CLI ブック 3：Cisco ASA シリーズ 9.9 VPN CLI コンフィギュレーション ガイド

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

目 次

このマニュアルについて

ここでは、このガイドを使用する方法について説明します。

本書の目的

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 Adaptive Security Device Manager（ASDM）を使用して、ASA を設定および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全般に該当します。

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、文字、表示、および警告に関する次の規則に準拠しています。

文字表記法

表記法	説明
boldface	コマンド、キーワード、ボタン ラベル、フィールド名、およびユーザ入力テキストは、**boldface**で示しています。メニューベース コマンドの場合は、メニュー項目を [ ] で囲み、コマンドのフル パスを示しています。
italic	ユーザが値を指定する変数は、イタリック体で示しています。 イタリック体は、マニュアル タイトルと一般的な強調にも使用されています。
等幅	システムが表示するターミナル セッションおよび情報は、等幅文字で記載されます。
{x | y | z}	どれか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。
[ ]	角カッコの中の要素は、省略可能です。
[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。
[ ]	システム プロンプトに対するデフォルトの応答も、角カッコで囲んで記載されます。
< >	パスワードなどの出力されない文字は、山カッコ（< >）で囲んで示しています。
!、#	コードの先頭に感嘆符（!）または番号記号（#）がある場合は、コメント行であることを示します。

読者への警告

このマニュアルでは、読者への警告に以下を使用しています。

（注） 「注釈」です。役立つ情報やこのマニュアルに記載されていない参照資料を紹介しています。

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。

ワンポイント アドバイス	時間を節約する方法です。ここに紹介している方法で作業を行うと、時間を短縮できます。
警告	**「警告」の意味です。人身事故を予防するための注意事項が記述されています。**

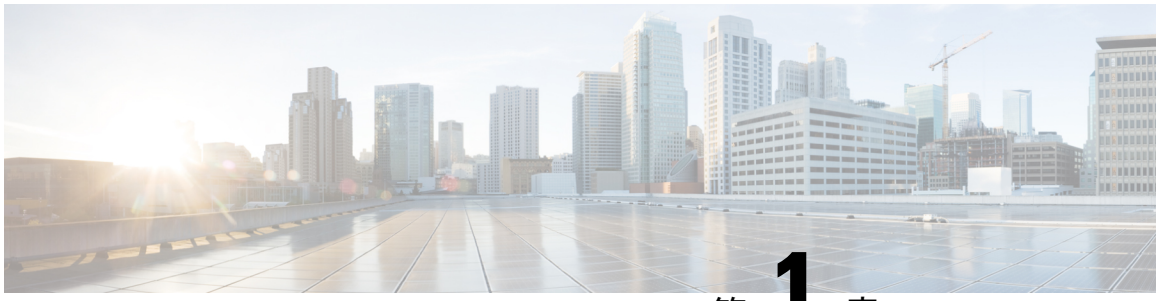
マニュアルの入手方法およびテクニカル サポート

ドキュメントの入手、Cisco Bug Search Tool（BST）の使用、サービス要求の送信、追加情報の収集の詳細については、『What's New in Cisco Product Documentation』を参照してください。

新しく作成された、または改訂されたシスコのテクニカル コンテンツをお手元で直接受け取るには、『』をご購読ください。RSS フィードは無料のサービスです。

第 部

サイト間 VPN およびクライアント VPN



第 1 章

IPsec および ISAKMP

トンネリング、IPsec、および ISAKMP について

このトピックでは、バーチャルプライベートネットワーク（VPN）の構築に使用するインターネットプロトコルセキュリティ（IPsec）標準と Internet Security Association and Key Management Protocol（ISAKMP）標準について説明します。

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、LAN-to-LAN VPN 接続に IPsec が使用され、client-to-LAN VPN 接続に IPsec を使用することもできます。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することができます。IPsec client-to-LAN 接続では、ASA は応答側としてのみ機能します。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。

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

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デフィーヘルマン グループ。ASA はこのアルゴリズムを使用して、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。
- ASA が暗号キーを使用する時間の制限。この時間が経過すると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。

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 によって暗号マップに対する 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 （50 ページ） 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暗号マップを自動的に削除します。

IPsec VPN のライセンス

（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。

IKEv2 を使用した IPsec リモート アクセス VPN には、別途購入可能な AnyConnect Plus または Apex ライセンスが必要です。AnyConnect ライセンスを購入する場合は、次の最大値を参照してください。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 サイト間 VPN では、基本ライセンスに付属の Other VPN ライセンスが使用されます。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越えることはできません。

モデル	ライセンス要件

ASA 5506-X、5506H-X、5506W-X	• IKEv2 を使用した IPsec リモート アクセス VPN：50 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：50 セッション。

ASA 5508-X	100 セッションです。
ASA 5512-X	250 セッションです。
ASA 5515-X	250 セッションです。
ASA 5516-X	300 セッションです。
ASA 5525-X	750 セッションです。

モデル	ライセンス要件
ASA 5545-X	2500 セッションです。
ASA 5555-X	5000 セッションです。
ASA 5585-X（SSP-10）	5000 セッションです。
ASA 5585-X（SSP-20、-40、および -60）	10,000 セッションです。
ASASM	10,000 セッションです。
ASAv5	250 セッションです。
ASAv10	250 セッションです。
ASAv30	750 セッションです。

IPsec VPN のガイドライン

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。Anyconnect Apex ライセンスは、マルチコンテキストモードのリモートアクセス VPN に必要です。ASA は AnyConnect Apex ライセンスを特異的に認識しませんが、プラットフォーム制限へのライセンス済み AnyConnect Premium、携帯電話用 AnyConnect、Cisco VPN フォン用 AnyConnect、および Advanced Endpoint Assessment など、Apex ライセンスのライセンス特性を適用します。

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。

ISAKMP の設定

IKEv1 ポリシーと IKEv2 ポリシーの設定

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。

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。

手順

ステップ 1 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。

例：

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

（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。

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。

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

例：

```
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。

hash [md5 | sha]

例：

```
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。

authentication[pre-shared]rsa-sig]

例：

```
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。

group[1 | 2 | 5]

例：

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

ステップ 6 SA ライフタイムを指定します。デフォルトは 86400 秒（24 時間）です。

lifetime *seconds*

例：

この例では、4 時間（14400 秒）のライフタイムを設定します。

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

ステップ 7 IKEv1 ポリシー キーワード、IKEv2 ポリシー キーワード、および IKE ポリシー キーワードと値 （8 ページ） で入力した値を使用して追加設定を指定します。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。

IKE ポリシー キーワードと値

	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。
	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て拡張が困難ですが、小規模ネットワークではセットアップが容易です。
encryption	**des** **3des**（デフォルト）	56 ビット DES-CBC 168 ビット Triple DES	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。
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。

	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。

	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 3des（デフォルト）	56 ビット DES-CBC 168 ビット Triple DES	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。

	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。

	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。 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。
	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）	
	14 19 20 21 24		
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。

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 を有効にするには、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）。Agressive 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。

（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。

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。

```
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、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)#  no crypto ikev1 am-disable
```

IKEv1 および IKEv2 ISAKMP ピアの識別方式の決定

IKEv1 または IKEv2 ISAKMP フェーズ I ネゴシエーションでは、ピアが相互に相手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。

Address	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。

Automatic （デフォルト）	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
Hostname	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。
Key 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。

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
```

INVALID_SELECTORS 通知

IPsec システムが SA 上で着信パケットを受信し、そのパケットのヘッダー フィールドが SA 用のセレクタに適合しなかった場合は、そのパケットを廃棄する必要があります。このイベントの監査ログ エントリには、現在の日時、SPI、IPsec プロトコル、パケットの送信元と宛先、その他の入手可能なパケットのベクトル値、および関連 SA エントリのセレクタ値が含まれます。システムは、セレクタ チェックに合格しなかったために受信パケットが破棄されたことを示す INVALID_SELECTORS の IKE 通知を生成して、送信元（IPsec ピア）に送信します。

ASA は、次に示す既存の syslog を使用して、CTM 内にこのイベントのロギングを実装しています。

```
%ASA-4-751027: IKEv2 Received INVALID_SELECTORS Notification from peer: <peer IP>. Peer
received a packet (SPI=<spi>) from <local_IP>. The decapsulated inner packet didn't match
 the negotiated policy in the SA. Packet destination <pkt_daddr>, port <pkt_dest_port>,
source <pkt_saddr>, port <pkt_src_port>, protocol <pkt_prot>
```

管理者は、SA 用のトラフィック セレクタと一致しない着信パケットが SA 上で受信された場合に、ピアへの IKEv2 通知の送信を有効または無効にできるようになりました。有効にした場

合は、IKEv2 通知メッセージが 5 秒ごとに SA あたり 1 つの通知メッセージに制限されます。IKEv2 通知は、IKEv2 情報交換でピアに送信されます。

16 進数の IKEv2 事前共有キーの設定

ローカルとリモートの両方の事前共有キー コマンドにキーワードの *hex* を追加することによって、16 進数の IKEv2 事前共有キーを設定することができます。

```
ikev2 local-authentication pre-shared-key [ 0 | 8 | hex ] <string>
ikev2 remote-authentication pre-shared-key [ 0 | 8 | hex ] <string>
```

IKE 通知の送信の有効化または無効化

管理者は、IKEv2 IPsec VPN 接続上でその接続用のトラフィック セレクタと一致しない着信パケットが受信された場合に、ピアへの IKE 通知の送信を有効または無効にすることができます。この通知の送信はデフォルトで無効になっています。ASDM 証明書でユーザ名を認可する場合の IKE INVALID_SELECTORS 通知の送信は、次の CLI を使用して有効または無効にします。

[**no**] **crypto ikev2 notify invalid-selectors**

証明書認証の実行時は、証明書内の CN がユーザ名であり、認可がローカル サーバに対して実行されます。"service-type" 属性が取得された場合は、前述のように処理されます。

IKEv2 フラグメンテーション オプションの設定

ASA では、IKEv2 フラグメンテーションをイネーブルまたはディセーブルにすることができ、IKEv2 パケットのフラグメント化で使用する MTU（最大伝送ユニット）を指定できます。また、管理者は次のコマンドを使用して、優先するフラグメンテーション方式を設定できます。

[**no**] **crypto ikev2 fragmentation** [**mtu** <*mtu-size*>] | [**preferred-method** [**ietf** | **cisco**]]

デフォルトでは、すべての IKEv2 フラグメンテーション方式がイネーブルになり、MTU は 576（IPv4 の場合）または 1280（IPv6 の場合）、優先される方式は IETF 標準 RFC-7383 となります。

次の点を考慮して、[**mtu** <*mtu-size*>] を指定してください。

- 使用する MTU 値には、IP（IPv4/IPv6）ヘッダー＋UDP ヘッダーのサイズを含める必要があります。
- 管理者によって指定されていない場合、デフォルトの MTU は 576（IPv4 の場合）または 1280（IPv6 の場合）となります。
- 指定すると、同じ MTU が IPv4 と IPv6 の両方で使用されます。
- 有効範囲は 68 ～ 1500 です。

次のサポートされているフラグメンテーション方式のいずれかを、IKEv2 の優先フラグメンテーション方式 [**preferred-method** [**ietf** | **cisco**]] として設定できます。

- IETF RFC-7383 標準ベースの IKEv2 フラグメンテーション。
  - この方式は、両方のピアがネゴシエーション中にサポートとプリファレンスを指定する場合に使用されます。
  - この方式を使用すると、フラグメンテーションの後に暗号化が実行され、各 IKEv2 フラグメント メッセージが個別に保護されます。
- シスコ独自のフラグメンテーション。
  - この方式は、これが AnyConnect クライアントなどのピアによって提供される唯一の方法である場合、または両方のピアがネゴシエーション中にサポートとプリファレンスを指定する場合に使用されます。
  - この方式を使用すると、暗号化の後にフラグメンテーションが実行されます。受信側のピアは、すべてのフラグメントを受信するまで、メッセージを復号することも認証することもできません。
  - この方式は、シスコ以外のピアとの相互運用性はありません。

show running-config crypto ikev2 コマンドは現在の設定を表示し、**show crypto ikev2 sa detail** コマンドは、SA に対してフラグメンテーションが使用された場合に符号化された MTU を表示します。

始める前に

- パス MTU ディスカバリはサポートされていません。MTU は、ネットワークのニーズに合わせて手動で設定する必要があります。
- この設定はグローバルであり、設定の適用後に確立される SA に影響を及ぼします。適用以前の SA は影響を受けません。フラグメンテーションがディセーブルになっている場合でも同様です。
- 最大 100 のフラグメントを受信できます。

例

- IKEv2 フラグメンテーションをディセーブルにする場合：

```
no crypto ikev2 fragmentation
```

- デフォルト動作に戻す場合：

```
crypto ikev2 fragmentation
```

または

```
crypto ikev2 fragmentation mtu 576
preferred-method ietf
```

- MTU の値を 600 に変更する場合：

```
crypto ikev2 fragmentation mtu 600
```

- デフォルトの MTU 値に戻す場合：

```
no crypto ikev2 fragmentation mtu 576
```

- 優先するフラグメンテーション方式をシスコ方式に変更する場合：

```
crypto ikev2 fragmentation preferred-method cisco
```

- 優先するフラグメンテーション方式を IETF に戻す場合：

```
no crypto ikev2 fragmentation preferred-method cisco
```

または

```
crypto ikev2 fragmentation preferred-method ietf
```

AAA 認証と認可

```
aaa authentication http console LOCAL
aaa authorization http console radius
```

AAA 認証は、ユーザが入力したユーザ名とパスワードを使用して、ローカル サーバに対して実行されます。追加の認可は、同じユーザ名を使用して *RADIUS* サーバに対して実行されます。 *service-type* 属性が取得された場合は、前述のように処理されます。

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。

Options	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
Option 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、LAN-to-LAN とリモート アクセス ネットワークの両方ではなく、どちらかで動作する単一の NAT/PAT デバイスの背後に設置された複数の IPsec ピアをサポートします。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 を使用するには、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 モードで次のサイト間手順を実行します。

手順

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。

例：

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 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。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。

（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。ASA とその接続先クライアントの両方で IPsec over TCP をイネーブルにします。ASA では、すべての IKEv1 対応インターフェイス上で動作するようにグローバルにイネーブルにされます。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。

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
```

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、**use the 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、Organizational Unit (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。

手順

ステップ 1 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。

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

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

ポリシー	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 ルックアップ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、サブジェクト識別名（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すべて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。

ステップ 2 コンフィギュレーションでトンネル 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 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* はルールの優先順位で、tunnel-group name は既存のトンネル グループでなければなりません。

例

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
```

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
```

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
```

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
```

IPsec の設定

ここでは、IPsec を使用して VPN を実装するときの ASA の設定に必要な手順について説明します。

暗号マップの定義

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。使用できるキーワードには次のものがあります。

- 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 （34 ページ） 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 モードで暗号マップを作成または暗号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、暗号マップを追加する暗号マップ 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、同じ名前を持つ暗号マップがそれぞれ区別されます。暗号マップに割り当てられているシーケンス番号によって、暗号マップセット内の暗号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。暗号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 トラフィックと暗号マップ セット内の暗号マップを、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（PFS）に使用する ECDH グループを指定します。暗号マップに対して 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 *map_name seq-num* **set reverse-route** [**dynamic**]

この暗号マップエントリに基づく任意の接続に対してリバースルートインジェクション（RRI）を有効にします。ダイナミックが指定されていない場合、RRI は設定時に実行され、静的とみなされます。設定が変更または削除されるまでそのままになります。ASA は、ルーティング テーブルにスタティック ルートを自動的に追加し、OSPF を使用してそれらのルートをプライベート ネットワークまたはボーダー ルータに通知します。

ダイナミックが指定されている場合、ルートは IPsec セキュリティアソシエーション（SA）の確立成功時に作成され、IPsec SA が削除されると削除されます。

（注）　ダイナミック RRI は IKEv2 ベースのスタティック暗号マップだけに適用されます。

[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。

暗号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*

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、暗号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暗号マップによって、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、スタティック暗号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暗号マップを探しますが、見つからない場合は、暗号マップセット内のダイナミック暗号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暗号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暗号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、暗号マップを 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。別の暗号マップを作成し、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。次の表に、暗号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。

クリプト マップ評価の結果	Response
permit 文が含まれている ACE の基準と一致	パケットを暗号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、暗号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。

クリプト マップ評価の結果	Response
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。

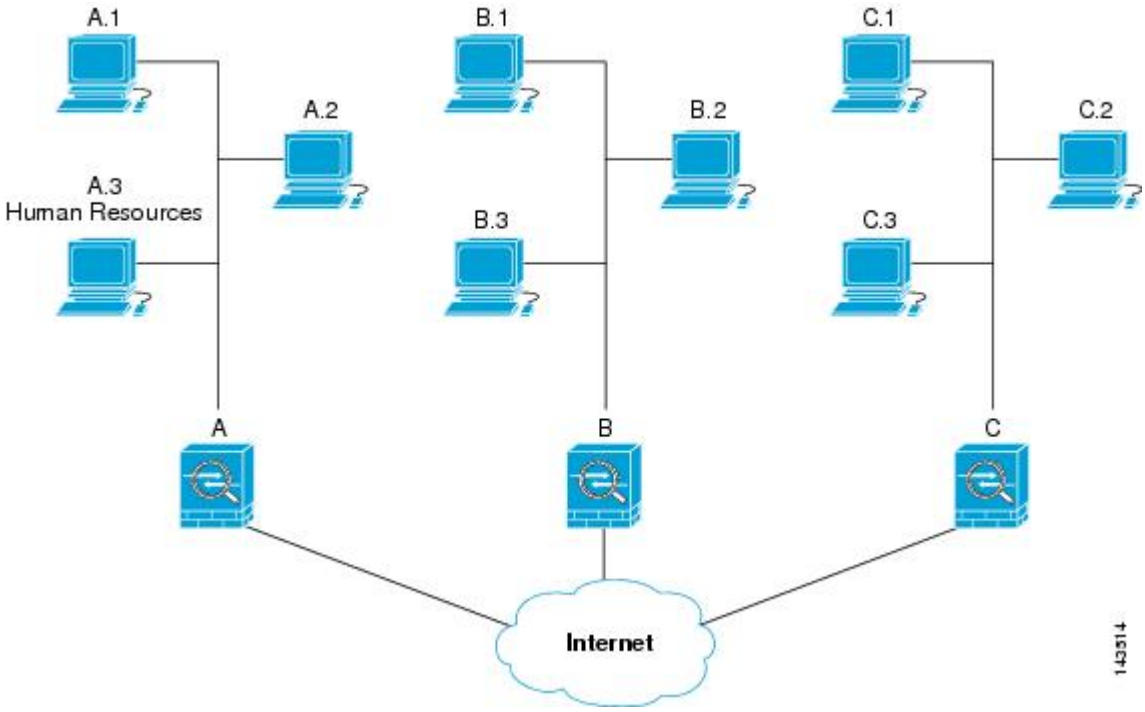
暗号化された着信パケットに対しては、セキュリティアプライアンスは送信元アドレスと ESP SPI を使用して、パラメータの復号化を決定します。セキュリティアプライアンスは、パケットを復号化した後で、復号化されたパケットの内部ヘッダーを、そのパケットの SA に関連付けられている ACL の許可 ACE と比較します。内部ヘッダーがプロキシと一致しない場合、セキュリティアプライアンスはそのパケットをドロップします。内部ヘッダーがプロキシと一致する場合、セキュリティ アプライアンスはそのパケットをルーティングします。

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、ACE の許可の前に ACE の拒否を挿入します。

LAN-to-LAN 暗号マップの例

この LAN-to-LAN ネットワークの例において、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、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。



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。

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 つの暗号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
```

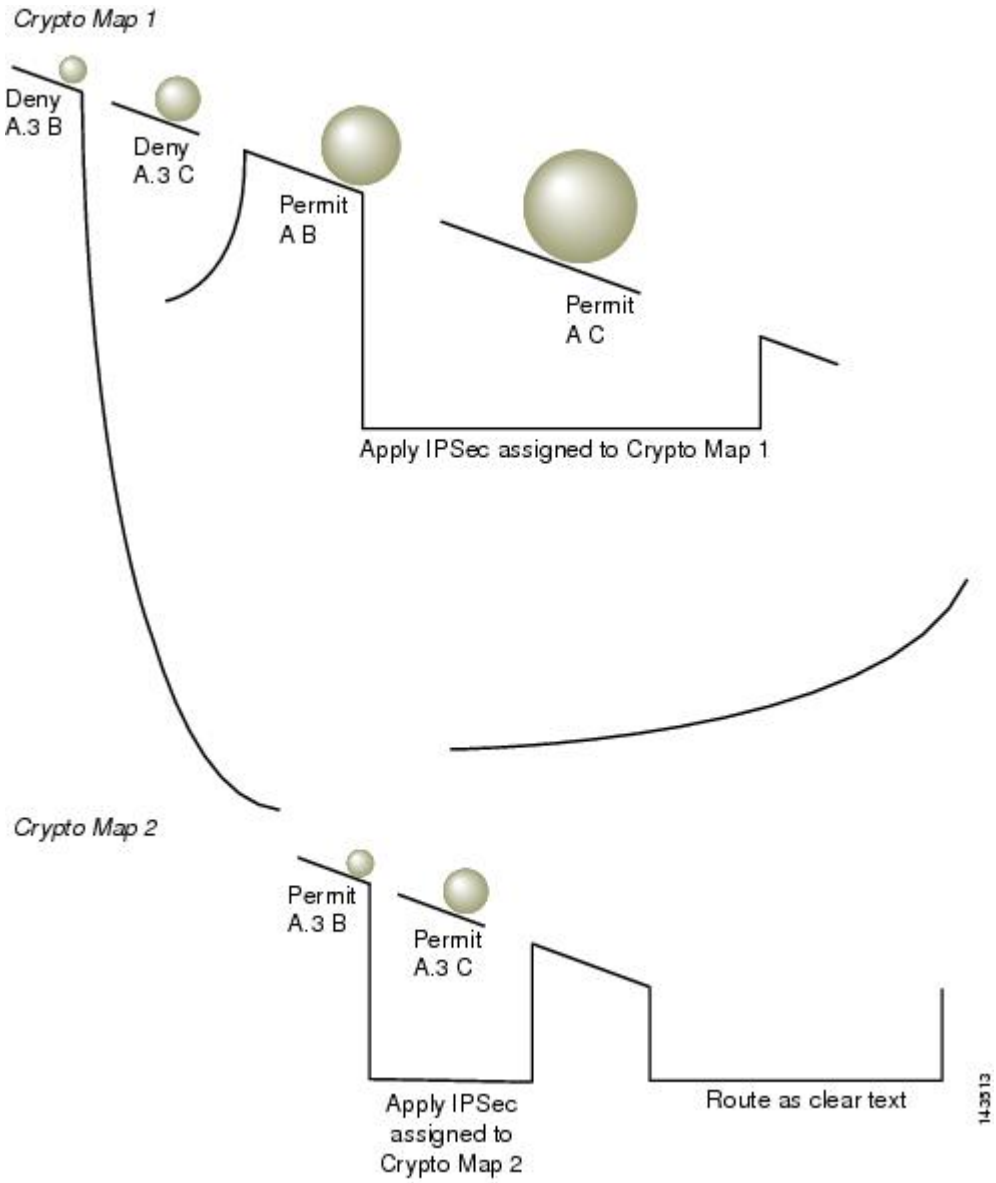
ACL を作成したら、一致するパケットごとに必要な IPsec を適用するためのトランスフォームセットを各暗号マップに割り当てます。

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。暗号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暗号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暗号マップ、または異なるセキュリティを必要とする別の暗号マップの 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、暗号マップ セット内の評価の順序が決まります。

次の図に、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。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* : 暗号マップ セット内のカスケード *ACL*



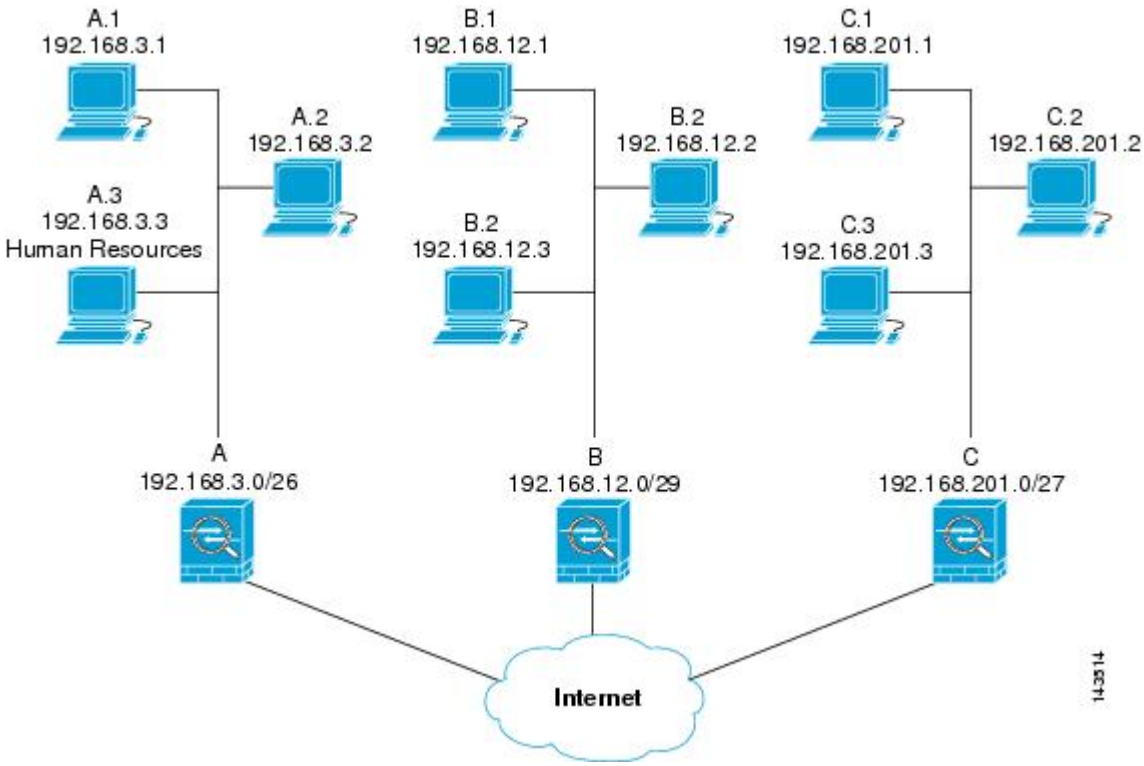
セキュリティ アプライアンス A は、ホスト A.3 から発信されたパケットが許可 ACE と一致するまで評価し、クリプト マップに関連付けられている IPsec セキュリティの割り当てを試行します。このパケットが拒否 ACE と一致すると、ASA はこの暗号マップの残りの ACE を無視し、次の暗号マップ（暗号マップに割り当てられているシーケンス番号で判断する）との照合と評価を再開します。この例では、セキュリティ アプライアンス A がホスト A.3 から発信されたパケットを受信すると、このパケットを最初のクリプト マップの拒否 ACE と照合し、次のクリプト マップでの照合と評価を再開しま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

ネットワーク例の ASA 設定を完了するために、ASA B と C にミラー暗号マップを割り当てますが、ASA は、暗号化された着信トラフィックの評価時に deny ACE を無視するため、deny A.3 B ACE と deny A.3 C ACE のミラーに相当するものを除外できます。したがって、暗号マップ 2 のミラーに相当するものは必要ありません。このため、ASA B と C のカスケード ACL の設定は不要です。

次の表に、ASA A、B、および C のすべてに設定された暗号マップに割り当てられる ACL を示します。

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 Sequence いいえ。	ACE パターン	クリプト マップ Sequence いいえ。	ACE パターン	クリプト マップ Sequence いいえ。	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				

次の図は、上で示した概念上のアドレスを実際の IP アドレスにマッピングしたものです。



次の表に示す実際の ACE では、そのネットワーク上で評価されるすべての IPsec パケットに適切な IPsec 設定が適用されます。

セキュリティアプライアンス	クリプトマップ **Sequence** いいえ。	**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

セキュリティ アプライアンス	クリプト マップ Sequence いいえ。	ACE パターン	実際の ACE
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）キーの設定

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。

始める前に

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

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]

クリプト マップのインターフェイスへの適用

暗号マップ 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。暗号マップ 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暗号マップ 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 データ構造も初期設定されます。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暗号マップ 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）。

暗号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。各暗号マップは 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 暗号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** エントリにだけ適用されます）。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。

（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暗号マップも削除します。

現在 1 つまたは複数の暗号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暗号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暗号マップで 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、暗号マップは不完全なものになり、ASA は、前の完全な暗号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、すべての暗号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。

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。

手順

ステップ 1 IPsec に使用する ACL を作成します。

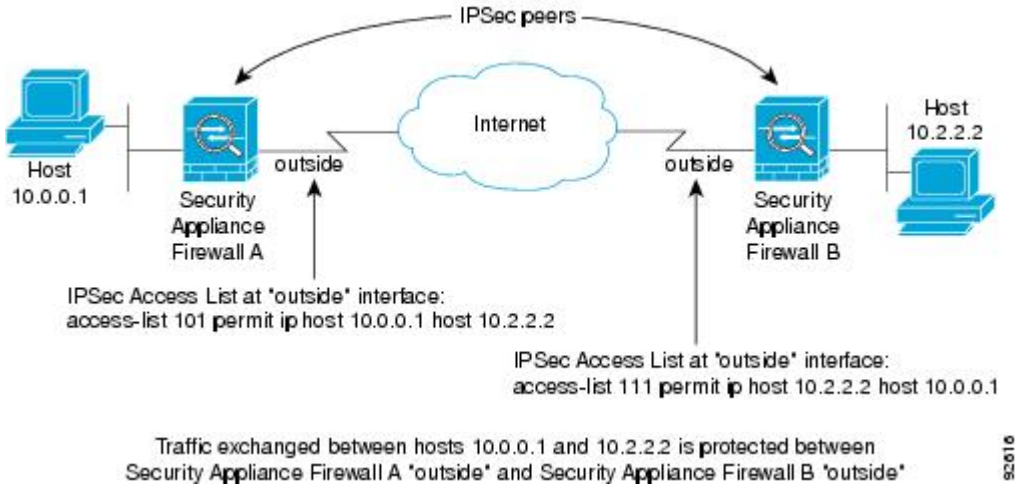
ステップ 2 作成したアクセス リストを、同じクリプトマップ名を使用して1つまたは複数のクリプトマップにマッピングします。

ステップ 3 データ フローに IPsec を適用するために、暗号マップに 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。

例

この例では、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。



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。

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。

暗号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、暗号マップは、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。

VPN ルーティングの変更

デフォルトでは、外部 ESP パケットに対してはパケット単位の隣接関係ルックアップが行われ、IPSec トンネル経由で送信されるパケットに対してはルックアップが行われません。

一部のネットワーク トポロジでは、ルーティング アップデートによって内部パケットのパスが変更され、ローカル IPsec トンネルが引き続きアップ状態である場合、トンネル経由のパケットは正しくルーティングされず、宛先に到達しません。

これを防止するには、IPSec 内部パケットに対してパケット単位のルーティング ルックアップをイネーブルにします。

始める前に

この機能がデフォルトでディセーブルになっているのは、こうしたルックアップによるパフォーマンスの低下を回避するためです。この機能は、必要な場合にのみイネーブルにしてください。

手順

IPSec 内部パケットに対してパケット単位のルーティング ルックアップをイネーブルにします。

[no] [crypto] ipsec inner-routing-lookup

例

```
ciscoasa(config)# crypto ipsec inner-routing-lookup
ciscoasa(config)# show run crypto ipsec
 crypto ipsec ikev2 ipsec-proposal GCM
 protocol esp encryption aes-gcm
 protocol esp integrity null
 crypto ipsec inner-routing-lookup
```

スタティック暗号マップの作成

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。

手順

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*

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。

例：

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

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。

例：

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。

```
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
```

ステップ 3 トラフィックを保護する方法も定義する IKEv2 プロポーザルを設定するには、次のコマンドを入力します。

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。

プロポーザルを作成し、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。このコンフィギュレーション モードでは、プロポーザルに対して複数の暗号化タイプと整合性タイプを指定できます。

例：

```
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
```

例：

このコマンドでは、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。

[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。

[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 4 （任意）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。

[no] crypto ipsec security-association pmtu-aging *reset-interval*

ステップ 5 暗号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 を暗号マップに割り当てます。

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

暗号マップセットとは、暗号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。

例：

この例では、ACL 101 が暗号マップ mymap に割り当てられます。

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

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*

例：

```
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 つの暗号マップに最大 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*]

または

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。各暗号マップ 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 の場合のこの例では、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。

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

d) （任意）IKEv2 では、トンネルに ESP 暗号化と認証を適用するための **mode** を指定します。これにより、ESP が適用されるオリジナルの IP パケットの部分が決定されます。

crypto map *map-name seq-num***set ikev2 mode** [**transport | tunnel | transport-require**]

- [Tunnel mode]（デフォルト）：カプセル化モードがトンネル モードになります。トンネル モードでは、ESP 暗号化と認証が元の IP パケット全体（IP ヘッダーとデータ）

に適用されるため、本来の送信元アドレスと宛先アドレスが非表示になります。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）。

- [Transport mode]：ピアがサポートしていない場合、カプセル化モードは、トンネル モードにフォールバックするオプション付きの転送モードになります。転送モードでは、IP ペイロードだけが暗号化され、元の IP ヘッダーはそのままになります。

  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。transport モードでは、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。

- [Transport Required]：カプセル化モードは転送モードにしかなりません。トンネル モードにフォールバックすることはできません。

ここでは、**tunnel** カプセル化モードがデフォルトです。**transport** カプセル化モードは、ピアがこのモードをサポートしていない場合に tunnel モードにフォールバックできる転送モードであり、**transport-require** カプセル化モードでは、転送モードのみが適用されます。

（注） 転送モードは、リモート アクセス VPN には推奨されません。

カプセル化モードのネゴシエーションの例は次のとおりです。

- イニシエータが転送モードを提案し、レスポンダがトンネル モードで応答した場合、イニシエータはトンネル モードにフォールバックします。
- 発信側が tunnel モードを提示し、応答側が transport モードで応答した場合、応答側は tunnel モードにフォールバックします。
- 発信側が tunnel モードを提示し、応答側が transport-require モードの場合、応答側はプロポーザルを送信しません。
- 同様に、発信側が transport-require モードを提示し、応答側が tunnel モードの場合、応答側はプロポーザルを送信しません。

e) （任意）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** *number* | **kilobytes** {*number* | **unlimited**}}

map-name では、暗号マップ セットの名前を指定します。*seq-num* では、暗号マップ エントリに割り当てる番号を指定します。時間または送信されたデータに基づいて両方のライフタイムを設定できます。ただし、データ送信ライフタイムはサイト間 VPN にのみ適用され、リモート アクセス VPN には適用されません。

例：

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。

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

f) （任意）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 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**]

例：

この例では、暗号マップ 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。

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

g) （任意）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（RRI）をイネーブルにします。

crypto map *map_name seq-num* **set reverse-route** [**dynamic**]

ダイナミックが指定されていない場合、RRI は設定時に行われ、静的とみなされます。設定が変更または削除されるまでそのままになります。ASA は、ルーティング テーブルにスタティック ルートを自動的に追加し、OSPF を使用してそれらのルートをプライベート ネットワークまたはボーダー ルータに通知します。

ダイナミックが指定されている場合、ルートはIPsecセキュリティアソシエーション（SA）の確立成功時に作成され、IPsec SA が削除されると削除されます。

（注） ダイナミック RRI は IKEv2 ベースのスタティック暗号マップだけに適用されます。

例：

```
crypto map mymap 10 set reverse-route dynamic
```

ステップ 6 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、暗号マップ 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。

例：

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暗号マップ mymap と照合して評価し、保護が必要かどうかを判断します。

```
crypto map mymap interface outside
```

ダイナミック暗号マップの作成

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、スタティック暗号マップでピアの 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暗号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。

ダイナミック暗号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、ダイナミック暗号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。ダイナミック暗号マップでは、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。ダイナミック暗号マップのセットには、暗号マップ 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 が他の暗号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。ダイナミック暗号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 ダイナミック暗号マップ 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。

シングル コンテキスト モードとマルチ コンテキスト モードのどちらかを使用して、ダイナミック暗号マップのエントリを作成します。1 つのクリプト マップ セット内で、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ができます。

手順

ステップ 1 （任意） ACL をダイナミック暗号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暗号マップを参照する暗号マップ エントリの名前を指定します。*dynamic-seq-num* では、ダイナミック暗号マップ エントリに対応するシーケンス番号を指定します。

例：

この例では、ACL 101 がダイナミック暗号マップ 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。

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

ステップ 2 このダイナミック暗号マップに対して、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暗号マップを参照する暗号マップ エントリの名前を指定します。*dynamic-seq-num* では、ダイナミック暗号マップ 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 の場合のこの例では、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。

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

ステップ 3 （任意）グローバル ライフタイム値を無効にする場合は、暗号ダイナミック マップ エントリの 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** *number* | **kilobytes** {*number* | **unlimited**}}

dynamic-map-name では、既存のダイナミック暗号マップを参照する暗号マップ エントリの名前を指定します。*dynamic-seq-num* では、ダイナミック暗号マップ エントリに対応するシーケンス番号を指定します。時間または送信されたデータに基づいて両方のライフタイムを設定できます。ただし、データ送信ライフタイムはサイト間 VPN にのみ適用され、リモート アクセス VPN には適用されません。

例：

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。

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

ステップ 4 （任意） IPsec がこのダイナミック暗号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暗号マップを参照する暗号マップ エントリの名前を指定します。*dynamic-seq-num* では、ダイナミック暗号マップ エントリに対応するシーケンス番号を指定します。

例：

```
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、暗号マップ 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暗号マップを参照する暗号マップ エントリの名前を指定します。

例：

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

サイトツーサイト冗長性の実現

暗号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、暗号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。暗号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 VPN の管理

IPsec コンフィギュレーションの表示

これらは、IPsec コンフィギュレーションに関する情報を表示するためにシングルまたはマルチ コンテキスト モードで入力できるコマンドです。

表 *1 : 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

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。

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場合に限り 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。

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と、**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。

手順

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

例：

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

接続解除の前にピアに警告する

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 では、（LAN-to-LAN コンフィギュレーションまたは VPN クライアントの）限定されたピアに対して、セッションが接続解除される直前に通知できます。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）

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。

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。

次の表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 *2: IPsec SA* のクリアおよび再初期化用のコマンド

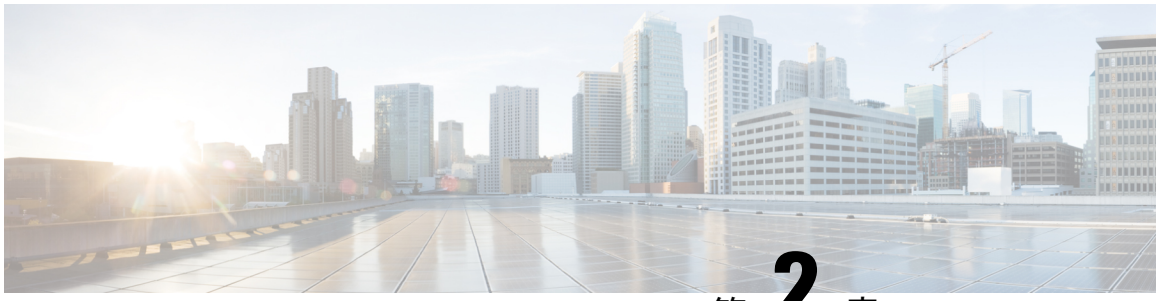
clear configure crypto	IPsec、クリプトマップ、ダイナミック クリプト マップ、ISAKMP など、暗号コンフィギュレーション全体を削除します。
clear configure crypto ca trustpoint	すべてのトラストポイントを削除します。
clear configure crypto dynamic-map	すべてのダイナミック クリプトマップを削除します。特定のダイナミック クリプトマップを削除できるキーワードもあります。
clear configure crypto map	すべてのクリプト マップを削除します。特定のクリプト マップを削除でき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。

暗号マップ 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、暗号マップ、ダイナミック暗号マップ、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。



第 2 章

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。

L2TP over IPsec/IKEv1 VPN について

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、一般的操作用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。

