface id is 1
       6 packets sent, 6 received, 84 bytes sent, 0 received
hostname#
hostname# show vpdn session
PPPoE Session Information (Total tunnels=1 sessions=1)
Remote Internet Address is 10.0.0.1
  Session state is SESSION_UP
    Time since event change 65887 secs, interface outside
    PPP interface id is 1
    6 packets sent, 6 received, 84 bytes sent, 0 received
hostname#
hostname# show vpdn tunnel
PPPoE Tunnel Information (Total tunnels=1 sessions=1)
Tunnel id 0, 1 active sessions
   time since change 65901 secs
   Remote Internet Address 10.0.0.1
   Local Internet Address 199.99.99.3
   6 packets sent, 6 received, 84 bytes sent, 0 received
hostname#
```

設定の消去

コンフィギュレーションからすべての **vpdn group** コマンドを削除するには、グローバル コンフィギュレーション モードで **clear configure vpdn group** コマンドを使用します。

```
hostname(config)# clear configure vpdn group
```

すべての **vpdn username** コマンドを削除するには、**clear configure vpdn username** コマンドを使用します。

```
hostname(config)# clear configure vpdn username
```

これらのコマンドのいずれを入力しても、アクティブな PPPoE 接続には影響しません。

関連するコマンドの使用

次のコマンドを使用して、PPP/IPCP ネゴシエーションの一環としてアクセス コンセントレータが提供した WINS アドレスと DNS アドレスが DHCP サーバで使用されるようにします。

```
hostname(config)# dhcpd auto_config [client_ifx_name]
```

このコマンドは、サービス プロバイダーが RFC 1877 の規定に従ってこの情報を提供する場合に限り必要になります。*client_ifx_name* パラメータを使用して、DHCP **auto_config** オプションによってサポートされるインターフェイスを指定します。PPPoE クライアントは 1 つの外部インターフェイスだけでサポートされるため、このキーワードはこの時点では不要です。

CHAPTER 9

LAN-to-LAN IPsec VPN

LAN-to-LAN VPN は、地理的に異なる場所にあるネットワークを接続します。

2 つのピアの内部および外部ネットワークが IPv4 の場合（内部および外部インターフェイス上のアドレスが IPv4 の場合）、ASA で、シスコまたはサードパーティのピアとの LAN-to-LAN VPN 接続がサポートされます。

IPv4 アドレッシングと IPv6 アドレッシングが混在した、またはすべて IPv6 アドレッシングを使用する LAN-to-LAN 接続については、両方のピアが ASA の場合、および両方の内部ネットワークのアドレッシング方式が一致している場合（両方が IPv4 または両方が IPv6 の場合）は、セキュリティ アプライアンスで VPN トンネルがサポートされます。

具体的には、両方のピアが ASA の場合、次のトポロジがサポートされます。

- ASA の内部ネットワークが IPv4 で、外部ネットワークが IPv6（内部インターフェイス上のアドレスが IPv4 で、外部インターフェイス上のアドレスが IPv6）
- ASA の内部ネットワークが IPv6 で、外部ネットワークが IPv4（内部インターフェイス上のアドレスが IPv6 で、外部インターフェイス上のアドレスが IPv4）
- ASA の内部ネットワークが IPv6 で、外部ネットワークが IPv6（内部および外部インターフェイス上のアドレスが IPv6）

（注） ASA は、シスコのピアや、関連するすべての標準に準拠したサードパーティのピアとの LAN-to-LAN IPsec 接続をサポートしています。

この章では、LAN-to-LAN VPN 接続の構築方法について説明します。内容は次のとおりです。

コンフィギュレーションのまとめ

ここでは、この章で説明するサンプルの LAN-to-LAN コンフィギュレーションの概要を説明します。後の項で、手順の詳細を説明します。

```
hostname(config)# interface ethernet0/0
hostname(config-if)# ip address 10.10.4.100 255.255.0.0
hostname(config-if)# nameif outside
hostname(config-if)# no shutdown
hostname(config)# crypto ikev1 policy 1
hostname(config-ikev1-policy)# authentication pre-share
hostname(config-ikev1-policy)# encryption 3des
hostname(config-ikev1-policy)# hash sha
hostname(config-ikev1-policy)# group 2
hostname(config-ikev1-policy)# lifetime 43200
hostname(config)# crypto ikev1 enable outside
hostname(config)# crypto ikev2 policy 1
hostname(config-ikev2-policy)# encryption 3des
hostname(config-ikev2-policy)# group 2
hostname(config-ikev12-policy)# prf sha
hostname(config-ikev2-policy)# lifetime 43200
hostname(config)# crypto ikev2 enable outside
hostname(config)# crypto ipsec ikev1 transform-set FirstSet esp-3des esp-md5-hmac
hostname(config)# crypto ipsec ikev2 ipsec-proposal secure
hostname(config-ipsec-proposal)# protocol esp encryption 3des aes des
hostname(config-ipsec-proposal)# protocol esp integrity sha-1
hostname(config)# access-list l2l_list extended permit ip 192.168.0.0 255.255.0.0
150.150.0.0 255.255.0.0
hostname(config)# tunnel-group 10.10.4.108 type ipsec-l2l
hostname(config)# tunnel-group 10.10.4.108 ipsec-attributes
hostname(config-tunnel-ipsec)# ikev1 pre-shared-key 44kkaol59636jnfx
hostname(config)# crypto map abcmap 1 match address l2l_list
hostname(config)# crypto map abcmap 1 set peer 10.10.4.108
hostname(config)# crypto map abcmap 1 set ikev1 transform-set FirstSet
hostname(config)# crypto map abcmap 1 set ikev2 ipsec-proposal secure
hostname(config)# crypto map abcmap interface outside
hostname(config)# write memory
```

マルチコンテキスト モードでのサイトツーサイト VPN の設定

マルチモードでサイトツーサイト VPN をサポートするには、次の手順を実行します。これらの手順を実行して、リソース割り当てがどのように分解されるのかを確認できます。

ステップ 1　マルチモードの VPN を設定し、リソース クラスを設定し、許可されたリソースの一部として VPN ライセンスを選択します。「Configuring a Class for Resource Management」で、これらの設定手順を説明します。次に設定例を示します。

```
class ctx1
    limit-resource VPN Burst Other 100
    limit-resource VPN Other 1000
```

ステップ 2　コンテキストを設定し、VPN ライセンスを許可する設定したクラスのメンバーにします。「Configuring a Security Context」でこれらの手順を説明します。次に設定例を示します。

```
context context1
    member ctx1
    allocate-interface GigabitEthernet3/0.2
    allocate-interface GigabitEthernet3/1.2
    allocate-interface Management0/0
    config-url disk0:/sm_s2s_ik1_ip4_no_webvpn.txt
    join-failover-group 1
```

ステップ 3　接続プロファイル、ポリシー、クリプト マップなどを、サイトツーサイト VPN のシングル コンテキストの VPN 設定と同様に設定します。

インターフェイスの設定

ASA には、少なくとも 2 つのインターフェイスがあり、これらをここでは外部と内部と言います。一般に、外部インターフェイスはパブリック インターネットに接続されます。一方、内部インターフェイスは、プライベート ネットワークに接続され、一般のアクセスから保護されます。

最初に、ASA の 2 つのインターフェイスを設定し、イネーブルにします。次に、名前、IP アドレス、およびサブネット マスクを割り当てます。オプションで、セキュリティ レベル、速度、およびセキュリティ アプライアンスでの二重操作を設定します。

（注）　ASA の外部インターフェイス アドレス（IPv4 と IPv6 の両方）は、プライベート側のアドレス空間と重複していてはなりません。

インターフェイスを設定するには、例に示すコマンド構文を使用して、次の手順を実行します。

ステップ 1　インターフェイス コンフィギュレーション モードに入るには、グローバル コンフィギュレーション モードで、設定するインターフェイスのデフォルト名を指定して **interface** コマンドを入力します。次の例で、インターフェイスは ethernet0 です。

```
hostname(config)# interface ethernet0/0
hostname(config-if)#
```

ステップ 2　インターフェイスの IP アドレスとサブネット マスクを設定するには、**ip address** コマンドを入力します。次の例で、IP アドレスは 10.10.4.100、サブネット マスクは 255.255.0.0 です。

```
hostname(config-if)# ip address 10.10.4.100 255.255.0.0
hostname(config-if)#
```

ステップ 3　インターフェイスに名前を付けるには、**nameif** コマンドを入力します。最大 48 文字です。この名前は、設定した後での変更はできません。次の例で、ethernet0 インターフェイスの名前は outside です。

```
hostname(config-if)# nameif outside
hostname(config-if)##
```

ステップ 4　インターフェイスをイネーブルにするには、**shutdown** コマンドの **no** バージョンを入力します。デフォルトでは、インターフェイスはディセーブルです。

```
hostname(config-if)# no shutdown
hostname(config-if)#
```

ステップ 5　変更を保存するには、**write memory** コマンドを入力します。

```
hostname(config-if)# write memory
hostname(config-if)#
```

ステップ 6　同じ手順で、2 番目のインターフェイスを設定します。

ISAKMP ポリシーの設定と外部インターフェイスでの ISAKMP のイネーブル化

ISAKMP は、2 台のホストで IPsec Security Association（SA; セキュリティ アソシエーション）の構築方法を一致させるためのネゴシエーション プロトコルです。これは、SA 属性のフォーマットに合意するための共通のフレームワークを提供します。これには、SA に関するピアとのネゴシエーション、および SA の変更または削除が含まれます。ISAKMP のネゴシエーションは 2 つのフェーズ（フェーズ 1 とフェーズ 2）に分かれています。フェーズ 1 は、以後の ISAKMP ネゴシエーション メッセージを保護する最初のトンネルを作成します。フェーズ 2 では、データを保護するトンネルが作成されます。

IKE は、IPsec を使用するための SA の設定に ISAKMP を使用します。IKE は、ピアの認証に使用される暗号キーを作成します。

ASA は、レガシー Cisco VPN Client から接続するための IKEv1、および AnyConnect VPN クライアントの IKEv2 をサポートしています。

ISAKMP ネゴシエーションの条件を設定するには、IKE ポリシーを作成します。このポリシーには、次のものが含まれます。

- IKEv1 ピアに要求する認証タイプ。証明書を使用する RSA 署名または事前共有キー（PSK）です。
- データを保護し、プライバシーを守る暗号化方式。
- 送信者を特定し、搬送中にメッセージが変更されていないことを保証する Hashed Message Authentication Code（HMAC）方式。
- 暗号キー決定アルゴリズムの強度を決定する Diffie-Hellman グループ。このアルゴリズムを使用して、ASA は暗号キーとハッシュ キーを導出します。
- IKEv2 では、別個の Pseudo-Random Function（PRF; 疑似乱数関数）をアルゴリズムとして使用して、IKEv2 トンネルの暗号化に必要なキー関連情報とハッシュ操作を取得していました。
- この暗号キーを使用する時間の上限。この時間が経過すると ASA は暗号キーを置き換えます。

IKEv1 ポリシーを使用して、パラメータごとに 1 つの値を設定します。IKEv2 では、単一のポリシーに対して、複数の暗号化タイプと認証タイプ、および複数の整合性アルゴリズムを設定できます。ASA は、設定をセキュア度が最も高いものから最も低いものに並べ替え、その順序を使用してピアとのネゴシエーションを行います。これによって、IKEv1 と同様に、許可される各組み合わせを送信することなく、許可されるすべてのトランスフォームを伝送するために単一のプロポーザルを送信できます。

ここでは、IKEv1 および IKEv2 ポリシーを作成して、インターフェイスでイネーブルにする手順について説明します。

- 「IKEv1 接続の ISAKMP ポリシーの設定」（P.9-5）
- 「IKEv2 接続の ISAKMP ポリシーの設定」（P.9-6）

IKEv1 接続の ISAKMP ポリシーの設定

IKEv1 接続の ISAKMP ポリシーを設定するには、**crypto ikev1 policy** *priority* コマンドを使用して IKEv1 ポリシー コンフィギュレーション モードを開始します。ここでは IKEv1 のパラメータを設定できます。

次の手順を実行し、ガイドとして次の例で示すコマンド構文を使用します。

ステップ 1　IPSec IKEv1 ポリシー コンフィギュレーション モードを開始します。次に例を示します。

```
hostname(config)# crypto ikev1 policy 1
hostname(config-ikev1-policy)#
```

ステップ 2　認証方式を設定します。次の例では、事前共有キーを設定します。

```
hostname(config-ikev1-policy)# authentication pre-share
hostname(config-ikev1-policy)#
```

ステップ 3　暗号方式を設定します。次の例では、3DES に設定します。

```
hostname(config-ikev1-policy)# encryption 3des
hostname(config-ikev1-policy)#
```

ステップ 4　HMAC 方式を設定します。次の例では、SHA-1 に設定します。

```
hostname(config-ikev1-policy)# hash sha
hostname(config-ikev1-policy)#
```

ステップ 5　Diffie-Hellman グループを設定します。次の例では、グループ 2 に設定します。

```
hostname(config-ikev1-policy)# group 2
hostname(config-ikev1-policy)#
```

ステップ 6　暗号キーのライフタイムを設定します。次の例では、43,200 秒（12 時間）に設定します。

```
hostname(config-ikev1-policy)# lifetime 43200
hostname(config-ikev1-policy)#
```

ステップ 7　シングル コンテキスト モードまたはマルチ コンテキスト モードで、outside というインターフェイス上の IKEv1 をイネーブルにします。

```
hostname(config)# crypto ikev1 enable outside
hostname(config)#
```

ステップ 8　変更を保存するには、**write memory** コマンドを入力します。

```
hostname(config)# write memory
hostname(config)#
```

IKEv2 接続の ISAKMP ポリシーの設定

IKEv2 接続の ISAKMP ポリシーを設定するには、**crypto ikev2 policy** *priority* コマンドを使用して IKEv2 ポリシー コンフィギュレーション モードを開始します。ここでは IKEv2 のパラメータを設定できます。

次の操作を行ってください。

ステップ 1　IPsec IKEv2 ポリシー コンフィギュレーション モードを開始します。次に例を示します。

```
hostname(config)# crypto ikev2 policy 1
hostname(config-ikev2-policy)#
```

ステップ 2　暗号方式を設定します。次の例では、3DES に設定します。

```
hostname(config-ikev2-policy)# encryption 3des
hostname(config-ikev2-policy)#
```

ステップ 3　Diffie-Hellman グループを設定します。次の例では、グループ 2 に設定します。

```
hostname(config-ikev2-policy)# group 2
hostname(config-ikev2-policy)#
```

ステップ 4　アルゴリズムとして使用する疑似乱数関数（PRF）を設定し、IKEv2 トンネルの暗号化に必要なキー関連情報とハッシュ操作を取得します。次の例では、SHA-1（HMAC バリアント）を設定します。

```
hostname(config-ikev12-policy)# prf sha
hostname(config-ikev2-policy)#
```

ステップ 5　暗号キーのライフタイムを設定します。次の例では、43,200 秒（12 時間）に設定します。

```
hostname(config-ikev2-policy)# lifetime seconds 43200
hostname(config-ikev2-policy)#
```

ステップ 6　outside というインターフェイス上の IKEv2 をイネーブルにします。

```
hostname(config)# crypto ikev2 enable outside
hostname(config)#
```

ステップ 7　変更を保存するには、**write memory** コマンドを入力します。

```
hostname(config)# write memory
hostname(config)#
```

IKEv1 トランスフォーム セットの作成

IKEv1 トランスフォーム セットは、暗号化方式と認証方式を組み合わせたものです。ピアは、ISAKMP との IPsec セキュリティ アソシエーションのネゴシエート中に、特定のデータ フローを保護する特定のトランスフォーム セットの使用に同意します。トランスフォーム セットは、両方のピアで同じである必要があります。

トランスフォーム セットにより、関連付けられたクリプト マップ エントリで指定された ACL のデータ フローが保護されます。ASA 設定でトランスフォーム セットを作成して、クリプト マップまたはダイナミック クリプト マップ エントリでトランスフォーム セットの最大数 11 を指定できます。

表 9-1 に、有効な暗号化方式と認証方式を示します。

表 9-1　有効な暗号化方式と認証方式

有効な暗号化方式	有効な認証方式
esp-des	esp-md5-hmac
esp-3des（デフォルト）	esp-sha-hmac（デフォルト）
esp-aes（128 ビット暗号化）	
esp-aes-192	
esp-aes-256	
esp-null	

パブリック インターネットなどの非信頼ネットワークを介して接続された 2 つの ASA 間で IPsec を実装する通常の方法は、トンネル モードです。トンネル モードはデフォルトであり、設定は必要ありません。

トランスフォーム セットを設定するには、シングル コンテキスト モードまたはマルチ コンテキスト モードで次のサイト間タスクを実行します。

ステップ 1　グローバル コンフィギュレーション モードで、**crypto ipsec ikev1 transform-set** コマンドを入力します。次の例では、名前が FirstSet で、暗号化と認証にそれぞれ esp-3des と esp-md5-hmac を使用するトランスフォーム セットを設定しています。構文は次のようになります。

crypto ipsec ikev1 transform-set *transform-set-name* ***encryption-method authentication-method***

```
hostname(config)# crypto ipsec transform-set FirstSet esp-3des esp-md5-hmac
hostname(config)#
```

ステップ 2　変更を保存します。

```
hostname(config)# write memory
hostname(config)#
```

IKEv2 プロポーザルの作成

IKEv2 では、単一のポリシーに対して、複数の暗号化タイプと認証タイプ、および複数の整合性アルゴリズムを設定できます。ASA は、設定をセキュア度が最も高いものから最も低いものに並べ替え、その順序を使用してピアとのネゴシエーションを行います。これによって、IKEv1 と同様に、許可される各組み合わせを送信することなく、許可されるすべてのトランスフォームを伝送するために単一のプロポーザルを送信できます。

表 9-2 に、有効な IKEv2 暗号化方式と認証方式を示します。

表 9-2　有効な IKEv2 暗号化方式と整合性方式

有効な暗号化方式	有効な整合性方式
des	sha（デフォルト）
3des（デフォルト）	md5
aes	

表 9-2　有効な IKEv2 暗号化方式と整合性方式（続き）

有効な暗号化方式	有効な整合性方式
aes-192	
aes-256	

IKEv2 プロポーザルを設定するには、シングル コンテキスト モードまたはマルチ コンテキスト モードで次のタスクを実行します。

ステップ 1　グローバル コンフィギュレーション モードで **crypto ipsec ikev2 ipsec-proposal** コマンドを使用して、プロポーザルの複数の暗号化および整合性タイプを指定できる IPSec プロポーザル コンフィギュレーション モードを開始します。この例では、プロポーザルの名前は *secure* です。

```
hostname(config)# crypto ipsec ikev2 ipsec-proposal secure
hostname(config-ipsec-proposal)#
```

ステップ 2　次に、プロトコルおよび暗号化タイプを入力します。サポートされている唯一のプロトコルは ESP です。次に例を示します。

```
hostname(config-ipsec-proposal)# protocol esp encryption 3des aes des
hostname(config-ipsec-proposal)#
```

ステップ 3　整合性タイプを入力します。次に例を示します。

```
hostname(config-ipsec-proposal)# protocol esp integrity sha-1
hostname(config-ipsec-proposal)#
```

ステップ 4　変更を保存します。

ACL の設定

ASA は、アクセス コントロール リストを使用してネットワーク アクセスをコントロールします。デフォルトでは、適応型セキュリティ アプライアンスはすべてのトラフィックを拒否します。トラフィックを許可する ACL を設定する必要があります。詳細については、一般的な操作のコンフィギュレーション ガイドの「Information About Access Control Lists」を参照してください。

この LAN-to-LAN VPN 制御接続で設定する ACL は、送信元 IP アドレスと変換された宛先 IP アドレスに基づいています。接続の両側に、互いにミラーリングする ACL を設定します。

VPN トラフィック用の ACL は、変換アドレスを使用します。

ACL を設定するには、次の手順を実行します。

ステップ 1　**access-list extended** コマンドを入力します。次の例では、192.168.0.0 のネットワーク内にある IP アドレスから 150.150.0.0 のネットワークにトラフィックを送信する、l2l_list という名前の ACL を設定します。構文は、**access-list** *listname* **extended permit ip** *source-ipaddress source-netmask destination-ipaddress destination-netmask* です。

```
hostname(config)# access-list l2l_list extended permit ip 192.168.0.0 255.255.0.0
150.150.0.0 255.255.0.0
hostname(config)#
```

ステップ 2　接続のもう一方の側の ASA に、ACL をミラーリングする ACL を設定します。次の例では、該当ピアのプロンプトは hostname2 です。

```
hostname2(config)# access-list l2l_list extended permit ip 150.150.0.0 255.255.0.0
192.168.0.0 255.255.0.0
hostname(config)#
```

（注）　VPN フィルタを使用した ACL の設定方法の詳細については、「リモート アクセスの VLAN の指定またはグループ ポリシーへの統合アクセス コントロール ルール」（P.4-47）を参照してください。

トンネル グループの定義

トンネル グループは、トンネル接続ポリシーを格納したレコードのセットです。AAA サーバを識別するトンネル グループを設定し、接続パラメータを指定し、デフォルトのグループ ポリシーを定義します。ASA は、トンネル グループを内部的に保存します。

ASA には、2 つのデフォルト トンネル グループがあります。1 つはデフォルトの IPsec リモート アクセス トンネル グループである DefaultRAGroup で、もう 1 つはデフォルトの IPsec LAN-to-LAN トンネル グループである DefaultL2Lgroup です。これらは変更可能ですが、削除はできません。

IKE バージョン 1 および 2 の主な相違点は、使用できる認証方式にあります。IKEv1 では、両方の VPN エンドで 1 つのタイプの認証のみが許可されます（つまり、事前共有キーまたは証明書）。しかし、IKEv2 では、別のローカルおよびリモート認証 CLI を使用して非対称認証方式を設定できます（つまり、送信元に対しては事前共有キー認証を設定し、応答側に対しては証明書認証を設定できます）。したがって、IKEv2 を使用すると、両方の側がそれぞれ異なるクレデンシャルで認証する非対称認証を使用できます（事前共有キー、証明書、）。

また、環境に合った新しいトンネル グループを 1 つ以上作成することもできます。トンネル ネゴシエーションで識別された特定のトンネル グループがない場合は、ASA は、これらのグループを使用して、リモート アクセスおよび LAN-to-LAN トンネル グループのデフォルト トンネル パラメータを設定します。

基本的な LAN-to-LAN 接続を確立するには、次のように 2 つの属性をトンネル グループに設定する必要があります。

- 接続タイプを IPsec LAN-to-LAN に設定します。
- IP アドレスの認証方式を設定します。次の例では、IKEv1 および IKEv2 に事前共有キーを設定します。

（注）　トンネル グループなどの VPN を使用するには、ASA はシングル ルーテッド モードでなければなりません。トンネルグループ パラメータを設定するためのコマンドは、他のどのモードにも表示されません。

ステップ 1　接続タイプを IPsec LAN-to-LAN に設定するには、**tunnel-group** コマンドを入力します。構文は、**tunnel-group** *name* **type** *type* です。ここで、*name* はトンネル グループに割り当てる名前であり、*type* はトンネルのタイプです。CLI で入力するトンネル タイプは次のとおりです。

- **remote-access**（IPsec、SSL、およびクライアントレス SSL リモート アクセス）
- **ipsec-l2l**（IPsec LAN-to-LAN）

次の例では、トンネル グループの名前は、LAN-to-LAN ピアの IP アドレスである 10.10.4.108 です。

```
hostname(config)# tunnel-group 10.10.4.108 type ipsec-l2l
hostname(config)#
```

（注）　IP アドレス以外の名前が付いている LAN-to-LAN トンネル グループは、トンネル認証方式がデジタル証明書である、またはピアが Aggressive モードを使用するように設定されている（あるいはその両方）の場合に限り使用できます。

ステップ 2　事前共有キーを使用するように認証方式を設定するには、ipsec 属性モードに入り、**ikev1 pre-shared-key** コマンドを入力して事前共有キーを作成します。この LAN-to-LAN 接続の両方の ASA で、同じ事前共有キーを使用する必要があります。

キーは、1 ～ 128 文字の英数字文字列です。

次の例で、IKEv1 事前共有キーは 44kkaol59636jnfx です。

```
hostname(config)# tunnel-group 10.10.4.108 ipsec-attributes
hostname(config-tunnel-ipsec)# pre-shared-key 44kkaol59636jnfx
```

次の例で、IKEv2 事前共有キーも 44kkaol59636jnfx に設定されています。

```
hostname(config-tunnel-ipsec)# ikev2 local-authentication pre-shared-key 44kkaol59636jnfx
```

（注）　認証を完了するには、**ikev2 remote-authentication pre-shared-key** コマンドまたは **ikev2 remote-authentication certificate** コマンドを設定する必要があります。

ステップ 3　変更を保存します。

```
hostname(config)# write memory
hostname(config)#
```

トンネルが稼働中であることを確認するには、**show vpn-sessiondb summary**、**show vpn-sessiondb detail l2l**、または **show cry ipsec sa** コマンドを使用します。

クリプト マップの作成とインターフェイスへの適用

クリプト マップ エントリは、IPsec セキュリティ アソシエーションの次のような各種要素をまとめたものです。

- IPsec で保護する必要のあるトラフィック（ACL で定義）
- IPsec で保護されたトラフィックの送信先（ピアで指定）
- トラフィックに適用される IPsec セキュリティ（トランスフォーム セットで指定）
- IPsec トラフィックのローカル アドレス（インターフェイスにクリプト マップを適用して指定）

IPsec が成功するためには、両方のピアに互換性のあるコンフィギュレーションを持つクリプト マップ エントリが存在する必要があります。2 つのクリプト マップ エントリが互換性を持つためには、両者が少なくとも次の基準を満たす必要があります。

- クリプト マップ エントリに、互換性を持つ暗号 ACL（たとえば、ミラー イメージ ACL）が含まれている。応答するピアがダイナミック クリプト マップを使用している場合は、ASA の暗号 ACL のエントリがピアの暗号 ACL によって「許可」されている必要があります。

- 各クリプト マップ エントリが他のピアを識別する（応答するピアがダイナミック クリプト マップを使用していない場合）。
- クリプト マップ エントリに、共通のトランスフォーム セットが少なくとも 1 つ存在する。

所定のインターフェイスに対して複数のクリプト マップ エントリを作成する場合は、各エントリのシーケンス番号（seq-num）を使用して、エントリにランクを付けます。seq-num が小さいほど、プライオリティが高くなります。クリプト マップ セットを持つインターフェイスでは、ASA はまずトラフィックをプライオリティの高いマップ エントリと照合して評価します。

次の条件のいずれかに当てはまる場合は、所定のインターフェイスに対して複数のクリプト マップ エントリを作成します。

- 複数のピアで異なるデータ フローを処理する場合。
- 異なるタイプのトラフィック（同一または個別のピアへの）に異なる IPsec セキュリティを適用する場合。たとえば、あるサブネット セット間のトラフィックは認証し、別のサブネット セット間のトラフィックは認証および暗号化するような場合です。この場合は、異なるタイプのトラフィックを 2 つの個別の ACL で定義し、各 暗号 ACL に対して個別にクリプト マップ エントリを作成します。

クリプト マップを作成してグローバル コンフィギュレーション モードで外部インターフェイスに適用するには、シングル コンテキスト モードまたはマルチ コンテキスト モードで次の手順を実行します。

ステップ 1　ACL をクリプト マップ エントリに割り当てるには、**crypto map match address** コマンドを入力します。

構文は、**crypto map** *map-name seq-num* **match address** *aclname* です。次の例では、マップ名は abcmap、シーケンス番号は 1、ACL 名は **l2l_list** です。

```
hostname(config)# crypto map abcmap 1 match address l2l_list
hostname(config)#
```

ステップ 2　IPsec 接続用のピアを指定するには、**crypto map set peer** コマンドを入力します。

構文は、**crypto map** *map-name seq-num* **set peer** {*ip_address1* | hostname*1*}[*... ip_address10* | hostname*10*] です。次の例では、ピア名は 10.10.4.108 です。

```
hostname(config)# crypto map abcmap 1 set peer 10.10.4.108
hostname(config)#
```

ステップ 3　クリプト マップ エントリに IKEv1 トランスフォーム セットを指定するには、**crypto map ikev1 set transform-set** コマンドを入力します。

構文は、**crypto map** *map-name seq-num* **ikev1 set transform-set** *transform-set-name* です。次の例では、トランスフォーム セット名は *FirstSet* です。

```
hostname(config)# crypto map abcmap 1 set transform-set FirstSet
hostname(config)#
```

ステップ 4　クリプト マップ エントリに IKEv2 プロポーザルを指定するには、**crypto map ikev2 set ipsec-proposal** コマンドを入力します。

構文は、**crypto map** *map-name seq-num set* **ikev2 ipsec-proposal** ***proposal-name*** です。次の例では、プロポーザル名は *secure* です。

crypto map コマンドでは、1 つのマップ インデックスに複数の IPsec プロポーザルを指定できます。この場合、複数のプロポーザルがネゴシエーションの一部として IKEv2 ピアに送信され、プロポーザルの順序はクリプト マップ エントリの順序付け時に管理者が決定します。

（注）　連結モード（AES-GCM/GMAC）および通常モード（その他すべて）のアルゴリズムが IPsec プロポーザルにある場合、ピアに単一のプロポーザルを送信できません。この場合、2 つのプロポーザルが必要となります（連結モードのアルゴリズムに 1 つ、通常モードのアルゴリズムに 1 つ）。

```
hostname(config)# crypto map abcmap 1 set ikev2 ipsec-proposal secure
hostname(config)#
```

クリプト マップのインターフェイスへの適用

クリプト マップ セットは、IPsec トラフィックが通過する各インターフェイスに適用する必要があります。ASA は、すべてのインターフェイスで IPsec をサポートします。クリプト マップ セットをインターフェイスに適用すると、ASA はすべてのインターフェイス トラフィックをクリプト マップ セットと照合して評価し、接続時やセキュリティ アソシエーションのネゴシエート時に、指定されたポリシーを使用します。

また、クリプト マップをインターフェイスにバインドすると、セキュリティ アソシエーション データベースやセキュリティ ポリシー データベースなどのランタイム データ構造も初期化されます。クリプト マップを後から変更すると、ASA は自動的にその変更を実行コンフィギュレーションに適用します。既存の接続はすべてドロップされ、新しいクリプト マップの適用後に再確立されます。

設定済みのクリプト マップを外部インターフェイスに適用するには、次の手順を実行します。

ステップ 1　**crypto map interface** コマンドを入力します。構文は、**crypto map** *map-name* **interface** *interface-name* です。

```
hostname(config)# crypto map abcmap interface outside
hostname(config)#
```

ステップ 2　変更を保存します。

```
hostname(config)# write memory
hostname(config)#
```

CHAPTER 10

AnyConnect VPN Client 接続

この章では、AnyConnect VPN Client 接続を設定する方法について説明します。次の項目を取り上げます。

AnyConnect VPN Client 接続に関する情報

Cisco AnyConnect Secure Mobility Client によりリモート ユーザは、ASA へのセキュアな SSL 接続または IPsec/IKEv2 接続を確立できます。事前にクライアントがインストールされていない場合、リモート ユーザは、SSL または IPsec/IKEv2 VPN 接続を受け入れるように設定されているインターフェイスの IP アドレスをブラウザに入力します。ASA が、http:// 要求を https:// にリダイレクトするように設定されていない限り、ユーザは URL を https://*<address>* の形式で入力する必要があります。

URL が入力されると、ブラウザはそのインターフェイスに接続し、ログイン画面を表示します。ユーザがログインと認証に成功し、そのユーザがクライアントを要求していると ASA で識別されると、セキュリティ アプライアンスは、リモート コンピュータのオペレーティング システムに合うクライアントをダウンロードします。ダウンロード後、クライアントは自分自身でインストールと設定を行い、セキュアな SSL または IPsec/IKEv2 接続を確立します。接続の終了時には、（設定に応じて）そのまま残るか、または自分自身をアンインストールします。

以前にインストールされているクライアントの場合は、ユーザの認証時に、ASA がクライアントのリビジョンを検査して、必要に応じてクライアントをアップグレードします。

クライアントが ASA と SSL VPN 接続をネゴシエートした場合は、Transport Layer Security（TLS）を使用して接続します。状況に応じて、Datagram Transport Layer Security（DTLS）が使用されます。DTLS により、一部の SSL 接続で発生する遅延および帯域幅の問題が回避され、パケット遅延の影響を受けやすいリアルタイム アプリケーションのパフォーマンスが向上します。

AnyConnect クライアントは、ASA からダウンロードできます。または、システム管理者が手動でリモート PC にインストールできます。クライアントを手動でインストールする方法の詳細については、『*Cisco AnyConnect VPN Client Administrator Guide*』を参照してください。

ASA は、ユーザが確立している接続のグループ ポリシーまたはユーザ名属性に基づきクライアントをダウンロードします。自動的にクライアントをダウンロードするように ASA を設定するか、またはクライアントをダウンロードするかをリモート ユーザに確認するように設定できます。後者の場合、ユーザが応答しなかった場合は、タイムアウト時間が経過した後にクライアントをダウンロードするか、ログイン ページを表示するように ASA を設定できます。

AnyConnect 接続のライセンス要件

（注）　この機能は、ペイロード暗号化機能のないモデルでは使用できません。

モデル	ライセンス要件
ASA 5512-X	次のいずれかを使用します。 • AnyConnect Premium ライセンス： – 基本ライセンス：2 セッション。 – *オプションの永続または時間ベースのライセンス：10、25、50、100、または 250 セッション。* – *オプションの共有ライセンス：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。* • AnyConnect Essentials ライセンス：250 セッション。
ASA 5515-X	次のいずれかを使用します。 • AnyConnect Premium ライセンス： – 基本ライセンス：2 セッション。 – *オプションの永続または時間ベースのライセンス：10、25、50、100、または 250 セッション。* – *オプションの共有ライセンス：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。* • AnyConnect Essentials ライセンス：250 セッション。
ASA 5525-X	次のいずれかを使用します。 • AnyConnect Premium ライセンス： – 基本ライセンス：2 セッション。 – *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、または 750 セッション。* – *オプションの共有ライセンス：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。* • AnyConnect Essentials ライセンス：750 セッション。

モデル	ライセンス要件
ASA 5545-X	次のいずれかを使用します。 • AnyConnect Premium ライセンス： – 基本ライセンス：2 セッション。 – *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、750、1000、または 2500 セッション。* – *オプションの共有ライセンス：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。* • AnyConnect Essentials ライセンス：2500 セッション。
ASA 5555-X	次のいずれかを使用します。 • AnyConnect Premium ライセンス： – 基本ライセンス：2 セッション。 – *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、750、1000、2500、または 5000 セッション。* – *オプションの共有ライセンス：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。* • AnyConnect Essentials ライセンス：5000 セッション。
ASA 5585-X（SSP-10）	次のいずれかを使用します。 • AnyConnect Premium ライセンス： – 基本ライセンス：2 セッション。 – *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、750、1000、2500、または 5000 セッション。* – *オプションの共有ライセンス：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。* • AnyConnect Essentials ライセンス：5000 セッション。
ASA 5585-X（SSP-20、-40、および -60）	次のいずれかを使用します。 • AnyConnect Premium ライセンス： – 基本ライセンス：2 セッション。 – *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、750、1000、2500、5000、または 10000 セッション。* – *オプションの共有ライセンス：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。* • AnyConnect Essentials ライセンス：10000 セッション。

モデル	ライセンス要件
ASASM	次のいずれかを使用します。 • AnyConnect Premium ライセンス： – 基本ライセンス：2 セッション。 – *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、750、1000、2500、5000、または 10000 セッション。* – *オプションの共有ライセンス：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。* • AnyConnect Essentials ライセンス：10000 セッション。
ASAv（仮想 CPU X 1 を搭載）	• 標準ライセンス：2 セッション。 • Premium ライセンス：250 セッション。
ASAv（仮想 CPU X 4 を搭載）	• 標準ライセンス：2 セッション。 • Premium ライセンス：750 セッション。

（注） クライアントレス SSL VPN セッションを開始した後、ポータルから AnyConnect クライアント セッションを開始した場合は、合計 1 つのセッションが使用されています。これに対して、最初に AnyConnect クライアントを（スタンドアロン クライアントなどから）開始した後、クライアントレス SSL VPN ポータルにログインした場合は、2 つのセッションが使用されています。

すべてのタイプの組み合わせ VPN セッションの最大数は、この表に示す最大セッション数を超えることはできません。ASA 5505 では、組み合わせセッションの最大数は 10（基本ライセンスの場合）または 25（Security Plus ライセンスの場合）です。

共有ライセンスによって、ASA は複数のクライアントの ASA の共有ライセンス サーバとして機能します。共有ライセンス プールは大規模ですが、個々の ASA によって使用されるセッションの最大数は、永続的なライセンスで指定される最大数を超えることはできません。

AnyConnect Essentials ライセンスにより、AnyConnect VPN クライアントは ASA へのアクセスが可能になります。このライセンスでは、ブラウザベースの SSL VPN アクセスまたは Cisco Secure Desktop はサポートされていません。これらの機能に対しては、AnyConnect Essentials ライセンスの代わりに AnyConnect Premium ライセンスがアクティブ化されます。AnyConnect Essentials ライセンスを所有する VPN ユーザは、Web ブラウザを使用してログインし、AnyConnect クライアントをダウンロードおよび起動（WebLaunch）することができます。このライセンスと AnyConnect Premium SSL VPN ライセンスのいずれでイネーブル化されたかには関係なく、AnyConnect クライアント ソフトウェアには同じクライアント機能のセットが装備されています。特定の ASA では、AnyConnect Premium ライセンス（全タイプ）または Advanced Endpoint Assessment ライセンスを、AnyConnect Essentials ライセンスと同時にアクティブにすることはできません。ただし、同じネットワーク内の異なる ASA で、AnyConnect Essentials ライセンスと AnyConnect Premium ライセンスを実行することは可能です。デフォルトでは、ASA は AnyConnect Essentials ライセンスを使用しますが（存在する場合）、**no anyconnect-essentials** コマンドを使用すると、AnyConnect Essentials ライセンスをディセーブルにして他のライセンスを使用できます。AnyConnect Essentials ライセンスおよび AnyConnect Premium ライセンスでサポートされている機能の詳細なリストについては、『*AnyConnect Secure Mobility Client Features, Licenses, and OSs*』を参照してください。http://www.cisco.com/en/US/products/ps10884/products_feature_guides_list.html

ガイドラインと制限事項

この項では、この機能のガイドラインと制限事項について説明します。

リモート PC のシステム要件

AnyConnect Secure Mobility Client を実行するエンドポイント コンピュータの要件については、ASA で展開する AnyConnect クライアント バージョンのリリース ノートを参照してください。

リモート HTTPS 証明書の制限事項

ASA では、リモート HTTPS 証明書は確認されません。

AnyConnect 接続の設定

ここでは、ASA がAnyConnect VPN クライアント接続を受け入れるように設定するための前提条件、制限事項、および詳細なタスクについて説明します。

クライアントを Web 展開するための ASA の設定

この項では、AnyConnect クライアントを Web 展開するように ASA を設定する手順について説明します。

前提条件

TFTP や別の方法を使用して、クライアント イメージ パッケージを ASA にコピーします。

手順の詳細

	コマンド	目的
ステップ 1	anyconnect image *filename order* 例： hostname(config-webvpn)#**anyconnect image anyconnect-win-2.3.0254-k9.pkg 1** hostname(config-webvpn)#**anyconnect image anyconnect-macosx-i386-2.3.0254-k9.pkg 2** hostname(config-webvpn)#**anyconnect image anyconnect-linux-2.3.0254-k9.pkg 3**	フラッシュのファイルを AnyConnect クライアント パッケージ ファイルとして指定します。 ASA は、リモート PC にダウンロードするために、キャッシュ メモリのファイルを展開します。複数のクライアントがある場合は、order 引数を使用して、クライアント イメージに順序を割り当てます。 ASA は、リモート PC のオペレーティング システムと一致するまで、指定されている順序で各クライアントの一部をダウンロードします。そのため、最も一般的に使用されているオペレーティング システム用のイメージには、最も低い数値を割り当てます。 （注） **anyconnect image xyz** コマンドで AnyConnect イメージを設定した後に **anyconnect enable** コマンドを発行する必要があります。**anyconnect enable** コマンドをイネーブルにしない場合、AnyConnect の動作は不完全になり、**show webvpn anyconnect** コマンドは SSL VPN クライアントがイネーブルにされていないと見なし、インストールされた AnyConnect パッケージをリストしません。
ステップ 2	**enable** *interface* 例： hostname(config)# **webvpn** hostname(config-webvpn)# **enable outside**	クライアントレス接続または AnyConnect SSL 接続のインターフェイスの SSL をイネーブルにします。
ステップ 3	**anyconnect enable**	このコマンドを発行しないと、AnyConnect は想定したとおりに機能せず、**show webvpn anyconnect** コマンドは、インストールされた AnyConnect パッケージをリストする代わりに、「SSL VPN is not enabled」というメッセージを返します。
ステップ 4	**ip local pool** *poolname startaddr-endaddr* **mask** *mask* 例： hostname(config)# **ip local pool vpn_users 209.165.200.225-209.165.200.254 mask 255.255.255.224**	（オプション）アドレス プールを作成します。DHCP やユーザによる割り当てのアドレスの指定など、別のアドレス割り当ての方法を使用することもできます。
ステップ 5	**address-pool** *poolname* 例： hostname(config)# **tunnel-group telecommuters general-attributes** hostname(config-tunnel-general)# **address-pool vpn_users**	アドレス プールをトンネル グループに割り当てます。
ステップ 6	**default-group-policy** *name* 例： hostname(config-tunnel-general)# **default-group-policy sales**	デフォルトのグループ ポリシーをトンネル グループに割り当てます。

	コマンド	目的
ステップ 7	**group-alias** *name* **enable** 例： hostname(config)# **tunnel-group telecommuters webvpn-attributes** hostname(config-tunnel-webvpn)# **group-alias sales_department enable**	クライアントレス ポータルおよび AnyConnect GUI のログイン ページでのトンネルグループ リストの表示をイネーブルにします。エイリアスのリストは、*group-alias name enable* コマンドによって定義されます。
ステップ 8	**tunnel-group-list enable** 例： hostname(config)# **webvpn** hostname(config-webvpn)# **tunnel-group-list enable**	グループまたはユーザの許可された VPN トンネリング プロトコルとして AnyConnect クライアントを指定します。
ステップ 9	**vpn-tunnel-protocol** 例： hostname(config)# **group-policy sales attributes** hostname(config-group-policy)# **webvpn** hostname(config-group-webvpn)# **vpn-tunnel-protocol**	グループまたはユーザの許可された VPN トンネリング プロトコルとして SSL を指定します。その他のプロトコルを追加して指定することもできます。詳細については、コマンド リファレンスの **vpn-tunnel-protocol** コマンドを参照してください。 グループ ポリシーに対するユーザの割り当ての詳細については、第 6 章「接続プロファイル、グループ ポリシー、およびユーザの設定」を参照してください。

永続的なクライアント インストールのイネーブル化

永続的なクライアント インストールをイネーブルにすると、クライアントの自動アンインストール機能がディセーブルになります。クライアントは、後続の接続のためにリモート コンピュータにインストールされたままなので、リモート ユーザの接続時間が短縮されます。

特定のグループまたはユーザに対する永続的なクライアント インストールをイネーブルにするには、グループ ポリシー webvpn モードまたはユーザ名 webvpn モードで **anyconnect keep-installer** コマンドを使用します。

anyconnect keep-installer installer

デフォルトでは、クライアントの永続的なインストールはイネーブルになっています。セッションの終了時に、クライアントはリモート コンピュータ上に残ります。次の例では、セッションの終了時点でリモート コンピュータのクライアントを削除するように既存のグループ ポリシー *sales* を設定します。

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-policy)# anyconnect keep-installer installed none
```

DTLS の設定

Datagram Transport Layer Security（DTLS）を使用すると、SSL VPN 接続を確立している AnyConnect クライアントで、2 つのトンネル（SSL トンネルと DTLS トンネル）を同時に使用できます。DTLS を使用すると、SSL 接続で発生する遅延および帯域幅の問題が回避され、パケット遅延の影響を受けやすいリアルタイム アプリケーションのパフォーマンスが向上します。

デフォルトでは、DTLS がイネーブルになるのは、インターフェイスで SSL VPN アクセスをイネーブルにした場合です。DTLS をディセーブルにすると、SSL VPN 接続は SSL VPN トンネルだけに接続します。

（注）　DTLS を TLS 接続にフォール バックさせるには、デッド ピア検知（DPD）をイネーブルにする必要があります。DPD をイネーブルにしない場合、DTLS 接続で問題が発生すると、TLS にフォール バックする代わりに接続は終了します。DPD のイネーブル化の詳細については、「Dead Peer Detection のイネーブル化と調整」（P.10-17）を参照してください。

webvpn コンフィギュレーション モードで、**enable** コマンドの **tls-only** オプションを使用すると、すべての AnyConnect クライアント ユーザに対して DTLS をディセーブルにできます。

enable <*interface*> **tls-only**

次に例を示します。

hostname(config-webvpn)# **enable outside tls-only**

デフォルトでは、特定のグループまたはユーザに対して DTLS をイネーブルにするには、グループ ポリシー webvpn コンフィギュレーション モードまたはユーザ名 webvpn コンフィギュレーション モードで、**anyconnect ssl dtls** コマンドを使用します。

[**no**] **anyconnect ssl dtls {enable interface | none}**

DTLS をディセーブルにする必要がある場合は、このコマンドの **no** 形式を使用します。次に例を示します。

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# no anyconnect ssl dtls none
```

リモート ユーザに対するプロンプト

ASA で、リモート SSL VPN クライアント ユーザがクライアントをダウンロードするためのプロンプトをイネーブルにするには、グループ ポリシー webvpn コンフィギュレーション モードまたはユーザ名 webvpn コンフィギュレーション モードで **anyconnect ask** コマンドを使用します。

[**no**] **anyconnect ask** {**none** | **enable** [**default** {**webvpn** | } **timeout** *value*]}

anyconnect enable を指定すると、クライアントをダウンロードするか、クライアントレス ポータル ページに移動するかをリモート ユーザに尋ねるプロンプトを表示し、ユーザの応答を無期限に待機します。

anyconnect ask enable default を指定すると、クライアントをすぐにダウンロードします。

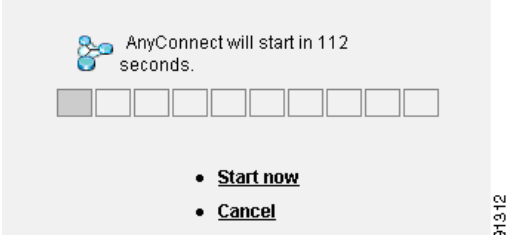
anyconnect ask enable default webvpn を指定すると、ポータル ページにすぐに移動します。

anyconnect ask enable default timeout *value* を指定すると、クライアントをダウンロードするか、またはクライアントレス ポータル ページに移動するかを尋ねるプロンプトをリモート ユーザに表示し、デフォルト アクション（クライアントのダウンロード）を実行する前に、*value* の間待機します。

anyconnect ask enable default clientless timeout *value* を指定すると、クライアントをダウンロードするか、またはクライアントレス ポータル ページに移動するかを尋ねるプロンプトをリモート ユーザに表示し、デフォルト アクション（クライアントレス ポータル ページの表示）を実行する前に、*value* の間待機します。

図 10-1 に、**default anyconnect timeout** *value* または **default webvpn timeout** *value* が設定された場合にリモート ユーザに表示されるプロンプトを示します。

図 10-1　　SSL VPN Client のダウンロードに関してリモート ユーザに表示されるプロンプト



次の例では、ASA でクライアントをダウンロードするか、またはクライアントレス ポータル ページに移動するかを尋ねるプロンプトを表示して、クライアントをダウンロードする前に*応答を 10 秒*待機するように設定しています。

```
hostname(config-group-webvpn)# anyconnect ask enable default anyconnect timeout 10
```

AnyConnect クライアント プロファイル ダウンロードのイネーブル化

AnyConnect プロファイルで Cisco AnyConnect Secure Mobility Client 機能をイネーブルにします（コア クライアントのコンフィギュレーション設定と VPN 機能、およびオプションのクライアント モジュールのコンフィギュレーション設定を含む XML ファイル、ネットワーク アクセス マネージャ（NAM）、ポスチャ、テレメトリ、Web Security）。ASA は AnyConnect のインストールおよびアップデート中にプロファイルを展開します。ユーザがプロファイルの管理や修正を行うことはできません。

ASDM のプロファイル エディタ

プロファイルは、AnyConnect プロファイル エディタを使用して設定できます。このエディタは、ASDM から起動できる便利な GUI ベースの設定ツールです。Windows 用 AnyConnect ソフトウェア パッケージ バージョン 2.5 以降には、エディタが含まれています。このエディタは、AnyConnect パッケージを ASA にロードし、AnyConnect クライアント イメージとして指定するとアクティブ化されます。

スタンドアロン プロファイル エディタ

ASDM に統合されたプロファイル エディタの代わりに、Windows 用プロファイル エディタのスタンドアロン バージョンも使用できます。クライアントを事前展開する場合は、ソフトウェア管理システムを使用してコンピュータに展開する、VPN サービス用のプロファイルおよびその他のモジュールを、スタンドアロンのプロファイル エディタを使用して作成できます。プロファイル エディタの使用の詳細については、『Cisco AnyConnect Secure Mobility Client Administrator Guide』を参照してください。

（注）　AnyConnect クライアント プロトコルのデフォルトは SSL です。IPsec IKEv2 をイネーブルにするには、ASA で IKEv2 設定を設定し、また、クライアント プロファイルのプライマリ プロトコルとして IKEv2 を設定する必要があります。IKEv2enabled プロファイルは、エンドポイント コンピュータに展開する必要があります。それ以外の場合、クライアントは SSL を使用して接続を試行します。詳細については、『Cisco AnyConnect Secure Mobility Client Administrator Guide』を参照してください。

次の手順に従いプロファイルを編集し、ASA でプロファイルのリモート クライアントへのダウンロードをイネーブルにします。

ステップ 1　ASDM のプロファイル エディタまたはスタンドアロン プロファイル エディタを使用して、プロファイルを作成します。詳細については、『Cisco AnyConnect Secure Mobility Client Administrator Guide』を参照してください。

ステップ 2　tftp または別の方式を使用して、ASA のフラッシュ メモリにプロファイル ファイルをロードします。

ステップ 3　webvpn コンフィギュレーション モードで **anyconnect profiles** コマンドを使用して、キャッシュ メモリにロードするクライアント プロファイルとしてこのファイルを識別します。

次に、プロファイルとしてファイル *sales_hosts.xml* と *engineering_hosts.xml* を指定する例を示します。

```
asa1(config-webvpn)# anyconnect profiles sales disk0:/sales_hosts.xml
asa1(config-webvpn)# anyconnect profiles engineering disk0:/engineering_hosts.xml
```

これで、プロファイルをグループ ポリシーに利用できます。

キャッシュ メモリにロードされたプロファイルを表示するには、**dir cache:stc/profiles** コマンドを使用します。

```
hostname(config-webvpn)# dir cache:/stc/profiles

Directory of cache:stc/profiles/

0      ----  774         11:54:41 Nov 22 2006  engineering.xml
0      ----  774         11:54:29 Nov 22 2006  sales.xml

2428928 bytes total (18219008 bytes free)
hostname(config-webvpn)#
```

ステップ 4　グループ ポリシー webvpn コンフィギュレーション モードを開始し、**anyconnect profiles** コマンドを使用して、グループ ポリシーのクライアント プロファイルを指定します。

使用可能なプロファイルを表示するには、**anyconnect profiles value** コマンドに続けて、疑問符（**?**）を入力します。次に例を示します。

```
asa1(config-group-webvpn)# anyconnect profiles value ?

config-group-webvpn mode commands/options:
Available configured profile packages:
engineering
  sales
```

次の例では、クライアント プロファイル タイプが *vpn* のプロファイル *sales* を使用するようにグループ ポリシーを設定します。

```
asa1(config-group-webvpn)# anyconnect profiles value sales type vpn
asa1(config-group-webvpn)#
```

AnyConnect クライアントの遅延アップグレードのイネーブル化

AnyConnect ユーザは、遅延アップグレードを使用して、クライアント アップグレードのダウンロードを遅らせることができます。クライアント アップデートが使用できる場合、AnyConnect は、更新するか、またはアップグレードを延期するかを尋ねるダイアログを開きます。

遅延アップグレードをイネーブルにするには、カスタム属性タイプと名前付きの値を ASA に追加して、グループ ポリシーでこれらの属性を参照および設定します。

次のカスタム属性は遅延アップグレードをサポートします。

表 10-1　遅延アップグレードのカスタム属性

カスタム属性タイプ	有効値	デフォルト値	注記
DeferredUpdateAllowed	true false	false	[true] を指定すると、延期アップデートが有効になります。延期アップデートが無効（false）の場合、下記の設定は無視されます。
DeferredUpdateMinimumVersion	x.y.z	0.0.0	アップデートを延期できるようにするため、インストールする必要がある最小バージョンの AnyConnect。 最小バージョンのチェックは、ヘッドエンドで有効になっているすべてのモジュールに適用されます。VPN を含む有効な任意のモジュールがインストールされていない、または最小要件を満たしていない場合、接続して延期アップデートすることはできません。 この属性が指定されていない場合、エンドポイントにインストールされているバージョンに関係なく、延期プロンプトが表示されるか（自動的に却下されます）。
DeferredUpdateDismissTimeout	0 ～ 300（秒）	none（無効）	遅延アップグレード プロンプトが表示され、自動的に却下されるまでの秒数。この属性は、延期アップデート プロンプトを表示する場合のみ適用されます（最小バージョンの属性が最初に評価されます）。 この属性が見つからない場合、自動却下機能が無効になり、ユーザが応答するまで（必要に応じて）ダイアログが表示されます。 この属性をゼロに設定すると、次に基づいて強制的に自動延期またはアップグレードが実施されます。 • インストール済みバージョンと DeferredUpdateMinimumVersion の値 • DeferredUpdateDismissResponse の値
DeferredUpdateDismissResponse	defer update	update	DeferredUpdateDismissTimeout 発生時に実施するアクション。

ステップ 1　webvpn コンフィギュレーション モードで **anyconnnect-custom-attr** コマンドを使用してカスタム属性タイプを作成します。

[no] anyconnect-custom-attr *attr-type* **[description** *description***]**

次に、カスタム属性タイプ DeferredUpdateAllowed および DeferredUpdateDismissTimeout を追加する例を示します。

```
hostame(config)# anyconnect-custom-attr DeferredUpdateAllowed description Indicates if the
deferred update feature is enabled or not
hostame(config)# anyconnect-custom-attr DeferredUpdateDismissTimout
```

ステップ 2　グローバル コンフィギュレーション モードで **anyconnect-custom-data** コマンドを使用してカスタム属性の名前付きの値を追加します。

[no] anyconnect-custom-data *attr-type attr-name attr-value*

次に、カスタム属性タイプ DeferredUpdateDismissTimout の名前付きの値と、DeferredUpdateAllowed をイネーブルにするための名前付きの値を追加する例を示します。

```
hostname(config)# anyconnect-custom-data DeferredUpdateDismissTimout def-timeout 150
hostname(config)# anyconnect-custom-data DeferredUpdateAllowed def-allowed true
```

ステップ 3　**anyconnect-custom** コマンドを使用して、カスタム属性の名前付きの値をグループ ポリシーに追加するか、グループ ポリシーから削除します。

anyconnect-custom *attr-type* **value** *attr-name*

anyconnect-custom *attr-type* **none**

no anyconnect-custom *attr-type*

次に、sales という名前のグループ ポリシーで延期アップデートを有効にしてタイムアウトを 150 秒に設定する例を示します。

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-policy)# anyconnect-custom DeferredUpdateAllowed value def-allowed
hostname(config-group-policy)# anyconnect-custom DeferredUpdateDismissTimeout value
def-timout
```

追加の AnyConnect クライアント機能のイネーブル化

ダウンロード時間を最小限に抑えるために、クライアントは必要なコア モジュールのダウンロード（ASA から）だけを要求します。追加機能が AnyConnect クライアントで使用可能になったら、それらの機能を使用できるようにするためにリモート クライアントをアップデートする必要があります。

新しい機能をイネーブルにするには、グループ ポリシー webvpn またはユーザ名 webvpn コンフィギュレーション モードで **anyconnect modules** コマンドを使用して、新しいモジュール名を指定する必要があります。

[no] anyconnect modules {**none** | **value** *string*}

複数のストリングを指定する場合は、カンマで区切ります。

各クライアント機能に対して入力する値のリストについては、Cisco AnyConnect VPN Client のリリース ノートを参照してください。

Start Before Logon のイネーブル化

Start Before Logon（SBL）を使用すると、Windows PC にインストールされている AnyConnect クライアントに対するログイン スクリプト、パスワード キャッシング、ドライブ マッピングなどが使用できるようになります。SBL では、AnyConnect クライアントの Graphical Identification and Authentication（GINA）をイネーブルにするモジュールをダウンロードするように ASA をイネーブルにする必要があります。次の手順は、SBL をイネーブルにする方法を示しています。

ステップ 1　グループ ポリシー webvpn またはユーザ名 webvpn コンフィギュレーション モードで **anyconnect modules** *vpngina* コマンドを使用して、ASA で特定のグループまたはユーザに VPN 接続に対する GINA モジュールをダウンロードできるようにします。

次の例では、ユーザはグループ ポリシー *telecommuters* でグループ ポリシー属性モードを開始し、そのグループ ポリシーで webvpn コンフィギュレーション モードを開始し、ストリング *vpngina* を指定します。

```
hostname(config)# group-policy telecommuters attributes
hostname(config-group-policy)# webvpn
hostame(config-group-webvpn)#anyconnect modules value vpngina
```

ステップ 2　クライアント プロファイル ファイル（AnyConnectProfile.tmpl）のコピーを取得します。

ステップ 3　プロファイル ファイルを編集して SBL がイネーブルであることを指定します。次の例では、Windows 用のプロファイル ファイル（AnyConnectProfile.tmpl）の関係部分を示しています。

```
<Configuration>
    <ClientInitialization>
        <UseStartBeforeLogon>false</UseStartBeforeLogon>
    </ClientInitialization>
```

<UseStartBeforeLogon> タグによって、クライアントが SBL を使用するかどうかが決まります。SBL をオンにするには、*false* を *true* で置き換えます。次の例は、SBL がオンになっているタグを示しています。

```
    <ClientInitialization>
        <UseStartBeforeLogon>true</UseStartBeforeLogon>
    </ClientInitialization>
```

ステップ 4　AnyConnectProfile.tmpl に対する変更を保存し、webvpn コンフィギュレーション モードで **profile** コマンドを使用して、ASA のグループまたはユーザに対するプロファイル ファイルをアップデートします。次に例を示します。

```
asa1(config-webvpn)#anyconnect profiles sales disk0:/sales_hosts.xml
```

AnyConnect ユーザ メッセージの言語の変換

ASA には、ブラウザベースのクライアントレス SSL VPN 接続を開始するユーザに表示されるポータルと画面、および Cisco AnyConnect VPN Client ユーザに表示されるインターフェイスの言語変換機能があります。

この項では、これらのユーザ メッセージを変換するために ASA を設定する方法について説明します。次の項目を取り上げます。

- 「言語変換の概要」（P.10-14）
- 「変換テーブルの作成」（P.10-14）

言語変換の概要

リモート ユーザに可視である機能エリアとそれらのメッセージは、変換ドメイン内にまとめられています。*Cisco AnyConnect VPN Client のユーザ インターフェイスに表示されるすべてのメッセージは、AnyConnect ドメイン内にあります。*

ASA のソフトウェア イメージ パッケージには、AnyConnect ドメインの変換テーブル テンプレートが含まれています。このテンプレートはエクスポートでき、入力する URL にテンプレートの XML ファイルが作成されます。このファイルのメッセージ フィールドは空です。メッセージを編集して、テンプレートをインポートし、フラッシュ メモリに置かれる新しい変換テーブル オブジェクトを作成できます。

既存の変換テーブルをエクスポートすることもできます。作成した XML ファイルに事前に編集したメッセージが表示されます。この XML ファイルを同じ言語名で再インポートすると、変換テーブル オブジェクトの新しいバージョンが作成され、以前のメッセージが上書きされます。AnyConnect ドメインの変換テーブルに対する変更は、ただちに AnyConnect クライアント ユーザに表示されます。

変換テーブルの作成

次の手順では、AnyConnect ドメインの変換テーブルを作成する方法について説明します。

ステップ 1　特権 EXEC モードで **export webvpn translation-table** コマンドを使用して、コンピュータに変換テーブル テンプレートをエクスポートします。

次の例では、**show webvpn translation-table** コマンドによって、使用可能な変換テーブル テンプレートとテーブルを表示しています。

```
hostname# show import webvpn translation-table
Translation Tables' Templates:
customization
AnyConnect
CSD
PortForwarder
url-list
webvpn
Citrix-plugin
RPC-plugin
Telnet-SSH-plugin
VNC-plugin

Translation Tables:
```

次に、AnyConnect 変換ドメイン用の変換テーブルをエクスポートします。作成された XML ファイルのファイル名は *client* という名前が付けられ、空のメッセージ フィールドが含まれています。

```
hostname# export webvpn translation-table AnyConnect template
tftp://209.165.200.225/client
```

次の例では、*zh* という名前の変換テーブルをエクスポートします。このテーブルは、テンプレートから事前にインポートされたものです。zh は中国語について Microsoft Internet Explorer で使用される省略形です。

```
hostname# export webvpn translation-table customization language zh
tftp://209.165.200.225/chinese_client
```

ステップ 2　変換テーブルの XML ファイルを編集します。次の例は、AnyConnect テンプレートの一部を示しています。この出力の最後には、*Connected* メッセージのメッセージ ID フィールド（msgid）とメッセージ文字列フィールド（msgstr）が含まれています。このメッセージは、クライアントが VPN 接続を確立するときに AnyConnect クライアント GUI に表示されます。完全なテンプレートには、多くのメッセージ フィールドのペアが含まれています。

```
# SOME DESCRIPTIVE TITLE.
# Copyright (C) YEAR THE PACKAGE'S COPYRIGHT HOLDER
# This file is distributed under the same license as the PACKAGE package.
# FIRST AUTHOR <EMAIL@ADDRESS>, YEAR.
#
#, fuzzy
msgid ""
msgstr ""
"Project-Id-Version: PACKAGE VERSION\n"
"Report-Msgid-Bugs-To: \n"
"POT-Creation-Date: 2006-11-01 16:39-0700\n"
"PO-Revision-Date: YEAR-MO-DA HO:MI+ZONE\n"
"Last-Translator: FULL NAME <EMAIL@ADDRESS>\n"
"Language-Team: LANGUAGE <LL@li.org>\n"
"MIME-Version: 1.0\n"
"Content-Type: text/plain; charset=CHARSET\n"
"Content-Transfer-Encoding: 8bit\n"

#: C:\cygwin\home\<user>\cvc\main\Api\AgentIfc.cpp:23
#: C:\cygwin\home\<user>\cvc\main\Api\check\AgentIfc.cpp:22
#: C:\cygwin\home\<user>\cvc\main\Api\save\AgentIfc.cpp:23
#: C:\cygwin\home\<user>\cvc\main\Api\save\AgentIfc.cpp~:20
#: C:\cygwin\home\<user>\cvc\main\Api\save\older\AgentIfc.cpp:22
msgid "Connected"
msgstr ""
```

msgid には、デフォルト変換が含まれています。msgid に続く msgstr が変換を提供します。変換を作成するには、msgstr 文字列の引用符の間に変換対象のテキストを入力します。たとえば、メッセージ「Connected」をスペイン語で変換するには、引用符の間にスペイン語のテキストを挿入します。

```
msgid "Connected"
msgstr "Conectado"
```

ファイルは必ず保存してください。

ステップ 3　特権 EXEC モードで **import webvpn translation-table** コマンドを使用して、変換テーブルをインポートします。ブラウザと互換性がある言語の省略形を付けて新しい変換テーブルの名前を指定します。

次の例では、米国内スペイン語圏について Microsoft Internet Explorer で使用される省略形である *es-us* で XML ファイルがインポートされます。

```
hostname# import webvpn translation-table AnyConnect language es-us
tftp://209.165.200.225/client
hostname# !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
hostname# show import webvpn translation-table
Translation Tables' Templates:
AnyConnect
PortForwarder
csd
customization
keepout
url-list
webvpn
Citrix-plugin
```

```
RPC-plugin
Telnet-SSH-plugin
VNC-plugin

Translation Tables:
es-us AnyConnect
```

高度な AnyConnect SSL 機能の設定

次の項では、AnyConnect SSL VPN 接続を調整する高度な機能について説明します。次の項目を取り上げます。

キーの再生成のイネーブル化

ASA と AnyConnect クライアントが SSL VPN 接続でキー再生成を行うときは、暗号キーと初期化ベクトルを再ネゴシエーションして、接続のセキュリティを高めます。

特定のグループまたはユーザの SSL VPN 接続で、クライアントによるキー再生成の実行をイネーブルにするには、グループ ポリシー webvpn モードまたはユーザ名 webvpn モードで **anyconnect ssl rekey** コマンドを使用します。

[no]anyconnect ssl rekey {**method** {**new-tunnel** | **none** | **ssl**} | **time** *minutes*}

method new-tunnel は、キーの再生成中にクライアントが新規トンネルを確立するように指定します。

method ssl は、キー再生成中にクライアントが新規トンネルを確立するように指定します。

method none は、キー再生成をディセーブルにします。

（注） キーの再生成方法を **ssl** または **new-tunnel** に設定すると、キー再生成時に SSL 再ネゴシエーションが行われず、クライアントがキー再生成時に新規トンネルを確立することが指定されます。**anyconnect ssl rekey** コマンドの履歴に関するコマンド リファレンスを参照してください。

time *minutes* は、セッションの開始からまたは前回のキー再生成から、キーの再生成が行われるまでの時間を 1 から 10080（1 週間）の分数で指定します。

次の例では、セッション開始の 30 分後に実施されるキー再生成中に、既存のグループ ポリシー *sales* に対する SSL との再ネゴシエーションを実施するようにクライアントを設定しています。

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# anyconnect ssl rekey method ssl
hostname(config-group-webvpn)# anyconnect ssl rekey time 30
```

Dead Peer Detection のイネーブル化と調整

Dead Peer Detection（DPD）により、ピアの応答がなく接続が失敗している場合には、ASA（ゲートウェイ）またはクライアント側で瞬時に検出できます。

ASA またはクライアントで特定のグループまたはユーザについて DPD をイネーブルにし、ASA またはクライアントが DPD を実行する頻度を設定するには、グループ ポリシーまたはユーザ名 webvpn モードで **anyconnect dpd-interval** コマンドを使用します。

anyconnect dpd-interval {[**gateway** {*seconds* | **none***}*] | [**client** {*seconds* | **none***}*]}

値は次のとおりです。

gateway seconds は、ASA（ゲートウェイ）で実行する DPD をイネーブルにして、ASA（ゲートウェイ）での DPD の実行頻度（5 ～ 3600 秒）を指定します。

gateway none は、ASA による DPD をディセーブルにします。

client *seconds* は、クライアントによる DPD をイネーブルにし、クライアントが DPD を実行する頻度（5 ～ 3600 秒）を指定します。

client none は、クライアントによって実行される DPD をディセーブルにします。

anyconnect dpd-interval コマンドをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

no anyconnect dpd-interval {[**gateway** {*seconds* | **none***}*] | [**client** {*seconds* | **none***}*]}

（注）　DTLS をイネーブルにすると、Dead Peer Detection（DPD）もイネーブルになります。DPD により、失敗した DTLS 接続の TLS へのフォールバックがイネーブルになります。それ以外の場合、接続は終了します。

次の例では、ASA による DPD の実行頻度が 30 秒に設定され、クライアントによる既存のグループ ポリシー *sales* に対する DPD の実行頻度が 10 秒に設定されています。

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# anyconnect dpd-interval gateway 30
hostname(config-group-webvpn)# anyconnect dpd-interval client 10
```

キープアライブのイネーブル化

キープアライブ メッセージの頻度を調整することで、接続がアイドルでいられる時間がデバイスによって制限されている場合でも、プロキシ、ファイアウォール、または NAT デバイス経由の SSL VPN 接続をオープンのまま維持します。また、頻度を調整すると、リモート ユーザが Microsoft Outlook または Microsoft Internet Explorer などのソケット ベース アプリケーションをアクティブに実行していない場合でも、クライアントは切断および再接続されません。

（注）　キープアライブはデフォルトでイネーブルになっています。キープアライブをディセーブルにすると、フェールオーバー イベントの際に、SSL VPN クライアント セッションはスタンバイ デバイスに引き継がれません。

キープアライブ メッセージの頻度を設定するには、グループ ポリシー webvpn またはユーザ名 webvpn コンフィギュレーション モードで、次のように **keepalive** コマンドを使用します。

[no] anyconnect ssl keepalive {none | *seconds***}**

none は、クライアントのキープアライブ メッセージをディセーブルにします。

seconds は、クライアントによるキープアライブ メッセージの送信をイネーブルにし、メッセージの頻度を 15 ～ 600 秒の範囲で指定します。

デフォルトでは、キープアライブ メッセージはイネーブルになっています。

コンフィギュレーションからこのコマンドを削除して、値が継承されるようにするには、コマンドの **no** 形式を使用します。

次の例では、既存のグループ ポリシー *sales* に対して、クライアントがキープアライブ メッセージを 300 秒（5 分）の頻度で送信できるように ASA を設定しています。

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)#anyconnect ssl keepalive 300
```

圧縮の使用

圧縮により、低帯域幅の接続に転送されるパケットのサイズが減少し、ASA とクライアント間の通信パフォーマンスが向上します。デフォルトでは、ASA では、グローバル レベルと特定のグループまたはユーザの両方において、すべての SSL VPN 接続に対する圧縮がイネーブルになっています。

（注） ブロードバンド接続の圧縮を実装する場合は、圧縮が損失が少ない接続に依存していることを慎重に考慮する必要があります。これが、ブロードバンド接続ではデフォルトで圧縮がイネーブルになっていない主な理由です。

圧縮は、グローバル コンフィギュレーション モードで **anyconnect ssl compression** コマンドを使用してグローバルにオンにする必要があります。そうすることで、グループ ポリシーおよびユーザ名 webvpn モードで **anyconnect ssl compression** コマンドを使用して、特定のグループまたはユーザに圧縮を設定することができます。

圧縮のグローバルな変更

グローバルな圧縮の設定を変更するには、グローバル コンフィギュレーション モードで **anyconnect ssl compression** コマンドを使用します。

compression

no compression

このコマンドをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

次の例では、すべての SSL VPN 接続の圧縮は、グローバルにディセーブルになっています。

```
hostname(config)# no compression
```

グループおよびユーザに対する圧縮の変更

特定のグループまたはユーザに対する圧縮を変更するには、グループ ポリシーおよびユーザ名 webvpn モードで **anyconnect ssl compression** コマンドを使用します。

anyconnect ssl compression {**deflate** | **none**}

no anyconnect ssl compression {**deflate** | **none**}

デフォルトでは、グループおよびユーザに対する SSL 圧縮は *deflate*（イネーブル）に設定されています。

コンフィギュレーションから **anyconnect ssl compression** コマンドを削除し、グローバル設定から値が継承されるようにするには、このコマンドの **no** 形式を使用します。

次に、グローバル ポリシー sales の圧縮をディセーブルにする例を示します。

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# no anyconnect ssl compression none
```

MTU サイズの調整

クライアントによって確立された SSL VPN 接続の MTU サイズ（256 ～ 1406 バイト）は、グループ ポリシー webvpn またはユーザ名 webvpn コンフィギュレーション モードで **anyconnect mtu** コマンドを使用して調整できます。

[no]anyconnect mtu *size*

このコマンドは、AnyConnect クライアントのみに影響します。レガシー Cisco SSL VPN クライアント（SVC）は、さまざまな MTU サイズに調整できません。

デフォルトのグループ ポリシーでのこのコマンドのデフォルトは、**no anyconnect mtu** です。MTU サイズは、接続で使用されているインターフェイスの MTU に基づき、IP/UDP/DTLS のオーバーヘッドを差し引いて、自動的に調整されます。

このコマンドは、SSL で確立されたクライアント接続、および SSL with DTLS で確立されたクライアント接続に影響を与えます。

例

次の例では、グループ ポリシー *telecommuters* の MTU サイズを 1200 バイトに設定します。

```
hostname(config)# group-policy telecommuters attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)#anyconnect mtu 1200
```

AnyConnect クライアント イメージのアップデート

ASA のクライアント イメージは、次の手順を使用していつでもアップデートできます。

ステップ 1　特権 EXEC モードで **copy** コマンドを使用して、または別の方法で新しいクライアント イメージを ASA にコピーします。

ステップ 2　新しいクライアント イメージ ファイルの名前がすでにロードされているファイルと同じファイル名の場合は、コンフィギュレーションにある **anyconnect image** コマンドを再入力します。新しいファイル名が異なっている場合は、**noanyconnect image** コマンドを使用して古いファイルをアンインストールします。次に、**anyconnect image** コマンドを使用して、イメージに順序を割り当て、ASA が新しいイメージをロードするようにします。

IPv6 VPN アクセスのイネーブル化

IPv6 アクセスを設定する場合は、コマンドライン インターフェイスを使用します。ASA のリリース 9.0（x）では、外部インターフェイスへの IPv6 VPN 接続（SSL および IKEv2/IPsec プロトコルを使用）のサポートが追加されています。

IPv6 アクセスをイネーブルにするには、SSL VPN 接続のイネーブル化の一部として **ipv6 enable** コマンドを使用します。次は、外部インターフェイスで IPv6 をイネーブルにする IPv6 接続の例です。

```
hostname(config)# interface GigabitEthernet0/0
hostname(config-if)# ipv6 enable
```

IPV6 SSL VPN をイネーブルにするには、次の一般的なアクションを実行します。

1. 外部インターフェイスで IPv6 をイネーブルにする。
2. 内部インターフェイスで IPv6 および IPv6 アドレスをイネーブルにする。
3. クライアント割り当て IP アドレス用に IPv6 アドレス ローカル プールを設定する。
4. IPv6 トンネルのデフォルト ゲートウェイを設定する。

この手順を実装するには、次の手順を実行します。

ステップ 1　インターフェイスを設定します。

```
interface GigabitEthernet0/0
     nameif outside
     security-level 0
     ip address 192.168.0.1 255.255.255.0
     ipv6 enable          ; Needed for IPv6.
    !
interface GigabitEthernet0/1
     nameif inside
     security-level 100
     ip address 10.10.0.1 255.255.0.0
     ipv6 address 2001:DB8::1/32        ; Needed for IPv6.
    ipv6 enable           ; Needed for IPv6.
```

ステップ 2　「ipv6 local pool」（IPv6 アドレスの割り当てに使用）を設定します。

```
ipv6 local pool ipv6pool 2001:DB8:1:1::5/32 100     ; Use your IPv6 prefix here
```

（注）　AnyConnect クライアントに IPv4 アドレスと IPv6 アドレスの一方または両方を割り当てるように ASA を設定できます。このようにするには、ASA 上で内部的なアドレス プールを作成するか、ASA 上のローカル ユーザに専用アドレスを割り当てます。

ステップ 3　IPv6 アドレス プールをトンネル グループ ポリシー（またはグループ ポリシー）に追加します。

```
tunnel-group YourTunGrp1 general-attributes  ipv6-address-pool ipv6pool
```

（注）　ここでは「address-pool」コマンドを使用して IPv4 アドレス プールも設定する必要があります。

ステップ 4　IPv6 トンネルのデフォルト ゲートウェイを設定します。

```
ipv6 route inside ::/0 X:X:X:X::X tunneled
```

AnyConnect 接続のモニタリング

アクティブなセッションについての情報を表示するには、**show vpn-sessiondb** を使用します。

コマンド	目的
show vpn-sessiondb	アクティブなセッションに関する情報を表示します。
vpn-sessiondb logoff	VPN セッションをログオフします。
show vpn-sessiondb anyconnect	VPN セッションの要約を拡張して、OSPFv3 セッション情報を表示します。
show vpn-sessiondb ratio encryption	Suite-B のアルゴリズム（AES-GCM-128、AES-GCM-192、AES-GCM-256、AES-GMAC-128 など）用のトンネル数およびパーセンテージを表示します。

例

Inactivity フィールドに、AnyConnect セッションが接続を失ってからの経過時間が表示されています。セッションがアクティブな状態の場合、このフィールドには 00:00m:00s が表示されます。

```
hostname# show vpn-sessiondb

Session Type: SSL VPN Client

Username     : lee
Index        : 1                      IP Addr      : 209.165.200.232
Protocol     : SSL VPN Client         Encryption   : 3DES
Hashing      : SHA1                   Auth Mode    : userPassword
TCP Dst Port : 443                    TCP Src Port : 54230
Bytes Tx     : 20178                  Bytes Rx     : 8662
Pkts Tx      : 27                     Pkts Rx      : 19
Client Ver   : Cisco STC 1.1.0.117
Client Type  : Internet Explorer
Group        : DfltGrpPolicy
Login Time   : 14:32:03 UTC Wed Mar 20 2007
Duration     : 0h:00m:04s
Inactivity   : 0h:00m:04s
Filter Name  :

hostname# vpn-sessiondb logoff
INFO: Number of sessions of type "" logged off : 1

hostname# vpn-sessiondb logoff name tester
Do you want to logoff the VPN session(s)?[confirm]
INFO: Number of sessions with name "tester" logged off : 1
```

AnyConnect VPN セッションのログオフ

すべての VPN セッションをログオフするには、グローバル コンフィギュレーション モードで **vpn-sessiondb logoff** コマンドを使用します。

vpn-sessiondb logoff

次に、すべての VPN セッションをログオフする例を示します。

```
hostname# vpn-sessiondb logoff
INFO: Number of sessions of type "" logged off : 1
```

name 引数または index 引数のいずれかを使用して、個々のセッションをログオフできます。

vpn-session-db logoff name *name*

vpn-session-db logoff index *index*

ライセンス容量に達して新しいユーザがログインできなくることがないように、非アクティブの状態が最長時間続いたセッションはアイドル状態になります（自動的にログオフされます）。そのセッションが後で再開すると、そのセッションは非アクティブ リストから削除されます。

ユーザ名とインデックス番号（クライアント イメージの順序で設定される）は、両方とも **show vpn-sessiondb anyconnect** コマンドの出力で確認できます。次の例は、ユーザ名 *lee* とインデックス番号 *1* を示しています。

```
hostname# show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : lee                    Index        : 1
Assigned IP  : 192.168.246.1           Public IP    : 10.139.1.2
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : RC4 AES128             Hashing      : SHA1
Bytes Tx     : 11079                  Bytes Rx     : 4942
Group Policy : EngPolicy            Tunnel Group : EngGroup
Login Time   : 15:25:13 EST Fri Jan 28 2011
Duration     : 0h:00m:15s
Inactivity   : 0h:00m:00s
NAC Result   : Unknown
VLAN Mapping : N/A                    VLAN         : none
```

次の例は、**vpn-session-db logoff** コマンドの **name** オプションを使用してセッションを終了しています。

```
hostname# vpn-sessiondb logoff name lee
Do you want to logoff the VPN session(s)?[confirm]
INFO: Number of sessions with name “lee” logged off : 1

hostname#
```

AnyConnect 接続をイネーブルにする設定例

次の例は、L2TP over IPsec を設定する方法を示しています。

```
ip local pool sales_addresses 209.165.202.129-209.165.202.158
aaa-server sales_server protocol radius
crypto ipsec transform-set sales_l2tp_transform esp-3des esp-sha-hmac
crypto ipsec transform-set sales_l2tp_transform mode transport
crypto ipsec security-association lifetime seconds 28800
crypto ipsec security-association lifetime kilobytes 4608000
l2tp tunnel hello 100

group-policy sales_policy internal
group-policy sales_policy attributes
 wins-server value 209.165.201.3 209.165.201.4
 dns-server value 209.165.201.1 209.165.201.2
 vpn-tunnel-protocol l2tp-ipsec
tunnel-group sales_tunnel type remote-access
tunnel-group sales_tunnel general-attributes
 address-pool sales_addresses
 authentication-server-group none
 accounting-server-group sales_server
 default-group-policy sales_policy
tunnel-group sales_tunnel ppp-attributes
 authentication pap
```

AnyConnect 接続の機能履歴

表 10-2 に、この機能のリリース履歴を示します。

表 10-2　AnyConnect 接続の機能履歴

機能名	リリース	機能情報
AnyConnect 接続	7.2(1)	**authentication eap-proxy**、**authentication ms-chap-v1**、**authentication ms-chap-v2**、**authentication pap**、**l2tp tunnel hello**、および **vpn-tunnel-protocol l2tp-ipsec** コマンドが導入または変更されました。
IPsec IKEv2	8.4(1)	AnyConnect および LAN-to-LAN の IPsec IKEv2 接続をサポートする IKEv2 が追加されました。

AnyConnect ホスト スキャン

[Configuration] > [Remote Access VPN] > [Host Scan Image]

AnyConnect ポスチャ モジュールにより、AnyConnect Secure Mobility Client はホストにインストールされているオペレーティング システム、およびアンチウイルス、アンチスパイウェア、ファイアウォールの各ソフトウェアを識別できます。この情報は、ホスト スキャン アプリケーションによって収集されます。

Adaptive Security Device Manager（ASDM）で Secure Desktop Manager ツールを使用すると、ホスト スキャンによって識別されるオペレーティング システム、およびアンチウイルス、アンチスパイウェア、ファイアウォールの各ソフトウェアを評価するプリログイン ポリシーを作成できます。プリログイン ポリシーの評価結果に基づいて、どのホストがセキュリティ アプライアンスへのリモート アクセス接続を確立できるかを制御できます。

ホスト スキャン サポート表には、プリログイン ポリシーで使用するアンチウイルス、アンチスパイウェア、およびファイアウォール アプリケーションの製品名とバージョン情報が含まれます。シスコでは、ホスト スキャン パッケージにホスト スキャン、ホスト スキャン サポート表、および他のコンポーネントを含めて提供しています。

AnyConnect Secure Mobility Client リリース 3.0 以降では、ホスト スキャンは CSD とは別に使用できます。これは、CSD をインストールしなくてもホスト スキャンの機能を展開できることを意味します。また、最新のホスト スキャン パッケージに更新することで、ホスト スキャン サポート表を更新できます。

ポスチャ アセスメントおよび AnyConnect テレメトリ モジュールは、ホストにホスト スキャンがインストールされている必要があります。

この章の内容は、次のとおりです。

ホスト スキャンの依存関係およびシステム要件

依存関係

AnyConnect Secure Mobility Client をポスチャ モジュールとともに使用するには、最低でも次のような ASA コンポーネントが必要です。

- ASA 8.4
- ASDM 6.4

次の AnyConnect 機能は、ポスチャ モジュールをインストールする必要があります。

- SCEP 認証
- AnyConnect テレメトリ モジュール

システム要件

ポスチャ モジュールは、次のいずれかのプラットフォームにインストールできます。

- Windows XP（x86 版、および x64 環境で動作する x86 版）
- Windows Vista（x86 版、および x64 環境で動作する x86 版）
- Windows 7（x86 版、および x64 環境で動作する x86 版）
- Mac OS X 10.5、10.6（32 ビット版、および 64 ビット環境で動作する 32 ビット版）
- Linux（32 ビット版、および 64 ビット環境で動作する 32 ビット版）
- Windows Mobile

ライセンス

ポスチャ モジュールには、次の AnyConnect ライセンシング要件があります。

- 基本ホスト スキャン用の AnyConnect Premium。
- 次の場合は、Advanced Endpoint Assessment ライセンスが必要です。
  - 修正
  - モバイル デバイス管理

ホスト スキャン パッケージ

ASA へのホスト スキャン パッケージは次のいずれかの方法でロードできます。

- **hostscan-*version*.pkg** は、スタンドアロン パッケージとしてアップロードできます。
- **anyconnect-NGC-win-*version*-k9.pkg** は、AnyConnect セキュア モビリティをアップロードすることによって、アップロードできます。
- **csd_version-k9.pkg** は、Cisco Secure Desktop をアップロードすることによって、アップロードできます。

ファイル	説明
hostscan-*version*.pkg	このファイルには、ホスト スキャン ソフトウェア、ホスト スキャン ライブラリ、およびサポート表が含まれています。
anyconnect-NGC-win-*version*-k9.pkg	このパッケージには、hostscan-*version*.pkg ファイルなど、Cisco AnyConnect Secure Mobility Client のすべての機能が含まれています。
csd_*version*-k9.pkg	このファイルには、ホスト スキャン ソフトウェア、ホスト スキャン ライブラリ、サポート表など、Cisco Secure Desktop のすべての機能が含まれています。 この方式には、Cisco Secure Desktop 用の別個のライセンスが必要です。

ASA 上でのホスト スキャンのインストールとイネーブル化

次のタスクでは、ASA 上でのホスト スキャンのインストールとイネーブル化について説明します。

- ホスト スキャンのインストールまたはアップグレード
- ホスト スキャンのイネーブル化またはディセーブル化
- ASA でイネーブルになっているホスト スキャンのバージョンの表示
- ホスト スキャンのアンインストール
- グループ ポリシーへの AnyConnect フィーチャ モジュールの割り当て

ホスト スキャンのインストールまたはアップグレード

この手順では、ASA のコマンドライン インターフェイスを使用してホスト スキャン パッケージをインストールまたはアップグレードし、イネーブルにします。

前提条件

- ASA にログオンし、グローバル コンフィギュレーション モードを開始します。グローバル コンフィギュレーション モードでは、ASA は hostname(config)# プロンプトを表示します。
- hostscan_version-k9.pkg ファイルまたは anyconnect-NGC-win-version-k9.pkg ファイルを ASA にアップロードします。

手順の詳細

	コマンド	目的
ステップ 1	**webvpn** **例：** hostname(config)# webvpn	webvpn コンフィギュレーション モードを開始します。
ステップ 2	**csd hostscan image** path **例：** ASAName(webvpn)#**csd hostscan image disk0:/*hostscan-3.6.0-k9.pkg*** ASAName(webvpn)#**csd hostscan image disk0:/anyconnect-NGC-win-3.0.0327-k9.pkg**	ホスト スキャン イメージとして指定するパッケージのパスを指定します。ホスト スキャン パッケージとして、スタンドアロンのホスト スキャン パッケージ、または AnyConnect Secure Mobility Client パッケージを指定することができます。 **（注）** Windows、Linux、および Mac OS X のどのオペレーティング システムの場合も、anyconnect-NGC-win-*version*-k9.pkg ファイルをアップロードする必要があります。これは、エンドポイントがホスト スキャンをインストールできるようにするためです。
ステップ 3	**csd enable** **例：** ASAName(webvpn)#**csd enable**	前の手順で指定したホスト スキャン イメージをイネーブルにします。
ステップ 4	write memory **例：** hostname(webvpn)# write memory	実行コンフィギュレーションをフラッシュ メモリに保存します。 新しいコンフィギュレーションがフラッシュ メモリに正常に保存されると、[OK] メッセージが表示されます。

ホスト スキャンのイネーブル化またはディセーブル化

これらのコマンドは、ASA のコマンドライン インターフェイスを使用して、インストール済みのホスト スキャン イメージをイネーブルまたはディセーブルにします。

前提条件

ASA にログオンし、グローバル コンフィギュレーション モードを開始します。グローバル コンフィギュレーション モードでは、ASA は hostname(config)# プロンプトを表示します。

ホスト スキャンをイネーブルにするための詳細な手順

	コマンド	目的
ステップ 1	**webvpn** **例：** `hostname(config)# webvpn`	webvpn コンフィギュレーション モードを開始します。
ステップ 2	**csd enable** **例：** hostname(config)# **csd enable**	スタンドアロンのホスト スキャン イメージ、または AnyConnect Secure Mobility Client パッケージ内のホスト スキャン イメージをイネーブルにします（まだ ASA からアンインストールされていない場合）。このどちらのタイプのパッケージもインストールされておらず、CSD パッケージがインストールされている場合は、この手順を実行すると CSD パッケージ内のホスト スキャン機能がイネーブルになります。

ホスト スキャンをディセーブルにするための詳細な手順

	コマンド	目的
ステップ 1	**webvpn** **例：** `hostname(config)# webvpn`	webvpn コンフィギュレーション モードを開始します。
ステップ 2	**no csd enable** **例：** hostname(config)# **no csd enable**	すべてのインストール済みホスト スキャン パッケージのホスト スキャンをディセーブルにします。 **（注）** イネーブルになっているホスト スキャン イメージをアンインストールする前に、このコマンドを使用して、ホスト スキャンをディセーブルにする必要があります。

ASA でイネーブルになっているホスト スキャンのバージョンの表示

この手順では、ASA のコマンドライン インターフェイスを使用して、イネーブルになっているホスト スキャンのバージョンを特定します。

前提条件

ASA にログインし、特権 EXEC モードを開始します。ASA の特権 EXEC モードでは、表示されるプロンプトは **hostname#** となります。

コマンド	目的
`show webvpn csd hostscan` **例：** `hostname# show webvpn csd hostscan`	ASA 上でイネーブルになっているホスト スキャンのバージョンを表示します。

ホスト スキャンのアンインストール

ホスト スキャン パッケージをアンインストールすると、ASDM インターフェイス上のビューから削除されます。これにより、ホスト スキャンまたは CSD がイネーブルの場合でも ASA によるホスト スキャン パッケージの展開が回避されます。ホスト スキャンをアンインストールしても、フラッシュ ドライブのホスト スキャン パッケージは削除されません。

前提条件

ASA にログオンし、グローバル コンフィギュレーション モードを開始します。ASA のグローバル コンフィギュレーション モードでは、表示されるプロンプトは **hostname(config)#** となります。

手順の詳細

	コマンド	目的
ステップ 1	**webvpn** **例：** hostname(config)# webvpn	webvpn コンフィギュレーション モードを開始します。
ステップ 2	**no csd enable** **例：** ASAName(webvpn)#**no csd enable**	アンインストールするホスト スキャン イメージをディセーブルにします。
ステップ 3	**no csd hostscan image** path **例：** hostname(webvpn)#no csd hostscan image disk0:/hostscan-3.6.0-k9.pkg hostname(webvpn)#no csd hostscan image disk0:/anyconnect-NGC-win-3.0.0327-k9.pkg	アンインストールするホスト スキャン イメージへのパスを指定します。スタンドアロンのホスト スキャン パッケージ、または AnyConnect Secure Mobility Client パッケージがホスト スキャン パッケージとして指定されている場合があります。
ステップ 4	write memory **例：** hostname(webvpn)# write memory	実行コンフィギュレーションをフラッシュ メモリに保存します。 新しいコンフィギュレーションがフラッシュ メモリに正常に保存されると、[OK] メッセージが表示されます。

グループ ポリシーへの AnyConnect フィーチャ モジュールの割り当て

次の手順で、AnyConnect フィーチャ モジュールとグループ ポリシーを関連付けます。VPN ユーザが ASA に接続するときに、ASA はこれらの AnyConnect フィーチャ モジュールをエンドポイント コンピュータにダウンロードしてインストールします。

前提条件

ASA にログオンし、グローバル コンフィギュレーション モードを開始します。グローバル コンフィギュレーション モードでは、ASA は **hostname(config)#** プロンプトを表示します。

手順の詳細

	コマンド	目的
ステップ 1	**group-policy** *name* **internal** **例：** hostname(config)# group-policy PostureModuleGroup internal	ネットワーク クライアント アクセス用の内部グループ ポリシーを追加します。
ステップ 2	**group-policy** *name* **attributes** **例：** hostname(config)# group-policy PostureModuleGroup attributes	新しいグループ ポリシーを編集します。このコマンドを入力した後は、グループ ポリシー コンフィギュレーション モードのプロンプト **hostname(config-group-policy)#** が表示されます。
ステップ 3	webvpn **例：** hostname(config-group-policy)# webvpn	グループ ポリシー webvpn コンフィギュレーション モードを開始します。このコマンドを入力した後は、次に示す ASA のプロンプトが表示されます。 hostname(config-group-webvpn)#

	コマンド	目的
ステップ 4	`hostname(config-group-webvpn)# anyconnect modules value AnyConnect Module Name` **例：** `hostname(config-group-webvpn)# anyconnect modules value websecurity,telemetry,posture`	グループ内のすべてのユーザに AnyConnect フィーチャ モジュールがダウンロードされるように、グループ ポリシーを設定します。anyconnect module コマンドの value には、次の値の 1 つ以上を指定することができます。複数のモジュールを指定する場合は、値をカンマで区切ります。 **value** **AnyConnect モジュール名** **dart** AnyConnect DART（診断およびレポート ツール） **nam** AnyConnect ネットワーク アクセス マネージャ **vpngina** AnyConnect SBL（Start Before Logon） **websecurity** AnyConnect Web Security モジュール **telemetry** AnyConnect テレメトリ モジュール **posture** AnyConnect ポスチャ モジュール **none** 単独で使用され、グループ ポリシーからすべての AnyConnect モジュールを削除します。 モジュールの 1 つを削除するには、保持したいモジュールの値だけを指定したコマンドを再送信します。たとえば、このコマンドは Web セキュリティ モジュールを**削除**します。 `hostname(config-group-webvpn)# anyconnect modules value telemetry,posture`
ステップ 5	`write memory` **例：** `hostname(config-group-webvpn)# write memory`	実行コンフィギュレーションをフラッシュ メモリに保存します。 新しいコンフィギュレーションが正常にフラッシュ メモリに保存されると、[OK] というメッセージが表示され、次に示す ASA のプロンプトが表示されます。 hostname(config-group-webvpn)#

ホスト スキャンに関するその他の重要なマニュアル

ホスト スキャンがエンドポイント コンピュータからポスチャ クレデンシャルを収集した後は、情報を活用するために、ユーザはプリログイン ポリシーの設定、ダイナミック アクセス ポリシーの設定、Lua の式の使用などのサブジェクトを理解する必要があります。

これらの内容については、次のマニュアルで詳しく説明します。

- 『Cisco Secure Desktop Configuration Guides』
- 『Cisco Adaptive Security Device Manager Configuration Guides』

また、AnyConnect クライアントでのホスト スキャンの動作の詳細については、『Cisco *AnyConnect Secure Mobility Client Administrator Guide, Release 3.0*』を参照してください。

認可および認証用の外部サーバ

この章では、ASA で AAA をサポートするための外部 LDAP、RADIUS、または TACACS+ サーバの設定方法について説明します。外部サーバを使用するように ASA を設定する前に、正しい ASA 認可属性で AAA サーバを設定し、それらの属性のサブセットから個々のユーザに対する個別の許可を割り当てる必要があります。

認可属性のポリシー実施の概要

ASA は、ユーザ認可属性（ユーザ権利またはユーザ権限とも呼ばれる）を VPN 接続に適用するためのいくつかの方法をサポートしています。ASA を設定して、次のいずれかの組み合わせからユーザ属性を取得できます。

- ASA のダイナミック アクセス ポリシー（DAP）
- 外部 RADIUS または LDAP 認証および許可サーバ（およびその両方）
- ASA のグループ ポリシー

ASA がすべてのソースから属性を受信すると、その属性が評価され、集約されてユーザ ポリシーに適用されます。属性の間で衝突がある場合、DAP 属性が優先されます。

ASA によって属性が適用される順序は次のとおりです（図 12-1 を参照）。

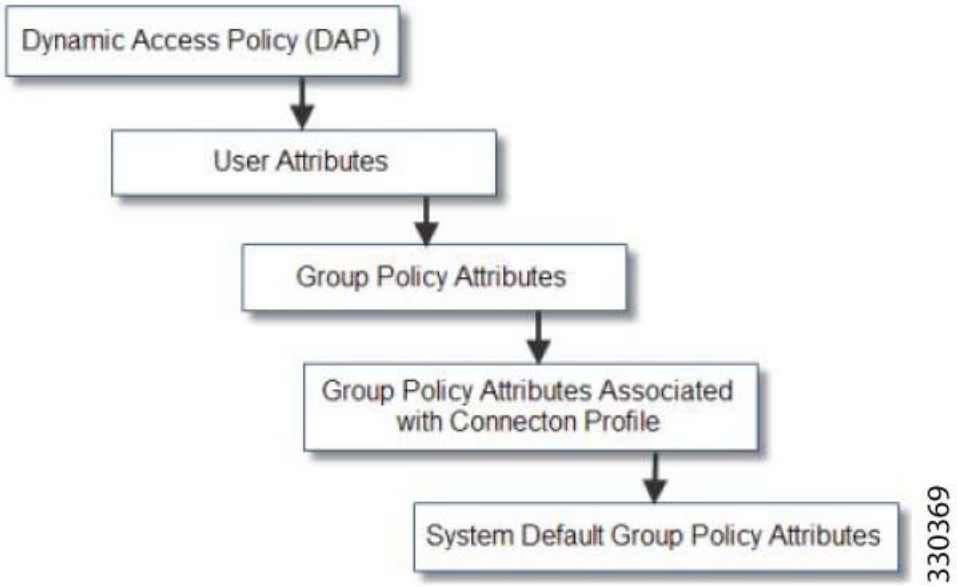
1. ASA 上の DAP 属性：バージョン 8.0(2) で導入されたこの属性は、他のすべての属性よりも優先されます。DAP 内でブックマークまたは URL リストを設定した場合は、グループ ポリシーで設定されているブックマークや URL リストよりも優先されます。
2. AAA サーバ上のユーザ属性：ユーザ認証や認可が成功すると、サーバからこの属性が返されます。これらの属性を、ASA のローカル AAA データベースの個々のユーザに設定されている属性（ASDM のユーザ アカウント）と混同しないでください。
3. ASA 上で設定されているグループ ポリシー：RADIUS サーバからユーザの RADIUS CLASS 属性 IETF-Class-25（OU=*group-policy*）の値が返された場合は、ASA はそのユーザを同じ名前のグループ ポリシーに入れて、そのグループ ポリシーの属性のうち、サーバから返されないものを適用します。

   LDAP サーバでは、任意の属性名を使用してセッションのグループ ポリシーを設定できます。ASA 上で設定されている LDAP 属性マップによって、LDAP 属性が Cisco 属性 IETF-Radius-Class にマッピングされます。

4. 接続プロファイル（CLI では「トンネル グループ」と呼ばれます）によって割り当てられたグループ ポリシー：接続プロファイルには、接続の事前設定が含まれているほか、認証前にユーザに適用されるデフォルトのグループ ポリシーが含まれています。ASA に接続するすべてのユーザは、最初にこのグループに所属します。このグループでは、DAP、サーバから返されるユーザ属性、またはユーザに割り当てられたグループ ポリシーにはない属性が定義されています。
5. ASA で割り当てられたデフォルトのグループ ポリシー（DfltGrpPolicy）：システムのデフォルト属性は、DAP、ユーザ属性、グループ ポリシー、または接続プロファイルで不 足している値を提供します。

ASA LDAP コンフィギュレーションの定義

図 12-1　　ポリシー実施フロー



認可では、権限または属性を使用するプロセスを参照します。認証または認可サーバとして定義されている LDAP サーバは、権限または属性（設定されている場合）を適用します。

ガイドライン

ASA は、数値の ID ではなく属性名に基づいて LDAP 属性を使用します。RADIUS 属性は、名前ではなく数値 ID によって適用されます。

ASDM バージョン 7.0 の LDAP 属性には、cVPN3000 プレフィックスが含まれています。ASDM バージョン 7.1 以降では、このプレフィックスは削除されています。

LDAP 属性は、RADIUS の章に記載されている RADIUS 属性のサブセットです。

Active Directory/LDAP VPN リモート アクセス認可の例

この項では、Microsoft Active Directory サーバを使用している ASA で認証および認可を設定するための手順の例を示します。説明する項目は次のとおりです。

その他の設定例については、Cisco.com にある次のテクニカル ノートを参照してください。

- 『*ASA/PIX: Mapping VPN Clients to VPN Group Policies Through LDAP Configuration Example*』
  http://www.cisco.com/en/US/products/ps6120/products_configuration_example09186a008089149d.shtml
- 『*PIX/ASA 8.0: Use LDAP Authentication to Assign a Group Policy at Login*』
  http://www.cisco.com/en/US/products/ps6120/products_configuration_example09186a00808d1a7c.shtml

ユーザベースの属性ポリシーの適用

すべての標準 LDAP 属性は、予約済みのベンダー固有属性（VSA）にマッピングできます。また、1 つ以上の LDAP 属性を 1 つ以上の Cisco LDAP 属性にマッピングできます。

次の例では、AD LDAP サーバで設定されたユーザに対し、簡単なバナーを適用するように ASA を設定します。サーバ上で [General] タブの [Office] フィールドを使用してバナー テキストを入力します。このフィールドでは、physicalDeliveryOfficeName という名前の属性を使用します。ASA で、physicalDeliveryOfficeName を Cisco 属性 Banner1 にマッピングする属性マップを作成します。認証の間に、ASA はサーバから physicalDeliveryOfficeName の値を取得し、その値を Cisco 属性 Banner1 にマッピングしてユーザにバナーを表示します。

この例は、IPsec VPN クライアント、AnyConnect SSL VPN クライアント、クライアントレス SSL VPN など、どの接続タイプにも適用されます。この例では、User1 はクライアントレス SSL VPN 接続を使用して接続します。

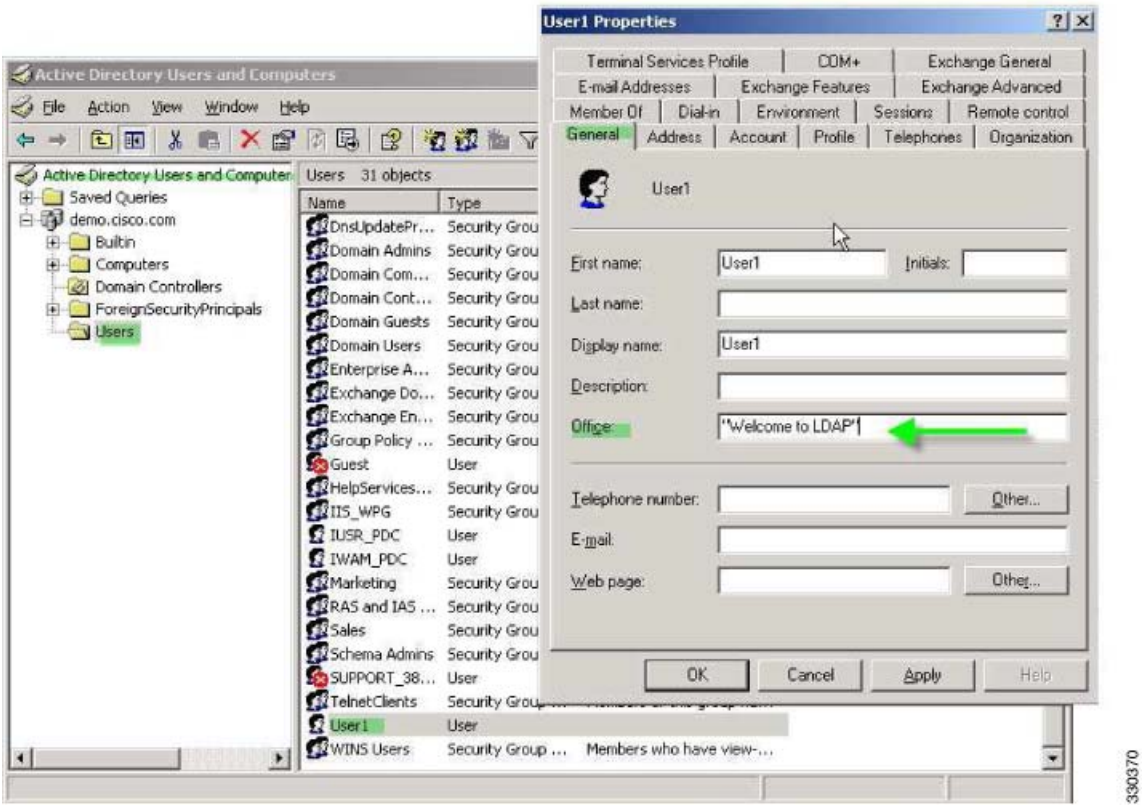
ユーザの属性を AD または LDAP サーバ上で設定するには、次の手順を実行します。

ステップ 1　ユーザを右クリックします。

[Properties] ダイアログボックスが表示されます（図 12-2 を参照）。

ステップ 2　**[General]** タブをクリックし、バナー テキストを [Office] フィールドに入力します。このフィールドでは、AD/LDAP 属性 physicalDeliveryOfficeName が使用されます。

図 12-2　　LDAP ユーザの設定



ステップ 3　ASA 上で LDAP 属性マップを作成します。

次の例では、Banner というマップを作成し、AD/LDAP 属性 physicalDeliveryOfficeName を Cisco 属性 Banner1 にマッピングします。

```
hostname(config)# ldap attribute-map Banner
hostname(config-ldap-attribute-map)# map-name physicalDeliveryOfficeName Banner1
```

ステップ 4　LDAP 属性マップを AAA サーバに関連付けます。

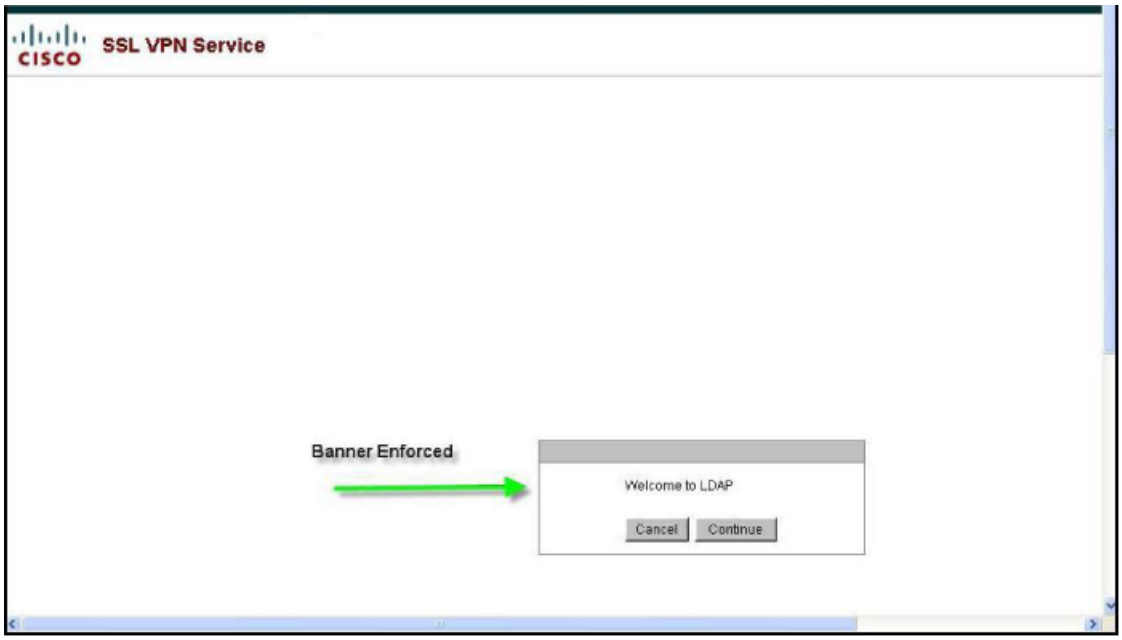
次の例では、AAA サーバ グループ MS_LDAP のホスト 10.1.1.2 の AAA サーバ ホスト コンフィギュレーション モードを開始し、ステップ 3 で作成した属性マップ Banner を関連付けます。

```
hostname(config)# aaa-server MS_LDAP host 10.1.1.2
hostname(config-aaa-server-host)# ldap-attribute-map Banner
```

ステップ 5　バナーの適用をテストします。

クライアントレス SSL 接続の例を次に示します。このバナーは、ユーザ認証後に属性マップ経由で適用されたものです（図 12-3 を参照）。

図 12-3　　表示されたバナー



特定のグループ ポリシーへの LDAP ユーザの配置

次に示す例では、AD LDAP サーバ上の User1 を ASA 上の特定のグループ ポリシーに対して認証する方法について説明します。サーバで、[Organization] タブの [Department] フィールドを使用して、グループ ポリシーの名前を入力します。次に、属性マップを作成し、Department を Cisco 属性である IETF-Radius-Class にマッピングします。認証の間に、ASA はサーバから Department の値を取得し、その値を IETF-Radius-Class にマッピングして User1 をグループ ポリシーに配置します。

この例は、IPsec VPN クライアント、AnyConnect SSL VPN クライアント、クライアントレス SSL VPN など、どの接続タイプにも適用されます。この例では、User1 はクライアントレス SSL VPN 接続経由で接続します。