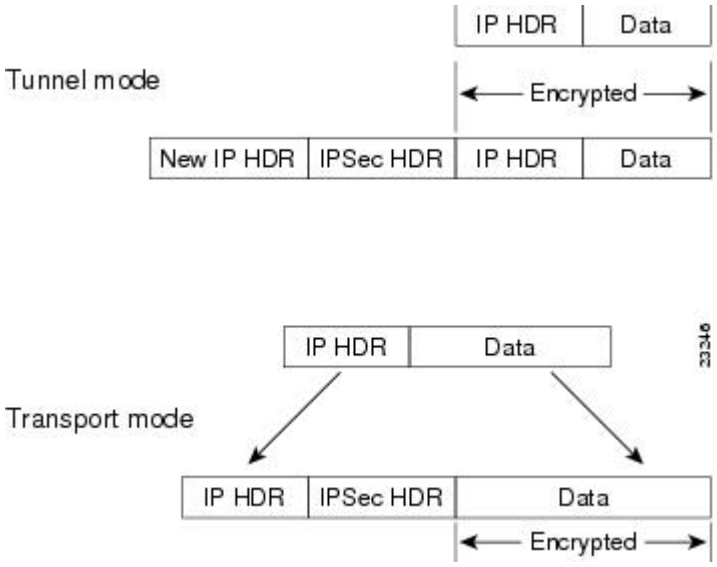
（注） ASA で IPsec を使用する L2TP を設定すると、Windows、MAC OS X、Android および Cisco IOS などのオペレーティング システムに統合されたネイティブ VPN クライアントと LNS が相互運用できるようになります。サポートされているのは、IPsec を使用する L2TP だけで、ネイティブの L2TP そのものは、ASA ではサポートされていません。 Windows クライアントがサポートしている IPsec セキュリティ アソシエーションの最短ライフタイムは 300 秒です。ASA でライフタイムを 300 秒未満に設定している場合、Windows 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。次の図に、IPsec のトンネル モードと転送モードの違いを示します。

図 *2 : IPsec* のトンネル モードと転送モード



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。

L2TP over IPsec 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。

IKEv2 を使用した IPsec リモート アクセス VPN には、別途購入可能な AnyConnect Plus または Apex ライセンスが必要です。AnyConnect ライセンスを購入する場合は、次の最大値を参照してください。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 サイト間 VPN では、基本ライセンスに付属の Other VPN ライセンスが使用されます。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越えることはできません。

モデル	ライセンス要件

ASA 5506-X、5506H-X、5506W-X	• IKEv2 を使用した IPsec リモート アクセス VPN：50 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：50 セッション。

ASA 5508-X	100 セッションです。
ASA 5512-X	250 セッションです。
ASA 5515-X	250 セッションです。
ASA 5516-X	300 セッションです。
ASA 5525-X	750 セッションです。
ASA 5545-X	2500 セッションです。
ASA 5555-X	5000 セッションです。
ASA 5585-X（SSP-10）	5000 セッションです。
ASA 5585-X（SSP-20、-40、および -60）	10,000 セッションです。
ASASM	10,000 セッションです。
ASAv5	250 セッションです。
ASAv10	250 セッションです。
ASAv30	750 セッションです。

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。

- グループ ポリシー：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。

- 接続プロファイル：「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。

注意事項と制約事項

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 モードとマルチ コンテキスト モードでサポートされています。AnyConnect Apex ライセンスは、マルチコンテキスト モードのリモートアクセス VPN に必要です。ASA は AnyConnect Apex ライセンスを特異的に認識しませんが、プラットフォーム制限へのライセンス済み AnyConnect Premium、携帯電話用 AnyConnect、Cisco VPN フォン用 AnyConnect、および Advanced Endpoint Assessment など、Apex ライセンスのライセンス特性を適用します。

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 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 上の L2TP over IPsec 接続は、次の図に示す PPP 認証タイプだけをサポートします。

表 *3: 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 *4: PPP* 認証タイプの特性

キーワード	**Authentication Type**	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。

キーワード	Authentication Type	特性
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。

CLI を使用した L2TP over IPsec の設定

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 に VPN 接続できるように IKEv1（ISAKMP）ポリシーを設定する必要があります。

- 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）

手順

ステップ 1 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。

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
```

ステップ 2 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。

crypto ipsec ike_version transform-set *trans_name***mode transport**

例：

```
crypto ipsec ikev1 transform-set my-transform-set-ikev1 mode transport
```

ステップ 3 L2TP/IPsec を vpn トンネリング プロトコルとして指定します。

vpn-tunnel-protocol *tunneling_protocol*

例：

```
hostname(config)# group-policy DfltGrpPolicy attributes
hostname(config-group-policy)# vpn-tunnel-protocol l2tp-ipsec
```

ステップ 4 （任意） 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。

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
```

ステップ 5 （任意） 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。

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
```

ステップ 6 （任意） IP アドレス プールを作成します。

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
```

ステップ 7 （任意） 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。

address-pool *pool_name*

例：

```
hostname(config)# tunnel-group DefaultRAGroup general-attributes
hostname(config-tunnel-general)# address-pool sales_addresses
```

ステップ 8 接続プロファイル（トンネル グループ）を作成します。

tunnel-group *name***type remote-access**

例：

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

ステップ 9 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。

default-group-policy name

例：

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

ステップ 10 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。

authentication-server-group *server_group* [**local**]

例：

```
hostname(config)# tunnel-group DefaultRAGroup general-attributes
hostname(config-tunnel-general)# authentication-server-group sales_server LOCAL
```

ステップ 11 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。

authentication *auth_type*

例：

```
hostname(config)# tunnel-group name ppp-attributes
hostname(config-ppp)# authentication ms-chap-v1
```

ステップ 12 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。

tunnel-group *tunnel group name***ipsec-attributes**

例：

```
hostname(config)# tunnel-group DefaultRAGroup ipsec-attributes
hostname(config-tunnel-ipsec)# ikev1 pre-shared-key cisco123
```

ステップ 13 （任意） 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。

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
```

ステップ 14 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。

l2tp tunnel hello *seconds*

例：

```
hostname(config)# l2tp tunnel hello 100
```

ステップ 15 （任意） 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。

crypto isakmp nat-traversal *seconds*

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。

例：

```
hostname(config)# crypto ikev1 enable
hostname(config)# crypto isakmp nat-traversal 1500
```

ステップ 16 （任意）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。

strip-group

strip-realm

例：

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

ステップ 17 （任意）ユーザ名 **jdoe**、パスワード **j!doe1** でユーザを作成します。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。

username *name***password** *password***mschap**

例：

```
asa2(config)# username jdoe password j!doe1 mschap
```

ステップ 18 フェーズ 1 の IKE ポリシーを作成し、番号を割り当てます。

crypto ikev1 policy *priority*

group *Diffie-Hellman Group*

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、isakamp ポリシーが使用されます。

例：

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

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。

ASA の L2TP over IPsec を設定する手順に従います。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、このタスクに新しいステップを追加します。

手順

ステップ 1 既存の IKE ポリシーの属性と番号をすべて表示します。

例：

```
hostname(config)# show run crypto ikev1
```

ステップ 2 IKE ポリシーを設定します。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。

crypto ikev1 policy *number*

ステップ 3 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。

例：

```
hostname(config-ikev1-policy)# authentication pre-share
```

ステップ 4 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** または **aes**（128 ビット AES の場合）、または **aes-256** を選択します。

encryption 3desaesaes-256

ステップ 5 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。

例：

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

ステップ 6 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。

例：

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

ステップ 7 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。

例：

```
hostname(config-ikev1-policy)# lifetime 86400
```

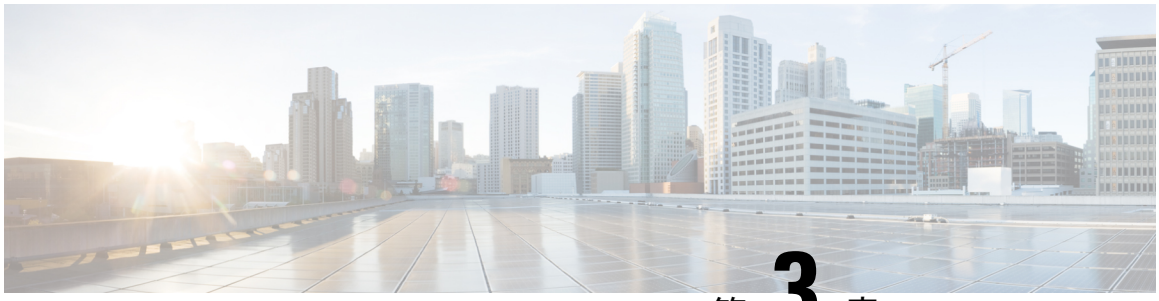
L2TP over IPsec の設定例

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 trans esp-des esp-sha-hmac
crypto ipsec ikev1 transform-set trans 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

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。



第 3 章

ハイアベイラビリティ オプション

ハイアベイラビリティ オプション

分散型 VPN クラスタリング、ロード バランシング、およびフェールオーバーは、それぞれ機能と要件が異なるハイアベイラビリティ機能です。状況によっては、複数の機能を導入環境で使用することがあります。以降では、これらの機能について説明します。分散型VPNとフェールオーバーの詳細については、『ASA General Operations CLI Configuration Guide』の適切なリリースを参照してください。ロード バランシングの詳細は以下に記載されています。

FXOS シャーシ上の VPN とクラスタリング

ASA FXOS クラスタは、S2S VPN に対する相互排他的な 2 つのモード（集中型または分散型）のいずれかをサポートしています。

- 集中型 VPN モード。デフォルト モードです。集中モードでは、VPN 接続はクラスタのマスターとのみ確立されます。

  VPN 機能を使用できるのはマスター ユニットだけであり、クラスタのハイ アベイラビリティ能力は活用されません。マスターユニットで障害が発生した場合は、すべての既存の VPN 接続が失われ、VPN 接続されたユーザにとってはサービスの中断となります。新しいマスターが選定されたときに、VPN 接続を再確立する必要があります。

  VPN トンネルをスパンド インターフェイスのアドレスに接続すると、接続が自動的にマスター ユニットに転送されます。VPN 関連のキーと証明書は、すべてのユニットに複製されます。

- 分散型 VPN モード。このモードでは、S2S IPsec IKEv2 VPN 接続が ASA クラスタのメンバー全体に分散され、拡張性が提供されます。クラスタのメンバー全体に VPN 接続を分散することで、クラスタの容量とスループットの両方を最大限に活用できるため、集中型 VPN の機能を超えて大幅に VPN サポートを拡張できます。

（注） 集中型 VPN クラスタリング モードは、S2S IKEv1 と S2S IKEv2 をサポートしています。

分散型 VPN クラスタリング モードは、S2S IKEv2 のみをサポートしています。

分散型 VPN クラスタリング モードは、Firepower 9300 でのみサポートされています。

リモート アクセス VPN は、集中型または分散型の VPN クラスタリング モードではサポートされていません。

ロード バランシング

ロードバランシングは、仮想クラスタ内のデバイス間でリモート アクセス VPN トラフィックを均一に分散するメカニズムです。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伝送します。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 コンフィギュレーションでは、2台の同一のASAが専用のフェールオーバー リンクで接続され、必要に応じて、ステートフル フェールオーバー リンク（任意）でも接続されます。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設定をサポートしています。

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 トラフィックを渡すことができます。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

ロード バランシングの概要

リモート クライアント コンフィギュレーションで、複数の ASA を同じネットワークに接続してリモート セッションを処理している場合、これらのデバイスでセッション負荷を分担するように設定できます。この機能は、ロード バランシングと呼ばれます。ロード バランシングでは、最も負荷の低いデバイスにセッション トラフィックが送信されます。このため、すべてのデバイス間で負荷が分散されます。これにより、システム リソースを効率的に利用でき、パフォーマンスと可用性が向上します。

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 間ネットワーク上の複数のデバイスを、論理的に仮想クラスタとしてグループ化します。

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。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、着信接続要求をバックアップ 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 回目のトランザクションで、クライアントは直接そのホストに接続します（この動作はユーザには透過的です）。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。

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。

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、同じリリースまたは混在リリースの ASA から構成できます。ただし、次の制約があります。

- 同じリリースの 2 台の ASA から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 を含む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達しない可能性があります。

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が伝送す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 リリース 7.0(x) ソフトウェア用のロードバランシングの計算からの逸脱を意味しています。つまり、このプラットフォームでは、いずれも一部のハードウェア プラットフォームにおいて、IPsec セッションの負荷とは異なる SSL VPN セッションの負荷を計算する重み付けアルゴリズムを使用しています。

クラスタの仮想マスターは、クラスタのメンバ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。

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。

一般的な混在クラスタ シナリオの例

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 リリース 7.1(1) ソフトウェアおよび ASA リリース 7.0(x) ソフトウェアを実行しているさまざまな ASA 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、クラスタはさまざまな ASA 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。

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、クラスタがさまざまな ASA 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 SSL VPN 接続だけでなく IPsec 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。これは、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 バランシングについての FAQ

マルチ コンテキスト モード

Q. ロード バランシングはマルチコンテキスト モードでサポートされていますか。

A. ロード バランシングもステートフル フェールオーバーもマルチコンテキスト モードではサポートされていません。

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 バランシングのライセンス

VPN ロード バランシングを使用するには、Security Plus ライセンスを備えた ASA モデル 5512-X、または ASA モデル 5515-X 以降が必要です。また、VPN ロード バランシングには、アクティブな 3DES/AES ライセンスも必要です。セキュリティ アプライアンスは、ロード バランシングをイネーブルにする前に、この暗号ライセンスが存在するかどうかをチェックします。アクティブな 3DES または AES のライセンスが検出されない場合、セキュリティ アプライアンスはロードバランシングをイネーブルにせず、ライセンスでこの使用方法が許可されて

いない場合には、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抑止します。

VPN ロード バランシングに関するガイドラインと制限事項

ロード バランシングの前提条件 （74 ページ）も参照してください。

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。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 Secure Mobility Client（リリース 3.0 以降）
- Cisco ASA 5505 セキュリティ アプライアンス（Easy VPN クライアントとして動作する場合）
- IKE リダイレクトをサポートする 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）

クライアントの考慮事項

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 を含めて、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、ロード バランシングには参加できません。

複数の ASA ノードがロードバランシングのためにクラスタ化され、AnyConnect クライアント接続にグループ URL の使用が必要な場合、個々の ASA ノードは以下を行う必要があります。

- 各リモート アクセス接続プロファイルに、各ロード バランシング仮想クラスタ アドレス（IPv4 および IPv6）のグループ URL を設定します。
- このノードの VPN ロード バランシング パブリック アドレスに対してグループ URL を設定します。

コンテキスト モード

マルチ コンテキスト モードでは、VPN ロード バランシングはサポートされません。

証明書の確認

AnyConnect でロード バランシングの証明書確認を実行し、IP アドレスによって接続がリダイレクトされている場合、クライアントにより、この IP アドレスを通してその名前チェックが

すべて実行されます。リダイレクト IP アドレスが証明書の一般名、つまり subject alt name に一覧表示されていることを確認する必要があります。IP アドレスがこれらのフィールドに存在しない場合、証明書は非信頼と見なされます。

RFC 2818 で定義されたガイドラインに従って、**subject alt name** が証明書に組み込まれている場合、名前チェックにのみ **subject alt name** を使用し、一般名は無視します。証明書を提示しているサーバの IP アドレスが証明書の **subject alt name** で定義されていることを確認します。

スタンドアロン ASA の場合、IP アドレスはその ASA の IP です。クラスタリング環境では、証明書の設定により異なります。クラスタが 1 つの証明書を使用している場合、証明書は、クラスタ IP アドレスおよびクラスタ FQDN の SAN 拡張機能を保持するほか、各 ASA の IP および FQDN を備えたサブジェクト代替名の拡張機能を含む必要があります。クラスタが複数の証明書を使用している場合、各 ASA の証明書は、クラスタ IP の SAN 拡張機能、クラスタ FQDN、個々の ASA の IP アドレスおよび FQDN を保持する必要があります。

地理的ロード バランシング

ロード バランシング環境において DNS 解決が一定の間隔で変化する場合は、存続可能時間（TTL）の値をどのように設定するかを慎重に検討する必要があります。DNS ロード バランス設定が AnyConnect との組み合わせで適切に機能するには、マッピングを処理する ASA の名前が、その ASA が選択された時点からトンネルが完全に確立されるまでの間、同じである必要があります。所定の時間が経過してもクレデンシャルが入力されない場合は、ルックアップが再び開始して別の IP アドレスが解決済みアドレスとなることがあります。DNS のマッピング先が別の ASA に変更された後でクレデンシャルが入力された場合は、VPN トンネルの確立に失敗します。

VPN の地理的ロード バランシングでは、Cisco Global Site Selector（GSS）が使用されることがあります。GSS では DNS がロード バランシングに使用され、DNS 解決の存続可能時間（TTL）のデフォルト値は 20 秒となっています。GSS での TTL の値を大きくすると、接続失敗の確率を大幅に引き下げることができます。値を大きくすると、ユーザがクレデンシャルを入力してトンネルを確立するときの認証フェーズに十分な時間を取ることができます。

クレデンシャル入力のための時間を増やすには、「起動時接続」をディセーブルにすることも検討してください。

ロード バランシングの設定

リモート クライアント コンフィギュレーションで、複数の ASA を同じネットワークに接続してリモート セッションを処理している場合、これらのデバイスでセッション負荷を分担するように設定できます。この機能はロード バランシングと呼ばれ、最も負荷の低いデバイスにセッション トラフィックが送信されます。このため、すべてのデバイス間で負荷が分散されます。ロード バランシングにより、システム リソースが効率的に使用され、パフォーマンスとシステム アベイラビリティが向上します。

ロード バランシングを使用するには、クラスタ内の各デバイスで以下を実行します。

- 共通の VPN ロードバランシング クラスタ属性を設定することによってロードバランシング クラスタを設定します。これには、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 共有秘密が含まれます。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。

- デバイスでロード バランシングを有効にし、パブリック アドレスとプライベート アドレスなどのデバイス固有のプロパティを定義することにより、参加するデバイスを設定します。これらの値はデバイスによって異なります。

ロード バランシングの前提条件

VPN ロード バランシングに関するガイドラインと制限事項 （72 ページ）も参照してください。

- 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。
- 最初にパブリック（外部）およびプライベート（内部）インターフェイスを設定しておく必要があります。この項では、これ以降の参照に外部および内部の名前を使用します。

  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。
- 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する必要があります。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 共有秘密を確立します。
- 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。
- 暗号化を使用する場合は、インターフェイス内にロードバランシングを設定する必要があります。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。
- 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。

手順

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。

例：

```
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。

例：

```
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。値の範囲は 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。

例：

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。

例：

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。

手順

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。

例：

```
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から、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。

例：

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。

例：

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 （任意）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。

（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、指定した内部インターフェイスで **crypto ikev1 enable** コマンドを使用します。

例：

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

ステップ 5 クラスタの暗号化をイネーブルにする場合は、**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。

例：

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。

例：

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

次のタスク

複数の ASA ノードがロード バランシングのためにクラスタ化され、AnyConnect クライアント接続にグループ URL の使用が必要な場合、個々の ASA ノードで以下を行う必要があります。

- 各リモート アクセス接続プロファイルに、各ロード バランシング仮想クラスタ アドレス（IPv4 および IPv6）のグループ URL を設定します。
- このノードの VPN ロード バランシング パブリック アドレスに対してグループ URL を設定します。

これらのグループ URL を設定するには、**tunnel-group**、**general-attributes**、**group-url** コマンドを使用します。

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

デフォルトで、ASA はロードバランシング リダイレクションの 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 クライアント接続を別のクラスタ デバイス（クラスタ内の別の ASA）にリダイレクトするときに、この ASA は VPN クラスタ マスターとして、DNS 逆ルックアップを使用し、そのクラスタ デバイスの（外部 IP アドレスではなく）完全修飾ドメイン名（FQDN）を送信できます。

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するリダイレクションを有効または無効にするには、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。

始める前に

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。

手順

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。

[**no**] **redirect-fqdn** {**enable** | **disable**}

例：

```
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 で DNS サーバ IP アドレスを定義します（例：dns name-server 10.2.3.4（DNS サーバの IP アドレス）。

VPN ロード バランシングの設定例

基本の VPN ロード バランシング CLI 設定

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
```

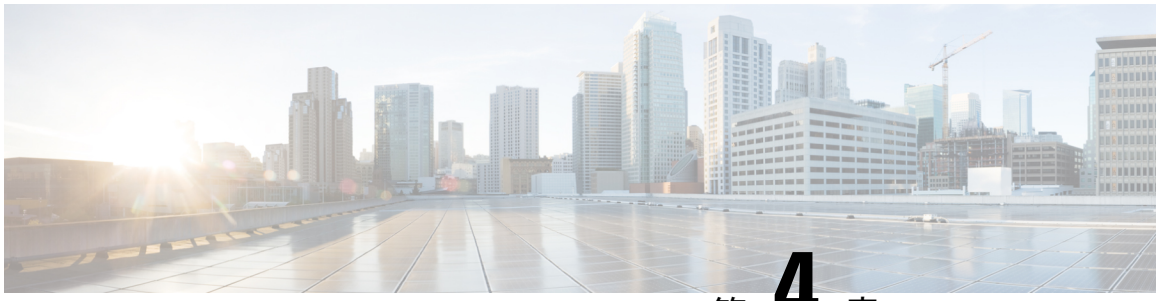
ロード バランシングの表示

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# show vpn 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
```



第 4 章

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。

注意事項と制約事項

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 モードとマルチ コンテキスト モードでサポートされています。『ASA General Operations CLI Configuration Guide』の適切なリリース では、マルチ コンテキスト モードでサポートされていないもののリストについては『*Guidelines for Multiple Context Mode*』を参照してください。また「*New Features*」には、リリースを通して追加されたものの明細が示されています。

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 モードはサポートされていません。

ACL をバイパスするための IPsec の設定

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ます。

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アクセス グループ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。

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-vpn** 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。

sysopt connection permit-vpn は、その対象のトラフィックの暗号マップが有効になっているインターフェイスに対する ACL（インとアウトの両方）と、他のすべてのインターフェイスの出力（アウト）ACL（入力（イン）ACL ではない）をバイパスします。

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へ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。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。

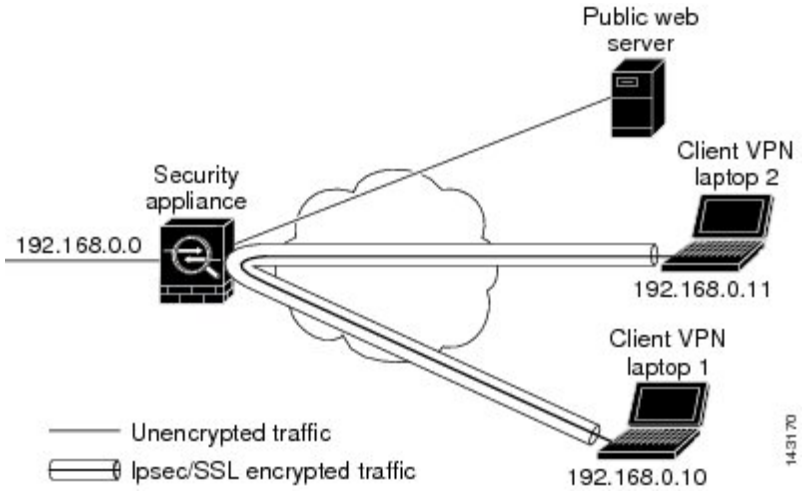
インターフェイス内トラフィックの許可（ヘアピニング）

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。

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することもできます。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つ可能性があります。

下の図は、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:* 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が許可されます。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、「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」に記載されているように、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セッションの最大数を1から最大数まで指定します。

（注） 正しいライセンス、用語、階層、およびユーザ数は、これらのコマンドで決定されなくなりました。『AnyConnect Ordering Guide』を参照してください。 http://www.cisco.com/c/dam/en/us/products/collateral/security/anyconnect-og.pdf

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 セッションの最大数を 1 から最大数まで指定します。これには、Cisco VPN Client（IPsec IKEv1）および LAN-to-LAN 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、更新を実行するメカニズムをユーザに提供できます。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、ソフトウェアを更新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、ソフトウェアを更新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。

手順

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のタイプは、**win9X**（Windows 95、Windows 98、および Windows ME プラットフォームを含む）、**winnt**（Windows NT 4.0、Windows 2000、および Windows XP プラットフォームを含む）、**windows**（Windows ベースのすべてのプラットフォームを含む）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、ソフトウェアを更新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、ソフトウェアを更新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。

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）。

（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 （任意）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、次回ログオ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。

次のタスク

（注） クライアント更新のタイプを **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** のクライアント更新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。

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（IKEv1）クライアントと 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

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。

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、ライセンスのセクションを探します。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の情報を示しています。もう一方の出力は明確にするために編集されています。

```
hostname(config)# show version
...
Licensed features for this platform:
Maximum Physical Interfaces       : Unlimited      perpetual
Maximum VLANs                     : 500            perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Active  perpetual
Encryption-DES                    : Enabled        perpetual
Encryption-3DES-AES               : Enabled        perpetual
Security Contexts                 : 100            perpetual
Carrier                           : Enabled        perpetual
AnyConnect Premium Peers          : 5000           perpetual
AnyConnect Essentials             : 5000           perpetual
Other VPN Peers                   : 5000           perpetual
Total VPN Peers                   : 5000           perpetual
AnyConnect for Mobile             : Enabled        perpetual
AnyConnect for Cisco VPN Phone    : Enabled        perpetual
Advanced Endpoint Assessment      : Enabled        perpetual
Shared License                    : Disabled       perpetual
Total TLS Proxy Sessions          : 3000           perpetual
Botnet Traffic Filter             : Disabled       perpetual
```

```
IPS Module                          : Disabled       perpetual
Cluster                             : Enabled        perpetual
Cluster Members                     : 2              perpetual

This platform has an ASA5555 VPN Premium license.
```

ライセンス リソース割り当ての表示

リソース割り当てを表示するには、次のコマンドを使用します。

```
asa2(config)# sh resource allocation
Resource       Total    % of Avail
Conns[rate]    100(U)      0.00%
Inspects[rate] unlimited
Syslogs[rate]  unlimited
Conns          unlimited
Hosts          unlimited
IPsec          unlimited
Mac-addresses  unlimited
ASDM           10          5.00%
SSH            10          10.00%
Telnet         10          10.0%
Xlates         unlimited
AnyConnect     1000        10%
AnyConnectBurst 200        2%
OtherVPN       2000        20%
OtherVPNBurst  1000        10%
```

ライセンス リソース使用率の表示

リソース使用率を表示するには、次のコマンドを使用します。

（注） **sh resource usage system controller all 0** コマンドを使用して、プラットフォーム制限として制限があるシステム レベルの使用率を表示することもできます。

```
ASA(config-ca-trustpoint)# sh resource usage
Resource        Current  Peak  Limit  Denied  Context
Conns           1        16    280000 0       System
Hosts           2        10    N/A    0       System
AnyConnect      2        25    1000   0       cust1
AnyConnectBurst 0        0     200    0       cust1
OtherVPN        1        1     2000   0       cust2
OtherVPNBurst   0        0     1000   0       cust2
```

VPN セッションの制限

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。

ASA のライセンスで 500 の SSL VPN セッションが許可されていて、AnyConnect 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)#
```

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

対称型マルチプロセッシング（SMP）プラットフォームでの暗号化コアの割り当てを変更して、AnyConnect TLS/DTLS トラフィックのスループットを向上させることができます。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。

暗号化コア再分散が利用できるのは、次のプラットフォームです。

- 5585-X
- 5545-X

- 5555-X
- ASASM

手順

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。

crypto engine accelerator-bias

- [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。

例：

```
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
```

アクティブな VPN セッションの表示

次のトピックでは、VPN セッション情報を表示する方法について説明します。

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。

- エンドポイントのパブリック 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。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 p-ipversion {v4 | v6}

- エンドポイントの割り当てられた 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。

show vpn-sessiondb anyconnect filter a-ipversion {v4 | v6}

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

```
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
```

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。

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 webvpn filter ipversion {v4 | v6}

例

```
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。

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。

show vpn-sessiondb l2l filter ipversion {v4 | v6}

ISE ポリシー適用について

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 アクセスとゲスト アクセスを提供し、個人所有デバイス持ち込み（BYOD）イニシアティブをサポートし、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）は、ASA によって確立された各 VPN セッションにアクセス コントロール リスト（ACL）を適用する必要はありません。

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

- IPSec
- AnyConnect
- L2TP/IPSec

（注） ダイナミック ACL（dACL）やセキュリティ グループ タグ（SGT）などの一部のポリシー要素はサポートされていますが、VLAN 割り当てや IP アドレス割り当てなどのポリシー要素はサポートされていません。

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 にポリシーの更新を送信します。これにより、ネットワーク アクセス権限を高める新しいユーザ ACL が識別されます。

（注） 後続の CoA 更新を介し、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。

ISE ポリシー適用に関する RADIUS サーバ グループの設定

ISE ポリシーの評価と適用をイネーブルにするには、ISE サーバの RADIUS AAA サーバ グループを設定し、サーバをグループに追加します。VPN にトンネル グループを設定する場合は、グループで AAA サービスにこのサーバ グループを指定します。

手順

ステップ 1 RADIUS AAA サーバ グループを作成します。

aaa-server *group_name***protocol radius**

```
hostname(config)# aaa-server servergroup1 protocol radius
hostname(config-aaa-server-group)#
```

ステップ 2 AAA サーバ グループの RADIUS 動的認可（CoA）サービスをイネーブルにします。

dynamic-authorization [**port** *number*]

ポートの指定は任意です。デフォルトは 1700 です。指定できる範囲は 1024 ～ 65535 です。

VPN トンネルでサーバ グループを使用すると、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 ポリシー更新用ポートをリッスンします。

```
hostname(config-aaa-server-group)# dynamic-authorization
```

ステップ 3 認証に ISE を使用しない場合は、RADIUS サーバ グループに対し認可専用モードを有効にします。

authorize-only

これは、サーバ グループを認可に使用するときに、RADIUS アクセス要求メッセージが、AAA サーバ用に設定されているパスワード方式に反して、「認可専用」要求として構築されることを示しています。RADIUS サーバの共通パスワードを **radius-common-pw** コマンドを使用して設定すると、そのパスワードは無視されます。

たとえば、認証にこのサーバ グループではなく証明書を使用する場合には、認可専用モードを使用します。VPN トンネルでの認可とアカウンティングにこのサーバ グループを使用する可能性があるからです。

```
hostname(config-aaa-server-group)# authorize-only
```

ステップ 4 RADIUS 中間アカウンティング アップデート メッセージの定期的な生成をイネーブルにします。

interim-accounting-update [**periodic** [*hours*]]

ISE は、ASA などの NAS デバイスから受信するアカウンティング レコードに基づいて、アクティブ セッションのディレクトリを保持します。ただし、セッションがアクティブであるとい

う通知（アカウンティング メッセージまたはポスチャ トランザクション）を 5 日間受信しなかった場合、ISE はデータベースからそのセッションのレコードを削除します。存続時間の長い VPN 接続が削除されないようにするには、すべてのアクティブ セッションについて ISE に定期的に中間アカウンティング更新メッセージを送信するように、グループを設定します。

- **periodic** [*hours*] 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。オプションで、これらの更新の送信間隔（時間単位）を含めることができます。デフォルトは 24 時間で、指定できる範囲は 1 ～ 120 時間です。
- （パラメータなし）。**periodic** キーワードなしでこのコマンドを使用すると、ASA 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ときにのみ中間アカウンティング更新メッセージを送信します。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。

```
hostname(config-aaa-server-group)# interim-accounting-update periodic 12
```

ステップ 5 （任意）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。

merge-dacl {**before-avpair** | **after-avpair**}

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 を結合するかどうかを決定します。ASA で設定されている ACL には適用されません。

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 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 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 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。

```
hostname(config)# aaa-server servergroup1 protocol radius
hostname(config-aaa-server-group)# merge-dacl before-avpair
```

ステップ 6 （任意）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。

max-failed-attempts *number*

範囲は、1 ～ 5 です。デフォルトは 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として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。

```
hostname(config-aaa-server-group)# max-failed-attempts 2
```

ステップ 7 （任意）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。

reactivation-mode {**depletion** [**deadtime** *minutes*] | **timed**}

それぞれの説明は次のとおりです。

- **depletion** [**deadtime** *minutes*] は、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でのみ、障害が発生したサーバを再アクティブ化します。これがデフォルトの再アクティブ化モードです。グループ内の最後のサーバがディセーブルになってから、その後すべてのサーバを再度イネーブルにするまでの時間を 0 ～ 1440 分の範囲で指定できます。デフォルトは 10 分です。
- **timed** 30 秒のダウン時間の後、障害が発生したサーバを再アクティブ化します。

```
hostname(config-aaa-server-group)# reactivation-mode deadtime 20
```

ステップ 8 （任意）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。

accounting-mode simultaneous

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。

```
hostname(config-aaa-server-group)# accounting-mode simultaneous
```

ステップ 9 グループに ISE RADIUS サーバを追加します。

aaa-server *group_name* [(*interface_name*)] **host** {*server_ip* | *name*} [*key*]

それぞれの説明は次のとおりです。

- *group_name* は、RADIUS サーバ グループの名前です。
- (*interface_name*) は、サーバが到達するために使用するインターフェイスの名前です。デフォルトは (inside) です。カッコは必須です。
- **host** {*server_ip* | *name*} は、ISE RADIUS サーバの IP アドレスまたはホスト名です。
- *key* は、接続を暗号化するためのオプション キーです。aaa-server-host モードに入った後で **key** コマンドを使用することで、このキーをより簡単に入力できます。キーを設定しないと、接続は暗号化されません（プレーン テキスト）。このキーは 127 文字までの英数字か

ら構成され、大文字と小文字の区別があり、RADIUS サーバ上のキーと同じ値になります。

グループには複数のサーバを追加できます。

```
hostname(config)# aaa-server servergroup1 (inside) host 10.1.1.3
hostname(config-aaa-server-host)# key sharedsecret
hostname(config-aaa-server-host)# exit
```

ISE ポリシーの適用の設定例

パスワードによる ISE ダイナミック認証のための VPN トンネルの設定

次の例は、ISE サーバ グループに、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を設定する方法を示しています。ISE によるパスワード認証を設定するトンネル グループ設定が含まれています。

```
ciscoasa(config)# aaa-server ise protocol radius
ciscoasa(config-aaa-server-group)# interim-accounting-update periodic 1
ciscoasa(config-aaa-server-group)# dynamic-authorization
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server ise (inside) host 10.1.1.3
ciscoasa(config-aaa-server-host)# key sharedsecret
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)# tunnel-group aaa-coa general-attributes
ciscoasa(config-tunnel-general)# address-pool vpn
ciscoasa(config-tunnel-general)# authentication-server-group ise
ciscoasa(config-tunnel-general)# accounting-server-group ise
ciscoasa(config-tunnel-general)# exit
```

ISE 認証のみの VPN トンネルの設定

次に、ISE で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。サーバ グループは認証用に使用されないため、authorize-only コマンドをサーバ グループ コンフィギュレーションに組み込みます。

```
ciscoasa(config)# aaa-server ise protocol radius
ciscoasa(config-aaa-server-group)# authorize-only
ciscoasa(config-aaa-server-group)# interim-accounting-update periodic 1
ciscoasa(config-aaa-server-group)# dynamic-authorization
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server ise (inside) host 10.1.1.3
ciscoasa(config-aaa-server-host)# key sharedsecret
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)# tunnel-group aaa-coa general-attributes
ciscoasa(config-tunnel-general)# address-pool vpn
ciscoasa(config-tunnel-general)# authentication certificate
ciscoasa(config-tunnel-general)# authorization-server-group ise
ciscoasa(config-tunnel-general)# accounting-server-group ise
```

```
ciscoasa(config-tunnel-general)# exit
```

ポリシーの適用の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
```

SSL の詳細設定

ASA は、Secure Sockets Layer（SSL）プロトコルと Transport Layer Security（TLS）を使用して、ASDM、クライアントレス SSL VPN、VPN、およびブラウザベースの各セッションのセキュアなメッセージ伝送を実現します。ASA が SSL ベースの VPN 接続と管理接続でサポートしているプロトコルは、SSLv3、TLSv1、TLSv1.1、および TLSv1.2 です。また、DTLS は AnyConnect VPN クライアントの接続に使用されます。

説明したように、次の暗号方式がサポートされています。

Cipher	TLSv1.1 / DTLS V1	TLSV1.2
AES128-GCM-SHA256	no	yes
AES128-SHA	yes	yes
AES128-SHA256	no	yes
AES256-GCM-SHA384	no	yes
AES256-SHA	yes	yes
AES256-SHA256	no	yes
DERS-CBC-SHA	no	no
DES-CBC-SHA	yes	yes
DHE-RSA-AES128-GCM-SHA256	no	yes
DHE-RSA-AES128-SHA	yes	yes
DHE-RSA-AES128-SHA256	no	yes
DHE-RSA-AES256-GCM-SHA384	no	l

Cipher	TLSv1.1 / DTLS V1	TLSV1.2
DHE-RSA-AES256-SHA	yes	yes
ECDHE-ECDSA-AES128-GCM-SHA256	no	yes
ECDHE-ECDSA-AES128-SHA256	no	yes
ECDHE-ECDSA-AES256-GCM-SHA384	no	yes
ECDHE-ECDSA-AES256-SHA384	no	yes
ECDHE-RSA-AES128-GCM-SHA256	yes	yes
ECDHE-RSA-AES128-SHA256	no	yes
ECDHE-RSA-AES256-GCM-SHA384	no	yes
ECDHE-RSA-AES256-SHA384	no	yes
NULL-SHA	no	no
RC4-MD5	no	no
RC4-SHA	no	no

（注） リリース 9.4（1）では、SSLv3 キーワードはすべて ASA 設定から削除されており、SSLv3 のサポートが ASA から削除されました。SSLv3 がイネーブルになっている場合は、SSLv3 オプションを指定したコマンドからブート時エラーが表示されます。ASA はデフォルトの TLSv1 に戻ります。

Citrix モバイル レシーバは TLS 1.1/1.2 プロトコルをサポートしていない可能性があります。互換性については、https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/citrix-receiver-feature-matrix.pdf を参照してください。

ASA が SSL/TLS 接続をネゴシエートする最小プロトコル バージョンを指定するには、次の手順を実行します。

手順

ステップ 1 ASA が接続をネゴシエートする最小プロトコル バージョンを設定します。

ssl server-version ［**tlsv1** | **tlsv1.1** | **tlsv1.2** ］

それぞれの説明は次のとおりです。

- **tlsv1**：SSLv2 クライアントの hello を受け入れ、TLSv1（以降）をネゴシエートするには、このキーワードを入力します。
- **tlsv1.1**：SSLv2 クライアントの hello を受け入れ、TLSv1.1（以降）をネゴシエートするには、このキーワードを入力します。

- **tlsv1.2** ：SSLv2 クライアントの hello を受け入れ、TLSv1.2（以降）をネゴシエートするには、このキーワードを入力します。

例：

例：

```
hostname(config)# ssl server-version tlsv1.1
```

ステップ 2 ASA がクライアントとして動作する場合に使用する SSL プロトコルおよび TLS プロトコルのバージョンを指定します。

```
ssl client-version [tlsv1 | tlsv1.1 | tlsv1.2]
```

```
hostname(config)# ssl client-version tlsv1
```

tlsv1 キーワードを指定すると、ASA は TLSv1 クライアントの hello を送信し、TLSv1 以上をネゴシエートします。tlsv1.1 キーワードを指定すると、ASA は TLSv1.1 クライアントの hello を送信し、TLSv1.1 以上をネゴシエートします。tlsv1.2 キーワードを指定すると、ASA は TLSv1.2 クライアントの hello を送信し、TLSv1.2 以上をネゴシエートします。（SSL クライアントロールに対して DTLS は使用不可）

ステップ 3 SSL、DTLS、および TLS プロトコルの暗号化アルゴリズムを指定します。

ssl cipher *version* [*level* | **custom** *string*

それぞれの説明は次のとおりです。

- *version* 引数は、SSL、DTLS、または TLS プロトコル バージョンを指定します。サポートされているバージョンは次のとおりです。
  - default：発信接続用の暗号セット。
  - dtlsv1：DTLSv1 着信接続用の暗号。
  - dtlsv1.2：DTLSv1.2 着信接続用の暗号。
  - tlsv1：TLSv1 着信接続用の暗号。
  - tlsv1.1：TLSv1.1 着信接続用の暗号。
  - tlsv1.2：TLSv1.2 着信接続用の暗号。
- *level* 引数は、暗号強度を指定し、設定されている暗号の最低レベルを示します。次に、強度の有効な値を強度の低い順に示します。
  - all：NULL-SHA を含むすべての暗号が含まれます。
  - low：NULL-SHA を除くすべての暗号が含まれます。
  - medium（これはすべてのプロトコルバージョンのデフォルト値です）：NULL-SHA、DES-CBC-SHA、および RC4-MD5 を除くすべての暗号が含まれます。

- fips：FIPS 準拠の暗号がすべて含まれます（NULL-SHA、DES-CBC-SHA、RC4-MD5、RC4-SHA、および DES-CBC3-SHA を除く）。
- high（TLSv1.2 にのみ適用）：SHA-2 暗号を使用する AES-256 のみが含まれます。

- **custom** *string* オプションを指定すると、OpenSSL 暗号定義文字列を使用して暗号スイートを詳細に管理できます。詳細については、https://www.openssl.org/docs/apps/ciphers.html を参照してください。

推奨設定は **medium** です。**high** を使用すると、接続が制限される場合があります。custom を使用すると、少数の暗号のみが設定されている場合は、機能が制限されることがあります。デフォルトのカスタム値を制限すると、クラスタリングを含めて発信接続が制限されることがあります。