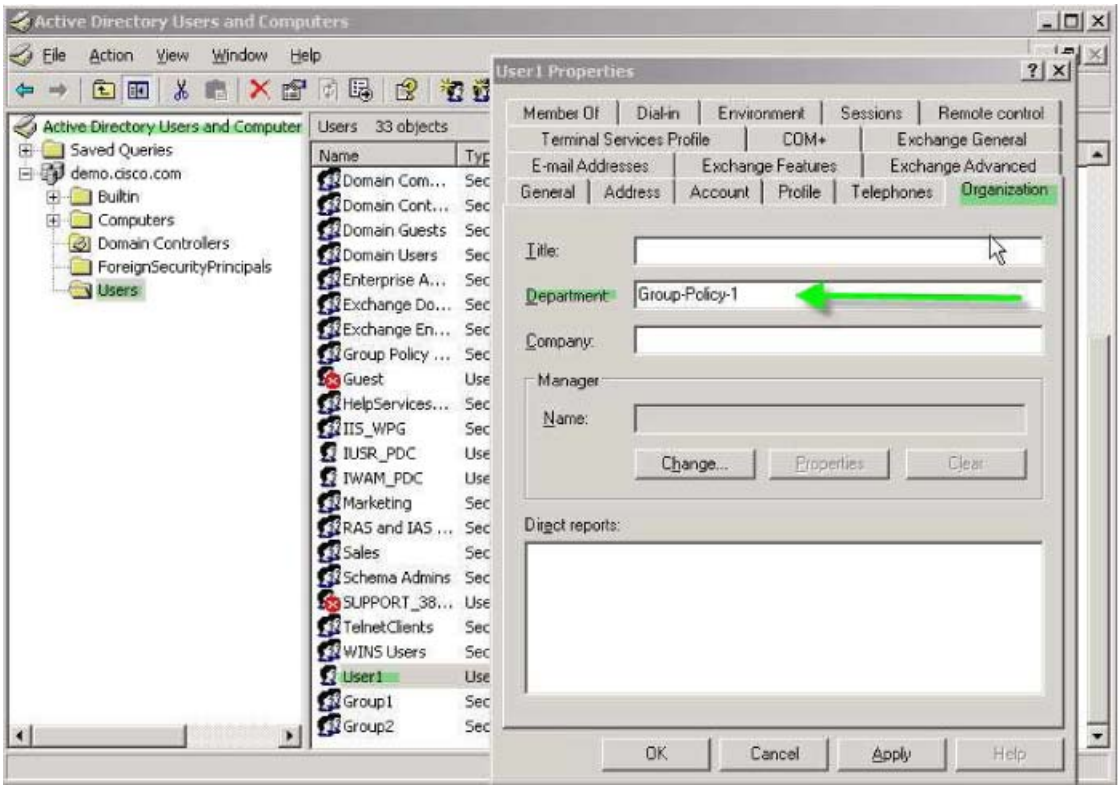
AD LDAP サーバ上のユーザの属性を設定するには、次の手順を実行します。

ステップ 1　ユーザを右クリックします。

[Properties] ダイアログボックスが表示されます（図 12-4 を参照）。

ステップ 2　**[Organization]** タブをクリックして、[Department] フィールドに **Group-Policy-1** と入力します。

図 12-4　　AD/LDAP の [Department] 属性



ステップ 3　ステップ 1 に示した LDAP コンフィギュレーションの属性マップを定義します。

次の例では、AD 属性 Department を Cisco 属性 IETF-Radius-Class にマッピングする方法について説明します。

```
hostname(config)# ldap attribute-map group_policy
hostname(config-ldap-attribute-map)# map-name Department IETF-Radius-Class
```

ステップ 4　LDAP 属性マップを AAA サーバに関連付けます。

次の例では、AAA サーバ グループ MS_LDAP のホスト 10.1.1.2 の AAA サーバ ホスト コンフィギュレーション モードを開始し、ステップ 3 で作成した属性マップ group_policy を関連付けます。

```
hostname(config)# aaa-server MS_LDAP host 10.1.1.2
hostname(config-aaa-server-host)# ldap-attribute-map group_policy
```

ステップ 5　ASA で新しい group-policy を追加し、ユーザに割り当てるために必要なポリシー属性を設定します。次の例では、Group-policy-1 を作成します。この名前は、サーバで [Department] フィールドに入力したものです。

```
hostname(config)# group-policy Group-policy-1 external server-group LDAP_demo
hostname(config-aaa-server-group)#
```

ステップ 6　このユーザとして VPN 接続を確立し、Group-Policy1 からの属性（およびその他に適用可能な、デフォルトのグループ ポリシーからの属性）がセッションに継承されていることを確認します。

ステップ 7　ASA とサーバの間の通信をモニタするには、特権 EXEC モードで **debug ldap 255** コマンドをイネーブルにします。このコマンドからの出力の例を次に示します。これは、主要なメッセージがわかるように編集済みです。

```
[29] Authentication successful for user1 to 10.1.1.2
[29] Retrieving user attributes from server 10.1.1.2
[29] Retrieved Attributes:
[29] department: value = Group-Policy-1
[29] mapped to IETF-Radius-Class: value = Group-Policy-1
```

AnyConnect トンネルへのスタティック IP アドレスの割り当て

この例では、AnyConnect クライアント ユーザ Web1 を、特定のスタティック IP アドレスを受信するように設定します。そのアドレスを、AD LDAP サーバで [Dialin] タブの [Assign Static IP Address] フィールドに入力します。このフィールドでは、msRADIUSFramedIPAddress 属性を使用します。この属性を Cisco 属性 IETF-Radius-Framed-IP-Address にマッピングする属性マップを作成します。

認証時に、ASA は msRADIUSFramedIPAddress の値をサーバから取得し、その値を Cisco 属性 IETF-Radius-Framed-IP-Address にマッピングし、スタティック アドレスを User1 に渡します。

次の例が当てはまるのは、フルトンネル クライアント、つまり IPsec クライアントや SSL VPN クライアント（AnyConnect クライアント 2.x および SSL VPN クライアント）などです。

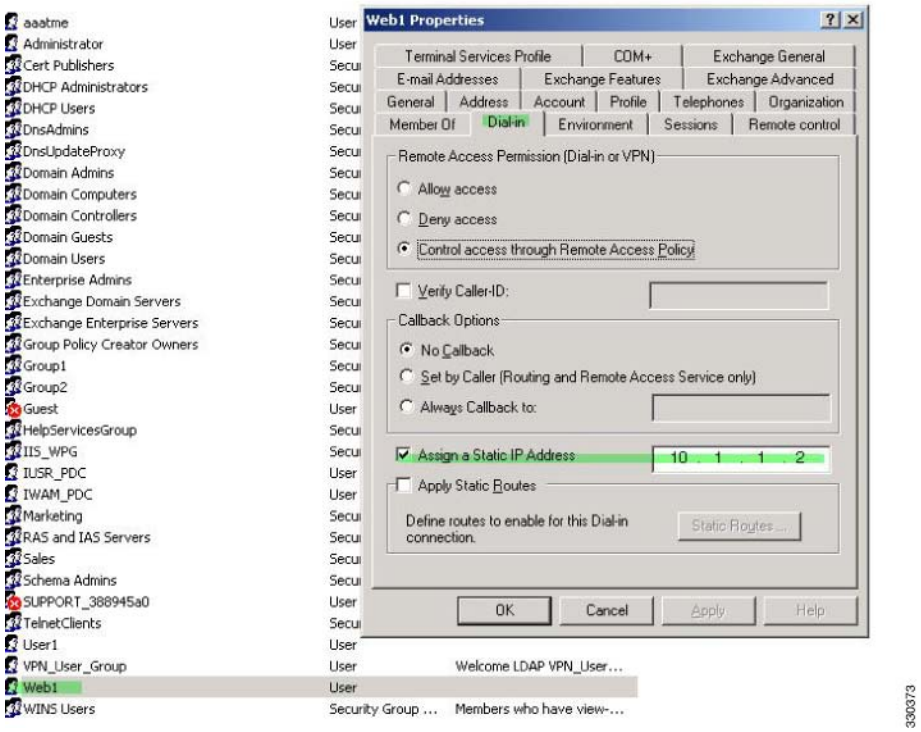
AD/LDAP サーバ上でユーザ属性を設定するには、次の手順を実行します。

ステップ 1　ユーザ名を右クリックします。

[Properties] ダイアログボックスが表示されます（図 12-5 を参照）。

ステップ 2　**[Dialin]** タブをクリックし、**[Assign Static IP Address]** チェックボックスをオンにして、IP アドレス 10.1.1.2 を入力します。

図 12-5　　スタティック IP アドレスの割り当て



ステップ 3　ステップ 1 に示した LDAP コンフィギュレーションの属性マップを作成します。

次の例では、スタティック アドレス フィールドで使用されている AD 属性 msRADIUSFramedIPAddress を Cisco 属性 IETF-Radius-Framed-IP-Address にマッピングする方法を示します。

```
hostname(config)# ldap attribute-map static_address
hostname(config-ldap-attribute-map)# map-name msRADIUSFramedIPAddress
IETF-Radius-Framed-IP-Address
```

ステップ 4　LDAP 属性マップを AAA サーバに関連付けます。

次の例では、AAA サーバ グループ MS_LDAP のホスト 10.1.1.2 の AAA サーバ ホスト コンフィギュレーション モードを開始し、ステップ 3 で作成した属性マップ static_address を関連付けます。

```
hostname(config)# aaa-server MS_LDAP host 10.1.1.2
hostname(config-aaa-server-host)# ldap-attribute-map static_address
```

ステップ 5　**vpn-address-assignment** コマンドが AAA を指定するように設定されているかどうかを確認するために、コンフィギュレーションのこの部分を **show run all vpn-addr-assign** コマンドで表示します。

```
hostname(config)# show run all vpn-addr-assign
vpn-addr-assign aaa    << この部分が設定されていることを確認します >>
no vpn-addr-assign dhcp
vpn-addr-assign local
hostname(config)#
```

ステップ 6　ASA と AnyConnect クライアントとの接続を確立します。次のことを確認します。

- バナーがクライアントレス接続と同じシーケンスで受信されている（図 12-6 を参照）。
- サーバ上で設定されて ASA にマッピングされた IP アドレスをユーザが受信している（図 12-7 を参照）。

図 12-6　　AnyConnect セッションのバナーの確認

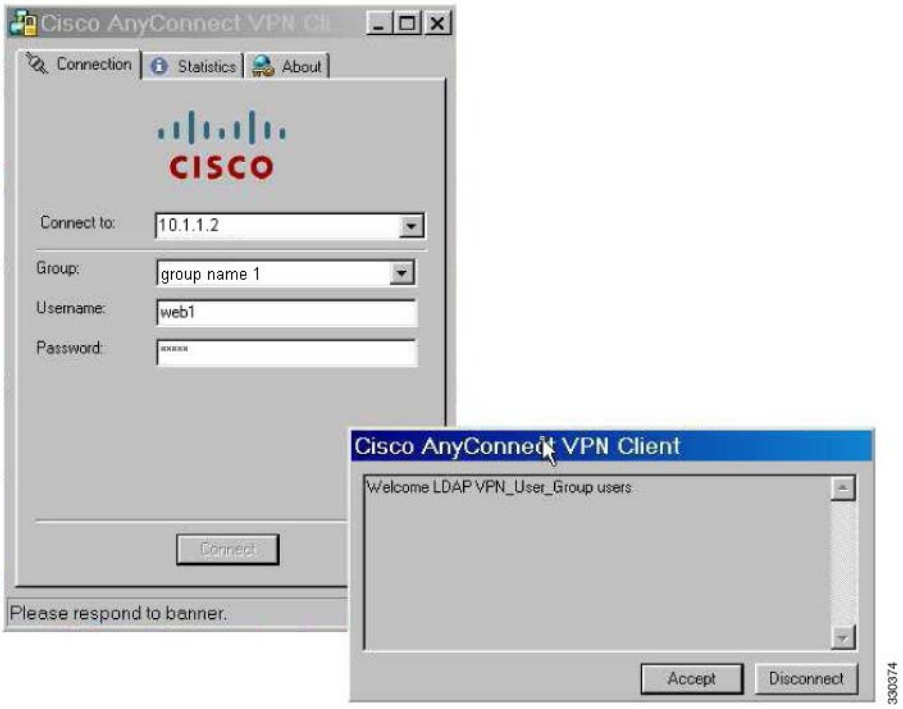


図 12-7　　確立された AnyConnect セッション

ステップ 7　**show vpn-sessiondb svc** コマンドを使用してセッションの詳細を表示し、割り当てられたアドレスを確認します。

```
hostname# show vpn-sessiondb svc

Session Type: SVC
Username     : web1                   Index        : 31
Assigned IP  : 10.1.1.2              Public IP    : 10.86.181.70
Protocol     : Clientless SSL-Tunnel DTLS-Tunnel
Encryption   : RC4 AES128             Hashing      : SHA1
Bytes Tx     : 304140                 Bytes Rx     : 470506
Group Policy : VPN_User_Group         Tunnel Group : Group1_TunnelGroup
Login Time   : 11:13:05 UTC Tue Aug 28 2007
Duration     : 0h:01m:48s
NAC Result   : Unknown
VLAN Mapping : N/A                    VLAN         : none
```

ダイヤルインの許可または拒否アクセスの適用

次の例では LDAP 属性マップを作成し、ユーザによって許可されるトンネリング プロトコルを指定します。[Dialin] タブでの許可アクセスと拒否アクセスの設定を、Cisco 属性 Tunneling-Protocol にマッピングします。この属性では、表 12-1 に示すビットマップ値がサポートされます。

表 12-1　Cisco Tunneling-Protocol 属性のビットマップ値

値	トンネリング プロトコル
1	PPTP
2	L2TP
4[1]	IPsec（IKEv1）
8[2]	L2TP/IPsec
16	クライアントレス SSL
32	SSL クライアント：AnyConnect または SSL VPN クライアント
64	IPsec（IKEv2）

1. IPsec と L2TP over IPsec は同時にはサポートされません。そのため、値 4 と 8 は相互排他値となります。
2. 注 1 を参照してください。

この属性を使用して、プロトコルの [Allow Access]（TRUE）または [Deny Access]（FALSE）の条件を作成し、ユーザがアクセスを許可される方法を適用します。

この単純化した例では、トンネル プロトコル IPsec/IKEv1（4）をマッピングすることによって、Cisco VPN Client の許可（true）条件を作成できます。また、WebVPN（16）と SVC/AC（32）を値 48（16+32）としてマッピングし、拒否（false）条件を作成します。これで、ユーザは ASA に IPsec を使用して接続できるようになりますが、クライアントレス SSL または AnyConnect クライアントを使用して接続しようとすると拒否されます。

ダイヤルイン許可アクセスまたは拒否アクセスを適用する別の例については、次の URL にあるテクニカル ノート『*ASA/PIX: Mapping VPN Clients to VPN Group Policies Through LDAP Configuration Example*』を参照してください。

http://www.cisco.com/en/US/products/ps6120/products_configuration_example09186a008089149d.shtml

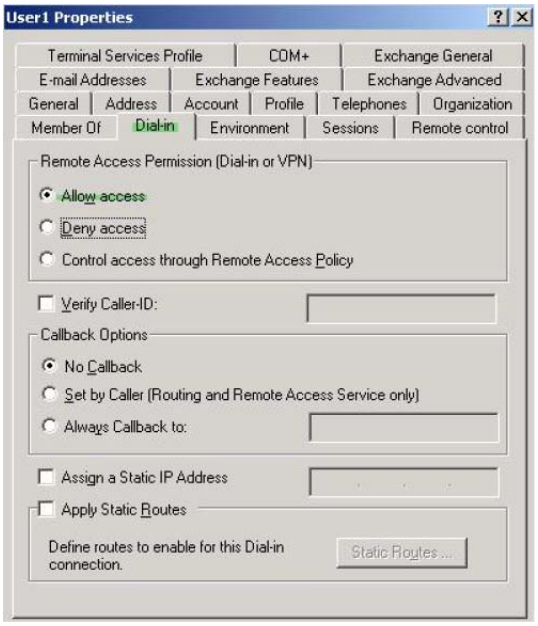
AD/LDAP サーバ上のユーザに属性を設定するには、次の手順を実行します。

ステップ 1　ユーザを右クリックします。

[Properties] ダイアログボックスが表示されます。

ステップ 2　**[Dial-in]** タブをクリックしてから、**[Allow Access]** オプション ボタンをクリックします（図 12-8）。

図 12-8　　AD/LDAP User1 - 許可アクセス



（注）　[Control access through the Remote Access Policy] オプションを選択した場合は、値はサーバから返されず、適用される権限は ASA の内部グループ ポリシー設定に基づいて決定されます。

ステップ 3　IPsec と AnyConnect の両方の接続を許可するがクライアントレス SSL 接続を拒否する属性マップを作成します。

この例では、初めに tunneling_protocols というマップを作成します。次に、[Allow Access] 設定で使用される AD 属性 msNPAllowDialin を、**map-name** コマンドを使用して Cisco 属性 Tunneling-Protocols にマッピングします。次に、マップ値を **map-value** コマンドで追加します。

```
hostname(config)# ldap attribute-map tunneling_protocols
hostname(config-ldap-attribute-map)# map-name msNPAllowDialin Tunneling-Protocols
hostname(config-ldap-attribute-map)# map-value msNPAllowDialin FALSE 48
hostname(config-ldap-attribute-map)# map-value msNPAllowDialin TRUE 4
```

ステップ 4　LDAP 属性マップを AAA サーバに関連付けます。

次の例では、AAA サーバ グループ MS_LDAP のホスト 10.1.1.2 の AAA サーバ ホスト コンフィギュレーション モードを開始し、ステップ 2 で作成した属性マップ tunneling_protocols を関連付けます。

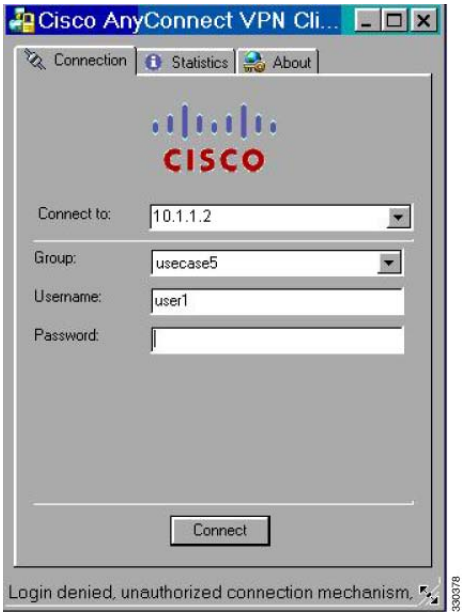
```
hostname(config)# aaa-server MS_LDAP host 10.1.1.2
hostname(config-aaa-server-host)# ldap-attribute-map tunneling_protocols
```

ステップ 5　属性マップが設定したとおりに機能することを確認します。

ステップ 6　クライアントレス SSL、AnyConnect クライアント、および IPsec クライアントを使用して接続を試みます。クライアントレス SSL と AnyConnect では接続に失敗し、その原因が認可されていない接続メカニズムにあることを示すメッセージが表示されます。IPsec クライアントの接続は成功します。IPsec は、属性マップに従って許可されるトンネリング プロトコルであるためです（図 12-9 および図 12-10 を参照）。

図 12-9　クライアントレス ユーザへのログイン拒否メッセージ

図 12-10　AnyConnect クライアント ユーザへのログイン拒否メッセージ



ログイン時間と Time-of-Day ルールの適用

次の例では、クライアントレス SSL ユーザ（たとえばビジネス パートナー）にネットワークへのアクセスを許可する時間帯を設定して適用する方法を示します。

AD サーバ上で、[Office] フィールドを使用してパートナーの名前を入力します。このフィールドでは、physicalDeliveryOfficeName 属性が使用されます。次に、ASA で属性マップを作成し、その属性を Cisco 属性 Access-Hours にマッピングします。認証時に、ASA はサーバから physicalDeliveryOfficeName の値を取得して Access-Hours にマッピングします。

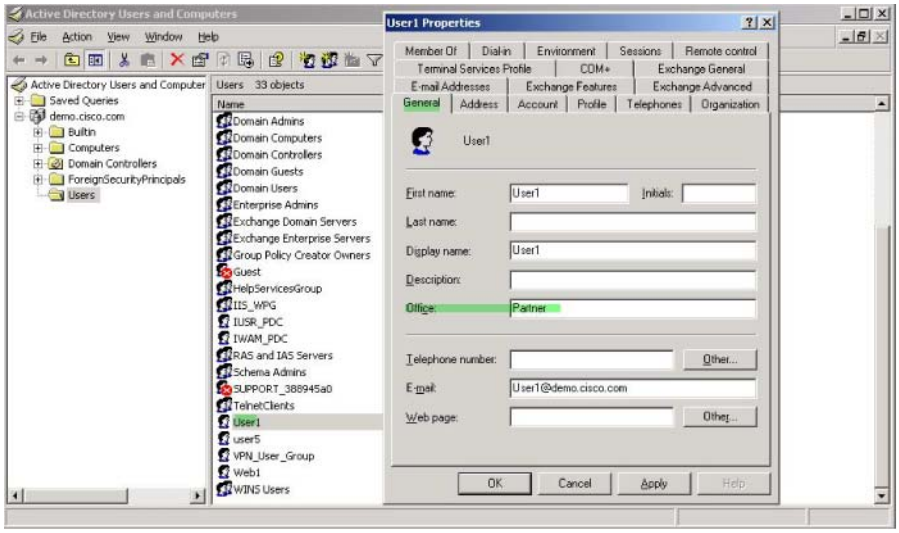
AD/LDAP サーバ上でユーザ属性を設定するには、次の手順を実行します。

ステップ 1　ユーザを選択して **[Properties]** を右クリックします。

[Properties] ダイアログボックスが表示されます（図 12-11 を参照）。

ステップ 2　**[General]** タブをクリックします。

図 12-11　Active Directory [Properties] ダイアログボックス



ステップ 3　属性マップを作成します。

次の例では、属性マップ access_hours を作成して AD 属性 physicalDeliveryOfficeName（[Office] フィールドで使用）を Cisco 属性 Access-Hours にマッピングする方法を示します。

```
hostname(config)# ldap attribute-map access_hours
hostname(config-ldap-attribute-map)# map-name physicalDeliveryOfficeName Access-Hours
```

ステップ 4　LDAP 属性マップを AAA サーバに関連付けます。

次の例では、AAA サーバ グループ MS_LDAP のホスト 10.1.1.2 の AAA サーバ ホスト コンフィギュレーション モードを開始し、ステップ 3 で作成した属性マップ access_hours を関連付けます。

```
hostname(config)# aaa-server MS_LDAP host 10.1.1.2
hostname(config-aaa-server-host)# ldap-attribute-map access_hours
```

ステップ 5　各値にサーバで許可された時間範囲を設定します。

次の例では、Partner のアクセス時間が月曜日から金曜日の午前 9 時から午後 5 時に設定されています。

```
hostname(config)# time-range Partner
hostname(config-time-range)# periodic weekdays 09:00 to 17:00
```

VPN のための LDAP での許可の設定

VPN アクセスのための LDAP 認証が成功すると、ASA は、LDAP 属性を返す LDAP サーバのクエリーを実行します。通常これらの属性には、VPN セッションに適用される認可データが含まれます。

この許可メカニズムとは別の異なる許可を LDAP ディレクトリ サーバから取得することが必要な場合があります。たとえば、認証に SDI または証明書サーバを使用している場合、認可情報は返されません。この場合、ユーザ認可では、認証の成功後に LDAP ディレクトリのクエリーを実行するため、認証と認可は 2 つのステップで行われます。

LDAP を使用した VPN ユーザ許可を設定するには、次の手順を実行します。

手順の詳細

	コマンド	目的
ステップ 1	**aaa-server** *server_group* **protocol {kerberos | ldap | nt | radius | sdi | tacacs+}** **例：** `hostname(config)# aaa-server servergroup1 protocol ldap` `hostname(config-aaa-server-group)`	AAA サーバ グループを作成します。
ステップ 2	**tunnel-group** *groupname* **例：** `hostname(config)# tunnel-group remotegrp`	「remotegrp」という名前の IPsec リモート アクセス トンネル グループを作成します。
ステップ 3	**tunnel-group** *groupname* **general-attributes** **例：** `hostname(config)# tunnel-group remotegrp general-attributes`	サーバ グループとトンネル グループを関連付けます。
ステップ 4	**authorization-server-group** *group-tag* **例：** `hostname(config-general)# authorization-server-group ldap_dir_1`	以前作成した認証のための AAA サーバ グループに新しいトンネル グループを割り当てます。

例

特定の要件で使用できる許可関連のコマンドとオプションは他にもありますが、次の例では、LDAP でのユーザ許可をイネーブルにするコマンドを示します。この例では、remote-1 という名前の IPsec リモート アクセス トンネル グループを作成し、すでに作成してある許可用の ldap_dir_1 AAA サーバ グループにその新しいトンネル グループを割り当てています。

```
hostname(config)# tunnel-group remote-1 type ipsec-ra
hostname(config)# tunnel-group remote-1 general-attributes
hostname(config-general)# authorization-server-group ldap_dir_1
hostname(config-general)#
```

この設定が完了したら、次のコマンドを入力して、ディレクトリ パスワード、ディレクトリ検索の開始点、ディレクトリ検索の範囲など、追加の LDAP 許可パラメータを設定できます。

```
hostname(config)# aaa-server ldap_dir_1 protocol ldap
hostname(config-aaa-server-group)# aaa-server ldap_dir_1 host 10.1.1.4
hostname(config-aaa-server-host)# ldap-login-dn obscurepassword
hostname(config-aaa-server-host)# ldap-base-dn starthere
hostname(config-aaa-server-host)# ldap-scope subtree
hostname(config-aaa-server-host)#
```

PART 2

クライアントレス SSL VPN

CHAPTER 13

クライアントレス SSL VPN の概要

2014 年 4 月 14 日

クライアントレス SSL VPN の概要

クライアントレス SSL VPN を使用すると、エンド ユーザは SSL 対応 Web ブラウザを使用して、任意の場所から社内ネットワークのリソースに安全にアクセスできます。ユーザは、まず、クライアントレス SSL VPN ゲートウェイで認証し、事前設定されたネットワーク リソースにアクセスできるようにします。

（注） クライアントレス SSL VPN がイネーブルになっている場合、セキュリティ コンテキスト（ファイアウォール マルチモードとも呼ばれる）とアクティブ/アクティブステートフル フェールオーバーはサポートされません。

クライアントレス SSL VPN は、ソフトウェアまたはハードウェア クライアントを必要とせずに、Web ブラウザを使用して ASA へのセキュアなリモート アクセス VPN トンネルを作成します。HTTP 経由でインターネットに接続できるほとんどのデバイスから、幅広い Web リソースと、Web 対応およびレガシー アプリケーションに安全かつ簡単にアクセスできます。具体的には以下のとおりです。

- 内部 Web サイト
- Web 対応アプリケーション
- NT/Active Directory ファイル共有
- 電子メール プロキシ（POP3S、IMAP4S、SMTPS など）
- Microsoft Outlook Web Access Exchange Server 2000、2003、および 2007
- Microsoft Web App to Exchange Server 2010（8.4(2) 以降において）
- Application Access（他の TCP ベースのアプリケーションにアクセスするためのスマート トンネルまたはポート転送）

クライアントレス SSL VPN は Secure Sockets Layer（SSL）プロトコルおよびその後継の Transport Layer Security（SSL/TLS1）を使用して、リモート ユーザと、内部サイトで設定した特定のサポートされている内部リソースとの間で、セキュアな接続を提供します。ASA はプロキシで処理する必要がある接続を認識し、HTTP サーバは認証サブシステムと対話してユーザを認証します。

ネットワーク管理者は、クライアントレス SSL VPN セッションのユーザに対してグループ単位でリソースへのアクセスを提供します。ユーザは、内部ネットワーク上のリソースに直接アクセスすることはできません。

前提条件

ASA Release 9.0 でサポートされているプラットフォームおよびブラウザについては、『*Supported VPN Platforms, Cisco ASA Series*』を参照してください。

ガイドラインと制限事項

- ActiveX ページでは、ActiveX リレーをイネーブルにするか、関連するグループ ポリシーに **activex-relay** を入力しておくことが必要です。あるいは、スマート トンネル リストをポリシーに割り当て、エンドポイント上のブラウザ プロキシ例外リストでプロキシが指定されるようにしておきます。ユーザはそのリストに「shutdown.webvpn.relay.」エントリを追加する必要があります。
- ASA では、Windows 7、Vista、Internet Explorer 8 ～ 10、Mac OS X、および Linux から Windows 共有（CIFS）Web フォルダへのクライアントレス アクセスはサポートされていません。
- DoD Common Access Card および SmartCard を含む証明書認証は、Safari キーチェーンだけで動作します。
- ASA は、クライアントレス SSL VPN 接続では DSA または RSA 証明書をサポートしていません。
- 一部のドメインベースのセキュリティ製品には、ASA から送信された要求を超える要件があります。
- コンフィギュレーション制御の検査機能およびモジュラ ポリシー フレームワークにおけるその他の検査機能はサポートされません。
- グループ ポリシーの *vpn-filter* コマンドは、クライアント ベースのアクセス用であり、サポートされません。グループ ポリシーのクライアントレス SSL VPN モードの *フィルタ*は、クライアントレス ベースのアクセス用です。
- NAT および PAT はクライアントに適用可能ではありません。
- ASA は、**police** や **priority-queue** などの QoS レート制限コマンドの使用をサポートしません。
- ASA は、接続制限値の使用、スタティックまたはモジュラ ポリシー フレームワークの **set connection** コマンドを使用した確認をサポートしません。
- クライアントレス SSL VPN のコンポーネントの一部には、Java ランタイム環境（JRE）が必要です。Mac OS X v10.7 以降では Java はデフォルトではインストールされていません。Mac OS X で Java をインストールする方法については、http://java.com/en/download/faq/java_mac.xml を参照してください。

クライアントレス ポータル用に設定された複数のグループ ポリシーがある場合は、ログイン ページのドロップダウンに表示されます。リストにある最初のグループ ポリシーで証明書が必要な場合は、ユーザはマッチング証明書が必要です。グループ ポリシーの一部が証明書を使用しない場合、非証明書ポリシーを最初に表示するには、リストを設定します。また、「0-Select-a-group」の名前でダミー グループ ポリシーを作成することもできます。

ヒント　グループ ポリシーの名前をアルファベット順に付けることで、最初に表示されるポリシーを制御できます。また、ポリシーの先頭に数字を付けることもできます。たとえば、1-AAA、2-Certificate とします。

基本的なクライアントレス SSL VPN のコンフィギュレーション

改訂日：2014 年 3 月 12 日

クライアントレス SSL VPN セキュリティ対策

デフォルトでは、ASA はすべての Web リソース（HTTPS、CIFS、RDP、プラグインなど）に対するすべてのポータル トラフィックを許可します。クライアントレス SSL VPN は、ASA だけに意味のあるものに各 URL をリライトします。ユーザは、要求した Web サイトに接続されていることを確認するために、この URL を使用できません。フィッシング Web サイトからの危険にユーザがさらされるのを防ぐには、クライアントレス アクセスに設定しているポリシー（グループ ポリシー、ダイナミック アクセス ポリシー、またはその両方）に Web ACL を割り当ててポータルからのトラフィック フローを制御します。これらのポリシーの URL エントリをオフに切り替えて、何にアクセスできるかについてユーザが混乱しないようにすることをお勧めします。

図 14-1　　ユーザが入力した URL の例

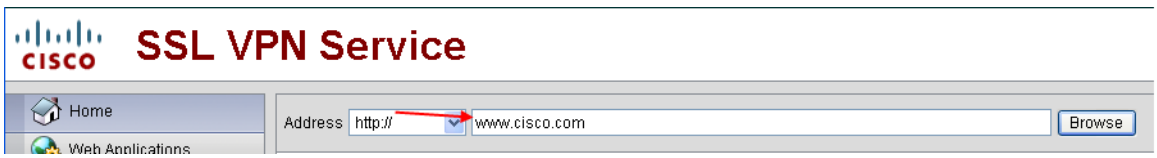
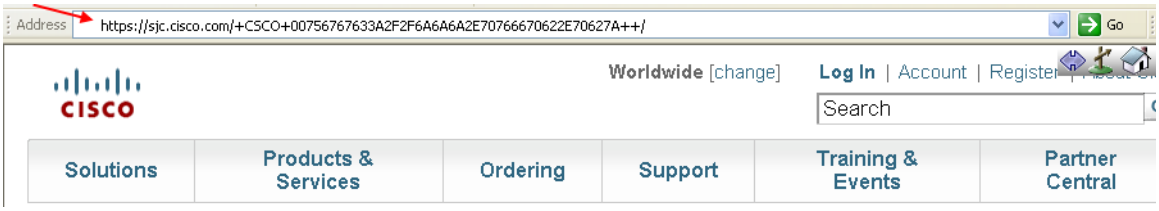


図 14-2　セキュリティ アプライアンスによって書き換えられ、ブラウザ ウィンドウに表示された同じ URL



ポータル ページでの URL エントリのオフへの切り替え

ユーザがブラウザ ベースの接続を確立したときにポータル ページが開きます。

前提条件

クライアントレス SSL VPN アクセスを必要とするすべてのユーザのグループ ポリシーを設定し、そのグループ ポリシーに対してだけクライアントレス SSL VPN をイネーブルにします。

手順の詳細

	コマンド	目的
ステップ 1	`webvpn`	グループ ポリシーのクライアントレス SSL VPN コンフィギュレーション モードに切り替えます。
ステップ 2	`url-entry`	ユーザが HTTP/HTTPS URL を入力する機能を制御します。
ステップ 3	（オプション）`url-entry disable`	URL エントリをオフに切り替えます。

クライアントレス SSL VPN サーバ証明書の確認

クライアントレス SSL VPN 経由でリモート SSL 対応サーバに接続する場合は、リモート サーバを信頼できること、また、接続先が実際にサーバであることを認識することが重要です。ASA 9.0 には、クライアントレス SSL VPN の信頼できる認証局（CA）証明書のリストに対する SSL サーバ証明書の検証のためのサポートが追加されています。

HTTPS プロトコルを使用して Web ブラウザ経由でリモート サーバに接続する場合、サーバはサーバ自体を識別するために認証局（CA）が署名したデジタル証明書を提供します。Web ブラウザには、サーバ証明書の有効性を検証するために使用される一連の CA 証明書が含まれています。これは、公開キー インフラストラクチャ（PKI）の 1 つの形式です。

ASA は信頼できるプール証明書の管理機能を trustpool の形式で提供します。これは、複数の既知の CA 証明書を表すトラストポイントの特殊なケースと見なすことができます。ASA には Web ブラウザに備わっているものと同様のデフォルトの一連の証明書が含まれています。**`crypto ca import default`** コマンドを発行して、管理者が実行するまでは動作しません。

（注）　ASA trustpool は Cisco IOS trustpool と似ていますが、同じではありません。

プラグインへのブラウザ アクセスの設定

次の項では、クライアントレス SSL VPN のブラウザ アクセス用のブラウザ プラグインの統合について説明します。

ブラウザ プラグインは、Web ブラウザによって呼び出される独立したプログラムで、ブラウザ ウィンドウ内でクライアントをサーバに接続するなどの専用の機能を実行します。ASA により、クライアントレス SSL VPN セッションでリモート ブラウザにダウンロードするためのプラグインをインポートできます。通常、シスコでは再配布するプラグインのテストを行っており、再配布できないプラグインの接続性をテストする場合もあります。ただし、現時点では、ストリーミング メディアをサポートするプラグインのインポートは推奨しません。

プラグインをフラッシュ デバイスにインストールすると、ASA は次の処理を実行します。

- （シスコが配布したプラグインのみ）URL で指定した jar ファイルを解凍する。
- ASA ファイル システムにファイルを書き込む。
- ASDM の URL 属性の横にあるドロップダウン リストに情報を入力します。
- 以後のすべてのクライアントレス SSL VPN セッションでプラグインをイネーブルにし、メイン メニュー オプションと、ポータル ページの [Address] フィールドの横にあるドロップダウン リストについてのオプションを追加します。

表 14-1 に、次の項で説明するプラグインを追加したときの、ポータル ページのメイン メニューと [Address] フィールドの変更点を示します。

表 14-1　　クライアントレス SSL VPN ポータル ページへのプラグインの影響

プラグイン	ポータル ページに追加されるメイン メニュー オプション	ポータル ページに追加される [Address] フィールド オプション
ica	Citrix MetaFrame Services	ica://
rdp	Terminal Servers	rdp://
rdp2*	Terminal Servers Vista	rdp2://
ssh,telnet	Secure Shell	ssh://
	Telnet services（v1 および v2 をサポート）	telnet://
vnc	Virtual Network Computing services	vnc://

* 推奨されないプラグイン。

クライアントレス SSL VPN セッションでユーザがポータル ページの関連付けられたメニュー オプションをクリックすると、ポータル ページにはインターフェイスへのウィンドウとヘルプ ペインが表示されます。ドロップダウン リストに表示されたプロトコルをユーザが選択して [Address] フィールドに URL を入力すると、接続を確立できます。

プラグインは、シングル サインオン（SSO）をサポートします。実装の詳細については、「HTTP Form プロトコルを使用した SSO の設定」（P.18-12）を参照してください。

前提条件

- プラグインへのリモート アクセスを提供するには、ASA でクライアントレス SSL VPN をイネーブルにする必要があります。
- プラグインに対して SSO サポートを設定するには、プラグインをインストールし、サーバへのリンクを表示するためのブックマーク エントリを追加します。また、ブックマークを追加するときに、SSO サポートを指定します。
- リモートで使用するために必要な最低限のアクセス権は、ゲスト特権モードに属しています。
- プラグインには、ActiveX または Oracle Java ランタイム環境（JRE）が必要です。バージョン要件については、「compatibility matrix」を参照してください。

制限

（注） Remote Desktop Protocol プラグインでは、セッション ブローカを使用したロード バランシングはサポートされていません。プロトコルによるセッション ブローカからのリダイレクションの処理方法のため、接続に失敗します。セッション ブローカが使用されていない場合、プラグインは動作します。

- プラグインは、シングル サインオン（SSO）をサポートします。プラグインは、クライアントレス SSL VPN セッションを開くときに入力したクレデンシャルと*同じ*クレデンシャルを使用します。プラグインはマクロ置換をサポートしないため、内部ドメイン パスワードなどのさまざまなフィールドや、RADIUS または LDAP サーバの属性で SSO を実行するオプションはありません。
- ステートフル フェールオーバーが発生すると、プラグインを使用して確立されたセッションは保持されません。ユーザはフェールオーバー後に再接続する必要があります。
- ステートフル フェールオーバーではなくステートレス フェールオーバーを使用する場合は、ブックマーク、カスタマイゼーション、ダイナミック アクセス ポリシーなどのクライアントレス機能はフェールオーバー ASA ペア間で同期されません。フェールオーバーの発生時に、これらの機能は動作しません。

プラグインのためのセキュリティ アプライアンスの準備

プラグインをインストールする前に、ASA で次のような準備を行います。

前提条件

クライアントレス SSL VPN が ASA インターフェイスでイネーブルになっていることを確認します。

制限

SSL 証明書の一般名（CN）として IP アドレスを指定しないでください。リモート ユーザは、ASA と通信するために FQDN の使用を試行します。リモート PC は、DNS または System32\drivers\etc\hosts ファイル内のエントリを使用して、FQDN を解決できる必要があります。

手順の詳細

	コマンド	目的
ステップ 1	`show running-config`	クライアントレス SSL VPN が ASA でイネーブルかどうかを示します。
ステップ 2	ASA インターフェイスに SSL 証明書をインストールします。	リモート ユーザ接続の完全修飾ドメイン名（FQDN）を指定します。

クライアントレス SSL VPN アクセスに提供するプラグインのタイプを指定する項に進んでください。

- 「シスコによって再配布されたプラグインのインストール」（P.14-5）
- 「Citrix XenApp Server へのアクセスの提供」（P.14-7）

シスコによって再配布されたプラグインのインストール

シスコでは、Java ベースのオープン ソース コンポーネントを再配布しています。これは、クライアントレス SSL VPN セッションで Web ブラウザのプラグインとしてアクセスされるコンポーネントで、次のものがあります。

前提条件

ASA のインターフェイス上でクライアントレス SSL VPN がイネーブルになっていることを確認します。そのためには、**show running-config** コマンドを入力します。

表 14-2　　シスコが再配布しているプラグイン

プロトコル	説明	再配布しているプラグインのソース *
RDP	Windows Vista および Windows 2003 R2 でホストされる Microsoft Terminal Services にアクセスします。 リモート デスクトップ ActiveX コントロールをサポートします。 RDP および RDP2 の両方をサポートするこのプラグインを使用することをお勧めします。RDP および RDP2 の 5.1 までのバージョンのみがサポートされています。バージョン 5.2 以降はサポートされていません。	http://properjavardp.sourceforge.net/
RDP2	Windows Vista および Windows 2003 R2 でホストされる Microsoft Terminal Services にアクセスします。 リモート デスクトップ ActiveX コントロールをサポートします。 **（注）** この古いプラグインは、RDP2 だけをサポートします。このプラグインを使用することは推奨しません。代わりに、上記の RDP プラグインを使用してください。	http://properjavardp.sourceforge.net/

表 14-2　シスコが再配布しているプラグイン

プロトコル	説明	再配布しているプラグインのソース *
SSH	Secure Shell-Telnet プラグインにより、リモート ユーザはリモート コンピュータへの Secure Shell（v1 または v2）または Telnet 接続を確立できます。 （注）　キーボード インタラクティブ認証は JavaSSH ではサポートされていないため、（異なる認証メカニズムの実装に使用される）SSH プラグインではサポートされません。	http://javassh.org/
VNC	Virtual Network Computing プラグインを使用すると、リモート ユーザはリモート デスクトップ共有（VNC サーバまたはサービスとも呼ばれる）をオンにしたコンピュータを、モニタ、キーボード、およびマウスを使用して表示および制御できます。このバージョンでは、テキストのデフォルトの色が変更されています。また、フランス語と日本語のヘルプ ファイルもアップデートされています。	http://www.tightvnc.com/

*展開の設定と制限については、プラグインのマニュアルを参照してください。

これらのプラグインは、「Cisco Adaptive Security Appliance Software Download」サイトで入手できます。

手順の詳細

（注）　ASA は、**import webvpn plug-in protocol** コマンドをコンフィギュレーションに保持しません。その代わりに、csco-config/97/plugin ディレクトリの内容を自動的にロードします。セカンダリ ASA は、プライマリ ASA からプラグインを取得します。

	コマンド	目的
ステップ 1	**import webvpn plug-in** *protocol* [**rdp** | **rdp2** | [**ssh** | **telnet**] | **vnc**] *URL* **例：** `hostname# import webvpn plug-in protocol ssh,telnet tftp://local_tftp_server/plugins/ssh-plugin.jar` `Accessing tftp://local_tftp_server/plugins/ssh-plugin.jar...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!` `Writing file disk0:/csco_config/97/plugin/ssh...` `!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!` `238510 bytes copied in 3.650 secs (79503 bytes/sec)`	ASA のフラッシュ デバイスにプラグインをインストールします。*protocol* は次のいずれかの値になります。**ssh**、**telnet** は、セキュア シェル サービスと Telnet サービスの*両方*へのプラグイン アクセスを提供します。 （注）　SSH 用と Telnet 用にこのコマンドをそれぞれ入力しないでください。ssh,telnet ストリングを入力する場合は、両者の間にスペースは挿入しません。 *URL* は、プラグイン .jar ファイルへのリモート パスです。TFTP または FTP サーバのホスト名またはアドレス、およびプラグインへのパスを入力します。

	コマンド	目的
ステップ 2	（オプション） **revert webvpn plug-in protocol** *protocol* **例：** hostname# **revert webvpn plug-in protocol rdp**	プラグインに対するクライアントレス SSL VPN のサポートをオフに切り替えて削除し、ASA のフラッシュ デバイスからも削除します。

Citrix XenApp Server へのアクセスの提供

サードパーティのプラグインに、クライアントレス SSL VPN ブラウザ アクセスを提供する方法の例として、この項では、Citrix XenApp Server Client にクライアントレス SSL VPN のサポートを追加する方法について説明します。

ASA に Citrix プラグインがインストールされている場合、クライアントレス SSL VPN ユーザは、ASA への接続を使用して、Citrix XenApp サービスにアクセスできます。

ステートフル フェールオーバーでは、Citrix プラグインを使用して確立したセッションは保持されません。Citrix のユーザは、フェールオーバー後に再認証を行う必要があります。

Citrix プラグインへのアクセスを提供するには、次の項で説明する手順に従ってください。

- クライアントレス SSL VPN アクセスのための Citrix XenApp Server の準備
- Citrix プラグインの作成とインストール

クライアントレス SSL VPN アクセスのための Citrix XenApp Server の準備

（Citrix）「セキュア ゲートウェイ」を使用しないモードで動作するように、Citrix Web Interface ソフトウェアを設定する必要があります。この設定をしないと、Citrix クライアントは Citrix XenApp Server に接続できません。

（注） プラグインに対するサポートをまだ提供していない場合は、「プラグインのためのセキュリティ アプライアンスの準備」（P.14-4）の説明に従い作業を行った後に、この項を参照してください。

Citrix プラグインの作成とインストール

手順の詳細

ステップ 1　シスコのソフトウェア ダウンロード Web サイトから ica-plugin.zip ファイルをダウンロードします。

このファイルには、Citrix プラグインを使用するためにシスコがカスタマイズしたファイルが含まれています。

ステップ 2　Citrix のサイトから Citrix Java クライアントをダウンロードします。

Citrix Web サイトのダウンロード領域で **[Citrix Receiver]** と **[Receiver for Other Platforms]** を選択し、**[Find]** をクリックします。**[Receiver for Java]** ハイパーリンクをクリックしアーカイブをダウンロードします。

ステップ 3　アーカイブから次のファイルを抽出し、それらを ica-plugin.zip ファイルに追加します。

- JICA-configN.jar
- JICAEngN.jar

ステップ 4　Citrix Java クライアントに含まれている EULA によって、Web サーバ上にクライアントを配置するための権限が与えられていることを確認します。

ステップ 5　ASDM を使用するか、または特権 EXEC モードで次の CLI コマンドを入力して、プラグインをインストールします。

import webvpn plug-in protocol ica *URL*

URL はホスト名または IP アドレス、および ica-plugin.zip ファイルへのパスです。

（注）　Citrix セッションに SSO サポートを提供する場合は、ブックマークの追加は必須です。次のように、ブックマークで便利な表示を提供する URL パラメータを使用することを推奨します。

ica://10.56.1.114/?DesiredColor=4&DesiredHRes=1024&DesiredVRes=768

ステップ 6　SSL VPN クライアントレス セッションを確立し、ブックマークをクリックするか、Citrix サーバの URL を入力します。

必要に応じて、『Client for Java Administrator's Guide』を参照してください。

セキュリティ アプライアンスにインストールされているプラグインの表示

手順の詳細

	コマンド	目的
ステップ 1	**show import webvpn plug-in** **例：** hostname# **show import webvpn plug** ssh rdp vnc ica	クライアントレス SSL VPN のユーザが使用できる Java ベースのクライアント アプリケーションを一覧表示します。
ステップ 2	**show import webvpn plug detail** **例：** hostname **show import webvpn plug** post GXN2BIGGOAOkBMibDQsMu2GWZ3Q= Tues, 29 Apr 2008 19:57:03 GMT rdp fHeyReIOUwDCgAL9HdTs PnjdBoo= Tues, 15 Sep 2009 23:23:56 GMT rdp2 shw8c22T2SsILLk6zyCd6H6VOz8= Wed, 11 Feb 2009 21:17:54 GMT	プラグインのハッシュおよび日付を含めます。

ポート転送の設定

次の項では、ポート転送とその設定方法について説明します。

ポート転送に関する情報

ポート転送により、ユーザはクライアントレス SSL VPN 接続を介して TCP ベースのアプリケーションにアクセスできます。TCP ベースのアプリケーションには次のようなものがあります。

- Lotus Notes
- Microsoft Outlook
- Microsoft Outlook Express
- Perforce
- Sametime
- Secure FTP（FTP over SSH）
- SSH
- Telnet
- Windows Terminal Service
- XDDTS

その他の TCP ベースのアプリケーションも動作する可能性はありますが、シスコではテストを行っていません。UDP を使用するプロトコルは動作しません。

ポート転送は、クライアントレス SSL VPN 接続を介して TCP ベースのアプリケーションをサポートするためのレガシー テクノロジーです。ポート転送テクノロジーをサポートする設定を事前に構築している場合は、ポート転送の使用を選択することもできます。

ポート転送の代替方法として次のことを検討してください。

- スマート トンネル アクセスを使用すると、ユーザには次のような利点があります。
  - スマート トンネルは、プラグインよりもパフォーマンスが向上します。
  - ポート転送とは異なり、スマート トンネルでは、ローカル ポートへのローカル アプリケーションのユーザ接続を要求しないことにより、ユーザ エクスペリエンスが簡略化されます。
  - ポート転送とは異なり、スマート トンネルでは、ユーザは管理者特権を持つ必要がありません。
- ポート転送およびスマート トンネル アクセスとは異なり、プラグインでは、クライアント アプリケーションをリモート コンピュータにインストールする必要がありません。

ASA でポート転送を設定する場合は、アプリケーションが使用するポートを指定します。スマート トンネル アクセスを設定する場合は、実行ファイルまたはそのパスの名前を指定します。

前提条件

- リモート ホストで、次のいずれかの 32 ビット バージョンが実行されている必要があります。
  - Microsoft Windows Vista、Windows XP SP2 または SP3、または Windows 2000 SP4
  - Apple Mac OS X 10.4 または 10.5 と Safari 2.0.4(419.3)
  - Fedora Core 4
- また、リモート ホストで Oracle Java ランタイム環境（JRE）5 以降が動作している必要もあります。
- Mac OS X 10.5.3 上の Safari のブラウザベースのユーザは、Safari での URL の解釈方法に従って、使用するクライアント証明書を、1 回目は末尾にスラッシュを含め、もう 1 回はスラッシュを含めずに、ASA の URL を使用して指定する必要があります。次に例を示します。
  - https://example.com/
  - https://example.com

  詳細については、『Safari, Mac OS X 10.5.3: Changes in client certificate authentication』を参照してください。
- ポート転送またはスマート トンネルを使用する Microsoft Windows Vista 以降のユーザは、ASA の URL を信頼済みサイト ゾーンに追加する。信頼済みサイト ゾーンにアクセスするには、Internet Explorer を起動し、**[Tools] > [Internet Options] > [Security]** タブを選択する必要があります。Vista（以降の）ユーザは保護モードをオフに切り替えるとスマート トンネル アクセスを使用することもできます。ただし、攻撃に対するコンピュータの脆弱性が増すため、この方法の使用はお勧めしません。
- ポート転送（アプリケーション アクセス）およびデジタル証明書をサポートするために、リモート コンピュータに Oracle Java ランタイム環境（JRE）1.5.x 以降がインストールされていることを確認します。JRE 1.4.x が実行中で、ユーザがデジタル証明書で認証される場合、JRE が Web ブラウザの証明書ストアにアクセスできないため、アプリケーションは起動しません。

制限

- ポート転送は、スタティック TCP ポートを使用する TCP アプリケーションのみをサポートしています。ダイナミック ポートまたは複数の TCP ポートを使用するアプリケーションはサポートしていません。たとえば、ポート 22 を使用する SecureFTP は、クライアントレス SSL VPN のポート転送を介して動作しますが、ポート 20 と 21 を使用する標準 FTP は動作しません。
- ポート転送は、UDP を使用するプロトコルをサポートしていません。
- ポート転送は Microsoft Outlook Exchange（MAPI）プロキシをサポートしていません。しかし、Microsoft Outlook Exchange Server と連携することにより、Microsoft Office Outlook のスマート トンネル サポートを設定することができます。
- ステートフル フェールオーバーでは、Application Access（ポート転送またはスマート トンネル アクセス）を使用して確立したセッションは保持されません。ユーザはフェールオーバー後に再接続する必要があります。
- ポート転送は、携帯情報端末（PDA）への接続はサポートしていません。
- ポート転送を使用するには、Java アプレットをダウンロードしてローカル クライアントを設定する必要があります。これには、ローカル システムに対する管理者の許可が必要になるため、ユーザがパブリック リモート システムから接続した場合に、アプリケーションを使用できない可能性があります。

Java アプレットは、エンド ユーザの HTML インターフェイスにあるアプレット独自のウィンドウに表示されます。このウィンドウには、ユーザが使用できる転送ポートのリストの内容、アクティブなポート、および送受信されたトラフィック量（バイト単位）が表示されます。

- ローカル IP アドレス 127.0.0.1 が使用されており、ASA からのクライアントレス SSL VPN 接続によって更新できない場合、ポート転送アプレットはローカル ポートとリモート ポートを同一として表示します。その結果、ASA は、127.0.0.2、127.0.0.3 など、ローカル プロキシ ID の新しい IP アドレスを作成します。hosts ファイルを変更して異なるループバックを使用できるため、リモート ポートはアプレットでローカル ポートとして使用されます。接続するには、ポートを指定せずにホスト名を指定して Telnet を使用します。正しいローカル IP アドレスをローカル ホスト ファイルで使用できます。

ポート転送用の DNS の設定

ポート転送では、リモート サーバのドメイン名またはその IP アドレスを ASA に転送して、解決および接続を行います。つまり、ポート転送アプレットは、アプリケーションからの要求を受け入れて、その要求を ASA に転送します。ASA は適切な DNS クエリーを作成し、ポート転送アプレットの代わりに接続を確立します。ポート転送アプレットは、ASA に対する DNS クエリーだけを作成します。ポート転送アプレットはホスト ファイルをアップデートして、ポート転送アプリケーションが DNS クエリーを実行したときに、クエリーがループバック アドレスにリダイレクトされるようにします。次のように、DNS 要求をポート転送アプレットから受け入れるように、ASA を設定します。

	コマンド	目的
ステップ 1	**dns server-group**	DNS サーバ グループ モードを開始します。 example.com という名前の DNS サーバ グループを設定します。
ステップ 2	**domain-name** **例：** hostname(config)# **dns server-group example.com** hostname(config-dns-server-group)# **domain-name example.com**	ドメイン名を指定します。デフォルトのドメイン名設定は DefaultDNS です。
ステップ 3	**name-server** **例：** hostname(config-dns-server-group)# **name-server 192.168.10.10**	ドメイン名を IP アドレスに解決します。
ステップ 4	**webvpn**	クライアントレス SSL VPN コンフィギュレーション モードに切り替えます。

	コマンド	目的
ステップ 5	**tunnel-group webvpn**	トンネルグループ クライアントレス SSL VPN コンフィギュレーション モードに切り替えます。
ステップ 6	（デフォルトのドメイン名 [DefaultDNS] 以外のドメイン名を使用している場合にだけ必要） **dns-group** **例：** asa2(config-dns-server-group)# **exit** asa2(config)# **tunnel-group DefaultWEBVPNGroup webvpn-attributes** asa2(config-tunnel-webvpn)# **dns-group example.com**	そのトンネル グループで使用されるドメイン名を指定します。デフォルトでは、セキュリティ アプライアンスがクライアントレス接続のデフォルトのトンネル グループとしてデフォルトのクライアントレス SSL VPN グループを割り当てます。ASA がこのトンネル グループを使用して設定をクライアントレス接続に割り当てる場合は、この手順を実行します。それ以外の場合は、クライアントレス接続に対して設定されたトンネルごとにこの手順を実行します。

アプリケーションのポート転送適格化

各 ASA のクライアントレス SSL VPN コンフィギュレーションは、*ポート転送リスト*をサポートしています。それぞれのリストでは、アクセスを提供するアプリケーションが使用するローカル ポートとリモート ポートを指定します。各グループ ポリシーまたはユーザ名は 1 つのポート転送リストのみをサポートするため、サポートされる CA のセットをグループ化してリストを作成する必要があります。ASA コンフィギュレーションにすでに存在するポート転送リストのエントリを表示するには、次のコマンドを入力します。

手順の詳細

	コマンド	目的
ステップ 1	**show run webvpn port-forward**	ASA 設定にすでに存在するポート転送リスト エントリを表示します。
ステップ 2	**webvpn**	クライアントレス SSL VPN コンフィギュレーション モードに切り替えます。

	コマンド	目的
ステップ 3	**port-forward {<list name> <local port> <remote server> <remote port> <description>}** **例：** hostname(config)# **webvpn** hostname(config-webvpn)# **port-forward SalesGroupPorts 20143 IMAP4Sserver 143 Get Mail** hostname(config-webvpn)# **port-forward SalesGroupPorts 20025 SMTPSserver 25 Send Mail** hostname(config-webvpn)# **port-forward SalesGroupPorts 20022 DDTSserver 22 DDTS over SSH** hostname(config-webvpn)# **port-forward SalesGroupPorts 20023 Telnetserver 23 Telnet**	ポート転送のエントリをリストに追加します。 • *list_name*：クライアントレス SSL VPN セッションのユーザがアクセスするアプリケーションのセット（理論的には、転送 TCP ポートのセット）の名前です。名前を認識しない場合、ASA は、ユーザが入力した名前を使用してリストを作成します。認識した場合は、そのポート転送のエントリをリストに追加します。最大 64 文字です。 • *local_port*：ユーザのコンピュータで実行しているアプリケーションの TCP トラフィックをリッスンするポートです。ローカル ポートの番号は、各ポート転送リストに対して一度だけ使用できます。1 ～ 65535 の範囲のポート番号、またはポート名を入力します。既存サービスとの競合を避けるために、1024 よりも大きいポート番号を使用します。 • *remote_server*：アプリケーションに対するリモート サーバの DNS 名または IP アドレスです。IP アドレスは IPv4 または IPv6 形式で指定できます。特定の IP アドレス用にクライアント アプリケーションを設定しなくて済むように、DNS 名を指定することをお勧めします。 **（注）** DNS 名は、前の項で説明した手順に従って、トンネルを確立し、IP アドレスに解決するためにトンネル グループに割り当てられた DNS 名と一致する必要があります。その項で説明した **domain-name** **group** および **dns-group** の両方のコマンドに対するデフォルト設定は DefaultDNS です。 • *remote_port*：このアプリケーションが接続するリモート サーバのポートです。これは、アプリケーションで使用する実際のポートです。1 ～ 65535 の範囲のポート番号、またはポート名を入力します。 • *description*：エンド ユーザの Port Forwarding Java アプレット画面に表示されるアプリケーション名または簡単な説明です。最大 64 文字です。 これらのアプリケーションへのアクセスを提供する SalesGroupPorts という名前のポート転送リストを作成する方法を示します。

	コマンド	目的
ステップ 4	(オプション) **no port-forward <list name> <local port>**	リストとローカル ポートの両方を指定して、リストからエントリを削除します。

ポート転送リストの設定に続けて、次の項で説明するように、そのリストをグループ ポリシーまたはユーザ名に割り当てます。

ポート転送リストの割り当て

クライアントレス SSL VPN 接続によるアクセスに適用されるユーザまたはグループ ポリシーに関連付ける TCP アプリケーションの名前付きリストを追加または編集できます。グループ ポリシーとユーザ名ごとに、次のいずれかを行うようにクライアントレス SSL VPN を設定できます。

- ユーザのログイン時に自動的にポート転送アクセスを開始する。

(注) これらのオプションは、各グループ ポリシーとユーザ名に対して互いに排他的です。1 つだけ使用してください。

前提条件

port-forward enable <list_name> コマンドを開始する前に、ユーザは、クライアントレス SSL VPN ポータル ページの **[Application Access] > [Start Applications]** を使用して、ポート転送を手動で開始する必要があります。

手順の詳細

これらのコマンドは、各グループ ポリシーとユーザ名で使用可能です。各グループ ポリシーとユーザ名のコンフィギュレーションは、これらのコマンドを一度に 1 つだけサポートします。そのため、1 つのコマンドを入力すると、ASA が、該当のグループ ポリシーまたはユーザ名のコンフィギュレーションに存在するコマンドを新しいコマンドで置き換えます。または、後者のコマンドの場合は、グループ ポリシーまたはユーザ名コンフィギュレーションから **port-forward** コマンドが単純に削除されます。

	コマンド	目的
ステップ 1	**port-forward auto-start <list name>**	ユーザのログイン時に自動的にポート転送を開始します。
	port-forward enable <list name>	ユーザのログイン時にポート転送をイネーブルにします。
	port-forward disable	ポート転送を禁止します。
	no port-forward [**auto-start** **<list name>** | **enable** **<list name>** | **disable**]	**port-forward** コマンドをグループ ポリシーまたはユーザ名コンフィギュレーションから削除し、[**no**] **port-forward** コマンドをデフォルト グループ ポリシーから継承します。**no port-forward** コマンドの後にあるキーワードはオプションですが、これらのキーワードは削除対象をその名前の **port-forward** コマンドに限定します。

ポート転送の自動化

ユーザのログイン時にポート転送を自動的に開始するには、次のコマンドを入力します。

手順の詳細

	コマンド	目的
ステップ 1	**webvpn**	クライアントレス SSL VPN コンフィギュレーション モードに切り替えます。
ステップ 2	**group-policy webvpn** **username webvpn**	グループ ポリシーのクライアントレス SSL VPN コンフィギュレーション モードに切り替えます。 ユーザ名のクライアントレス SSL VPN コンフィギュレーション モードに切り替えます。
ステップ 3	**port-forward auto-start <list name>** **例**： hostname(config-group-policy)# **webvpn** hostname(config-group-webvpn)# **port-forward auto-start apps1**	ユーザのログイン時に自動的にポート転送を開始します。 *list_name* は ASA クライアントレス SSL VPN コンフィギュレーションにすでに存在するポート転送リストの名前です。複数のポート転送リストをグループ ポリシーまたはユーザ名に割り当てることはできません。 apps1 という名前のポート転送リストをグループ ポリシーに割り当てます。

	コマンド	目的
ステップ 4	**show run webvpn port-forward**	ASA 設定に存在するポート転送リスト エントリを表示します。
ステップ 5	（オプション） **no port-forward**	**port-forward** コマンドをグループ ポリシーまたはユーザ名から削除し、デフォルトに戻します。

ポート転送のイネーブル化と切り替え

デフォルトでは、ポート転送はオフになっています。

手順の詳細

	コマンド	目的
ステップ 1	**port-forward [enable <list name> | disable]** **例：** hostname(config-group-policy)# **webvpn** hostname(config-group-webvpn)# **port-forward enable apps1**	ポート転送をイネーブルにします。前の表の **port-forward auto-start** ***list_name*** を入力した場合は、ポート転送を手動で開始する必要はありません。 *list_name* は、ASA クライアントレス SSL VPN コンフィギュレーションにすでに存在するポート転送リストの名前です。複数のポート転送リストをグループ ポリシーまたはユーザ名に割り当てることはできません。 apps1 という名前のポート転送リストをグループ ポリシーに割り当てます。
ステップ 2	**show running-config port-forward**	ポート転送リストのエントリを表示します。
ステップ 3	（オプション） **no port-forward**	port-forward コマンドをグループ ポリシーまたはユーザ名から削除し、デフォルトに戻します。
ステップ 4	（オプション） **port-forward disable**	ポート転送をオフに切り替えます。

ファイル アクセスの設定

クライアントレス SSL VPN は、リモート ユーザに HTTPS ポータル ページを提供しています。このページは、ASA で実行するプロキシ CIFS クライアントまたは FTP クライアント（あるいはその両方）と連動しています。クライアントレス SSL VPN は、CIFS または FTP を使用して、ユーザが認証の要件を満たしているファイルのプロパティがアクセスを制限しない限り、ネットワーク上のファイルへのネットワーク アクセスをユーザに提供します。CIFS クライアントおよび FTP クライアントは透過的です。クライアントレス SSL VPN から送信されるポータル ページでは、ファイル システムに直接アクセスしているかのように見えます。

ユーザがファイルのリストを要求すると、クライアントレス SSL VPN は、そのリストが含まれるサーバの IP アドレスをマスター ブラウザに指定されているサーバに照会します。ASA はリストを入手してポータル ページ上のリモート ユーザに送信します。

クライアントレス SSL VPN は、ユーザの認証要件とファイルのプロパティに応じて、ユーザが次の CIFS および FTP の機能を呼び出すことができるようにします。

- ドメインとワークグループ、ドメインまたはワークグループ内のサーバ、サーバ内部の共有、および共有部分またはディレクトリ内のファイルのナビゲートとリスト。
- ディレクトリの作成。
- ファイルのダウンロード、アップロード、リネーム、移動、および削除。

ASA は、通常、ASA と同じネットワーク上か、またはこのネットワークからアクセス可能な場所のマスター ブラウザ、WINS サーバ、または DNS サーバを使用して、リモート ユーザがクライアントレス SSL VPN セッション中に表示されるポータル ページのメニュー上またはツールバー上の **[Browse Networks]** をクリックしたときに、ネットワークでサーバのリストを照会します。

マスター ブラウザまたは DNS サーバは、ASA 上の CIFS/FTP クライアントに、クライアントレス SSL VPN がリモート ユーザに提供する、ネットワーク上のリソースのリストを表示します。

（注） ファイル アクセスを設定する前に、ユーザ アクセス用のサーバに共有を設定する必要があります。

CIFS ファイル アクセスの要件と制限事項

`\\server\share\subfolder\personal` *フォルダ*にアクセスするには、最低限、共有自体を含むすべての親フォルダに対する読み取り権限がユーザに必要です。

CIFS ディレクトリとローカル デスクトップとの間でファイルをコピー アンド ペーストするには、**[Download]** または **[Upload]** を使用します。[Copy] ボタンおよび [Paste] ボタンはリモート間のアクションのみで使用でき、ローカルからリモートまたはリモートからローカルへのアクションには使用できません。

CIFS ブラウズ サーバ機能は、2 バイト文字の共有名（13 文字を超える共有名）をサポートしていません。これは、表示されるフォルダのリストに影響を与えるだけで、フォルダへのユーザ アクセスには影響しません。回避策として、2 バイトの共有名を使用する CIFS フォルダのブックマークを事前に設定するか、ユーザが cifs://server/<long-folder-name> 形式でフォルダの URL またはブックマークを入力します。次に例を示します。

```
cifs://server/Do you remember?
cifs://server/Do%20you%20remember%3F
```

ファイル アクセスのサポートの追加

次の手順を実行して、ファイル アクセスを設定します。

（注） この手順では、マスター ブラウザおよび WINS サーバを指定する方法について説明します。代わりに、ASDM を使用して、ファイル共有へのアクセスを提供する URL リストとエントリを設定することもできます。

ASDM での共有の追加には、マスター ブラウザまたは WINS サーバは必要ありません。ただし、Browse Networks リンクへのサポートは提供されません。**nbns-server** コマンドを入力するときは、ホスト名または IP アドレスを使用して ServerA を参照できます。ホスト名を使用する場合、ASA はホスト名を IP アドレスに解決するように DNS サーバに要求します。

手順の詳細

	コマンド	目的
ステップ 1	**webvpn**	クライアントレス SSL VPN コンフィギュレーション モードに切り替えます。
ステップ 2	**tunnel-group webvpn**	トンネルグループ クライアントレス SSL VPN コンフィギュレーション モードに切り替えます。
ステップ 3	**nbns-server** {IPaddress | hostname} **[master] [timeout timeout] [retry retries]** **例：** hostname(config-tunnel-webvpn)# **nbns-server 192.168.1.20 master** hostname(config-tunnel-webvpn)# **nbns-server 192.168.1.41** hostname(config-tunnel-webvpn)# **nbns-server 192.168.1.47**	各 NetBIOS ネーム サーバ（NBNS）のネットワークまたはドメインをブラウズします。 • **master** は、マスター ブラウザに指定されるコンピュータです。マスター ブラウザは、コンピュータおよび共有リソースのリストを維持します。コマンドのマスター部分を入力せずにこのコマンドで指定する任意の NBNS サーバは、Windows Internet Naming Server（WINS）である必要があります。まずマスター ブラウザを指定してから、WINS サーバを指定してください。マスター ブラウザを含め、接続プロファイル用のサーバは最大 3 つまで指定できます。 • *timeout* は、ASA が、クエリーを再度サーバに送信する前に待機する秒数です。このとき、サーバが 1 つしかない場合は同じサーバに送信し、サーバが複数存在する場合は別のサーバに送信します。デフォルトのタイムアウトは 2 秒で、指定できる範囲は 1 ～ 30 秒です。 • *retries* は、NBNS サーバに対するクエリーのリトライ回数です。ASA は、この回数だけサーバのリストを再利用してからエラー メッセージを送信します。デフォルト値は 2 で、指定できる範囲は 1 ～ 10 です。
ステップ 4	hostname# **show tunnel-group webvpn-attributes**	接続プロファイル コンフィギュレーションにすでに存在する NBNS サーバを表示します。

	コマンド	目的
ステップ 5	（オプション） **character-encoding *charset*** **例：** hostname(config)# **webvpn** hostname(config-webvpn)# **character-encoding shift_jis** hostname(config-webvpn)# **customization DfltCustomization** hostname(config-webvpn-custom)# **page style background-color:white**	クライアントレス SSL VPN ポータル ページをリモート ユーザに送信するために符号化する文字セットを指定します。デフォルトでは、リモート ブラウザ上の符号化タイプ セットでクライアントレス SSL VPN ポータル ページの文字セットが決定されるため、ユーザは、ブラウザで符号化を適切に実行するために必要となる場合に限り、文字の符号化を設定する必要があります。 *charset* は、最大 40 文字からなる文字列で、http://www.iana.org/assignments/character-sets で指定されたいずれかの有効文字セットと同じです。このページに示されている文字セットの名前またはエイリアスのいずれかを使用できます。たとえば、iso-8859-1、shift_jis、ibm850 などです。 **（注）** character-encoding の値および file-encoding の値は、ブラウザによって使用されるフォント ファミリを排除するものではありません。次の例に示すように日本語の Shift_JIS 文字エンコーディングを使用する場合などは、webvpn カスタマイゼーション コマンド モードで **page style** コマンドを使用してフォント ファミリを置換し、これらの値の設定を補 足するか、または webvpn カスタマイゼーション コマンド モードで **no page style** コマンドを入力してフォント ファミリを削除する必要があります。 日本語 Shift_JIS 文字をサポートする character-encoding 属性を設定し、フォント ファミリを削除し、デフォルトの背景色を保持します。
ステップ 6	（オプション） **file-encoding {server-name | server-ip-address} *charset*** **例：** hostname(config-webvpn)# **file-encoding 10.86.5.174 cp860**	特定の CIFS サーバのクライアントレス SSL VPN ポータル ページの符号化を指定します。このため、これ以外の文字の符合化が必要な各 CIFS サーバに対し、異なるファイル符号化値を使用できます。 CIFS サーバ 10.86.5.174 の file-encoding 属性を設定して、IBM860（エイリアス「CP860」）文字をサポートします。

これらのコマンドの詳しい説明については、コマンド リファレンスを参照してください。

SharePoint アクセスのためのクロックの精度の確認

ASA のクライアントレス SSL VPN サーバは、クッキーを使用して、エンドポイントの Microsoft Word などのアプリケーションと対話します。ASA で設定されたクッキーの有効期間により、ASA の時間が正しくない場合、SharePoint サーバ上の文書にアクセスするときに Word が正しく機能しなくなる可能性があります。このような誤作動を回避するには、ASA クロックを正しく設定します。NTP サーバとダイナミックに同期化されるように ASA を設定することをお勧めします。手順については、一般的な操作のコンフィギュレーション ガイドの日付と時刻の設定の項を参照してください。

仮想デスクトップ インフラストラクチャ（VDI）

ASA は、Citrix サーバおよび VMware VDI サーバへの接続をサポートします。

- Citrix の場合、ASA ではクライアントレス ポータルを介してユーザの実行中の Citrix レシーバへアクセスできます。
- VMware は、（スマート トンネル）のアプリケーションとして設定されます。

VDI サーバには、他のサーバ アプリケーションのように、クライアントレス ポータルのブックマークを介してアクセスできます。

制限事項

- 自動サインオンの場合、証明書またはスマート カードを使用する認証はサポートされません。これは、これらの認証形式では間にある ASA を許可しないためです。
- XML サービスは XenApp サーバおよび XenDesktop サーバにインストールし、設定する必要があります。
- スタンドアロン モバイル クライアントを使用している場合は、クライアント証明書の確認、二重認証、内部パスワードと CSD（Vault だけでなく、すべての CSD）はサポートされません。

Citrix モバイルのサポート

Citrix レシーバを実行しているモバイル ユーザは、次を実行して Citrix サーバに接続できます。

- AnyConnect で ASA に接続してから Citrix サーバに接続する。
- AnyConnect クライアントを使用せずに ASA を介して Citrix サーバに接続する。ログオン クレデンシャルには次を含めることができます。
  - Citrix ログオン画面の接続プロファイルのエイリアス（トンネル グループ エイリアスとも呼ばれる）。VDI サーバは、それぞれ別の権限と接続設定を備えた複数のグループ ポリシーを持つことができます。
  - RSA サーバが設定されている場合は RSA SecureID トークンの値。RSA サポートには、無効なエントリ用の次のトークンと、最初の PIN または期限切れ PIN 用の新しい PIN を入力するための次のトークンが含まれています。

サポートされているモバイル デバイス

- iPad：Citrix Receiver バージョン 4.x 以降
- iPhone/iTouch：Citrix Receiver バージョン 4.x 以降
- Android 2.x/3.x/4.0/4.1 電話機：Citrix Receiver バージョン 2.x 以降
- Android 4.0 電話機：Citrix Receiver バージョン 2.x 以降

制限事項

証明書の制限

- 証明書/スマートカード認証は自動サインオンの手段としてはサポートされていません。
- クライアント証明書の確認および CSD はサポートされていません。
- 証明書の Md5 署名は、iOS の既知の問題であるセキュリティ上の問題（http://support.citrix.com/article/CTX132798）から動作していません。
- SHA2 シグニチャは Citrix Web サイト（http://www.citrix.com/）の説明に従って Windows を除き、サポートされていません。
- 1024 以上のキー サイズはサポートされていません。

その他の制限

- HTTP リダイレクトはサポートされません。Citrix レシーバ アプリケーションはリダイレクトでは機能しません。
- XML サービスは XenApp サーバおよび XenDesktop サーバにインストールし、設定する必要があります。

Citrix Mobile Receiver のユーザ ログオンについて

Citrix サーバに接続しているモバイル ユーザのログオンは、ASA が Citrix サーバを VDI サーバとして設定したか、または VDI プロキシ サーバとして設定したかによって異なります。

Citrix サーバが VDI サーバとして設定されている場合:

1. AnyConnect Secure Mobility Client を使用し、VPN クレデンシャルで ASA に接続します。
2. Citrix Mobile Receiver を使用し、Citrix サーバ クレデンシャルで Citrix サーバに接続します（シングルサインオンを設定している場合は、Citrix クレデンシャルは不要です）。

ASA が VDI プロキシ サーバとして設定されている場合:

1. Citrix Mobile Receiver を使用し、VPN と Citrix サーバの両方のクレデンシャルを入力して ASA に接続します。最初の接続後、正しく設定されている場合は、以降の接続に必要なのは VPN クレデンシャルだけです。

Citrix サーバをプロキシする ASA の設定

ASA を Citrix サーバのプロキシとして動作するように設定し、ASA への接続が Citrix サーバへの接続であるかのようにユーザに見せることができます。ASDM の VDI プロキシがイネーブルになっている場合は AnyConnect クライアントは不要です。次の手順は、エンド ユーザーから Citrix に接続する方法の概要を示します。

1. モバイル ユーザが Citrix レシーバを起動し、ASA の URL に接続します。
2. Citrix のログイン画面で、XenApp サーバのクレデンシャルと VPN クレデンシャルを指定します。
3. 以降、Citrix サーバに接続する場合に必要になるのは、VPN クレデンシャルだけです。

XenDesktop および XenApp のプロキシとして ASA を使用すると Citrix アクセス ゲートウェイは必要なくなります。XenApp サーバ情報が ASA に記録され、ASDM に表示されます。

Citrix サーバのアドレスおよびログイン クレデンシャルを設定し、グループ ポリシーまたはユーザ名にその VDI サーバを割り当てます。ユーザ名とグループ ポリシーの両方を設定した場合は、ユーザ名の設定によってグループ ポリシー設定がオーバーライドされます。

その他の情報

http://www.youtube.com/watch?v=JMM2RzppaG8：このビデオでは、その ASA を Citrix プロキシとして使用する利点について説明します。

グループ ポリシーへの VDI サーバの割り当て

VDI サーバを設定し、グループ ポリシーに割り当てる方法は次のとおりです。

- [VDI Access] ペインで VDI サーバを追加し、サーバにグループ ポリシーを割り当てる。
- グループ ポリシーに VDI サーバを追加する。

ユーザ名とグループ ポリシーが両方とも設定されている場合、ユーザ名の設定は、グループ ポリシーに優先します。次を入力します。

```
configure terminal
    group-policy DfltGrpPolicy attributes
        webvpn
            vdi type <citrix> url <url> domain <domain> username <username> password
            <password>
configure terminal
    username <username> attributes
        webvpn
            vdi type <citrix> url <url> domain <domain> username <username> password
            <password>]
```

構文オプションは、次のように定義されます。

- type：VDI のタイプ。Citrix Receiver タイプの場合、この値は *citrix* にする必要があります。
- url：http または https、ホスト名、ポート番号、および XML サービスへのパスを含む XenApp または XenDesktop サーバの完全な URL。
- username：仮想化インフラストラクチャ サーバにログインするためのユーザ名。この値は、クライアントレス マクロにすることができます。
- password：仮想化インフラストラクチャ サーバにログインするためのパスワード。この値は、クライアントレス マクロにすることができます。

- domain：仮想化インフラストラクチャ サーバにログインするためのドメイン。この値は、クライアントレス マクロにすることができます。

内部サーバにアクセスするための SSL の使用

	コマンド	目的
ステップ 1	webvpn	グループ ポリシーのクライアントレス SSL VPN コンフィギュレーション モードに切り替えます。
ステップ 2	url-entry disable	URL エントリをオフに切り替えます。

クライアントレス SSL VPN は SSL およびその後継である TLS1 を使用して、リモート ユーザと、内部サイトにある特定のサポートされている内部リソースとの間でセキュアな接続を提供します。

- 「クライアントレス SSL VPN セッションでの HTTPS の使用」（P.14-23）
- 「クライアントレス SSL VPN ポートと ASDM ポートの設定」（P.14-24）
- 「プロキシ サーバのサポートの設定」（P.14-24）
- 「SSL/TLS 暗号化プロトコルの設定」（P.14-27）

クライアントレス SSL VPN セッションでの HTTPS の使用

前提条件

Web ブラウザには、ASA のアドレスを *https:// address* 形式で入力します。*address* は ASA インターフェイスの IP アドレスまたは DNS ホスト名です。

制限

- ユーザの接続先の ASA インターフェイス上でクライアントレス SSL VPN セッションをイネーブルにする必要があります。
- ASA またはロードバランシング クラスタへのアクセスに HTTPS を使用する必要があります。

	コマンド	目的
ステップ 1	**webvpn**	クライアントレス SSL VPN コンフィギュレーション モードに切り替えます。
ステップ 2	**enable** <クライアントレス SSL VPN セッションに使用するインターフェイスの名前> **例：** hostname(config)# **webvpn** hostname(config-webvpn)# **enable outside**	outside という名前のインターフェイス上でクライアントレス SSL VPN セッションをイネーブルにします。

クライアントレス SSL VPN ポートと ASDM ポートの設定

バージョン 8.0(2) 以降、ASA は、クライアントレス SSL VPN セッションと ASDM 管理セッションの両方を、外部インターフェイスのポート 443 で同時にサポートするようになりました。さまざまなインターフェイスでこれらのアプリケーションを設定できます。

	コマンド	目的
ステップ 1	**webvpn**	クライアントレス SSL VPN コンフィギュレーション モードに切り替えます。
ステップ 2	**port** *port_number* **例：** hostname(config)# **http server enable** hostname(config)# **http 192.168.3.0 255.255.255.0 outside** hostname(config)# **webvpn** hostname(config-webvpn)# **port 444** hostname(config-webvpn)# **enable outside**	クライアントレス SSL VPN の SSL リスニング ポートを変更します。 外部インターフェイスのポート 444 上でクライアントレス SSL VPN をイネーブルにします。このコンフィギュレーションでは、リモート ユーザは、ブラウザに https://<outside_ip>:444 を入力してクライアントレス SSL VPN セッションを開始します。
ステップ 3	**http server enable** **例：** hostname(config)# **http server enable** hostname(config)# **http 192.168.3.0 255.255.255.0 outside** hostname(config)# **webvpn** hostname(config-webvpn)# **enable outside**	（特権モード）ASDM のリスニング ポートを変更します。 HTTPS ASDM セッションが外部インターフェイスのポート 444 を使用することを指定します。クライアントレス SSL VPN も外部インターフェイスでイネーブルになり、デフォルト ポート（443）を使用します。このコンフィギュレーションでは、リモート ユーザは https://<outside_ip>:444 を入力して ASDM セッションを開始します。

プロキシ サーバのサポートの設定

ASA は HTTPS 接続を終了して、HTTP および HTTPS 要求をプロキシ サーバに転送できます。これらのサーバは、ユーザとパブリック ネットワークまたはプライベート ネットワーク間を中継する機能を果たします。組織が管理するプロキシ サーバを経由したネットワークへのアクセスを必須にすると、セキュアなネットワーク アクセスを確保して管理面の制御を保証するためのフィルタリング導入の別のきっかけにもなります。

HTTP および HTTPS プロキシ サービスに対するサポートを設定する場合、プリセット クレデンシャルを割り当てて、基本認証に対する各要求とともに送信できます。HTTP および HTTPS 要求から除外する URL を指定することもできます。

制限

プロキシ自動設定（PAC）ファイルを HTTP プロキシ サーバからダウンロードするように指定できますが、PAC ファイルを指定するときにプロキシ認証を使用しない場合があります。

	コマンド	目的
ステップ 1	**webvpn**	クライアントレス SSL VPN コンフィギュレーション モードに切り替えます。
ステップ 2	**http-proxy および https-proxy**	外部プロキシ サーバを使用して HTTP および HTTPS 要求を処理するように ASA を設定します。 **（注）** プロキシ NTLM 認証は **http-proxy** ではサポートされていません。認証なしのプロキシと基本認証だけがサポートされています。
ステップ 3	**http-proxy** *host* [*port*] [**exclude** *url*] [**username** *username* {**password** *password*}]	HTTP プロキシを設定します。
ステップ 4	**https-proxy** *host* [*port*] [**exclude** *url*] [**username** *username* {**password** *password*}]	HTTPS プロキシを設定します。
ステップ 5	**http-proxy pac** *url*	PAC ファイル URL を設定します。
ステップ 6	（オプション） exclude	URL をプロキシ サーバに送信される可能性がある URL から除外します。
ステップ 7	*host*	外部プロキシ サーバのホスト名または IP アドレスを指定します。
ステップ 8	pac	ASA にダウンロードされた、各 URL のプロキシを識別するために JavaScript 機能を使用するプロキシ自動コンフィギュレーション ファイル。
ステップ 9	（任意。ユーザ名を指定した場合にのみ使用可能） password	基本的なプロキシ認証を提供するためにパスワードとともに各プロキシ要求と一緒に送信します。
ステップ 10	*password*	各 HTTP または HTTPS 要求とともにプロキシ サーバに送信するパスワード。
ステップ 11	（オプション） *port*	プロキシ サーバが使用するポート番号を指定します。デフォルトの HTTP ポートは 80 です。デフォルトの HTTPS ポートは 443 です。代替値を指定しない場合、ASA はこれらの各ポートを使用します。範囲は 1 ～ 65535 です。

	コマンド	目的
ステップ 12	*url*	**exclude** を入力した場合は、プロキシ サーバに送信される可能性がある URL から除外する URL またはカンマで区切った複数の URL のリストを入力します。このストリングには文字数の制限はありませんが、コマンド全体で 512 文字以下となるようにする必要があります。リテラル URL を指定するか、次のワイルドカードを使用できます。 – * は、スラッシュ（/）とピリオド（.）を含む任意の文字列と一致します。このワイルドカードは、英数字ストリングとともに使用する必要があります。 – **?**は、スラッシュおよびピリオドを含む、任意の 1 文字に一致します。 – [*x*-*y*] は、*x* から *y* の範囲にある任意の 1 文字に一致します。ここで、*x* は ANSI 文字セット内の 1 文字を、*y* は ANSI 文字セット内の別の 1 文字を示します。 – [**!***x*-*y*] は、この範囲内に存在しない任意の 1 文字に一致します。
ステップ 13	**http-proxy pac** を入力した場合、**http://** に続けてプロキシ自動設定ファイルの URL を入力します（**http://** の部分を省略すると、CLI はコマンドを無視します）。	—
ステップ 14	（オプション） `username`	基本的なプロキシ認証のためにユーザ名とともに各 HTTP プロキシ要求と一緒に送信します。このキーワードは、**http-proxy** *host* コマンドでのみサポートされています。
ステップ 15	*username*	各 HTTP または HTTPS 要求とともにプロキシ サーバに送信するユーザ名。
ステップ 16	**例：** `hostname(config-webvpn)# http-proxy 209.165.201.1 user jsmith password mysecretdonttell` `hostname(config-webvpn)`	次の設定の HTTP プロキシ サーバの使用を設定する方法を示します。IP アドレスが 209.165.201.1 で、デフォルト ポートを使用し、各 HTTP 要求とともにユーザ名とパスワードを送信する。
ステップ 17	**例：** `hostname(config-webvpn)# http-proxy 209.165.201.1 exclude www.example.com username jsmith password mysecretdonttell` `hostname(config-webvpn)`	同じコマンドの例を示しますが、前の例とは異なり、この例では、ASA が HTTP 要求で www.example.com という特定の URL を受信した場合には、プロキシ サーバに渡すのではなく自分自身で要求を解決します。
ステップ 18	**例：** `hostname(config-webvpn)# http-proxy pac http://www.example.com/pac` `hostname(config-webvpn)`	ブラウザにプロキシ自動設定ファイルを提供する URL を指定する方法を示します。

ASA クライアントレス SSL VPN コンフィギュレーションは、それぞれ 1 つの **http-proxy** コマンドと 1 つの **https-proxy** コマンドのみサポートしています。たとえば、**http-proxy** コマンドの 1 インスタンスが実行コンフィギュレーションにすでに存在する場合に別のコマンドを入力すると、CLI が前のインスタンスを上書きします。

（注）　プロキシ NTLM 認証は **http-proxy** ではサポートされていません。認証なしのプロキシと基本認証だけがサポートされています。

SSL/TLS 暗号化プロトコルの設定

ポート転送には、Oracle Java ランタイム環境（JRE）が必要です。クライアントレス SSL VPN のユーザがいくつかの SSL バージョンに接続する場合、ポート転送は機能しません。サポートされている JRE バージョンについては、「compatibility matrix」を参照してください。

デジタル証明書による認証

SSL はデジタル証明書を使用して認証を行います。ASA は、ブート時に自己署名の SSL サーバ証明書を作成します。または、PKI コンテキストで発行された SSL 証明書を ASA にインストールできます。HTTPS の場合、この証明書をクライアントにインストールする必要があります。

制限

MS Outlook、MS Outlook Express、Eudora などの電子メール クライアントは、証明書ストアにアクセスできません。

デジタル証明書を使用する認証と認可については、一般的な操作のコンフィギュレーション ガイドの証明書とユーザ ログイン クレデンシャルの使用に関する項を参照してください。

クライアント/サーバ プラグインへのブラウザ アクセスの設定

[Client-Server Plug-in] テーブルには、ASA によってクライアントレス SSL VPN セッションのブラウザで使用できるようになるプラグインが表示されます。

プラグインを追加、変更、または削除するには、次のいずれかを実行します。

- プラグインを追加するには、**[Import]** をクリックします。[Import Plug-ins] ダイアログボックスが開きます。
- プラグインを削除するには、そのプラグインを選択して **[Delete]** をクリックします。

次の項では、クライアントレス SSL VPN のブラウザ アクセス用のブラウザ プラグインの統合について説明します。

- ブラウザ プラグインのインストールについて
- プラグインのためのセキュリティ アプライアンスの準備
- シスコによって再配布されたプラグインのインストール

ブラウザ プラグインのインストールについて

ブラウザ プラグインは、Web ブラウザによって呼び出される独立したプログラムで、ブラウザ ウィンドウ内でクライアントをサーバに接続するなどの専用の機能を実行します。ASA により、クライアントレス SSL VPN セッションでリモート ブラウザにダウンロードするためのプラグインをインポートできます。通常、シスコでは再配布するプラグインのテストを行っており、再配布できないプラグインの接続性をテストする場合もあります。ただし、現時点では、ストリーミング メディアをサポートするプラグインのインポートは推奨しません。

プラグインをフラッシュ デバイスにインストールすると、ASA は次の処理を実行します。

- （シスコが配布したプラグインのみ）*URL* で指定した jar ファイルを解凍する。
- ASA ファイル システムの csco-config/97/plugin ディレクトリにファイルを書き込む。
- ASDM の URL 属性の横にあるドロップダウン リストに情報を入力します。
- 以後のすべてのクライアントレス SSL VPN セッションでプラグインをイネーブルにし、メイン メニュー オプションと、ポータル ページの [Address] フィールドの横にあるドロップダウン リストについてのオプションを追加します。

  表 14-3 に、次の項で説明するプラグインを追加したときの、ポータル ページのメイン メニューと [Address] フィールドの変更点を示します。

表 14-3　　クライアントレス SSL VPN ポータル ページへのプラグインの影響

プラグイン	ポータル ページに追加されるメイン メニュー オプション	ポータル ページに追加される [Address] フィールド オプション
ica	Citrix Client	citrix://
rdp	Terminal Servers	rdp://
rdp2	Terminal Servers Vista	rdp2://
ssh,telnet	SSH	ssh://
	Telnet	telnet://
vnc	VNC Client	vnc://

（注） セカンダリ ASA は、プライマリ ASA からプラグインを取得します。

クライアントレス SSL VPN セッションでユーザがポータル ページの関連付けられたメニュー オプションをクリックすると、ポータル ページにはインターフェイスへのウィンドウとヘルプ ペインが表示されます。ドロップダウン リストに表示されたプロトコルをユーザが選択して [Address] フィールドに URL を入力すると、接続を確立できます。

（注） Java プラグインによっては、宛先サービスへのセッションが設定されていない場合でも、接続済みまたはオンラインというステータスがレポートされることがあります。open-source プラグインは、ASA ではなくステータスをレポートします。

1 つ目のプラグインをインストールする前に、次の項の指示に従う必要があります。

前提条件

- セキュリティ アプライアンスでクライアントレス セッションがプロキシ サーバを使用するように設定している場合、プラグインは機能しません。

（注）　Remote Desktop Protocol プラグインでは、セッション ブローカを使用したロード バランシングはサポートされていません。プロトコルによるセッション ブローカからのリダイレクションの処理方法のため、接続に失敗します。セッション ブローカが使用されていない場合、プラグインは動作します。

- プラグインは、シングル サインオン（SSO）をサポートします。プラグインは、クライアントレス SSL VPN セッションを開くときに入力したクレデンシャルと*同じ*クレデンシャルを使用します。プラグインはマクロ置換をサポートしないため、内部ドメイン パスワードなどのさまざまなフィールドや、RADIUS または LDAP サーバの属性で SSO を実行するオプションはありません。
- プラグインに対して SSO サポートを設定するには、プラグインをインストールし、サーバへのリンクを表示するためのブックマーク エントリを追加します。また、ブックマークを追加するときに、SSO サポートを指定します。
- リモートで使用するために必要な最低限のアクセス権は、ゲスト特権モードに属しています。

要件

- シスコでは、GNU 一般公的使用許諾（GPL）に従い、変更を加えることなくプラグインを再配布しています。GPL により、これらのプラグインを直接改良できません。
- プラグインへのリモート アクセスを提供するには、ASA でクライアントレス SSL VPN をイネーブルにする必要があります。
- ステートフル フェールオーバーが発生すると、プラグインを使用して確立されたセッションは保持されません。ユーザはフェールオーバー後に再接続する必要があります。
- プラグインには、ActiveX または Oracle Java ランタイム環境（JRE）1.4.2（以降）がブラウザでイネーブルになっている必要があります。64 ビット ブラウザには、RDP プラグインの ActiveX バージョンはありません。

RDP プラグイン ActiveX デバッグのクイック リファレンス

RDP プラグインをセットアップして使用するには、新しい環境変数を追加する必要があります。

ステップ 1　**[My Computer]** を右クリックし、[System Properties] を開いて **[Advanced]** タブを選択します。

ステップ 2　[Advanced] タブで、[Environment Variables] ボタンを選択します。

ステップ 3　[New User Variable] ダイアログボックスで、RF_DEBUG 変数を入力します。

ステップ 4　[User variables] セクションの新しい環境変数を確認します。

ステップ 5　バージョン 8.3 以前のクライアントレス SSL VPN のバージョンでクライアント コンピュータを使用していた場合、古い Cisco Portforwarder Control を削除してください。C:/WINDOWS/Downloaded Program Files ディレクトリを開いて、Portforwarder Control を右クリックして、**[Remove]** を選択します。

ステップ 6　Internet Explorer ブラウザのすべてのキャッシュをクリアします。

ステップ 7　クライアントレス SSL VPN セッションを起動して、RDP ActiveX プラグインを使用して RDP セッションを確立します。

これで Windows アプリケーションのイベント ビューアでイベントを確認できるようになります。

プラグインのためのセキュリティ アプライアンスの準備

ステップ 1　クライアントレス SSL VPN が ASA インターフェイスでイネーブルになっていることを確認します。

ステップ 2　リモート ユーザが完全修飾ドメイン名（FQDN）を使用して接続する ASA インターフェイスに SSL 証明書をインストールします。

（注）　SSL 証明書の一般名（CN）として IP アドレスを指定しないでください。リモート ユーザは、ASA と通信するために FQDN の使用を試行します。リモート PC は、DNS または System32\drivers\etc\hosts ファイル内のエントリを使用して、FQDN を解決できる必要があります。

ASA で新しい HTML ファイルを使用するための設定

手順の詳細

	コマンド	目的
ステップ 1	**import webvpn webcontent <file> <url>** **例：** hostname# **import webvpn webcontent /+CSCOU+/login.inc tftp://209.165.200.225/login.inc** !!!!* Web resource `+CSCOU+/login.inc' was successfully initialized hostname#	ファイルおよびイメージを Web コンテンツとしてインポートします。
ステップ 2	**export webvpn customization <file> <URL>** **例：** hostname2# **export webvpn customization template tftp://209.165.200.225/sales_vpn_login** !!! %INFO: Customization object 'Template' was exported to tftp://10.21.50.120/sales_vpn_login	カスタマイゼーション テンプレートをエクスポートします。

	コマンド	目的
ステップ 3	ファイル内の full customization mode タグを enable に変更します。 **例：** `<full-customization>` `<mode>`**`enable`**`</mode>` `<url>`**`/+CSCOU+/login.inc`**`</url>` `</full-customization>`	ASA メモリに格納されているログイン ファイルの URL を指定します。
ステップ 4	ファイルを新しいカスタマイゼーション オブジェクトとしてインポートします。 **例：** `hostname#` **`import webvpn customization sales_vpn_login tftp://10.21.50.120/sales_vpn_login`**`$` `!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!` `%INFO: customization object 'sales_vpn_login' was successfully imported`	—
ステップ 5	接続プロファイル（トンネル グループ）にカスタマイゼーション オブジェクトを適用します。 **例：** `hostname(config)#` **`tunnel-group Sales webvpn-attributes`** `hostname(config-tunnel-webvpn)#`**`customization sales_vpn_login`**	—

CHAPTER 15

高度なクライアントレス SSL VPN のコンフィギュレーション

2013 年 9 月 13 日

Microsoft Kerberos Constrained Delegation ソリューション

多くの組織では、現在 ASA SSO 機能によって提供される以上の認証方式を使用して、クライアントレス VPN ユーザを認証し、ユーザの認証クレデンシャルを Web ベースのリソースにシームレスに拡張する必要があります。スマート カードおよびワンタイム パスワード（OTP）を使用したリモート アクセス ユーザの認証に対する要求が大きくなっていますが、SSO 機能ではこの要求を満たすには不十分です。SSO 機能では、認証が必要になると、従来のユーザ クレデンシャル（スタティックなユーザ名とパスワードなど）をクライアントレス Web ベースのリソースに転送するだけであるためです。

たとえば、証明書ベースまたは OTP ベースの認証方式には、ASA が Web ベースのリソースへの SSO アクセスをシームレスに実行するために必要な従来のユーザ名とパスワードは含まれていません。証明書を使用して認証する場合、ASA が Web ベースのリソースへ拡張するためにユーザ名とパスワードは必要ありません。そのため、SSO でサポートされない認証方式になっています。これに対し、OTP にはスタティックなユーザ名が含まれていますが、パスワードはダイナミックであり、VPN セッション中に後で変更されます。一般に、Web ベースのリソースはスタティックなユーザ名とパスワードを受け入れるように設定されるため、OTP も SSO でサポートされない認証方式になっています。

Microsoft の Kerberos Constrained Delegation（KCD）は、ASA のソフトウェア リリース 8.4 で導入された新機能であり、プライベート ネットワーク内の Kerberos で保護された Web アプリケーションへのアクセスを提供します。この利点により、証明書ベースおよび OTP ベースの認証方式を Web アプリケーションにシームレスに拡張できます。したがって、SSO と KCD は独立しながら連携し、多くの組織では、ASA でサポートされるすべての認証方式を使用して、クライアントレス VPN ユーザを認証し、ユーザの認証クレデンシャルを Web アプリケーションにシームレスに拡張できます。

要件

kcd-server コマンドが機能するには、ASA はソースドメイン（ASA が常駐するドメイン）とターゲットまたはリソースドメイン（Web サービスが常駐するドメイン）間の信頼関係を確立する必要があります。ASA は、その独自のフォーマットを使用して、サービスにアクセスするリモート アクセス ユーザの代わりに、ソースから宛先ドメインへの認証パスを越えて、必要なチケットを取得します。

このように認証パスを越えることは、クロスレルム認証と呼ばれます。クロスレルム認証の各フェーズで、ASA は特定のドメインのクレデンシャルおよび後続のドメインとの信頼関係に依存しています。

KCD の機能概要

Kerberos は、ネットワーク内のエンティティのデジタル識別情報を検証するために、信頼できる第三者に依存しています。これらのエンティティ（ユーザ、ホスト マシン、ホスト上で実行されるサービスなど）は、プリンシパルと呼ばれ、同じドメイン内に存在している必要があります。秘密キーの代わりに、Kerberos では、サーバに対するクライアントの認証にチケットが使用されます。チケットは秘密キーから導出され、クライアントのアイデンティティ、暗号化されたセッション キー、およびフラグで構成されます。各チケットはキー発行局によって発行され、ライフタイムが設定されます。

Kerberos セキュリティ システムは、エンティティ（ユーザ、コンピュータ、またはアプリケーション）を認証するために使用されるネットワーク認証プロトコルであり、情報の受け手として意図されたデバイスのみが復号化できるようにデータを暗号化することによって、ネットワーク伝送を保護します。クライアントレス SSL VPN ユーザに Kerberos で保護された任意の Web サービスへの SSO アクセスを提供するように KCD を設定できます。このような Web サービスやアプリケーションの例として、Outlook Web Access（OWA）、SharePoint、および Internet Information Server（IIS）があります。

Kerberos プロトコルに対する 2 つの拡張機能として、*プロトコル移行*および*制約付き委任*が実装されました。これらの拡張機能によって、クライアントレス SSL VPN リモート アクセス ユーザは、プライベート ネットワーク内の Kerberos で認証されるアプリケーションにアクセスできます。

*プロトコル移行*では、ユーザ認証レベルでさまざまな認証メカニズムをサポートし、後続のアプリケーション レイヤでセキュリティ機能（相互認証や制約付き委任など）について Kerberos プロトコルに切り替えることによって、柔軟性とセキュリティが強化されます。*制約付き委任*では、ドメイン管理者は、アプリケーションがユーザの代わりを務めることができる範囲を制限することによって、アプリケーション信頼境界を指定して強制適用できます。この柔軟性は、信頼できないサービスによる危険の可能性を減らすことで、アプリケーションのセキュリティ設計を向上させます。

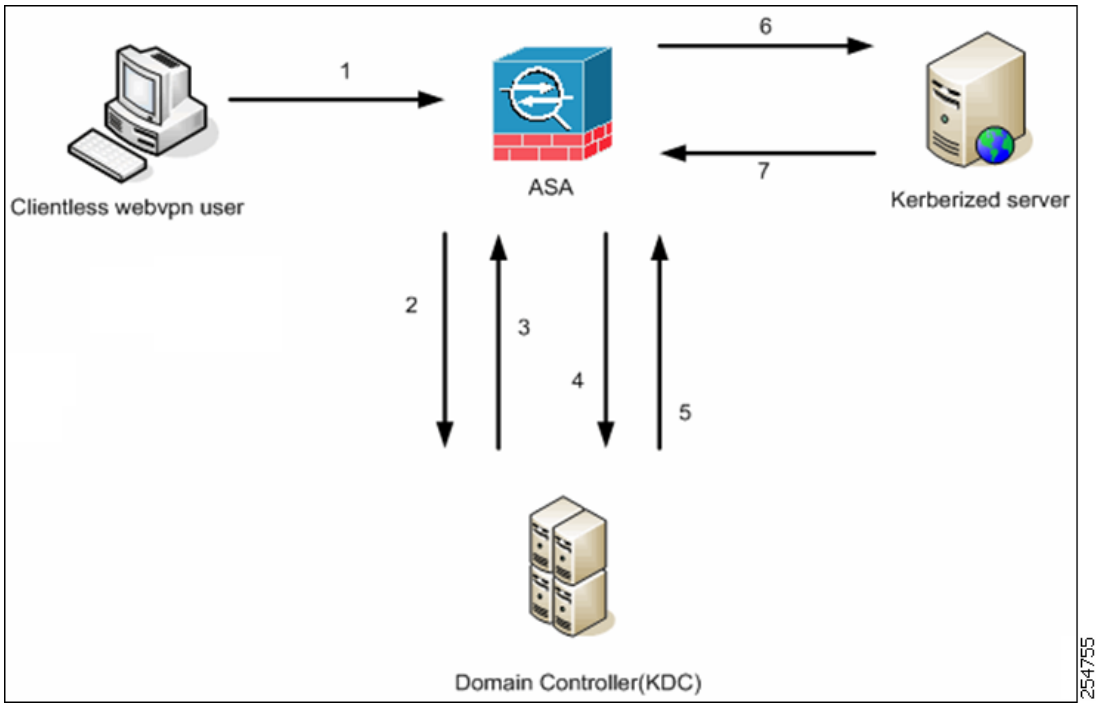
制約付き委任の詳細については、IETF の Web サイト（http://www.ietf.org）にアクセスして、RFC 1510 を参照してください。

KCD の認証フロー

図 15-1 に、委任に対して信頼されたリソースにユーザがクライアントレス ポータルによってアクセスするときに、直接的および間接的に体験するパケットおよびプロセス フローを示します。このプロセスは、次のタスクが完了していることを前提としています。

- ASA 上で設定された KCD
- Windows Active Directory への参加、およびサービスが委任に対して信頼されたことの確認
- Windows Active Directory ドメインのメンバーとして委任された ASA

図 15-1　　KCD プロセス



（注） クライアントレス ユーザ セッションが、ユーザに設定されている認証メカニズムを使用して ASA により認証されます （スマートカード クレデンシャルの場合、ASA によって、デジタル証明書の userPrincipalName を使用して Windows Active Directory に対して LDAP 認可が実行されます）。

1. 認証が成功すると、ユーザは、ASA クライアントレス ポータル ページにログインします。ユーザは、URL をポータル ページに入力するか、ブックマークをクリックして、Web サービスにアクセスします。この Web サービスで認証が必要な場合、サーバは、ASA クレデンシャルの認証確認を行い、サーバでサポートされている認証方式のリストを送信します。

   （注）　クライアントレス SSL VPN の KCD は、すべての認証方式（RADIUS、RSA/SDI、LDAP、デジタル証明書など）に対してサポートされています。次の AAA のサポートに関する表を参照してください。
   http://www.cisco.com/en/US/docs/security/asa/asa84/configuration/guide/access_aaa.html#wp1069492

2. 認証確認時の HTTP ヘッダーに基づいて、ASA は、サーバで Kerberos 認証が必要かどうかを決定します （これは SPNEGO メカニズムの一部です）。バックエンド サーバとの接続で、Kerberos 認証が必要な場合、ASA は、ユーザの代わりにそれ自体のために、サービス チケットをキー発行局から要求します。
3. キー発行局は、要求されたチケットを ASA に返します。これらのチケットは ASA に渡されますが、ユーザの認可データが含まれています。ASA は、ユーザがアクセスする特定のサービス用の KDC からのサービス チケットを要求します。

   （注）　ステップ 1 ～ 3 では、プロトコル移行が行われます。これらのステップの後、Kerberos 以外の認証プロトコルを使用して ASA に対して認証を行うユーザは、透過的に、Kerberos を使用してキー発行局に対して認証されます。

4. ASA は、ユーザがアクセスする特定のサービス用のキー発行局からのサービス チケットを要求します。
5. キー発行局は、特定のサービスのサービス チケットを ASA に返します。
6. ASA は、サービス チケットを使用して、Web サービスへのアクセスを要求します。
7. Web サーバは、Kerberos サービス チケットを認証して、サービスへのアクセスを付与します。認証が失敗した場合は、適切なエラー メッセージが表示され、確認を求められます。Kerberos 認証が失敗した場合、予期された動作は基本認証にフォールバックします。

KCD を設定する前に

クロスレルム認証用に ASA を設定するには、次のコマンドを使用する必要があります。

	コマンド	目的
ステップ 1	**ntp** hostname **例：** hostname(config)# **configure terminal** #Create an alias for the Domain Controller hostname(config)# **name 10.1.1.10 DC** #Configure the Name server	Active Directory ドメインに参加します。 （インターフェイス内で到達可能な）10.1.1.10 ドメイン コントローラ。

	コマンド	目的
ステップ 2	**dns domain-lookup** **dns server-group** 例： hostname(config)# **ntp server DC** #Enable a DNS lookup by configuring the DNS server and Domain name hostname(config)# **dns domain-lookup inside** hostname(config)# **dns server-group DefaultDNS** hostname(config-dns-server-group)# **name-server DC** hostname(config-dns-server-group)# **domain-name private.net** #Configure the AAA server group with Server and Realm hostname(config)# **aaa-server KerberosGroup protocol Kerberos** hostname(config-asa-server-group)# **aaa-server KerberosGroup (inside) host DC** hostname(config-asa-server-group)# **Kerberos-realm PRIVATE.NET** #Configure the Domain Join hostname(config)# **webvpn** hostname(config-webvpn)# **kcd-server KerberosGroup username dcuser password dcuser123!** hostname(config)#	検索を実行します。 private.net のドメイン名、およびユーザ名 dcuser、パスワード dcuser123! を使用するドメイン コントローラの サービス アカウント。

KCD の設定

ASA を Windows Active Directory ドメインに参加させ、成功または失敗のステータスを返すには、次の手順を実行します。

手順の詳細

	コマンド	目的
ステップ 1	**webvpn**	クライアントレス SSL VPN コンフィギュレーション モードに切り替えます。
ステップ 2	**kcd-server**	KCD を設定します。

	コマンド	目的
ステップ 3	**kcd-server** *aaa-server-group* **例：** ASA(config)# **aaa-server KG protocol kerberos** ASA(config)# **aaa-server KG (inside) host DC** ASA(config-aaa-server-host)# **kerberos-realm test.edu** ASA(webvpn-config)# **kcd-server KG username user1 password abc123** ASA(webvpn-config)# **no kcd-server**	ドメイン コントローラ名およびレルムを指定します。AAA サーバ グループは、Kerberos タイプである必要があります。
ステップ 4	（オプション） **no kcd-server**	ASA の指定した動作を削除します。
ステップ 5	（オプション） **kcd-server reset**	内部状態にリセットします。
ステップ 6	**kcd domain-join username** <*user*> **password** <*pass*> user：特定の管理ユーザには対応せず、単に Windows ドメイン コントローラでデバイスを追加するためのサービス レベル権限を持つユーザに対応します。 pass：パスワードは、特定のパスワードには対応せず、単に Windows のドメイン コントローラでデバイスを追加するためのサービス レベル パスワード権限を持つユーザに対応します。	KCD サーバが表示されていることを確認し、ドメイン参加プロセスを開始します。 Active Directory のユーザ名とパスワードは EXEC モードでだけ使用され、設定には保存されません。 **（注）** 最初の参加には、管理者権限が必要です。ドメイン コントローラのサービス レベル権限を持つユーザはアクセスできません。
ステップ 7	kcd domain-leave	KCD サーバ コマンドが有効なドメイン参加ステータスを持っているかどうかを確認し、ドメイン脱退を開始します。

KCD ステータス情報の表示

ドメイン コントローラ情報およびドメイン参加ステータスを表示するには、次の手順を実行します。

	コマンド	目的
ステップ 8	**show webvpn kcd** **例：** ASA# show webvpn kcd KCD-Server Name: DC User : user1 Password : **** KCD State : Joined	ドメイン コントローラの情報およびドメイン参加ステータスを表示します。

キャッシュされた Kerberos チケットの表示

ASA でキャッシュされているすべての Kerberos チケットを表示するには、次のコマンドを入力します。

	コマンド	目的
ステップ 9	**show aaa kerberos**	ASA でキャッシュされているすべての Kerberos チケットを表示します。
ステップ 10	**show aaa kerberos [username *user* | host *ip* | *hostname*]** **例：** ASA# **show aaa kerberos** Default Principal Valid Starting Expires Service Principal asa@example.COM 10/06/29 18:33:00 10/06/30 18:33:00 krbtgt/example.COM@example.COM kcduser@example.COM10/06/29 17:33:00 10/06/30 17:33:00 asa$/example.COM@example.COM kcduser@example.COM10/06/29 17:33:00 10/06/30 17:33:00 http/owa.example.com@example.COM ASA# show aaa kerberos username kcduser Default Principal Valid Starting Expires Service Principal kcduser@example.COM10/06/29 17:33:00 10/06/30 17:33:00 asa$/example.COM@example.COM kcduser@example.COM10/06/29 17:33:00 10/06/30 17:33:00 http/owa.example.com@example.COM ASA# show aaa kerberos host owa.example.com Default Principal Valid Starting Expires Service Principal kcduser@example.COM10/06/2910/06/30 17:33:00 http/owa.example.com@example.COM ASA# show aaa kerberos username kcduser Default Principal Valid Starting Expires Service Principal kcduser@example.COM10/06/29 17:33:00 10/06/30 17:33:00 asa$/example.COM@example.COM kcduser@example.COM10/06/29 17:33:00 10/06/30 17:33:00 http/owa.example.com@example.COM ASA# show aaa kerberos host owa.example.com Default Principal Valid Starting Expires Service Principal kcduser@example.COM10/06/29 10/06/30 17:33:00 http/owa.example.com@example.COM	• user：特定のユーザの Kerberos チケットの表示に使用します。 • hostname：特定のホストに発行された Kerberos チケットの表示に使用します。