ASA によってサポートされる暗号の優先順位は次のとおりです。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。

このコマンドは、バージョン 9.3(2) から廃止された ssl encryption コマンドに代わるものです。

ステップ 4 1 つのインターフェイスで複数のトラストポイントを可能にします。

ssl trust-point *name* [[**interface** *vpnlb-ip*] | **domain** *domain-name*]

```
hostname(config)# ssl trust-point www-cert domain www.example.com
```

name 引数は、トラストポイントの名前を指定します。**interface** 引数は、トラストポイントが設定されているインターフェイスの名前を指定します。vpnlb-ip キーワードは、インターフェイスにのみ適用され、このトラストポイントをこのインターフェイス上の VPN ロード バランシング クラスタの IP アドレスに関連付けます。**domain***domain-name* キーワードと引数のペアは、インターフェイスへのアクセスに使用される特定のドメイン名に関連付けられたトラストポイントを指定します。

インターフェイスあたり最大 16 個のトラストポイントを設定できます。

インターフェイスまたはドメインを指定しない場合は、トラストポイントが設定されていないすべてのインターフェイス用のフォールバック トラストポイントが作成されます。

ssl trustpoint ? コマンドを入力すると、使用可能な設定済みのトラストポイントが表示されます。**ssl trust-point** *name* **?** コマンド（たとえば、**ssl trust-point mysslcert ?**）を入力した場合、trustpoint-SSL 証明書アソシエーションに使用可能な設定済みのインターフェイスが表示されます。

このコマンドを使用するときは、次のガイドラインに従ってください。

- trustpoint の値は、**crypto ca trustpoint name** コマンドで設定された CA トラストポイントの name である必要があります。
- interface の値は、あらかじめ設定されたインターフェイスの nameif 名である必要があります。
- トラストポイントを削除すると、そのトラストポイントを参照する **ssl trust-point** エントリも削除されます。

- ssl trust-point エントリは、インターフェイスごとに 1 つと、インターフェイスを指定しないもの 1 つを保持できます。
- 同じトラストポイントを複数のエントリで再利用できます。
- domain キーワードで設定したトラストポイントは、複数のインターフェイスに適用されることがあります（接続方法によって異なります）。
- *domain-name* 値ごとに 1 つの **ssl trust-point** のみを保持できます。
- このコマンドを入力すると、次のエラーが表示される場合があります。

```
error:0B080074:x509 certificate routines:X509_check_private_key:key values
mismatch@x509_cmp.c:339
```

これは、ユーザが新しい証明書を設定して、以前に設定された証明書と置き換えたことを示しています。特に対処の必要はありません。

- 証明書は次の順序で選択されます。
  - 接続が **domain** キーワードの値に一致した場合、その証明書が最初に選択されます。（**ssl trust-point***name***domain***domain-name* コマンド）
  - ロードバランシングアドレスへの接続が確立された場合、vpnlb-ip 証明書が選択されます。（**ssl trust-point** *name* **interface** *vpnlb-ip* コマンド）
  - インターフェイスに対して設定された証明書。（**ssl trust-point** *name* interface コマンド）
  - インターフェイスに関連付けられていないデフォルトの証明書。（**ssl trust-point** *name*）
  - ASA の自己署名付き自己生成証明書。

ステップ 5 TLS の DHE-RSA 暗号方式で使用される DH グループを指定します。

```
ssl dh-group [group1 | group2 | group5 | group14 | group24]

hostname(config)# ssl dh-group group5
```

group1 キーワードは、DH グループ 1（768 ビット モジュラス）を設定します。group2 キーワードは、DH グループ 2（1024 ビット モジュラス）を設定します。group5 キーワードは、DH グループ 5（1536 ビット モジュラス）を設定します。group14 キーワードは、DH グループ 14（2048 ビット モジュラス、224 ビット素数位数サブグループ）を設定します。group24 キーワードは、DH グループ 24（2048 ビット モジュラス、256 ビット素数位数サブグループ）を設定します。

グループ 1 および 2 は、Java 7 およびそれ以前のバージョンと互換性があります。グループ 5、14、および 24 は、Java 7 と互換性がありません。すべてのグループが Java 8 と互換性があります。グループ 14 と 24 は FIPS 準拠です。デフォルト値は ssl dh-group group2 です。

ステップ 6 TLS の ECDHE-ECDSA 暗号方式で使用されるグループを指定します。

```
ssl ecdh-group [group19 | group20 | group21]

hostname(config)# ssl ecdh-group group20
```

group19 キーワードは、グループ 19（256 ビット EC）を設定します。group20 キーワードは、グループ 20（384 ビット EC）を設定します。group21 キーワードは、グループ 21（521 ビット EC）を設定します。

デフォルト値は ssl ecdh-group group19 です。

（注） 優先度が最も高いのは ECDSA 暗号および DHE 暗号です。

例

永続的 IPSec トンネル フロー

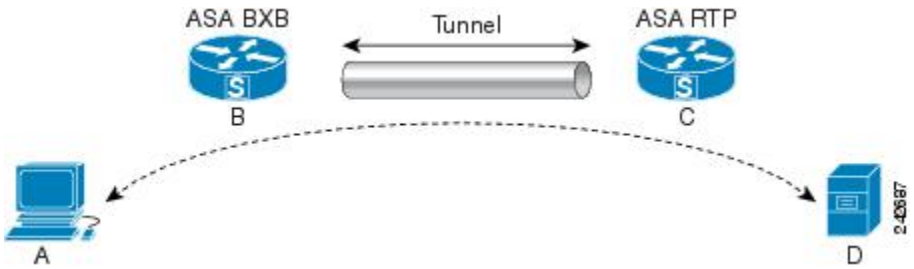
リリース 8.0.4 よりも前の ASA ソフトウェア バージョンを実行するネットワークでは、IPSec トンネルを通過する既存の IPsec LAN-to-LAN またはリモート アクセス TCP トラフィック フローは、トンネルがドロップするとドロップされます。これらのフローは、トンネルが元に戻ると、必要に応じて再作成されます。このポリシーは、リソース管理およびセキュリティの観点から有効です。ただし、このような動作がユーザ（特に PIX から ASA のみの環境に移行しているユーザ）およびレガシー TCP アプリケーション（容易に再起動しない、またはトンネルを頻繁にドロップするゲートウェイが含まれたネットワーク内にある）に問題を引き起こす場合があります（詳細については、CSCsj40681 および CSCsi47630 を参照してください）。

永続的な IPsec トンネル フロー機能で、この問題に対処します。この機能をイネーブルにすると、ASA はステートフル（TCP）トンネル フローを維持して再開します。他のすべてのフローは、トンネルがドロップしたときにドロップされ、新しいトンネルが設定されたときに再確立する必要があります。

（注） この機能は、ネットワーク拡張モードで実行されている IPsec LAN-to-LAN トンネルおよび IPsec リモート アクセス トンネルをサポートします。IPSec または AnyConnect/SSL VPN リモート アクセス トンネルはサポートしていません。

次に、永続的 IPSec トンネル フロー機能がどのように動作するかの例を示します。

図 *4:* ネットワーク シナリオ



この例では、BXB および RTP ネットワークが 1 対のセキュリティ アプライアンスによりセキュア LAN-to-LAN トンネルを介して接続しています。BXB ネットワークの PC は RTP ネットワークのサーバからセキュア トンネルを介して FTP 転送を実行しています。このシナリオでは、PC がサーバにログインし、転送を開始した後でトンネルが何らかの理由でドロップしたと想定しています。この時点でもデータは流れようとしているため、トンネルは再確立されていますが、FTP転送が完了しません。ユーザは、サーバにログインして転送を終了させ、もう一度やり直す必要があります。ただし、永続的 IPsec トンネル フローがイネーブルになっていれば、タイムアウト間隔以内にトンネルが再作成される限り、セキュリティ アプライアンスはこのフローの履歴（状態情報）を維持するため、データは新しいトンネルを通じて正常に流れ続けます。

シナリオ

次の項では、ドロップ後に復旧されたトンネルのデータ フローの状態を、永続的 IPsec トンネル フロー機能がディセーブルになっている場合と、この機能がイネーブルになっている場合の順に説明します。どちらの場合も、ネットワークのイラストについては前の図を参照してください。この図の場合：

- フロー B-C は、トンネルを定義し、暗号化された ESP データを伝送します。
- フロー A-D は、FTP 転送の TCP 接続で、フロー B-C で定義されたトンネルを通過します。このフローには、ファイアウォールで TCP/FTP フローを検査するときに使用される状態情報も含まれています。状態情報は重要であり、転送が進行するとファイアウォールによって継続的にアップデートされます。

（注） 各方向の逆フローは簡略化のため省略されています。

ディセーブル化された永続的な IPsec トンネル フロー

LAN-2-LAN トンネルがドロップすると、A-D フローと B-C フローの両方と、それらに属するすべての状態情報が削除されます。その後、トンネルが再確立され、フロー B-C が再作成され、トンネリングされたデータの伝送を再開できるようになります。ただし、TCP/FTP フロー A-D に問題が発生します。この時点までの FTP 転送のフローを説明する状態情報が削除されているため、ステートフル ファイアウォールは、インフライト FTP データをブロックし、A-D フローの作成を拒否します。今まで存在していたこのフロー履歴が失われると、ファイアウォー

ルは FTP 転送を迷子の TCP パケットとして処理し、ドロップします。これはデフォルトの動作です。

イネーブル化された永続的な IPsec トンネル フロー

永続的 IPsec トンネル フロー機能がイネーブルの場合、タイムアウト時間内にトンネルが再作成される限り、ASA は A-D フローの状態情報にアクセスできるため、データは正常に流れ続けます。

この機能がイネーブルの場合、ASA はフローを個別に処理します。つまり、B-C フローによって定義されたトンネルがドロップされても、A-D フローは削除されません。ASA はステートフル（TCP）トンネル フローを維持し、再開します。他のフローはすべてドロップされ、新しいトンネルで再確立される必要があります。これは、トンネル フローのセキュリティ ポリシーを弱めることはありません。ASA はトンネルがダウンしているときに A-D フローに到着するパケットをドロップするからです。

トンネル TCP フローはドロップされないため、クリーンアップは TCP タイムアウトに依存します。ただし、特定のトンネル フローのタイムアウトがディセーブルになってる場合、手動または他の方法（ピアからの TCP RST など）によってクリアされるまで、そのフローはシステム内で保持されます。

CLI を使用した永続的 IPsec トンネル フローの設定

設定例

永続的な IPsec トンネル フローのトラブルシューティング

show asp table コマンドと **show conn** コマンドは両方とも、永続的 IPsec トンネル フローの問題のトラブルシューティングに役立ちます。

永続的 IPsec トンネル フロー機能はイネーブルになっていますか?

特定のトンネルでこの機能がイネーブルになっているかを確認するには、**show asp table** コマンドを使用してトンネルに関連付けられた VPN コンテキストを調べます。show asp table vpn-context コマンドは、次の例に示すように（読みやすくするために太字を追加）、トンネルがドロップした後にステートフル フローを維持する各コンテキストに「+PRESERVE」フラグを表示します。

```
hostname(config)# show asp table vpn-context
VPN CTX=0x0005FF54, Ptr=0x6DE62DA0, DECR+ESP+PRESERVE, UP, pk=0000000000, rk=0000000000,
 gc=0
VPN CTX=0x0005B234, Ptr=0x6DE635E0, ENCR+ESP+PRESERVE, UP, pk=0000000000, rk=0000000000,
 gc=0

------------------------------------------------------------------------------

hostname(config)# show asp table vpn-context detail

VPN CTX  = 0x0005FF54
```

```
Peer IP  = ASA_Private
Pointer  = 0x6DE62DA0
State    = UP
Flags    = DECR+ESP+PRESERVE
SA       = 0x001659BF
SPI      = 0xB326496C
Group    = 0
Pkts     = 0
Bad Pkts = 0
Bad SPI  = 0
Spoof    = 0
Bad Crypto = 0
Rekey Pkt  = 0
Rekey Call = 0

VPN CTX  = 0x0005B234

Peer IP  = ASA_Private
Pointer  = 0x6DE635E0
State    = UP
Flags    = ENCR+ESP+PRESERVE
SA       = 0x0017988D
SPI      = 0x9AA50F43
Group    = 0
Pkts     = 0
Bad Pkts = 0
Bad SPI  = 0
Spoof    = 0
Bad Crypto = 0
Rekey Pkt  = 0
Rekey Call = 0
hostname(config)#
Configuration and Restrictions
This configuration option is subject to the same CLI configuration restrictions as other
 sysopt VPN CLI.
```

孤立したフローの検索

LAN-to-LANまたはネットワーク拡張モードトンネルがドロップし、タイムアウト前に復旧しなかった場合、孤立したトンネルフローが数多く発生することがあります。このようなフローはトンネルのダウンによって切断されませんが、これらのフローを介して通過を試みるすべてのデータがドロップされます。これらのフローを確認するには、**show conn** コマンドを次の例に示すように使用します（強調するため、およびユーザ入力を示すために太字を追加）。

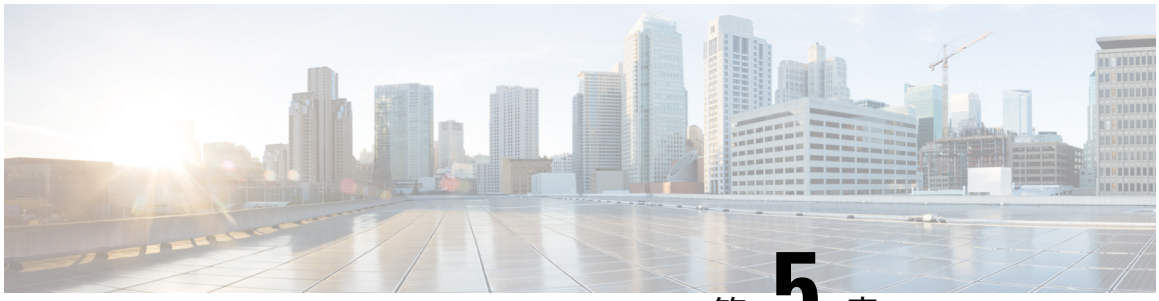
```
asa2(config)# show conn detail
9 in use, 14 most used
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
       B - initial SYN from outside, C - CTIQBE media, D - DNS, d - dump,
       E - outside back connection, F - outside FIN, f - inside FIN,
       G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data,
       i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
       k - Skinny media, M - SMTP data, m - SIP media, n - GUP
       O - outbound data, P - inside back connection, p - Phone-proxy TFTP connection,
       q - SQL*Net data, R - outside acknowledged FIN,
       R - UDP SUNRPC, r - inside acknowledged FIN, S - awaiting inside SYN,
       s - awaiting outside SYN, T - SIP, t - SIP transient, U - up,
       V - VPN orphan, W - WAAS,
       X - inspected by service module
```

次の例に、**show conn** コマンドの出力例を示します。**V** フラグで示されているとおり、孤立したフローが存在します。

```
hostname# show conn
16 in use, 19 most used
TCP out 192.168.110.251:7393 in 192.168.150.252:21 idle 0:00:00 bytes 1048 flags UOVB
TCP out 192.168.110.251:21137 in 192.168.150.252:21 idle bytes 1048 flags UIOB
```

孤立したフローがあるこのような接続へのレポートを制限するには、次の例で示すように、**show conn state** コマンドに **vpn_orphan** オプションを追加します。

```
hostname# show conn state vpn_orphan
14 in use, 19 most used
TCP out 192.168.110.251:7393 in 192.168.150.252:5013 idle 0:00:00 bytes 2841019 flags
UOVB
```



第 5 章

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。

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。

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。

（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（DefaultL2Lgroup）、IKEv2 VPN 用のデフォルトのリモート アクセス接続プロファイル（DefaultRAgroup）、クライアントレス SSL および AnyConnect SSL 接続用のデフォルトの接続プロファイル（DefaultWEBVPNgroup）、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、一般的操作用コンフィギュレーション ガイドの第 20 章「Objects」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. Dynamic Access Policy（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 レコードには存在しないため、セキュリティ アプライアンスは適用する値を見つけるために、ユーザ名および必要に応じてグローバル ポリシーの AAA 属性に移動して検索します。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、IPSEC リモート アクセス接続用の DefaultRAgroup、および SSL VPN（ブラウザベースおよび Anyconnect Client 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。
- 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。

  領域は @ 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 はユーザ名およびグループ（ある場合）を認証に使用します。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る場合、およびリモート 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できます。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 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（163 ページ） 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。

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。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

次の表は、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 （136 ページ） 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」が「トンネル グループ」と呼ばれていました。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、この 2 つの用語が同義的によく使用されています。

表 *5 : SSL VPN* 用接続プロファイルの属性

	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。 AnyConnect クライアント接続にグループ URL を使用するロード バランシング展開では、クラスタ内の各 ASA ノードで、ノードのロード バランシングのパブリック アドレスのグループ URL と同様に、仮想クラスタ アドレスのグループ URL を設定する必要があります。
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。

	機能
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


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 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

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。

- 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）

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 （120 ページ）.
- リモート アクセス接続プロファイルの一般属性の設定 （121 ページ）.
- 二重認証の設定 （126 ページ）
- リモート アクセス接続プロファイルの IPSec IKEv1 属性の設定 （128 ページ）.
- IPSec リモート アクセス接続プロファイルの PPP 属性の設定 （130 ページ）

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

手順

	コマンドまたはアクション	目的
ステップ 1	**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。 **例：**	リモート アクセス トンネルの場合、タイプは **remote-access** です。 **tunnel-group** *tunnel_group_name* **type remote-access**

	コマンドまたはアクション	目的

	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。

手順

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-groupFinGroup
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』ガイドの 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 つのアクセス コントロール サーバを設定します。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領域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 が、サーバ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 で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（154 ページ）を参照してください。

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。

（注） 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 サーバとのみ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

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。

手順

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 に指示できます。

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 | 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 client
hostname(config-tunnel-general)# secondary-pre-fill-username 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。デフォルト値はプライマリです。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。

手順

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る場合、およびリモート 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。

手順

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（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 （133 ページ）
- LAN-to-LAN 接続プロファイルの一般属性の設定 （133 ページ）
- LAN-to-LAN IPSec IKEv1 属性の設定 （134 ページ）

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
 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。

手順

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。

tunnel-group *tunnel-group-name* **general-attributes**

例：

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)#
```

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。

ステップ 2 デフォルト グループ ポリシーの名前を指定します。

default-group-policy *policyname*

例：

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。

手順

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る場合、およびリモート 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 （136 ページ）
- 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 （140 ページ）

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。

手順

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、VPN の IP アドレス （223 ページ） 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 が、サーバ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 で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 （154 ページ）を参照してください。

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。

手順

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)#
```

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] [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 アドレスを指定します。

group-url *url*[**enable** | **disable**]

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。*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。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。各 URL またはアドレスは、個別にイネーブル（デフォルト）またはディセーブルにできます。

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 リストが表示され、ユーザは選択を行う必要があります。

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。

例：

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 （146 ページ）を参照してください。

AnyConnect クライアント接続にグループ URL を使用するロード バランシング展開では、クラスタ内の各 ASA ノードで、ノードのロード バランシングのパブリック アドレスのグループ URL と同様に、仮想クラスタ アドレスのグループ URL を設定する必要があります。

例：

次のようなアドレスが設定されているクラスタ内での 2 つの ASA ノードを使用したロード バランシング展開に適した group-url を設定します。

- ロード バランシングの仮想 IP = https://vip-vpn.example.com/groupname
- ASA1 = https://asa1.example.com/groupname
- ASA2 = https://asa2.example.com/groupname

ASA1 のトンネルグループ設定では、次の group-url が設定されている必要があります。

```
hostname(config)# tunnel-group LB1 type webvpn
hostname(config)# tunnel-group LB1 general-attributes
hostname(config-tunnel-general)# group-url  https://vip-vpn.example.com/groupname
hostname(config-tunnel-general)# group-url  https://asa1.example.com/groupname
```

ASA2 のトンネルグループ設定では、次の group-url が設定されている必要があります。

```
hostname(config)# tunnel-group LB2 type webvpn
hostname(config)# tunnel-group LB2 general-attributes
hostname(config-tunnel-general)# group-url  https://vip-vpn.example.com/groupname
```

```
hostname(config-tunnel-general)# group-url  https://asa2.example.com/groupname
```

ステップ 6 （任意）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 の Hostscan アプリケーション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 [anyconnect]
hostname(config-tunnel-webvpn)#
```

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。

この免除を AnyConnect 接続のみに制限する場合は、**anyconnect** キーワードを含めます。キーワードを含めないと、この免除はクライアントレス接続、レイヤ 3 接続、および AnyConnect 接続に適用されます。

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 （任意） 認証と認可で使用するクライアント証明書から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 **pre-fill-username** コマンドを使用します。

```
hostname(config)# pre-fill-username {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。証明書機能からこの事前充填ユーザ名を使用するには、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 client
hostname(config-tunnel-webvpn)#
```

ステップ 9 認証または許可を目的としたクライアント証明書からのセカンダリ ユーザ名の抽出を有効にするには、tunnel-group webvpn-attributes モード内で **secondary-pre-fill-username** コマンドを使用します。

```
hostname(config)# secondary-pre-fill-username {client | clientless}
```

ステップ 10 （任意） 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 11 （任意） 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)#
```

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。

手順

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、クライアントレス SSL VPN の概要 （333 ページ） 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。

標準ベースの IKEv2 クライアントのトンネル グループについて

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。

IPSec リモートアクセスのデフォルト トンネル グループは DefaultRAGroup です。デフォルト トンネル グループは、変更することはできますが、削除することはできません。

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または EAP 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、または EAP）。

DefaultRAGroup は EAP 認証用に設定する必要があります。これは、証明書認証が証明書 DN 照合に使用されていなければ、これらのクライアント接続を特定のトンネル グループにマッピングすることができないためです。

標準ベースの IKEv2 属性のサポート

ASA では、次の IKEv2 属性がサポートされます。

- INTERNAL_IP4_ADDRESS/INTERNAL_IP6_ADDRESS：IPv4 または IPv6 アドレス

（注） デュアル スタック（IPv4 と IPv6 の両方のアドレス割り当て）は、IKEv2 ではサポートされません。IPv4 アドレスと IPv6 アドレスの両方が要求され、両方のアドレスが割り当て可能な場合は、IPv4 アドレスのみが割り当てられます。

- INTERNAL_IP4_NETMASK：IPv4 アドレス ネットワーク マスク
- INTERNAL_IP4_DNS/INTERNAL_IP6_DNS：プライマリ/セカンダリ DNS アドレス
- INTERNAL_IP4_NBNS：プライマリ/セカンダリ WINS アドレス
- INTERNAL_IP4_SUBNET/INTERNAL_IP6_SUBNET：スプリット トンネリングのリスト
- APPLICATION_VERSION：無視されます。セキュリティ上の理由から、ASA のバージョン情報を伝達しないように応答は送信されません。ただし、クライアント設定ペイロード要求にこの属性を含めることができ、文字列が ASA の **vpn-sessiondb** コマンド出力と syslog に表示されます。

DAP のサポート

接続タイプごとの DAP ポリシー設定を許可するには、新しいクライアント タイプの IPsec-IKEv2-Generic-RA を使用してこの接続タイプに特定のポリシーを適用することができます。

リモート アクセス クライアントのトンネル グループ選択

次の表に、リモート アクセス クライアントと使用可能なトンネル グループ オプションのリストを示します。

リモート アクセス クライアント	トンネル グループ リスト	グループ URL	証明書 DN 照合	Default Group (DefaultRAGroup)	Other
AnyConnect VPN クライアント	Yes	Yes	Yes	Yes	該当なし
Windows L2TP/IPsec（メイン モード IKEv1）	No	No	• Yes（ローカル マシンの証明書を使用する場合） • No（PSK を使用する場合）	Yes	該当なし
標準ベースの IKEv2	No	No	• Yes（ローカル マシンの証明書を使用する場合） • No（EAP 認証を使用する場合）	Yes （注） DefaultRAGroup トンネル グループを使用する必要があります。	該当なし

標準ベースの IKEv2 クライアントの認証サポート

次の表に、標準ベースの IKEv2 クライアントとサポートされている認証方式のリストを示します。

（注） 認証方式の制限は、ASA 上ではなく、クライアント上のサポートの有無に基づきます。すべての EAP 方式の認証は、クライアントと EAP サーバ間で ASA によってプロキシされます。EAP 方式のサポートは、クライアントと EAP サーバの EAP 方式のサポートに基づきます。

クライアントタイプ/認証方式	EAP-TLS	EAP-MSCHAPv2	EAP-MD5	証明書のみ	PSK
Linux 上の StrongSwan	該当なし	• ISE：対応 • ACS：対応 • FreeRadius：対応 • FreeRadius 経由の AD：対応	• ISE：対応 • ACS：対応 • FreeRadius：対応 • FreeRadius 経由の AD：対応	Yes	Yes
Android 上の StrongSwan	該当なし	• ISE：対応 • ACS：対応 • FreeRadius：対応 • FreeRadius 経由の AD：対応	なし	Yes	該当なし
Windows 7/8/8.1	• ISE：対応 • ACS：対応 • FreeRadius：対応 • FreeRadius 経由の AD：対応	• ISE：対応 • ACS：対応 • FreeRadius：対応 • FreeRadius 経由の AD：対応	該当なし	Yes	該当なし

クライアント タイプ/認証方式	EAP-TLS	EAP-MSCHAPv2	EAP-MD5	証明書のみ	PSK
Windows Phone	• ISE：対応 • ACS：対応 • FreeRadius：対応 • FreeRadius 経由の AD：対応	• ISE：対応 • ACS：対応 • FreeRadius：対応 • FreeRadius 経由の AD：対応	該当なし	該当なし	該当なし
Samsung Knox	該当なし	• ISE：対応 • ACS：対応 • FreeRadius：対応 • FreeRadius 経由の AD：対応	• ISE：対応 • ACS：対応 • FreeRadius：対応 • FreeRadius 経由の AD：対応	Yes	該当なし
iOS 8	• ISE：対応 • ACS：対応 • FreeRadius：対応 • FreeRadius 経由の AD：対応	• ISE：対応 • ACS：対応 • FreeRadius：対応 • FreeRadius 経由の AD：対応	該当なし	Yes	Yes
Android ネイティブ クライアント	該当なし	• ISE：対応 • ACS：対応 • FreeRadius：対応 • FreeRadius 経由の AD：対応	該当なし	Yes	Yes

複数証明書認証の追加

マルチ証明書認証のプロトコル交換を定義し、これを両方のセッションタイプで利用できるように、集約認証プロトコルが拡張されました。クライアントがSSL接続を行なって集約認証を開始すると、別の SSL 接続が行なわれ、ASA は、クライアントが証明書認証を必要としクライアント証明書を要求していることを確認します。

ASA は、リモート アクセス タイプのトンネル グループの AnyConnect 接続に必要な認証を設定します。トンネルグループ マッピングは、証明書ルール マッピング、group-url などの既存の方法で実行されますが、必要な認証方法はクライアントとネゴシエートされます。

例

tunnel-group <name> webvpn-attributes

authentication {{aaa {certificate | multiple-certificate})| saml}

認証オプションは、AAA のみ、証明書のみ、複数証明書のみ、AAA と証明書、AAA と複数証明書、および SAML です。

```
ASA(config)# tunnel-group AnyConnect webvpn-attributes
ASA(config-tunnel-webvpn)# authentication?
tunnel-group-webvpn mode commands/options:
aaa         Use username and password for authentication
certificate Use certificate for authentication
multiple-certificate Use multiple certificates for authentication
saml   Use SAML for authentication
ASA(config-tunnel-webvpn)# authentication multiple-certificate?

tunnel-group-webvpn mode commands/options:
aaa  Use username and password for authentication
<cr>

ASA(config-tunnel-webvpn)# authentication aaa?

tunnel-group-webvpn mode commands/options:
certificate Use certificate for authentication
multiple-certificate Use multiple certificates for authentication
<cr>
```

EAP ID を取得するためのクエリ ID オプションの設定

Microsoft Windows 7 IKEv2 クライアントは、Cisco ASA サーバがトンネル グループ検索に使用できないようにするために、IP アドレスをインターネット キー交換（IKE）ID として送信します。ASA は、ASA がクライアントから有効な EAP ID を取得できるように、EAP 認証用の **query-identity** オプションを使用して設定する必要があります。

証明書ベースの認証の場合は、次のように、ASA サーバと Microsoft Windows 7 クライアントの証明書に拡張キー使用法（EKU）フィールドが含まれている必要があります。

- クライアント証明書では、EKU フィールド = クライアント認証証明書です。
- サーバ証明書では、EKU フィールド = サーバ認証証明書です。

証明書は、Microsoft Certificate Server またはその他の CA サーバから取得できます。

EAP 認証の場合は、Microsoft Windows 7 IKEv2 クライアントが他の EAP 要求の前に EAP ID 要求を待ちます。クライアントに EAP ID 要求を送信するには、IKEv2 ASA サーバ上のトンネル グループ プロファイル内で **query-identity** キーワードが設定されていることを確認してください。

（注） Windows でスプリット トンネリングが実行できるように IKEv2 では DHCP 代行受信がサポートされます。この機能は、IPv4 スプリット トンネリング属性でのみ動作します。

手順

ステップ 1 接続タイプを IPsec リモート アクセスに設定するには、 **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。

次の例では、IKEv2 事前共有キーが 44kkaol59636jnfx に設定されます。

```
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 2 標準ベースのサードパーティ IKEv2 リモート アクセス クライアントを使用したユーザ認証をサポートする方式として拡張認証プロトコル（EAP）を指定するには、**ikev2 remote-authentication eap** [**query-identity**] コマンドを使用します。

（注） リモート認証で EAP をイネーブルにするには、証明書を使用してローカル認証を設定し、**ikev2 local-authentication** {**certificate** *trustpoint*} コマンドを使用して有効なトラストポイントを設定する必要があります。そうしなかった場合は、EAP認証要求が拒否されます。

クライアントが、リモート認証用に設定されたオプションのすべてではなく、一部を使用できるようにする複数のオプションがあります。

IKEv2接続の場合、トンネル グループのマッピングで、リモート認証に使用できる認証方式（PSK、証明書、およびEAP）とローカル認証に使用できる認証方式（PSKおよび証明書）、およびローカル認証で使用するトラストポイントを特定する必要があります。現在、マッピングの実行には、ピアまたはピア証明書のフィールドの値から取得（証明書マップを使用）された IKE ID が使用されます。両方のオプションが失敗した場合は、着信接続がデフォルトのリモート アクセス トンネル グループ DefaultRAGroup にマッピングされます。証明書マップは、リモート ピアが証明書で認証された場合にのみ適用されるオプションです。このマップにより、異なるトンネル グループへのマッピングが可能です。証明書認証の場合のみ、ルールまたはデフォルトの設定を使用してトンネル グループの参照が行われます。EAP 認証および PSK 認証の場合は、クライアント（トンネル グループ名が一致するクライアント）の IKE ID またはデフォルトの設定を使用してトンネル グループの参照が行われます。

EAP 認証で、クライアントが IKE ID とユーザ名を個別に設定できない場合は、DefaultRAGroup トンネル グループを使用する必要があります。

次の例では、EAP 認証要求が拒否されています。

```
ciscoasa(config-tunnel-ipsec)# ikev2 remote-authentication eap query-identity
ciscoasa(config-tunnel-ipsec)# ikev2 remote-authentication certificate
ciscoasa(config-tunnel-ipsec)# ikev2 local-authentication pre-shared-key 12345678
ERROR: The local-authentication method is required to be certificate based
if remote-authentication allows EAP
ciscoasa(config-tunnel-ipsec)# ikev2 local-authentication certificate myIDcert
```

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** または **show crypto ipsec sa** コマンドを使用します。

パスワード管理用の Microsoft Active Directory の設定

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 が、サーバ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 で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 の用語に言及しています。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。

手順

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 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。

このユーザが次回ログインするときに、ASA で次のプロンプトが表示されます「New password required.Password change required.You must enter a new password with a minimum length *n* to continue.」最小必須パスワード長 *n* は、[Start] > [Programs] > [Administrative Tools] > [Domain Security Policy] > [Windows Settings] > [Security Settings] > [Account Policies] > [Password Policy] で Active Directory 設定の一部として設定できます。[Minimum password length] 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。

（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。

手順

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。

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。

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。

手順

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。

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。

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。

手順

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、[Enable] を選択します。

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。

（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。

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、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。このメッセージ テキストは、ASA が SDI サーバと直接通信している場合と RADIUS プロキシを経由して通信している場合とで異なります。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（157 ページ） 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。

手順

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。

例：

```
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。

次の表に、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照合します。

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。

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
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 のテキストを変更します。

```
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"
```

Group Policies

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。

- Identity
- 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
- Filters
- 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 ポリシーの変更

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。コマンドの構文は、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

  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、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 で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 を設定した場合、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。したがって、外部グループは、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にすぎません。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、適切な ASA 認可属性を指定してサーバを設定し、それらの属性のサブセットから個々のユーザに対する特定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、VPN の外部 AAA サーバの設定 （317 ページ） の説明に従ってください。

手順

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 名とパスワードとともにグループ 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 ポリシーが作成します。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） VPN の外部 AAA サーバの設定 （317 ページ） 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 （164 ページ）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 500 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。

VPN リモート クライアントでのログイン後に表示される全体的なバナーの長さは、ASA バージョン 9.5.1 で 510 ～ 4000 文字に増加しました。

（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** 形式を使用すると、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

始める前に

IPv4 アドレス プールを作成します。

手順

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

group-policy *value***attributes**

例：

```
hostname> en
hostname# config t
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)#
```

ステップ 2 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。

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)#
```

ステップ 3 （任意） 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。

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)#
```

ステップ 4 （任意） **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。

```
hostname(config-group-policy)# address-pools none
hostname(config-group-policy)#
```

ステップ 5 （任意） **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。

```
hostname(config-group-policy)# no address-pools none
hostname(config-group-policy)#
```

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

始める前に

IPv6 アドレス プールを作成します。VPN の IP アドレス （223 ページ）を参照してください。

手順

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

group-policy *value***attributes**

例：

```
hostname> en
hostname# config t
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)#
```

ステップ 2 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。

例：

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。

```
hostname(config-group-policy)# ipv6-address-pools value ipv6-pool1 ipv6-pool2 ipv6-pool3
hostname(config-group-policy)#
```

ステップ 3 （任意） 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。

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)#
```

ステップ 4 （任意） この属性が DfltGrpPolicy など他のポリシーのソースから継承されないようにするには、**ipv6-address-pools none** コマンドを使用します。

```
hostname(config-group-policy)# ipv6-address-pools none
hostname(config-group-policy)#
```

ステップ 5 （任意） **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）に戻すには、**no ipv6-address pools none** コマンドを使用します。

```
hostname(config-group-policy)# no ipv6-address-pools none
hostname(config-group-policy)#
```

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には次のものがあります。

- 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 ルールの適用

フィルタは複数のルールから構成されています。これらのルールは、ASA を介して着信したトンネリング データ パケットを許可するか拒否するかを、送信元アドレス、宛先アドレス、プロトコルなどに基づいて決定します。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。

（注） IPv6 を使用して VLAN マッピングを実行する場合、復号化されたトラフィックが内部ネットワークにルーティングされるようにするために、外部（宛先）アドレスは VLAN ごとに固有にする必要があります。異なる VLAN およびルート メトリックに対して同じ宛先ネットワークを使用することはできません。

- 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。

  [**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、一般的操作用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 ポリシーの VPN アクセス時間の指定

始める前に

時間の範囲を作成します。一般的操作用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

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

group-policy *value***attributes**

例：

```
hostname> en
hostname# config t
hostname(config)# group-policy FirstGroup attributes
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 **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。

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** *integer* 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。

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。一致していない場合、ASA はユーザが接続できないようにします。グループロックを設定しない場合、ASA は、割り当てられたグループとは関係なく、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

手順

ステップ 1 （任意）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** {*minutes* コマンドを使用して、VPN 接続の最大時間を設定します。

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。

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)#
```

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
hostname(config-username)#
```

[**no**] **vpn-session-timeout** {*minutes* | **none**} コマンドを使用したその他のアクションは次のとおりです。

- このポリシーから属性を削除し、継承を許可するには、このコマンドの **no vpn-session-timeout** 形式を入力します。
- 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、**vpn-session-timeout none** を入力します。

ステップ 2 **vpn-session-timeout alert-interval** {*minutes* | } 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指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
```

[**no**] **vpn-session-timeout alert-interval** {*minutes* | **none**} コマンドを使用したその他のアクションは次のとおりです。

- 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。

  ```
  hostname(config-webvpn)# no vpn-session-timeout alert-interval
  ```

- **vpn-session-timeout alert-interval none** は、ユーザがアラートを受信しないことを示します。

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

手順

ステップ 1 （任意） VPN アイドル タイムアウト期間を設定するには、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** *minutes* コマンドを使用します。

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。最小時間は 1 分、最大時間は 35791394 分であり、デフォルトは 30 分です。

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)#
```

[**no**] **vpn-idle-timeout** {*minutes* | **none**} コマンドを使用したその他のアクションは次のとおりです。

- VPN アイドル タイムアウトを無効にし、タイムアウト値を継承しないようにするには、**vpn-idle-timeout none** を入力します。

  ```
  hostname(config)# group-policy FirstGroup attributes
  hostname(config-group-policy)# vpn-idle-timeout none
  hostname(config-group-policy)#
  ```

これにより、AnyConnect（SSL と IPsec/IKEv2 の両方）およびクライアントレス VPN がグローバル webvpn **default-idle-timeout** *seconds* 値を使用するようになります。このコマンドは、webvpn コンフィギュレーション モードで入力します。たとえば、`hostnamee(config-webvpn)# default-idle-timeout 300` のように入力します。デフォルトは 1800 秒（30 分）で、範囲は 60 ～ 86400 秒です。

すべての webvon 接続の場合、**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。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。

サイト間（IKEv1、IKEv2）および IKEv1 リモート アクセス VPN の場合は、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することを推奨します。

- このグループ ポリシーまたはユーザ ポリシーのアイドル タイムアウトを無効にするには、**no vpn-idle-timeout** を入力します。値は継承されます。
- **vpn-idle-timeout** をまったく設定しない場合、値は継承されます。デフォルトは 30 分です。

ステップ 2 （任意） オプションで、**vpn-idle-timeout alert-interval** {*minutes*} 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できます。

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。デフォルトのアラート間隔は 1 分です。

次の例は、anyuser という名前のユーザに 3 分の VPN アイドル タイムアウト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 alert-interval 3
hostname(config-username)#
```

[no] vpn-idle-timeout alert-interval {*minutes* | **none**} コマンドを使用したその他のアクションは次のとおりです。

- **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。

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-idle-timeout none
hostname(config-username)#
```

- このグループまたはユーザ ポリシーのアラート間隔を削除するには、**no vpn-idle-timeout alert-interval** を入力します。値は継承されます。
- このパラメータをまったく設定しない場合、デフォルトのアラート間隔は 1 分です。

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。

手順

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（任意）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**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（任意）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。DNS サーバ アドレスは最大 4 つ、IPv4 アドレスと IPv6 アドレスで 2 つずつ指定できます。

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 **DefaultDNS 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
```

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。

split-tunnel-policy {**tunnelall** | **tunnelspecified** | **excludespecified**}

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。

ipv6-split-tunnel-policy {**tunnelall** | **tunnelspecified** | **excludespecified**}

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。

- **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。

（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 リスト内のネットワークは、クライアントで無視されます。

- **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。

例

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。

```
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ネットワーク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。

（注） 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 ドメイン名を識別します。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、**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 代行受信によって、Microsoft Windows XP クライアントは ASA でスプリット トンネリングを使用できるようになります。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
```

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。

手順

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、クライアント デバイスのブラウザでプロキシ サーバの設定を指定していません。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 **no-modify** 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)#
```

使用できる方法は、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—**このクライアントデバイスでは、ブラウザの HTTP プロキシ設定をディセーブルにします。
- **use-server—msie-proxy server** コマンドで設定されている値を使用するには、ブラウザで HTTP プロキシ サーバを設定します。

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または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)#
```

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。

手順

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、パスワードの保管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、対話的なハードウェア クライアント認証やハードウェア クライアントの個別ユーザ認証には適用されません。

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。

ヒント 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)#
```

完全秘密転送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。

完全秘密転送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、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。

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

手順

ステップ 1 （任意） 次のコマンドを使用して、ネットワーク拡張モードを設定します。

[**no**] **nem** [**enable** | **disable**]

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。PAT は適用されません。したがって、Easy VPN サーバの背後にあるデバイスは、Easy VPN リモートの背後にあるプライベート ネットワーク上のデバイスに、トンネルを介して（トンネルを介してのみ）直接アクセスできます。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。

例：

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
```

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 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。

ステップ 2 （任意） 次のコマンドを使用して、セキュア ユニット認証を設定します。

[**no**] **secure-unit-authentication** [**enable** | **disable**]

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 クライアントは保存されているユーザ名とパスワードを使用しません（設定されている場合）。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。

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、どのバックアップ サーバにもセキュア ユニット認証を設定する必要があります。

（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。

例：

次の例は、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方法を示しています。