キャッシュされた Kerberos チケットのクリア

ASA のすべての Kerberos チケット情報をクリアするには、次の手順を実行します。

	コマンド	目的
ステップ 11	`clear aaa kerberos`	ASA のすべての Kerberos チケット情報をクリアします。
ステップ 12	`clear aaa kerberos [username` *user* `| host` *ip* `|` *hostname*`]`	• *user*：特定のユーザの Kerberos チケットのクリアに使用します。 • *host*：特定のホストの Kerberos チケットのクリアに使用します。

アプリケーション プロファイル カスタマイゼーション フレームワークの設定

クライアントレス SSL アプリケーション プロファイル カスタマイゼーション フレームワーク（APCF）オプションにより、ASA は標準以外のアプリケーションや Web リソースを処理し、クライアントレス SSL VPN 接続で正しく表示できます。APCF プロファイルには、特定のアプリケーションに関して、いつ（事前、事後）、どこの（ヘッダー、本文、要求、応答）、何（データ）を変換するかを指定するスクリプトがあります。スクリプトは XML 形式で記述され、sed（ストリーム エディタ）の構文を使用して文字列およびテキストを変換します。

ASA では複数のAPCF プロファイルを並行して設定および実行できます。1 つの APCF プロファイルのスクリプト内に複数の APCF ルールを適用することができます。ASA は、設定履歴に基づいて最も古いルールを最初に処理し、次に 2 番目に古いルールを処理します。

APCF プロファイルは、ASA のフラッシュ メモリ、HTTP サーバ、HTTPS サーバ、または TFTP サーバに保存できます。

制限

APCF プロファイルは、シスコの担当者のサポートが受けられる場合のみ設定することをお勧めします。

APCF パケットの管理

手順の詳細

	コマンド	目的
ステップ 1	**webvpn**	クライアントレス SSL VPN コンフィギュレーション モードに切り替えます。
ステップ 2	**apcf** **例：** hostname(config)# **webvpn** hostname(config-webvpn)# **apcf flash:/apcf/apcf1.xml** hostname(config)# **webvpn** hostname(config-webvpn)# **apcf** **https://myserver:1440/apcf/apcf2.xml**	ASA 上にロードする APCF プロファイルを特定および検索します。 フラッシュ メモリに保存されている apcf1.xml という名前の APCF プロファイルをイネーブルにする方法を示します。 ポート番号 1440、パスが /apcf の myserver という名前の HTTPS サーバにある APCF プロファイル apcf2.xml をイネーブルにする方法を示します。

APCF 構文

APCF プロファイルは、XML フォーマットおよび sed スクリプトの構文を使用します。表 15-1 に、この場合に使用する XML タグを示します。

ガイドライン

APCF プロファイルの使い方を誤ると、パフォーマンスが低下したり、好ましくない表現のコンテンツになる場合があります。シスコのエンジニアリング部では、ほとんどの場合、APCF プロファイルを提供することで特定アプリケーションの表現上の問題を解決しています。

表 15-1　APCF XML タグ

タグ	使用目的
<APCF>...</APCF>	すべての APCF XML ファイルを開くための必須のルート要素。
<version>1.0</version>	APCF の実装バージョンを指定する必須のタグ。現在のバージョンは 1.0 だけです。
<application>...</application>	XML 記述の本文を囲む必須タグ。
<id> text </id>	この特定の APCF 機能を記述する必須タグ。
<apcf-entities>...</apcf-entities>	単一または複数の APCF エンティティを囲む必須タグ。

表 15-1　APCF XML タグ（続き）

タグ	使用目的
<js-object>…</js-object> <html-object>…</html-object> <process-request-header>...</process-request-header> <process-response-header>...</process-response-header> <preprocess-response-body>...</preprocess-response-body> <postprocess-response-body>...</postprocess-response-body>	これらのタグのうちの 1 つが、コンテンツの種類または APCF 処理が実施される段階を指定します。
<conditions>… </conditions>	処理前および処理後の子要素タグで、次の処理基準を指定します。 • http-version（1.1、1.0、0.9 など） • http-method（get、put、post、webdav） • http-scheme（"http/"、"https/"、その他） • server-regexp（"a".."z" | "A".."Z" | "0".."9" | ".-_*[]?" を含む正規表現） • server-fnmatch（"a".."z" | "A".."Z" | "0".."9" | ".-_*[]?+()\{}," を含む正規表現） • user-agent-regexp • user-agent-fnmatch • request-uri-regexp • request-uri-fnmatch • 条件タグのうち 2 つ以上が存在する場合は、ASA はすべてのタグに対して論理 AND を実行します。
<action> … </action>	指定した条件で 1 つ以上のアクションをコンテンツでラップします。これらのアクションを定義するには、次のタグを使用できます（下記参照）。 • <do> • <sed-script> • <rewrite-header> • <add-header> • <delete-header>

表 15-1　APCF XML タグ（続き）

タグ	使用目的
<do>…</do>	次のいずれかのアクションの定義に使用されるアクション タグの子要素です。 • <no-rewrite/>：リモート サーバから受信したコンテンツを上書きしません。 • <no-toolbar/>：ツールバーを挿入しません。 • <no-gzip/>：コンテンツを圧縮しません。 • <force-cache/>：元のキャッシュ命令を維持します。 • <force-no-cache/>：オブジェクトをキャッシュできないようにします。 • < downgrade-http-version-on-backend>：リモート サーバに要求を送信するときに HTTP/1.0 を使用します。
<sed-script> TEXT </sed-script>	テキストベースのオブジェクトのコンテンツの変更に使用されるアクション タグの子要素です。TEXT は有効な Sed スクリプトである必要があります。<sed-script> は、これより前に定義された <conditions> タグに適用されます。
<rewrite-header></rewrite-header>	アクション タグの子要素です。<header> の子要素タグで指定された HTTP ヘッダーの値を変更します（以下を参照してください）。
<add-header></add-header>	<header> の子要素タグで指定された新しい HTTP ヘッダーの追加に使用されるアクション タグの子要素です（以下を参照してください）。
<delete-header></delete-header>	<header> の子要素タグで指定された特定の HTTP ヘッダーの削除に使用されるアクション タグの子要素です（以下を参照してください）。
<header></header>	上書き、追加、または削除される HTTP ヘッダー名を指定します。たとえば、次のタグは Connection という名前の HTTP ヘッダーの値を変更します。 <rewrite-header> <header>Connection</header> <value>close</value> </rewrite-header>

APCF の設定例

例：

```
<APCF>
<version>1.0</version>
<application>
  <id>Do not compress content from example.com</id>
  <apcf-entities>
      <process-request-header>
         <conditions>
           <server-fnmatch>*.example.com</server-fnmatch>
         </conditions>
```

```
            <action>
              <do><no-gzip/></do>
            </action>
      </process-request-header>
  </apcf-entities>
</application>
</APCF>
```

例：

```
<APCF>
<version>1.0</version>
<application>
 <id>Change MIME type for all .xyz objects</id>
 <apcf-entities>
      <process-response-header>
        <conditions>
            <request-uri-fnmatch>*.xyz</request-uri-fnmatch>
        </conditions>
         <action>
           <rewrite-header>
                <header>Content-Type</header>
                <value>text/html</value>
           </rewrite-header>
         </action>
      </process-response-header>
 </apcf-entities>
</application>
</APCF>
```

エンコーディング

エンコーディングを使用すると、クライアントレス SSL VPN ポータル ページの文字エンコーディングを表示または指定できます。

*文字エンコーディング*は「文字コード」や「文字セット」とも呼ばれ、raw データ（0 や 1 など）を文字と組み合わせ、データを表します。使用する文字エンコード方式は、言語によって決まります。単一の方式を使う言語もあれば、使わない言語もあります。通常は、地域によってブラウザで使用されるデフォルトのコード方式が決まりますが、リモート ユーザが変更することもできます。ブラウザはページに指定されたエンコードを検出することもでき、そのエンコードに従ってドキュメントを表示します。

エンコード属性によりポータル ページで使用される文字コード方式の値を指定することで、ユーザがブラウザを使用している地域や、ブラウザに対する何らかの変更に関係なく、ページが正しく表示されるようにできます。

デフォルトでは、ASA は「Global Encoding Type」を Common Internet File System（共通インターネット ファイル システム）サーバからのページに適用します。CIFS サーバと適切な文字エンコーディングとのマッピングを、[Global Encoding Type] 属性によってグローバルに、そしてテーブルに示されているファイル エンコーディング例外を使用して個別に行うことにより、ファイル名やディレクトリ パス、およびページの適切なレンダリングが問題となる場合に、CIFS ページが正確に処理および表示できるようにします。

手順の詳細

ステップ 1　[Global Encoding Type] によって、表に記載されている CIFS サーバからの文字エンコーディングを除いて、すべてのクライアントレス SSL VPN ポータル ページが継承する文字エンコーディングが決まります。文字列を入力するか、ドロップダウン リストから選択肢を 1 つ選択します。リストには、最も一般的な次の値だけが表示されます。

- big5
- gb2312
- ibm-850
- iso-8859-1
- shift_jis

（注）　日本語の Shift_jis 文字エンコーディングを使用している場合は、関連付けられている [Select Page Font] ペインの [Font Family] 領域にある [Do Not Specify] をクリックして、このフォント ファミリを削除します。

- unicode
- windows-1252
- none

（注）　[none] をクリックするか、またはクライアントレス SSL VPN セッションのブラウザがサポートしていない値を指定した場合には、ブラウザのデフォルトのコードが使用されます。

最大 40 文字から成り、http://www.iana.org/assignments/character-sets で指定されているいずれかの有効文字セットと同じ文字列を入力できます。このページに示されている文字セットの名前またはエイリアスのいずれかを使用できます。このストリングは、大文字と小文字が区別されません。ASA の設定を保存したときに、コマンド インタープリタが大文字を小文字に変換します。

ステップ 2　エンコーディング要件が「Global Encoding Type」属性設定とは異なる CIFS サーバの名前または IP アドレスを入力します。ASA では、指定した大文字と小文字の区別が保持されますが、名前をサーバと照合するときには大文字と小文字は区別されません。

ステップ 3　CIFS サーバがクライアントレス SSL VPN ポータル ページに対して指定する必要のある文字エンコーディングを選択します。文字列を入力するか、ドロップダウン リストから選択します。リストには、最も一般的な次の値だけが登録されています。

- big5
- gb2312
- ibm-850
- iso-8859-1
- shift_jis

（注）　日本語の Shift_jis 文字エンコーディングを使用している場合は、関連付けられている [Select Page Font] ペインの [Font Family] 領域にある [Do Not Specify] をクリックして、このフォント ファミリを削除します。

- unicode
- windows-1252
- none

[none] をクリックするか、またはクライアントレス SSL VPN セッションのブラウザがサポートしていない値を指定した場合には、ブラウザのデフォルトのコードが使用されます。

最大 40 文字から成り、http://www.iana.org/assignments/character-sets で指定されているいずれかの有効文字セットと同じ文字列を入力できます。このページに示されている文字セットの名前またはエイリアスのいずれかを使用できます。このストリングは、大文字と小文字が区別されません。ASA の設定を保存したときに、コマンド インタープリタが大文字を小文字に変換します。

クライアントレス SSL VPN を介した電子メールの使用

クライアントレス SSL VPN は、電子メールにアクセスする方法をいくつかサポートしています。ここでは、次の方式について説明します。

- 電子メール プロキシの設定
- Web 電子メールの設定：MS Outlook Web App

電子メール プロキシの設定

クライアントレス SSL VPN は、IMAP、POP3、および SMTP 電子メール プロキシをサポートしています。次の属性は、電子メール プロキシ ユーザにグローバルに適用されます。

制限

MS Outlook、MS Outlook Express、Eudora などの電子メール クライアントは、証明書ストアにアクセスできません。

手順の詳細

	コマンド	目的
ステップ 1	**accounting-server-group**	前に設定されているアカウンティング サーバを電子メール プロキシで使用するように指定します。
ステップ 2	**authentication**	電子メール プロキシ ユーザの認証方式を指定します。デフォルト値は次のとおりです。 • IMAP：メールホスト（必須） • POP3：メールホスト（必須） • SMTP：AAA
ステップ 3	**authentication-server-group**	前に設定されている認証サーバを電子メール プロキシで使用するように指定します。デフォルトは LOCAL です。

	コマンド	目的
ステップ 4	**authorization-server-group**	クライアントレス SSL VPN で使用するように事前に設定されている認可サーバを指定します。
ステップ 5	**authorization-required**	ユーザが接続するには、正常に認可される必要があります。デフォルトではオフになっています。
ステップ 6	**authorization-dn-attributes**	認可のユーザ名として使用するピア証明書の DN を指定します。デフォルトの設定は次のとおりです。 • プライマリ属性：CN • セカンダリ属性：OU
ステップ 7	**default-group-policy**	使用するグループ ポリシーの名前を指定します。デフォルトは DfltGrpPolicy です。
ステップ 8	**enable**	指定したインターフェイスでの電子メール プロキシをイネーブルにします。デフォルトではオフになっています。
ステップ 9	**name-separator**	電子メールと VPN のユーザ名とパスワードとの間の区切り記号を定義します。デフォルトはコロン（:）です。
ステップ 10	**outstanding**	未処理の未承認セッションの最大数を設定します。デフォルト値は 20 です。
ステップ 11	**port**	電子メール プロキシがリッスンするポートを設定します。デフォルトは次のとおりです。 • IMAP：143 • POP3：110 • SMTP：25
ステップ 12	**server**	デフォルトの電子メール サーバを指定します。
ステップ 13	**server-separator**	電子メールとサーバ名との間の区切り記号を定義します。デフォルトは@です。

Web 電子メールの設定：MS Outlook Web App

ASA は、Microsoft Outlook Web App to Exchange Server 2010 および Microsoft Outlook Web Access to Exchange Server 2007、2003、および 2000 をサポートしています。

手順の詳細

ステップ 1　アドレス フィールドに電子メール サービスの URL を入力するか、クライアントレス SSL VPN セッションでの関連するブックマークをクリックします。

ステップ 2　プロンプトが表示されたら、電子メール サーバのユーザ名を *domain\username* 形式で入力します。

ステップ 3　電子メール パスワードを入力します。

CHAPTER 16

ポリシー グループ

2014 年 4 月 14 日

リソース アクセスのためのクライアントレス SSL VPN ポリシーの作成と適用

内部サーバにあるリソースへのアクセスを制御するクライアントレス SSL VPN ポリシーを作成および適用するには、次のタスクを実行します。

- グループ ポリシーへのユーザの割り当て

グループ ポリシーへのユーザの割り当て

ユーザをグループ ポリシーに割り当てると、複数のユーザにポリシーを適用することで設定が容易になります。ユーザをグループ ポリシーに割り当てるには、ASA の内部認証サーバ、外部 RADIUS または LDAP サーバを使用できます。グループ ポリシーで設定を簡素化する方法の詳細な説明については、第 4 章の「接続プロファイル、グループ ポリシー、およびユーザ」を参照してください。

クライアントレス SSL VPN の接続プロファイルの属性の設定

表 16-1 は、クライアントレス SSL VPN に固有の接続プロファイル属性のリストです。これらの属性に加えて、すべての VPN 接続に共通の一般接続プロファイルの属性を設定します。接続プロファイルの設定に関する手順ごとの情報については、第 4 章の「接続プロファイル、グループ ポリシー、およびユーザ」を参照してください。

（注） 以前のリリースでは、「接続プロファイル」は「トンネル グループ」と呼ばれていました。**tunnel-group** コマンドを使用して接続プロファイルを設定します。この章では、この 2 つの用語が同義的によく使用されています。

表 16-1　クライアントレス SSL VPN 用接続プロファイルの属性

コマンド	機能
authentication	認証方式を設定します。
customization	適用するすでに定義済みのカスタマイゼーションの名前を指定します。
exit	トンネル グループのクライアントレス SSL VPN 属性コンフィギュレーション モードを終了します。
nbns-server	CIFS 名前解決に使用する NetBIOS ネーム サービス サーバ（nbns-server）の名前を指定します。
group-alias	サーバが接続プロファイルの参照に使用できる代替名を指定します。
group-url	1 つ以上のグループ URL を指定します。この属性で URL を確立すると、ユーザがその URL を使用してアクセスするときにこのグループが自動的に選択されます。
dns-group	DNS サーバ名、ドメイン名、ネーム サーバ、リトライの回数、およびタイムアウト値を指定する DNS サーバ グループを指定します。
help	トンネル グループ コンフィギュレーション コマンドのヘルプを提供します。
hic-fail-group-policy	Cisco Secure Desktop Manager を使用して、グループベース ポリシー属性を「Use Failure Group-Policy」または「Use Success Group-Policy, if criteria match」に設定する場合は、VPN 機能ポリシーを指定します。
no	属性値のペアを削除します。
override-svc-download	AnyConnect VPN クライアントをリモート ユーザにダウンロードするために、設定されているグループ ポリシー属性またはユーザ名属性のダウンロードが上書きされます。
pre-fill-username	このトンネル グループにユーザ名と証明書のバインディングを設定します。
proxy-auth	特定のプロキシ認証トンネル グループとしてこのトンネル グループを識別します。
radius-reject-message	認証が拒否されたときに、ログイン画面に RADIUS 拒否メッセージを表示します。
secondary-pre-fill-username	このトンネル グループにセカンダリ ユーザー名と証明書のバインディングを設定します。
without-csd	トンネル グループの CSD をオフに切り替えます。

クライアントレス SSL VPN のグループ ポリシー属性とユーザ属性の設定

表 16-2 に、クライアントレス SSL VPN のグループ ポリシー属性とユーザ属性のリストを示します。設定グループ ポリシーとユーザ属性の段階を追った手順については、『Cisco ASA シリーズ VPN CLI コンフィギュレーション ガイド』の「グループ ポリシー属性とユーザ属性の設定」または「接続プロファイル、グループ ポリシー、およびユーザ」を参照してください。

表 16-2　クライアントレス SSL VPN のグループ ポリシー属性とユーザ属性

コマンド	機能
activex-relay	クライアントレス SSL VPN セッションを確立したユーザが、ブラウザを使用して Microsoft Office アプリケーションを起動できるようになります。アプリケーションは、セッションを使用して ActiveX のダウンロードとアップロードを行います。ActiveX のリレーは、クライアントレス SSL VPN セッションを終了するまで有効なままです。
auto-sign-on	自動サインオンの値を設定します。設定ではクライアントレス SSL VPN への接続にユーザ名およびパスワードのクレデンシャルが 1 回のみ必要です。
customization	カスタマイゼーション オブジェクトをグループ ポリシーまたはユーザに割り当てます。
deny-message	クライアントレス SSL VPN に正常にログインできるが VPN 特権を持たないリモート ユーザに送信するメッセージを指定します。
file-browsing	ファイル サーバとファイル共有の CIFS ファイル ブラウジングをイネーブルにします。ブラウズには、NBNS（マスター ブラウザまたは WINS）が必要です。
file-entry	アクセスするファイル サーバ名の入力をユーザに許可します。
filter	webtype アクセス リストの名前を設定します。
hidden-shares	非表示の CIFS 共有ファイルの可視性を制御します。
homepage	ログイン時に表示される Web ページの URL を設定します。
html-content-filter	このグループ ポリシー用の HTML からフィルタリングするコンテンツとオブジェクトを設定します。
http-comp	圧縮を設定します。
http-proxy	HTTP 要求の処理に外部プロキシ サーバを使用するように ASA を設定します。 **（注）**　プロキシ NTLM 認証は **http-proxy** ではサポートされていません。認証なしのプロキシと基本認証だけがサポートされています。
keep-alive-ignore	セッション タイマーのアップデートを無視するオブジェクトの最大サイズを設定します。
port-forward	転送するクライアントレス SSL VPN TCP ポートのリストを適用します。ユーザ インターフェイスにこのリストのアプリケーションが表示されます。
post-max-size	ポストするオブジェクトの最大サイズを設定します。
smart-tunnel	スマート トンネルを使用するプログラムと複数のスマート トンネル パラメータのリストを設定します。

表 16-2　クライアントレス SSL VPN のグループ ポリシー属性とユーザ属性（続き）

コマンド	機能
sso-server	SSO サーバの名前を設定します。
storage-objects	セッションとセッションの間に保存されたデータのストレージ オブジェクトを設定します。
svc	SSL VPN クライアント属性を設定します。
unix-auth-gid	UNIX グループ ID を設定します。
unix-auth-uid	UNIX ユーザ ID を設定します。
upload-max-size	アップロードするオブジェクトの最大サイズを設定します。
url-entry	ユーザが HTTP/HTTPS URL を入力する機能を制御します。
url-list	エンドユーザのアクセス用にクライアントレス SSL VPN のポータル ページに表示されるサーバと URL のリストを適用します。
user-storage	セッション間のユーザ データを保存する場所を設定します。

スマート トンネル アクセスの設定

次の項では、クライアントレス SSL VPN セッションでスマート トンネル アクセスをイネーブルにする方法、それらのアクセスを提供するアプリケーションの指定、および使用上の注意について説明します。

スマート トンネル アクセスの設定

スマート トンネル アクセスを設定するには、スマート トンネル リストを作成します。このリストには、スマート トンネル アクセスに適した 1 つ以上のアプリケーション、およびこのリストに関連付けられたエンドポイント オペレーティング システムを含めます。各グループ ポリシーまたはローカル ユーザ ポリシーでは 1 つのスマート トンネル リストがサポートされているため、ブラウザベースではないアプリケーションをサポート対象とするために、グループ化してスマート トンネル リストに加える必要があります。リストを作成したら、1 つ以上のグループ ポリシーまたはローカル ユーザ ポリシーにそのリストを割り当てます。

次の項では、スマート トンネルおよびその設定方法について説明します。

- スマート トンネルについて
- スマート トンネルを使用する理由
- スマート トンネル アクセスに適格なアプリケーションの追加
- スマート トンネル アクセスに適格なアプリケーションの追加
- スマート トンネル リストについて
- スマート トンネルのトンネル ポリシーの設定および適用
- スマート トンネル自動サインオン サーバ リストの作成
- スマート トンネル自動サインオン サーバ リストへのサーバの追加
- スマート トンネル アクセスのイネーブル化とオフへの切り替え

スマート トンネルについて

スマート トンネルは、TCP ベースのアプリケーションとプライベート サイト間の接続です。このスマート トンネルは、セキュリティ アプライアンスをパスウェイとして、また、ASA をプロキシ サーバとして使用するクライアントレス（ブラウザベース）SSL VPN セッションを使用します。スマート トンネル アクセスを許可するアプリケーションを特定し、各アプリケーションのローカル パスを指定できます。Microsoft Windows で実行するアプリケーションの場合は、チェックサムの SHA-1 ハッシュの一致を、スマート トンネル アクセスを許可する条件として要求もできます。

Lotus SameTime および Microsoft Outlook は、スマート トンネル アクセスを許可するアプリケーションの例です。

スマート トンネルを設定するには、アプリケーションがクライアントであるか、Web 対応アプリケーションであるかに応じて、次の手順のいずれかを実行する必要があります。

- クライアント アプリケーションの 1 つ以上のスマート トンネル リストを作成し、スマート トンネル アクセスを必要とするグループ ポリシーまたはローカル ユーザ ポリシーにそのリストを割り当てます。
- スマート トンネル アクセスに適格な Web 対応アプリケーションの URL を指定する 1 つ以上のブックマーク リスト エントリを作成し、スマート トンネル アクセスを必要とするグループ ポリシーまたはローカル ユーザ ポリシーにそのリストを割り当てます。

また、クライアントレス SSL VPN セッションを介したスマート トンネル接続でのログイン クレデンシャルの送信を自動化する Web 対応アプリケーションのリストも作成できます。

スマート トンネルを使用する理由

スマート トンネル アクセスでは、クライアントの TCP ベースのアプリケーションは、ブラウザベースの VPN 接続を使用してサービスにアクセスできます。この方法では、プラグインやレガシー テクノロジーであるポート転送と比較して、ユーザには次のような利点があります。

- スマート トンネルは、プラグインよりもパフォーマンスが向上します。
- ポート転送とは異なり、スマート トンネルでは、ローカル ポートへのローカル アプリケーションのユーザ接続を要求しないことにより、ユーザ エクスペリエンスが簡略化されます。
- ポート転送とは異なり、スマート トンネルでは、ユーザは管理者特権を持つ必要がありません。

プラグインの利点は、クライアント アプリケーションをリモート コンピュータにインストールする必要がないという点です。

前提条件

ASA Release 9.0 のスマート トンネルでサポートされているプラットフォームおよびブラウザについては、『*Supported VPN Platforms, Cisco ASA Series*』を参照してください。

次の要件と制限事項が Windows でのスマート トンネル アクセスには適用されます。

- Windows では ActiveX または Oracle Java ランタイム環境（JRE）4 Update 15 以降（JRE 6 以降を推奨）をブラウザでイネーブルにしておく必要がある。

  ActiveX ページでは、関連するグループ ポリシーに **activex-relay** コマンドを入力しておくことが必要です。コマンドを入力しているか、ポリシーにスマート トンネル リストを割り当てていて、エンドポイントのブラウザのプロキシ例外リストでプロキシが指定されている場合、このリストに「shutdown.webvpn.relay.」エントリを追加する必要があります。

- Winsock 2 の TCP ベースのアプリケーションだけ、スマート トンネル アクセスに適する。
- Mac OS X の場合に限り、Java Web Start をブラウザでイネーブルにしておく必要がある。

制限

- スマート トンネルは、Microsoft Windows を実行しているコンピュータとセキュリティ アプライアンス間に配置されたプロキシだけをサポートする。スマート トンネルは、Windows でシステム全体のパラメータを設定する Internet Explorer 設定を使用します。この設定がプロキシ情報を含む場合があります。
  - Windows コンピュータで、プロキシが ASA にアクセスする必要がある場合は、クライアントのブラウザにスタティック プロキシ エントリが必要であり、接続先のホストがクライアントのプロキシ例外のリストに含まれている必要があります。
  - Windows コンピュータで、プロキシが ASA にアクセスする必要がなく、プロキシがホスト アプリケーションにアクセスする必要がある場合は、ASA がクライアントのプロキシ例外のリストに含まれている必要があります。

  プロキシ システムはスタティック プロキシ エントリまたは自動設定のクライアントの設定、または PAC ファイルによって定義できます。現在、スマート トンネルでは、スタティック プロキシ設定だけがサポートされています。
- スマート トンネルでは、Kerberos Constrained Delegation（KCD）はサポートされない。
- Windows の場合、コマンド プロンプトから開始したアプリケーションにスマート トンネル アクセスを追加する場合は、スマート トンネル リストの 1 つのエントリの Process Name に「cmd.exe」を指定し、別のエントリにアプリケーション自体へのパスを指定する必要がある。これは「cmd.exe」がアプリケーションの親であるためです。
- HTTP ベースのリモート アクセスによって、いくつかのサブネットが VPN ゲートウェイへのユーザ アクセスをブロックすることがある。これを修正するには、Web とエンド ユーザの場所との間のトラフィックをルーティングするために ASA の前にプロキシを配置します。このプロキシが CONNECT 方式をサポートしている必要があります。認証が必要なプロキシの場合、スマート トンネルは、基本ダイジェスト認証タイプだけをサポートします。
- スマート トンネルが開始されると、ASA は、ブラウザ プロセスが同じである場合に VPN セッション経由ですべてのブラウザ トラフィックをデフォルトで送信する。また、tunnel-all ポリシーが適用されている場合にのみ、ASA は同じ処理を行います。ユーザがブラウザ プロセスの別のインスタンスを開始すると、VPN セッション経由ですべてのトラフィックが送信されます。ブラウザ プロセスが同じで、セキュリティ アプライアンスが URL へのアクセスを提供しない場合、ユーザはその URL を開くことはできません。回避策として、tunnel-all ではないトンネル ポリシーを割り当てます。
- ステートフル フェールオーバーが発生したとき、スマート トンネル接続は保持されない。ユーザはフェールオーバー後に再接続する必要があります。
- スマート トンネルの Mac バージョンは、POST ブックマーク、フォームベースの自動サインオン、または POST マクロ置換をサポートしない。
- Mac OS ユーザの場合、ポータル ページから起動されたアプリケーションだけがスマート トンネル セッションを確立できる。この要件には、Firefox に対するスマート トンネルのサポートも含まれます。スマート トンネルを最初に使用する際に、Firefox を使用して Firefox の別のインスタンスを起動するには、csco_st という名前のユーザ プロファイルが必要です。このユーザ プロファイルが存在しない場合、セッションでは、作成するようにユーザに要求します。
- Mac OS X では、SSL ライブラリにダイナミックにリンクされた、TCP を使用するアプリケーションをスマート トンネルで使用できる。

- Mac OS X では、スマート トンネルは次をサポートしない。
  - プロキシ サービス
  - 自動サインオン
  - 2 つのレベルの名前スペースを使用するアプリケーション
  - Telnet、SSH、cURL などのコンソールベースのアプリケーション
  - dlopen または dlsym を使用して libsocket コールを見つけ出すアプリケーション
  - libsocket コールを見つけ出すスタティックにリンクされたアプリケーション
- Mac OS X では、プロセスへのフル パスが必要である。また、このパスは大文字と小文字が区別されます。各ユーザ名のパスを指定しないようにするには、部分パスの前にチルダ（~）を入力します（例：~/bin/vnc）。

スマート トンネル アクセスに適格なアプリケーションの追加

各 ASA のクライアントレス SSL VPN コンフィギュレーションは、*スマート トンネル リスト*をサポートしています。各リストは、スマート トンネル アクセスに適格な 1 つ以上のアプリケーションを示します。各グループ ポリシーまたはユーザ名は 1 つのスマート トンネル リストのみをサポートするため、サポートされる各アプリケーションのセットをスマート トンネル リストにグループ化する必要があります。

スマート トンネル リストについて

グループ ポリシーとユーザ名ごとに、次のいずれかを行うようにクライアントレス SSL VPN を設定できます。

- ユーザのログイン時に自動的にスマート トンネル アクセスを開始する。
- ユーザのログイン時にスマート トンネル アクセスをイネーブルにするが、ユーザはクライアントレス SSL VPN ポータル ページの **[Application Access] > [Start Smart Tunnels]** ボタンを使用して、スマート トンネル アクセスを手動で開始するようにユーザに要求する。

制限

スマート トンネル ログオン オプションは、各グループ ポリシーとユーザ名に対して互いに排他的です。1 つだけ使用してください。

手順の詳細

次の smart tunnel コマンドは、各グループ ポリシーとユーザ名で使用可能です。各グループ ポリシーとユーザ名のコンフィギュレーションは、一度にこれらのコマンドの 1 つだけサポートします。そのため、1 つのコマンドを入力すると、ASA が、該当のグループ ポリシーまたはユーザ名のコンフィギュレーションに存在するコマンドを新しいコマンドで置き換えます。または、最後のコマンドの場合、グループ ポリシーまたはユーザ名にすでに存在する **smart-tunnel** コマンドが単純に削除されます。

	コマンド	目的
ステップ 1	**smart-tunnel auto-start** *list* または **smart-tunnel enable** *list* または **smart-tunnel disable** または **no smart-tunnel [auto-start list | enable list | disable]**	ユーザのログイン時にスマート トンネル アクセスを自動的に開始します。 ユーザ ログイン時にスマート トンネル アクセスをイネーブルにします。ただし、ユーザがクライアントレス SSL VPN ポータル ページの **[Application Access] > [Start Smart Tunnels]** ボタンを使用して、手動でスマート トンネル アクセスを開始する必要があります。 スマート トンネル アクセスを使用禁止にします。 **smart-tunnel** コマンドがグループ ポリシーまたはユーザ名コンフィギュレーションから削除され、**[no] smart-tunnel** コマンドがデフォルト グループ ポリシーから継承されます。**no smart-tunnel** コマンドの後にあるキーワードはオプションですが、これらのキーワードにより削除対象をその名前の **smart-tunnel** コマンドに限定します。
ステップ 2	必要なオプションについては、「スマート トンネル アクセスの自動化」を参照してください。	

スマート トンネル ポリシーの設定および適用

スマート トンネル ポリシーは、グループ ポリシーまたはユーザ名単位の設定が必要です。各グループ ポリシーまたはユーザ名は、グローバルに設定されたネットワークのリストを参照します。スマート トンネルをオンにすると、トンネル外部のトラフィックに、ネットワーク（ホストのセット）を設定する CLI および指定されたスマート トンネル ネットワークを使用してユーザに対してポリシーを適用する CLI の 2 つの CLI を使用できます。次のコマンドによって、スマート トンネル ポリシーを設定するために使用するホストのリストが作成されます。

手順の詳細

	コマンド	目的
ステップ 1	**webvpn**	クライアントレス SSL VPN コンフィギュレーション モードに切り替えます。
ステップ 2	**[no] smart-tunnel network** *network name* **ip** *ip netmask*	スマート トンネル ポリシー設定のために使用するホストのリストを作成します。*network name* は、トンネル ポリシーに適用する名前です。*ip* は、ネットワークの IP アドレスです。*netmask* は、ネットワークのネットマスクです。

	コマンド	目的
ステップ 3	**[no] smart-tunnel network** *network name* **host** *host mask*	*.cisco.com などのホスト名マスクを確立します。
ステップ 4	**[no] smart-tunnel tunnel-policy [{excludespecified | tunnelspecified}** *network name* **| tunnelall]** または **[no] smart-tunnel tunnel-policy {excludespecified | tunnelspecified}** *network* **name | tunnelall]**	特定のグループ ポリシーまたはユーザ ポリシーにスマート トンネル ポリシーを適用します。*network name* は、トンネリングされるネットワークのリストです。*tunnelall* は、すべてをトンネリング（暗号化）します。*tunnelspecified* は、network name で指定されたネットワークだけをトンネリングします。*excludespecified* は、network name で指定されたネットワークの外部のネットワークだけをトンネリングします。

スマート トンネルのトンネル ポリシーの設定および適用

SSL VPN クライアントでのスプリット トンネル設定と同様に、スマート トンネル ポリシーはグループ ポリシーおよびユーザ名単位の設定です。各グループ ポリシーおよびユーザ名は、グローバルに設定されたネットワークのリストを参照します。

コマンド	目的
[no] smart-tunnel tunnel-policy [{excludespecified | tunnelspecified} *network name* **| tunnelall]** または **[no] smart-tunnel tunnel-policy [{excludespecified | tunnelspecified}** *network name* **| tunnelall]**	グローバルに設定されたネットワークのリストを参照します。*network name* は、トンネリングされるネットワークのリストです。*tunnelall* は、すべてをトンネリング（暗号化）します。tunnelspecified は、network name で指定されたネットワークだけをトンネリングします。excludespecified は、network name で指定されたネットワークの外部のネットワークだけをトンネリングします。

コマンド	目的
ciscoasa(config-webvpn)# [no] smart-tunnel network *network name* **ip** *ip netmask* **ciscoasa(config-webvpn)# [no] smart-tunnel network** *network name* **host** *host mask*	グループ ポリシーおよびユーザ ポリシーにトンネル ポリシーを適用します。一方のコマンドによってホストが指定され、他方のコマンドによってネットワーク IP が指定されます。1 つのコマンドのみを使用します。 *network name*：トンネル ポリシーを適用するネットワークの名前 *ip address*：ネットワークの IP アドレス *netmask*：ネットワークのネットマスク *host mask*：ホスト名マスク（*.cisco.com など）
例： ciscoasa(config-webvpn)# **smart-tunnel network inventory ip 10.5.2.2** ciscoasa(config-webvpn)# **smart-tunnel network inventory host www.example.com**	パートナーがログイン時に最初にクライアントレス ポータルを介さずに内部インベントリ サーバ ページにクライアントレス アクセスできるようにしたいとベンダーが考えている場合、スマート トンネル ポリシー設定は適切なオプションです。1 つのホストだけを含むトンネル ポリシーを作成します（次の例では、インベントリ ページは www.example.com（10.5.2.2）でホストされており、ホストの IP アドレスと名前の両方を設定するものと仮定します）。
ciscoasa(config-group-webvpn)# **smart-tunnel tunnel-policy tunnelspecified inventory**	パートナーのグループ ポリシーに、指定したトンネルのトンネル ポリシーを適用します。
（オプション） ciscoasa(config-group-webvpn)# **homepage value http://www.example.com** ciscoasa(config-group-webvpn)# h**omepage use-smart-tunnel**	グループ ポリシーのホームページを指定して、そのページでスマート トンネルをイネーブルにします。スクリプトを記述したり何かをアップロードしなくても、管理者はどのページがスマート トンネル経由で接続するかを指定できます。
（オプション） ciscoasa(config-webvpn)# **smart-tunnel notification-icon**	スマート トンネルをイネーブルにした状態でブラウザによって開始されたすべてのプロセスはトンネルにアクセスできるため、デフォルトでは、スマート トンネル アプリケーションの設定は必須ではありません。ただし、ポータルが表示されないため、ログアウト通知アイコンをイネーブルにできます。

スマート トンネル自動サインオン サーバ リストの作成

コマンド	目的
webvpn	クライアントレス SSL VPN コンフィギュレーション モードに切り替えます。
smart-tunnel auto-sign-on *list* [*use-domain*] [**realm** *realm-string*] [**port** *port-num*]{**ip** *ip-address* [*netmask*] | **host** *hostname-mask*}	サーバ リストに追加する各サーバに対して使用します。 • *list*：リモート サーバのリストの名前を指定します。スペースを含む場合、名前の前後に引用符を使用します。文字列は最大 64 文字まで使用できます。コンフィギュレーション内にリストが存在しない場合、ASA はリストを作成します。存在する場合、リストにエントリを追加します。区別しやすい名前を割り当てます。 • use-domain（オプション）：認証で必要な場合は、Windows ドメインをユーザ名に追加します。このキーワードを入力する場合は、スマート トンネル リストを 1 つ以上のグループ ポリシーまたはユーザ名に割り当てるときにドメイン名を指定してください。 • *realm*：認証のレルムを設定します。レルムは Web サイトの保護領域に関連付けられ、認証時に認証プロンプトまたは HTTP ヘッダーのいずれかでブラウザに再度渡されます。自動サインオンが設定され、レルムの文字列が指定されたら、ユーザはレルムの文字列を Web アプリケーション（Outlook Web Access など）で設定し、Web アプリケーションにサインオンすることなくアクセスできます。 • *port*：自動サインオンを実行するポートを指定します。Firefox では、ポート番号が指定されていない場合、自動サインオンは、デフォルトのポート番号 80 および 443 でそれぞれアクセスされた HTTP および HTTPS に対して実行されます。 • *ip :* IP アドレスとネットマスクによってサーバを指定します。 • *ip-address*[*netmask*]：自動認証先のホストのサブネットワークを指定します。 • *host*：ホスト名またはワイルドカード マスクによってサーバを指定します。このオプションを使用すると、IP アドレスのダイナミックな変更からコンフィギュレーションを保護します。 • *hostname-mask*：自動認証する対象のホスト名またはワイルドカード マスクを指定します。
（オプション） [**no**] **smart-tunnel auto-sign-on** *list* [**use-domain**] [**realm** *realm-string*] [**port** *port-num*] {**ip** *ip-address* [*netmask*] | **host** *hostname-mask*}	ASA 設定に表示されるとおりにリストと IP アドレスまたはホスト名を指定して、サーバのリストからエントリを削除します。

コマンド	目的
show running-config webvpn smart-tunnel	スマート トンネル自動サインオン サーバ リストを表示します。
config-webvpn	config-webvpn コンフィギュレーション モードに切り替えます。
smart-tunnel auto-sign-on HR use-domain ip 93.184.216.119 255.255.255.0	サブネット内のすべてのホストを追加し、認証で必要な場合に Windows ドメインをユーザ名に追加します。
（オプション） **no smart-tunnel auto-sign-on HR use-domain ip 93.184.216.119 255.255.255.0**	削除されるエントリがリストの唯一のエントリである場合は、リストからそのエントリを削除し、HR という名前のリストも削除します。
no smart-tunnel auto-sign-on HR	ASA 設定からリスト全体を削除します。
smart-tunnel auto-sign-on intranet host *.example.com	ドメイン内のすべてのホストを intranet という名前のスマート トンネル自動サインオン リストに追加します。
no smart-tunnel auto-sign-on intranet host *.example.com	リストからエントリを削除します。

スマート トンネル自動サインオン サーバ リストのコンフィギュレーションに続き、次の項で説明するように、そのリストをグループ ポリシーまたはローカル ユーザ ポリシーに割り当ててアクティブにする必要があります。

次の手順は、サーバ リストにサーバを追加することです。

スマート トンネル自動サインオン サーバ リストへのサーバの追加

次の手順では、スマート トンネル接続での自動サインオンを提供するサーバのリストにサーバを追加し、そのリストをグループ ポリシーまたはローカル ユーザに割り当てる方法について説明します。

前提条件

smart-tunnel auto-sign-on *list* コマンドを使用して、最初にサーバのリストを作成する必要があります。グループ ポリシーまたはユーザ名に割り当てることができるリストは 1 つだけです。

制限

- スマート トンネル自動サインオン機能は、Internet Explorer および Firefox を使用した HTTP および HTTPS 通信を行うアプリケーションだけをサポートしています。
- Firefox では、管理者が正確なホスト名または IP アドレスを使用してホストを指定する必要があります（ワイルドカードを使用したホスト マスク、IP アドレスを使用したサブネット、およびネットマスクは使用できません）。たとえば、Firefox では、*.cisco.com を入力したり、email.cisco.com をホストする自動サインオンを期待したりすることはできません。

手順の詳細

クライアントレス（ブラウザベース）SSL VPN セッションでスマート トンネル自動サインオンをイネーブルにするには、次のコマンドを使用します。

	コマンド	目的
ステップ 1	**webvpn**	クライアントレス SSL VPN コンフィギュレーション モードに切り替えます。
ステップ 2	**group-policy webvpn** または **username webvpn**	グループ ポリシーのクライアントレス SSL VPN コンフィギュレーション モードに切り替えます。 ユーザ名のクライアントレス SSL VPN コンフィギュレーション モードに切り替えます。
ステップ 3	**smart-tunnel auto-sign-on enable**	スマート トンネル自動サインオン クライアントレス SSL VPN セッションをイネーブルにします。
ステップ 4	（オプション） **[no] smart-tunnel auto-sign-on enable** *list* **[domain** *domain***]**	スマート トンネル自動サインオン クライアントレス SSL VPN セッションをオフに切り替えて、グループ ポリシーまたはユーザ名からこのセッションを削除して、デフォルトを使用します。 • *list*：ASA クライアントレス SSL VPN コンフィギュレーションにすでに存在するスマート トンネル自動サインオン リストの名前です。 • （オプション）*domain*：認証中にユーザ名に追加されるドメインの名前です。ドメインを入力する場合、**use-domain** キーワードをリスト エントリに入力します。
ステップ 5	**show running-config webvpn smart-tunnel**	SSL VPN コンフィギュレーション内のスマート トンネル自動サインオン リストのエントリを表示します。
ステップ 6	**smart-tunnel auto-sign-on enable HR**	HR という名前のスマート トンネル自動サインオン リストをイネーブルにします。
ステップ 7	**smart-tunnel auto-sign-on enable HR domain CISCO**	HR という名前のスマート トンネル自動サインオン リストをイネーブルにし、認証中に CISCO という名前のドメインをユーザ名に追加します。
ステップ 8	（オプション） **no smart-tunnel auto-sign-on enable HR**	HR という名前のスマート トンネル自動サインオン リストをグループ ポリシーから削除し、デフォルトのグループ ポリシーからスマート トンネル自動サインオン リスト コマンドを継承します。

スマート トンネル アクセスの自動化

ユーザのログイン時にスマート トンネル アクセスを自動的に開始するには、次のコマンドを入力します。

要件

Mac OS X の場合は、自動開始設定が行われていてもいなくても、ポータルの [Application Access] パネルにあるアプリケーションのリンクをクリックする必要があります。

手順の詳細

	コマンド	目的
ステップ 1	**webvpn**	クライアントレス SSL VPN コンフィギュレーション モードに切り替えます。
ステップ 2	**group-policy webvpn** または **username webvpn**	グループ ポリシーのクライアントレス SSL VPN コンフィギュレーション モードに切り替えます。 ユーザ名のクライアントレス SSL VPN コンフィギュレーション モードに切り替えます。
ステップ 3	**smart-tunnel auto-start** *list* **例：** hostname(config-group-policy)# **webvpn** hostname(config-group-webvpn)# **smart-tunnel auto-start apps1**	ユーザのログイン時にスマート トンネル アクセスを自動的に開始します。*list* は、すでに存在するスマート トンネル リストの名前です。 apps1 という名前のスマート トンネル リストをグループ ポリシーに割り当てます。
ステップ 4	**show running-config webvpn smart-tunnel**	SSL VPN コンフィギュレーション内のスマート トンネル リストのエントリを表示します。
ステップ 5	（オプション） **no smart-tunnel**	**smart-tunnel** コマンドをグループ ポリシーまたはユーザ名から削除し、デフォルトに戻します。

スマート トンネル アクセスのイネーブル化とオフへの切り替え

デフォルトでは、スマート トンネルはオフになっています。

手順の詳細

	コマンド	目的
ステップ 1	**webvpn**	クライアントレス SSL VPN コンフィギュレーション モードに切り替えます。
ステップ 2	**group-policy webvpn** または **username webvpn**	グループ ポリシーのクライアントレス SSL VPN コンフィギュレーション モードに切り替えます。 ユーザ名のクライアントレス SSL VPN コンフィギュレーション モードに切り替えます。
ステップ 3	**smart-tunnel [enable** *list* **| disable]** **例：** hostname(config-group-policy)# **webvpn** hostname(config-group-webvpn)# **smart-tunnel enable apps1**	スマート トンネル アクセスをイネーブルにします。*list* は、すでに存在するスマート トンネル リストの名前です。前の表の **smart-tunnel auto-start list** を入力した場合は、スマート トンネル アクセスを手動で開始する必要はありません。 apps1 という名前のスマート トンネル リストをグループ ポリシーに割り当てます。
ステップ 4	**show running-config webvpn smart-tunnel**	SSL VPN コンフィギュレーション内のスマート トンネル リストのエントリを表示します。
ステップ 5	（オプション） **no smart-tunnel**	**smart-tunnel** コマンドをグループ ポリシーまたはローカル ユーザ ポリシーから削除し、デフォルトのグループ ポリシーに戻します。
ステップ 6	（オプション） **smart-tunnel disable**	スマート トンネル アクセスをオフに切り替えます。

スマート トンネルからのログオフの設定

ここでは、スマート トンネルからの適切なログオフ方法について説明します。すべてのブラウザ ウィンドウを閉じるか、通知アイコンを右クリックしてログアウトを確認すると、スマート トンネルからログオフできます。

（注） ポータルにあるログアウト ボタンを使用することを強くお勧めします。この方法は、クライアントレス SSL VPN 用であり、スマート トンネルが使用されているかどうかに関係なくログオフが行われます。通知アイコンは、ブラウザを使用しないスタンドアロン アプリケーションを使用する場合に限り使用する必要があります。

ペアレント プロセスの終了

この方法では、ログオフを示すためにすべてのブラウザを閉じることが必要です。スマート トンネルのライフタイムは現在、プロセスのライフタイムの開始に結び付けられています。たとえば、Internet Explorer からスマート トンネルを開始した場合、iexplore.exe が実行されていないとスマート トンネルがオフになります。スマート トンネルは、ユーザがログアウトせずにすべてのブラウザを閉じた場合でも、VPN セッションが終了したと判断します。

（注） 場合によっては、ブラウザ プロセスがエラーの結果として、意図的にではなく残っていることがあります。また、Secure Desktop を使用しているときに、ユーザが Secure Desktop 内ですべてのブラウザを閉じてもブラウザ プロセスが別のデスクトップで実行されている場合があります。したがって、スマート トンネルは、現在のデスクトップで表示されているウィンドウがない場合にすべてのブラウザ インスタンスが終了したと見なします。

手順の詳細

	コマンド	目的
ステップ 1	**[no] smart-tunnel notification-icon**	管理者が通知アイコンをグローバルでオンにすることを許可します。このコマンドは、ブラウザ ウィンドウを閉じることでログアウトを行うのではなく、ログアウト プロパティを設定し、ユーザにログアウトのためのログアウト アイコンが提示されるかどうかを制御します。また、このコマンドは通知アイコンをオンまたはオフにすると自動的にオンまたはオフになる親プロセスが終了する場合のログオフも制御します。 **notification-icon** は、ログアウトのためにアイコンを使用するタイミングを指定するキーワードです。 **（注）** このコマンドの no バージョンがデフォルトです。この場合、すべてのブラウザ ウィンドウを閉じることで SSL VPN セッションからログオフします。 **（注）** ポータルのログアウトは引き続き有効であり、影響を受けません。
ステップ 2	***.webvpn.**	プロキシを使用し、プロキシ リストの例外に追加すると、アイコンの使用に関係なく、ログオフ時にスマート トンネルが必ず適切に閉じられるようにします。

通知アイコンの利用

ブラウザを閉じてもセッションが失われないようにするために、ペアレント プロセスの終了時にログオフをオフに切り替えることもできます。この方法では、システム トレイの通知アイコンを使用してログアウトします。アイコンは、ユーザがアイコンをクリックしてログアウトするまで維持されます。ユーザがログアウトする前にセッションの期限が切れた場合、アイコンは、次回に接続を試行するまで維持されます。セッション ステータスがシステム トレイで更新されるまで時間がかかることがあります。

（注）　このアイコンが、SSL VPN からログアウトする別の方法です。これは、VPN セッション ステータスのインジケータではありません。

コンテンツ変換の設定

デフォルトでは、ASA は、コンテンツ変換およびリライト エンジンを通じ、JavaScript および Java などの高度な要素からプロキシ HTTP へのトラフィックを含む、すべてのクライアントレス SSL VPN トラフィックを処理します。このようなトラフィックでは、ユーザがアプリケーションにアクセスするのに SSL VPN デバイス内部からアクセスしているか、これらに依存せずにアクセスしているかによって、セマンティックやアクセス コントロールのルールが異なる場合があります。

Web リソースによっては、高度に個別の処理が要求される場合があります。次の項では、このような処理を提供する機能について説明します。

- リライトされた Java コンテンツに署名するための証明書の設定
- コンテンツのリライトの切り替え
- プロキシ バイパスの使用

組織や関係する Web コンテンツの要件に応じてこれらの機能のいずれかを使用する場合があります。

リライトされた Java コンテンツに署名するための証明書の設定

クライアントレス SSL VPN が変換した Java オブジェクトは、その後、トラストポイントに関連付けられた PKCS12 デジタル証明書により署名されます。

手順の詳細

	コマンド	目的
ステップ 1	**crypto ca import**	証明書をインポートします。
ステップ 2	**ava-trustpoint** **例：t** hostname(config)# **crypto ca import mytrustpoint pkcs12 mypassphrase** Enter the base 64 encoded PKCS12. End with the word “quit” on a line by itself. [PKCS12 data omitted] **quit** INFO: Import PKCS12 operation completed successfully. hostname(config)# **webvpn** hostname(config)# **java-trustpoint mytrustpoint**	証明書を採用します。 mytrustpoint という名前のトラストポイントの作成、および Java オブジェクトに署名するための割り当てを示します。

コンテンツのリライトの切り替え

公開 Web サイトなどの一部のアプリケーションや Web リソースによっては、ASA を通過しない設定が求められる場合があります。このため、ASA では、特定のサイトやアプリケーションを ASA を通過せずにブラウズできるリライト ルールを作成できます。これは、IPsec VPN 接続におけるスプリット トンネリングによく似ています。

	コマンド	目的
ステップ 1	**webvpn**	クライアントレス SSL VPN コンフィギュレーション モードに切り替えます。
ステップ 2	**rewrite**	クライアントレス SSL VPN トンネルの外部にアクセスするためのアプリケーションとリソースを指定します。このコマンドは複数回使用できます。
ステップ 3	**disable**	**rewrite** コマンドとともに使用します。セキュリティ アプライアンスはリライト ルールを順序番号に従って検索するため、ルールの順序番号は重要です。このとき、最下位の番号から順に検索して行き、最初に一致したルールが適用されます。

プロキシ バイパスの使用

ユーザはプロキシ バイパスを使用するように ASA を設定できます。これは、プロキシ バイパスが提供する特別なコンテンツ リライト機能を使用した方が、アプリケーションや Web リソースをより有効活用できる場合に設定します。プロキシ バイパスはコンテンツの書き換えに代わる手法であり、元のコンテンツの変更を最小限に抑えます。多くの場合、カスタム Web アプリケーションでこれを使用すると有効です。

proxy-bypass コマンドは複数回使用できます。エントリを設定する順序は重要ではありません。インターフェイスとパス マスク、またはインターフェイスとポートにより、プロキシ バイパス ルールが一意に指定されます。

パス マスクではなくポートを使用してプロキシ バイパスを設定する場合、ネットワーク コンフィギュレーションによっては、これらのポートが ASA にアクセスできるようにするために、ファイアウォール コンフィギュレーションの変更が必要になることがあります。この制限を回避するには、パス マスクを使用します。ただし、パス マスクは変化することがあるため、複数のパス マスク ステートメントを使用して変化する可能性をなくすことが必要になる場合があります。

パスは、URL で .com や .org、またはその他のタイプのドメイン名の後に続く全体です。たとえば、www.example.com/hrbenefits という URL では、*hrbenefits* がパスになります。同様に、www.example.com/hrinsurance という URL では、*hrinsurance* がパスです。すべての hr サイトでプロキシ バイパスを使用する場合は、*（ワイルドカード）を /hr* のように使用して、コマンドを複数回使用しないようにできます。

手順の詳細

	コマンド	目的
ステップ 1	**webvpn**	クライアントレス SSL VPN コンフィギュレーション モードに切り替えます。
ステップ 2	**proxy-bypass**	プロキシ バイパスを設定します。

ポータル アクセス ルールの設定

この拡張機能により、カスタマーは、HTTP ヘッダー内に存在するデータに基づいて、クライアントレス SSL VPN セッションを許可または拒否するグローバルなクライアントレス SSL VPN アクセス ポリシーを設定することができます。ASA がクライアントレス SSL VPN セッションを拒否する場合、ただちにエンドポイントにエラー コードを返します。

ASA は、このアクセス ポリシーを、エンドポイントが ASA に対して認証する前に評価します。その結果、拒否の場合は、エンドポイントからの追加の接続試行による ASA の処理リソースの消費はより少なくなります。

前提条件

ASA にログインし、グローバル コンフィギュレーション モードを開始します。グローバル コンフィギュレーション モードでは、ASA は次のプロンプトを表示します。

```
hostname(config)#
```

手順の詳細

	コマンド	目的
ステップ 1	**webvpn** **例：** hostname(config)# webvpn	クライアントレス SSL VPN コンフィギュレーション モードに入ります。
ステップ 2	**portal-access-rule** *priority* [{**permit** | **deny** [**code** *code*]} {**any** | **user-agent match** *string*} **例：** hostname(config-webvpn)# portal-access-rule 1 deny code 403 user-agent match *Thunderbird* hostname(config-webvpn)# portal-access-rule 1 deny code 403 user-agent match “*my agent*”	HTTP ヘッダー内の HTTP ヘッダー コードまたは文字列に基づいて、クライアントレス SSL VPN セッションの作成を許可または拒否します。 2 番目の例では、スペースを含む文字列を指定するための適切な構文を示しています。文字列はワイルドカード（*）で囲み、さらに引用符（" "）で囲みます。

クライアントレス SSL VPN のパフォーマンスの最適化

ASA には、クライアントレス SSL VPN のパフォーマンスと機能性を最適化するいくつかの方法があります。パフォーマンスの改善には、Web オブジェクトのキャッシングと圧縮が含まれます。機能性の調整には、コンテンツ変換およびプロキシ バイパスの制限の設定が含まれます。その他に、APCF でコンテンツ変換を調整することもできます。次の項では、これらの機能について説明します。

- キャッシングの設定
- コンテンツ変換の設定

キャッシングの設定

キャッシングを行うとクライアントレス SSL VPN のパフォーマンスが向上します。頻繁に再利用されるオブジェクトをシステム キャッシュに格納することで、書き換えの繰り返しやコンテンツの圧縮の必要性を低減します。また、クライアントレス SSL VPN とリモート サーバ間のトラフィックが軽減されるため、多くのアプリケーションが今までよりはるかに効率的に実行できるようになります。

デフォルトでは、キャッシングはイネーブルになっています。キャッシュ モードでキャッシング コマンドを使用すると、ユーザの環境に応じてキャッシング動作をカスタマイズできます。

クライアントレス SSL VPN リモート ユーザ

2013 年 9 月 13 日

この章は、エンド ユーザのためのクライアントレス（ブラウザベース）SSL VPN を設定するシステム管理者を対象としています。ここでは、ユーザ リモート システムの設定要件と作業の概要を説明します。また、ユーザがクライアントレス SSL VPN の使用を開始するために、ユーザに伝える必要のある情報も明確にします。

- ユーザ名とパスワードの要求
- セキュリティのヒントの通知
- クライアントレス SSL VPN の機能を使用するためのリモート システムの設定
- クライアントレス SSL VPN データのキャプチャ

（注） 次の説明では、すでにクライアントレス SSL VPN 用に ASA が設定済みと想定しています。

ユーザ名とパスワードの要求

ネットワークによっては、リモート セッション中にユーザが、コンピュータ、インターネット サービス プロバイダー、クライアントレス SSL VPN、メール サーバ、ファイル サーバ、企業アプリケーションの一部またはすべてにログインする必要が生じることがあります。ユーザはさまざまなコンテキストで認証を行うために、固有のユーザ名、パスワード、PIN などさまざまな情報が要求される場合があります。必要なアクセス権があることを確認してください。

表 17-1 に、クライアントレス SSL VPN ユーザが知っておく必要のあるユーザ名とパスワードのタイプを示します。

表 17-1　クライアントレス SSL VPN ユーザに通知するユーザ名とパスワード

ログイン ユーザ名/パスワード タイプ	目的	入力するタイミング
コンピュータ	コンピュータへのアクセス	コンピュータの起動
インターネット サービス プロバイダー	インターネットへのアクセス	インターネット サービス プロバイダーへの接続
クライアントレス SSL VPN	リモート ネットワークへのアクセス	クライアントレス SSL VPN セッションを開始するとき

表 17-1　クライアントレス SSL VPN ユーザに通知するユーザ名とパスワード（続き）

ログイン ユーザ名/パスワード タイプ	目的	入力するタイミング
ファイル サーバ	リモート ファイル サーバへのアクセス	クライアントレス SSL VPN ファイル ブラウジング機能を使用して、リモート ファイル サーバにアクセスするとき
企業アプリケーションへのログイン	ファイアウォールで保護された内部サーバへのアクセス	クライアントレス SSL VPN Web ブラウジング機能を使用して、保護されている内部 Web サイトにアクセスするとき
メール サーバ	クライアントレス SSL VPN 経由によるリモート メール サーバへのアクセス	電子メール メッセージの送受信

セキュリティのヒントの通知

セッションから必ずログアウトするようにユーザに通知してください。クライアントレス SSL VPN からログアウトするには、クライアントレス SSL VPN ツールバーの logout アイコンをクリックするか、またはブラウザを閉じます。

クライアントレス SSL VPN を使用してもすべてのサイトとの通信がセキュアであるとは限らないことを、ユーザに通知してください。クライアントレス SSL VPN は、企業ネットワーク上のリモート コンピュータやワークステーションと ASA との間のデータ転送のセキュリティを保証するものです。したがって、ユーザが HTTPS 以外の Web リソース（インターネット上や内部ネットワーク上にあるもの）にアクセスする場合、企業の ASA から目的の Web サーバまでの通信はセキュアではありません。

クライアントレス SSL VPN の機能を使用するためのリモート システムの設定

表 17-2 に、クライアントレス SSL VPN を使用するためのリモート システムの設定に関する、次の各種情報を示します。

- クライアントレス SSL VPN の起動
- クライアントレス SSL VPN フローティング ツールバーの使用
- Web ブラウジング
- ネットワーク ブラウジングとファイル管理
- アプリケーションの使用（ポート転送）
- ポート転送を介した電子メールの使用、Web アクセス、または電子メール プロキシ

表 17-2 には、次の項目に関する情報も記載されています。

- クライアントレス SSL VPN の要件（機能別）
- クライアントレス SSL VPN がサポートされているアプリケーション
- クライアント アプリケーションのインストールとコンフィギュレーションの要件
- エンド ユーザに提供する必要のある情報
- エンド ユーザのためのヒントや使用上の推奨事項

ユーザ アカウントを異なって設定したことにより、クライアントレス SSL VPN ユーザがそれぞれに使用できる機能が異なる可能性があります。表 17-2 に、ユーザ アクティビティ別の情報をまとめています。使用できない機能の情報についてはスキップしてください。

表 17-2　クライアントレス SSL VPN リモート システム コンフィギュレーションとエンド ユーザの要件

タスク	リモート システムまたはエンド ユーザの要件	仕様または使用上の推奨事項
クライアントレス SSL VPN の起動	インターネットへの接続	サポートされているインターネット接続は、次のとおりです。 • 家庭の DSL、ケーブル、ダイヤルアップ • 公共のキオスク • ホテルの回線 • 空港の無線ノード • インターネット カフェ
	クライアントレス SSL VPN がサポートされているブラウザ	クライアントレス SSL VPN には、次のブラウザを推奨します。他のブラウザでは、クライアントレス SSL VPN 機能が完全にサポートされていない可能性があります。 Microsoft Windows の場合： • Internet Explorer 8 • Firefox 8 Linux の場合： • Firefox 8 Mac OS X の場合： • Safari 5 • Firefox 8
	ブラウザでイネーブルにされているクッキー	ポート転送を介してアプリケーションにアクセスするために、ブラウザでクッキーをイネーブルにする必要があります。
	クライアントレス SSL VPN の URL	HTTPS アドレスの形式は次のとおりです。 https://*address* *address* は、クライアントレス SSL VPN がイネーブルになっている ASA（またはロード バランシング クラスタ）のインターフェイスの IP アドレスまたは DNS ホスト名です。たとえば、https://10.89.192.163 または https://cisco.example.com のようになります。
	クライアントレス SSL VPN のユーザ名とパスワード	
	（オプション）ローカル プリンタ	クライアントレス SSL VPN は、Web ブラウザからネットワーク プリンタへの印刷をサポートしていません。ローカル プリンタへの印刷はサポートされています。

表 17-2　クライアントレス SSL VPN リモート システム コンフィギュレーションとエンド ユーザの要件（続き）

タスク	リモート システムまたはエンド ユーザの要件	仕様または使用上の推奨事項
クライアントレス SSL VPN 接続でのフローティング ツールバーの使用		フローティング ツールバーを使用すると、クライアントレス SSL VPN を簡単に使用できます。ツールバーを使用して、メインのブラウザ ウィンドウに影響を与えずに、URL の入力、ファイルの場所のブラウズ、設定済み Web 接続の選択ができます。 ポップアップをブロックするようにブラウザが設定されている場合、フローティング ツールバーは表示できません。 フローティング ツールバーは、現在のクライアントレス SSL VPN セッションを表します。[Close] ボタンをクリックすると、ASA によってクライアントレス SSL VPN セッションを閉じることを求めるメッセージが表示されます。 **ヒント**　テキストをテキスト フィールドに貼り付けるには、**Ctrl** を押した状態で **V** を押します（クライアントレス SSL VPN ツールバーでは、右クリックはイネーブルになっていません）。

表 17-2　クライアントレス SSL VPN リモート システム コンフィギュレーションとエンド ユーザの要件（続き）

タスク	リモート システムまたはエンド ユーザの要件	仕様または使用上の推奨事項
Web ブラウジング	保護されている Web サイトのユーザ名とパスワード	クライアントレス SSL VPN を使用しても、すべてのサイトとの通信がセキュアになるわけではありません。「セキュリティのヒントの通知」を参照してください。
		クライアントレス SSL VPN での Web ブラウジングのルックアンドフィールは、ユーザが使い慣れたものと異なる場合があります。次に例を示します。 • クライアントレス SSL VPN のタイトル バーが各 Web ページの上部に表示される。 • Web サイトへのアクセス方法： – [Clientless SSL VPN Home] ページ上の [Enter Web Address] フィールドに URL を入力する。 – [Clientless SSL VPN Home] ページ上にある設定済みの Web サイト リンクをクリックする。 – 上記 2 つのどちらかの方法でアクセスした Web ページ上のリンクをクリックする。 また、特定のアカウントの設定によっては、次のようになる場合もあります。 • 一部の Web サイトがブロックされている。 • アクセス可能な Web サイトが、[Clientless SSL VPN Home] ページにリンクとして表示されるサイトに限定される。
ネットワーク ブラウジングとファイル管理	共有リモート アクセス用に設定されたファイル アクセス権	クライアントレス SSL VPN を介してアクセスできるのは、共有フォルダと共有ファイルに限られます。
	保護されているファイル サーバのサーバ名とパスワード	—
	フォルダとファイルが存在するドメイン、ワークグループ、およびサーバ名	ユーザは、組織ネットワークを介してファイルを見つける方法に慣れていない場合があります。
	—	コピー処理の進行中は、**Copy File to Server** コマンドを中断したり、別の画面に移動したりしないでください。コピー処理を中断すると、不完全なファイルがサーバに保存される可能性があります。

表 17-2　クライアントレス SSL VPN リモート システム コンフィギュレーションとエンド ユーザの要件（続き）

タスク	リモート システムまたはエンド ユーザの要件	仕様または使用上の推奨事項
アプリケーションの使用 （ポート転送またはアプリケーション アクセスと呼ばれる）	**（注）** Mac OS X の場合、この機能をサポートしているのは Safari ブラウザだけです。	
	（注） この機能を使用するには、Oracle Java Runtime Environment（JRE）をインストールしてローカル クライアントを設定する必要があります。これには、ローカル システムで管理者の許可が必要になるため、ユーザがパブリック リモート システムから接続した場合に、アプリケーションを使用できない可能性があります。	
	⚠ **注意** ユーザは、**[Close]** アイコンをクリックしてアプリケーションを終了したら、必ず [Application Access] ウィンドウを閉じる必要があります。このウィンドウを正しく閉じないと、Application Access またはアプリケーション自体にアクセスできなくなる可能性があります。	
	インストール済みのクライアント アプリケーション	—
	ブラウザでイネーブルにされているクッキー	—
	管理者特権	ユーザは、DNS 名を使用してサーバを指定する場合、hosts ファイルを変更するのに必要になるため、コンピュータに対する管理者アクセス権が必要になります。
	インストール済みの Oracle Java Runtime Environment（JRE）バージョン 1.4.x と 1.5.x ブラウザで JavaScript をイネーブルにする必要があります。デフォルトではイネーブルに設定されています。	JRE がインストールされていない場合は、ポップアップ ウィンドウが表示され、インストールを開始できるサイトがユーザに示されます。 まれに、Java 例外エラーで、ポート転送アプレットが失敗することがあります。このような状況が発生した場合は、次の手順を実行します。 1. ブラウザのキャッシュをクリアして、ブラウザを閉じます。 2. Java アイコンがコンピュータのタスク バーに表示されていないことを確認します。Java のインスタンスをすべて閉じます。 3. クライアントレス SSL VPN セッションを確立し、ポート転送 Java アプレットを起動します。

表 17-2　クライアントレス SSL VPN リモート システム コンフィギュレーションとエンド ユーザの要件（続き）

タスク	リモート システムまたはエンド ユーザの要件	仕様または使用上の推奨事項
	設定済みのクライアント アプリケーション（必要な場合）。 **（注）** Microsoft Outlook クライアントの場合、この設定手順は不要です。 Windows 以外のすべてのクライアント アプリケーションでは、設定が必要です。 Windows アプリケーションの設定が必要かどうかを確認するには、[Remote Server] の値をチェックします。 • [Remote Server] にサーバ ホスト名が含まれている場合、クライアント アプリケーションの設定は不要です。 • [Remote Server] フィールドに IP アドレスが含まれている場合、クライアント アプリケーションを設定する必要があります。	クライアント アプリケーションを設定するには、ローカルにマッピングされたサーバの IP アドレスとポート番号を使用します。この情報を見つけるには、次の手順を実行します。 1. リモート システムでクライアントレス SSL VPN を起動し、[Clientless SSL VPN Home] ページで Application Access リンクをクリックします。[Application Access] ウィンドウが表示されます。 2. [Name] カラムで、使用するサーバ名を確認し、このサーバに対応するクライアント IP アドレスとポート番号を [Local] カラムで確認します。 3. この IP アドレスとポート番号を使用して、クライアント アプリケーションを設定します。設定手順は、クライアント アプリケーションによって異なります。
	（注） クライアントレス SSL VPN で実行されているアプリケーションで URL（電子メール内の URL など）をクリックしても、クライアントレス SSL VPN ではそのサイトは開きません。クライアントレス SSL VPN でこのようなサイトを開くには、[Enter (URL) Address] フィールドに URL をカット アンド ペーストします。	

表 17-2　クライアントレス SSL VPN リモート システム コンフィギュレーションとエンド ユーザの要件（続き）

タスク	リモート システムまたはエンド ユーザの要件	仕様または使用上の推奨事項
Application Access を介した電子メールの使用	Application Access の要件を満たす（「アプリケーションの使用」を参照）	電子メールを使用するには、[Clientless SSL VPN Home] ページから Application Access を起動します。これにより、メール クライアントが使用できるようになります。
	（注） IMAP クライアントの使用中にメール サーバとの接続が中断したり、新しく接続を確立できない場合は、IMAP アプリケーションを終了してクライアントレス SSL VPN を再起動します。	
	他の電子メール クライアント	Microsoft Outlook Express バージョン 5.5 および 6.0 はテスト済みです。 クライアントレス SSL VPN は、Lotus Notes や Eudora などの、ポート転送を介したその他の SMTPS、POP3S、または IMAP4S 電子メール プログラムをサポートしますが、動作確認は行っていません。
Web アクセスを介した電子メールの使用	インストールされている Web ベースの電子メール製品	サポートされている製品は次のとおりです。 • Outlook Web Access 最適な結果を得るために、Internet Explorer 8.x 以上、または Firefox 8 で OWA を使用してください。 • Lotus Notes その他の Web ベースの電子メール製品も動作しますが、動作確認は行っていません。
電子メール プロキシを介した電子メールの使用	インストール済みの SSL 対応メール アプリケーション ASA SSL バージョンを TLSv1 Only に設定しないでください。Outlook および Outlook Express では TLS はサポートされません。	サポートされているメール アプリケーションは次のとおりです。 • Microsoft Outlook • Microsoft Outlook Express バージョン 5.5 および 6.0 その他の SSL 対応クライアントも動作しますが、動作確認は行っていません。
	設定済みのメール アプリケーション	

クライアントレス SSL VPN データのキャプチャ

CLI キャプチャ コマンドにより、クライアントレス SSL VPN 接続では正しく表示されない Web サイトに関する情報を記録できます。このデータは、シスコ カスタマー サポート エンジニアによる問題のトラブルシューティングに役立ちます。次の各項では、キャプチャ コマンドの使用方法について説明します。

- キャプチャ ファイルの作成
- キャプチャ データを表示するためのブラウザの使用

（注）　クライアントレス SSL VPN キャプチャをイネーブルにすると、ASA のパフォーマンスに影響します。トラブルシューティングに必要なキャプチャ ファイルを生成したら、キャプチャを必ずオフに切り替えます。

キャプチャ ファイルの作成

手順の詳細

ステップ 1　クライアントレス SSL VPN キャプチャ ユーティリティを開始するには、特権 EXEC モードから **capture** コマンドを実行します。

capture *capture-name* **type webvpn user** *csslvpn-username*

値は次のとおりです。

- *capture_name* は、キャプチャに割り当てる名前です。これは、キャプチャ ファイルの名前の先頭にも付加されます。
- *csslvpn-username* は、キャプチャの対象となるユーザ名です。

キャプチャ ユーティリティが開始されます。

ステップ 2　ユーザがログインするとクライアントレス SSL VPN セッションが開始します。キャプチャ ユーティリティは、パケットをキャプチャしています。

コマンドの **no** バージョンを使用してキャプチャを停止します。

no capture *capture-name*

キャプチャ ユーティリティは *capture-name*.zip ファイルを作成し、このファイルはパスワード **koleso** で暗号化されます。

ステップ 3　.zip ファイルをシスコに送信するか、Cisco TAC サービス リクエストに添付します。

ステップ 4　.zip ファイルの内容を確認するには、パスワード **koleso** を使用してファイルを解凍します。

次の例では、*hr* という名前のキャプチャを作成します。これは、user2 へのクライアントレス SSL VPN トラフィックを次のようにファイルにキャプチャします。

```
hostname# capture hr type webvpn user user2
WebVPN capture started.
   capture name   hr
   user name      user2
hostname# no capture hr
```

キャプチャ データを表示するためのブラウザの使用

手順の詳細

ステップ 1　クライアントレス SSL VPN キャプチャ ユーティリティを開始するには、特権 EXEC モードから **capture** コマンドを実行します。

capture *capture-name* **type webvpn user** *csslvpn-username*

値は次のとおりです。

- *capture_name* は、キャプチャに割り当てる名前です。これは、キャプチャ ファイルの名前の先頭にも付加されます。
- *csslvpn-username* は、キャプチャの対象となるユーザ名です。

キャプチャ ユーティリティが開始されます。

ステップ 2　ユーザがログインするとクライアントレス SSL VPN セッションが開始します。キャプチャ ユーティリティは、パケットをキャプチャしています。

コマンドの **no** バージョンを使用してキャプチャを停止します。

ステップ 3　ブラウザを開き、[Address] ボックスに次のように入力します。

https://*IP address or hostname of the ASA***/webvpn_capture.html**

キャプチャされたコンテンツが sniffer 形式で表示されます。

ステップ 4　キャプチャ コンテンツを調べ終えたら、コマンドの **no** バージョンを使用してキャプチャを停止します。

CHAPTER 18

クライアントレス SSL VPN ユーザ

2014 年 4 月 14 日

概要

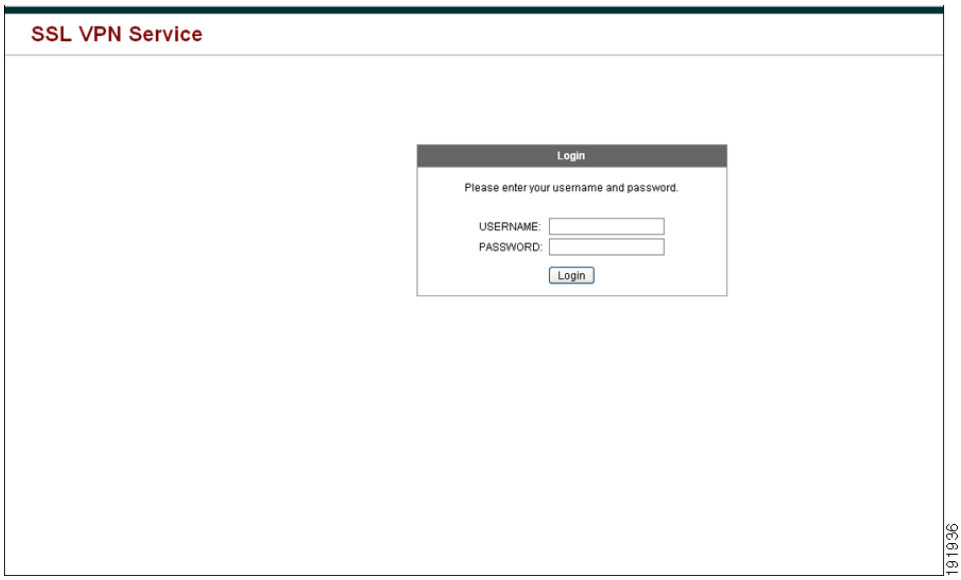
この項では、ユーザがクライアントレス SSL VPN の使用を開始するために、ユーザに伝える必要のある情報も明確にします。説明する項目は次のとおりです。

- 「パスワードの管理」（P.18-4）
- 「セキュリティのヒントの通知」（P.18-23）
- 「クライアントレス SSL VPN の機能を使用するためのリモート システムの設定」（P.18-24）

エンド ユーザ インターフェイスの定義

クライアントレス SSL VPN エンド ユーザ インターフェイスは一連の HTML パネルで構成されます。ユーザは、ASA インターフェイスの IP アドレスを https://*address* 形式で入力することにより、クライアントレス SSL VPN にログインします。最初に表示されるパネルは、ログイン画面（図 18-1）です。

図 18-1　　クライアントレス SSL VPN の [Login] 画面



クライアントレス SSL VPN ホームページの表示

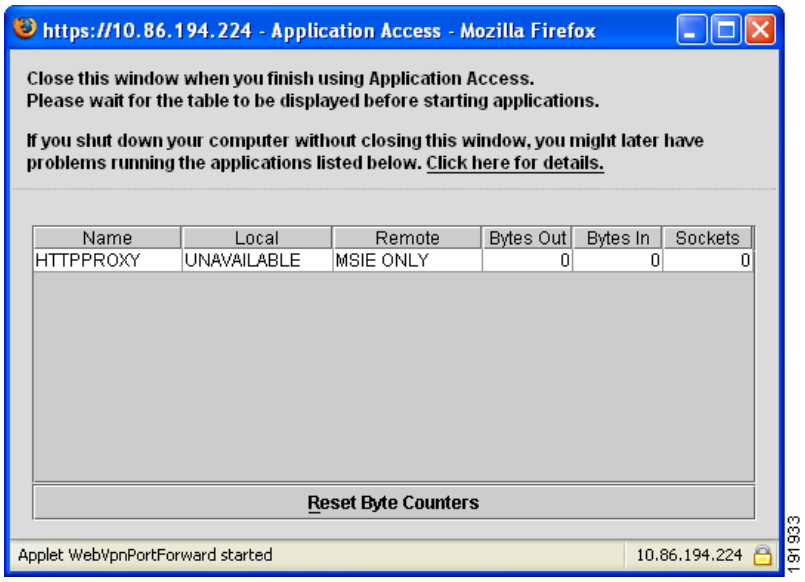
ユーザがログインすると、ポータル ページが開きます。

ホームページには設定済みのクライアントレス SSL VPN 機能がすべて表示され、選択済みのロゴ、テキスト、および色が外観に反映されています。このサンプル ホームページには、特定のファイル共有の指定機能以外のすべてのクライアントレス SSL VPN 機能が表示されています。ユーザはこのホームページを使用して、ネットワークのブラウズ、URL の入力、特定の Web サイトへのアクセス、および Application Access（ポート転送とスマート トンネル）による TCP アプリケーションへのアクセスを実行できます。

クライアントレス SSL VPN の Application Access パネルの表示

ポート転送またはスマート トンネルを開始するには、[Application Access] ボックスの **[Go]** ボタンをクリックします。[Application Access] ウィンドウが開きます（図 18-2）。

図 18-2　　クライアントレス SSL VPN の [Application Access] ウィンドウ



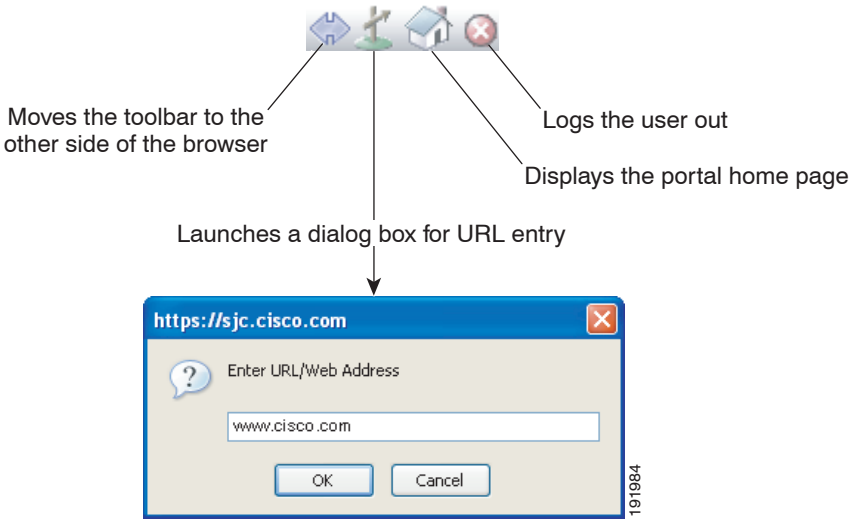
このウィンドウには、このクライアントレス SSL VPN 接続用に設定された TCP アプリケーションが表示されます。このパネルを開いたままでアプリケーションを使用する場合は、通常の方法でアプリケーションを起動します。

（注）　ステートフル フェールオーバーでは、Application Access を使用して確立したセッションは保持されません。ユーザはフェールオーバー後に再接続する必要があります。

フローティング ツールバーの表示

図 18-3 に示すフローティング ツールバーは、現在のクライアントレス SSL VPN セッションを表します。

図 18-3　　クライアントレス SSL VPN フローティング ツールバー



フローティング ツールバーの次の特性に注意してください。

- ツールバーを使用して、メインのブラウザ ウィンドウに影響を与えずに、URL の入力、ファイルの場所のブラウズ、設定済み Web 接続の選択ができます。
- ポップアップをブロックするようにブラウザが設定されている場合、フローティング ツールバーは表示できません。
- ツールバーを閉じると、ASA はクライアントレス SSL VPN セッションを終了するよう促すメッセージを表示します。

クライアントレス SSL VPN の使用方法については、表 18-2（P.18-23）を参照してください。

パスワードの管理

オプションで、パスワードの期限切れが近づくとエンド ユーザに警告するように ASA を設定できます。

ASA では、RADIUS および LDAP プロトコルのパスワード管理をサポートします。「password-expire-in-days」オプションは、LDAP に対してのみサポートされます。

IPsec リモート アクセスと SSL VPN トンネルグループのパスワード管理を設定できます。

パスワード管理を設定すると、ASA は、リモート ユーザのログイン時に、現在のパスワードの期限切れが近づいていること、または期限が切れていることを通知します。それから ASA は、ユーザがパスワードを変更できるようにします。現行のパスワードが失効していない場合、ユーザはそのパスワードを使用してログインし続けることができます。

このコマンドは、そのような通知をサポートする AAA サーバに対して有効です。

ASA のリリース 7.1 以降では通常、LDAP による認証時、または MS-CHAPv2 をサポートする RADIUS コンフィギュレーションによる認証時に、次の接続タイプに対するパスワード管理がサポートされます。

- AnyConnect VPN クライアント
- IPsec VPN クライアント
- クライアントレス SSL VPN

RADIUS サーバ（Cisco ACS など）は、認証要求を別の認証サーバにプロキシする場合があります。ただし、ASA からは RADIUS サーバのみに対して通信しているように見えます。

前提条件

- ネイティブ LDAP には、SSL 接続が必要です。LDAP のパスワード管理を実行する前に、SSL 上での LDAP をイネーブルにする必要があります。デフォルトでは、LDAP はポート 636 を使用します。
- 認証に LDAP ディレクトリ サーバを使用している場合、パスワード管理は Sun JAVA System Directory Server（旧名称は Sun ONE Directory Server）および Microsoft Active Directory を使用してサポートされます。

  Sun：Sun ディレクトリ サーバにアクセスするために ASA に設定されている DN は、そのサーバ上のデフォルト パスワード ポリシーにアクセスできる必要があります。DN として、ディレクトリ管理者、またはディレクトリ管理者権限を持つユーザを使用することを推奨します。または、デフォルト パスワード ポリシーに ACI を設定できます。

Microsoft：Microsoft Active Directory を使用したパスワード管理をイネーブルにするには、LDAP over SSL を設定する必要があります。

制限

- MSCHAP をサポートする一部の RADIUS サーバは、現在 MSCHAPv2 をサポートしていません。このコマンドには MSCHAPv2 が必要なため、ベンダーに問い合わせてください。
- Kerberos/Active Directory（Windows パスワード）または NT 4.0 ドメインでは、これらの接続タイプのいずれについても、パスワード管理はサポート *されません*。
- LDAP でパスワードを変更するには、市販の LDAP サーバごとに独自の方法が使用されています。現在、ASA では Microsoft Active Directory および Sun LDAP サーバに対してのみ、独自のパスワード管理ロジックを実装しています。
- RADIUS または LDAP 認証が設定されていない場合、ASA ではこのコマンドが無視されます。

手順の詳細

（注） **password-management** コマンドはパスワードの期限が切れるまでの日数を変更しません。ただし、ASA がユーザにパスワードの期限が迫っていることについて警告を開始する、期限日前の日数を変更します。

	コマンド	目的
ステップ 1	`tunnel-group general-attributes`	一般属性モードに切り替えます。
ステップ 2	`password-management`	パスワードの期限切れが近づいていることをリモート ユーザに通知します。
ステップ 3	`password-expire-in-days`	パスワードの有効期限を指定します。
ステップ 4	日数を入力します。 **例：** `hostname(config)# tunnel-group testgroup type webvpn` `hostname(config)# tunnel-group testgroup general-attributes` `hostname(config-general)# password-management password-expire-in-days 90`	キーワードを指定する場合は、日数も指定する必要があります。日数を 0 に設定すると、このコマンドはオフになります。 （注） ASA は、ユーザに対して失効が迫っていることを通知しませんが、失効後にユーザはパスワードを変更できます。 接続プロファイル「testgroup」のパスワードの期限切れが近づいていることについて、警告を開始するまでの日数を 90 日に設定します。

クライアントレス SSL VPN でのシングル サインオンの使用

シングル サインオンのサポートを使用すると、クライアントレス SSL VPN のユーザは、ユーザ名とパスワードを 1 回入力するだけで、保護された複数のサービスや Web サーバにアクセスできます。一般に、SSO のメカニズムは AAA プロセスの一部として開始されるか、または AAA サーバのユーザ認証に成功した直後に開始されます。ASA で実行するクライアントレス SSL VPN サーバは、認証サーバに対するユーザのプロキシとして動作します。ユーザがログインすると、クライアントレス SSL VPN サーバは、ユーザ名とパスワードを含む SSO 認証要求を認証サーバに送信します。サーバが認証要求を受け入れた場合は、クライアントレス SSL VPN サーバに SSO 認証クッキーを戻します。ASA は、ユーザの代わりにこのクッキーを保持し、ユーザの認証にこのクッキーを使用して、SSO サーバで保護されているドメイン内の Web サイトの安全を守ります。

この項では、クライアントレス SSL VPN でサポートされる 4 つの SSO 認証方法について説明します。これらの認証方法には、HTTP Basic 認証と NTLMv1（NT LAN Manager）認証、Computer Associates の eTrust SiteMinder SSO サーバ（以前の Netegrity SiteMinder）、および Security Assertion Markup Language（SAML）のバージョン 1.1、POST-type SSO サーバ認証があります。

この項では、次の内容について説明します。

HTTP Basic 認証または NTLM 認証による SSO の設定

この項では、HTTP Basic 認証または NTLM 認証を使用するシングル サインオンについて説明します。この方法のいずれかまたは両方を使用して SSO を実装するように ASA を設定することができます。**auto-sign-on** コマンドを使用すると、ASA はクライアントレス SSL VPN ユーザのログインのクレデンシャル（ユーザ名およびパスワード）を内部サーバに自動的に渡すように設定されます。複数の **auto-sign-on** コマンドを入力できます。コマンドを複数回入力すると、ASA は入力順（先に入力されたコマンドを優先）にこれらを処理します。IP アドレスと IP マスク、または URI マスクのいずれかを使用してログインのクレデンシャルを受信するようにサーバに指定します。

クライアントレス SSL VPN コンフィギュレーション、クライアントレス SSL VPN グループポリシー モード、またはクライアントレス SSL VPN ユーザ名モードの 3 つのモードのいずれかで、**auto-sign-on** コマンドを使用します。ユーザ名はグループより優先され、グループはグローバルより優先されます。認証に必要な範囲のモードを選択します。

モード	範囲
webvpn コンフィギュレーション	クライアントレス SSL VPN ユーザ全員に対するグローバルな範囲
webvpn グループ ポリシー コンフィギュレーション	グループ ポリシーで定義されるクライアントレス SSL VPN ユーザのサブセット
webvpn ユーザ名コンフィギュレーション	個々のクライアントレス SSL VPN ユーザ

手順の詳細

次の例では、モードと引数の組み合わせが可能なさまざまなコマンドについて説明します。

	コマンド	目的
ステップ 1	例： `hostname(config)# webvpn` `hostname(config-webvpn)# auto-sign-on allow ip 10.1.1.1 255.255.255.0 auth-type ntlm`	NTLM 認証を使用し、10.1.1.0 ～ 10.1.1.255 の IP アドレス範囲に存在するサーバに対するすべてのクライアントレス SSL VPN ユーザからのアクセスに auto-sign-on を設定します。
ステップ 2	例： `hostname(config)# webvpn` `hostname(config-webvpn)# auto-sign-on allow uri https://*.example.com/* auth-type basic`	基本の HTTP 認証を使用するすべてのクライアントレス SSL VPN ユーザに対し、URI マスク https://*.example.com/* で定義されたサーバへのアクセスに auto-sign-on を設定します。
ステップ 3	例： `hostname(config)# group-policy ExamplePolicy attributes` `hostname(config-group-policy)# webvpn` `hostname(config-group-webvpn)# auto-sign-on allow uri https://*.example.com/* auth-type all`	基本認証または NTLM 認証を使用して、ExamplePolicy グループ ポリシーと関連付けられているクライアントレス SSL VPN セッションに対し、URI マスクで定義されたサーバへのアクセスに auto-sign-on を設定します。
ステップ 4	例： `hostname(config)# username Anyuser attributes` `hostname(config-username)# webvpn` `hostname(config-username-webvpn)# auto-sign-on allow ip 10.1.1.1 255.255.255.0 auth-type basic`	HTTP 基本認証を使用し、10.1.1.0 ～ 10.1.1.255 の IP アドレス範囲に存在するサーバに対する Anyuser と名付けられたユーザからのアクセスに auto-sign-on を設定します。
ステップ 5	`(config-webvpn)# smart-tunnel auto-sign-on` *`host-list`* `[use-domain] [realm` *`realm string`*`] [port` *`port num`*`] [host` *`host mask`* `| ip` *`address subnet mask`*`]`	特定のポートで自動サインオンを設定し、認証のレルムを設定します。

SiteMinder を使用した SSO 認証の設定

この項では、SiteMinder を使用して SSO をサポートするための ASA の設定について説明します。ユーザの Web サイトのセキュリティ インフラストラクチャにすでに SiteMinder を組み込んでいる場合は、SiteMinder を使用して SSO を実装するのが一般的です。この方式では、SSO 認証は AAA とは分離され、AAA プロセスが完了するとこの認証が 1 回行われます。

前提条件

- SSO サーバの指定。
- ASA が SSO 認証要求を作成するための SSO サーバの URL の指定。
- ASA と SSO サーバとの間でセキュアな通信を確立するための秘密キーの指定。このキーはパスワードのようなもので、ユーザが作成および保存し、Cisco Java プラグイン認証スキームを使用して ASA および SiteMinder ポリシー サーバの両方で入力します。

これらの必須のタスクに加えて、次のようなオプションの設定タスクを行うことができます。

- 認証要求のタイムアウトの設定。
- 認証要求のリトライ回数の設定。

制限

クライアントレス SSL VPN アクセスを行うユーザまたはグループに SSO を設定するには、まず RADIUS サーバや LDAP サーバなどの AAA サーバを設定する必要があります。次に、クライアントレス SSL VPN に対する SSO のサポートを設定できます。

手順の詳細

この項では、CA SiteMinder による SSO 認証をサポートするための ASA の特定の設定手順について説明します。

	コマンド	目的
ステップ 1	**webvpn**	クライアントレス SSL VPN コンフィギュレーション モードに切り替えます。
ステップ 2	**sso-server type** *type* **例：** hostname(config)# **webvpn** hostname(config-webvpn)# **sso-server Example type siteminder** hostname(config-webvpn-sso-siteminder)#	SSO サーバを作成します。 タイプが siteminder の Example という名前の SSO サーバを作成します。
ステップ 3	**config-webvpn-sso-siteminder**	SiteMinder コンフィギュレーション モードに切り替えます。
ステップ 4	**web-agent-url** **例：** hostname(config-webvpn-sso-siteminder)# **web-agent-url http://www.Example.com/webvpn** hostname(config-webvpn-sso-siteminder)#	SSO サーバの認証 URL を指定します。 http://www.Example.com/webvpn という URL に認証要求を送信します。
ステップ 5	**policy-server-secret** *secret* **例：** hostname(config-webvpn-sso-siteminder)# **policy-server-secret AtaL8rD8!** hostname(config-webvpn-sso-siteminder)#	ASA と SiteMinder との間でセキュアな認証通信を確立するための秘密キーを指定します。 秘密キー AtaL8rD8! を作成します。キーの長さは、標準またはシフト式英数字を使用した任意の文字長にできますが、ASA と SSO サーバの両方で同じキーを入力する必要があります。
ステップ 6	**request-timeout** *seconds* **例：** hostname(config-webvpn-sso-siteminder)# **request-timeout 8** hostname(config-webvpn-sso-siteminder)#	失敗した SSO 認証試行をタイムアウトさせるまでの秒数を設定します。デフォルトの秒数は 5 で、1 ～ 30 秒までの範囲で指定できます。 要求がタイムアウトするまでの秒数を 8 に変更します。
ステップ 7	**max-retry-attempts** **例：** hostname(config-webvpn-sso-siteminder)# **max-retry-attempts 4** hostname(config-webvpn-sso-siteminder)#	失敗した SSO 認証試行を ASA が再試行する回数を設定します。この回数を超えて失敗すると認証タイムアウトになります。デフォルトの再試行回数は 3 で、1 回から 5 回までの範囲で指定できます。 再試行回数を 4 に設定します。

	コマンド	目的
ステップ 8	**username-webvpn** **group-policy-webvpn**	ユーザの認証を指定する場合。 グループの認証を指定する場合。
ステップ 9	**sso-server value** *value* **例：** hostname(config)# **username Anyuser attributes** hostname(config-username)# **webvpn** hostname(config-username-webvpn)# **sso-server value** *value* hostname(config-username-webvpn)#	グループまたはユーザの SSO 認証を指定します。 Example という名前の SSO サーバを Anyuser という名前のユーザに割り当てます。
ステップ 10	**test sso-server** *server* **username** *username* **例：** hostname# **test sso-server Example username Anyuser** INFO: Attempting authentication request to sso-server Example for user Anyuser INFO: STATUS: Success hostname#	SSO サーバの設定をテストします。 Example という名前の SSO サーバをユーザ名 Anyuser を使用してテストします。

シスコの認証スキームの SiteMinder への追加

SiteMinder による SSO を使用するための ASA の設定に加え、Java プラグインとして提供されているシスコの認証スキーム（シスコの Web サイトからダウンロード）を使用するようにユーザの CA SiteMinder ポリシー サーバを設定する必要もあります。

前提条件

SiteMinder ポリシー サーバを設定するには、SiteMinder の経験が必要です。

手順の詳細

この項では、手順のすべてではなく、一般的なタスクを取り上げます。

ステップ 1　SiteMinder Administration ユーティリティを使用して、次の特定の引数を使用できるようにカスタム認証スキームを作成します。

- [Library] フィールドに、**smjavaapi** と入力します。
- [Secret] フィールドに、ASA に設定したものと同じ秘密キーを入力します。

  コマンドライン インターフェイスで **policy-server-secret** コマンドを使用して、ASA に秘密キーを設定します。
- [Parameter] フィールドに、**CiscoAuthAPI** と入力します。

ステップ 2　Cisco.com にログインして、http://www.cisco.com/cisco/software/navigator.html から **cisco_vpn_auth.jar** ファイルをダウンロードして、SiteMinder サーバのデフォルトのライブラリ ディレクトリにコピーします。この .jar ファイルは、Cisco ASA CD にも含まれています。

SAML Browser Post Profile を使用した SSO 認証の設定

この項では、認可されたユーザに対し、Security Assertion Markup Language（SAML）、バージョン 1.1 POST プロファイル シングル サインオン（SSO）をサポートするための ASA の設定について説明します。

セッション開始後、ASA は設定済みの AAA 方式に対してユーザを認証します。次に、ASA（アサーティング パーティ）は、SAML サーバが提供するコンシューマ URL サービスであるリライング パーティに対してアサーションを生成します。SAML の交換が成功すると、ユーザは保護されているリソースへのアクセスを許可されます。

前提条件

SAML Browser Post Profile を使用して SSO を設定するには、次のタスクを実行する必要があります。

- **sso-server** コマンドを使用した SSO サーバの指定
- 認証要求を行うための SSO サーバの URL の指定（**assertion-consumer-url** コマンド）
- 認証要求を発行するコンポーネントとしての ASA ホスト名の指定（**issuer** コマンド）
- SAML Post Profile アサーションの署名に使用するトラストポイント証明書の指定（**trustpoint** コマンド）

これらの必須タスクに加えて、次のようなオプションの設定タスクを行うことができます。

- 認証要求のタイムアウトの設定（**request-timeout** コマンド）
- 認証要求のリトライ回数の設定（**max-retry-attempts** コマンド）

制限

- SAML SSO は、クライアントレス SSL VPN セッションに対してのみサポートされています。
- ASA は、現在、SAML SSO サーバの Browser Post Profile タイプのみをサポートしています。
- SAML Browser Artifact プロファイル方式のアサーション交換はサポートされていません。

手順の詳細

この項では、SAML-V1.1-POST プロファイルによる SSO 認証をサポートするための ASA の特定の設定手順について説明します。

	コマンド	目的
ステップ 1	**webvpn**	クライアントレス SSL VPN コンフィギュレーション モードに切り替えます。
ステップ 2	**sso-server type** *type* **例：** hostname(config)# **webvpn** hostname(config-webvpn)# **sso-server sample type SAML-V1.1-post** hostname(config-webvpn-sso-saml)#	SSO サーバを作成します。 タイプが SAML-V1.1-POST の Sample という名前の SSO サーバを作成します。
ステップ 3	**sso saml**	クライアントレス SSL VPN sso-saml コンフィギュレーション モードに切り替えます。

	コマンド	目的
ステップ 4	**assertion-consumer-url** *url* **例：** hostname(config-webvpn-sso-saml)# **assertion-consumer-url http://www.example.com/webvpn** hostname(config-webvpn-sso-saml)#	SSO サーバの認証 URL を指定します。 http://www.Example.com/webvpn という URL に認証要求を送信します。
ステップ 5	**issuer** *string* **例：** hostname(config-webvpn-sso-saml)# **issuer myasa** hostname(config-webvpn-sso-saml)#	ASA でアサーションを生成する場合は、ASA 自体を識別します。通常、この issuer 名は ASA のホスト名になります。
ステップ 6	**trust-point** hostname(config-webvpn-sso-saml)# **trust-point mytrustpoint**	アサーションに署名するための ID 証明書を指定します。
ステップ 7	（オプション） **request-timeout** **例：** hostname(config-webvpn-sso-saml)# **request-timeout 8** hostname(config-webvpn-sso-saml)#	失敗した SSO 認証試行をタイムアウトさせるまでの秒数を設定します。 要求がタイムアウトするまでの秒数を 8 に設定します。デフォルトの秒数は 5 で、1 秒から 30 秒までの範囲で指定できます。
ステップ 8	（オプション） **max-retry-attempts** **例：** hostname(config-webvpn-sso-saml)# **max-retry-attempts 4** hostname(config-webvpn-sso-saml)#	認証がタイムアウトするまでに ASA が失敗した SSO 認証を再試行する回数を設定します。 再試行回数を 4 に設定します。デフォルトの再試行回数は 3 で、1 回から 5 回までの範囲で指定できます。
ステップ 9	webvpn	クライアントレス SSL VPN コンフィギュレーション モードに切り替えます。
ステップ 10	**group-policy-webvpn** **username-webvpn**	SSO サーバをグループ ポリシーに割り当てる場合。 SSO サーバをユーザ ポリシーに割り当てる場合。
ステップ 11	**sso-server value** **例：** hostname(config)# **username Anyuser attributes** hostname(config-username)# **webvpn** hostname(config-username-webvpn)# **sso-server value sample** hostname(config-username-webvpn)#	グループまたはユーザの SSO 認証を指定します。 Example という名前の SSO サーバを Anyuser という名前のユーザに割り当てます。

	コマンド	目的
ステップ 12	**test sso-server** **例：** hostname# **test sso-server Example username Anyuser** INFO: Attempting authentication request to sso-server sample for user Anyuser INFO: STATUS: Success	（特権 EXEC モード）SSO サーバの設定をテストします。 Example という名前の SSO サーバをユーザ名 Anyuser を使用してテストします。

SAML POST SSO サーバの設定

サーバ ソフトウェア ベンダーが提供する SAML サーバのマニュアルに従って、SAML サーバを Relying Party モードで設定します。

手順の詳細

ステップ 1　アサーティング パーティ（ASA）を表す SAML サーバ パラメータを設定します。

- Recipient consumer URL（ASA で設定する assertion consumer URL と同一）
- Issuer ID（通常はアプライアンスのホスト名である文字列）
- Profile type：Browser Post Profile

ステップ 2　証明書を設定します。

ステップ 3　アサーティング パーティのアサーションには署名が必要なことを指定します。

ステップ 4　SAML サーバがユーザを特定する方法を、次のように選択します。

- Subject Name Type が DN
- Subject Name format が uid=<user>

HTTP Form プロトコルを使用した SSO の設定

この項では、SSO における HTTP Form プロトコルの使用について説明します。HTTP Form プロトコルは、SSO 認証を実行するための手段で、AAA 方式としても使用できます。このプロトコルは、クライアントレス SSL VPN のユーザおよび認証を行う Web サーバの間で認証情報を交換するセキュアな方法を提供します。RADIUS サーバや LDAP サーバなどの他の AAA サーバと組み合わせて使用することができます。

前提条件

HTTP プロトコルを使用して SSO を正しく設定するには、認証と HTTP プロトコル交換についての詳しい実務知識が必要です。

制限

これは、一般的なプロトコルとして、認証に使用する Web サーバ アプリケーションの次の条件に一致する場合にだけ適用できます。

- 認証クッキーは、正常な要求に対して設定され、未許可のログインに対して設定されないようにする必要があります。この場合、ASA は、失敗した認証から正常な要求を識別することはできません。

手順の詳細

ASA は、ここでも認証 Web サーバに対するクライアントレス SSL VPN のユーザのプロキシとして機能しますが、この場合は、要求に対して HTTP Form プロトコルと POST 方式を使用します。フォーム データを送受信するように ASA を設定する必要があります。図 18-4 は、次の SSO 認証手順を示しています。

ステップ 1　最初に、クライアントレス SSL VPN のユーザは、ユーザ名とパスワードを入力して ASA 上のクライアントレス SSL VPN サーバにログオンします。

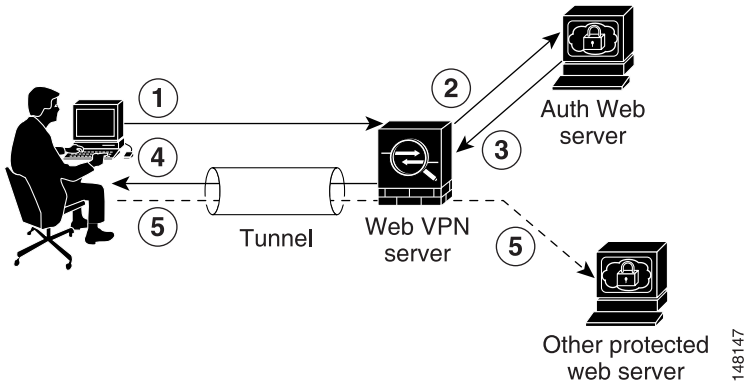
ステップ 2　ユーザのプロキシとして動作するクライアントレス SSL VPN サーバは、このフォーム データ（ユーザ名およびパスワード）を、POST 認証要求を使用して認証 Web サーバに転送します。

ステップ 3　認証 Web サーバがユーザのデータを承認した場合は、認証クッキーをユーザの代行で保存していたクライアントレス SSL VPN サーバに戻します。

ステップ 4　クライアントレス SSL VPN サーバはユーザまでのトンネルを確立します。

ステップ 5　これでユーザは、ユーザ名やパスワードを再入力しなくても、保護された SSO 環境内の他の Web サイトにアクセスできるようになります。

図 18-4　HTTP Form を使用した SSO 認証



ASA でユーザ名やパスワードなどの POST データを含めるようにフォーム パラメータを設定しても、Web サーバが要求する非表示のパラメータが追加されたことに、ユーザが最初に気付かない可能性があります。認証アプリケーションの中には、ユーザ側に表示されず、ユーザが入力することもない非表示データを要求するものもあります。ただし、認証 Web サーバが要求する非表示パラメータを見つけるのは可能です。これは、ASA を仲介役のプロキシとして使用せずに、ユーザのブラウザから Web サーバに直接認証要求を出す方法で行います。HTTP ヘッダー アナライザを使用して Web サーバの応答を分析すると、非表示パラメータが次のような形式で表示されます。

```
<param name>=<URL encoded value>&<param name>=<URL encoded>
```

非表示パラメータには、必須のパラメータとオプションのパラメータとがあります。Web サーバが非表示パラメータのデータを要求すると、Web サーバはそのデータを省略するすべての認証 POST 要求を拒否します。ヘッダー アナライザは、非表示パラメータが必須かオプションかについては伝えないため、必須のパラメータが判別できるまではすべての非表示パラメータを含めておくことをお勧めします。

HTTP Form プロトコルを使用した SSO を設定するには、次を実行する必要があります。

- フォーム データ（**action-uri**）を受信および処理するために、認証 Web サーバのユニフォーム リソース識別子を設定する。
- ユーザ名パラメータ（**user-parameter**）を設定する。
- ユーザ パスワード パラメータ（**password-parameter**）を設定する。

認証 Web サーバの要件によっては次のタスクが必要になる場合もあります。

- 認証 Web サーバがログイン前のクッキー交換を必要とする場合は、開始 URL（**start-url**）を設定する。
- 認証 Web サーバが要求する任意の非表示認証パラメータ（**hidden-parameter**）を設定する。
- 認証 Web サーバによって設定される認証クッキーの名前（**auth-cookie-name**）を設定する。

	コマンド	目的
ステップ 1	**aaa-server-host**	AAA サーバ ホスト コンフィギュレーション モードに切り替えます。
ステップ 2	**start-url** **例：** hostname(config)# **aaa-server testgrp1 protocol http-form** hostname(config)# **aaa-server testgrp1 host 10.0.0.2** hostname(config-aaa-server-host)# **start-url http://example.com/east/Area.do?Page-Grp1** hostname(config-aaa-server-host)#	認証 Web サーバが要求する場合は、認証 Web サーバから事前ログイン クッキーを取得するための URL を指定します。 http://example.com/east/Area.do?Page-Grp1 の URL 認証 Web サーバを、IP アドレス 10.0.0.2 の testgrp1 サーバ グループに指定します。

	コマンド	目的
ステップ 3	**action-uri** **例：** http://www.example.com/auth/index.html/appdir/authc/forms/MCOlogin.fcc?TYPE=33554433&REALMOID=06-000a1311-a828-1185-ab41-8333b16a0008&GUID=&SMAUTHREASON=0&METHOD=GET&SMAGENTNAME=SM5FZmjnk3DRNwNjk2KcqVCFbIrNT9%2bJ0H0KPshFtg6rB1UV2PxkHqLw%3d%3d&TARGET=https%3A%2F%2Fauth.example.com このアクション URI を指定するには、次のコマンドを入力します。 hostname(config-aaa-server-host)# **action-uri http://www.example.com/auth/index.htm** hostname(config-aaa-server-host)# **action-uri l/appdir/authc/forms/MCOlogin.fcc?TYP** hostname(config-aaa-server-host)# **action-uri 554433&REALMOID=06-000a1311-a828-1185** hostname(config-aaa-server-host)# **action-uri -ab41-8333b16a0008&GUID=&SMAUTHREASON** hostname(config-aaa-server-host)# **action-uri =0&METHOD=GET&SMAGENTNAME=SM5FZmjnk** hostname(config-aaa-server-host)# **action-uri 3DRNwNjk2KcqVCFbIrNT9%2bJ0H0KPshFtg6r** hostname(config-aaa-server-host)# **action-uri B1UV2PxkHqLw%3d%3d&TARGET=https%3A%2F** hostname(config-aaa-server-host)# **action-uri %2Fauth.example.com** hostname(config-aaa-server-host)#	認証 Web サーバ上の認証プログラムの URI を指定します。 1 つの URI を連続する複数行にわたって入力することができます。1 行あたりの最大文字数は 255 です。URI 全体の最大文字数は 2048 です。 アクション URI にホスト名とプロトコルを含める必要があります。この例では、これらは http://www.example.com の URI の最初に表示されます。
ステップ 4	**user-parameter** **例：** hostname(config-aaa-server-host)# **user-parameter userid** hostname(config-aaa-server-host)#	HTTP POST 要求の **userid** のユーザ名パラメータを設定します。
ステップ 5	**password-parameter** **例：** hostname(config-aaa-server-host)# **password-parameter user_password** hostname(config-aaa-server-host)#	HTTP POST 要求の **user_password** ユーザ パスワード パラメータを設定します。

	コマンド	目的
ステップ 6	**hidden-parameter** **例：** SMENC=ISO-8859-1&SMLOCALE=US-EN&target=https%3A%2F%2Fwww.example.com%2Femco%2Fappdir%2FAreaRoot.do%3FEMCOPageCode%3DENG&smauthreason=0 この非表示パラメータを指定するには、次のコマンドを入力します。 hostname(config)# **aaa-server testgrp1 host example.com** hostname(config-aaa-server-host)# **hidden-parameter SMENC=ISO-8859-1&SMLOCALE=US-EN&targe** hostname(config-aaa-server-host)# **hidden-parameter t=https%3A%2F%2Fwww.example.com%2Femc** hostname(config-aaa-server-host)# **hidden-parameter o%2Fappdir%2FAreaRoot.do%3FEMCOPageCo** hostname(config-aaa-server-host)# **hidden-parameter de%3DENG&smauthreason=0** hostname(config-aaa-server-host)#	認証 Web サーバと交換するための非表示パラメータを指定します。 POST 要求から抜粋した非表示パラメータの例を示します。この非表示パラメータには、間を & で区切った 4 つの Form エントリとその値が含まれています。エントリとその値は次のとおりです。 • SMENC、値は ISO-8859-1。 • SMLOCALE、値は US-EN。 • target エントリおよび値 https%3A%2F%2Fwww.example.com%2Femco%2Fappdir%2FAreaRoot.do • %3FEMCOPageCode%3DENG。 • smauthreason、値は 0。
ステップ 7	（オプション） **auth-cookie-name** *cookie-name* **例：** hostname(config-aaa-server-host)# **auth-cookie-name SsoAuthCookie** hostname(config-aaa-server-host)#	認証クッキーの名前を指定します。 SsoAuthCookie の認証クッキー名を指定します。
ステップ 8	**tunnel-group general-attributes**	トンネル グループ一般属性コンフィギュレーション モードに切り替えます。
ステップ 9	**authentication-server-group** **例：** hostname(config)# **tunnel-group testgroup general-attributes** hostname(config-tunnel-general)**#authentication-server-group testgrp1**	前の手順で設定された SSO サーバを使用するためのトンネル グループを設定します。 /testgrp1/ という名前の SSO サーバを使用するための、/testgroup/ という名前のトンネル グループを設定します。
ステップ 10	**aaa-server-host**	AAA サーバ ホスト コンフィギュレーション モードに切り替えます。