```
hostname(config)#group-policy FirstGroup attributes
hostname(config-group-policy)# secure-unit-authentication enable
```

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。

ステップ 3 （任意） 次のコマンドを使用して、ユーザ認証を設定します。

[**no**] **user-authentication** [**enable** | **disable**]

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。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。

プライマリ ASA でユーザ認証が必要な場合は、どのバックアップ サーバにもユーザ認証を設定する必要があります。

例：

次の例は、FirstGroup という名前のグループ ポリシーに対して、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
```

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。

ステップ 4 次のコマンドを使用して、認証した個々のユーザのアイドル タイムアウトを設定します。

[**no**] **user-authentication-idle-timeout** *minutes* | **none**]

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させます。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。

例：

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 enable
hostname(config-group-policy)#user-authentication-idle-timeout 45
```

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。ヌル値を設定すると、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。

（注） **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。

ステップ 5 次のコマンドを使用して、IP Phone Bypass を設定します。

ip-phone-bypass enable

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。これは、IUA がイネーブルになっている場合にのみ適用されます。

（注） また、これらのクライアントの認証を免除するには、クライアントに MAC アドレス免除を設定する必要があります。

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。このオプションにより、別のグループ ポリシーから IP Phone Bypass の値を継承できます。

ステップ 6 次のコマンドを使用して、LEAP Bypass を設定します。

leap-bypass enable

LEAP Bypass は、**user-authentication** がイネーブルになっている場合にのみ適用されます。このコマンドにより、Cisco ワイヤレス アクセス ポイント デバイスからの LEAP パケットは、

LEAP 認証を確立してから、ユーザ認証ごとに認証を実行できるようになります。LEAP Bypass は、デフォルトでディセーブルになっています。

ハードウェア クライアントの後ろにいる LEAP ユーザには、面倒な問題があります。トンネルで中央サイト デバイスの後ろにある RADIUS サーバにクレデンシャルを送信することができないため、LEAP 認証をネゴシエートできません。トンネル経由でクレデンシャルを送信できない理由は、無線ネットワークで認証されていないためです。この問題を解決するために、LEAP バイパスは、個別のユーザ認証の前に LEAP パケット（LEAP パケットだけ）をトンネルで転送し、RADIUS サーバへの無線接続を認証できるようにします。これによって、ユーザは、個別のユーザ認証に進むことができます。

LEAP Bypass は、次の条件下で適切に機能します。

- **secure-unit-authentication** がディセーブルになっていること。インタラクティブ ユニット認証がイネーブルの場合、トンネルを使用して LEAP デバイスが接続できるようになる前に、非 LEAP（有線）デバイスがハードウェア クライアントを認証する必要があります。
- **user-authentication** がイネーブルになっていること。イネーブルになっていないと、LEAP Bypass が適用されません。
- 無線環境のアクセス ポイントが、Cisco Discovery Protocol（CDP）を実行している Cisco Aironet Access Point であること。PC の NIC カードは、他のブランドの製品でもかまいません。

例：

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)# user-authentication enable
hostname(config-group-policy)# leap-bypass enable
```

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 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。

AnyConnect Secure Mobility Client 接続のグループ ポリシー属性の設定

AnyConnect VPN Client 接続 （261 ページ）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。

手順

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** キーワードを指定して 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 デッドピア検出の設定 （280 ページ）

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、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。これを行うには、次を使用してキープアライブ メッセージの頻度を調整します。
anyconnect ssl keepalive command:

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、使用可能な場合は常に、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。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**} or **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)#
```

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、バックアップ サーバ ポリシーがグループ内のクライアントにプッシュされ、クライアント上のバックアップ サーバ リスト（設定されている場合）が置き換わります。

（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 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なしの認証が終わると、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。

手順

ステップ 1 （任意） 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。このタイマーの期限が切れると、ホストのポスチャの変更を調べるクエリー（ステータス クエリー）が発行されます。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、継承元の代替グループ 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アクセス コントロール サーバ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、継承元の代替グループ 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 用デフォルト 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、継承元の代替グループ 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 を適用します。
- **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、継承元の代替グループ 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。

[Client Firewall] タブの [Add or Edit Group Policy] ダイアログボックスでは、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と認識します）。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 ポリシーとして指定します。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。

始める前に

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。

手順

ステップ 1 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。

webvpn

例：

```
hostname(config)# group-policy ac-client-group attributes
hostname(config-group-policy)# webvpn
```

ステップ 2 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 インターフェイスに適用されるルールです。

anyconnect firewall-rule client-interface {private | public} value *[RuleName]*

```
hostname(config-group-webvpn)# anyconnect firewall-rule client-interface private value
ClientFWRule
```

ステップ 3 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。

show runn group-policy [value]

例：

```
hostname(config-group-webvpn)# show run group-policy FirstGroup
group-policy FirstGroup internal
group-policy FirstGroup attributes
webvpn
  anyconnect firewall-rule client-interface private value ClientFWRule
```

ステップ 4 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。

no anyconnect firewall-rule client-interface private value [*RuleName*]

例：

```
hostname(config-group-webvpn)# no anyconnect firewall-rule client-interface private value

hostname(config-group-webvpn)#
```

Zone Labs Integrity サーバの使用

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。

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 サーバを設定するには、次の手順を実行します。

手順

ステップ 1 IP アドレス 10.0.0.5 を使用して Integrity サーバを設定します。

```
zonelabs-Integrity server-address {hostname1 | ip-address1}
```

例：

```
hostname(config)# zonelabs-Integrity server-address 10.0.0.5
```

ステップ 2 ポート 300 を指定します（デフォルト ポートは 5054 です）。

```
zonelabs-integrity port port-number
```

例：

```
hostname(config)# zonelabs-integrity port 300
```

ステップ 3 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。

```
zonelabs-integrity interface interface
```

例：

```
hostname(config)# zonelabs-integrity interface inside
```

ステップ 4 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。

```
zonelabs-integrity fail-timeout timeout
```

例：

```
hostname(config)# zonelabs-integrity fail-timeout 12
```

ステップ 5 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。

```
zonelabs-integrity fail-close
```

例：

```
hostname(config)# zonelabs-integrity fail-close
```

ステップ 6 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。

```
zonelabs-integrity fail-open
```

例：

```
hostname(config)# zonelabs-integrity fail-open
```

ステップ 7 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。

```
zonelabs-integrity ssl-certificate-port cert-port-number
```

例：

```
hostname(config)# zonelabs-integrity ssl-certificate-port 300
```

ステップ 8 サーバの SSL 証明書が常に認証される間、Integrity サーバのクライアント SSL 証明書が認証されるように指定します。

```
zonelabs-integrity ssl-client-authentication {enable | disable}
```

例：

```
hostname(config)# zonelabs-integrity ssl-client-authentication enable
```

ファイアウォール クライアント タイプの Zone Labs への設定

手順

	コマンドまたはアクション	目的
ステップ 1	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。 例： `hostname(config)# client-firewall req zonelabs-integrity`	**client-firewall {opt | req} zonelabs-integrity**

次のタスク

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 （202 ページ）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 （202 ページ）を参照してください。

- Cisco 統合ファイアウォール

```
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 *6 : 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?」という確認メッセージが表示されます。応答がない場合は、ASA によって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。
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。許可ルールを定義しないと、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 command** 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]
```

次の表に、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 *7 : 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。

パラメータ	説明
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。値の小さいプライオリティ 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*	フリー形式の文字列を介してデバイスのタイプを識別します。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 などの自由形式の文字列を使用して、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。

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。

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 testuse
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** 形式を使用します。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]
```

下記の表に、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。

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

手順

ステップ 1 （任意） VPN アイドル タイムアウト期間を設定するには、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** *minutes* コマンドを使用します。

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。最小時間は 1 分、最大時間は 35791394 分であり、デフォルトは 30 分です。

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)#
```

[**no**] **vpn-idle-timeout** {*minutes* | **none**} コマンドを使用したその他のアクションは次のとおりです。

- VPN アイドル タイムアウトを無効にし、タイムアウト値を継承しないようにするには、**vpn-idle-timeout none** を入力します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-idle-timeout none
hostname(config-group-policy)#
```

これにより、AnyConnect（SSL と IPsec/IKEv2 の両方）およびクライアントレス VPN がグローバル webvpn **default-idle-timeout** *seconds* 値を使用するようになります。このコマンドは、webvpn コンフィギュレーション モードで入力します。たとえば、`hostnamee(config-webvpn)# default-idle-timeout 300` のように入力します。デフォルトは 1800 秒（30 分）で、範囲は 60 ～ 86400 秒です。

すべての webvon 接続の場合、**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。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。

サイト間（IKEv1、IKEv2）および IKEv1 リモート アクセス VPN の場合は、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することを推奨します。

- このグループ ポリシーまたはユーザ ポリシーのアイドル タイムアウトを無効にするには、**no vpn-idle-timeout** を入力します。値は継承されます。
- **vpn-idle-timeout** をまったく設定しない場合、値は継承されます。デフォルトは 30 分です。

ステップ 2 （任意） オプションで、**vpn-idle-timeout alert-interval** {*minutes*} 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できます。

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。デフォルトのアラート間隔は 1 分です。

次の例は、anyuser という名前のユーザに 3 分の VPN アイドル タイムアウト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 alert-interval 3
hostname(config-username)#
```

[**no**] **vpn-idle-timeout alert-interval** {*minutes* | **none**} コマンドを使用したその他のアクションは次のとおりです。

- **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。

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-idle-timeout none
hostname(config-username)#
```

- このグループまたはユーザ ポリシーのアラート間隔を削除するには、**no vpn-idle-timeout alert-interval** を入力します。値は継承されます。
- このパラメータをまったく設定しない場合、デフォルトのアラート間隔は 1 分です。

最大接続時間の設定

手順

ステップ 1 （任意）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** {*minutes* コマンドを使用して、VPN 接続の最大時間を設定します。

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。

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)#
```

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
hostname(config-username)#
```

[**no**] **vpn-session-timeout** {*minutes* | **none**} コマンドを使用したその他のアクションは次のとおりです。

- このポリシーから属性を削除し、継承を許可するには、このコマンドの **no vpn-session-timeout** 形式を入力します。
- 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、**vpn-session-timeout none** を入力します。

ステップ 2 **vpn-session-timeout alert-interval** {*minutes* | } 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指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
```

[**no**] **vpn-session-timeout alert-interval** {*minutes* | **none**} コマンドを使用したその他のアクションは次のとおりです。

- 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。

```
hostname(config-webvpn)# no vpn-session-timeout alert-interval
```

- **vpn-session-timeout alert-interval none** は、ユーザがアラートを受信しないことを示します。

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、グループ ポリシーから値を継承できます。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 では、**vpn-filter** コマンドで定義された ACL は使用されません。

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。一致していない場合、ASA はユーザが接続できないようにします。グループロックを設定しない場合、ASA は、割り当てられたグループとは関係なく、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

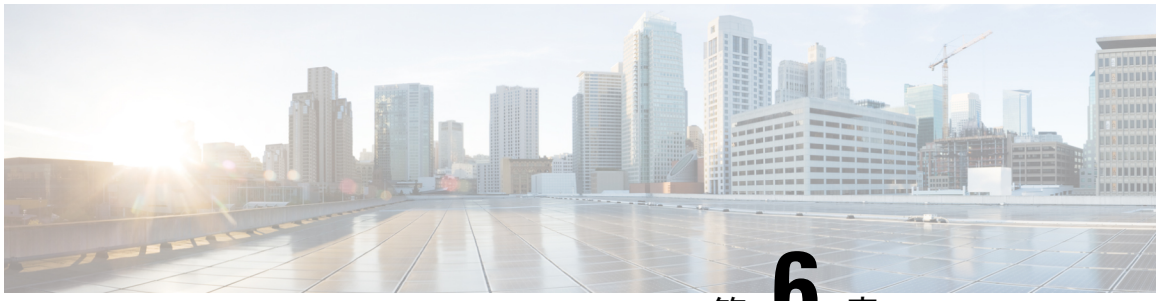
ユーザがログイン パスワードをクライアント システム上に保存するかどうかを指定します。パスワード保存は、デフォルトでディセーブルになっています。セキュア サイトにあることがわかっているシステム上でのみ、パスワードの保管をイネーブルにしてください。パスワード保存をディセーブルにするには、**disable** キーワードを指定して **password-storage** コマンドを入力します。password-storage 属性を実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を入力します。これにより、password-storage の値をグループ ポリシーから継承できます。

```
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)
```



第 6 章

VPN の IP アドレス

IP アドレス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。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、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。

次のいずれかの方式を使用して、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。

IPv4 アドレス割り当ての設定

手順

ASA のアドレス割り当て方式を有効にして、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。

vpn-addr-assign {**aaa** | **dhcp** | **local** [**reuse-delay** *minutes*]}

例：

たとえば、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。

```
hostname(config)#vpn-addr-assign aaa
hostname(config)#vpn-addr-assign local reuse-delay 180
```

この例では、コマンドの no 形式を使用してアドレス割り当て方式を無効にします。

```
hostname(config)# no vpn-addr-assign dhcp
```

IPv6 アドレス割り当ての設定

手順

ASA のアドレス割り当て方式を有効にして、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。

ipv6-vpn-addr-assign {**aaa** | local}

例：

```
hostname(config)# ipv6-vpn-addr-assign aaa
```

この例では、コマンドの no 形式を使用してアドレス割り当て方式を無効にします。

```
hostname(config)# no ipv6-vpn-addr-assign local
```

アドレス割り当て方式の表示

手順

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。

- IPv4 アドレス割り当ての表示

  設定されているアドレス割り当て方式を表示します。設定されているアドレス方式は、aaa、dhcp、または local です。

```
show running-config all vpn-addr-assign
vpn-addr-assign aaa
vpn-addr-assign dhcp
vpn-addr-assign local
```

- IPv6 アドレス割り当ての表示

  設定されているアドレス割り当て方式を表示します。設定されているアドレス方式は、aaa または local となります。

```
show running-config all ipv6-vpn-addr-assign
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、接続用の接続プロファイルまたはトンネル グループ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 プールを設定すると、ASA は追加された順でそれらのプールを使用します。

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 IPv4 アドレス プールの設定

手順

ステップ 1 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。**local** 引数を指定して **vpn-addr-assign** コマンドを入力します。

例：

```
hostname(config)# vpn-addr-assign local
```

ステップ 2 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。

ip local pool*poolname first_address-last_address***mask***mask*

例：

この例では、*firstpool* という IP アドレス プールを設定します。開始アドレスは 10.20.30.40、終了アドレスは 10.20.30.50 です。ネットワーク マスクは 255.255.255.0 です。

```
hostname(config)# ip local pool firstpool 10.20.30.40-10.20.30.50 mask 255.255.255.0
```

この例では、**firstpool** という IP アドレス プールを削除します。

```
hostname(config)# no ip local pool firstpool
```

ローカル IPv6 アドレス プールの設定

手順

ステップ 1 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。**local** 引数を指定して **vpn-addr-assign** コマンドを入力します。

例：

```
hostname(config)# ipv6-vpn-addr-assign local
```

ステップ 2 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。

ipv6 local pool *pool_name starting_address prefix_length number_of_addresses*

例：

この例では、*ipv6pool* という IP アドレス プールを設定します。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。

```
hostname(config)# ipv6 local pool ipv6pool 2001:DB8::1/32 100
```

この例では、*ipv6pool* という IP アドレス プールを削除します。

```
hostname(config)# no ipv6 local pool ipv6pool
```

AAA アドレス指定の設定

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)# 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。

手順

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)#
```

次のタスク

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 アドレス指定の設定

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。

注意事項と制約事項

IPv4 アドレスを使用して、クライアント アドレスを割り当てる DHCP サーバを識別できます。

DHCP アドレス指定の設定

手順

ステップ 1 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。

vpn-addr-assign dhcp

ステップ 2 リモート アクセス接続プロファイルとして *firstgroup* という名前の接続プロファイルを設定します。

tunnel-group *firstgroup* **type remote-access**

ステップ 3 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。

tunnel-group *firstgroup* **general-attributes**

ステップ 4 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 アドレスの取得を試みるときに、指定された 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。

dhcp-server *IPv4_address_of_DHCP_server*

例：

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。

```
hostname(config-general)# dhcp-server 172.33.44.19
hostname(config-general)#
```

ステップ 5 トンネル グループ モードを終了します。

```
 hostname(config-general)# exit
hostname(config)#
```

ステップ 6 *remotegroup* 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 remotegroup internal
```

例：

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。

```
 hostname(config)# group-policy remotegroup attributes
hostname(config-group-policy)#
```

ステップ 7 （任意） 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。

例：

```
hostname(config)# group-policy remotegroup attributes
```

ステップ 8 （任意） *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。

```
 hostname(config-group-policy)# dhcp-network-scope 192.86.0.0
hostname(config-group-policy)#
```

（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。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。

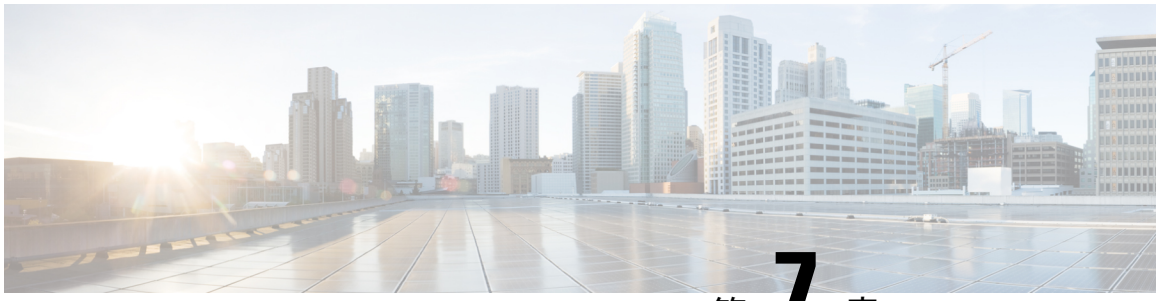
例

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
```

次のタスク

詳細については、『Cisco Security Appliance Command Reference』ガイドで **dhcp-server** コマンドを参照してください。



第 7 章

リモート アクセス IPSec VPN

リモート アクセス IPsec VPN について

リモート アクセス VPN を使用すると、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。ここでは、次の項目について説明します。

- 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。

• 暗号キーを置き換える前に、ASA がその暗号キーを使用する時間の上限。

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。特定のデータ フローを保護する場合、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、特定のトランスフォーム セットを使用することに同意します。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、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 （237 ページ）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。

Mobike およびリモート アクセス VPN について

モバイル IKEv2（mobike）は、モバイル デバイスのローミングをサポートするために ASA RA VPN を拡張します。このサポートは、デバイスが現在の接続ポイントから別のポイントに移動するときに、モバイル デバイスの IKE/IPSEC セキュリティ アソシエーション（SA）のエンドポイント IP アドレスが削除されるのではなく更新できることを意味します。

Mobike はバージョン 9.8(1) 以降は ASA でデフォルトにより利用可能です。つまり、Mobike は「常にオン」になります。Mobike は、クライアントがそれを提案し、ASA が受け入れるときにだけ、各 SA に対して有効になります。このネゴシエーションは、IKE_AUTH 交換の一部として行われます。

mobike サポートが有効な状態で SA が確立された後、クライアントはいつでもアドレスを変更して、新しいアドレスを示す UPDATE_SA_ADDRESS ペイロードを含む情報交換を使用して ASA に通知できます。ASA はこのメッセージを処理し、新しいクライアント IP アドレスで SA を更新します。

（注） `show crypto ikev2 sa detail` コマンドを使用して、現在のすべての SA で mobike が有効になっているかどうかを判別できます。

現在の Mobike の実装では、次の機能がサポートされています。

- IPv4 アドレスのみ
- NAT マッピングの変更
- オプションのリターン ルータビリティ チェックによるパス接続と停止検出
- アクティブ/スタンバイ フェールオーバー
- VPN ロード バランシング

RRC（リターン ルータビリティ チェック）機能が有効になっている場合、モバイル クライアントにRRCメッセージが送信され、SAが更新される前に新しいIPアドレスが確認されます。

リモート アクセス IPsec VPN for 3.1 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。

IKEv2 を使用した IPsec リモート アクセス VPN には、別途購入可能な AnyConnect Plus または Apex ライセンスが必要です。AnyConnect ライセンスを購入する場合は、次の最大値を参照してください。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 サイト間 VPN では、基本ライセンスに付属の Other VPN ライセンスが使用されます。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越えることはできません。

モデル	ライセンス要件

ASA 5506-X、5506H-X、5506W-X	• IKEv2 を使用した IPsec リモート アクセス VPN：50 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：50 セッション。

ASA 5508-X	100 セッションです。
ASA 5512-X	250 セッションです。
ASA 5515-X	250 セッションです。
ASA 5516-X	300 セッションです。

モデル	ライセンス要件
ASA 5525-X	750 セッションです。
ASA 5545-X	2500 セッションです。
ASA 5555-X	5000 セッションです。
ASA 5585-X（SSP-10）	5000 セッションです。
ASA 5585-X（SSP-20、-40、および -60）	10,000 セッションです。
ASASM	10,000 セッションです。
ASAv5	250 セッションです。
ASAv10	250 セッションです。
ASAv30	750 セッションです。

IPsec VPN の制約事項

- ファイアウォール モード ガイドライン：ルーテッド ファイアウォール モードでのみサポートされます。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 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

このセクションでは、リモート アクセス VPN の設定方法について説明します。

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および内部と言います。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。

手順

ステップ 1 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。

interface {*interface*}

例：

```
hostname(config)# interface ethernet0
hostname(config-if)#
```

ステップ 2 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。

ip address *ip_address* [*mask*] [*standby ip_address*]

例：

```
hostname(config)# interface ethernet0
hostname(config-if)# ip address 10.10.4.200 255.255.0.0
```

ステップ 3 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。

nameif *name*

例：

```
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します。デフォルトで、インターフェイスはディセーブルです。shutdown

例：

```
hostname(config-if)# no shutdown
hostname(config-if)#
```

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

手順

ステップ 1 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。

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 IKE ポリシー内で使用する暗号化方式を指定します。

crypto ikev1 policy *priority***encryption** {**aes** | **aes-192** | **aes-256** | **des** | **3des**}

例：

```
hostname(config)# crypto ikev1 policy 1 encryption 3des
hostname(config)#
```

ステップ 3 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。

crypto ikev1 policy *priority***hash** {**md5** | **sha**}

例：

```
hostname(config)# crypto ikev1 policy 1 hash sha
hostname(config)#
```

ステップ 4 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。

crypto ikev1 policy *priority***group** {**1** | **2** | **5**}

例：

```
hostname(config)# crypto ikev1 policy 1 group 2
hostname(config)#
```

ステップ 5 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。

crypto ikev1 policy *priority***lifetime** {*seconds*}

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。

例：

```
hostname(config)# crypto ikev1 policy 1 lifetime 43200
hostname(config)#
```

ステップ 6 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。

crypto ikev1 enable *interface-name*

例：

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

ステップ 7 変更をコンフィギュレーションに保存します。

write memory

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。

手順

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。

ip local pool *poolname first-address—last-address* [**mask** *mask*]

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。

例：

```
hostname(config)# ip local pool testpool 192.168.0.10-192.168.0.15
hostname(config)#
```

ユーザの追加

手順

ユーザ、パスワード、および特権レベルを作成します。

username *name* {**nopassword** | **password** *password* [**mschap** | **encrypted** | **nt-encrypted**]} [**privilege** *priv_level*]

例：

```
Hostname(config)# username testuser password 12345678
```

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。

次の手順では、IKEv1 および IKEv2 プロポーザルを作成する方法を示します。

手順

ステップ 1 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。

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

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：Triple 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。

例：

IKEv1 トランスフォーム セットの設定手順

```
hostname(config)# crypto ipsec transform set FirstSet esp-3des esp-md5-hmac
hostname(config)#
```

ステップ 2 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、カプセル化セキュリティ ペイロード（ESP）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）。

crypto ipsec ikev2 ipsec-proposal *proposal_name*

protocol {**esp**} {**encryption** {**des** | **3des** | **aes** | **aes-192** | **aes-256** | **null**} | **integrity** {**md5** | **sha-1**}

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、ESP の整合性保護のために米国連邦情報処理標準（FIPS）で定義されたセキュア ハッシュ アルゴリズム（SHA）SHA-1 を指定します。

IKEv2 プロポーザルの設定手順

```
hostname(config)# crypto ipsec ikev2 ipsec-proposal secure_proposal
hostname(config-ipsec-proposal)# protocol esp encryption des integrity md5
```

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のコレクションです。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。これらのグループは変更できますが、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。

手順

ステップ 1 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。

tunnel-group *name***type** *type*

例：

```
hostname(config)# tunnel-group testgroup type ipsec-ra
hostname(config)#
```

ステップ 2 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。

tunnel-group *name***general-attributes**

例：

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

ステップ 3 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。

address-pool [*(interface name)*] *address_pool1* [*...address_pool6*]

例：

```
hostname(config-general)# address-pool testpool
```

ステップ 4 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。

tunnel-group *name***ipsec-attributes**

例：

```
hostname(config)# tunnel-group testgroup ipsec-attributes
hostname(config-tunnel-ipsec)#
```

ステップ 5 （任意） 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。

ikev1 pre-shared-key キー

例：

```
hostname(config-tunnel-ipsec)# pre-shared-key 44kkaol59636jnfx
```

ダイナミック クリプト マップの作成

ダイナミック クリプトマップは、すべてのパラメータが設定されているわけではないポリシー テンプレートを定義します。これにより、ASA は、リモート アクセス クライアントなどの 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。

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できます。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

ステップ 1 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。

- 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*

• 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 ikev1 transform-set FirstSet
hostname(config)#

hostname(config)# crypto dynamic-map dyn1 1 set ikev2 ipsec-proposal FirstSet
hostname(config)#
```

ステップ 2 （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。

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)#
```

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

クリプトマップエントリを作成します。これにより、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、前の項で作成したものです。

手順

ステップ 1 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。

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

例：

```
hostname(config)# crypto map mymap 1 ipsec-isakmp dynamic dyn1
```

ステップ 2 クリプト マップを外部インターフェイスに適用します。

crypto map *map-name***interface** *interface-name*

例：

```
hostname(config)# crypto map mymap interface outside
```

ステップ 3 変更をコンフィギュレーションに保存します。

write memory

マルチコンテキスト モードでの IPSec IKEv2 リモート アクセス VPN の設定

リモート アクセス IPsec VPN の設定の詳細については、次の項を参照してください。

- インターフェイスの設定 （234 ページ）
- アドレス プールの設定 （237 ページ）
- ユーザの追加 （237 ページ）
- 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 （237 ページ）
- トンネル グループの定義 （239 ページ）
- ダイナミック クリプト マップの作成 （240 ページ）
- 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 （241 ページ）

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)# crypto ikev1 policy 10
hostname(config-ikev1-policy)# authentication pre-share
hostname(config-ikev1-policy)# encryption aes-256
hostname(config-ikev1-policy)# hash sha
hostname(config-ikev1-policy)# group 2
hostname(config)# crypto ikev1 enable outside
hostname(config)# ip local pool POOL 192.168.0.10-192.168.0.15
hostname(config)# username testuser password 12345678
hostname(config)# crypto ipsec ikev1 transform set AES256-SHA
esp-aes-256 esp-sha-hmac
hostname(config)# tunnel-group RAVPN type remote-access
hostname(config)# tunnel-group RAVPN general-attributes
hostname(config-general)# address-pool POOL
hostname(config)# tunnel-group RAVPN ipsec-attributes
hostname(config-ipsec)# ikev1 pre-shared-key ravpnkey
hostname(config)# crypto dynamic-map DYNMAP 1 set ikev1
transform-set AES256-SHA
hostname(config)# crypto dynamic-map DYNMAP 1 set reverse-route
hostname(config)# crypto map CMAP 1 ipsec-isakmp dynamic DYNMAP
hostname(config)# crypto map CMAP interface outside
```

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)# crypto ikev2 policy 1
hostname(config-ikev2-policy)# group 2
hostname(config-ikev2-policy)# integrity sha512
hostname(config-ikev2-policy)# prf sha512
hostname(config)# crypto ikev2 enable outside
hostname(config)# ip local pool POOL 192.168.0.10-192.168.0.15
hostname(config)# username testuser password 12345678
hostname(config)# crypto ipsec ikev2 ipsec-proposal  AES256-SHA512
hostname(config-ipsec-proposal)# protocol esp encryption  aes-256
hostname(config-ipsec-proposal)# protocol esp integrity sha-512
hostname(config)# tunnel-group RAVPN type remote-access
hostname(config)# tunnel-group RAVPN general-attributes
hostname(config-general)# address-pool POOL
hostname(config)# tunnel-group RAVPN ipsec-attributes
hostname(config-tunnel-ipsec)# ikev2 local-authentication
pre-shared-key localravpnkey
hostname(config-tunnel-ipsec)# ikev2 remote-authentication
pre-shared-key remoteravpnkey
hostname(config)# crypto dynamic-map DYNMAP 1 set ikev2
ipsec-proposal AES256-SHA512
hostname(config)# crypto dynamic-map DYNMAP 1 set reverse-route
hostname(config)# crypto map CMAP 1 ipsec-isakmp dynamic DYNMAP
hostname(config)# crypto map CMAP interface outside
```

マルチコンテキスト モードでの標準ベース IPSec IKEv2 リモート アクセス VPN の設定例

次の例は、マルチコンテキスト モードで標準ベース リモート アクセス IPsec/IKEv2 VPN 用の ASA を設定する方法を示しています。この例では、システム コンテキストおよびユーザ コンテキストの設定について、それぞれ情報を提供します。

システム コンテキストの設定：

```
class default
  limit-resource All 0
  limit-resource Mac-addresses 65536
  limit-resource ASDM 5
  limit-resource SSH 5
  limit-resource Telnet 5
  limit-resource VPN AnyConnect 4.0%

hostname(config)#context CTX2
hostname(config-ctx)#member default   ===============> License allotment for contexts
using class
hostname(config-ctx)#allocate-interface Ethernet1/1.200
hostname(config-ctx)#allocate-interface Ethernet1/3.100
hostname(config-ctx)#config-url disk0:/CTX2.cfg
```

ユーザ コンテキストの設定：

```
hostname/CTX2(config)#ip local pool CTX2-pool 1.1.2.1-1.1.2.250 mask 255.255.255.0
hostname/CTX2(config)#aaa-server ISE protocol radius
```

```
hostname/CTX2(config)#aaa-server ISE (inside) host 10.10.190.100
hostname/CTX2(config-aaa-server-host)#key *****
hostname/CTX2(config-aaa-server-host)#exit
hostname/CTX2(config)#

hostname/CTX2(config)#group-policy GroupPolicy_CTX2-IKEv2 internal
hostname/CTX2(config)#group-policy GroupPolicy_CTX2-IKEv2 attributes
hostname/CTX2(config-group-policy)#vpn-tunnel-protocol ikev2
hostname/CTX2(config-group-policy)#exit
hostname/CTX2(config)#

hostname/CTX2(config)#crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set ikev2
ipsec-proposal AES256 AES192 AES 3DES DES
hostname/CTX2(config)#crypto map outside_map 65535 ipsec-isakmp dynamic
SYSTEM_DEFAULT_CRYPTO_MAP
hostname/CTX2(config)#crypto map outside_map interface outside
```

デフォルトでは、標準ベース クライアントからの IPSec/IKEv2 リモート アクセス接続は、トンネル グループ「DefaultRAGroup」に分類されます。

```
hostname/CTX2(config)#tunnel-group DefaultRAGroup type remote-access
hostname/CTX2(config)#tunnel-group DefaultRAGroup general-attributes
hostname/CTX2(config-tunnel-general)#default-group-policy GroupPolicy_CTX2-IKEv2
hostname/CTX2(config-tunnel-general)#address-pool CTX2-pool
hostname/CTX2(config-tunnel-general)#authentication-server-group ISE
hostname/CTX2(config-tunnel-general)#exit
hostname/CTX2(config)#

hostname/CTX2(config)#tunnel-group DefaultRAGroup ipsec-attributes
hostname/CTX2(config-tunnel-ipsec)#ikev2 remote-authentication eap query-identity
hostname/CTX2(config-tunnel-ipsec)#ikev2 local-authentication certificate ASDM_TrustPoint0
hostname/CTX2(config-tunnel-ipsec)#exit
hostname/CTX2(config)#

hostname/CTX2(config)#crypto ikev2 enable outside client-services port 443
hostname/CTX2(config)#crypto ikev2 remote-access trustpoint ASDM_TrustPoint0
```

マルチコンテキスト モードでの AnyConnect IPSec IKEv2 リモート アクセス VPN の設定例

次の例は、マルチコンテキスト モードで AnyConnect リモート アクセス IPsec/IKEv2 VPN 用の ASA を設定する方法を示しています。この例では、システム コンテキストおよびユーザ コンテキストの設定について、それぞれ情報を提供します。

システム コンテキストの設定：

```
class default
    limit-resource All 0
    limit-resource Mac-addresses 65536
    limit-resource ASDM 5
    limit-resource SSH 5
    limit-resource Telnet 5
    limit-resource VPN AnyConnect 4.0%
```

```
hostname(config)#context CTX3
hostname(config-ctx)#member default   ===============> License allotment for contexts
using class
hostname(config-ctx)#allocate-interface Ethernet1/1.200
hostname(config-ctx)#allocate-interface Ethernet1/3.100
hostname(config-ctx)#config-url disk0:/CTX3.cfg
```

各コンテキストの仮想ファイル システムの作成では、イメージ、プロファイルなどの Cisco Anyconnect ファイルを使用できます。

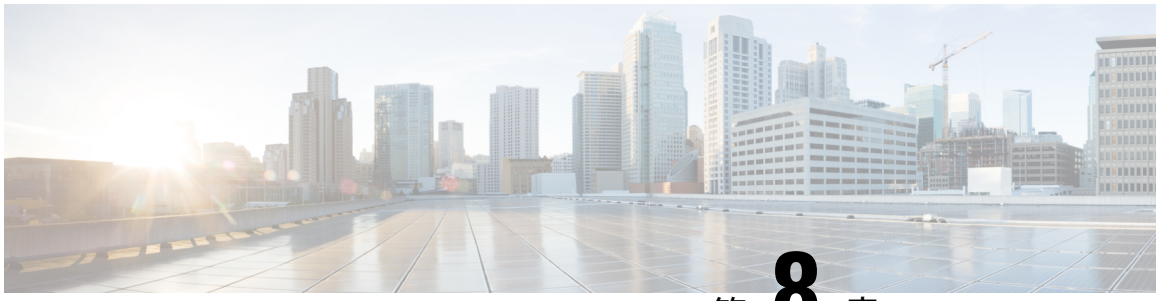
```
hostname(config-ctx)#storage-url shared disk0:/shared disk0
```

ユーザ コンテキストの設定：

```
hostname/CTX3(config)#ip local pool ctx3-pool 1.1.3.1-1.1.3.250 mask 255.255.255.0
hostname/CTX3(config)#webvpn
hostname/CTX3(config-webvpn)#enable outside
hostname/CTX3(config-webvpn)# anyconnect image
disk0:/anyconnect-win-4.6.00010-webdeploy-k9.pkg 1
hostname/CTX3(config-webvpn)#anyconnect profiles IKEv2-ctx1 disk0:/ikev2-ctx1.xml
hostname/CTX3(config-webvpn)#anyconnect enable
hostname/CTX3(config-webvpn)#tunnel-group-list enable


hostname/CTX3(config)#username cisco password *****
hostname/CTX3(config)#ssl trust-point ASDM_TrustPoint0 outside
hostname/CTX3(config)#group-policy GroupPolicy_CTX3-IKEv2 internal
hostname/CTX3(config)#group-policy GroupPolicy_CTX3-IKEv2 attributes


hostname/CTX3(config-group-policy)#vpn-tunnel-protocol ikev2 ssl-client
hostname/CTX3(config-group-policy)#dns-server value 10.3.5.6
hostname/CTX3(config-group-policy)#wins-server none
hostname/CTX3(config-group-policy)#default-domain none
hostname/CTX3(config-group-policy)#webvpn
hostname/CTX3(config-group-webvpn)#anyconnect profiles value IKEv2-ctx1 type user


hostname/CTX3(config)#crypto ikev2 enable outside client-services port 443
hostname/CTX3(config)#crypto ikev2 remote-access trustpoint ASDM_TrustPoint0
hostname/CTX3(config)#crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set ikev2
ipsec-proposal AES256 AES192 AES 3DES DES
hostname/CTX3(config)#crypto map outside_map 65535 ipsec-isakmp dynamic
SYSTEM_DEFAULT_CRYPTO_MAP
hostname/CTX3(config)#crypto map outside_map interface outside


hostname/CTX3(config)#tunnel-group CTX3-IKEv2 type remote-access
hostname/CTX3(config)#tunnel-group CTX3-IKEv2 general-attributes
hostname/CTX3(config-tunnel-general)#default-group-policy GroupPolicy_CTX3-IKEv2
hostname/CTX3(config-tunnel-general)#address-pool ctx3-pool
hostname/CTX3(config)#tunnel-group CTX3-IKEv2 webvpn-attributes
hostname/CTX3(config-tunnel-webvpn)#group-alias CTX3-IKEv2 enable
```

リモート アクセス VPN 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。
リモート アクセス VPN の自動 mobike サポート。	9.8(1)	IPsec IKEv2 RA VPN に対するモバイル IKE（mobike）のサポートが追加されました。Mobike は常にオンになっています。 IKEv2 RA VPN 接続のための mobike 通信時のリターン ルータビリティ チェックを有効にできるよう、`ikev2 mobike-rrc` コマンドが追加されました。
マルチコンテキスト モードでの IPsec IKEv2 のリモート アクセス VPN	9.9(2)	AnyConnect やサードパーティ製標準ベース IPSec IKEv2 VPN クライアントがマルチコンテキスト モードで稼働する ASA へのリモート アクセス VPN セッションを確立できるように、ASA を構成することをサポートします。



第 8 章

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。

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 接続を作成できます。これらのピアは、IPv4 と IPv6 のアドレッシングを使用して、内部アドレスと外部アドレスの任意の組み合わせを持つことができます。

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。

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。

手順

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。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および内部と言います。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。

手順

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デフィーヘルマン グループ。ASA はこのアルゴリズムを使用して、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。
- ASA が暗号キーを使用する時間の制限。この時間が経過すると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 （251 ページ）
- IKEv2 接続の ISAKMP ポリシーの設定 （252 ページ）

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。

手順

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。

手順

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。特定のデータ フローを保護する場合、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、特定のトランスフォーム セットを使用することに同意します。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。

次の表に、有効な暗号化方式と認証方式を示します。

表 *8 :* 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。

手順

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-nameencryption-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。

次の表に、有効な IKEv2 暗号化方式と認証方式を示します。

表 *9:* 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	
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。

手順

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、secure がプロポーザルの名前です。

```
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、一般的操作用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。

（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 ルールの適用 （169 ページ） を参照してください。

手順

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 ACL をミラーリングする接続のもう一方の側の ASA に、ACL を設定します。2 つの異なる暗号 ACLで定義され、同じクリプト マップに接続されたサブネットは重複できません。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)#
```

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（事前共有キーまたは証明書）。

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（つまり、IKEv1 と IKEv2 用の事前共有キー）を設定します。

手順

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。

1.

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、**ikev1pre-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)# ikev1-pre-shared-key 44kkaol59636jnfx
```

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 crypto 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。

手順

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 | hostname1}[... ip_address10 | hostname10] 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。

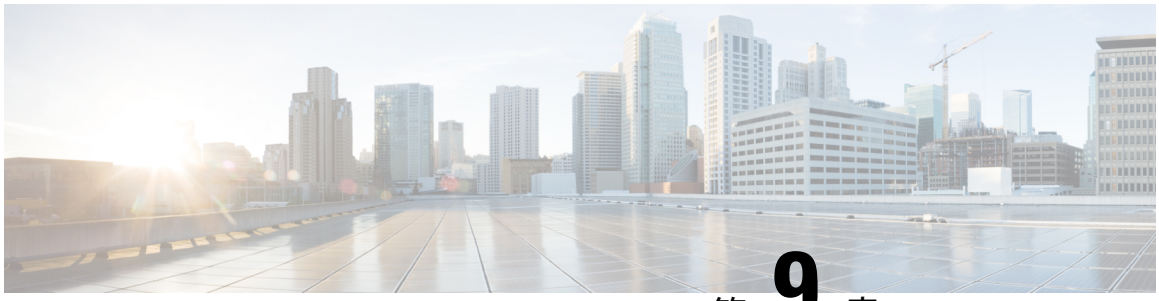
手順

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)#
```



第 9 章

AnyConnect VPN Client 接続

この項では、AnyConnect VPN Client 接続を設定する方法について説明します。

AnyConnect VPN Client について

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。

以前から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 によってクライアントのリビジョンが点検され、必要に応じてアップグレードされます。

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。クライアントの手動インストールの詳細については、『Cisco AnyConnect Secure Mobility Configuration Guide』の適切なリリース http://www.cisco.com/c/en/us/support/security/anyconnect-secure-mobility-client/tsd-products-support-configure.html 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 の要件

AnyConnect Secure Mobility Client を実行しているエンドポイント コンピュータの要件については、『Cisco AnyConnect Secure Mobility Release Notes』の適切なリリース を参照してください。

AnyConnect の注意事項と制約事項

- ASA では、リモート HTTPS 証明書は確認されません。
- 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。AnyConnect Apex ライセンスは、マルチコンテキスト モードのリモートアクセス VPN に必要です。ASA は AnyConnect Apex ライセンスを特異的に認識しませんが、プラットフォーム制限へのライセンス済み AnyConnect Premium、携帯電話用 AnyConnect、Cisco VPN フォン用 AnyConnect、および Advanced Endpoint Assessment など、Apex ライセンスのライセンス特性を適用します。共有ライセンス、AnyConnect Essentials、フェールオーバー ライセンス集約、およびフレックス/時間ベースのライセンスはサポートされていません。

AnyConnect 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。

VPN ライセンスには、別途購入可能な AnyConnect Plus または Apex ライセンスが必要です。AnyConnect ライセンスを購入する場合は、次の最大値を参照してください。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越えることはできません。

モデル	ライセンス要件
ASA 5506-X、5506H-X、5506W-X	50 セッションです。 共有ライセンスはサポートされていません。
ASA 5508-X	100 セッションです。 共有ライセンスはサポートされていません。
ASA 5512-X	• 250 セッションです。 • 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	• 250 セッションです。 • 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 5516-X	• 300 セッションです。 共有ライセンスはサポートされていません。
ASA 5525-X	• 750 セッションです。 • 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	• 2500 セッションです。 • 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	• 5000 セッションです。 • 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 5585-X（SSP-10）	• 5000 セッションです。 • 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）	• 10,000 セッションです。 • 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	• 10,000 セッションです。 • 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）。
ASAv5	50 セッションです。
ASAv10	250 セッションです。
ASAv30	750 セッションです。

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。

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。

始める前に

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

ステップ 1 フラッシュ上のファイルを 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。

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
```

（注） **anyconnect image** 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 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 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。

enable *interface*

例：

```
hostname(config)# webvpn
hostname(config-webvpn)# enable outside
```

ステップ 3 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。

AnyConnect のイネーブル

ステップ 4 （任意） 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。

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
```

ステップ 5 アドレス プールをトンネル グループに割り当てます。

address-pool *poolname*

例：

```
hostname(config)# tunnel-group telecommuters general-attributes
hostname(config-tunnel-general)# address-pool vpn_users
```

ステップ 6 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。

default-group-policy *name*

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

ステップ 7 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。

group-alias *name* **enable**

例：

```
hostname(config)# tunnel-group telecommuters webvpn-attributes
hostname(config-tunnel-webvpn)# group-alias sales_department enable
```

ステップ 8 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。

tunnel-group-list enable

例：

```
hostname(config)# webvpn
hostname(config-webvpn)# tunnel-group-list enable
```

ステップ 9 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。

vpn-tunnel-protocol

例：

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# vpn-tunnel-protocol
```

次のタスク

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。

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。

始める前に

このヘッドエンドで DTLS を設定し、使用する DTLS のバージョンを確認するには、SSL の詳細設定 （100 ページ） を参照してください。

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 の詳細については、デッドピア検出の設定 （280 ページ）を参照してください。

手順

ステップ 1 AnyConnect VPN 接続に対して DTLS オプションを指定します。

a) webvpn モードのインターフェイスで SSL と DTLS を有効にします。

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。

```
hostname(config)# webvpn
hostname(config-webvpn)# enable outside
```

webvpn コンフィギュレーション モードで、**enable** *interface* **tls-only** コマンドを使用し、すべての AnyConnect クライアント ユーザに対して DTLS をディセーブルにします。

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。

```
hostname(config)# webvpn
hostname(config-webvpn)# enable outside tls-only
```

b) **port** および **dtls port** コマンドを使用して SSL および DTLS のポートを設定します。

```
hostname(config)# webvpn
hostname(config-webvpn)# enable outside
hostname(config-webvpn)# port 555
hostname(config-webvpn)# dtls port 556
```

ステップ 2 特定のグループ ポリシーに対して DTLS オプションを指定します。

a) 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** コマンドを使用して特定のグループまたはユーザに対して DTLS をイネーブルにします。

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# anyconnect ssl dtls enable
```

b) 必要に応じて、anyconnect dtls compression コマンドを使用して DTLS 圧縮をイネーブルにします。

```
hostname(config-group-webvpn)# anyconnect dtls compression lzs
```

リモート ユーザに対するプロンプト

手順

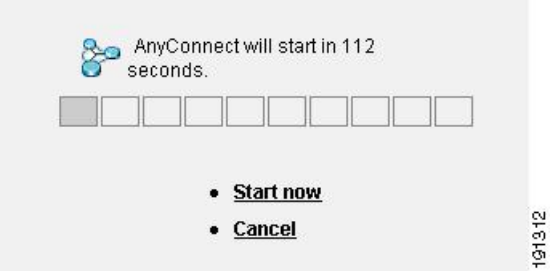
ASA で、リモート SSL VPN クライアント ユーザがクライアントをダウンロードするためのプロンプトをイネーブルにするには、グループ ポリシー webvpn コンフィギュレーション モードまたはユーザ名 webvpn コンフィギュレーション モードで **anyconnect ask** コマンドを使用します。

[**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尋ねるプロンプトをリモート ユーザに表示し、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、すぐにクライアントがダウンロードされます。
- **anyconnect ask enable default webvpn** を指定すると、すぐにポータル ページに移動します。
- **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。

次の図に、**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 *5:* リモート ユーザに表示される *SSL VPN* クライアントのダウンロードを求めるプロンプト



例

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ユーザに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（コア クライアントとその VPN 機能のコンフィギュレーション設定、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）で Cisco AnyConnect Secure Mobility クライアント機能をイネーブルにします。ASA は、AnyConnect のインストールと更新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。

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 または ISE から起動できる便利な GUI ベースの構成ツールです。Windows 用 AnyConnect ソフトウェア パッケージにはエディタが含まれています。このエディタは、AnyConnect パッケージを選択したヘッドエンド デバイスにロードし、AnyConnect クライアント イメージとして指定するとアクティブになります。

ASDM または ISE 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。

AnyConnect クライアントおよびプロファイル エディタの詳細については、『Cisco AnyConnect Secure Mobility Configuration Guide』の適切なリリースhttp://www.cisco.com/c/en/us/support/security/anyconnect-secure-mobility-client/tsd-products-support-configure.html 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。

手順

ステップ 1 ASDM/ISE 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。

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。

例：

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。

dir cache:stc/profiles コマンドを使用して、キャッシュ メモリにロードされたプロファイルを表示します。

```
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。

例：

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。AnyConnect プロファイル設定で AutoUpdate が [Enabled] に設定されていない限り、このアップグレード ダイアログは表示されません。

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* : 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	有効な値	デフォルト値	注意
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（ディセーブル）	延期アップグレード 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。

手順

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*]

例：

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-webvpn)# anyconnect-custom-attr DeferredUpdateAllowed
description Indicates if the deferred update feature is enabled or not
hostame(config-webvpn)# anyconnect-custom-attr DeferredUpdateDismissTimeout
```

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*

例：

次に、カスタム属性タイプ DeferredUpdateDismissTimeout 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 DeferredUpdateDismissTimeout
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*

例：

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)# anyconnect-custom DeferredUpdateAllowed
value def-allowed
hostname(config-group-policy)# anyconnect-custom DeferredUpdateDismissTimeout
value def-timeout
```

DSCP の保存の有効化

Windows または OS X プラットフォームでは、DTLS 接続の場合にのみ別のカスタム属性を設定することで DiffServ コード ポイント（DSCP）を制御できます。DSCP の保存を有効にすると、デバイスは遅延の影響を受けやすいトラフィックを優先することができます。ルータでは、これが設定されているかどうかが反映され、アウトバウンド接続品質の向上のために優先トラフィックがマークされます。

手順

ステップ 1 webvpn コンフィギュレーション モードで **anyconnect-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 DSCPPreservationAllowed description Set to control Differentiated Services Code Point (DSCP) on Windows or OS X platforms for DTLS connections only.

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 DSCPPreservationAllowed true

（注） デフォルトでは、AnyConnect は DSCP の保存を実行します（true）。無効にするには、ヘッドエンドでカスタム属性を false に設定し、接続を再実行します。

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 または ISE 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。

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。

手順

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、特定のグループまたはユーザへの VPN 接続のための GINA モジュールを ASA でダウンロードする機能を有効にします。

例：

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。

言語変換について

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。すべての Cisco AnyConnect VPN Client のユーザ インターフェイスに表示されるメッセージは、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。

手順

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 import 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

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、テンプレートからインポートした *zh* という名前の変換テーブルをエクスポートします。zh は Microsoft Internet Explorer における中国語の省略形です。

```
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、米国スペイン語用の 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

customization
keepout
url-list
webvpn
Citrix-plugin
RPC-plugin
Telnet-SSH-plugin
VNC-plugin

Translation Tables:
es-us AnyConnect
```

変換テーブルの削除

変換テーブルが必要なくなった場合は、削除できます。

手順

ステップ 1 既存の変換テーブルを一覧表示します。

次の例では、**show import 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。フランス語（fr）、日本語（ja）、ロシア語（ru）のさまざまなテーブルが用意されています。

```
hostname# show import webvpn translation-table
Translation Tables' Templates:
  AnyConnect
  PortForwarder
  banners
  csd
  customization
  url-list
  webvpn
Translation Tables:
  fr                    PortForwarder
  fr                    AnyConnect
```

```
fr                    customization
fr                    webvpn
ja                    PortForwarder
ja                    AnyConnect
ja                    customization
ja                    webvpn
ru                    PortForwarder
ru                    customization
ru                    webvpn
```

ステップ 2 不要な変換テーブルを削除します。

revert webvpn translation-table *translationdomain***language** *language*

translationdomain は上記に示す変換テーブルの右側に記載されているドメインで、*language* は 2 文字の言語名です。

各テーブルを個別に削除する必要があります。1 つのコマンドを使用して、特定の言語のテーブルをすべて削除することはできません。

たとえば、AnyConnect のフランス語の変換テーブルを削除するには：

```
ciscoasa# revert webvpn translation-table anyconnect language fr
ciscoasa#
```

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。

キー再生成の有効化

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有効にするには、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** キーの再生成中にクライアントによって新しいトンネルが確立されることを指定します。
- **method ssl** キーの再生成中にクライアントによって新しいトンネルが確立されることを指定します。
- **method none** キーの再生成を無効にします。
- **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。

（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 コマンドの履歴については、コマンド リファレンスを参照してください。

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
```

デッドピア検出の設定

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。デッドピア検出（DPD）を有効にし、AnyConnect クライアントまたは ASA ゲートウェイが DPD を実行する頻度を設定するには、以下の手順を実行します。

始める前に

- この機能は、ASA ゲートウェイと AnyConnect SSL VPN クライアント間の接続のみに適用されます。DPD はパディングを許可しない標準の実装に基づいているため IPsec を使用できず、クライアントレス SSL VPN がサポートされません。
- 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。
- ASA で DPD が有効になっているとき、Optimal MTU（OMTU）機能を使用すると、クライアントが DTLS パケットを正常に渡すことができる最大のエンドポイント MTU を見つけることができます。最大 MTU までパディングされた DPD パケットを送信することによって、OMTU を実装します。ペイロードの正しいエコーをヘッドエンドから受信すると、MTU サイズが受け入れられます。受け入れられなかった場合、MTU は小さくされ、プロトコルで許可されている最小 MTU に到達するまで、繰り返しプローブが送信されます。

手順

ステップ 1 目的のグループ ポリシーに移動します。

グループ ポリシーまたはユーザ名 webvpn モードを開始します。

```
hostname(config)# group-policy group-policy-name  attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)#
```

または

```
hostname# username username attributes
hostname(config-username)# webvpn
hostname (config-username-webvpn #
```

ステップ 2 ゲートウェイ側の検出を設定します。

[**no**] **anyconnect dpd-interval** {[**gateway** {*seconds* | **none**}] コマンドを使用します。

gateway は、ASA のことです。DPD を有効にし、ASA が DPD テストを実行する頻度を 30 秒（デフォルト）から 3600 秒（1 時間）の範囲で指定します。値 300 が推奨されます。

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。このコマンドを設定から削除するには、**no anyconnect dpd-interval** を使用します。

ステップ 3 クライアント側の検出を設定します。

[**no**] **anyconnect dpd-interval** {[**client** {*seconds* | **none**}]} コマンドを使用します。

クライアントは、AnyConnect クライアントのことです。DPD を有効にし、クライアントが DPD テストを実行する頻度を 30 秒（デフォルト）から 3600 秒（1 時間）の範囲で指定します。値 300 が推奨されます。

clientnone を指定すると、クライアントにより実行される DPD が無効になります。このコマンドを設定から削除するには、**no anyconnect dpd-interval** を使用します。

例

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
```

Enable Keepalive

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。

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 モードから **keepalive** コマンドを使用します。設定からコマンドを削除して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。

[**no**] **anyconnect ssl keepalive** {**none** | *seconds*}

- **none** は、クライアントのキープアライブ メッセージを無効にします。
- *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。

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 **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 **compression** コマンドを使用します。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。

[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 sslcompression** 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（576 ～ 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。また、SSL で確立されたクライアント接続と DTLS による SSL で確立された接続は、このコマンドの影響を受けます。

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。

たとえば、ISE Posture AnyConnect モジュールの実行時に、「MTU configuration sent from the secure gateway is too small」というメッセージが表示されることがあります。**anyconnect ssl df-bit-ignore disable** と一緒に **anyconnect mtu 1200** を入力すると、これらのシステム スキャン エラーを回避できます。

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。

手順

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、[**no**]**anyconnect image**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。

手順

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 接続の監視

アクティブなセッションに関する情報を表示するには、**show vpn-sessiondb** コマンドを使用します。

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。

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-sessiondb logoff name *name*
vpn-sessiondb 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な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）。後でセッションが再開されると、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。

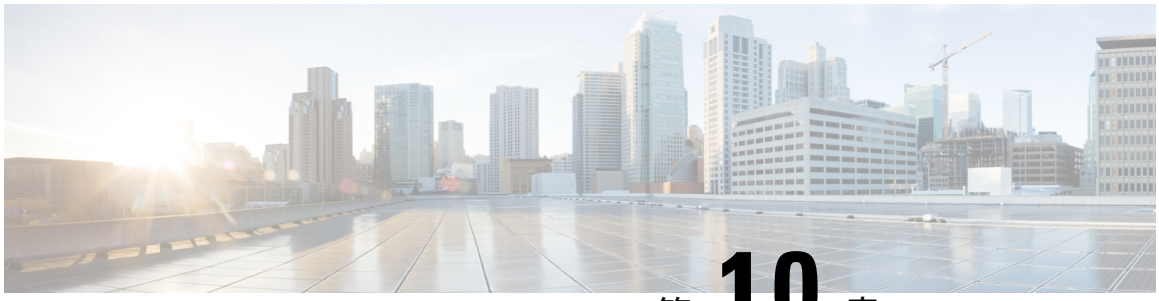
```
hostname# vpn-sessiondb logoff name lee
Do you want to logoff the VPN session(s)? [confirm]
INFO: Number of sessions with name “lee” logged off : 1

hostname#
```

AnyConnect 接続の機能履歴

次の表に、この機能のリリース履歴を示します。

表 *11 : 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。



第 10 章

AnyConnect HostScan

AnyConnect ポスチャ モジュールにより、AnyConnect Secure Mobility クライアント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、マルウェア対策、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、HostScan アプリケーションによって収集されます。ポスチャ アセスメントでは、ホストに HostScan がインストールされている必要があります。

HostScan の前提条件

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

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 7、8、8.1、10、10 RS1、RS2、RS3 x86（32 ビット）および x64（64 ビット）

- macOS 10.11、10.12、10.13
- Linux Red Hat 6、7、Ubuntu 14.04（LTS）および 16.04（LTS）（64 ビットのみ）

ホスト スキャンのライセンス

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 HostScan 用 AnyConnect Apex。
- 修復のためには AnyConnect Plus が必要です。

HostScan パッケージ

HostScan パッケージを ASA にスタンドアロン パッケージ **hostscan-version.pkg** としてロードすることができます。このファイルには、HostScan ソフトウェアとともに、HostScan ライブラリおよびサポート表が含まれています。

HostScan 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 HostScan パッケージをインストールまたはアップグレードし、有効にします。

始める前に

（注） HostScan バージョン 4.3.x 以前から 4.6.x 以降にアップグレードしようとしている場合、以前に確立した既存の AV/AS/FW DAP ポリシーおよび LUA スクリプトがすべて HostScan 4.6.x 以降と非互換であるという事実に起因するエラー メッセージが表示されます。

設定を適応させるために実行する必要があるワンタイム移行手順が存在します。この手順では、このダイアログボックスを閉じて、この設定を保存する前に HostScan 4.4.x と互換になるように設定を移行します。この手順を中止し、『AnyConnect HostScan 4.3.x to 4.6.x Migration Guide』で詳細な手順を参照してください。つまり、移行するには ASDM DAP のポリシー ページに移動して、互換性のない AV/AS/FW 属性を確認して手動で削除してから、LUA スクリプトを確認し、書き換える必要があります。

- 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 ファイルを ASA にアップロードします。

手順

ステップ 1 webvpn コンフィギュレーション モードを開始します。

例：

```
hostname(config)# webvpn
```

ステップ 2 HostScan 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。スタンドアロンの HostScan パッケージ、または AnyConnect セキュア モビリティ クライアント パッケージを HostScan パッケージとして指定することができます。

hostscan image *path*

例：

```
ASAName(webvpn)#hostscan image disk0:/ hostscan-3.6.0-k9.pkg
```

ステップ 3 前の手順で指定した HostScan イメージを有効にします。

例：

```
ASAName(webvpn)#hostscan enable
```

ステップ 4 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。

例：

```
hostname(webvpn)# write memory
```

ステップ 5

HostScan の有効化または無効化

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 HostScan イメージを有効または無効にします。

始める前に

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

ステップ 1 webvpn コンフィギュレーション モードを開始します。

例：

webvpn

ステップ 2 ASA からスタンドアロンの HostScan イメージがアンインストールされていない場合、このイメージを有効にします。

hostscan enable

ステップ 3 インストールされているすべての HostScan パッケージの HostScan を無効にします。

（注） 有効になっている HostScan 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、HostScan を無効にする必要があります。

no hostscan enable

ASA で有効になっている HostScan 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、有効になっている HostScan のバージョンを特定します。

始める前に

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。

手順

ASA 上で有効になっている HostScan のバージョンを表示します。

show webvpn hostscan

HostScan のアンインストール

HostScan 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、HostScan が有効になっている場合でも ASA による HostScan パッケージの展開が回避されます。HostScan をアンインストールしても、HostScan パッケージはフラッシュ ドライブから削除されません。

始める前に

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

ステップ 1 webvpn コンフィギュレーション モードを開始します。

webvpn

ステップ 2 アンインストールする HostScan イメージを無効にします。

no hostscanenable

ステップ 3 アンインストールする HostScan イメージへのパスを指定します。スタンドアロンの HostScan パッケージが HostScan パッケージとして指定されている場合があります。

no hostscan image *path*

例：

```
hostname(webvpn)#no hostscan image disk0:/hostscan-3.6.0-k9.pkg
```

ステップ 4 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。

write memory

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。

始める前に

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

ステップ 1 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。

group-policy *name* **internal**

例：

```
hostname(config)# group-policy PostureModuleGroup internal
```

ステップ 2 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。

group-policy *name* **attributes**

例：

```
hostname(config)# group-policy PostureModuleGroup attributes
```

ステップ 3 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)#

webvpn

ステップ 4 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 modules value *AnyConnect Module Name*

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）
vpngina	AnyConnect SBL（Start Before Logon）
websecurity	AnyConnect Web セキュリティ 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
nam	AnyConnect ネットワーク アクセス マネージャ
none	グループ ポリシーからすべての AnyConnect モジュールを削除する場合に使用します。

例：

```
hostname(config-group-webvpn)# anyconnect modules value websecurity,telemetry,posture
```

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 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)#

write memory

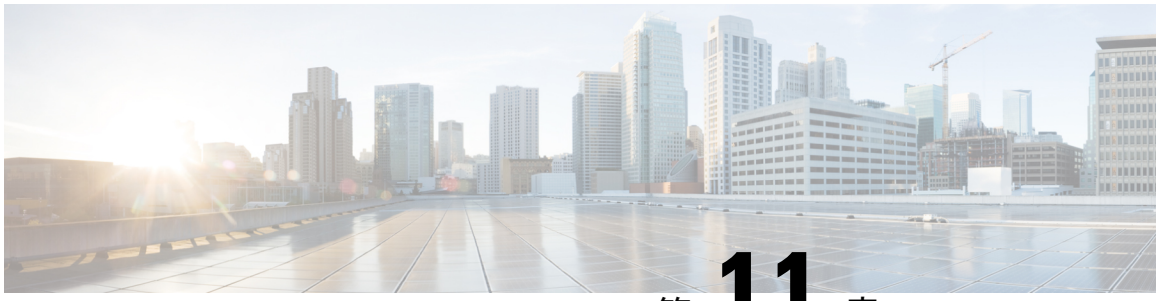
HostScan の関連マニュアル

HostScan 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、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 HostScan の動作の詳細については、『Cisco *AnyConnect Secure Mobility Client Administrator Guide*』を参照してください。



第 11 章

Easy VPN

この章では、Easy VPN サーバとして任意の ASA を設定する方法、および Easy VPN リモート ハードウェア クライアントとして Cisco ASA with FirePOWER- 5506-X、5506W-X、5506H-X、5508-X モデルを設定する方法について説明します。

Easy VPN について

Cisco Ezvpn は、リモート オフィスおよびモバイル ワーカー向けの VPN の設定と導入を大幅に簡素化します。Cisco Easy VPN は、サイト間 VPN とリモート アクセス VPN の両方に対応した柔軟性、拡張性、使いやすさを備えています。Cisco Unity クライアント プロトコルの実装により、管理者は Easy VPN サーバで大部分の VPN パラメータを定義できるので、Easy VPN リモートの設定がシンプルになります。

Cisco ASA with FirePOWER の 5506-X、5506W-X、5506H-X、および 5508-X モデルは、Easy VPN サーバへの VPN トンネルを開始するハードウェア クライアントして Easy VPN リモートをサポートします。Easy VPN サーバとして、別の ASA（任意のモデル）または Cisco IOS ベースのルータを使用できます。ASA は、同時に Easy VPN リモートと Easy VPN サーバの両方として動作することはできません。

（注） Cisco ASA 5506-X、5506W-X、5506H-X、および 5508-X モデルは、L2 スイッチングではなく、L3 スイッチングをサポートしています。内部ネットワーク上で複数のホストやデバイスとともに Easy VPN リモートを使用する場合は、外部スイッチを使用します。ASA の内部ネットワーク上に単一のホストしかない場合、スイッチは必要はありません。

次のセクションでは、Easy VPN のオプションと設定について説明します。

Easy VPN インターフェイス

システムの起動時に、セキュリティ レベルによって Easy VPN の外部および内部インターフェイスが決定されます。最もセキュリティ レベルが低い物理インターフェイスは、Easy VPN サーバへの外部接続に使用されます。最もセキュリティ レベルが高い物理または仮想インターフェイスは、セキュアなリソースへの内部接続に使用されます。Easy VPN で、同じ最高セキュリティ レベルの複数のインターフェイスがあることが特定されると、Easy VPN が無効になります。

必要に応じて、**vpnclient secure interface** コマンドを使用して、内部セキュア インターフェイスを物理インターフェイスから仮想インターフェイスに、あるいは仮想インターフェイスから物理インターフェイスに変更することができます。外部インターフェイスを自動的に選択されたデフォルトの物理インターフェイスから変更することはできません。

たとえば、ASA5506 プラットフォームでは、工場出荷時の設定により、BVI が、最高セキュリティ レベル インターフェイスを示す 100 に設定され（メンバー インターフェイスもレベル 100 に設定）、外部インターフェイスのセキュリティ レベルが 0 になっています。Easy VPN はデフォルトでこれらのインターフェイスを選択します。

仮想インターフェイス（ブリッジ型仮想インターフェイスまたは BVI）が起動時に選択されると、または管理者によって内部のセキュアなインターフェイスとして割り当てられると、次の内容が適用されます。

- すべての BVI メンバー インターフェイスは、自身のセキュリティ レベルに関係なく、内部のセキュアなインターフェイスであるとみなされます。
- ACL および NAT ルールをすべてのメンバー インターフェイスに追加する必要があります。AAA ルールは BVI インターフェイスのみに追加されます。

Easy VPN の接続

Easy VPN は IPsec IKEv1 トンネルを使用します。Easy VPN リモート ハードウェア クライアントの設定は、Easy VPN サーバ ヘッドエンドの VPN の設定と互換性を保つようにする必要があります。セカンダリ サーバを使用する場合は、それらの設定をプライマリ サーバと同じにする必要があります。

ASA Easy VPN リモートはプライマリ Easy VPN サーバの IP アドレスを設定し、必要に応じて、最大 10 台のセカンダリ（バックアップ）サーバを設定します。これらのサーバを設定するには、グローバル コンフィギュレーション モードで **vpnclient server** コマンドを使用します。 プライマリ サーバへのトンネルをセットアップできない場合、クライアントは最初のセカンダリ VPN サーバへの接続を試み、次に VPN サーバのリストの上から順に 8 秒間隔で接続を試行します。最初のセカンダリ VPN サーバへのトンネルをセットアップできず、その間にプライマリ サーバがオンライン状態になった場合、クライアントは、引き続き 2 番目のセカンダリ VPN サーバへのトンネルのセットアップを試みます。

デフォルトでは、Easy VPN ハードウェア クライアントとサーバは IPSec をユーザ データグラム プロトコル（UDP）パケット内でカプセル化します。一部の環境（特定のファイアウォール ルールが設定されている環境など）または NAT デバイスや PAT デバイスでは、UDP を使用できません。そのような環境で標準のカプセル化セキュリティ プロトコル（ESP、プロトコル

50）またはインターネット キー エクスチェンジ（IKE、UDP 500）を使用するには、TCP パケット内に IPsec をカプセル化してセキュアなトンネリングをイネーブルにするようにクライアントとサーバを設定します。これを設定するには、**vpnclient ipsec-over-tcp** コマンドを使用します。 ただし、UDP が許可されている環境では、IPsec over TCP を設定すると不要なオーバーヘッドが発生します。

Easy VPN トンネル グループ

トンネルの確立後、Easy VPN リモートは Easy VPN サーバで設定されたトンネル グループを指定し、これを接続に使用します。Easy VPN サーバは、トンネルの動作を決定する Easy VPN リモート ハードウェア クライアントにグループ ポリシーまたはユーザ属性をプッシュします。特定の属性を変更するには、プライマリまたはセカンダリ Easy VPN サーバとして設定されている ASA でその属性を変更する必要があります。

Easy VPN リモート クライアントは、**vpnclient vpngroup** コマンドを使用してグループ ポリシーを指定し、その名前と事前共有鍵を設定します。または、**vpnclient trustpoint** コマンドを使用して、事前設定されているトラストポイントを指定します。

Easy VPN モードの動作

企業ネットワークからトンネル経由で Easy VPN リモートの背後にあるホストにアクセスできるかどうは、モードによって決まります。

- クライアント モードはポート アドレス変換（PAT）モードとも呼ばれ、Easy VPN リモート プライベート ネットワーク上のすべてのデバイスを、企業ネットワークのデバイスから分離します。Easy VPN リモートは、内部ホストのすべての VPN トラフィックに対してポート アドレス変換（PAT）を実行します。Easy VPN リモートのプライベート側のネットワークとアドレスは非表示になっており、直接アクセスすることはできません。Easy VPN クライアントの内部インターフェイスまたは内部ホストに対して、IP アドレスの管理は必要ありません。
- ネットワーク拡張モード（NEM）は、内部インターフェイスとすべての内部ホストが、トンネルを介して企業ネットワーク全体にルーティングできるようにします。内部ネットワークのホストは、スタティック IP アドレスで事前設定されたアクセス可能なサブネット（スタティックまたは DHCP を介して）から IP アドレスを取得します。NEM では、PAT は VPN トラフィックに適用されません。このモードでは、内部ネットワークのホストごとの VPN 設定やトンネルは必要ありません。Easy VPN リモートによってすべてのホストにトンネリングが提供されます。

Easy VPN サーバはデフォルトでクライアント モードになります。NEM モードを設定するには、グループ ポリシー コンフィギュレーション モードで **nem enable** コマンドを使用します。Easy VPN リモートにはデフォルト モードがないため、トンネルを確立する前に、必ず、Easy VPN リモートにいずれかの動作モードを指定する必要があります。PAT または NEM を設定するには、Easy VPN リモートで **vpnclient mode** コマンドを使用します。

（注） NEM モード用に設定された Easy VPN リモート ASA は、自動トンネル起動をサポートしています。自動起動には、トンネルのセットアップに使用するクレデンシャルの設定とストレージが必要です。セキュアユニット認証がイネーブルの場合は、トンネルの自動開始がディセーブルになります。

複数のインターフェイスが設定されているネットワーク拡張モードの Easy VPN リモートは、最もセキュリティレベルが高いインターフェイスからのローカルに暗号化されたトラフィックに対してのみトンネルを構築します。

Easy VPN ユーザ認証

ASA Easy VPN リモートは、**vpnclient username** コマンドを使用して、自動ログイン用にユーザ名とパスワードを保存できます。

セキュリティを強化するために、Easy VPN サーバは以下を要求できます。

- セキュアユニット認証（SUA）：設定されているユーザ名およびパスワードを無視して、ユーザに手動による認証を要求します。デフォルトでは、SUA はディセーブルになっており、**secure-unit-authentication enable** コマンドを使用して、Easy VPN サーバで SUA をイネーブルにします。
- 個別ユーザ認証（IUA）：Easy VPN リモートの背後にいるユーザは、企業 VPN ネットワークへのアクセス権限を得るために、ユーザ認証を受ける必要があります。デフォルトでは、IUA はディセーブルになっており、**user-authentication enable** コマンドを使用して、Easy VPN サーバで IUA をイネーブルにします。

  IUA を使用する場合は、ハードウェア クライアントの背後にある特定のデバイス（Cisco IP Phone やプリンタなど）が個々のユーザ認証をバイパスできるようにする必要があります。これを設定するには、Easy VPN サーバで **ip-phone-bypass** コマンドを使用して IP Phone Bypass を指定し、Easy VPN リモートで **mac-exempt** コマンドを使用して MAC アドレス免除を指定します。

  さらに、Easy VPN サーバは、クライアントのアクセスを終了させるまでのアイドル タイムアウト時間を設定または削除できます。これを行うには、Easy VPN サーバで **user-authentication-idle-timeout** コマンドを使用します。

ユーザ名とパスワードが設定されていない場合、SUA がディセーブルになっている場合、または IUA がイネーブルになっている場合、Cisco Easy VPN サーバは HTTP トラフィックを代行受信し、ユーザをログイン ページにリダイレクトします。HTTP リダイレクションが自動で、Easy VPN サーバ上のコンフィギュレーションが必要ない。

リモート 管理

Easy VPN リモート ハードウェア クライアントとして動作する ASA は、さらに IPsec 暗号化されるかどうかにかかわらず、SSH または HTTPS を使用して管理アクセスをサポートします。

デフォルトでは、管理トンネルは、SSH または HTTPS 暗号化で IPsec 暗号化を使用します。IPsec 暗号化レイヤをクリアすると、VPN トンネルの外部に管理アクセスできます。これを行うには、**vpnclient management clear** コマンドを使用します。トンネル管理をクリアしても、IPsec の暗号化レベルが削除されるだけで、SSH や HTTPS など、その接続に存在する他の暗号化には影響しません。

セキュリティを強化するために、Easy VPN リモートは、IPsec 暗号化および企業側の特定のホストまたはネットワークへの管理アクセスの制限を要求できます。これを行うには、グローバル コンフィギュレーション モードで **vpnclient management tunnel** コマンドを使用します。

デフォルトのリモート管理操作に戻すには、**no vpnclient management** を使用します。

（注） NAT デバイスが ASA Easy VPN リモートとインターネットの間で動作している場合は、ASA Easy VPN リモート上に管理トンネルを設定しないでください。そのような設定では、**vpnclient management clear** コマンドを使用して、リモート管理をクリアしてください。

コンフィギュレーションにかかわらず、DHCP 要求（更新メッセージを含む）は IPSec トンネル上を流れません。vpnclient management tunnel を使用しても、DHCP トラフィックは許可されません。

Easy VPN リモートの設定

始める前に

Easy VPN リモートの設定に必要な次の情報を取得します。

- プライマリ Easy VPN サーバのアドレスと、セカンダリ サーバのアドレスのアドレス（セカンダリ サーバを使用できる場合）。
- Easy VPN リモートを動作させるアドレッシング モード（クライアントまたは NEM）。
- Easy VPN サーバ グループ ポリシーの名前とパスワード（事前共有鍵）、または目的のグループ ポリシーを選択して認証する事前設定されたトラストポイント。
- Easy VPN サーバに設定されている、VPN トンネルの使用を許可されたユーザ。
- リモート管理インターフェイスに対して BVI インターフェイスが使用されている場合、そのインターフェイスで **management-access** を設定する必要があります。

手順

ステップ 1 Easy VPN サーバのアドレスを入力します。

vpnclient server *ip-primary* [*ip-secondary-1... ip-secondary-n*]

- *ip_primary_address*：プライマリ Easy VPN サーバの IP アドレスまたは DNS 名。

- *ip-secondary-n*（任意）：最大 10 台のバックアップ Easy VPN サーバの IP アドレスまたは DNS 名のリスト。スペースを使用して、リスト内の項目を区切ります。

例：

```
asa(config)#vpnclient server 10.10.10.15 10.10.10.30 192.168.10.10
```

ステップ 2 （任意） 自動的に選択されたデフォルトのインターフェイスが望ましくない場合は、内部セキュア インターフェイスを再割り当てします。

起動時に最もセキュリティ レベルが高い物理インターフェイスまたはBVIがセキュアなリソースへの内部接続に使用されます。別のインターフェイスを使用する場合は、**vpnclient secure interface** *interface-name* コマンドを使用します。物理または仮想インターフェイスを割り当てることができます。

ステップ 3 動作モードを指定します。

vpnclient mode {**client-mode** | **network-extension-mode**}

- **client-mode**：ポートアドレス変換（PAT）モードを使用して、クライアントに関連する内部ホストのアドレスを企業ネットワークから分離します。
- **network-extension-mode**：内部ホストのアドレスは、企業ネットワークからアクセス可能です。

例：

```
asa(config)#vpnclient mode network-extension-mode
```

ステップ 4 （任意） 必要な場合は、TCP カプセル化 IPsec を使用するように Easy VPN ハードウェア クライアントを設定します。

vpnclient ipsec-over-tcp [**port** *tcp_port*]

指定されていない場合、Easy VPN ハードウェア クライアントはポート 10000 を使用します。

TCP カプセル化 IPsec を使用するように Easy VPN リモートを設定する場合は、**crypto ipsec df-bit clear-df outside** コマンドを入力して、カプセル化ヘッダーから Don't Fragment（DF）ビットをクリアします。DF ビットは、パケットを断片化できるかどうかを決定する IP ヘッダー内のビットです。このコマンドを使用すると、Easy VPN ハードウェア クライアントは MTU サイズよりも大きいパケットを送信できます。

例：

ポート 10501 で TCP カプセル化 IPsec を使用するように Easy VPN ハードウェア クライアントを設定し、外部インターフェイスを介して大きなパケットを送信できるようにします。

```
hostname(config)# vpnclient ipsec-over-tcp port 10501
hostname(config)# crypto ipsec df-bit clear-df outside
```

ステップ 5 次のいずれかの方法を使用して、Easy VPN サーバで設定されているトンネル グループを特定します。

- Easy VPN サーバ グループ ポリシーの名前とパスワード（事前共有鍵）を指定します。

vpnclient vpngroup *group_name***password** *preshared_key*

- *group_name*：Easy VPN サーバ上に設定された VPN トンネル グループの名前。接続を確立する前に、このトンネル グループをサーバ上に設定する必要があります。
- *preshared_key*：Easy VPN サーバで認証に使用される IKE 事前共有キー。

たとえば、次のコマンドを入力して、TestGroup1 と呼ばれる VPN トンネル グループと IKE 事前共有キー my_key123 を指定します。

```
hostname(config)# vpnclient vpngroup TestGroup1 password my_key123
hostname(config)#
```

- グループ ポリシーを選択して認証する事前設定されたトラストポイントを指定します。

  vpnclient trustpoint *trustpoint_name* [**chain**]

  - *trustpoint_name*：認証に使用する RSA 証明書を識別するトラストポイントを指定します。
  - **chain**（任意）：証明書チェーン全体を送信します。

  たとえば、次のコマンドを入力して central という名前の証明書を指定し、証明書チェーン全体を送信します。

```
hostname(config)# crypto ca trustpoint central
hostname(config)# vpnclient trustpoint central chain
hostname(config)#
```

ステップ 6 グループ ポリシーで NEM とスプリット トンネルが設定されている場合は、自動接続するように VPN トンネルを設定します。

vpnclient nem-st-autoconnect

ステップ 7 （任意） Easy VPN サーバのグループ ポリシーで個別ユーザ認証（IAU）と IP Phone Bypass が設定されている場合は、Cisco IP phone、ワイヤレス アクセスポイント、プリンタなどのデバイスには認証機能がないため、それらの認証を免除します。

vpnclient mac-exempt *mac_addr_1 mac_mask_1* [*mac_addr_2 mac_mask_2...mac_addr_n mac_mask_n*]

- アドレスのリストは 15 以下でなければなりません。
- *mac_addr*：個別ユーザ認証をバイパスするデバイスの MAC アドレス（ドット付きの 16 進数で表記）。
- *mac_mask*：対応する MAC アドレスのネットワーク マスク。

  MAC マスク ffff.ff00.0000 は、同一の製造業者が製造したすべてのデバイスに対応します。MAC マスク ffff.ffff.ffff は 1 つのデバイスに対応します。

  同じ製造業者のすべてのデバイスを MAC マスク ffff.ff00.0000 を使用して指定する場合は、特定の MAC アドレスの最初の 6 文字だけが必要です。

例：

Cisco IP Phone には、製造業者 ID として 00036b が設定されています。したがって、次のコマンドは、今後追加される可能性がある Cisco IP Phone も含めてすべての Cisco IP Phone を免除します。

```
hostname(config)# vpnclient mac-exempt 0003.6b00.0000 ffff.ff00.0000
hostname(config)#
```

（注） 次のように、個別ユーザ認証と IP Phone Bypass を Easy VPN サーバ グループ ポリシーに設定する必要があります。

```
hostname(config-group-policy)#user-authentication enable
hostname(config-group-policy)#ip-phone-bypass enable
```

ステップ 8 自動 Xauth ユーザ ログイン クレデンシャルを設定します。

vpnclient username *username***password** *password*

ステップ 9 （任意） Easy VPN リモートのリモート監視を設定します。

デフォルトでは、管理トンネルは、SSH または HTTPS 暗号化で IPsec 暗号化を使用します。IPsec 暗号化を削除するか、またはこの暗号化を保持して特定のホストにのみ ASA の管理を許可するには、次のコマンドのいずれかを使用します。

- **vpnclient management clear**

  IPsec 暗号化レイヤをクリアして、VPN トンネル外部への管理アクセスを許可します。

- **vpnclient management tunnel ip_addr_1 ip_mask_1** [*ip_addr_2 ip_mask_2...ip_addr_n ip_mask_n*]

例：

次のコマンドを入力して IPSec トンネルの作成を自動化し、IP アドレス 192.168.10.10 のホストに管理アクセス権限を与えます。