	コマンド	目的
ステップ 11	**hidden-parameter** **例：** SMENC=ISO-8859-1&SMLOCALE=US-EN&target=https%3A%2F%2Fwww.example.com%2Femco%2Fappdir%2FAreaRoot.do%3FEMCOPageCode%3DENG&smauthreason=0 この非表示パラメータを指定するには、次のコマンドを入力します。 hostname(config)# **aaa-server testgrp1 host example.com** hostname(config-aaa-server-host)# **hidden-parameter SMENC=ISO-8859-1&SMLOCALE=US-EN&targe** hostname(config-aaa-server-host)# **hidden-parameter t=https%3A%2F%2Fwww.example.com%2Femc** hostname(config-aaa-server-host)# **hidden-parameter o%2Fappdir%2FAreaRoot.do%3FEMCOPageCo** hostname(config-aaa-server-host)# **hidden-parameter de%3DENG&smauthreason=0** hostname(config-aaa-server-host)#	認証 Web サーバと交換するための非表示パラメータを指定します。 POST 要求から抜粋した非表示パラメータの例を示します。この非表示パラメータには、間を & で区切った 4 つの Form エントリとその値が含まれています。エントリとその値は次のとおりです。 • SMENC、値は ISO-8859-1。 • SMLOCALE、値は US-EN。 • target エントリおよび値 https%3A%2F%2Fwww.example.com%2Femco%2Fappdir%2FAreaRoot.do • %3FEMCOPageCode%3DENG。 • smauthreason、値は 0。
ステップ 12	（オプション） **auth-cookie-name** *cookie-name* **例：** hostname(config-aaa-server-host)# **auth-cookie-name SsoAuthCookie** hostname(config-aaa-server-host)#	認証クッキーの名前を指定します。 SsoAuthCookie の認証クッキー名を指定します。
ステップ 13	**tunnel-group general-attributes**	トンネル グループ一般属性モードに切り替えます。
ステップ 14	**authentication-server-group** *group* **例：** hostname(config)# **tunnel-group testgroup general-attributes** hostname(config-tunnel-general)**#authentication-server-group testgrp1**	前の手順で設定された SSO サーバを使用するためのトンネル グループを設定します。 /testgrp1/ という名前の SSO サーバを使用するための、/testgroup/ という名前のトンネル グループを設定します。

HTTP Form データの収集

この項では、必要な HTTP Form データを検出および収集する手順を示します。認証 Web サーバが要求するパラメータが何かわからない場合は、認証交換を分析するとパラメータ データを収集することができます。

前提条件

これらの手順では、ブラウザと HTTP ヘッダー アナライザが必要です。

手順の詳細

ステップ 1　ユーザのブラウザと HTTP ヘッダー アナライザを起動して、ASA を経由せずに Web サーバのログイン ページに直接接続します。

ステップ 2　Web サーバのログイン ページがユーザのブラウザにロードされてから、ログイン シーケンスを検証して交換時にクッキーが設定されているかどうか判別します。Web サーバによってログイン ページにクッキーがロードされている場合は、このログイン ページの URL を *start-URL* として設定します。

ステップ 3　Web サーバにログオンするためのユーザ名とパスワードを入力して、Enter を押します。この動作によって、ユーザが検証する認証 POST 要求が HTTP ヘッダー アナライザを使用して生成されます。

次に、ホストの HTTP ヘッダーおよび本文が記載された POST 要求の例を示します。

```
POST
/emco/myemco/authc/forms/MCOlogin.fcc?TYPE=33554433&REALMOID=06-000430e1-7443-125c-ac05-83
846dc90034&GUID=&SMAUTHREASON=0&METHOD=GET&SMAGENTNAME=$SM$5FZmjnk3DRNwNjk2KcqVCFbIrNT9%2b
J0H0KPshFtg6rB1UV2PxkHqLw%3d%3d&TARGET=https%3A%2F%2Fwww.example.com%2Femco%2Fmyemco%2FHTT
P/1.1

Host: www.example.com

(BODY)

SMENC=ISO-8859-1&SMLOCALE=US-EN&USERID=Anyuser&USER_PASSWORD=XXXXXX&target=https%3A%2F%2Fw
ww.example.com%2Femco%2Fmyemco%2F&smauthreason=0
```

ステップ 4　POST 要求を検証してプロトコル、ホストをコピーし、URL を入力して action-uri パラメータを設定します。

ステップ 5　POST 要求の本文を検証して、次の情報をコピーします。

a. ユーザ名パラメータ。上記の例では、このパラメータは *USERID* で、値 *anyuser* ではありません。

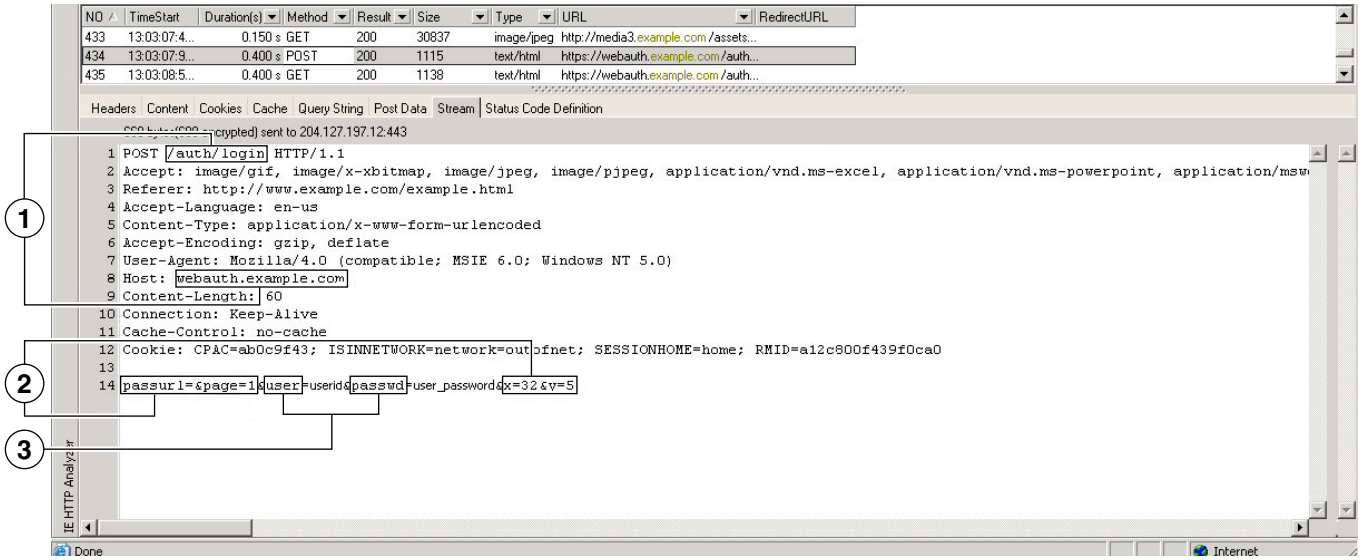
b. パスワード パラメータ。上記の例では、このパラメータは *USER_PASSWORD* です。

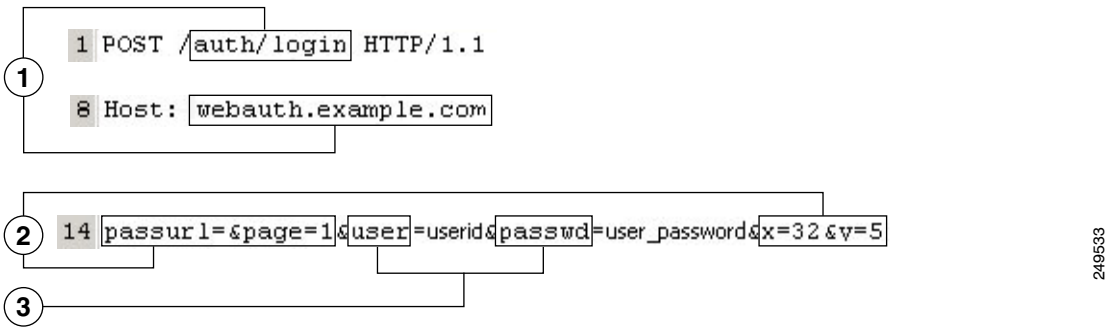
c. 非表示パラメータ。このパラメータは、POST 本文からユーザ名パラメータとパスワード パラメータを除くすべてです。前の例の非表示パラメータは次のとおりです。

SMENC=ISO-8859-1&SMLOCALE=US-EN&target=https%3A%2F%2Fwww.example.com%2Femco%2Fmyemco%2F&smauthreason=0

図 18-5 は、HTTP アナライザの出力例に表示されるアクション URI、非表示、ユーザ名、パスワードの各種パラメータを強調して示したものです。これは一例です。出力は Web サイトによって大幅に異なることがあります。

図 18-5　　action-uri、非表示、ユーザ名、パスワードの各種パラメータ





1	action URI パラメータ
2	非表示パラメータ
3	ユーザ名パラメータとパスワード パラメータ

ステップ 6　Web サーバへのログオンが成功したら、HTTP ヘッダー アナライザを使用して、サーバからユーザのブラウザに設定されているクッキー名を見つけ出すことによって、サーバの応答を検証します。これは **auth-cookie-name** パラメータです。

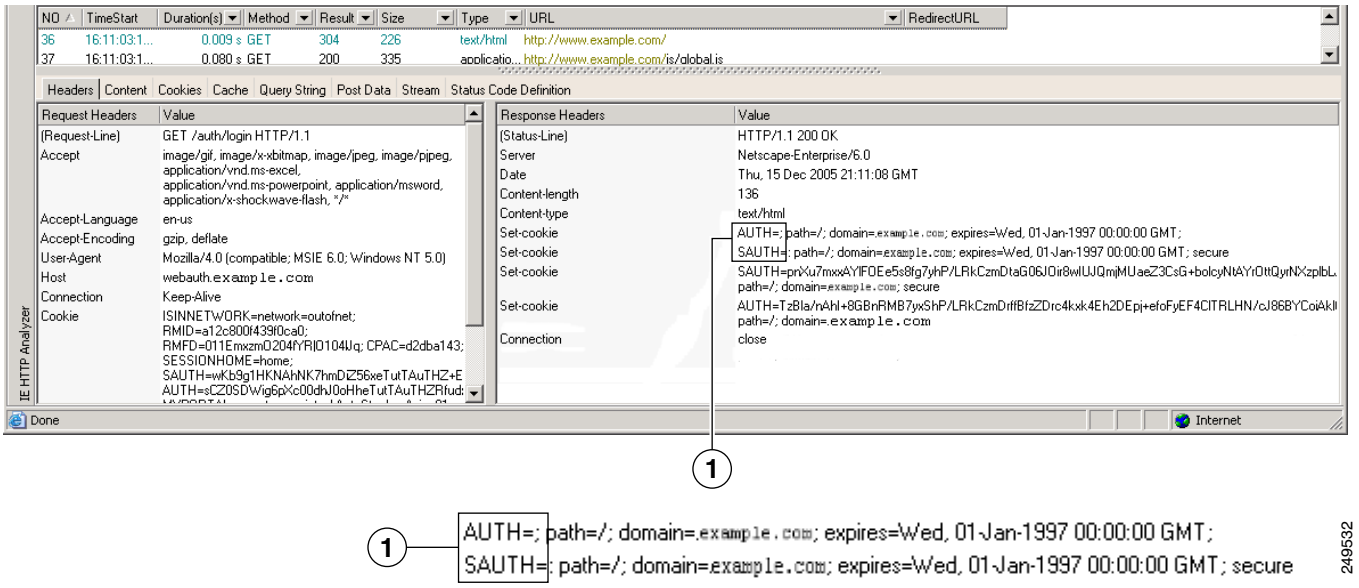
次のサーバ応答ヘッダーでは、SMSESSION がセッションのクッキーの名前です。必要なのはこの名前だけです。値は不要です。

```
Set-Cookie:

SMSESSION=yN4Yp5hHVNDgs4FT8dn7+Rwev41hsE49XlKc+1twie0gqnjbhkTkUnR8XWP3hvDH6PZPbHI
HtWLDKTa8ngDB/lbYTjIxrbDx8WPWwaG3CxVa3adOxHFR8yjD55GevK3ZF4ujgU1lhO6fta0dSSOSepWv
nsCb7IFxCw+MGiw0o88uHa2t4l+SillqfJvcpuXfiIAO06D/gtDF40Ow5YKHEl2KhDEvv+yQzxwfEz2cl
7Ef5iMr8LgGcDK7qvMcvrgUqx68JQOK2+RSwtHQ15bCZmsDU5vQVCvSQWC8OMHNGwpS253XwRLvd/h6S/
tM0k98QMv+i3N8oOdj1V7flBqecH7+kVrU01F6oFzr0zM1kMyLr5HhlVDh7B0k9wp0dUFZiAzaf43jupD
5f6CEkuLeudYW1xgNzsR8eqtPK6t1gFJyOn0s7QdNQ7q9knsPJsekRAH9hrLBhWBLTU/3B1QS94wEGD2Y
TuiW36TiP14hYwOlCAYRj2/bY3+lYzVu7EmzMQ+UefYxh4cF2gYD8RZL2RwmP9JV5l48I3XBFPNUw/3V5
jf7nRuLr/CdfK3OO8+Pa3V6/nNhokErSgyxjzMd88DVzM41LxxaUDhbcmkoHT9ImzBvKzJX0J+o7FoUDF
OxEdIqlAN4GNqk49cpi2sXDbIarALp6Bl3+tbB4MlHGH+0CPscZXqoi/kon9YmGauHyRs+0m6wthdlAmC
nvlJCDfDoXtn8DpabgiW6VDTrvl3SGPyQtUv7Wdahuq5SxbUzjY2JxQnrUtwB977NCzYu2sOtN+dsERwW
J6ueyJBbMzKyzUB4L3i5uSYN50B4PCv1w5KdRKa5p3N0Nfq6RM6dfipMEJw0Ny1sZ7ohz3fbvQ/YZ7lw/
k7ods/8VbaR15ivkE8dSCzuf/AInHtCzuQ6wApzEp9CUoG8/dapWriHjNoi4llJOgCst33wEhxFxcWy2U
Wxs4EZSjsI5GyBnefSQTPVfma5dc/emWor9vWr0HnTQaHP5rg5dTNqunkDEdMIHfbeP3F90cZejVzihM6
igiS6P/CEJAjE;Domain=.example.com;Path=/
```

図 18-6 に、HTTP アナライザによる認可クッキーの出力例を示します。これは一例です。出力は Web サイトによって大幅に異なることがあります。

図 18-6　　HTTP アナライザの出力例に表示された認可クッキー



1	認可クッキー

ステップ 7　場合によっては、認証の成否にかかわらず同じクッキーがサーバによって設定される可能性があり、このようなクッキーは、SSO の目的上、認められません。クッキーが異なっていることを確認するには、無効なログイン クレデンシャルを使用してステップ 1 からステップ 6 を繰り返し、「失敗」クッキーと「成功した」クッキーとを比較します。これで、HTTP Form プロトコルによる SSO を ASA に設定するために必要なパラメータ データを入手できました。

プラグインの SSO の設定

プラグインは、シングル サインオン（SSO）をサポートします。プラグインは、クライアントレス SSL VPN セッションを認証するときに入力したクレデンシャルと同じクレデンシャル（ユーザ名とパスワード）を使用します。プラグインはマクロ置換をサポートしないため、内部ドメイン パスワードなどのさまざまなフィールドや、RADIUS または LDAP サーバの属性で SSO を実行するオプションはありません。

プラグインに対して SSO サポートを設定するには、プラグインをインストールし、サーバへのリンクを表示するためのブックマーク エントリを追加します。また、csco_sso=1 パラメータを使用して SSO サポートを指定します。次に、SSO 用にイネーブルにするプラグインのブックマークの例を示します。

```
ssh://ssh-server/?cisco_sso=1
rdp://rdp-server/?Parameter1=value&Parameter2=value&csco_sso=1
```

マクロ置換による SSO の設定

ここでは、SSO のマクロ置換の使用について説明します。マクロ置換を使用して SSO を設定することで、ブックマークに特定の変数を挿入して動的な値に置換できます。

（注） スマート トンネル ブックマークでは、自動サインオンはサポートされていますが変数置換はサポートされていません。たとえば、スマート トンネル向けに設定された SharePoint ブックマークは、アプリケーションにログオンするために、クライアントレス SSL VPN にログオンするために使用するクレデンシャルと同じユーザ名とパスワードを使用します。変数置換および自動サインオンは同時に、または別々に使用できます。

一部の Web ページでの自動サインオンに、マクロ置換を含むブックマークを使用できるようになりました。以前の POST プラグイン アプローチは、管理者がサインオン マクロを含む POST ブックマークを指定し、POST 要求のポストの前にロードするキックオフ ページを受信できるようにするために作成されました。この POST プラグイン アプローチでは、クッキーまたはその他のヘッダー項目の存在を必要とする要求は排除されました。現在は、管理者は事前ロード ページおよび URL を決定し、これによってポスト ログイン要求の送信場所が指定されます。事前ロード ページによって、エンドポイント ブラウザは、クレデンシャルを含む POST 要求を使用するのではなく、Web サーバまたは Web アプリケーションに送信される特定の情報を取得できます。

次に、ブックマーク内の置換およびフォームベースの HTTP POST 操作が可能な変数（またはマクロ）を示します。

- CSCO_WEBVPN_USERNAME：ユーザのログイン ID
- CSCO_WEBVPN_PASSWORD：ユーザのログイン パスワード
- CSCO_WEBVPN_INTERNAL_PASSWORD：ユーザの内部（または、ドメイン）パスワード このキャッシュ済みクレデンシャルは、AAA サーバに対して認証されません。この値を入力すると、セキュリティ アプライアンスは、パスワードまたはプライマリ パスワードの値ではなく、この値を自動サインオンのパスワードとして使用します。

  （注） 上記の 3 つの変数は、GET ベースの HTTP（S）ブックマークでは使用できません。これらの値を使用できるのは、POST ベースの HTTP（S）および CIFS ブックマークだけです。

- CSCO_WEBVPN_CONNECTION_PROFILE：ユーザのログイン グループ ドロップダウン（接続プロファイル エイリアス）
- CSCO_WEBVPN_MACRO1：RADIUS-LDAP ベンダー固有属性（VSA）によって設定。LDAP から ldap-attribute-map コマンドをマッピングしている場合、このマクロの Cisco 属性である WebVPN-Macro-Substitution-Value1 を使用します。次の URL にある、Active Directory での LDAP 属性マッピングの例を参照してください。
  http://www.cisco.com/en/US/docs/security/asa/asa83/configuration/guide/ref_extserver.html#wp1572118

  RADIUS による CSCO_WEBVPN_MACRO1 のマクロ置換は、VSA#223 によって行われます（表 18-1 を参照）。

表 18-1　　VSA#223

WebVPN-Macro-Value1	Y	223	文字列	シングル	無制限
WebVPN-Macro-Value2	Y	224	文字列	シングル	無制限

  特定の DAP またはグループ ポリシーについて、https://CSCO_WEBVPN_MACRO1 や https://CSCO_WEBVPN_MACRO2 のようにすると、www.cisco.com/email などの値が、クライアントレス SSL VPN ポータルのブックマークに動的に読み込まれます。
- CSCO_WEBVPN_MACRO2：RADIUS-LDAP のベンダー固有属性（VSA）によって設定されます。LDAP から ldap-attribute-map コマンドをマッピングしている場合、このマクロの Cisco 属性である WebVPN-Macro-Substitution-Value2 を使用します。次の URL にある、Active Directory での LDAP 属性マッピングの例を参照してください。
  http://www.cisco.com/en/US/docs/security/asa/asa83/configuration/guide/ref_extserver.html#wp1572118

  RADIUS による CSCO_WEBVPN_MACRO2 のマクロ置換は、VSA#224 によって行われます（表 18-1 を参照）。

クライアントレス SSL VPN が（ブックマークの形式または POST 形式の）エンドユーザの要求内にあるこれらの 6 つの文字列のいずれかを認識するたびに、文字列がユーザ指定の値に置き換えられ、この要求がリモート サーバに渡されます。

ユーザ名とパスワードのルックアップが ASA で失敗した場合は、空の文字列で置き換えられ、動作は自動サインインが不可の場合の状態に戻されます。

ユーザ名とパスワードの要求

ネットワークによっては、リモート セッション中にユーザが、コンピュータ、インターネット サービス プロバイダー、クライアントレス SSL VPN、メール サーバ、ファイル サーバ、企業アプリケーションの一部またはすべてにログインする必要が生じることがあります。ユーザはさまざまなコンテキストで認証を行うために、固有のユーザ名、パスワード、PIN などさまざまな情報が要求される場合があります。

表 18-2 に、クライアントレス SSL VPN ユーザが知っておく必要のあるユーザ名とパスワードのタイプを示します。

表 18-2　クライアントレス SSL VPN セッションのユーザに提供するユーザ名とパスワード

ログイン ユーザ名/パスワード タイプ	目的	入力するタイミング
コンピュータ	コンピュータへのアクセス	コンピュータの起動
インターネット サービス プロバイダー	インターネットへのアクセス	インターネット サービス プロバイダーへの接続
クライアントレス SSL VPN	リモート ネットワークへのアクセス	クライアントレス SSL VPN の起動
ファイル サーバ	リモート ファイル サーバへのアクセス	クライアントレス SSL VPN ファイル ブラウジング機能を使用して、リモート ファイル サーバにアクセスするとき
企業アプリケーションへのログイン	ファイアウォールで保護された内部サーバへのアクセス	クライアントレス SSL VPN Web ブラウジング機能を使用して、保護されている内部 Web サイトにアクセスするとき
メール サーバ	クライアントレス SSL VPN 経由によるリモート メール サーバへのアクセス	電子メール メッセージの送受信

セキュリティのヒントの通知

ユーザはいつでもツールバーの [Logout] アイコンをクリックして、クライアントレス SSL VPN セッションを閉じることができます（ブラウザ ウィンドウを閉じてもセッションは閉じません）。

クライアントレス SSL VPN は、企業ネットワーク上のリモート PC やワークステーションと ASA との間のデータ転送のセキュリティを保証するものです。クライアントレス SSL VPN を使用してもすべてのサイトとの通信がセキュアであるとは限らないことを、ユーザに通知してください。したがって、ユーザが HTTPS 以外の Web リソース（インターネット上や内部ネットワーク上にあるもの）にアクセスする場合、企業の ASA から目的の Web サーバまでの通信は暗号化されていないため、プライベートではありません。

「クライアントレス SSL VPN セキュリティ対策」（P.1）に、セッション内で実行する手順に応じて、ユーザと通信するための追加のヒントを示します。

クライアントレス SSL VPN の機能を使用するためのリモート システムの設定

ここでは、クライアントレス SSL VPN を使用するためのリモート システムの設定方法について説明します。

ユーザ アカウントを別々に設定でき、各ユーザは異なるクライアントレス SSL VPN の機能を使用できます。

クライアントレス SSL VPN の起動

次のようなサポートされている接続を使用して、インターネットに接続できます。

- 家庭の DSL、ケーブル、ダイヤルアップ。
- 公共のキオスク。
- ホテルのホットスポット。
- 空港の無線ノード。
- インターネット カフェ。

（注）　クライアントレス SSL VPN がサポートする Web ブラウザのリストについては、『*Supported VPN Platforms, Cisco ASA Series*』を参照してください。

前提条件

- ポート転送を介してアプリケーションにアクセスするために、ブラウザでクッキーをイネーブルにする必要があります。
- クライアントレス SSL VPN の URL が必要です。URL は、https://*address* の形式の https アドレスである必要があります。*address* は、SSL VPN がイネーブルである ASA（またはロード バランシング クラスタ）のインターフェイスの IP アドレスまたは DNS ホスト名です。たとえば、https://cisco.example.com などです。
- クライアントレス SSL VPN のユーザ名とパスワードが必要です。

制限

- クライアントレス SSL VPN ではローカル印刷がサポートされていますが、VPN 経由による企業ネットワーク上のプリンタへの印刷はサポートされていません。

クライアントレス SSL VPN フローティング ツールバーの使用

フローティング ツールバーを使用すると、クライアントレス SSL VPN を簡単に使用できます。ツールバーを使用して、メインのブラウザ ウィンドウに影響を与えずに、URL の入力、ファイルの場所のブラウズ、設定済み Web 接続の選択ができます。

フローティング ツールバーは、現在のクライアントレス SSL VPN セッションを表します。[Close] ボタンをクリックすると、ASA によってクライアントレス SSL VPN セッションを閉じることを求めるメッセージが表示されます。

ヒント　テキストをテキスト フィールドに貼り付けるには、**Ctrl** を押した状態で **V** を押します（クライアントレス SSL VPN セッション中は、表示されるツールバー上での右クリックはオフになっています）。

制限

ポップアップをブロックするようにブラウザが設定されている場合、フローティング ツールバーは表示できません。

Web のブラウズ

クライアントレス SSL VPN を使用しても、すべてのサイトとの通信がセキュアになるわけではありません。「セキュリティのヒントの通知」を参照してください。

クライアントレス SSL VPN での Web ブラウジングのルックアンドフィールは、ユーザが使い慣れたものと異なる場合があります。次に例を示します。

- クライアントレス SSL VPN のタイトル バーが各 Web ページの上部に表示される。
- Web サイトへのアクセス方法：
  - クライアントレス SSL VPN [Home] ページ上の **[Enter Web Address]** フィールドに URL を入力する
  - クライアントレス SSL VPN [Home] ページ上にある設定済みの Web サイト リンクをクリックする
  - 上記 2 つのどちらかの方法でアクセスした Web ページ上のリンクをクリックする

また、特定のアカウントの設定によっては、次のようになる場合もあります。

- 一部の Web サイトがブロックされている
- 使用可能な Web サイトが、クライアントレス SSL VPN [Home] ページ上にリンクとして表示されるものに限られる

前提条件

保護されている Web サイトのユーザ名とパスワードが必要です。

制限

また、特定のアカウントの設定によっては、次のようになる場合もあります。

- 一部の Web サイトがブロックされている
- 使用可能な Web サイトが、クライアントレス SSL VPN [Home] ページ上にリンクとして表示されるものに限られる

ネットワークのブラウズ（ファイル管理）

ユーザは、組織ネットワークを介してファイルを見つける方法に慣れていない場合があります。

（注）　コピー処理の進行中は、**Copy File to Server** コマンドを中断したり、別の画面に移動したりしないでください。コピー処理を中断すると、不完全なファイルがサーバに保存される可能性があります。

前提条件

- 共有リモート アクセス用にファイル アクセス権を設定する必要があります。
- 保護されているファイル サーバのサーバ名とパスワードが必要です。
- フォルダとファイルが存在するドメイン、ワークグループ、およびサーバの名前が必要です。

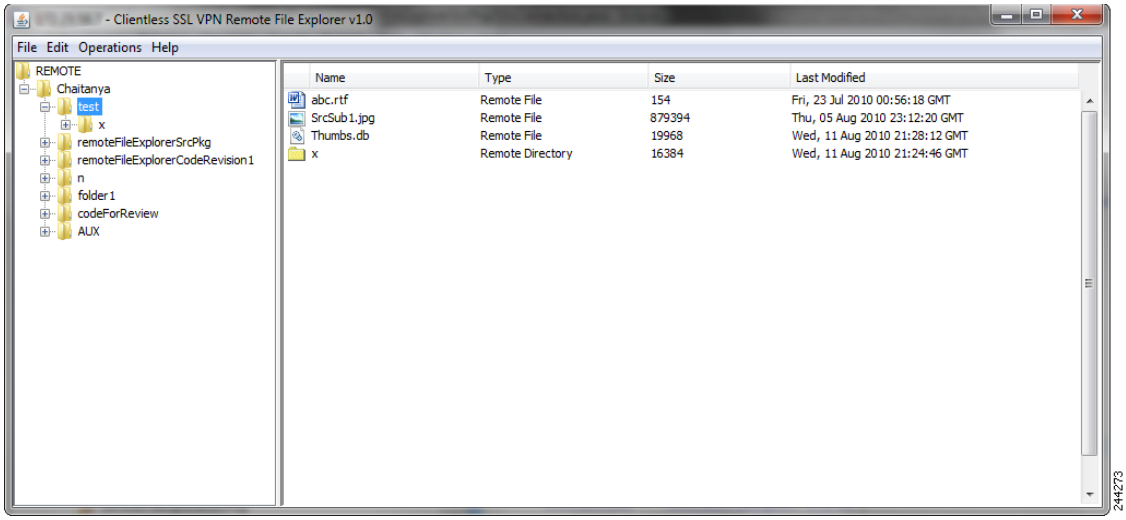
制限

クライアントレス SSL VPN を介してアクセスできるのは、共有フォルダと共有ファイルに限られます。

Remote File Explorer の使用

ユーザは、Remote File Explorer を使用して、Web ブラウザから企業ネットワークをブラウズできます。ユーザが Cisco SSL VPN ポータル ページの [Remote File System] アイコンをクリックすると、ユーザのシステムでアプレットが起動し、ツリーおよびフォルダ ビューにリモート ファイル システムが表示されます。

図 18-7　Clientless SSL VPN Remote File Explorer



ユーザはブラウザで次を実行できます。

- リモート ファイル システムのブラウズ。
- ファイルの名前の変更。
- リモート ファイル システム内、およびリモートとローカルのファイル システム間でのファイルの移動またはコピー。
- ファイルのバルク アップロードおよびダウンロードの実行。

（注） この機能では、ユーザのマシンに Oracle Java ランタイム環境（JRE）1.4 以降がインストールされ、Web ブラウザで Java がイネーブルになっている必要があります。リモート ファイルの起動には、JRE 1.6 以降が必要です。

ファイルまたはフォルダの名前変更

ファイルまたはフォルダの名前を変更するには、次の手順を実行します。

ステップ 1　名前を変更するファイルまたはフォルダをクリックします。

ステップ 2　**[Edit] > [Rename]** を選択します。

ステップ 3　プロンプトが表示されたら、ダイアログに新しい名前を入力します。

ステップ 4　**[OK]** をクリックして、ファイルまたはフォルダの名前を変更します。または、名前を変更しない場合は **[Cancel]** をクリックします。

リモート サーバでのファイルやフォルダの移動またはコピー

リモート サーバでファイルやフォルダを移動またはコピーするには、次の手順を実行します。

ステップ 1　移動またはコピーするファイルやフォルダが含まれている送信元フォルダに移動します。

ステップ 2　ファイルまたはフォルダをクリックします。

ステップ 3　ファイルをコピーするには、**[Edit] > [Copy]** を選択します。また、ファイルを移動するには、**[Edit] > [Cut]** を選択します。

ステップ 4　宛先フォルダに移動します。

ステップ 5　**[Edit] > [Paste]** を選択します。

ローカル システム ドライブからリモート フォルダへのファイルのコピー

ローカル ファイル システムとリモート ファイル システム間でファイルをコピーするには、リモート ファイル ブラウザの右ペインとローカル ファイル マネージャ アプリケーション間でファイルをドラッグ アンド ドロップします。

ファイルのアップロードおよびダウンロード

ファイルをダウンロードするには、ブラウザでファイルをクリックし、**[Operations] > [Download]** を選択し、**[Save]** ダイアログで場所と名前を指定してファイルを保存します。

ファイルをアップロードするには、宛先フォルダをクリックし、**[Operations] > [Upload]** を選択し、**[Open]** ダイアログでファイルの場所と名前を指定します。

この機能には次の制限があります。

- ユーザは、アクセスを許可されていないサブフォルダを表示できません。
- ユーザがアクセスを許可されていないファイルは、ブラウザに表示されても移動またはコピーできません。
- ネストされたフォルダの最大の深さは 32 です。
- ツリー ビューでは、ドラッグ アンド ドロップのコピーがサポートされていません。
- Remote File Explorer の複数のインスタンスの間でファイルを移動するときは、すべてのインスタンスが同じサーバを探索する必要があります（ルート共有）。
- Remote File Explorer は、1 つのフォルダに最大 1500 のファイルおよびフォルダを表示できます。フォルダがこの制限を超えた場合、フォルダは表示されません。

ポート転送の使用

（注）　ユーザは、**[Close]** アイコンをクリックしてアプリケーションを終了したら、必ず [Application Access] ウィンドウを閉じる必要があります。このウィンドウを正しく閉じないと、Application Access またはアプリケーション自体がオフに切り替わる可能性があります。詳細については、「Application Access 使用時の hosts ファイル エラーからの回復」（P.21-1）を参照してください。

前提条件

- Mac OS X の場合、この機能をサポートしているのは Safari ブラウザだけです。
- クライアント アプリケーションがインストールされている必要があります。
- ブラウザでクッキーをイネーブルにする必要があります。
- DNS 名を使用してサーバを指定する場合、hosts ファイルの変更に必要になるため、PC に対する管理者アクセス権が必要です。

- Oracle Java ランタイム環境（JRE）バージョン 1.4.x と 1.5.x がインストールされている必要があります。

  JRE がインストールされていない場合は、ポップアップ ウィンドウが表示され、インストールを開始できるサイトがユーザに示されます。まれに、Java 例外エラーで、ポート転送アプレットが失敗することがあります。このような状況が発生した場合は、次の手順を実行します。

  a. ブラウザのキャッシュをクリアして、ブラウザを閉じます。
  b. Java アイコンがコンピュータのタスク バーに表示されていないことを確認します。
  c. Java のインスタンスをすべて閉じます。
  d. クライアントレス SSL VPN セッションを確立し、ポート転送 Java アプレットを起動します。
- ブラウザで javascript をイネーブルにする必要があります。デフォルトではイネーブルに設定されています。
- 必要に応じて、クライアント アプリケーションを設定する必要があります。

（注） Microsoft Outlook クライアントの場合、この設定手順は不要です。Windows 以外のすべてのクライアント アプリケーションでは、設定が必要です。Windows アプリケーションの設定が必要かどうかを確認するには、[Remote Server] フィールドの値をチェックします。[Remote Server] フィールドにサーバ ホスト名が含まれている場合、クライアント アプリケーションの設定は不要です。[Remote Server] フィールドに IP アドレスが含まれている場合、クライアント アプリケーションを設定する必要があります。

制限

この機能を使用するには、Oracle Java ランタイム環境（JRE）をインストールしてローカル クライアントを設定する必要があります。これには、ローカル システムでの管理者の許可、または C:\windows\System32\drivers\etc の完全な制御が必要になるため、ユーザがパブリック リモート システムから接続した場合に、アプリケーションを使用できない可能性があります。

手順の詳細

クライアント アプリケーションを設定するには、ローカルにマッピングされたサーバの IP アドレスとポート番号を使用します。この情報を見つけるには、次の手順を実行します。

1. クライアントレス SSL VPN セッションを開始して、[Home] ページの **[Application Access]** リンクをクリックします。[Application Access] ウィンドウが表示されます。
2. [Name] カラムで、使用するサーバ名を確認し、このサーバに対応するクライアント IP アドレスとポート番号を [Local] カラムで確認します。
3. この IP アドレスとポート番号を使用して、クライアント アプリケーションを設定します。設定手順は、クライアント アプリケーションによって異なります。

（注） クライアントレス SSL VPN セッション上で実行しているアプリケーションで URL（電子メール メッセージ内のものなど）をクリックしても、サイトがそのセッションで開くわけではありません。サイトをセッション上で開くには、その URL を [Enter Clientless SSL VPN (URL) Address] フィールドに貼り付けます。

ポート転送を介した電子メールの使用

電子メールを使用するには、クライアントレス SSL VPN のホームページから Application Access を起動します。これにより、メール クライアントが使用できるようになります。

（注）　IMAP クライアントの使用中にメール サーバとの接続が中断したり、新しく接続を確立できない場合は、IMAP アプリケーションを終了してクライアントレス SSL VPN を再起動します。

前提条件

アプリケーション アクセスおよびその他のメール クライアントの要件を満たしている必要があります。

制限

Microsoft Outlook Express バージョン 5.5 および 6.0 はテスト済みです。

クライアントレス SSL VPN は、Lotus Notes および Eudora などの、ポート転送を介したその他の SMTPS、POP3S、または IMAP4S 電子メール プログラムをサポートしますが、動作確認は行っていません。

Web アクセスを介した電子メールの使用

次の電子メール アプリケーションがサポートされています。

- Microsoft Outlook Web App to Exchange Server 2010

  OWA には、Internet Explorer 7 以降、または Firefox 3.01 以降が必要です。
- Microsoft Outlook Web Access to Exchange Server 2007、2003、および 2000

  最適な結果を得るために、Internet Explorer 8.x 以降または Firefox 8.x で OWA を使用してください。
- Louts iNotes

前提条件

Web ベースの電子メール製品がインストールされている必要があります。

制限

その他の Web ベースの電子メール アプリケーションも動作しますが、動作確認は行っていません。

電子メール プロキシを介した電子メールの使用

次のレガシー電子メール アプリケーションがサポートされています。

- Microsoft Outlook 2000 および 2002
- Microsoft Outlook Express 5.5 および 6.0

メール アプリケーションの使用方法と例については、「クライアントレス SSL VPN を介した電子メールの使用」（P.15-14）を参照してください。

前提条件

- SSL 対応メール アプリケーションがインストールされている必要があります。
- ASA SSL バージョンを TLSv1 Only に設定しないでください。Outlook および Outlook Express では TLS はサポートされません。
- メール アプリケーションが正しく設定されている必要があります。

制限

その他の SSL 対応クライアントも動作しますが、動作確認は行っていません。

スマート トンネルの使用

スマート トンネルの使用に管理権限は必要ありません。

（注）　ポート フォワーダの場合と異なり、Java は自動的にダウンロードされません。

前提条件

- スマート トンネルには、Windows では ActiveX または JRE（1.4x および 1.5x）、Mac OS X では Java Web Start が必要です。
- ブラウザでクッキーをイネーブルにする必要があります。
- ブラウザで javascript をイネーブルにする必要があります。

制限

- Mac OS X では、フロントサイド プロキシはサポートされていません。
- 「スマート トンネル アクセスの設定」（P.16-4）で指定されているオペレーティング システムおよびブラウザだけがサポートされています。
- TCP ソケットベースのアプリケーションだけがサポートされています。

CHAPTER 19

モバイル デバイスでのクライアントレス SSL VPN

2013 年 9 月 13 日

モバイル デバイスでのクライアントレス SSL VPN の使用

Pocket PC または他の認定されたモバイル デバイスからクライアントレス SSL VPN にアクセスできます。認定されたモバイル デバイスでクライアントレスの SSL VPN を使用するために、ASA 管理者またはクライアントレス SSL VPN ユーザは特別なことを行う必要はありません。

シスコは、次のモバイル デバイス プラットフォームを認定しています。

HP iPaq H4150

Pocket PC 2003

Windows CE 4.20.0, build 14053

Pocket Internet Explorer (PIE)

ROM version 1.10.03ENG

ROM Date: 7/16/2004

クライアントレス SSL VPN のモバイル デバイスのバージョンによって、次のような相違点があります。

- ポップアップのクライアントレス SSL VPN ウィンドウはバナー Web ページに置き換わっています。
- 標準のクライアントレス SSL VPN フローティング ツールバーがアイコン バーに置き換わっています。このバーには、[Go]、[Home]、および [Logout] の各種ボタンが表示されます。
- メインのクライアントレス SSL VPN ポータル ページに [Show Toolbar] アイコンがありません。
- クライアントレス SSL VPN のログアウト時に、警告メッセージで PIE ブラウザを正しく閉じる手順が表示されます。この手順に従わないで通常の方法でブラウザのウィンドウを閉じると、クライアントレス SSL VPN または HTTPS を使用するすべてのセキュアな Web サイトから PIE が切断されません。

制限

- クライアントレス SSL VPN は、OWA 2000 版および OWA 2003 版の基本認証をサポートする。OWA サーバに基本認証を設定せずにクライアントレス SSL VPN ユーザがこのサーバにアクセスしようとするとアクセスは拒否されます。
- サポートされていないクライアントレス SSL VPN の機能
  - Application Access および他の Java 依存の各種機能
  - HTTP プロキシ
  - Citrix Metaframe 機能（PDA に対応する Citrix ICA クライアント ソフトウェアが装備されていない場合）

CHAPTER 20

クライアントレス SSL VPN のカスタマイズ

クライアントレス SSL VPN エンド ユーザの設定

この項は、エンド ユーザのためにクライアントレス SSL VPN を設定するシステム管理者を対象にしています。ここでは、エンド ユーザ インターフェイスをカスタマイズする方法について説明します。

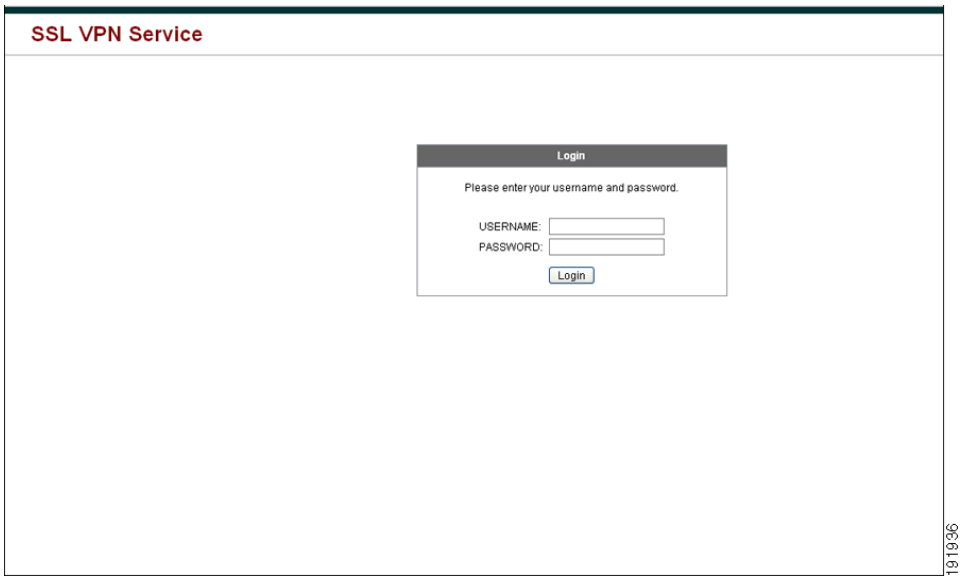
この項では、リモート システムの設定要件と作業の概要を説明します。ユーザがクライアントレス SSL VPN の使用を開始するために、ユーザに伝える必要のある情報を明確にします。説明する項目は次のとおりです。

- エンド ユーザ インターフェイスの定義
- クライアントレス SSL VPN ページのカスタマイズ
- カスタマイゼーションに関する情報
- カスタマイゼーション テンプレートのエクスポート
- カスタマイゼーション テンプレートの編集

エンド ユーザ インターフェイスの定義

クライアントレス SSL VPN エンド ユーザ インターフェイスは一連の HTML パネルで構成されます。ユーザは、ASA インターフェイスの IP アドレスを https://*address* 形式で入力することにより、クライアントレス SSL VPN にログインします。最初に表示されるパネルは、ログイン画面（図 20-1）です。

図 20-1　　クライアントレス SSL VPN の [Login] 画面



クライアントレス SSL VPN ホームページの表示

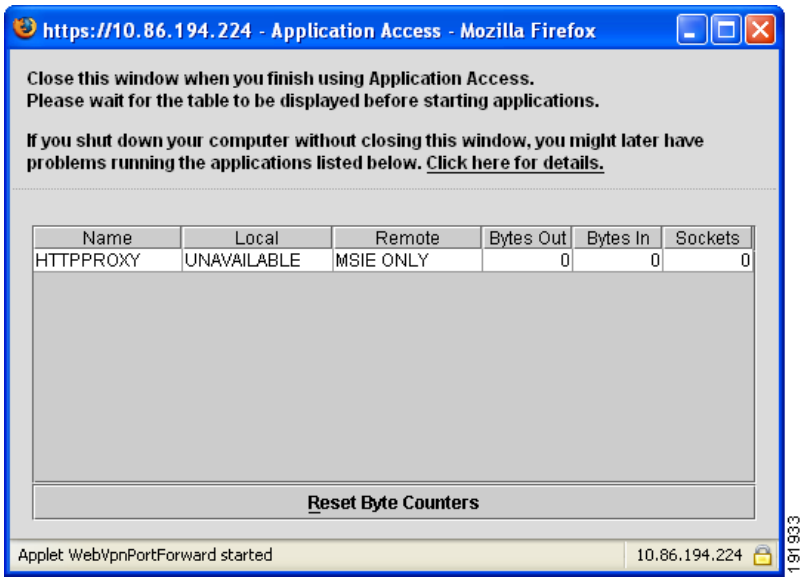
ユーザがログインすると、ポータル ページが開きます。

ホームページには設定済みのクライアントレス SSL VPN 機能がすべて表示され、選択済みのロゴ、テキスト、および色が外観に反映されています。このサンプル ホームページには、特定のファイル共有の指定機能以外のすべてのクライアントレス SSL VPN 機能が表示されています。ユーザはこのホームページを使用して、ネットワークのブラウズ、URL の入力、特定の Web サイトへのアクセス、および Application Access（ポート転送とスマート トンネル）による TCP アプリケーションへのアクセスを実行できます。

クライアントレス SSL VPN の Application Access パネルの表示

ポート転送またはスマート トンネルを開始するには、[Application Access] ボックスの **[Go]** ボタンをクリックします。[Application Access] ウィンドウが開きます（図 20-2）。

図 20-2　　クライアントレス SSL VPN の [Application Access] ウィンドウ



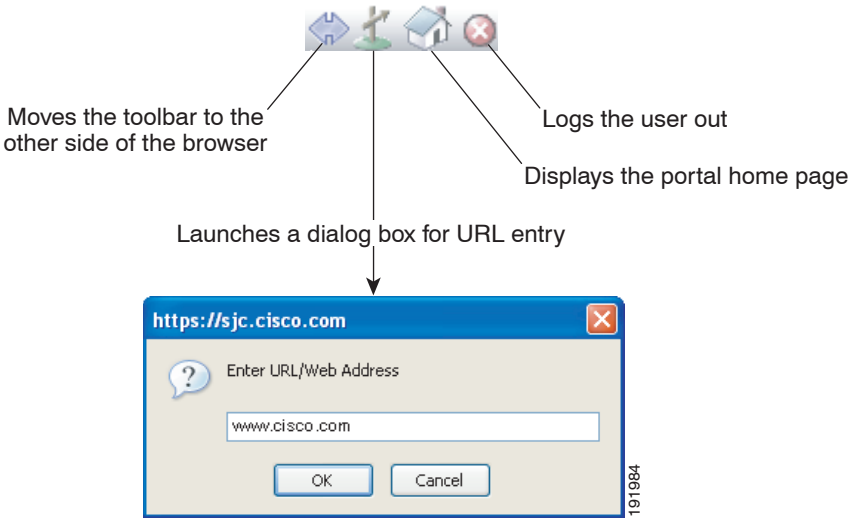
このウィンドウには、このクライアントレス SSL VPN 接続用に設定された TCP アプリケーションが表示されます。このパネルを開いたままでアプリケーションを使用する場合は、通常の方法でアプリケーションを起動します。

（注） ステートフル フェールオーバーでは、Application Access を使用して確立したセッションは保持されません。ユーザはフェールオーバー後に再接続する必要があります。

フローティング ツールバーの表示

図 20-3 に示すフローティング ツールバーは、現在のクライアントレス SSL VPN セッションを表します。

図 20-3　クライアントレス SSL VPN フローティング ツールバー



フローティング ツールバーの次の特性に注意してください。

- ツールバーを使用して、メインのブラウザ ウィンドウに影響を与えずに、URL の入力、ファイルの場所のブラウズ、設定済み Web 接続の選択ができます。
- ポップアップをブロックするようにブラウザが設定されている場合、フローティング ツールバーは表示できません。
- ツールバーを閉じると、ASA はクライアントレス SSL VPN セッションを終了するよう促すメッセージを表示します。

クライアントレス SSL VPN ページのカスタマイズ

クライアントレス SSL VPN ユーザに表示されるポータル ページの外観を変えることができます。変更できる外観には、ユーザがセキュリティ アプライアンスに接続するときに表示される [Login] ページ、セキュリティ アプライアンスのユーザ認証後に表示される [Home] ページ、ユーザがアプリケーションを起動するときに表示される [Application Access] ウィンドウ、およびユーザがクライアントレス SSL VPN セッションからログアウトするときに表示される [Logout] ページが含まれます。

ポータル ページのカスタマイズ後は、このカスタマイゼーションを保存して、特定の接続プロファイル、グループ ポリシー、またはユーザに適用できます。ASA をリロードするか、またはクライアントレス SSL をオフに切り替えてから再度イネーブルにするまで、変更は適用されません。

いくつものカスタマイゼーション オブジェクトを作成、保存して、個々のユーザまたはユーザグループに応じてポータル ページの外観を変更するようにセキュリティ アプライアンスをイネーブル化できます。

- 「カスタマイゼーションに関する情報」（P.20-5）
- 「カスタマイゼーション テンプレートのエクスポート」（P.20-5）
- 「カスタマイゼーション テンプレートの編集」（P.20-6）
- 「カスタマイゼーション オブジェクトのインポート」（P.20-12）
- 「接続プロファイル、グループ ポリシー、およびユーザへのカスタマイゼーションの適用」（P.20-12）
- 「ログイン画面の高度なカスタマイゼーション」（P.20-14）

カスタマイゼーションに関する情報

ASA は、カスタマイゼーション オブジェクトを使用して、ユーザ画面の外観を定義します。カスタマイゼーション オブジェクトは、リモート ユーザに表示されるカスタマイズ可能なすべての画面項目に対する XML タグを含む XML ファイルからコンパイルされます。ASA ソフトウェアには、リモート PC にエクスポートできるカスタマイゼーション テンプレートが含まれています。このテンプレートを編集して、新しいカスタマイゼーション オブジェクトとして ASA にインポートし戻すことができます。

カスタマイゼーション オブジェクトをエクスポートすると、XML タグを含む XML ファイルが、指定した URL に作成されます。カスタマイゼーション オブジェクトによって作成される *Template* という名前の XML ファイルには、空の XML タグが含まれており、新しいカスタマイゼーション オブジェクトを作成するための基礎として利用できます。このオブジェクトは変更したり、キャッシュ メモリから削除したりすることはできませんが、エクスポートし、編集して、新しいカスタマイゼーション オブジェクトとして再度 ASA にインポートできます。

カスタマイゼーション オブジェクト、接続プロファイル、およびグループ ポリシー

ユーザが初めて接続するときには、接続プロファイル（トンネル グループ）で指定されたデフォルトのカスタマイゼーション オブジェクト（*DfltCustomization*）がログイン画面の表示方法を決定します。接続プロファイル リストがイネーブルになっている場合に、独自のカスタマイゼーションがある別のグループをユーザが選択すると、その新しいグループのカスタマイゼーション オブジェクトを反映して画面が変わります。

リモート ユーザが認証された後は、画面の外観は、そのグループ ポリシーにカスタマイゼーション オブジェクトが割り当てられているかどうかによって決まります。

カスタマイゼーション テンプレートのエクスポート

カスタマイゼーション オブジェクトをエクスポートすると、指定した URL に XML ファイルが作成されます。カスタマイゼーション テンプレート（*Template*）は、空の XML タグを含んでおり、新しいカスタマイゼーション オブジェクトを作成するためのベースになります。このオブジェクトは変更したり、キャッシュ メモリから削除したりすることはできませんが、エクスポートし、編集して、新しいカスタマイゼーション オブジェクトとして再度 ASA にインポートできます。

手順の詳細

	コマンド	目的
ステップ 1	**export webvpn customization**	カスタマイゼーション オブジェクトをエクスポートし、XML タグの変更を許可します。
ステップ 2	**import webvpn customization** **例：** hostname# **export webvpn customization DfltCustomization tftp://209.165.200.225/dflt_custom** !!!!!!!!!!!!!!!!INFO: Customization object 'DfltCustomization' was exported to tftp://10.86.240.197/dflt_custom hostname#	新しいオブジェクトとしてファイルをインポートします。 デフォルトのカスタマイゼーション オブジェクト（DfltCustomization）をエクスポートして、*dflt_custom* という名前の XML ファイルを作成します。

カスタマイゼーション テンプレートの編集

この項では、カスタマイゼーション テンプレートの内容を示して、便利な図を提供しています。これらを参照して、正しい XML タグをすばやく選択して、画面表示を変更できます。

テキスト エディタまたは XML エディタを使用して、XML ファイルを編集できます。次の例は、カスタマイゼーション テンプレートの XML タグを示しています。一部の冗長タグは、見やすくするために削除してあります。