```
hostname(config)# vpnclient management tunnel 192.198.10.10 255.255.255.0
```

（注） NAT デバイスが ASA Easy VPN リモートとインターネットの間で動作している場合は、ASA Easy VPN リモート上に管理トンネルを設定しないでください。そのような設定では、**vpnclient management clear** コマンドを使用して、リモート管理をクリアしてください。

ステップ 10 ASA で Easy VPN ハードウェア クライアントをイネーブルにします。

vpnclient enable

Easy VPN リモートをイネーブルにする前に、サーバ アドレス、モード、およびトンネル グループの仕様を設定する必要があります。

ステップ 11 （任意） 構成で Easy VPN トンネルが必要な場合は、手動で Easy VPN トンネルを接続します。

vpnclient connect

Easy VPN サーバの設定

始める前に

すべてのセカンダリ Easy VPN サーバに、プライマリ Easy VPN サーバと同じオプションと設定が指定されていることを確認します。

手順

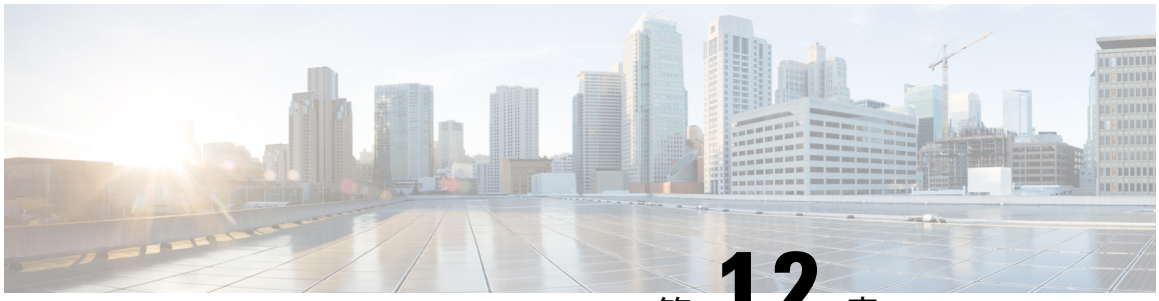
ステップ 1 IPsec IKEv1 のサポート用に Easy VPN サーバを設定します。接続プロファイル、グループ ポリシー、およびユーザ （111 ページ） を参照してください。

ステップ 2 特定の Easy VPN サーバ属性を設定します。VPN ハードウェア クライアントの属性の設定 （190 ページ） を参照してください。

Easy VPN の機能の履歴

機能名	リリース	機能情報
ASA 5506-X、5506W-X、5506H-X および 5508-X の Cisco Easy VPN クライアント	9.5(1)	このリリースは、ASA 5506-X シリーズでの Cisco Easy VPN の使用をサポートし、かつ ASA 5508-X 用の Cisco Easy VPN をサポートします。ASA は、VPN ヘッドエンドに接続すると VPN ハードウェア クライアントとして機能します。ASA の背後にある Easy VPN ポート上のデバイス（コンピュータ、プリンタなど）は、VPN 経由で通信できます。個別に VPN クライアントを実行する必要はありません。ASA インターフェイス 1 つのみで Easy VPN ポートとして機能できます。このポートに複数のデバイスを接続するには、レイヤ 2 スイッチをこのポート上に配置してから、このスイッチにデバイスを接続します。 次のコマンドが導入されました。**vpnclient enable**、**vpnclient server**、**vpnclient mode**、**vpnclient username**、**vpnclient ipsec-over-tcp**、**vpnclient management**、**vpnclient vpngroup**、**vpnclient trustpoint**、**vpnclient nem-st-autoconnect**、**vpnclient mac-exempt**

機能名	リリース	機能情報
BVI サポートのための Easy VPN 拡張	9.9(2)	Easy VPN は、ブリッジ型仮想インターフェイスを内部セキュア インターフェイスとしてサポートするように拡張され、管理者は新しい **vpnclient secure interface** [*interface-name*] コマンドを使用して内部セキュア インターフェイスを直接設定できるようになりました。 物理インターフェイスまたはブリッジ型仮想インターフェイスを内部セキュア インターフェイスとして割り当てることができます。これが管理者によって設定されていない場合、Easy VPN はそれが独立した物理インターフェイスまたは BVI かに関わらず、以前と同じセキュリティ レベルを使用してその内部セキュア インターフェイスを選択します。 また、管理アクセスがその BVI で有効になっている場合、**telnet**、**http**、**ssh** などの管理サービスを BVI で設定できるようになりました。 新規または変更されたコマンド：**vpnclient secure interface** [*interface-name*]、**https**、**telnet**、**ssh**、**management-access**



第 12 章

仮想トンネル インターフェイス

この章では、VTI トンネルの設定方法について説明します。

仮想トンネル インターフェイスについて

ASA は、仮想トンネルインターフェイス（VTI）と呼ばれる論理インターフェイスをサポートします。ポリシー ベース VPN の代替策として、仮想トンネル インターフェイスが設定されたピア間に VPN トンネルを作成することができます。これは、各トンネルの終端に IPsec プロファイルが付加されたルートベースの VPN をサポートします。これは、動的または静的なルートの使用が可能です。VTI からの出力トラフィックは暗号化されてピアに送信され、VTI への入力トラフィックは関連付けされた SA によって復号化されます。

VTI を使用することにより、静的暗号マップのアクセス リストを設定してインターフェイスにマッピングすることが不要になります。すべてのリモート サブネットを追跡し、暗号マップのアクセスリストに含める必要がなくなります。展開が簡単になるほか、ダイナミック ルーティング プロトコルのルート ベースの VPN をサポートする静的 VTI があると、仮想プライベート クラウドの多くの要件を満たすこともできます。

仮想トンネル インターフェイスの注意事項

IPv6

- IPv6 はサポートされていません。

一般的な設定時の注意事項

- VTI は IPsec モードのみで設定可能です。ASA で GRE トンネルを終了することはサポートされていません。

- トンネルインターフェイスを使用するトラフィックには、動的または静的なルートを使用することができます。
- VTI の MTU は、基盤となる物理インターフェイスに応じて自動的に設定されます。
- ネットワーク アドレス変換を適用する必要がある場合、IKE および ESP パケットは、UDP ヘッダーにカプセル化されます。
- IKE および IPsec のセキュリティ アソシエーションには、トンネル内のデータ トラフィックに関係なく、継続的にキーの再生成が行われます。これにより、VTI トンネルは常にアップした状態になります。
- トンネル グループ名は、ピアが自身の IKEv1 識別情報として送信するものと一致する必要があります。
- トンネル グループ名は、ピアが自身の IKEv1 または IKEv2 識別情報として送信するものと一致する必要があります。
- LAN-to-LAN トンネル グループの IKEv1 では、トンネルの認証方式がデジタル証明書である場合、かつ/またはピアがアグレッシブ モードを使用するように設定されている場合、IP アドレス以外の名前を使用できます。
- 暗号マップに設定されるピア アドレスと VTI のトンネル宛先が異なる場合、VTI 設定と暗号マップの設定を同じ物理インターフェイスに共存させることができます。
- デフォルトでは、VTI 経由のトラフィックは、すべて暗号化されます。
- VTI インターフェイスにはセキュリティ レベル設定はありません。
- VTI 経由のトラフィックを制御するため、VTI インターフェイスにアクセス リストを適用することができます。
- VTI では BGP のみサポートされます。

コンテキスト モード

シングル モードでだけサポートされています。

ファイアウォール モード

ルーテッド モードのみでサポートされます。

VTI トンネルの作成

VTI トンネルを設定するには、IPsec プロポーザル（トランスフォーム セット）を作成します。IPsec プロポーザルを参照する IPsec プロファイルを作成した後で、IPsec プロファイルを持つ VTI インターフェイスを作成します。リモートピアには、同じ IPsec プロポーザルおよび IPsec プロファイル パラメータを設定します。SA ネゴシエーションは、すべてのトンネル パラメータが設定されると開始します。

（注） VPN および VTI ドメインの両方に属し、物理インターフェイス上で BGP 隣接関係を持つ ASA では、次の動作が発生します。

インターフェイスヘルスチェックによって状態の変更がトリガーされると、物理インターフェイスでのルートは、新しいアクティブなピアとの BGP 隣接関係が再確立されるまで削除されます。この動作は、論理 VTI インターフェイスには該当しません。

手順

ステップ 1 IPsec プロポーザル（トランスフォーム セット）を追加します。

ステップ 2 IPsec プロファイルを追加します。

ステップ 3 VTI トンネルを追加します。

IPsec プロポーザル（トランスフォーム セット）の追加

トランスフォームセットは、VTI トンネル内のトラフィックを保護するために必要です。これは、VPN 内のトラフィックを保護するためのセキュリティ プロトコルとアルゴリズムのセットであり、IPsec プロファイルの一部として使用されます。

始める前に

- VTI に関連付けられた IKEv1 セッションを認証するには、事前共有キーまたは証明書のいずれかを使用できます。事前共有キーは、VTI に使用するトンネル グループの下に設定する必要があります。
- IKEv1 を使用しての証明書ベースの認証には、イニシエータで使用されるトラストポイントを指定する必要があります。レスポンダについては、tunnel-group コマンドでトラストポイントを設定する必要があります。
- VTI に関連付けられた IKE セッションを認証するには、事前共有キーまたは証明書のいずれかを使用できます。IKEv2 では、非対称認証方式とキーが使用できます。IKEv1 と IKEv2 のどちらも、VTI に使用するトンネル グループの下に事前共有キーを設定する必要があります。
- IKEv1 を使用しての証明書ベースの認証には、イニシエータで使用されるトラストポイントを指定する必要があります。レスポンダについては、tunnel-group コマンドでトラストポイントを設定する必要があります。IKEv2 では、イニシエータとレスポンダ両方について、認証に使用するトラストポイントを tunnel-group コマンドで設定する必要があります。

手順

セキュリティ アソシエーションを確立するための IKEv1 トランスフォーム セットまたは IKEv2 IPsec プロポーザルを追加します。

IKEv1 トランスフォーム セットを追加します。

crypto ipsec ikev1 transform-set {*transform-set-name* | *encryption* | *authentication*}

例：

```
ciscoasa(config)#crypto ipsec ikev1 transform-set SET1 esp-aes esp-sha-hmac
```

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。

IKEv2 IPsec プロポーザルを追加します。

（注） IOS プラットフォームについては、IKEv2 プロファイル コンフィギュレーション モードで **no config-exchange request** コマンドを使用し、設定の交換のオプションをディセーブルにします。詳細については、「http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/a1/sec-a1-cr-book/sec-cr-c2.html#wp3456426280」を参照してください。

- IPsec プロポーサルの名前を指定します。

  crypto ipsec ikev2 ipsec-proposal *IPsec proposal name*

例：

```
ciscoasa(config)#crypto ipsec ikev2 ipsec-proposal SET1
```

- crypto IPsec ikev2 ipsec-proposal コンフィギュレーション モードで、セキュリティ パラメータを指定します。

  protocol esp {encryption {des | 3des | aes | aes-192 | aes-256 | aes-gcm | aes-gcm-192 | aes-gcm-256 | aes-gmac | aes-gmac-192 | aes-gmac-256 | null} | integrity {md5 | sha-1 | sha-256 | sha-384 | sha-512 | null}

例：

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

IPsec プロファイルの追加

IPsec プロファイルには、その参照先の IPsec プロポーザルまたはトランスフォーム セット内にある必要なセキュリティ プロトコルおよびアルゴリズムが含まれています。これにより、2 つのサイト間 VTI VPN ピアの間でセキュアな論理通信パスが確保されます。

手順

ステップ 1 プロファイル名を設定します。

crypto ipsec profile *name*

例：

```
ciscoasa(config)#crypto ipsec profile PROFILE1
```

ステップ 2 IKEv1 または IKEv2 プロポーザルを設定します。IKEv1 トランスフォーム セットまたは IKEv2 IPsec プロポーザルのいずれかを選択できます。

a) IKEv1 トランスフォーム セットを設定します。

- IKEv1 プロポーザルを設定するには、crypto ipsec profile コマンド サブモードで次のコマンドを入力します。

  set ikev1 transform set *set_name*

  この例の SET1 は、以前に作成された IKEv1 プロポーザル セットです。

  ```
  ciscoasa(config-ipsec-profile)#set ikev1 transform-set SET1
  ```

b) IKEv2 プロポーザルを設定します。

- IKEv2 プロポーザルを設定するには、crypto ipsec profile コマンド サブモードで次のコマンドを入力します。

  set ikev2 ipsec-proposal *IPsec_proposal_name*

  この例では、SET1 は、以前に作成された IKEv2 IPsec プロポーザルです。

  ```
  ciscoasa(config-ipsec-profile)#set ikev2 ipsec-proposal SET1
  ```

ステップ 3 （任意）セキュリティ アソシエーションの期間を指定します。

set security-association lifetime {**seconds** *number* | **kilobytes** {*number* | **unlimited**}}

例：

```
ciscoasa(config-ipsec-profile)#set security-association lifetime
seconds 120 kilobytes 10000
```

ステップ 4 （任意）VTI トンネルの一端をレスポンダとしてのみ動作するように設定します。

responder-only

- VTI トンネルの一端をレスポンダとしてのみ動作するように設定できます。レスポンダのみの端は、トンネルまたはキー再生成を開始しません。
- IKEv2 を使用する場合、セキュリティ アソシエーションのライフタイム期間は、イニシエータ側の IPsec プロファイルのライフタイム値より大きく設定します。こうすることで、イニシエータ側での正常なキー再生成が促進され、トンネルのアップ状態が保たれます。
- イニシエータ側のキー再生成の設定が不明の場合、レスポンダのみのモードを解除して SA の確立を双方向にするか、レスポンダのみの端の IPsec ライフタイム値を無期限にして期限切れを防ぎます。

ステップ 5 （任意）PFS グループを指定します。Perfect Forward Secrecy（PFS）は、暗号化された各交換に対し、一意のセッション キーを生成します。この一意のセッション キーにより、交換は、後続の復号化から保護されます。PFS を設定するには、PFS セッション キーを生成する際に使用する Diffie-Hellman キー導出アルゴリズムを選択する必要があります。キー導出アルゴリズムは、IPsec セキュリティ アソシエーション（SA）キーを生成します。各グループでは、異なるサイズの係数が使用されます。係数が大きいほどセキュリティが強化されますが、処理時間が長くなります。Diffie-Hellman グループは、両方のピアで一致させる必要があります。

set pfs {**group1** | **group2** | **group5**}

例：

```
ciscoasa(config-ipsec-profile)#set pfs group2
```

ステップ 6 （任意）VTI トンネル接続の開始時に使用する証明書を定義するトラストポイントを指定します。

set trustpoint *name*

例：

```
ciscoasa(config-ipsec-profile)#set trustpoint TPVTI
```

VTI インターフェイスの追加

新しい VTI インターフェイスを作成して VTI トンネルを確立するには、次の手順を実行します。

（注） アクティブなトンネル内のルータが使用できないときにトンネルをアップした状態に保つため、IP SLA を実装します。http://www.cisco.com/go/asa-config の『ASA General Operations Configuration Guide』の「Configure Static Route Tracking」を参照してください。

手順

ステップ 1 新しいトンネル インターフェイスを作成します。

interface tunnel *tunnel_interface_number*

例：

```
ciscoasa(config)#interface tunnel 100
```

トンネル ID を 0 ～ 100 の範囲で指定します。最大 100 の VTI インターフェイスがサポートされます。

（注） 他のデバイスから ASA 5506 に設定を移行する場合は、トンネル ID 範囲に 1 ～ 100 を指定します。これは、ASA 5506 デバイスで使用可能なトンネル範囲 1 ～ 100 に対応させるためです。

ステップ 2 VTI インターフェイス の名前を入力します。

interface tunnel コマンド サブモードで、次のコマンドを入力します。

nameif *interface name*

例：

```
ciscoasa(config-if)#nameif vti
```

ステップ 3 VTI インターフェイスの IP アドレスを入力します。

ip address *IP addressmask*

例：

```
ciscoasa(config-if)#ip address 192.168.1.10 255.255.255.254
```

ステップ 4 トンネル送信元のインターフェイスを指定します。

tunnel source interface *interface name*

例：

```
ciscoasa(config-if)#tunnel source interface outside
```

ステップ 5 トンネル宛先の IP アドレスを指定します。

tunnel destination *IP address*

例：

```
ciscoasa(config-if)#tunnel destination 10.1.1.1
```

ステップ 6 トンネルにトンネル モード IPsec IPv4 を設定します。

tunnel mode ipsec *ipv4*

例：

```
ciscoasa(config-if)#tunnel mode ipsec ipv4
```

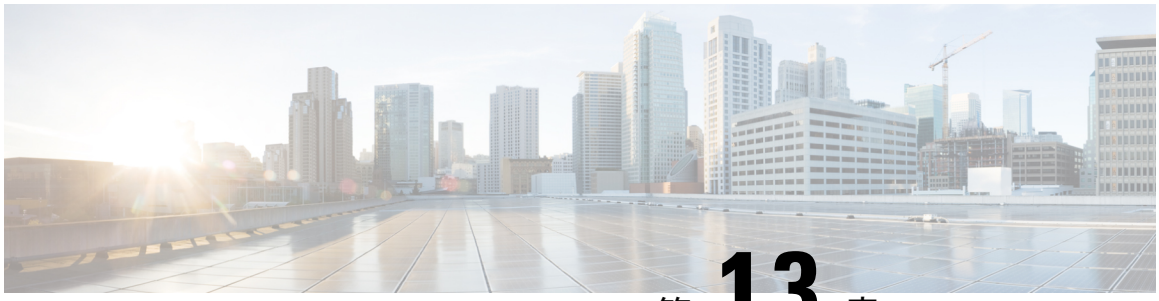
ステップ 7 トンネルに IPsec プロファイルを割り当てます。

tunnel protection ipsec *IPsec プロファイル*

例：

```
ciscoasa(config-if)#tunnel protection ipsec Profile1
```

この新しい VTI は、IPsec サイト間 VPN の作成に使用できます。



第 13 章

VPN の外部 AAA サーバの設定

外部 AAA サーバについて

この ASA は、外部の LDAP、RADIUS、TACACS+ サーバを使用して、ASA の認証、認可、アカウンティング（AAA）をサポートするように設定できます。外部 AAA サーバは、設定されたアクセス許可と属性を適用します。外部サーバを使用するように ASA を設定する前に、適切な ASA 許可属性を指定して外部 AAA サーバを設定し、それらの属性のサブセットから特定のアクセス許可を個々のユーザに割り当てる必要があります。

許可属性のポリシー適用の概要

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、それらの属性は評価されて集約され、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 は次の順序で属性を適用します。

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、他のど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 データベースで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）と混同しないようにしてください。
3. ASA で設定されているグループ ポリシー：RADIUS サーバからユーザに対して RADIUS CLASS 属性 IETF-Class-25 （OU=*group-policy*）の値が返された場合、ASA はそのユーザを同じ名前のグループ ポリシーに配置し、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 上に設定された 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 に接続してい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、DAP、サーバから返されるユーザ属性、ユーザに割り当てられているグループ ポリシーにはない属性が提供されます。
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、接続プロファイルで不足している値を提供します。

外部 AAA サーバを使用する際のガイドライン

ASA は、数値の ID ではなく属性名に基づいて LDAP 属性を適用します。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。

複数証明書認証の設定

AnyConnect SSL と IKEv2 クライアント プロトコルでセッションごとに複数の証明書を検証できるようになりました。複数証明書認証のためのプロトコル交換を定義し、両方のセッションタイプでこれを利用するように集約認証プロトコルが拡張されています。たとえば、マシン証明書の発行元が特定の CA と一致することでデバイスが企業から支給されたデバイスであることを確認できます。

複数証明書オプションを使用すると、証明書を通じたマシンとユーザ両方の証明書認証が可能になります。このオプションがなければ、両方ではなく一方のみの証明書認証しか行うことができません。

ユーザ名の事前入力フィールドでは、証明書のフィールドを解析し、AAA および証明書認証済みの接続で以降の AAA 認証に使用することができます。プライマリとセカンダリの両方の事前入力のユーザ名は、常にクライアントから受信した最初の証明書から取得されます。

複数証明書認証では、2 つの証明書が認証されます。クライアントから受信した最初の証明書は、事前入力および証明書由来のユーザ名のプライマリおよびセカンダリ ユーザ名による解析対象です。その後、1 番目と 2 番目にどの証明書が送信されるかを選択するクライアントのルールを設定できます。

既存の認証 webvpn 属性は、複数証明書認証のオプションを含めるように変更されます。

```
tunnel-group <name> webvpn-attributes
authentication {[aaa] [certificate | multiple-certificate] | saml}
```

複数証明書認証では、その接続試行を認証するために使用された証明書のフィールドに基づいてポリシー決定を行うことができます。複数証明書認証中にクライアントから受信したユーザおよびマシンの証明書は DAP にロードされ、証明書のフィールドに基づいてポリシーを設定することができます。接続試行を許可または拒否するルールを設定できるようにダイナミック アクセス ポリシー（DAP）を使用して複数証明書認証を追加するには、『ASA VPN ASDM Configuration Guide』の適切なリリースの「*Add Multiple Certificate Authentication to DAP*」を参照してください。

VPN の LDAP 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 サーバに対して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

ステップ 1 AAA サーバ グループを作成します。

aaa-server *server_group* **protocol** {**kerberos** | **ldap** | **nt** | **radius** | **sdi** | **tacacs+**}

例：

```
hostname(config)# aaa-server servergroup1 protocol ldap
hostname(config-aaa-server-group)
```

ステップ 2 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。

tunnel-group *groupname*

例：

```
hostname(config)# tunnel-group remotegrp
```

ステップ 3 サーバ グループとトンネル グループを関連付けます。

tunnel-group *groupname* **general-attributes**

例：

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

ステップ 4 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。

authorization-server-group *group-tag*

例：

```
hostname(config-general)# authorization-server-group ldap_dir_1
```

例

次に、LDAP を使用したユーザ許可を有効にするコマンドの例を示します。この例では、RAVPN 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 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 RAVPN type remote-access
hostname(config)# tunnel-group RAVPN general-attributes
hostname(config-general)# authorization-server-group (inside) LDAP
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 protocol ldap
hostname(config-aaa-server-group)# aaa-server LDAP (inside) host 10.0.2.128
hostname(config-aaa-server-host)# ldap-base-dn DC=AD,DC=LAB,DC=COM
hostname(config-aaa-server-host)# ldap-group-base-dn DC=AD,DC=LAB,DC=COM
hostname(config-aaa-server-host)# ldap-scope subtree
hostname(config-aaa-server-host)# ldap-login-dn AD\cisco
hostname(config-aaa-server-host)# ldap-login-password cisco123
hostname(config-aaa-server-host)# ldap-over-ssl enable
hostname(config-aaa-server-host)# server-type microsoft
```

Active Directory/LDAP VPN リモート アクセス許可の例

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』
- 『PIX/ASA 8.0: Use LDAP Authentication to Assign a Group Policy at Login』

ユーザ ベースの属性のポリシー適用

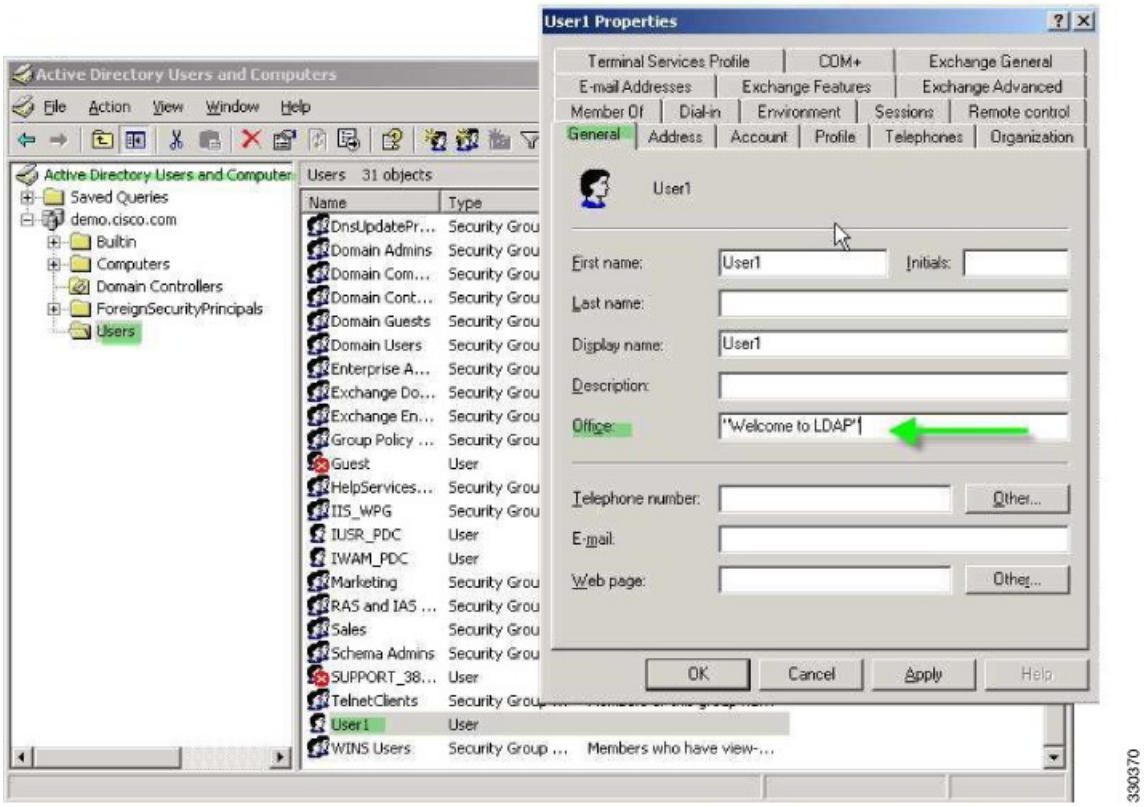
この例では、ユーザ向けの簡易バナーを表示して、標準の LDAP 属性を既知のベンダー固有属性（VSA）にマッピングする方法と 1 つ以上の LDAP 属性を 1 つ以上の Cisco LDAP 属性にマッピングする方法を示します。この例は、IPsec VPN クライアント、AnyConnect SSL VPN クライアント、クライアントレス SSL VPN など、どの接続タイプにも適用されます。

AD LDAP サーバ上で設定されたユーザに簡易バナーを適用するには、[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。

認証時、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。

手順

ステップ 1 ユーザ名を右クリックして、[Properties] ダイアログボックスの [General] タブを開き、AD/LDAP 属性 physicalDeliveryOfficeName を使用する [Office] フィールドにバナー テキストを入力します。



ステップ 2 ASA で LDAP 属性マップを作成します。

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 3 LDAP 属性マップを AAA サーバに関連付けます。

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、以前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 4 バナーの適用をテストします。

特定のグループ ポリシーへの LDAP ユーザの配置

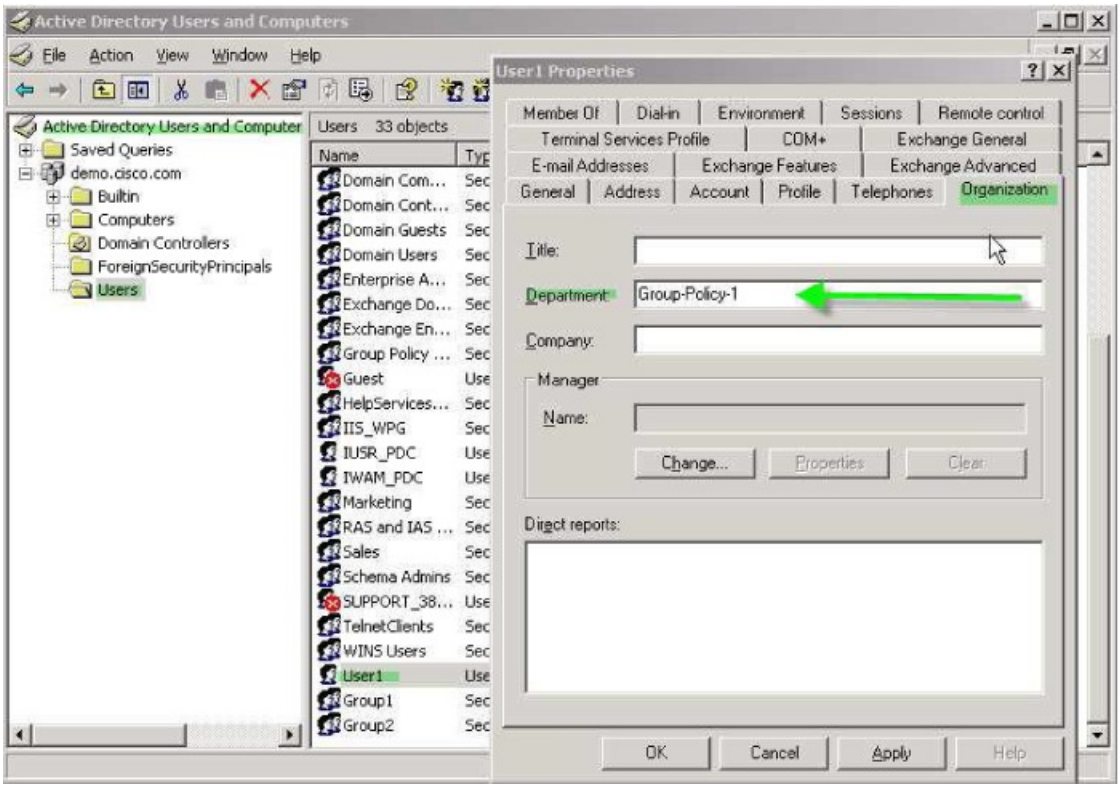
この例は、IPsec VPN クライアント、AnyConnect SSL VPN クライアント、クライアントレス SSL VPN など、どの接続タイプにも適用されます。この例では、User1 はクライアントレス SSL VPN 接続経由で接続します。

LDAP ユーザを特定のグループ ポリシーに配置するには、[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。

認証時、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。

手順

ステップ 1 ユーザ名を右クリックして、[Properties] ダイアログボックスの [Organization] タブを開き、[Department] フィールドに「**Group-Policy-1**」と入力します。



ステップ 2 LDAP コンフィギュレーションの属性マップを定義します。

AD 属性 Department を Cisco 属性 IETF-Radius-Class にマッピングします。

```
hostname(config)# ldap attribute-map group_policy
hostname(config-ldap-attribute-map)# map-name Department IETF-Radius-Class
```

ステップ 3 LDAP 属性マップを AAA サーバに関連付けます。

AAA サーバ グループ MS_LDAP のホスト 10.1.1.2 に対して 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、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 4 サーバの [Department] フィールドに入力されているグループ ポリシー *Group-policy-1* を ASA に追加し、ユーザに割り当てる必須ポリシー属性を設定します。

```
hostname(config)# group-policy Group-policy-1 external server-group LDAP_demo
hostname(config-aaa-server-group)#
```

ステップ 5 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 6 特権 EXEC モードで debug ldap 255**debug ldap 255**コマンドをイネーブルにして、ASA とサーバの間の通信をモニタします。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 トンネルのスタティック IP アドレス割り当ての適用

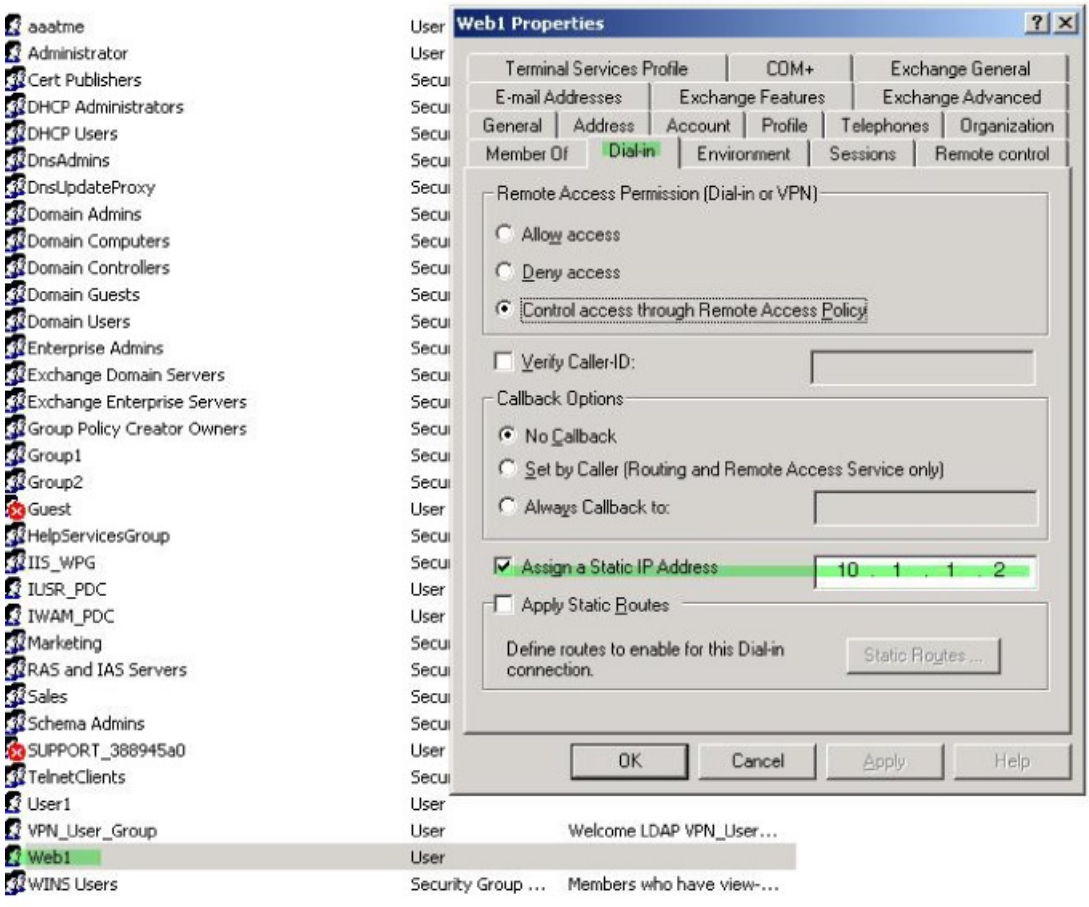
この例は、IPsec クライアントや SSL VPN クライアントなどのフルトンネル クライアントに適用されます。

スタティック AnyConnect スタティック IP 割り当てを適用するには、AnyConnect クライアント ユーザ Web1 をスタティック IP アドレスを受信するように設定して、そのアドレスを AD LDAP サーバの [Dialin] タブの [Assign Static IP Address] フィールド（このフィールドで msRADIUSFramedIPAddress 属性が使用される）に入力し、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 はサーバから msRADIUSFramedIPAddress の値を取得し、その値を Cisco 属性 IETF-Radius-Framed-IP-Address にマッピングして、User1 にスタティック アドレスを渡します。

手順

ステップ 1 ユーザ名を右クリックして、[Properties] ダイアログボックスの [Dial-in] タブを開き、[Assign Static IP Address] チェックボックスをオンにして、10.1.1.2 という IP アドレスを入力します。



ステップ 2 図に示す LDAP コンフィギュレーションの属性マップを作成します。

[Static Address] フィールドで使用される AD 属性 msRADIUSFramedIPAddress を Cisco 属性 IETF-Radius-Framed-IP-Address にマッピングします。

```
hostname(config)# ldap attribute-map static_address
hostname(config-ldap-attribute-map)# map-name msRADIUSFramedIPAddress
IETF-Radius-Framed-IP-Address
```

ステップ 3 LDAP 属性マップを AAA サーバに関連付けます。

AAA サーバ グループ MS_LDAP のホスト 10.1.1.2 に対して 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、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 4 vpn-address-assignment**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表示します。

```
hostname(config)# show run all vpn-addr-assign
vpn-addr-assign aaa    << Make sure this is configured >>
no vpn-addr-assign dhcp
vpn-addr-assign local
hostname(config)#
```

ステップ 5 ASA と AnyConnect クライアントとの接続を確立します。サーバで設定され、ASA にマッピングされた IP アドレスをユーザが受信することを確認します。

ステップ 6 show vpn-sessiondb svc**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
```

ダイヤルイン許可または拒否アクセスの適用

この例では、ユーザによって許可されるトンネリング プロトコルを指定する LDAP 属性マップを作成します。[Dialin] タブ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。この属性は次のビットマップ値をサポートします。

値	トンネリング プロトコル
1	PPTP
2	L2TP
4	IPsec（IKEv1）
8	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

値	トンネリング プロトコル
64	IPsec（IKEv2）

1 （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 （2）注 1 を参照。

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。

ダイヤルイン許可アクセスまたは拒否アクセスの適用に関するその他の例については、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。

手順

ステップ 1 ユーザ名を右クリックして、[Properties] ダイアログボックスの [Dial-in] タブを開き、[Allow Access] オプション ボタンをクリックします。

（注） [Control access through the Remote Access Policy] オプションを選択した場合は、サーバから値が返されず、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 2 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。

a) マップ tunneling_protocols を作成します。

```
hostname(config)# ldap attribute-map tunneling_protocols
```

b) [Allow Access] 設定で使用される AD 属性 msNPAllowDialin を Cisco 属性 Tunneling-Protocols にマッピングします。

```
hostname(config-ldap-attribute-map)# map-name msNPAllowDialin Tunneling-Protocols
```

c) マップ値を追加します。

```
hostname(config-ldap-attribute-map)# map-value msNPAllowDialin FALSE 48
hostname(config-ldap-attribute-map)# map-value msNPAllowDialin TRUE 4
```

ステップ 3 LDAP 属性マップを AAA サーバに関連付けます。

a) AAA サーバ グループ MS_LDAP でホスト 10.1.1.2 の AAA サーバ ホスト コンフィギュレーション モードを開始します。

```
hostname(config)# aaa-server MS_LDAP host 10.1.1.2
```

b) 作成した属性マップ tunneling_protocols を関連付けます。

```
hostname(config-aaa-server-host)# ldap-attribute-map tunneling_protocols
```

ステップ 4 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。

クライアントレス SSL を使用して接続を試みます。ユーザには、許可されていない接続メカニズムが接続の失敗の原因であることが通知されます。IPsec クライアントの接続は成功します。これは、属性マップに従って IPsec にトンネリング プロトコルが許可されるためです。

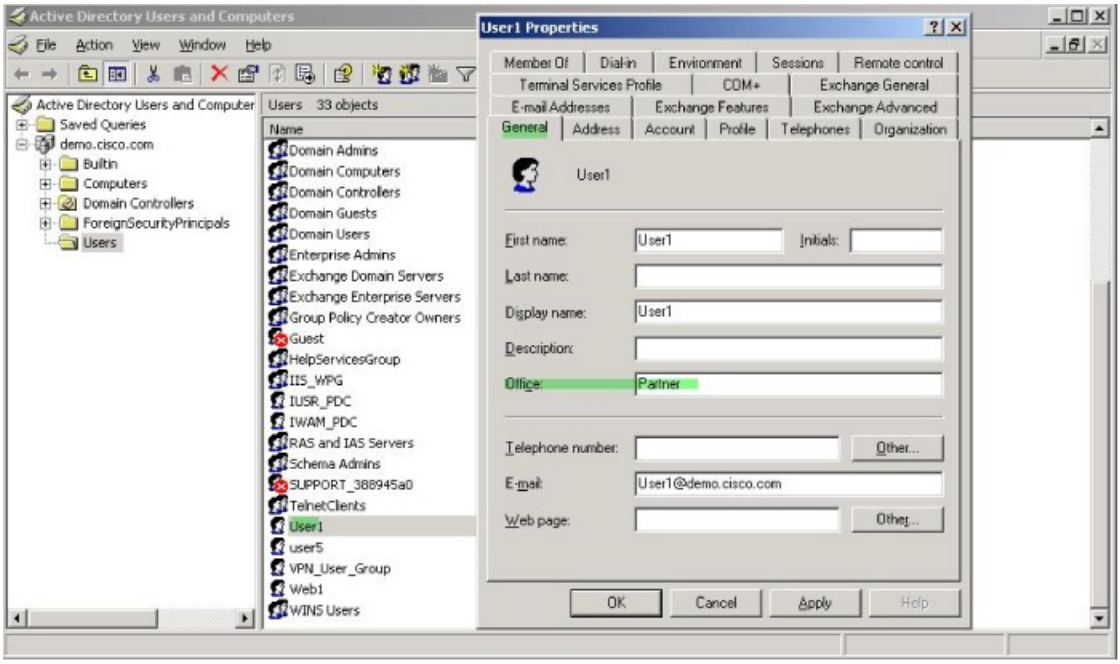
ログオン時間と Time-of-Day ルールの適用

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 physicalDeliveryOfficeName の値を取得して Access-Hours にマッピングします。

手順

ステップ 1 ユーザを選択して、[Properties] を右クリックし、[General] タブを開きます。



ステップ 2 属性マップを作成します。

属性マップ access_hours を作成し、[Office] フィールドで使用される AD 属性 physicalDeliveryOfficeName を Cisco 属性 Access-Hours にマッピングします。

```
hostname(config)# ldap attribute-map access_hours
hostname(config-ldap-attribute-map)# map-name physicalDeliveryOfficeName Access-Hours
```

ステップ 3 LDAP 属性マップを AAA サーバに関連付けます。

AAA サーバ グループ MS_LDAP のホスト 10.1.1.2 に対して 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、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
```

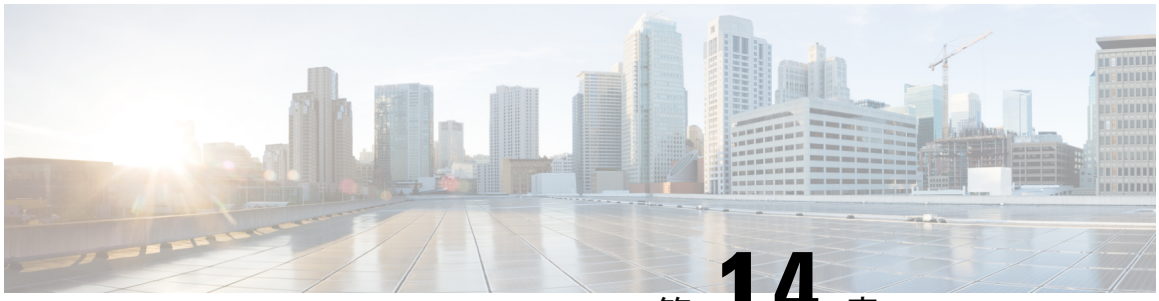
ステップ 4 各値にサーバで許可された時間範囲を設定します。

パートナー アクセス時間を月曜日から金曜日の午前 9 時から午後 5 時に設定します。

```
hostname(config)# time-range Partner
hostname(config-time-range)# periodic weekdays 09:00 to 17:00
```

第 II 部

クライアントレス SSL VPN



第 14 章

クライアントレス SSL VPN の概要

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 Active/Active 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。次の内容で構成されています。

- 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
- Microsoft Outlook Web Access Exchange Server 2000、2003、2007、および 2013。
- 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）プロトコルとその後継の Transport Layer Security（SSL/TLS1）を使用し、内部サーバとして設定されている特定のサポート対象内部リソースと、リモート ユーザとの間にセキュアな接続を実現します。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。

クライアントレス SSL VPN の前提条件

ASA 上のクライアントレス SSL VPN でサポートされるプラットフォームとブラウザについては、サポート対象の VPN プラットフォーム、Cisco ASA 5500 シリーズを参照してください。

クライアントレス SSL VPN に関する注意事項と制約事項

- 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にプロキシが指定されている場合、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。
- クライアントレス接続用に信頼できる証明書をインストールしても、クライアントには信頼できない証明書の警告が表示されることがあります。
- ASA は、クライアントレス SSL VPN 接続用の DSA 証明書をサポートしません。RSA 証明書はサポートされます。
- 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およびモジュラ ポリシー フレームワークのインスペクション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 の一部のコンポーネントには、Java Runtime Environment（JRE）が必要です。Mac OS X v10.7 以降では、Java はデフォルトでインストールされません。Mac OS X での Java のインストール方法については、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 VPN セッションを開始すると、RADIUS アカウンティング開始メッセージが生成されます。クライアントレス VPN セッションにはアドレスが割り当てられないため、開始メッセージには Framed-IP-Address が含まれません。レイヤ 3 VPN 接続がクライアントレス ポータル ページから順番に開始されるとアドレスが割り当てられ、暫定アップデート アカウンティング メッセージで RADIUS サーバに報告されます。weblaunch 機能を使用してレイヤ 3 VPN トンネルが確立される場合、同様の RADIUS の動作が期待できます。この状況では、ユーザが認証された後、レイヤ 3 トンネルが確立される前にアカウンティング開始メッセージがフレーム化 IP アドレスなしで送信されます。レイヤ 3 トンネルが確立されると、この開始メッセージに暫定アップデート メッセージが続きます。

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。

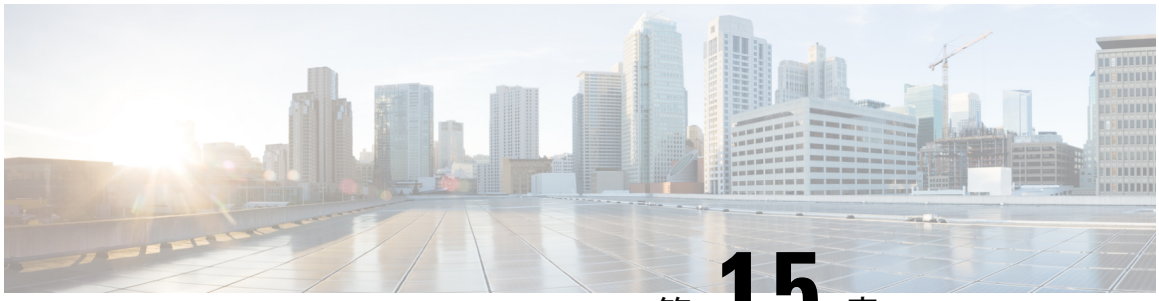
ヒント グループ ポリシーの名前をアルファベット順に付けることで、最初に表示されるポリシーを制御できます。また、ポリシーの先頭に数字を付けることもできます。たとえば、1-AAA、2-Certificate とします。

クライアントレス SSL VPN のライセンス

AnyConnect セキュア モビリティ クライアントを使用するには、AnyConnect Plus および Apex ライセンスを購入する必要があります。必要なライセンスは、使用する予定の AnyConnect VPN Client および Secure Mobility の機能と、サポートするセッションの数によって異なります。これらのユーザベースのライセンスには、一般的な BYOD のトレンドに合わせたサポートとソフトウェア更新へのアクセスが含まれます。

AnyConnect 4.4 ライセンスは、ASA（および ISR、CSR、ASR）で使用され、また、Identity Services Engine（ISE）、クラウド Web セキュリティ（CWS）、Web セキュリティ アプライアンス（WSA）などの非 VPN ヘッドエンドでも使用されます。ヘッドエンドに関係なく一貫したモデルが使用されるため、ヘッドエンドの移行が発生した場合も影響はありません。

AnyConnect のライセンス モデルについての詳細は、http://www.cisco.com/c/dam/en/us/products/collateral/security/anyconnect-og.pdf を参照してください。



第 15 章

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

各 URL の書き換え

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 を書き換えます。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 *6*：ユーザが入力した *URL* の例

図 7: 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。

始める前に

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

ステップ 1 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。

webvpn

ステップ 2 ユーザが HTTP/HTTPS URL を入力する機能を制御します。

url-entry

ステップ 3 （任意） URL エントリをオフに切り替えます。

url-entry disable

信頼できる証明書のプール

ASA は trustpool に信頼できる証明書をグループ化します。trustpool 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一連のデフォルト証明書が含まれています。これらの証明書は、crypto ca import default コマンドを発行して、管理者がアクティブ化するまで機能しません。

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、サーバは自身を証明するために認証局（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。

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、そのリモートサーバが信頼できるか、および適切なリモートサーバに接続しているかを確認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。

[Configuration] > **[Remote Access VPN]** > **[Certificate Management]** > **[Trusted Certificate Pool]** で、https サイトへの SSL 接続に対して証明書検証を有効にすることができます。また、信頼できる証明書プール内の証明書も管理できます。

（注） ASA trustpool は Cisco IOS trustpool に類似していますが、同一のものではありません。

trustpool 証明書の自動インポートの設定

スマートライセンスでは、Smart Call Home インフラストラクチャが使用されます。ASA はバックグラウンドで Smart Call Home 匿名レポートを設定するときに、Call Home サーバ証明書を発行した CA の証明書を含むトラストポイントを自動的に作成します。ASA は、サーバ証明書の発行階層が変更された場合に証明書の検証をサポートするようになりました。カスタマーが証明書階層の変更を調整する必要はありません。CA サーバの自己署名証明書が変更された場合に、Smart Call Home がアクティブな状態を維持できるように、定期的な trustpool バンドルの更新を自動化できます。この機能はマルチ コンテキスト展開ではサポートされません。

trustpool の証明書バンドルを自動的にインポートするには、ASA がバンドルのダウンロードとインポートに使用する URL を指定する必要があります。次のコマンドを入力すると、デフォルトの Cisco URL とデフォルトの時間（22 時間）を使用して、毎日一定の間隔でインポートが実行されます。

```
ciscoasa(config-ca-trustpool)# auto-import-url Default
```

また、次のコマンドを使用して、カスタム URL による自動インポートをイネーブルにできます。

```
ciscoasa(config-ca-trustpool)# auto-import url http://www.thawte.com
```

オフピーク時またはその他の都合のよい時間帯に柔軟にダウンロードを設定できるようにするには、次のコマンドを入力して、カスタム時間によるインポートをイネーブルにします。

```
ciscoasa(config-ca-trustpool)# auto-import time 23:23:23
```

カスタム URL とカスタム時間の両方による自動インポートを設定するには、次のコマンドを使用する必要があります。

```
ciscoasa(config-ca-trustpool)# auto-import time 23:23:23 url http://www.thawte.com
```

trustpool ポリシーのステータスの表示

trustpool ポリシーの現在のステータスを表示するには、次のコマンドを使用します。

```
show crypto ca trustpool policy
```

このコマンドは次のような情報を返します。

```
0 trustpool certificates installed
Trustpool auto renewal statistics:
 State: Not in progress
 Last import result: Not attempted N/A
 Current Jitter: 0

Trustpool auto import statistics:
 Last import result: N/A
 Next schedule import at 22:00:00 Tues Jul 21 2015

Trustpool Policy

 Trustpool revocation checking is disabled.
 CRL cache time: 60 seconds
 CRL next update field: required and enforced
 Auto import of trustpool is enabled
 Automatic import URL: http://www.cisco.com/security/pki/trs/ios_core.p7b
 Download time: 22:00:00

Policy Overrides:
 None configured
```

CA Trustpool のクリア

trustpool ポリシーをデフォルト状態にリセットするには、次のコマンドを使用します。

```
clear configure crypto ca trustpool
```

トラストポイント証明書の自動インポートはデフォルトでオフになるので、次のコマンドを使用して機能をディセーブにします。

信頼できる証明書プールのポリシーの編集

手順

ステップ 1 [Revocation Check]：プール内の証明書が失効しているかどうかをチェックするように設定し、さらに、失効のチェックに失敗した場合に、CLR または OCSP のいずれを使用するか、および証明書を無効にするかどうかを選択するように設定します。

ステップ 2 [Certificate Matching Rules]：失効または期限切れのチェックから除外する証明書マップを選択します。証明書マップは、AnyConnect またはクライアントレス SSL 接続プロファイル（別名「トンネル グループ」）に証明書をリンクします。

ステップ 3 [CRL Options]：CRL キャッシュの更新頻度を 1 ～ 1440 分（24 時間）の間隔で指定します。

ステップ 4 [Automatic Import]：シスコでは、信頼済み CA の「デフォルト」のリストを定期的に更新しています。[Enable Automatic Import] をオンにして、デフォルト設定を保持するように指定した場合、ASA は 24 時間ごとにシスコのサイトで信頼済み CA の最新リストをチェックします。リストが変更されると、ASA は新しいデフォルトの信頼済み CA リストをダウンロードしてインポートします。

プラグインへのブラウザ アクセスの設定

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 では、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。

- （Cisco 配布のプラグイン限定）URL で指定された jar ファイルのアンパック
- ASA ファイル システムにファイルを書き込みます。
- 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、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 リストにメイン メニュー オプションとオプションを追加します。

次に、以降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 メニューとアドレス フィールドの変更点を示します。

表 *12*：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	セキュア シェル	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。

プラグインに伴う前提条件

- プラグインへのリモート アクセスを実現するには、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。
- プラグインを使用するには、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、サポート対象の VPN プラットフォーム、Cisco ASA 5500 シリーズ互換性マトリクスを参照してください。

プラグインの使用上の制限

（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、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

始める前に

ASA インターフェイス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。

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

ステップ 1 クライアントレス SSL VPN が ASA で有効になっているかどうかを示します。

show running-config

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て、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。

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。

始める前に

ASA のインターフェイス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。確認するには、show running-config**show running-config**コマンドを入力します。

表 *13 :* 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 のバージョン 5.1 へのバージョンアップだけ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。 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。	

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。 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。

（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。

手順

ステップ 1 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。

import webvpn plug-in protocol [rdp | rdp2 | [ssh | telnet] | vnc] *URL*

（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** を入力する場合、両者の間にスペースは挿入しません。これによって、Secure Shell サービスと Telnet サービスの両方にプラグイン アクセスを提供します。

例：

次に、TFTP または FTP サーバのホスト名またはアドレスと、URL がプラグイン .jar ファイルへのリモート パスであるプラグインへのパスを入力する例を示します。

```
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)
```

ステップ 2 （任意） 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。

revert webvpn plug-in protocol *protocol*

例：

```
hostname# revert webvpn plug-in protocol rdp
```

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されたセッションが保持されません。フェールオーバー後に Citrix ユーザを再認証する必要があります。

Citrix プラグインの作成とインストール

始める前に

セキュリティ アプリケーションをプラグイン用に準備する必要があります。

（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。

手順

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]、[Receiver for Other Platforms] の順に選択し、[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て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）と 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

ステップ 1 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。

例：

```
hostname# show import webvpn plug
ssh
rdp
vnc
ica
```

ステップ 2 プラグインのハッシュおよび日付を含めます。

例：

```
hostname show import webvpn plug detail
post GXN2BIGGOAOkBMibDQsMu2GWZ3Q= Tues, 29 Apr 2008 19:57:03 GMT
rdp fHeyReIOUwDCgAL9HdTs PnjdBoo= Tues, 15 Sep 2009 23:23:56 GMT
```

ポート転送の設定

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。

ポート転送の前提条件

- 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。
- Mac OS X 10.5.3 上で Safari を使用しているブラウザベースのユーザは、ASA の URL と共に使用するためにクライアント証明書を区別する必要があります。Safari の URL 解釈方法により、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指定します。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 ゾーンに追加します。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。

ポート転送に関する制限事項

- 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 接続によってそれを更新できない場合、ポート転送アプレットでは、ローカル ポートとリモート ポートが同一のものとして表示されます。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

ポート転送機能は、解決および接続のために、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。ポート転送アプレットから DNS 要求を受け入れるように、次のように ASA を設定します。

手順

ステップ 1 DNS サーバ グループ モードを開始して、example.com という名前の DNS サーバ グループを設定します。

例：

```
hostname(config)# dns server-group example.com
```

ステップ 2 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。

例：

```
hostname(config-dns-server-group)# domain-name example.com
```

ステップ 3 ドメイン名を IP アドレスに解決します。

例：

```
hostname(config-dns-server-group)# name-server 192.168.10.10
```

ステップ 4 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。

webvpn

ステップ 5 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。

tunnel-group webvpn

ステップ 6 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。

例：

```
asa2(config-dns-server-group)# exit
asa2(config)# tunnel-group DefaultWEBVPNGroup webvpn-attributes
asa2(config-tunnel-webvpn)# dns-group example.com
```

ポート転送に対するアプリケーションの適格化

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、アプリケーションがアクセスの提供に使用するローカル 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。

手順

ステップ 1 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。

show run webvpn port-forward

ステップ 2 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。

webvpn

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。

（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。

- 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。

始める前に

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、手動でポート転送を開始する必要があります。

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 つのコマンドが入力されると、ASA は、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と置き換えます。最後の

コマンドの場合は、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すでに存在する **port-forward** コマンドが削除されるだけです。

手順

ステップ 1 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 auto-start <*list name*>

ステップ 2 ユーザ ログイン時のポート転送を許可または禁止します。

port-forward enable <*list name*>

port-forward disable

ステップ 3 （任意） **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。

no port-forward [**auto-start** <*list name*> | **enable** <*list name*> | **disable**]

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

ステップ 1 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。

webvpn

ステップ 2 グループ ポリシーまたは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。

group-policy webvpn または **username webvpn**

ステップ 3 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 auto-start *list_name*

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の既存の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。

例：

次のコマンドは、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。

```
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# port-forward auto-start apps1
```

ステップ 4 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。

show run webvpn port-forward

ステップ 5 （任意） グループ ポリシーまたはユーザ名から port-forward コマンドを削除し、デフォルトに戻します。

no port-forward

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

ステップ 1 ポート転送を有効にします。

port-forward auto-start *list_name* を入力した場合は、手動でポート転送を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既存の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。

port-forward [**enable** l<*list name*> | **disable**]

例：

次のコマンドは、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。

```
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# port-forward enable apps1
```

ステップ 2 ポート転送リストのエントリを表示します。

show running-config port-forward

ステップ 3 （任意） グループ ポリシーまたはユーザ名から port-forward コマンドを削除し、デフォルトに戻します。

no port-forward

ステップ 4 （任意） ポート転送をオフに切り替えます。

port-forward disable

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 はリストを取得して、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。

ポータル ページのメニュー内またはクライアントレス SSL VPN セッション中に表示されるツールバー上にある、[Browse Networks] をリモート ユーザがクリックすると、ASA は、通常、ASA と同じネットワーク上またはこのネットワークからアクセス可能な場所にある、マスター ブラウザ、WINS サーバ、または DNS サーバを使用して、サーバ リストをネットワークに照会します。

マスター ブラウザまたは DNS サーバは、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、ASA 上の CIFS/FTP クライアントに表示します。

（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

ユーザが `\\server\share\subfolder\personal` フォルダにアクセスするには、少なくとも、共有自体を含めたすべての親フォルダに対する読み取り権限を持っている必要があります。

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。

Web フォルダからワークステーションのフォルダにファイルをドラッグ アンド ドロップすると、一時ファイルのように見えることがあります。ビューを更新し、転送されたファイルを表示するには、ワークステーションのフォルダを更新します。

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

（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ことを DNS サーバに要求します。

手順

ステップ 1 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。

webvpn

ステップ 2 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。

tunnel-group webvpn

ステップ 3 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。

nbns-server {*IPaddress* | *hostname*} [**master**] [**timeout** *timeout*] [**retry** *retries*]

- **master** は、マスター ブラウザとして指定す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 つだけの場合は同じサーバに送信され、サーバが複数存在する場合は別のサーバに送信されます。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。

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
```

ステップ 4 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。

show tunnel-group webvpn-attributes

ステップ 5 （任意）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。

character-encoding *charset*

charset は、最大 40 文字からなる文字列で、http://www.iana.org/assignments/character-sets で指定されている有効文字セットのいずれかと同じです。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。

例：

次に、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する例を示します。

```
hostname(config)# webvpn
hostname(config-webvpn)# character-encoding shift_jis
hostname(config-webvpn)# customization DfltCustomization
hostname(config-webvpn-custom)# page style background-color:white
```

ステップ 6 （任意）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。

file-encoding {*server-name* | *server-ip-address*} *charset*

例：

次に、CIFS サーバ 10.86.5.174 のファイルエンコーディング属性を設定して、IBM860（エイリアス「CP860」）文字をサポートする例を示します。

```
hostname(config-webvpn)# file-encoding 10.86.5.174 cp860
```

SharePoint アクセスのためのクロックの正確性の確保

ASA 上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 の時間が正しくないと、SharePoint サーバ上の文書にアクセスしたときに、ASA で設定されたクッキーの有効期間によって Word が正常に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 サーバと時間をダイナミックに同期させるように、ASA を設定することをお勧めします。手順については、一般的操作用コンフィギュレーションガイドで「日付と時刻の設定」に関する項を参照してください。

Virtual Desktop Infrastructure（VDI）[VirtualDesktopInfrastructureVDI]

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 Receiver 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など、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。

VDI の制限事項

- 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 Receiver 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。

Citrix 用に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

Citrix の制限

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 Receiver 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 セキュア モビリティ クライアントを使用し、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ための 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 ユーザから Citrix に接続する方法の概要を示します。

手順

ステップ 1 モバイル ユーザが Citrix Receiver を起動し、ASA の URL に接続します。

ステップ 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。

ステップ 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 Access Gateway 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。

次のタスク

http://www.youtube.com/watch?v=JMM2RzppaG8：このビデオでは、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。

SSL を使用した内部サーバへのアクセス

手順

ステップ 1 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。

webvpn

ステップ 2 URL エントリをオフに切り替えます。

url-entry disable

クライアントレス SSL VPN は SSL とその後継である TLS1 を使用して、内部サーバでサポートされている特定の内部リソースと、リモートユーザとの間のセキュアな接続を実現します。

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) 以降の ASA では、外部インターフェイスのポート 443 で、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が同時にサポートされ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。

手順

ステップ 1 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。

webvpn

ステップ 2 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。

port *port_number*

例：

次の例では、外部インターフェイスのポート 444 でクライアント SSL VPN を有効にします。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。

```
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
```

ステップ 3 （特権モード）ASDM のリスニング ポートを変更します。

http server enable

例：

この例では、HTTPS ASDM セッションが外部インターフェイスのポート 444 を使用するように指定します。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。

```
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
```

クライアントレス SSL VPN セッションでの HTTPS の使用

HTTPS の設定に加えて、Web サイトをプロトコル ダウングレード攻撃や cookie ハイジャックから保護するのに役立つ Web セキュリティ ポリシー メカニズムである HTTP Strict-Transport-Security（HSTS）を有効にします。HSTS は、UA およびブラウザを HTTPS Web サイトにリダイレクトし、次のディレクティブを送信することにより指定したタイムアウト期限が切れるまで Web サーバに安全に接続します。

```
Strict-Transport-Security: max-age="31536000"; preload;
```

それぞれの説明は次のとおりです。

- max-age：（設定可能）Web サーバが HSTS ホストとしてみなされ、HTTPS のみを使用してセキュアにアクセスされる必要のある時間を秒単位で指定します。デフォルトは 18 週です（10,886,400 秒）。範囲は 8 時間 ～ 365 日です（0 ～ 31,536,000> 秒）。
- preload：ブラウザに対し、すでに UA およびブラウザに登録され、HSTS ホストとして取り扱う必要のあるドメインのリストの読み込みを指示します。プリロードされたリストの実装は UA およびブラウザに依存し、各 UA およびブラウザは他のディレクティブの振る舞いに対して追加の制限を指定することができます。たとえば、Chrome のプリロード リストは、HSTS の最大寿命が少なくとも 18 週（10,886,400 秒）であることを指定します。

手順

ステップ 1 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。

webvpn と入力します。

ステップ 2 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。

enable *interface-name* と入力します。

ステップ 3 HSTS を有効にします。

hsts enable と入力します。

HSTS を無効にするには、「no」形式のコマンド **no hsts enable** を使用します。

ステップ 4 HSTS の有効時間（秒数）を設定します。

hsts max-age *max-age-in-seconds* と入力します。

値の範囲は <0 ～ 31536000> 秒です。デフォルトは 10,886,400（18 週）です。この制限に達すると、HSTS は有効ではなくなります。

例

```
hostname(config)# webvpn
hostname(config-webvpn)# enable outside

hostname(config-webvpn)# hsts enable
hostname(config-webvpn)# hsts max-age 31536000
```

次のタスク

現在の設定を参照するには、**show running-config webvpn**[*hsts*] を使用します。

現在の設定をクリアするには、**clear configure webvpn** を使用します。

プロキシ サーバのサポートの設定

ASA は HTTPS 接続を終了させて、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。

始める前に

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。

手順

ステップ 1 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。

webvpn

ステップ 2 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。

http-proxy and https-proxy

（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 プロキシを設定します。

http-proxy *host* [*port*] [**exclude** *url*] [**username** *username* {**password** *password*}]

ステップ 4 HTTPS プロキシを設定します。

https-proxy *host* [*port*] [**exclude** *url*] [**username** *username* {**password** *password*}]

ステップ 5 PAC ファイル URL を設定します。

http-proxy pac *url*

ステップ 6 （任意） 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。

exclude

ステップ 7 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。

ホスト

ステップ 8 各 URL のプロキシを識別する JavaScript 関数を使用して ASA にプロキシ自動コンフィギュレーション ファイルをダウンロードします。

pac

ステップ 9 （任意）（ユーザ名を指定した場合に限り使用可能）各プロキシ要求にパスワードを付加して基本的なプロキシ認証を提供します。

password

ステップ 10 各 HTTP または HTTPS 要求とともにプロキシ サーバへのパスワードを送信します。

password

ステップ 11 （任意） 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。代替の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。

port

ステップ 12 **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 までの範囲の任意の 1 文字と一致します。x は ANSI 文字セット内のある 1 文字を表し、y は別の 1 文字を表します。
- [!x-y] は、範囲外の任意の 1 文字と一致します。

ステップ 13 **http-proxy pac** を入力した場合は、**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 （任意） 基本的なプロキシ認証のために各 HTTP プロキシ要求にユーザ名を付加します。このキーワードは、**http-proxy***host* コマンドでのみサポートされます。

username

ステップ 15 各 HTTP または HTTPS 要求とともにプロキシ サーバへのユーザ名を送信します。

username

ステップ 16 次のように設定されている HTTP プロキシ サーバの使用について設定方法を示します：IP アドレスが209.165.201.1、デフォルトポートを使用、各HTTP要求とともにユーザ名とパスワードを送信。

例：

```
hostname(config-webvpn)# http-proxy 209.165.201.1 user jsmith password
mysecretdonttell
```

ステップ 17 同じコマンドを示しますが、異なる点として、ASA は HTTP 要求で www.example.com という特定の URL を受信した場合、プロキシ サーバに渡すのではなく自身で要求を解決します。

例：

```
hostname(config-webvpn)# http-proxy 209.165.201.1 exclude www.example.com
username jsmith password mysecretdonttell
```

ステップ 18 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。

例：

```
hostname(config-webvpn)# http-proxy pac http://www.example.com/pac
```

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** コマンドのみをサポートしています。たとえば、**http-proxy** コマンドの1つの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している場合に別のコマンドを入力すると、CLI によって前のインスタンスが上書きされます。

（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、サポート対象の VPN プラットフォーム、Cisco ASA 5500 シリーズ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付き 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 証明書をユーザによって

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。

デジタル証明書認証の制限

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。

デジタル証明書による認証および認可については、一般的操作用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可能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。

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 では、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。

- （Cisco 配布のプラグイン限定）URL で指定された jar ファイルのアンパック
- 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みます。
- 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、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 リストにメイン メニュー オプションとオプションを追加します。

次の表に、以降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 メニューとアドレス フィールドの変更点を示します。

表 *14 :* 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。

ブラウザ プラグインのインストールの前提条件

- 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。

ブラウザ プラグインのインストールに関する要件

- 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 アクセスを実現するには、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。
- プラグインを使用するには、ブラウザで ActiveX または Oracle Java ランタイム環境（JRE）が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 プラグインのセットアップ

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。

手順

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 の前にクライアントレス 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

手順

ステップ 1 ASA インターフェイス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。

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。

新しい HTML ファイルを使用するための ASA の設定

手順

ステップ 1 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。

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#
```

ステップ 2 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。

export webvpn customization *<file> <URL>*

例：

```
hostname# 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
```

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：

この例では、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。

```
<full-customization>
          <mode>enable</mode>
          <url>/+CSCOU+/login.inc</url>
      </full-customization>
```

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。

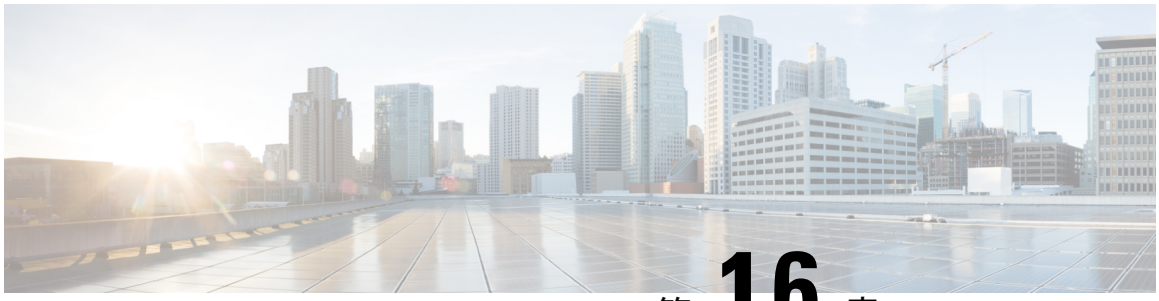
例：

```
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
```



第 16 章

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

Microsoft Kerberos Constrained Delegation ソリューション

多くの組織は、現在 ASA SSO 機能によって提供されるもの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ことを望んでいます。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、証明書ベースの認証方式にも OTP ベースの認証方式にも、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型のユーザ名とパスワードが含まれていません。証明書を使用して認証する場合、ASA が Web ベースのリソースに達するためにユーザ名とパスワードは必要ないので、この認証方式は SSO ではサポートされません。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 アプリケーションにアクセスできるようにします。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。SSO と KCD が独立しながら連携することにより、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。

KCD の機能

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 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、クライアントレスまたは 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。

プロトコル移行機能は、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）用に 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を向上させます。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。

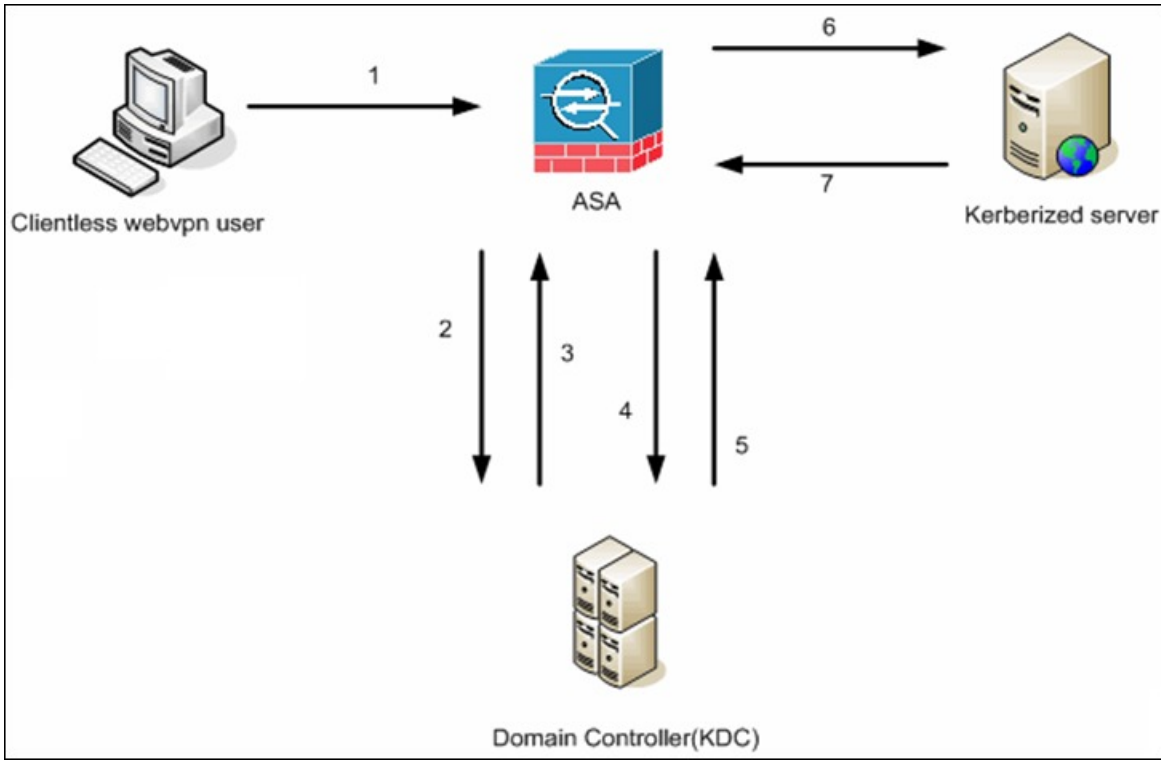
制約付き委任の詳細については、IETF の Web サイト（http://www.ietf.org）にアクセスして、RFC 1510 を参照してください。

KCD の認証フロー

次の図に、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 上に設定された 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 *8 : KCD* プロセス



（注） クライアントレス ユーザ セッションは、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 はデジタル証明書の userPrincipalName を使用して、Windows Active Directory に対して LDAP 許可を実行します）。

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、サーバがサポートし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判断します（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、ユーザに代わって、自身のサービス チケットをキー発行局に要求します。

3. キー発行局は、要求されたチケットを ASA に返します。ASA に渡される場合でも、これらのチケットには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のサービス チケットを KCD に要求します。

（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のサービス チケットをキー発行局に要求します。
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。

クロスレルム認証用の ASA の設定

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。

手順

ステップ 1 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。

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
```

ステップ 2 ルックアップを実行します。

dns domain-lookup

dns server-group

例：

この例では、ドメイン名 private.net と、ユーザ名 dcuser とパスワード dcuser123! を使用するドメイン コントローラ上のサービス アカウントを示します。

```
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)#
```

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が返されるようにするには、次の手順を実行します。

手順

ステップ 1 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。

webvpn

ステップ 2 KCD を設定します。

kcd-server

ステップ 3 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。

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
```

ステップ 4 （任意） ASA の動作を指定して削除します。

no kcd-server

ステップ 5 （任意） 内部状態にリセットします。

kcd-server reset

ステップ 6 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。

kcd domain-join username <*user*> **password** <*pass*>

user：特定の管理ユーザではなく、Windows ドメイン コントローラにデバイスを追加するサービス レベル権限を持つユーザと対応します。

pass：パスワードは、特定のパスワードではなく、Windows ドメイン コントローラにデバイスを追加するサービス レベル権限を持つユーザのパスワードと対応します。

ステップ 7 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 domain-leave

KCD ステータス情報の表示

手順

	コマンドまたはアクション	目的

ステップ 1	リリース 9.5.2 では、次のコマンドが、ADI 経由でドメイン メンバーシップを要求します。少なくとも、ドメイン参加ステータス（参加または不参加）と障害の原因（不明、サーバ到達不能、または無効な権限）が返されます（該当する場合）。
	例：
	`ASA#show webvpn kcd`
	`KCD-Server Name : DC`
	`User : user1`
	`Password : ****`
	`KCD State : Joined`
	`Failure Reason : Unknown`
		show webvpn kcd

KCD のデバッグ

次のコマンドは、KCD 固有のデバッグ メッセージの出力を制御するために使用します。バージョン 9.5.2 よりも前で行われていたように、ADI の syslog 発行レベルを制御するためではありません。

debug webvpn kcd

キャッシュされた Kerberos チケットの表示

ASA に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。

show aaa kerberos[**username** *user* | **host** *ip* | **hostname**]

例

```
ASA# show aaa kerberos

Default Principal     Valid Starting       Expires     Service Principal
asa@example.COM     06/29/10 18:33:00      06/30/10 18:33:00
krbtgt/example.COM@example.COM
kcduser@example.COM     06/29/10 17:33:00      06/30/10 17:33:00
asa$/example.COM@example.COM
kcduser@example.COM     06/29/10 17:33:00      06/30/10 17:33:00
http/owa.example.com@example.COM

ASA# show aaa kerberos username kcduser

Default Principal     Valid Starting      Expires     Service Principal
kcduser@example.COM     06/29/10 17:33:00      06/30/10 17:33:00
asa$/example.COM@example.COM
kcduser@example.COM     06/29/10 17:33:00      06/30/10 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.COM     06/29/10      06/30/10 17:33:00
```

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、次のコマンドを入力します。

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。
- hostname：特定のホストの Kerberos チケットのクリアに使用します。

Microsoft Kerberos の要件

kcd-server コマンドを機能させるために、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。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、ASA は独自のフォーマットを使用して、ソース ドメインから宛先ドメインへの認証パスを横断し、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において、ASA は特定のドメインのクレデンシャルおよび後続ドメインとの信頼関係に依存しています。

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 に組み込まれているアプリケーション プロファイル カスタマイゼーション フレームワーク（APCF）オプションを使用すると、標準以外のアプリケーションや Web リソースを ASA で処理して、クライアントレス SSL VPN 接続で正常に表示できるようになります。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。

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

ステップ 1 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。

webvpn

ステップ 2 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。

apcf

例：

この例では、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と、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。

```
hostname(config)# webvpn
hostname(config-webvpn)# apcf flash:/apcf/apcf1.xml

hostname(config)# webvpn
hostname(config-webvpn)# apcf https://myserver:1440/apcf/apcf2.xml
```

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。 次の表に、この場合に使用する XML タグを示します。

APCF のガイドライン

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 : 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。
<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。

タグ	使用目的
<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） • （"a".."z" | "A".."Z" | "0".."9" | ".-_*[]?"）を含む server-regexp 正規表現 • （"a".."z" | "A".."Z" | "0".."9" | ".-_*[]?+()\{},"）を含む server-fnmatch 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、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>

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）。

タグ	使用目的

<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

```
<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>

<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

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。

文字エンコーディングの表示または指定

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。

手順

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。

http://www.iana.org/assignments/character-sets で指定されている有効文字セットのいずれかと等しい文字列を、最大 40 文字まで入力できます。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 の設定を保存するときに、コマンド インタープリタによって大文字が小文字に変換されます。

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、ユーザが指定した大文字と小文字の区別は保持されますが、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。

http://www.iana.org/assignments/character-sets で指定されている有効文字セットのいずれかと等しい文字列を、最大 40 文字まで入力できます。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 の設定を保存するときに、コマンド インタープリタによって大文字が小文字に変換されます。

クライアントレス SSL VPN を介した電子メールの使用

Web 電子メールの設定：MS Outlook Web App

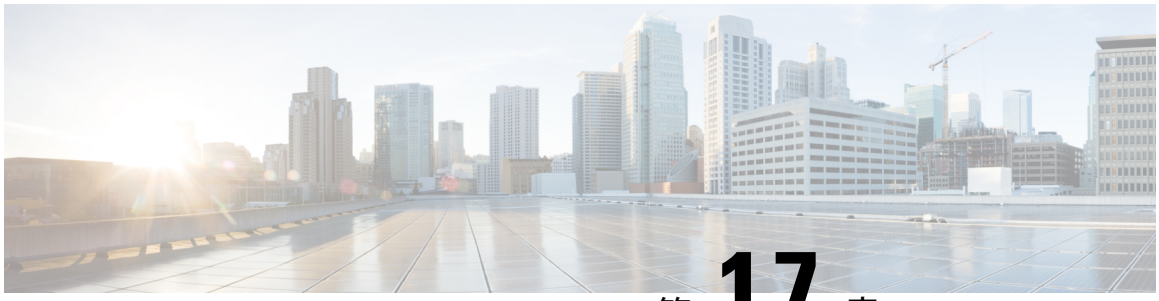
ASA は、Microsoft Outlook Web App to Exchange Server 2010 および Microsoft Outlook Web Access to Exchange Server 2007、2003、2000 をサポートしています。

手順

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 の形式で入力します。

ステップ 3 電子メール パスワードを入力します。



第 17 章

ポリシー グループ

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

内部サーバ上の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 に関するポリシーを作成して適用するには、グループ ポリシーを割り当てる必要があります。

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。ASA の内部認証サーバ、外部 RADIUS または LDAP サーバを使用して、ユーザをグループ 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 用接続プロファイルの属性

次の表は、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」が「トンネル グループ」と呼ばれていました。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、この 2 つの用語が同義的によく使用されています。

表 *16 :* 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。

コマンド	機能
secondary-pre-fill-username	このトンネル グループにセカンダリ ユーザ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

次の表に、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。グループ ポリシー属性とユーザ属性の設定手順については、クライアントレス SSL VPN セッションのグループ ポリシー属性の設定 （392 ページ） または 特定ユーザのクライアントレス SSL VPN アクセスの設定 （402 ページ）を参照してください。

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。

コマンド	機能
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。
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。
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。

クライアントレス SSL VPN セッションのグループ ポリシー属性の設定

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 はプロキシする必要がある接続を識別し、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
- 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**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。

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。

webvpn

no webvpn

次の例は、FirstGroup というグループ 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)#
```

拒否メッセージの指定

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 ユーザに送信す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** コマンドに文字列を入力するときは、コマンドがラップする場合でも続けて入力します。

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)
```

クライアントレス SSL VPN セッションのグループ ポリシー 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 セッションからの Java、ActiveX、イメージ、スクリプト、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** コマンドを実行したときに作成されるヌル値を含めて、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]
```

下記の表に、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 *17 : 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）。

次の例は、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方法を示しています。

```
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がログインしたときに表示される 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。

特定サーバへの特定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 URI を指定してこのコマンドの **no** 形式を使用します。すべてのサーバに対して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、グループ ポリシーから値を継承できます。

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 セッション用の ACL の指定

webvpn モードで **filter** コマンドを使用し、このグループ ポリシーまたはユーザ名に対してクライアントレス SSL VPN セッションで使用する 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 **value** 文字列で、設定した ACL の名前を指定します。

（注） クライアントレス SSL VPN セッションでは、**vpn-filter** コマンドで定義された ACL は使用されません。

次の例は、FirstGroup という名前のグループ ポリシーで acl_in という ACL を呼び出すフィルタの設定方法を示しています。

```
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 ポリシーのリスト内にある 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 リストが継承されないようにするには、**url-list none** コマンドを使用します。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
```

下記の表に、**url-list** コマンドのパラメータとその意味を示します。

表 *18 : 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 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)
```

グループポリシーに対するクライアントレス SSL VPN セッションで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 ポリシーでアプリケーション 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。ポートフォワーディングは、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** コマンドを入力して、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、別のグループ ポリシーからリストを継承できようになります。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、特定のユーザ ポリシーまたはグループ ポリシー用にエンド 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** オプションを指定すると、デフォルト名 Application Access が復元されます。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 タイマー更新時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、指定サイズ以下のメッセージをすべてキープアライブ メッセージと見なして、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に指定できます。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**形式を使用すると、コンフィギュレーションからこの指定が削除されます。

```
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、特定のグループまたはユーザに対してクライアントレス SSL VPN セッションを介した 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—**グループまたはユーザに対して圧縮をイネーブルにすることを指定します。これはデフォルト値です。
- **none—**そのグループまたはユーザに対し圧縮がディセーブルにされるよう指示します。

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 モードやユーザ名 webvpn モードで設定された **http-comp** コマンドよりも優先されます。

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)#
```