例：

```
<custom>
   <localization>
      <languages>en,ja,zh,ru,ua</languages>
      <default-language>en</default-language>
   </localization>
    <auth-page>
      <window>
          <title-text l10n="yes"><![CDATA[SSL VPN Service]]></title-text>
      </window>
      <full-customization>
          <mode>disable</mode>
          <url></url>
      </full-customization>
      <language-selector>
        <mode>disable</mode>
        <title l10n="yes">Language:</title>
        <language>
          <code>en</code>
          <text>English</text>
        </language>
        <language>
          <code>zh</code>
          <text>ä¸-å›½ (Chinese)</text>
        </language>
        <language>
          <code>ja</code>
          <text>æ—¥æœ¬ (Japanese)</text>
        </language>
        <language>
          <code>ru</code>
          <text>Ð ÑƒÑÑкиÐ¹ (Russian)</text>
        </language>
        <language>
          <code>ua</code>
          <text>Ð£ÐºÑ Ð°Ñ—Ð½ÑÑŒÐºÐ° (Ukrainian)</text>
        </language>
      </language-selector>
      <logon-form>
          <title-text l10n="yes"><![CDATA[Login]]></title-text>
          <title-background-color><![CDATA[#666666]]></title-background-color>
          <title-font-color><![CDATA[#ffffff]]></title-font-color>
          <message-text l10n="yes"><![CDATA[Please enter your username and
password.]]></message-text>
          <username-prompt-text l10n="yes"><![CDATA[USERNAME:]]></username-prompt-text>
          <password-prompt-text l10n="yes"><![CDATA[PASSWORD:]]></password-prompt-text>
          <internal-password-prompt-text l10n="yes">Internal
Password:</internal-password-prompt-text>
          <internal-password-first>no</internal-password-first>
          <group-prompt-text l10n="yes"><![CDATA[GROUP:]]></group-prompt-text>
          <submit-button-text l10n="yes"><![CDATA[Login]]></submit-button-text>
          <title-font-color><![CDATA[#ffffff]]></title-font-color>
```

```
            <title-background-color><![CDATA[#666666]]></title-background-color>
            <font-color>#000000</font-color>
            <background-color>#ffffff</background-color>
            <border-color>#858A91</border-color>
        </logon-form>
        <logout-form>
            <title-text l10n="yes"><![CDATA[Logout]]></title-text>
            <message-text l10n="yes"><![CDATA[Goodbye.<br>

For your own security, please:<br>

<li>Clear the browser's cache

<li>Delete any downloaded files

<li>Close the browser's window]]></message-text>
            <login-button-text l10n="yes">Logon</login-button-text>
            <hide-login-button>no</hide-login-button>
            <title-background-color><![CDATA[#666666]]></title-background-color>
            <title-font-color><![CDATA[#ffffff]]></title-font-color>
            <title-font-color><![CDATA[#ffffff]]></title-font-color>
            <title-background-color><![CDATA[#666666]]></title-background-color>
            <font-color>#000000</font-color>
            <background-color>#ffffff</background-color>
            <border-color>#858A91</border-color>
        </logout-form>
        <title-panel>
           <mode>enable</mode>
           <text l10n="yes"><![CDATA[SSL VPN Service]]></text>
           <logo-url l10n="yes">/+CSCOU+/csco_logo.gif</logo-url>
           <gradient>yes</gradient>
           <style></style>
           <background-color><![CDATA[#ffffff]]></background-color>
           <font-size><![CDATA[larger]]></font-size>
           <font-color><![CDATA[#800000]]></font-color>
           <font-weight><![CDATA[bold]]></font-weight>
        </title-panel>
        <info-panel>
          <mode>disable</mode>
          <image-url l10n="yes">/+CSCOU+/clear.gif</image-url>
          <image-position>above</image-position>
          <text l10n="yes"></text>
        </info-panel>
        <copyright-panel>
           <mode>disable</mode>
           <text l10n="yes"></text>
        </copyright-panel>
      </auth-page>
      <portal>
        <title-panel>
           <mode>enable</mode>
           <text l10n="yes"><![CDATA[SSL VPN Service]]></text>
           <logo-url l10n="yes">/+CSCOU+/csco_logo.gif</logo-url>
           <gradient>yes</gradient>
           <style></style>
           <background-color><![CDATA[#ffffff]]></background-color>
           <font-size><![CDATA[larger]]></font-size>
           <font-color><![CDATA[#800000]]></font-color>
           <font-weight><![CDATA[bold]]></font-weight>
        </title-panel>
        <browse-network-title l10n="yes">Browse Entire Network</browse-network-title>
        <access-network-title l10n="yes">Start AnyConnect</access-network-title>
        <application>
           <mode>enable</mode>
```

```
   <id>home</id>
   <tab-title l10n="yes">Home</tab-title>
   <order>1</order>
</application>
<application>
   <mode>enable</mode>
   <id>web-access</id>
   <tab-title l10n="yes"><![CDATA[Web Applications]]></tab-title>
   <url-list-title l10n="yes"><![CDATA[Web Bookmarks]]></url-list-title>
   <order>2</order>
</application>
<application>
   <mode>enable</mode>
   <id>file-access</id>
   <tab-title l10n="yes"><![CDATA[Browse Networks]]></tab-title>
   <url-list-title l10n="yes"><![CDATA[File Folder Bookmarks]]></url-list-title>
   <order>3</order>
</application>
<application>
   <mode>enable</mode>
   <id>app-access</id>
   <tab-title l10n="yes"><![CDATA[Application Access]]></tab-title>
   <order>4</order>
</application>
<application>
   <mode>enable</mode>
   <id>net-access</id>
   <tab-title l10n="yes">AnyConnect</tab-title>
   <order>4</order>
</application>
<application>
   <mode>enable</mode>
   <id>help</id>
   <tab-title l10n="yes">Help</tab-title>
   <order>1000000</order>
</application>
<toolbar>
   <mode>enable</mode>
   <logout-prompt-text l10n="yes">Logout</logout-prompt-text>
   <prompt-box-title l10n="yes">Address</prompt-box-title>
   <browse-button-text l10n="yes">Browse</browse-button-text>
</toolbar>
<column>
   <width>100%</width>
   <order>1</order>
</column>
<pane>
   <type>TEXT</type>
   <mode>disable</mode>
   <title></title>
   <text></text>
   <notitle></notitle>
   <column></column>
   <row></row>
   <height></height>
</pane>
<pane>
   <type>IMAGE</type>
   <mode>disable</mode>
   <title></title>
   <url l10n="yes"></url>
   <notitle></notitle>
   <column></column>
   <row></row>
```

```
            <height></height>
         </pane>
         <pane>
            <type>HTML</type>
            <mode>disable</mode>
            <title></title>
            <url l10n="yes"></url>
            <notitle></notitle>
            <column></column>
            <row></row>
            <height></height>
         </pane>
         <pane>
            <type>RSS</type>
            <mode>disable</mode>
            <title></title>
            <url l10n="yes"></url>
            <notitle></notitle>
            <column></column>
            <row></row>
            <height></height>
         </pane>
         <url-lists>
            <mode>group</mode>
         </url-lists>
         <home-page>
            <mode>standard</mode>
            <url></url>
         </home-page>
      </portal>
</custom>
```

図 20-4 に、[Login] ページとページをカスタマイズする XML タグを示します。これらのタグはすべて、上位レベルのタグ <auth-page> にネストされています。

図 20-4　[Login] ページと関連の XML タグ

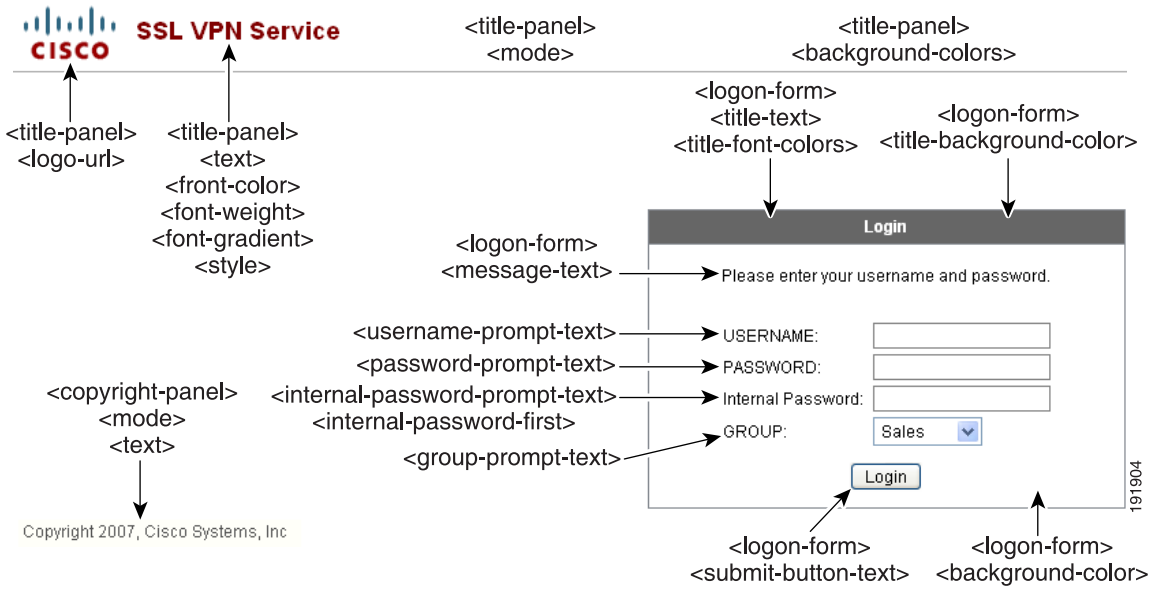


図 20-5 は、[Login] ページで使用可能な言語セレクタ ドロップダウン リストと、この機能をカスタマイズするための XML タグを示しています。これらのタグはすべて、上位レベルの <auth-page> タグにネストされています。

図 20-5　　[Login] 画面上の言語セレクタと関連の XML タグ

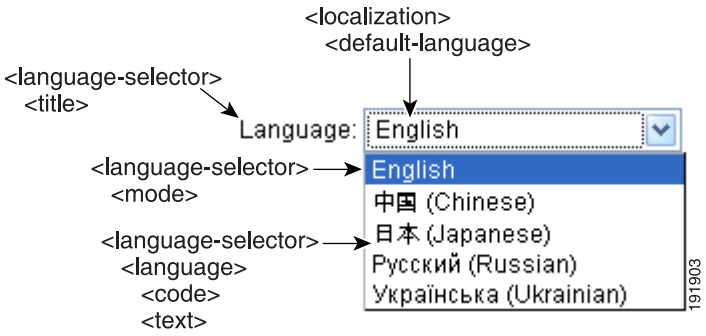
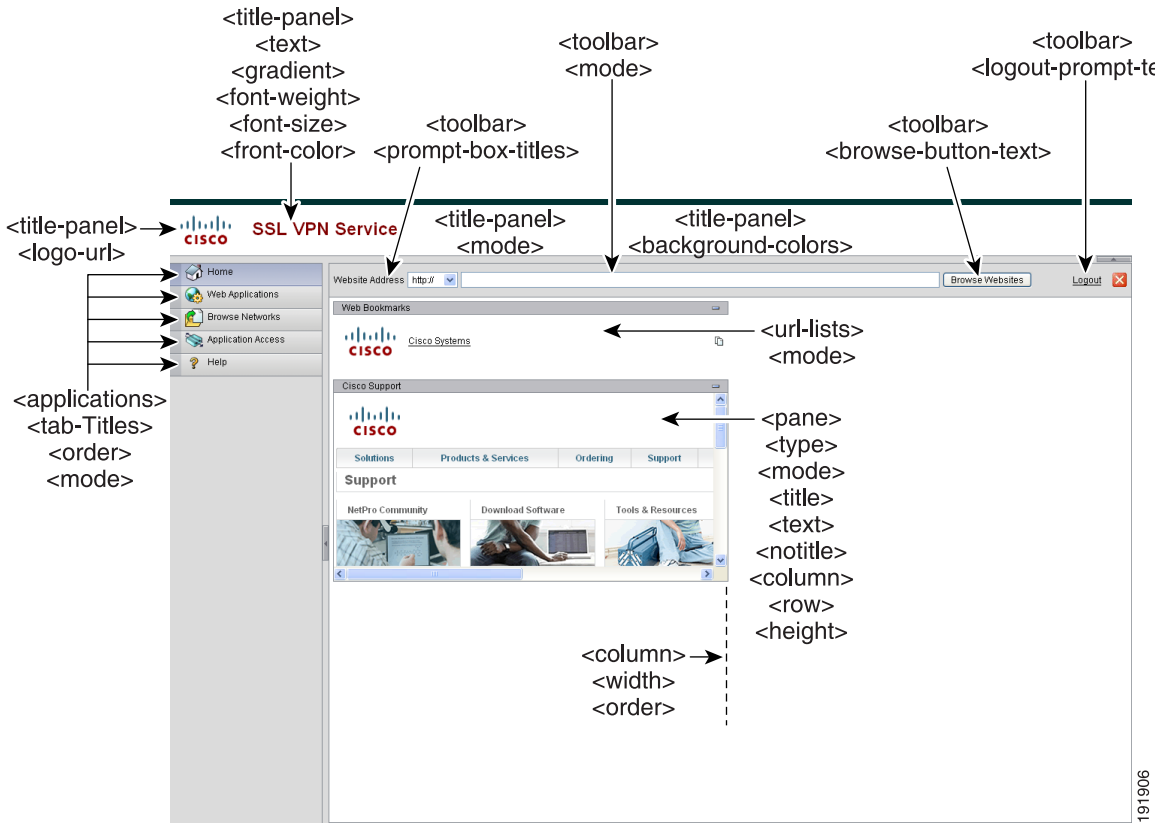


図 20-6 は、[Login] ページで使用できる Information Panel とこの機能をカスタマイズするための XML タグを示しています。この情報は [Login] ボックスの左側または右側に表示されます。これらのタグは、上位レベルの <auth-page> タグにネストされています。

図 20-6　　[Login] 画面上の Information Panel と関連の XML タグ

図 20-7 は、ポータル ページとこの機能をカスタマイズするための XML タグを示しています。これらのタグは、上位レベルの <auth-page> タグにネストされています。

図 20-7　ポータル ページと関連の XML タグ



カスタマイゼーション オブジェクトのインポート

XML ファイルを編集して保存した後、次のコマンドを使用して、ASA のキャッシュ メモリにインポートします。

手順の詳細

	コマンド	目的
ステップ 1	**import webvpn customization**	ASA のキャッシュ メモリに XML ファイルをインポートします。カスタマイゼーション オブジェクトをインポートする場合、ASA は XML コードの有効性をチェックします。コードが有効な場合、ASA はそのオブジェクトをキャッシュ メモリ内の非表示の場所に保存します。
	例： hostname# **import webvpn customization custom1 tftp://209.165.201.22/customization /General.xml** Accessing tftp://209.165.201.22/customization/General.xml...!!! Writing file disk0:/csco_config/97/custom1...!! 329994 bytes copied in 5.350 secs (65998 bytes/sec)	カスタマイゼーション オブジェクト *General.xml* を 209.165.201.22/customization の URL からインポートして、*custom1* という名前を付けます。

接続プロファイル、グループ ポリシー、およびユーザへのカスタマイゼーションの適用

カスタマイゼーションの作成後、**customization** コマンドを使用して、接続プロファイル（トンネル グループ）、グループ、またはユーザにそのカスタマイゼーションを適用できます。このコマンドで表示されるオプションは、使用中のモードによって異なります。

（注） ポータル ページのカスタマイズ後は、ASA をリロードするか、またはクライアントレス SSL をディセーブルにしてから再度イネーブルにするまで、変更は適用されません。

接続プロファイル、グループ ポリシー、およびユーザの設定に関する詳細については、『*Cisco ASA シリーズ VPN CLI コンフィギュレーション ガイド*』の「接続プロファイル、グループ ポリシー、およびユーザ」を参照してください。

手順の詳細

	コマンド	目的
ステップ 1	**webvpn**	クライアントレス SSL VPN コンフィギュレーション モードに切り替えます。
ステップ 2	**tunnel-group webvpn** または **group-policy webvpn** または **username webvpn**	トンネルグループ クライアントレス SSL VPN コンフィギュレーション モードに切り替えます。 グループ ポリシーのクライアントレス SSL VPN コンフィギュレーションに切り替えます。 ユーザ名のクライアントレス SSL VPN コンフィギュレーションに切り替えます。
ステップ 3	**customization** ***name*** **例：** hostname(config)# **tunnel-group cisco_telecommuters webvpn-attributes** hostname(tunnel-group-webvpn)# **customization cisco** または **customization {none | value** ***name*****}** **例：** hostname(config)# **group-policy cisco_sales attributes** hostname(config-group-policy)# **webvpn** hostname(config-username-webvpn)# **customization value ?** config-username-webvpn mode commands/options: Available configured customization profiles: DfltCustomization cisco hostname(config-group-webvpn)# **customization value cisco** **例：** hostname(config)# **username cisco_employee attributes** hostname(config-username)# **webvpn** hostname(config-username-webvpn)# **customization value cisco**	接続プロファイルにカスタマイゼーションを適用します。name は、接続プロファイルに適用するカスタマイゼーションの名前です。 トンネルグループ クライアントレス SSL VPN コンフィギュレーション モードを開始し、接続プロファイル *cisco_telecommutes* に対してカスタマイゼーション *cisco* をイネーブルにします。 グループまたはユーザにカスタマイゼーションを適用します。次のオプションが含まれます。 • **none** は、グループまたはユーザのカスタマイゼーションをディセーブルにして値が継承されないようにするオプションで、デフォルトのクライアントレス SSL VPN ページを表示します。 • **value** *name* は cu の名前です。 グループ ポリシー クライアントレス SSL VPN コンフィギュレーション モードを開始し、セキュリティ アプライアンスにカスタマイゼーションのリストのクエリーを実行し、グループ ポリシー *cisco_sales* に対してカスタマイゼーション *cisco* をイネーブルにします。 ユーザ名クライアントレス SSL VPN コンフィギュレーション モードを開始し、ユーザ *cisco_employee* に対してカスタマイゼーション *cisco* をイネーブルにします。

	コマンド	目的
ステップ 4	(オプション) `[no] customization name` または `[no] customization {none | value name}`	コンフィギュレーションからコマンドを削除して、接続プロファイルからカスタマイゼーションを削除します。 コンフィギュレーションからコマンドを削除し、デフォルトに戻します。
ステップ 5	**customization** コマンドに続けて疑問符（?）。	既存のカスタマイゼーションのリストを表示します。

ログイン画面の高度なカスタマイゼーション

提供されるログイン画面の特定の画面要素を変更するのではなく、独自のカスタム ログイン画面を使用する場合は、*フル カスタマイゼーション*機能を使用してこの高度なカスタマイゼーションを実行できます。

フル カスタマイゼーションを使用して、独自のログイン画面の HTML を入力し、ASA で関数を呼び出す Cisco HTML コードを挿入します。これで、Login フォームと言語セレクタ ドロップダウン リストが作成されます。

この項では、独自の HTML コードを作成するために必要な修正内容、および ASA が独自のコードを使用する場合に設定する必要があるタスクについて説明します。

図 20-8 に、クライアントレス SSL VPN ユーザに表示される標準の Cisco ログイン画面を示します。Login フォームは、HTML コードで呼び出す関数によって表示されます。

図 20-8　　標準の Cisco [Login] ページ

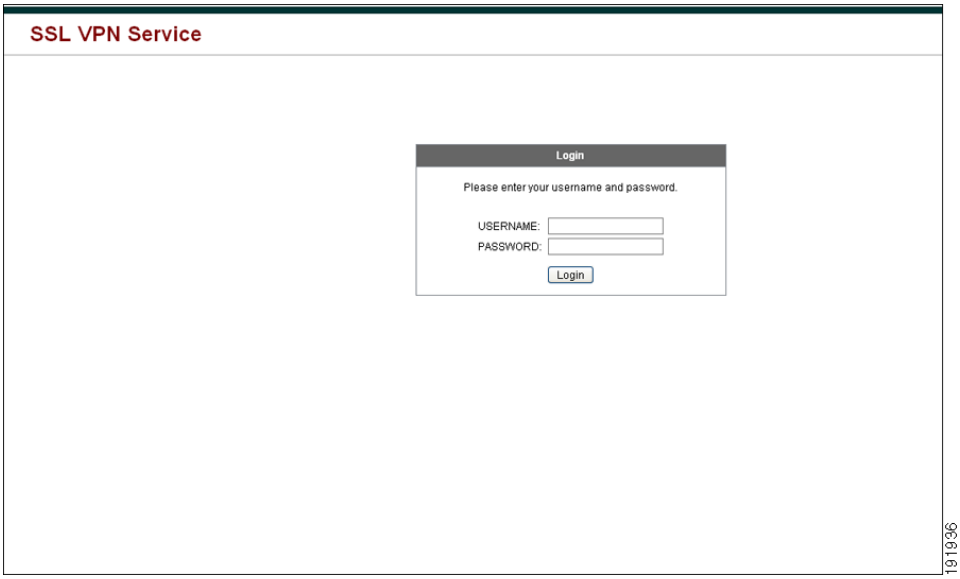


図 20-9 に、言語セレクタ ドロップダウン リストを示します。この機能は、クライアントレス SSL VPN ユーザにはオプションとなっており、ログイン画面の HTML コード内の関数によっても呼び出されます。

図 20-9　　言語セレクタ ドロップダウン リスト

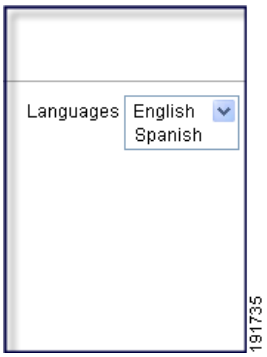
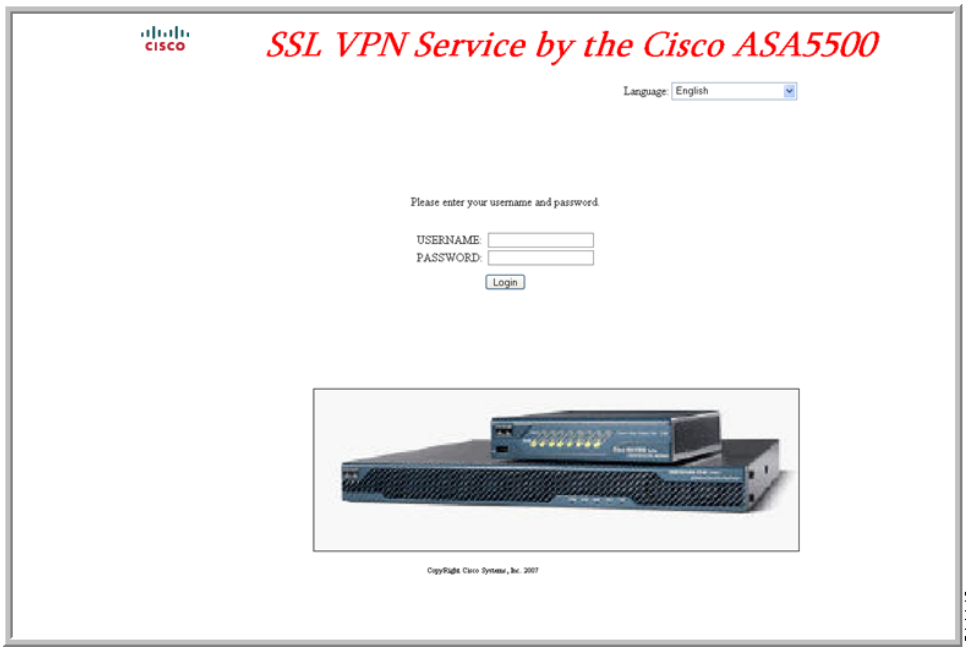


図 20-10 は、フル カスタマイゼーション機能によってイネーブル化される簡単なカスタム ログイン画面の例を示しています。

図 20-10　　ログイン画面のフル カスタマイゼーション例



次の HTML コードは例として使用され、表示するコードです。

例：

```
<head>
<meta http-equiv="Content-Type" content="text/html; charset=windows-1252">
<title>New Page 3</title>
<base target="_self">
</head>

<p align="center">
<img border="0" src="/+CSCOU+/cisco_logo.jpg" width="188" height="48"><font face="Snap
ITC" size="6" color="#FF00FF">
</font><font face="Snap ITC" color="#FF00FF" size="7"> </font><i><b><font
color="#FF0000" size="7" face="Sylfaen"> SSL VPN Service by the Cisco
ASA5500</font></b></i></p>

    <body onload="csco_ShowLoginForm('lform');csco_ShowLanguageSelector('selector')">

    <table>

    <tr><td colspan=3 height=20 align=right><div id="selector" style="width:
    300px"></div></td></tr>
    <tr><td></td><td></td><td></td></tr>
    <tr>
    <td height="379"></td>
    <td height="379"></td>
    <td align=middle valign=middle>
    <div id=lform >
    <p> </p>
    <p> </p>
    <p> </p>
    <p>Loading...</p>
    </div>
    </td>
    </tr>
    <tr>
    <td width="251"></td>
    <td width="1"></td>
    <td align=right valign=right width="800">
    <img border="1" src="/+CSCOU+/asa5500.jpg" width="660" height="220" align="middle">
    </td></tr>

    </table>
```

字下げされたコードは、画面に Login フォームと言語セレクタを挿入します。関数 **csco_ShowLoginForm('lform')** は Login フォームを挿入します。**csco_ShowLanguageSelector('selector')** は、言語セレクタを挿入します。

HTML ファイルの変更

手順の詳細

ステップ 1　ファイルに **login.inc** という名前を付けます。このファイルをインポートすると、ASA はこのファイル名をログイン画面として認識します。

ステップ 2　このファイルで使用されるイメージのパスに **/+CSCOU+/** を含めるように変更します。

認証前にリモート ユーザに表示されるファイルは、パス /+CSCOU+/ で表される ASA のキャッシュ メモリの特定のエリアに置く必要があります。そのため、このファイルにある各イメージのソースはこのパスに含める必要があります。次に例を示します。

```
src=”/+CSCOU+/asa5520.gif”
```

ステップ 3　下記の特別な HTML コードを挿入します。このコードには、Login フォームと言語セレクタを画面に挿入する前述のシスコの関数が含まれています。

```
<body onload="csco_ShowLoginForm('lform');csco_ShowLanguageSelector('selector')">

<table>

<tr><td colspan=3 height=20 align=right><div id="selector" style="width:
300px"></div></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr>
<td height="379"></td>
<td height="379"></td>
<td align=middle valign=middle>
<div id=lform >
<p> </p>
<p> </p>
<p> </p>
<p>Loading...</p>
</div>
</td>
</tr>
<tr>
<td width="251"></td>
<td width="1"></td>
<td align=right valign=right width="800">
<img border="1" src="/+CSCOU+/asa5500.jpg" width="660" height="220" align="middle">
</td></tr>

</table>
```

ブックマーク ヘルプのカスタマイズ

ASA は、選択した各ブックマークのアプリケーション パネルにヘルプの内容を表示します。これらのヘルプ ファイルをカスタマイズしたり、他の言語でヘルプ ファイルを作成したりできます。次に、後続のセッション中に表示するために、ファイルをフラッシュ メモリにインポートします。事前にインポートしたヘルプ コンテンツ ファイルを取得して、変更し、フラッシュ メモリに再インポートすることもできます。

各アプリケーションのパネルには、事前に設定されたファイル名を使用して独自のヘルプ ファイル コンテンツが表示されます。今後、各ファイルは、ASA のフラッシュ メモリ内の /+CSCOE+/help/*language*/ という URL に置かれます。表 20-1 に、VPN セッション用に保守できる各ヘルプ ファイルの詳細を示します。

表 20-1　VPN アプリケーションのヘルプ ファイル

アプリケーション タイプ	パネル	セキュリティ アプライアンスのフラッシュ メモリ内のヘルプ ファイルの URL	シスコが提供するヘルプ ファイルに英語版があるか
標準	Application Access	/+CSCOE+/help/*language*/app-access-hlp.inc	ある
標準	Browse Networks	/+CSCOE+/help/*language*/file-access-hlp.inc	ある
標準	AnyConnect Client	/+CSCOE+/help/*language*/net-access-hlp.inc	ある

表 20-1　VPN アプリケーションのヘルプ ファイル

アプリケーション タイプ	パネル	セキュリティ アプライアンスのフラッシュ メモリ内のヘルプ ファイルの URL	シスコが提供するヘルプ ファイルに英語版があるか
標準	Web Access	/+CSCOE+/help/*language*/web-access-hlp.inc	ある
プラグイン	MetaFrame Access	/+CSCOE+/help/*language*/ica-hlp.inc	ない
プラグイン	Terminal Servers	/+CSCOE+/help/*language*/rdp-hlp.inc	ある
プラグイン	Telnet/SSH Servers	/+CSCOE+/help/*language*/ssh,telnet-hlp.inc	ある
プラグイン	VNC Connections	/+CSCOE+/help/*language*/vnc-hlp.inc	ある

language は、ブラウザに表示される言語の省略形です。このフィールドは、ファイル変換には*使用されません*。ファイル内で使用される言語を示します。特定の言語コードを指定するには、ブラウザに表示される言語のリストからその言語の省略形をコピーします。たとえば、次の手順のいずれかを使用すると、ダイアログ ウィンドウに言語と関連の言語コードが表示されます。

- Internet Explorer を起動して、**[Tools] > [Internet Options] > [Languages] > [Add]** を選択します。
- Mozilla Firefox を起動して、**[Tools] > [Options] > [Advanced] > [General]** を選択し、[Languages] の隣にある **[Choose]** をクリックして、**[Select a language to add]** をクリックします。

ここでは、ヘルプ コンテンツのカスタマイズ方法について説明します。

- 「シスコが提供するヘルプ ファイルのカスタマイズ」（P.20-18）
- 「シスコが提供していない言語用のヘルプ ファイルの作成」（P.20-19）
- 「フラッシュ メモリへのヘルプ ファイルのインポート」（P.20-20）
- 「フラッシュ メモリからの事前にインポートしたヘルプ ファイルのエクスポート」（P.20-20）

シスコが提供するヘルプ ファイルのカスタマイズ

シスコが提供するヘルプ ファイルをカスタマイズするには、まずフラッシュ メモリ カードからファイルのコピーを取得する必要があります。次の手順で、コピーを取得してカスタマイズします。

手順の詳細

ステップ 1　ブラウザを使用して、ASA とのクライアントレス SSL VPN セッションを確立します。

ステップ 2　表 20-1 の「セキュリティ アプライアンスのフラッシュ メモリ内のヘルプ ファイルの URL」の中の文字列を、ASA のアドレスに追加し、Enter を押してヘルプ ファイルを表示します。

（注）　英語版のヘルプ ファイルを取得するには、*language* のところに *en* を入力します。

次のアドレス例は、Terminal Servers のヘルプの英語版を表示します。

https://*address_of_security_appliance***/+CSCOE+/help/en/rdp-hlp.inc**

ステップ 3　**[File] > [Save (Page) As]** を選択します。

（注）　[File name] ボックスの内容は変更しないでください。

ステップ 4　[Save as type] オプションを **[Web Page, HTML only]** に変更して、**[Save]** をクリックします。

ステップ 5　任意の HTML エディタを使用してファイルを変更します。

（注）　ほとんどの HTML タグは使用できますが、ドキュメントやその構造を定義するタグは使用 *できません*。たとえば、<html>、<title>、<body>、<head>、<h1>、<h2> などは使用しないでください。<b> タグなどの文字タグやコンテンツを構成する <p>、<ol>、<ul>、 などのタグは使用できます。

ステップ 6　元のファイル名と拡張子を指定して、HTML only としてファイルを保存します。

ステップ 7　ファイル名が表 20-1 にあるファイル名のいずれかと一致すること、および余分なファイル拡張子がないことを確認します。

シスコが提供していない言語用のヘルプ ファイルの作成

HTML を使用して、他の言語でヘルプ ファイルを作成します。

サポートするそれぞれの言語に別のフォルダを作成することをお勧めします。

HTML only としてファイルを保存します。表 20-1 の「セキュリティ アプライアンスのフラッシュ メモリ内のヘルプ ファイルの URL」の最後のスラッシュの後にあるファイル名を使用します。

VPN セッション中に表示するためにファイルをインポートする場合は、次の項を参照してください。

制限

ほとんどの HTML タグは使用できますが、ドキュメントやその構造を定義するタグは使用 *できません*。たとえば、<html>、<title>、<body>、<head>、<h1>、<h2> などは使用しないでください。<b> タグなどの文字タグやコンテンツを構成する <p>、<ol>、<ul>、 などのタグは使用できます。

フラッシュ メモリへのヘルプ ファイルのインポート

手順の詳細

	コマンド	目的
ステップ 1	**import webvpn webcontent** *destination_url source_url*	クライアントレス SSL VPN セッションで表示するために、フラッシュ メモリにヘルプ コンテンツ ファイルをインポートします。 • destination_url は、表 20-1VPN アプリケーションのヘルプ ファイルの「セキュリティ アプライアンスのフラッシュ メモリ内のヘルプ ファイルの URL」列の文字列です。 • *source_url* は、インポートするファイルの URL です。有効なプレフィックスは、ftp://、http://、および tftp:// です。
	例： hostname# **import webvpn webcontent /+CSCOE+/help/en/app-access-hlp.inc tftp://209.165.200.225/app-access-hlp.inc**	TFTP サーバ（209.165.200.225）からヘルプ ファイル *app-access-hlp.inc* をフラッシュ メモリにコピーします。この URL には英語の省略形である *en* が含まれています。

フラッシュ メモリからの事前にインポートしたヘルプ ファイルのエクスポート

手順の詳細

	コマンド	目的
ステップ 1	**export webvpn webcontent** *source_url destination_url*	後で編集するために事前にインポートしたヘルプ コンテンツ ファイルを取得します。 • *source_url* は、表 20-1 の「セキュリティ アプライアンスのフラッシュ メモリ内のヘルプ ファイルの URL」の文字列です。 • *destination_url* は、**ターゲット URL** です。有効なプレフィックスは、ftp:// と tftp:// です。最大文字数は 255 です。
	例： hostname# **export webvpn webcontent /+CSCOE+/help/en/file-access-hlp.inc tftp://209.165.200.225/file-access-hlp.inc**	[Browser Networks] パネルに表示される英語のヘルプ ファイル *file-access-hlp.inc* を TFTP サーバ（209.165.200.225）にコピーします。

ユーザ メッセージの言語の変換

ASA は、クライアントレス SSL VPN セッション全体の言語変換を提供します。これには、ログイン、ログアウト バナー、およびプラグインおよび AnyConnect などの認証後に表示されるポータル ページが含まれます。

この項では、これらのユーザ メッセージを変換するために ASA を設定する方法について説明します。

言語変換の概要

リモート ユーザに可視である機能エリアとそれらのメッセージは、変換ドメイン内にまとめられています。表 20-2 に、変換ドメインと変換される機能エリアを示します。

表 20-2　言語翻訳ドメインのオプション

変換ドメイン	変換される機能エリア
AnyConnect	Cisco AnyConnect VPN クライアントのユーザ インターフェイスに表示されるメッセージ。
banners	クライアントレス接続で VPN アクセスが拒否される場合に表示されるメッセージ。
CSD	Cisco Secure Desktop（CSD）のメッセージ。
customization	ログイン ページ、ログアウト ページ、ポータル ページのメッセージ、およびユーザによるカスタマイズが可能なすべてのメッセージ。
plugin-ica	Citrix プラグインのメッセージ。
plugin-rdp	Remote Desktop Protocol プラグインのメッセージ。
plugin-rdp2	Java Remote Desktop Protocol プラグインのメッセージ。
plugin-telnet,ssh	Telnet および SSH プラグインのメッセージ。
plugin-vnc	VNC プラグインのメッセージ。
PortForwarder	ポート転送ユーザに表示されるメッセージ。
url-list	ユーザがポータル ページの URL ブックマークに指定するテキスト。
webvpn	カスタマイズできないすべてのレイヤ 7 メッセージ、AAA メッセージ、およびポータル メッセージ。

ASA には、標準機能の一部である各ドメイン用の変換テーブル テンプレートが含まれています。プラグインのテンプレートはプラグインとともに含まれており、独自の変換ドメインを定義します。

変換ドメインのテンプレートをエクスポートできます。これで、入力する URL にテンプレートの XML ファイルが作成されます。このファイルのメッセージ フィールドは空です。メッセージを編集して、テンプレートをインポートし、フラッシュ メモリに置かれる新しい変換テーブル オブジェクトを作成できます。

既存の変換テーブルをエクスポートすることもできます。作成した XML ファイルに事前に編集したメッセージが表示されます。この XML ファイルを同じ言語名で再インポートすると、新しいバージョンの変換テーブルが作成され、以前のメッセージが上書きされます。

テンプレートにはスタティックのものも、ASA の設定に基づいて変化するものもあります。*クライアントレス ユーザのログインおよびログアウト ページ*、*ポータル ページ*、*および URL ブックマーク*はカスタマイズが可能なため、**ASA は customization** および **url-list** 変換ドメイン テンプレートをダイナミックに生成し、テンプレートは変更内容をこれらの機能エリアに自動的に反映させます。

変換テーブルを作成した後、このテーブルを使用して、カスタマイゼーション オブジェクトを作成し、グループ ポリシーまたはユーザ属性に適用できます。AnyConnect 変換ドメイン以外では、カスタマイゼーション オブジェクトを作成し、そのオブジェクトで使用する変換テーブルを識別し、グループ ポリシーまたはユーザに対してそのカスタマイゼーションを指定するまで、変換テーブルは影響を及ぼすことはなく、ユーザ画面のメッセージは変換されません。AnyConnect ドメインの変換テーブルに対する変更は、ただちに AnyConnect クライアント ユーザに表示されます。

変換テーブルの作成

シングル コンテキスト モードおよびマルチ コンテキスト モードの両方で変換テーブルを作成できます。

手順の詳細

	コマンド	目的
ステップ 1	**export webvpn translation-table** **例：** hostname# **show import webvpn translation-table** Translation Tables' Templates: customization AnyConnect CSD PortForwarder url-list webvpn Citrix-plugin RPC-plugin Telnet-SSH-plugin VNC-plugin Translation Tables: **例：** hostname# **export webvpn translation-table customization template tftp://209.165.200.225/portal**	コンピュータに変換テーブル テンプレートをエクスポートします。 使用可能な変換テーブル テンプレートとテーブルを示します。 customization ドメインの変換テーブル テンプレートをエクスポートします。これは、クライアントレス SSL VPN セッションのユーザに表示されるメッセージに影響を及ぼします。作成される XML ファイルのファイル名は *portal*（ユーザ指定）で、次の空のメッセージ フィールドが含まれています。

	コマンド	目的
ステップ 2	変換テーブルの XML ファイルを編集します。 **例：** `# Copyright (C) 2006 by Cisco Systems, Inc.` `#` `#, fuzzy` `msgid ""` `msgstr ""` `"Project-Id-Version: ASA\n"` `"Report-Msgid-Bugs-To: vkamyshe@cisco.com\n"` `"POT-Creation-Date: 2007-03-12 18:57 GMT\n"` `"PO-Revision-Date: YEAR-MO-DA HO:MI+ZONE\n"` `"Last-Translator: FULL NAME <EMAIL@ADDRESS>\n"` `"Language-Team: LANGUAGE <LL@li.org>\n"` `"MIME-Version: 1.0\n"` `"Content-Type: text/plain; charset=UTF-8\n"` `"Content-Transfer-Encoding: 8bit\n"` `#: DfltCustomization:24 DfltCustomization:64` `msgid "Clientless SSL VPN Service"` `msgstr ""`	*portal* としてエクスポートされたテンプレートの一部を示します。この出力の最後には、メッセージのメッセージ ID フィールド（msgid）とメッセージ文字列フィールド（msgstr）が含まれています。このメッセージは、ユーザがクライアントレス SSL VPN セッションを確立するときにポータル ページに表示されます。完全なテンプレートには、多くのメッセージ フィールドのペアが含まれています。
ステップ 3	**import webvpn translation-table** **例：** `hostname# import webvpn translation-table customization language es-us tftp://209.165.200.225/portal` `hostname# !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!` `hostname# show import webvpn translation-table` `Translation Tables' Templates:` `AnyConnect` `PortForwarder` `csd` `customization` `keepout` `url-list` `webvpn` `Citrix-plugin` `RPC-plugin` `Telnet-SSH-plugin` `VNC-plugin` `Translation Tables:` `es-us customization`	変換テーブルをインポートします。 XML ファイルをインポートします。*es-us* は米国スペイン語の省略形です。

AnyConnect ドメインの変換テーブルをインポートする場合、変更内容はすぐに有効になります。その他のドメインの変換テーブルをインポートする場合は、カスタマイゼーション オブジェクトを作成し、そのオブジェクトで使用する変換テーブルを指定して、グループ ポリシーまたはユーザに対してカスタマイゼーション オブジェクトを指定する必要があります。

カスタマイゼーション オブジェクトでの言語の参照

ここでは、カスタマイゼーション テンプレートを参照できるように、エクスポートし、編集して、カスタマイゼーション オブジェクトとしてインポートする方法について説明します。

前提条件

カスタマイゼーション オブジェクトでこれらの変換テーブルを正しく呼び出すには、テーブルが同じ名前ですでにインポートされている必要があります。これらの名前は、ブラウザの言語オプションと互換性がある必要があります。

手順の詳細

	コマンド	機能
ステップ 1	**export webvpn customization template** **例：** hostname# **export webvpn customization template tftp://209.165.200.225/sales**	編集作業ができる URL にカスタマイゼーション テンプレートをエクスポートします。 テンプレートをエクスポートし、指定した URL に *sales* のコピーを作成します。
ステップ 2	カスタマイゼーション テンプレートを編集し、以前インポートした変換テーブルを参照します。 **例：** <localization> 　<languages>en,ja,zh,ru,ua</languages> 　<default-language>en</default-language> </localization> **例：** <auth-page> 　.... 　<language-selector> 　<mode>enable</mode> 　<title l10n="yes">Language:</title> 　<language> 　<code>en</code> 　<text>English</text> 　</language> 　<language> 　<code>es-us</code> 　<text>Spanish</text> 　</language> </language-selector>	カスタマイゼーション テンプレートの XML コードの 2 つのエリアが変換テーブルに関係します。 使用する変換テーブルを指定します。 • XML コードの <languages> タグの後に、変換テーブルの名前を続けます。この例では、en、ja、zh、ru、および ua です。 • <default-language> タグは、リモート ユーザが ASA に接続したときに最初に表示する言語を指定します。上のコード例では、言語は英語です。 言語セレクタの表示に影響を与え、<language selector> タグとそれに関連付けられた <language> タグによって、言語セレクタをイネーブルにし、カスタマイズします。 • タグ グループ <language-selector> には、言語セレクタの表示をイネーブルおよびディセーブルにする <mode> タグと、言語を一覧表示するドロップダウン ボックスのタイトルを指定する <title> タグが含まれています。 • タグ グループ <language> には、<code> タグと <text> タグが含まれており、言語セレクタ ドロップダウン ボックスに表示される言語名と特定の変換テーブルをマッピングします。
ステップ 3	変更を行った後ファイルを保存します。	

	コマンド	機能
ステップ 4	**import webvpn customization** **例：** hostname# **import webvpn customization sales tftp://209.165.200.225/sales** hostname# **!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!**	新しいオブジェクトとしてカスタマイゼーション テンプレートをインポートします。
ステップ 5	**show import webvpn customization** **例：** hostname# **import webvpn customization sales tftp://209.165.200.225/sales** hostname# **!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!**	新しいカスタマイゼーション オブジェクト *sales* を表示します。

カスタマイゼーション オブジェクトを使用するためのグループ ポリシーまたはユーザ属性の変更

ここでは、特定のグループまたはユーザに対して変更をアクティブにする方法について説明します。

手順の詳細

	コマンド	目的
ステップ 1	**webvpn**	クライアントレス SSL VPN コンフィギュレーション モードに切り替えます。
ステップ 2	**group-policy webvpn**	グループ ポリシーのクライアントレス SSL VPN コンフィギュレーション モードに切り替えます。
ステップ 3	**customization** **例：** hostname(config)# **group-policy sales attributes** hostname(config-group-policy)# **webvpn** hostname(config-group-webvpn)# **customization value sales**	カスタマイゼーション オブジェクトをイネーブルにします。 グループ ポリシー *sales* でカスタマイゼーション オブジェクト *sales* がイネーブルになっていることを示します。

CHAPTER 21

クライアントレス SSL VPN のトラブルシューティング

2014 年 4 月 14 日

hosts ファイル エラーを回避するための Application Access の終了

Application Access の実行の妨げになる hosts ファイル エラーを回避するために、Application Access を使用し終えたら、Application Access ウィンドウを必ず閉じるようにします。ウィンドウを閉じるには、[Close] アイコンをクリックします。

Application Access 使用時の hosts ファイル エラーからの回復

Application Access ウィンドウを正しく閉じないと、次のエラーが発生する可能性があります。

- 次に Application Access を起動しようとしたときに、Application Access がオフに切り替わっている可能性があり、「`Backup HOSTS File Found`」エラー メッセージが表示される。
- アプリケーションをローカルで実行している場合でも、アプリケーション自体がオフに切り替わっているか、または動作しない。

このようなエラーは、Application Access ウィンドウを不適切な方法で終了したことが原因です。次に例を示します。

- Application Access の使用中に、ブラウザがクラッシュした。
- Application Access の使用中に、停電またはシステム シャットダウンが発生した。
- 作業中に Application Access ウィンドウを最小化し、このウィンドウがアクティブな状態（ただし最小化されている）でコンピュータをシャットダウンした。

hosts ファイルの概要

ローカル システム上の hosts ファイルは、IP アドレスをホスト名にマッピングしています。Application Access を起動すると、クライアントレス SSL VPN は hosts ファイルを修正し、クライアントレス SSL VPN 固有のエントリを追加します。Application Access ウィンドウを正しく閉じて Application Access を終了すると、hosts ファイルは元の状態に戻ります。

Application Access の起動前	hosts ファイルは元の状態です。
Application Access の起動時	• クライアントレス SSL VPN は hosts ファイルを hosts.webvpn にコピーして、バックアップを作成します。 • 次に、クライアントレス SSL VPN は hosts ファイルを編集し、クライアントレス SSL VPN 固有の情報を挿入します。
Application Access の終了時	• クライアントレス SSL VPN はバックアップ ファイルを `hosts` ファイルにコピーして、hosts ファイルを元の状態に戻します。 • クライアントレス SSL VPN は、hosts.webvpn を削除します。
Application Access の終了後	hosts ファイルは元の状態です。

（注）　Microsoft 社のアンチスパイウェア ソフトウェアは、ポート転送 Java アプレットによる hosts ファイルの変更をブロックします。アンチスパイウェア ソフトウェアの使用時に hosts ファイルの変更を許可する方法の詳細については、www.microsoft.com を参照してください。

不正な Application Access の終了

Application Access が正しく終了しなかった場合は、`hosts` ファイルは、クライアントレス SSL VPN 用にカスタマイズされた状態のままになっています。ユーザが次に Application Access を起動するときに、クライアントレス SSL VPN は hosts.webvpn ファイルを検索することで、Application Access の状態をチェックします。hosts.webvpn ファイルが検出されると、「`Backup HOSTS File Found`」というエラー メッセージが表示され、Application Access が一時的にオフに切り替わります。

Application Access を正しくシャットダウンしないと、リモート アクセス クライアント/サーバ アプリケーションが不安定な状態のままになります。クライアントレス SSL VPN を使用せずにこれらのアプリケーションを起動しようとすると、正しく動作しない場合があります。通常の接続先のホストが使用できなくなる場合があります。一般にこのような状況は、自宅からリモートでアプリケーションを実行し、Application Access ウィンドウを終了せずにコンピュータをシャットダウンし、その後職場でそのアプリケーションを実行しようとした場合に発生します。

クライアントレス SSL VPN による hosts ファイルの自動再設定

リモート アクセス サーバに接続できる場合は、hosts ファイルを再設定し、Application Access やアプリケーションを再度イネーブルにするために、次の手順を実行します。

手順の詳細

ステップ 1　クライアントレス SSL VPN を起動してログインします。ホームページが開きます。

ステップ 2　**[Applications Access]** リンクをクリックします。`Backup HOSTS File Found` メッセージが表示されます。

ステップ 3　次のいずれかのオプションを選択します。

- **[Restore from backup]**：クライアントレス SSL VPN は強制的に正しくシャットダウンされます。クライアントレス SSL VPN は hosts.webvpn backup ファイルを `hosts` ファイルにコピーし、hosts ファイルを元の状態に戻してから、hosts.webvpn を削除します。その後、Application Access を再起動する必要があります。
- **[Do nothing]**：Application Access は起動しません。リモート アクセスのホームページが再び表示されます。
- **[Delete backup]**：クライアントレス SSL VPN は hosts.webvpn ファイルを削除し、hosts ファイルをクライアントレス SSL VPN 用にカスタマイズされた状態にしておきます。元の `hosts` ファイル設定は失われます。Application Access は、クライアントレス SSL VPN 用にカスタマイズされた hosts ファイルを新しいオリジナルとして使用して起動します。このオプションは、hosts ファイル設定が失われても問題がない場合にだけ選択してください。Application Access が不適切にシャットダウンされた後に、ユーザまたはユーザが使用するプログラムによって hosts ファイルが編集された可能性がある場合は、他の 2 つのオプションのどちらかを選択するか、または hosts ファイルを手動で編集します （「手動による hosts ファイルの再設定」を参照）。

手動による hosts ファイルの再設定

現在の場所からリモート アクセス サーバに接続できない場合や、カスタマイズした hosts ファイルの編集内容を失いたくない場合は、次の手順に従って、hosts ファイルを再設定し、Application Access とアプリケーションを再度イネーブルにします。

手順の詳細

ステップ 1　hosts ファイルを見つけて編集します。最も一般的な場所は、c:\windows\system32\drivers\etc\hosts です。

ステップ 2　`# added by WebVpnPortForward` という文字列が含まれている行があるかどうかをチェックします。この文字列を含む行がある場合、hosts ファイルはクライアントレス SSL VPN 用にカスタマイズされています。hosts ファイルがクライアントレス SSL VPN 用にカスタマイズされている場合、次の例のようになっています。

```
server1 # added by WebVpnPortForward
server1.example.com invalid.cisco.com # added by WebVpnPortForward
server2 # added by WebVpnPortForward
server2.example.com invalid.cisco.com # added by WebVpnPortForward
server3 # added by WebVpnPortForward
server3.example.com invalid.cisco.com # added by WebVpnPortForward
```

```
# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to hostnames. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding hostname.
# The IP address and the hostname should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     cisco.example.com          # source server
#       38.25.63.10     x.example.com              # x client host

123.0.0.1       localhost
```

ステップ 3　`# added by WebVpnPortForward` という文字列が含まれている行を削除します。

ステップ 4　ファイルを保存して、閉じます。

ステップ 5　クライアントレス SSL VPN を起動してログインします。

ホームページが表示されます。

ステップ 6　**[Application Access]** リンクをクリックします。

[Application Access] ウィンドウが表示されます。これで Application Access がイネーブルになります。

データのキャプチャ

CLI **capture** コマンドを使用すると、クライアントレス SSL VPN セッションでは正しく表示されない Web サイトに関する情報を記録できます。このデータは、シスコ カスタマー サポート エンジニアによる問題のトラブルシューティングに役立ちます。次の項では、クライアントレス SSL VPN セッション データのキャプチャおよび表示方法について説明します。

- 「キャプチャ ファイルの作成」（P.21-5）
- 「キャプチャ データを表示するためのブラウザの使用」（P.21-6）

前提条件

- クライアントレス SSL VPN キャプチャをイネーブルにすると、セキュリティ アプライアンスのパフォーマンスに影響します。トラブルシューティングに必要なキャプチャ ファイルを生成したら、キャプチャを必ずオフに切り替えます。

キャプチャ ファイルの作成

手順の詳細

	コマンド	目的
ステップ 1	**capture *capture_name* type webvpn user *webvpn_username*** **例：** hostname# **capture hr type webvpn user user2** WebVPN capture started. capture name hr user name user2 hostname# **no capture hr**	クライアントレス SSL VPN のキャプチャ ユーティリティを開始します。 • *capture_name* は、キャプチャに割り当てる名前です。これは、キャプチャ ファイルの名前の先頭にも付加されます。 • *webvpn_user* は、キャプチャの対象となるユーザ名です。 hr という名前のキャプチャを作成します。これは、user2 へのトラフィックをファイルにキャプチャします。
ステップ 2	（オプション） **no capture capture_name**	ユーザがログインし、クライアントレス SSL VPN セッションを開始した後に、キャプチャ ユーティリティでのパケットの取得を停止します。キャプチャ ユーティリティは *capture_name*.zip ファイルを作成し、このファイルはパスワード **koleso** で暗号化されます。
ステップ 3	.zip ファイルをシスコに送信するか、Cisco TAC サービス リクエストに添付します。	
ステップ 4	パスワード *koleso* を使用してファイルの内容を解凍します。	

キャプチャ データを表示するためのブラウザの使用

手順の詳細

	コマンド	目的
ステップ 1	**capture** ***capture_name*** **type webvpn user** ***webvpn_username***	クライアントレス SSL VPN のキャプチャ ユーティリティを開始します。 • *capture_name* は、キャプチャに割り当てる名前です。これは、キャプチャ ファイルの名前の先頭にも付加されます。 • *webvpn_user* は、キャプチャの対象となるユーザ名です。
ステップ 2	（オプション） **no capture capture_name**	ユーザがログインし、クライアントレス SSL VPN セッションを開始した後に、キャプチャ ユーティリティでのパケットの取得を停止します。
ステップ 3	ブラウザを開き、次のように入力します。 **https://***asdm_enabled_interface_of_the_security_appliance***:***port***/admin/capture/***capture_name***/pcap **例**： **https://192.0.2.1:60000/admin/capture/hr/pcap**	hr という名前のキャプチャを sniffer 形式で表示します。
ステップ 4	ステップ 2 を繰り返します。	

CHAPTER 22

クライアントレス SSL VPN ライセンス

2013 年 9 月 13 日

ライセンス

（注） この機能は、ペイロード暗号化機能のないモデルでは使用できません。

モデル	ライセンス要件
ASA 5512-X	AnyConnect Premium ライセンス： • 基本ライセンス：2 セッション。 • *オプションの永続または時間ベースのライセンス：10、25、50、100、または 250 セッション。* • *オプションの共有ライセンス：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。*
ASA 5515-X	AnyConnect Premium ライセンス： • 基本ライセンス：2 セッション。 • *オプションの永続または時間ベースのライセンス：10、25、50、100、または 250 セッション。* • *オプションの共有ライセンス：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。*
ASA 5525-X	AnyConnect Premium ライセンス： • 基本ライセンス：2 セッション。 • *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、または 750 セッション。* • *オプションの共有ライセンス：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。*

モデル	ライセンス要件
ASA 5545-X	AnyConnect Premium ライセンス： • 基本ライセンス：2 セッション。 • *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、750、1000、または 2500 セッション。* • *オプションの共有ライセンス：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。*
ASA 5555-X	AnyConnect Premium ライセンス： • 基本ライセンス：2 セッション。 • *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、750、1000、2500、または 5000 セッション。* • *オプションの共有ライセンス：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。*
ASA 5585-X（SSP-10）	AnyConnect Premium ライセンス： • 基本ライセンス：2 セッション。 • *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、750、1000、2500、または 5000 セッション。* • *オプションの共有ライセンス：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。*
ASA 5585-X（SSP-20、-40、および -60）	AnyConnect Premium ライセンス： • 基本ライセンス：2 セッション。 • *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、750、1000、2500、5000、または 10000 セッション。* • *オプションの共有ライセンス：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。*
ASASM	AnyConnect Premium ライセンス： • 基本ライセンス：2 セッション。 • *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、750、1000、2500、5000、または 10000 セッション。* • *オプションの共有ライセンス：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。*
ASAv（仮想 CPU X 1 を搭載）	• 標準ライセンス：2 セッション。 • Premium ライセンス：250 セッション。
ASAv（仮想 CPU X 4 を搭載）	• 標準ライセンス：2 セッション。 • Premium ライセンス：750 セッション。

（注）　クライアントレス SSL VPN セッションを開始した後、ポータルから AnyConnect クライアント セッションを開始した場合は、合計 1 つのセッションが使用されています。これに対して、最初に AnyConnect クライアントを（スタンドアロン クライアントなどから）開始した後、クライアントレス SSL VPN ポータルにログインした場合は、2 つのセッションが使用されています。

すべてのタイプの組み合わせ VPN セッションの最大数は、この表に示す最大セッション数を超えることはできません。

共有ライセンスによって、ASA は複数のクライアントの ASA の共有ライセンス サーバとして機能します。共有ライセンス プールは大規模ですが、個々の ASA によって使用されるセッションの最大数は、永続的なライセンスで指定される最大数を超えることはできません。