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**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 モードを開始します。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 はプロキシする必要がある接続を識別し、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 モードのコマンドによって、ファイル、URL、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**webvpn** コマンドは、コマンドの設定を行ったユーザ名にのみ適用されます。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
- auto-signon
- AnyConnect Secure Mobility Client
- keep-alive ignore
- HTTP compression

次の例は、username anyuser attributes に対してユーザ名 webvpn コンフィギュレーション モードを開始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 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、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、グループ ポリシーから値を継承できます。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したときに表示される 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、グループ ポリシーから値を継承できます。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)#
```

拒否メッセージの指定

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 ユーザに送信す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** コマンドに文字列を入力するときは、コマンドがラップする場合でも続けて入力します。

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)
```

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、グループ ポリシーから値を継承できます。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 セッションで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 フォワーディングは、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、グループ ポリシーからリストを継承できます。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** コマンドを入力して、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、特定のユーザ用にエンド 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** オプションを指定すると、デフォルト名 Application Access が復元されます。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 タイマー更新時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、指定サイズ以下のメッセージをすべて

キープアライブ メッセージと見なして、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に指定できます。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** 形式を使用すると、コンフィギュレーションからこの指定が削除されます。

```
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、クライアントレス SSL VPN の特定ユーザのログイン 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。

特定サーバへの特定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 URI を指定してこのコマンドの **no** 形式を使用します。すべてのサーバに対して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、グループ ポリシーから値を継承できます。

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、サブネット マスク 255.255.255.0 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、IP アドレス 10.1.1.0 を持つサーバへの基本認証または NTLM 認証による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、特定のユーザに対してクライアントレス SSL VPN セッションを介した 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—**グループまたはユーザに対して圧縮をイネーブルにすることを指定します。これはデフォルト値です。
- **none—**そのグループまたはユーザに対し圧縮がディセーブルにされるよう指示します。

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 モードやユーザ名 webvpn モードで設定された **http-comp** コマンドよりも優先されます。

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)#
```

スマート トンネル アクセス

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 トンネルでは、セキュリティ アプライアンスをパスウェイ、ASA をプロキシ サーバとするクライアントレス（ブラウザベース）SSL VPN セッションが使用されます。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 トンネルのメリット

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。

スマート トンネルの前提条件

スマート トンネルでサポートされるプラットフォームとブラウザについては、サポート対象の VPN プラットフォーム、Cisco ASA 5500 シリーズ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 ではブラウザで ActiveX または Oracle Java ランタイム環境（JRE 6 以降を推奨）を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。

スマート トンネルのガイドライン

- 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ります。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）。
- Mac デバイスや Windows デバイスの Chrome ブラウザでスマート トンネルをサポートするための新しいメソッドが用意されました。Chrome Smart Tunnel Extension は、Netscape プラグインアプリケーションプログラムインターフェイス（NPAPI）に代わるものです。NPAPI は、Chrome ではサポートされなくなりました。

  この拡張プログラムをインストールしていない Chrome でスマート トンネルに対応したブックマークをクリックすると、ユーザは拡張プログラムを取得できるように Chrome ウェブストアにリダイレクトされます。Chrome を新規インストールする場合、ユーザは拡張プログラムを取得できるように Chrome ウェブストアに移動されます。この拡張プログラムは、スマート トンネルの実行に必要なバイナリを ASA からダウンロードします。

  Chrome のデフォルトのダウンロード場所が、現在のユーザの「ダウンロード」フォルダを指している必要があります。または、Chrome のダウンロード設定が [Ask every time] である場合は、ユーザは尋ねられたときに「ダウンロード」フォルダを選択する必要があります。

  スマート トンネルの使用中、通常のブックマークおよびアプリケーション設定は、新しい拡張機能のインストールとダウンロード場所指定のプロセス以外は変更されません。

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。ただし、ユーザはクライアントレス SSL VPN ポータル ページの [Application Access]**Application Access**> [Start Smart Tunnels]**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必要がある。

（注） 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。

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、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 つのコマンドが入力されると、ASA は、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と置き換えます。最後のコマンドの場合は、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 コマンドが削除されるだけです。

- **smart-tunnel auto-start** リスト

  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。

- **smart-tunnel enable** リスト

  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、ユーザはクライアントレス SSL VPN ポータル ページの [Application Access]**Application Access**> [Start Smart Tunnels]**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。

- **smart-tunnel disable**

  スマート トンネル アクセスを禁止します。

- **no smart-tunnel [auto-start list | enable list | disable]**

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って削除する smart-tunnel コマンドを限定します。

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

ステップ 1 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。

webvpn

ステップ 2 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。

[no] smart-tunnel network *network name***ip** *ip netmask*

- *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。

ステップ 3 *.cisco.com などのホスト名マスクを確立します。

[no] smart-tunnel network *network name***host** *host mask*

ステップ 4 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。

[no] smart-tunnel tunnel-policy [{excludespecified | tunnelspecified} *network name*| **tunnelall]**

- *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、ネットワーク名で指定されたネットワークだけをトンネリングする。
- *excludespecified* は、ネットワーク名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する。

スマート トンネル トンネルポリシーの設定と適用

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。

手順

ステップ 1 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。

[no]smart-tunnel tunnel-policy [{excludespecified | tunnelspecified} *network name* | *tunnelall]*

- *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、ネットワーク名で指定されたネットワークだけをトンネリングする。
- **excludespecified** は、ネットワーク名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する。

ステップ 2 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。

[no] smart-tunnel network *network name***ip** *ip netmask*

または

[no] smart-tunnel network *network name***host** *host mask*

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 つだけ使用してください。

- *network name* は、トンネル ポリシーを適用するネットワークの名前を指定します。
- *ip address* は、ネットワークの IP アドレスを指定します。
- *netmask* は、ネットワークのネットマスクを指定します。
- *host mask* は、ホスト名マスク（*.cisco.com など）を指定します。

例：

例：

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-webvpn)# smart-tunnel network inventory ip 10.5.2.2
or
ciscoasa(config-webvpn)# smart-tunnel network inventory host www.example.com
```

ステップ 3 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。

ciscoasa(config-group-webvpn)# **smart-tunnel tunnel-policy tunnelspecified inventory**

ステップ 4 （任意） 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。

例：

例：

```
ciscoasa(config-group-webvpn)# homepage value http://www.example.com
ciscoasa(config-group-webvpn)# homepage use-smart-tunnel
ciscoasa(config-webvpn)# smart-tunnel notification-icon
```

（注） 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。

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。

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

手順

ステップ 1 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。

webvpn

ステップ 2 サーバ リストに追加する各サーバに対して使用します。

smart-tunnel auto-sign-on *list* [**use-domain**] [**realm** *realm-string*] [**port** *port-num*]{**ip** *ip-address* [*netmask*] | **host** *hostname-mask*}

- *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（任意）：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。

ステップ 3 （任意） 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。

no smart-tunnel auto-sign-on *list* [**use-domain**] [**realm** *realm-string*] [**port** *port-num*]{**ip** *ip-address* [*netmask*] | **host** *hostname-mask*}

ステップ 4 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。

show running-config webvpn smart-tunnel

ステップ 5 config-webvpn コンフィギュレーション モードに切り替えます。

config-webvpn

ステップ 6 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。

smart-tunnel auto-sign-on HR use-domain ip 93.184.216.119 255.255.255.0

ステップ 7 （任意）削除す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 use-domain ip 93.184.216.119 255.255.255.0

ステップ 8 ASA 設定からリスト全体を削除します。

no smart-tunnel auto-sign-on HR

ステップ 9 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。

smart-tunnel auto-sign-on intranet host *.example.com

ステップ 10 リストからエントリを削除します。

no smart-tunnel auto-sign-on intranet host *.example.com

（注） スマート トンネル自動サインオン サーバ リストを設定した後、そのリストをアクティブにするには、グループ ポリシーまたはローカル ユーザ ポリシーにリストを割り当てる必要があります。詳細については、を参照してください。 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 （419 ページ）

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。

始める前に

- **smart-tunnel auto-sign-on** リスト コマンドを使用して、最初にサーバのリストを作成します。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。

（注） 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 を使用している場合は、正確なホスト名または IP アドレスを使用してホストが指定されていることを確認します（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

ステップ 1 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。

webvpn

ステップ 2 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。

group-policy webvpn

ステップ 3 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。

username webvpn

ステップ 4 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。

smart-tunnel auto-sign-on enable

ステップ 5 （任意） 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、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。

[**no**] **smart-tunnel auto-sign-on enable** *list* [**domain** *domain*]

- *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。
- （任意）*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 6 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。

show running-config webvpn smart-tunnel

ステップ 7 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。

smart-tunnel auto-sign-on enable HR

ステップ 8 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。

smart-tunnel auto-sign-on enable HR domain CISCO

ステップ 9 （任意） 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。

no smart-tunnel auto-sign-on enable HR

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、次の手順を実行します。

始める前に

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します。

手順

ステップ 1 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。

webvpn

ステップ 2 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。

group-policy webvpn

ステップ 3 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。

username webvpn

ステップ 4 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。

smart-tunnel auto-start *list*

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。

例：

```
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# smart-tunnel auto-start apps1
```

これにより、apps1 という名前のスマート トンネル リストがグループ ポリシーに割り当てられます。

ステップ 5 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。

show running-config webvpn smart-tunnel

ステップ 6 グループ ポリシーまたはユーザ名から smart-tunnel コマンドを削除し、デフォルトに戻します。

no smart-tunnel

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

ステップ 1 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。

webvpn

ステップ 2 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。

group-policy webvpn

ステップ 3 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。

username webvpn

ステップ 4 スマート トンネル アクセスをイネーブルにします。

smart-tunnel [enable *list* **| disable]**

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。

例：

```
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# smart-tunnel enable apps1
```

この例では、apps1 という名前のスマート トンネル リストがグループ ポリシーに割り当てられます。

ステップ 5 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。

show running-config webvpn smart-tunnel

ステップ 6 グループ ポリシーまたはローカル ユーザ ポリシーから smart-tunnel コマンドを削除し、デフォルトのグループ ポリシーに戻します。

no smart-tunnel

ステップ 7 スマート トンネル アクセスをオフに切り替えます。

smart-tunnel disable

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。

親プロセスが終了した場合のスマート トンネルからのログオフの設定

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 トンネルと開始した場合、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

ステップ 1 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。

[no] smart-tunnel notification-icon

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。

このコマンドの *no* 形式がデフォルトです。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。

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 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。

***.webvpn.**

通知アイコンを使用したスマート トンネルからのログオフの設定

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。

クライアントレス SSL VPN キャプチャ ツール

クライアントレス SSL VPN CLI には、WebVPN 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るキャプチャ ツールが含まれています。このツールが記録するデータは、シスコ カスタマーサポートの担当者が問題のトラブルシューティングを行う際に役立ちます。

クライアントレス SSL VPN キャプチャ ツールの出力には次の 2 つのファイルが含まれます。

- Web ページのアクティビティに応じて mangled.1,2,3,4... など。mangle ファイルは、クライアントレス SSL VPN 接続のページを転送する VPN コンセントレータの html のアクションを記録します。
- Web ページのアクティビティに応じて original.1,2,3,4... など。元のファイルは、URL が VPN コンセントレータに送信したファイルです。

キャプチャ ツールによってファイル出力を開き、表示するには、[Administration] > [File Management] に移動します。出力ファイルを圧縮し、シスコ サポート担当者に送信します。

（注） クライアントレスSSL VPNキャプチャ ツールを使用すると、VPN コンセントレータのパフォーマンスが影響を受けます。出力ファイルを生成した後に、キャプチャ ツールを必ずオフに切り替えます。

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 ポリシーを設定できます。ASA はクライアントレス 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。

始める前に

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 によって hostname(config)# プロンプトが表示されます。

手順

ステップ 1 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。

webvpn

ステップ 2 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。

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*"
```

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を最適化する複数の方法があります。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。

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。

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 エンジンを介して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。これには、JavaScript や Java などの高度な要素からプロキシHTTP へのトラフィックも含まれますが、そ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 SSL VPN デバイス内部からアクセスしているのか、それらのデバイスに依存せずにアクセスしているのかに応じて、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。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。

リライト済み Java コンテンツの署名用証明書の設定

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

ステップ 1 証明書をインポートします。

crypto ca import

ステップ 2 証明書を採用します。

ava-trustpoint

例：

```
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
```

この例では、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 リライトのオフへの切り替え

一部のアプリケーションや Web リソース（公開 Web サイトなど）が ASA を通過しないようにしたい場合があります。そのような場合、ASA では、ASA を通過せずに特定のサイトやアプリケーションをブラウズできるようにするリライト 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。

手順

ステップ 1 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。

webvpn

ステップ 2 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。

rewrite

このコマンドは複数回使用できます。

ステップ 3 rewrite コマンドとともに使用します。

disable

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

プロキシ バイパスを使用するように ASA を設定できます。この設定は、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行います。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。

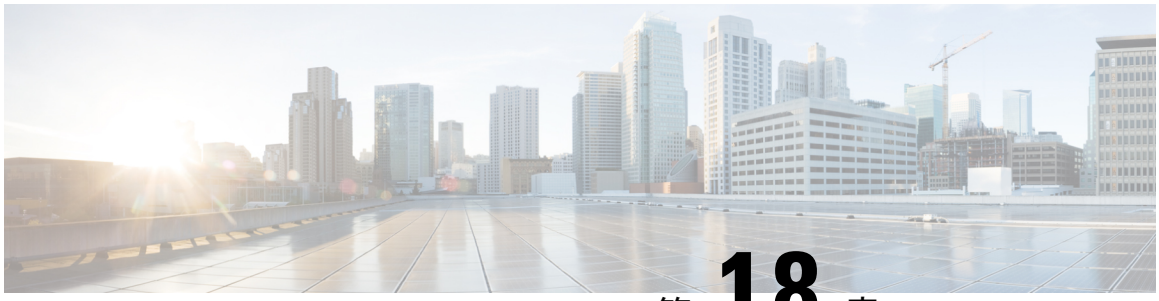
手順

ステップ 1 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。

webvpn

ステップ 2 プロキシ バイパスを設定します。

proxy-bypass



第 18 章

クライアントレス SSL VPN リモート ユーザ

この章では、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 の使用を開始できるようにします。内容は次のとおりです。

（注） ASA がクライアントレス SSL VPN 用に設定されていることを確認します。

クライアントレス SSL VPN リモート ユーザ

この章では、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 の使用を開始できるようにします。内容は次のとおりです。

（注） ASA がクライアントレス SSL VPN 用に設定されていることを確認します。

ユーザ名とパスワード

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。

次の表に、クライアントレス SSL VPN ユーザが理解し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 *19 :* 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/パスワードのタイプ		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
Internet Service Provider：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
File Server	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 ヒントの通知

次のセキュリティのヒントを通知してください。

- クライアントレス SSL VPN セッションから必ずログアウトします。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になるわけではありません。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 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リソース）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

次の表に、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連するタスク、タスクの要件と前提条件、および推奨される使用法を示します。

各ユーザ アカウントを異なる設定にしたことにより、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。この表では、情報をユーザ アクティビティ別にまとめています。

表 *20* : クライアントレス *SSL VPN* リモート システムの設定とエンドユーザ要件

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	

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
		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	
	（任意）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。

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、クライアントレス SSL VPN セッションの終了を求めるメッセージが ASA によって表示されます。 **ヒント** テキスト フィールドにテキストを貼り付けるには、Ctrl+V キーを使用します（クライアントレス SSL VPN ツールバーでは、右クリックは有効ではありません）。

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 ヒントの通知 （430 ページ）」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。

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
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**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。

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、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であるため、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は、アプリケーションを使用できない可能性があります。	
	アプリケーションを使用した後、ユーザは [**Close**] アイコンをクリックして必ず [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、ホスト 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。
	Java Runtime Environment（JRE）がインストール済み。 ブラウザで JavaScript をイネーブルにする必要があります。デフォルトでは有効に設定されています。	

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
		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、ユーザに対して使用可能なサイトが示されます。 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。
		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。

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。	
	（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。	
アプリケーションアクセス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。

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 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 capture コマンドを使用すると、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 （441 ページ）
- ブラウザによるキャプチャ データの表示 （441 ページ）

（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 のパフォーマンスが影響を受けます。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

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してパケットをキャプチャします。

capture *capture-name* **type webvpn user** *csslvpn-username*

- *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。

例：

```
hostname# capture hr type webvpn user user2
```

ステップ 2 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*

例：

```
hostname# no capture hr
```

キャプチャ ユーティリティは *capture-name*.zip ファイルを作成します。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。

ブラウザによるキャプチャ データの表示

手順

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します。

capture *capture-name* **type webvpn user** *csslvpn-username*

- *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。

例：

```
hostname# capture hr type webvpn user user2
```

ステップ 2 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**

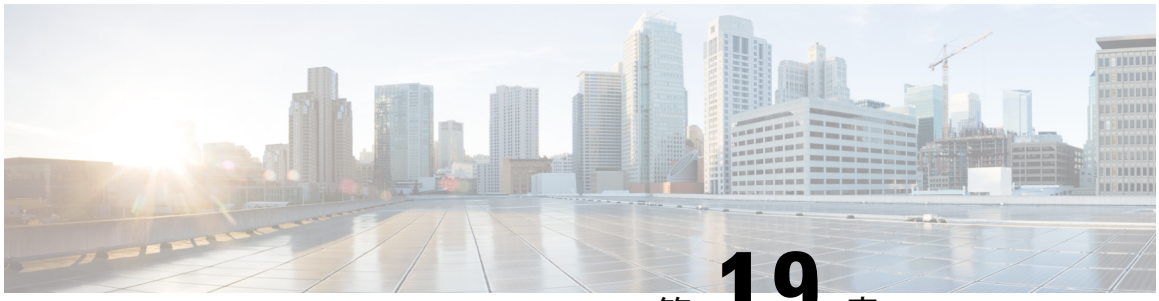
キャプチャされたコンテンツが sniffer 形式で表示されます。

ステップ 3 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*

例：

```
hostname# no capture hr
```



第 19 章

クライアントレス SSL VPN ユーザ

パスワードの管理

必要に応じて、パスワードの期限切れが近づいたときにエンド ユーザに警告するように ASA を設定できます。

ASA 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ています。「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、この通知をサポートしている 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 サーバとのみ通信しているように見えます。

始める前に

- 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 が、サーバのデフォルト 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 で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。
- 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。
- 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するものではありません。このコマンドは、ASA がパスワードの期限が近いことについてユーザへの警告を開始する、期限切れ前の日数を変更します。

手順

ステップ 1 一般属性モードに切り替えます。

tunnel-groupgeneral-attributes

ステップ 2 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。

password-management password-expire-in-days *days*

例：

```
hostname(config-general)# password-management password-expire-in-days 90
```

- 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。

• 日数を 0 に設定すると、このコマンドはオフになります。

この例では、ASA が有効期限の 90 日前にユーザへのパスワードの期限切れの警告を開始します。

（注） password-expire-in-days キーワードが設定されていない場合、ASA は期限切れが近いことをユーザに通知しませんが、ユーザは期限が切れた後にパスワードを変更できます。

クライアントレス SSL VPN でのシングル サインオンの使用

SAML 2.0 による SSO

SSO および SAML 2.0 について

ASA は SAML 2.0 をサポートしています。これにより、クライアントレス VPN のエンドユーザは、クレデンシャルを 1 回だけ入力して、クライアントレス VPN とプライベート ネットワーク外部のその他の SAAS アプリケーションとを切り替えることができるようになります。

たとえば、企業の顧客の場合は、SAML アイデンティティ プロバイダー(IdP）として PingIdentity をイネーブルにして、SAML 2.0 SSO 対応の Rally、Salesforce、Oracle OEM、Microsoft ADFS、onelogin、または Dropbox のアカウントを持ちます。サービス プロバイダー（SP）として 2.0 SAML SSO をサポートするように ASA を設定すると、エンドユーザは一度サインインするだけで、クライアントレス VPN などのあらゆるサービスにアクセスできるようになります。

さらに、AnyConnect 4.4 クライアントが SAML 2.0 を使用して SAAS ベースのアプリケーションにアクセスできるように、AnyConnect SAML サポートが追加されました。AnyConnect 4.6 では、組み込みブラウザとの SAML 統合が拡張され、これが以前のリリースからのネイティブ（外部）ブラウザ統合に置き換わります。組み込みブラウザを搭載した新しい拡張バージョンを使用するには、AnyConnect 4.6（またはそれ以降）および ASA 9.7.1.24（またはそれ以降）、9.8.2.28（またはそれ以降）、または 9.9.2.1（またはそれ以降）へのアップグレードが必要です。

トンネル グループやデフォルト トンネル グループなどの認証方式として SAML が設定されている場合、ASA は SP に対応します。クライアントレス VPN のエンドユーザは、イネーブルになっている ASA または SAML IdP にアクセスして、シングル サインオンを開始します。以下では、これらの各シナリオについて説明します。

SAML SP によって開始される SSO

エンドユーザがクライアントレス VPN を使用して ASA アクセスし、ログインを開始した場合、サインオン動作は次のように進行します。

1. クライアントレス VPN のエンドユーザが SAML 対応のトンネル グループにアクセスするか、またはグループを選択すると、そのユーザは認証のために SAML idP にリダイレクトされます。グループ URL に直接アクセスしない限り、ユーザは入力を要求されます。直接アクセスした場合、リダイレクトは行われません。

   ASA は、ブラウザによって SAML IdP にリダイレクトされる SAML 認証要求を生成します。

2. IdP がエンドユーザのクレデンシャルを確認し、エンドユーザがログインします。入力されたクレデンシャルは IdP の認証設定に合致していなければなりません。

3. IdP の応答がブラウザに返信され、ASA のサインイン URL に送信されます。ASA は応答を確認し、ログインを完了させます。

SAML IdP によって開始される SSL

エンドユーザが IdP にアクセスしてログインを開始した場合、サインオン動作は次のように進行します。

1. エンドユーザが IdP にアクセスします。IdP は、独自の認証設定に従ってエンドユーザのクレデンシャルを確認します。エンドユーザはクレデンシャルを入力し、IdP にログインします。
2. 一般的には、エンドユーザは、IdP で設定された SAML 対応サービスのリストを取得します。エンドユーザが ASA を選択します。

3. SAML の応答がブラウザに返信され、ASA のサインイン URL に送信されます。ASA は応答を確認し、ログインを完了させます。

信頼の輪

ASA と SAML アイデンティティ プロバイダーとの信頼関係は、設定されている証明書（ASA トラストポイント）によって確立されます。

エンドユーザと SAML アイデンティティ プロバイダーとの信頼関係は、IdP に設定されている認証によって確立されます。

SAML のタイムアウト

SAML アサーションには、次のような NotBefore と NotOnOrAfter があります：<saml:Conditions NotBefore="2015-03-10T19:47:41Z" NotOnOrAfter="2015-03-10T20:47:41Z">

ASA で設定されている SAML のタイムアウトと NotBefore の合計が NotOnOrAfter よりも早い場合は、そのタイムアウトが NotOnOrAfter よりも優先されます。NotBefore + タイムアウトが NotOnOrAfter よりも遅い場合は、NotOnOrAfter が有効になります。

タイムアウト後にアサーションによって再利用されないように、タイムアウトにはごく短い時間を設定してください。SAML 機能を使用するためには、ASA の Network Time Protocol（NTP）サーバを IdP NTP サーバと同期する必要があります。

プライベート ネットワークでのサポート

SAML 2.0 ベースのサービス プロバイダー IdP は、プライベート ネットワークでサポートされます。SAML IdP がプライベート クラウドに展開されると、ASA およびその他の SAML 対応サービスはピアの位置になり、すべてプライベート ネットワーク内になります。ASA をユーザとサービス間のゲートウェイとして、IdP の認証は制限された匿名の webvpn セッションで処理され、IdP とユーザ間のすべてのトラフィックは変換されます。ユーザがログインすると、ASA は対応する属性のセッションを修正し、IdP セッションを保存します。その後は、クレデンシャルを再度入力することなくプライベート ネットワークのサービス プロバイダーを使用できます。

SAML IdP *NameID* 属性は、ユーザのユーザ名を特定し、認証、アカウンティング、および VPN セッション データベースに使用されます。

（注） プライベート ネットワークとパブリック ネットワーク間で認証情報を交換することはできません。内部および外部の両方のサービス プロバイダーに同じ IdP を使用する場合、個別に認証する必要があります。内部専用の IdP を外部サービスで使用することはできません。外部専用の IdP は、プライベート ネットワーク内のサービス プロバイダーでは使用できません。

SAML 2.0 に関する注意事項と制約事項

- SAML 2.0 SSO サポートはクライアントレス VPN の 1 機能であるため、クライアントレス VPN と同じ制限事項と許可事項が適用されます。
  - マルチコンテキスト モードおよびロード バランシングはサポートされません。
  - アクティブ/スタンバイ フェールオーバーはサポートされますが、アクティブ/アクティブ フェールオーバーはサポートされません。
  - IPv4 および IPv6 セッションはサポートされます。
- ASA は、すべての SAML IdP でサポートされる SAML 2.0 Redirect-POST バインディングをサポートしています。
- ASA は SAML SP としてのみ機能します。ゲートウェイ モードやピア モードでアイデンティティ プロバイダーとして動作することはできません。
- この SP SAML SSO 機能は相互排他認証方式です。この方式は、AAA や証明書と併用できません。
- ユーザ名/パスワード認証、証明書認証、および KCD に基づく機能はサポートされません。たとえば、ユーザ名/パスワードの事前フィルタリング機能、フォーム ベースの自動サインオン、マクロ置換ベースの自動サインオン、KCD SSO などです。

- DAP は、SAML 対応のトンネル グループに対してサポートされません。
- 既存のクライアントレス VPN のタイムアウト設定は、まだ SAML セッションに適用されます。
- 認証アサーションが適切に処理され、タイムアウトが適切に機能するように、ASA の管理者は、ASA と SAML IdP とのクロック同期を確保する必要があります。
- ASA の管理者は、次の点を考慮して、ASA と IdP の両方で有効な署名証明書を保持する責任があります。
  - ASA に IdP を設定する際には、IdP の署名証明書が必須です。
  - ASA は、IdP から受け取った署名証明書に対して失効チェックを行いません。
- SAML アサーションには、NotBefore と NotOnOrAfter 条件があります。ASA SAML に設定されている**タイムアウト**と、これらの条件との相関関係は次のとおりです。
  - NotBefore とタイムアウトの合計が NotOnOrAfter よりも早い場合は、タイムアウトが NotOnOrAfter に優先します。
  - NotBefore + タイムアウトが NotOnOrAfter よりも遅い場合は、NotOnOrAfter が有効になります。
  - NotBefore 属性が存在しない場合、ASA はログイン要求を拒否します。NotOnOrAfter 属性が存在せず、SAML タイムアウトが設定されていない場合、ASA はログイン要求を拒否します。
- AnyConnect で SAML を使用する場合は、次の追加ガイドラインに従ってください。
  - 信頼できないサーバ証明書は、組み込みブラウザでは許可されません。
  - 組み込みブラウザ SAML 統合は、CLI モードまたは SBL モードではサポートされません。
  - Web ブラウザに確立された SAML 認証は AnyConnect と共有されず、その逆も同じです。
  - 設定に応じて、組み込みブラウザ搭載のヘッドエンドに接続するときに、さまざまな方法が使用されます。たとえば、AnyConnect では IPv6 接続よりも IPv4 接続の方が好ましく、組み込みブラウザでは IPv6 の方が好ましい場合もあります。あるいは、その逆もあります。同じく、プロキシを試して障害が発生したのに AnyConnect がどのプロキシにもフォールバックしない場合もあれば、プロキシを試して障害が発生した後で組み込みブラウザがナビゲーションを停止する場合もあります。
  - SAML 機能を使用するためには、ASA の Network Time Protocol（NTP）サーバを IdP NTP サーバと同期する必要があります。
  - ASDM の VPN ウィザードは現在、SAML 設定をサポートしていません。
  - 内部 IdP を使用してログインした後に SSO で内部サーバにアクセスすることはできません。

- SAML IdP NameID 属性は、ユーザのユーザ名を特定し、認証、アカウンティング、および VPN セッション データベースに使用されます。

SAML 2.0 アイデンティティ プロバイダー（IdP）の設定

始める前に

SAML（IdP）プロバイダーのサインイン URL とサインアウト URL を取得します。URL はプロバイダーの Web サイトから取得できます。また、プロバイダーがメタデータ ファイルで情報を提供していることもあります。

手順

ステップ 1 webvpn コンフィギュレーション モードで SAML アイデンティティ プロバイダーを作成し、webvpn で saml-idp サブモードを開始します。

[**no**] **saml idp** *idp-entityID*

idp-entityID：SAML IdP の entityID には 4 ~ 256 文字を指定します。

SAML IdP を削除するには、このコマンドの **no** 形式を使用します。

ステップ 2 IdP URL を設定します。

url [**sign-in** | **sign-out**] *value*

value：IdP にサインインするための URL、または IdP からサインアウトするときにリダイレクトされる URL です。**sign-in** URL は必須ですが、**sign-out** URL はオプションです。url の値には 4 ~ 500 文字を指定します。

ステップ 3 （任意） クライアントレス VPN のベース URL を設定します。

base-url *URL*

この URL は、エンドユーザを ASA にリダイレクトするために、サードパーティ製 IdP に提供されます。

base-url が設定されている場合、その URL は **show saml metadata** の AssertionConsumerService と SingleLogoutService 属性のベース URL として使用されます。

base-url が設定されていない場合、URL は ASA のホスト名とドメイン名から決定されます。たとえば、ホスト名が `ssl-vpn`、ドメイン名が `cisco.com` の場合は、`https://ssl-vpn.cisco.com` が使用されます。

base-url もホスト名/ドメイン名も設定されていない場合は、**show saml metadata** を入力するとエラーが発生します。

ステップ 4 IdP と SP（ASA）間のトラストポイントを設定します。

trustpoint [**idp** | **sp**] *trustpoint-name*

idp：ASA が SAML アサーションを検証するための IdP 証明書を含むトラストポイントを指定します。

sp（任意）：IdP が ASA（SP）の署名や暗号化 SAML アサーションを検証するための ASA（SP）証明書を含むトラストポイントを指定します。

trustpoint-name：設定されているトラストポイントを指定します。

ステップ 5 （任意） SAML タイムアウトを設定します。

timeout assertion *timeout-in-seconds*

指定した場合、NotBefore と timeout-in-seconds の合計が NotOnOrAfter よりも早い場合は、この設定が NotOnOrAfter に優先します。

指定しない場合は、セッションの NotBefore と NotOnOrAfter が有効期間の確認に使用されます。

（注） 既存の SAML IdP が設定済みのトンネル グループの場合、webvpn での saml idp CLI に対するすべての変更は、SAML がその特定のトンネル グループに再度有効にされたときにのみトンネル グループに適用されます。タイムアウトを設定すると、更新されたタイムアウトはトンネル グループの webvpn 属性の saml アイデンティティ プロバイダー CLI 再発行後にのみ有効になります。

ステップ 6 （任意） SAML 要求の署名をイネーブルまたはディセーブル（デフォルト設定）にします。

signature <value>

（注） SSO 2.5.1 へのアップグレードに伴い、デフォルトの署名方法は SHA1 から SHA256 に変更します。*value* に rsa-sha1、rsa-sha256、rsa-sha384、または rsa-sha512 を入力すると、希望する署名方法のオプションを設定できます。

ステップ 7 （オプション）IdP が内部ネットワークであることを特定するフラグを設定するには、**internal** コマンドを使用します。ASA はゲートウェイ モードで機能するようになります。

ステップ 8 設定を確認するには、 **show webvpn saml idp** を使用します。

ステップ 9 SAML 認証要求が発生したときに、以前のセキュリティ コンテキストに依存するのではなくアイデンティティ プロバイダーが直接認証するようにするには、**forceauthn** を使用します。この設定はデフォルトなので、無効にする場合は **no forceauthn** を使用します。

例

次の例では、salesforce_idp という名前の IdP を設定し、事前設定されたトラストポイントを使用します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)#saml idp salesforce_idp

ciscoasa(config-webvpn-saml-idp)#url sign-in
https://asa-dev-ed.my.salesforce.com/idp/endpoint/HttpRedirect
ciscoasa(config-webvpn-saml-idp)#url sign-out
https://asa-dev-ed.my.salesforce.com/idp/endpoint/HttpRedirect
```

```
ciscoasa(config-webvpn-saml-idp)#trustpoint idp salesforce_trustpoint
ciscoasa(config-webvpn-saml-idp)#trustpoint sp asa_trustpoint

ciscoasa(config)#show webvpn saml idp
saml idp salesforce_idp
url sign-in https://asa-dev-ed.my.salesforce.com/idp/endpoint/HttpRedirect
url sign-out https://asa-dev-ed.my.salesforce.com/idp/endpoint/HttpRedirect
trustpoint idp salesforce_trustpoint
trustpoint  sp asa_trustpoint
```

次の Web ページには、Onelogin の URL の取得方法について例が示されています。

https://onelogin.zendesk.com/hc/en-us/articles/202767260-Configuring-SAML-for-Clarizen

次の Web ページには、メタデータを使用して Onelogin から URL を検索する方法について、例が示されています。

http://onlinehelp.tableau.com/current/online/en-us/saml_config_onelogin.htm

次のタスク

SAML 2.0 サービス プロバイダー（SP）としての ASA の設定 （451 ページ） の説明に従って、SAML 認証を接続プロファイルに適用します。

SAML 2.0 サービス プロバイダー（SP）としての ASA の設定

特定のトンネル グループを SAML SP として設定するには、次の手順を実行します。

（注） AnyConnect 4.4 または 4.5 で SAML 認証を使用していて、ASA バージョン 9.7.1.24（またはそれ以降）、9.8.2.28（またはそれ以降）、または 9.9.2.1（またはそれ以降）（リリース日付：2018 年 4 月 18 日）を展開している場合、SAML のデフォルトの動作は、AnyConnect 4.4 および 4.5 でサポートされていない組み込みブラウザになります。したがって、AnyConnect 4.4 および 4.5 クライアントが外部（ネイティブ）ブラウザを使用して、SAML で認証するには、トンネル グループ設定で **saml external-browser** コマンドを使用する必要があります。

saml external-browser コマンドは、AnyConnect 4.6 以降にアップグレードするクライアントの移行のために使用されます。セキュリティ上の制限のため、AnyConnect ソフトウェアをアップグレードする際の一時的な移行の一環としてのみこのソリューションを使用してください。今後、このコマンド自体がサポートされなくなります。

始める前に

事前に IdP を設定しておく必要があります。SAML 2.0 アイデンティティ プロバイダー（IdP）の設定 （449 ページ）を参照してください。

手順

ステップ 1 トンネルグループ webvpn サブモードで、saml identify-provider コマンドを使用して IdP を割り当てます。

[**no**] **saml identify-provider** *idp-entityID*

idp-entityID：設定されている既存の IdP のいずれかを指定します。

SAML SP 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。

ステップ 2 現在のトンネル グループに対して SAML SP 機能をイネーブルにします。

authentication saml

SAML 認証方式は相互に排他的です。

例

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# tunnel-group-list enable
ciscoasa(config)# tunnel-group cloud_idp_onelogin type remote-access
ciscoasa(config)# tunnel-group cloud_idp_onelogin webvpn-attributes
ciscoasa(config-tunnel-webvpn)# authentication saml
ciscoasa(config-tunnel-webvpn)# group-alias cloud_idp enable
ciscoasa(config-tunnel-webvpn)# saml identity-provider
https://app.onelogin.com/saml/metadata/462950
```

SAML 2.0 と Onelogin の例

以下の例を実行する際は、Onelogin の情報とネーミングの代わりにサードパーティ製の SAML 2.0 IdP を使用してください。

1. IdP と ASA（SP）間での時刻の同期を設定します。

   ```
   ciscoasa(config)# ntp server 209.244.0.4
   ```

2. サードパーティ製 IdP で指定されている手順に従って、IdP から IdP の SAML メタデータを取得します。

3. トラストポイントに IdP の署名証明書をインポートします。

   ```
   ciscoasa(config)# crypto ca trustpoint onelogin
   ciscoasa(config-ca-trustpoint)# enrollment terminal
   ciscoasa(config-ca-trustpoint)# no ca-check
   ciscoasa(config-ca-trustpoint)# crypto ca authenticate onelogin
   Enter the base 64 encoded CA certificate.
   End with the word "quit" on a line by itself
   quit
   INFO: Certificate has the following attributes:
   Fingerprint:     85de3781 07388f5b d92d9d14 1e22a549
   Do you accept this certificate? [yes/no]: yes
   Trustpoint CA certificate accepted.
   % Certificate successfully imported
   ```

4. トラストポイントに SP（ASA）署名 PKCS12 をインポートします

   ```
   ciscoasa(config)# crypto ca import asa_saml_sp pkcs12 password
   Enter the base 64 encoded pkcs12.
   End with the word "quit" on a line by itself:
   quit
   INFO: Import PKCS12 operation completed successfully
   ```

5. SAML IdP を追加します。

```
ciscoasa(config-webvpn)# saml idp https://app.onelogin.com/saml/metadata/462950
```

6. saml-idp サブモードで属性を設定します。

   IdP サインイン URL とサインアウト URL を設定します。

```
ciscoasa(config-webvpn-saml-idp)# url sign-in
https://ross.onelogin.com/trust/saml2/http-post/sso/462950
ciscoasa(config-webvpn-saml-idp)# url sign-out
https://ross.onelogin.com/trust/saml2/http-redirect/slo/462950
```

   IdP トラストポイントと SP トラストポイントを設定します

```
ciscoasa(config-webvpn-saml-idp)# trustpoint idp onelogin
ciscoasa(config-webvpn-saml-idp)# trustpoint sp asa_saml_sp
```

   クライアントレス VPN ベース URL、SAML 要求の署名、および SAML アサーション タイムアウトを設定します。

```
ciscoasa(config-webvpn-saml-idp)# base-url https://172.23.34.222
ciscoasa(config-webvpn-saml-idp)# signature
ciscoasa(config-webvpn-saml-idp)# timeout assertion 7200
```

7. トンネル グループの IdP を設定し、SAML 認証をイネーブルにします。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# tunnel-group-list enable
ciscoasa(config)# tunnel-group cloud_idp_onelogin type remote-access
ciscoasa(config)# tunnel-group cloud_idp_onelogin webvpn-attributes
ciscoasa(config-tunnel-webvpn)# authentication saml
ciscoasa(config-tunnel-webvpn)# group-alias cloud_idp enable
ciscoasa(config-tunnel-webvpn)# saml identity-provider
https://app.onelogin.com/saml/metadata/462950
```

8. ASA の SAML SP メタデータを表示します。

   ASA の SAML SP メタデータは、`https://172.23.34.222/saml/sp/metadata/cloud_idp_onelogin` から取得できます。この URL の `cloud_idp_onelogin` は、トンネル グループ名です。

9. サードパーティ製 IdP で指定されている手順に従って、その IdP で SAML SP を設定します。

SAML 2.0 のトラブルシューティング

SAML 2.0 の動作をデバッグするには、**debug webvpn saml***value* を使用します。*value* に応じて次の SAML メッセージが表示されます。

- 8：エラー
- 16：警告およびエラー
- 128 または 255：デバッグ、警告、およびエラー

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。ASA は複数のコマンドを入力順に処理します（先に入力されたコマンドを優先）。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	スコープ
webvpn configuration	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 group-policy configuration	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 username configuration	個々のクライアントレス SSL VPN ユーザ

例

- 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。

```
hostname(config-webvpn)# auto-sign-on allow ip 10.1.1.1 255.255.255.0 auth-type
ntlm
```

- 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。

```
hostname(config-webvpn)# auto-sign-on allow uri https://*.example.com/* auth-type
```

- 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。

```
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
```

- *Anyuser* というユーザが IP アドレス範囲 10.1.1.0 ～ 10.1.1.255 のサーバに、HTTP 基本認証によって自動サインオンするように設定します。

```
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
```

- 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。

```
smart-tunnel auto-sign-on host-list [use-domain] [realm realm string] [port port
num] [host host mask | ip address subnet mask]
```

HTTP Form プロトコルによる 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。

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 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。

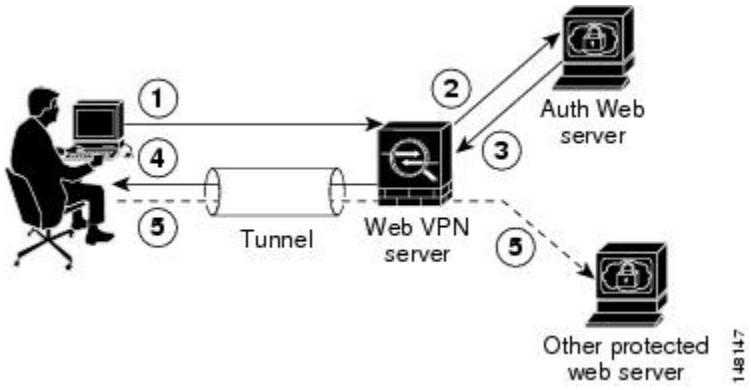
HTTP プロトコルを使用して SSO を正しく設定するには、認証と HTTP プロトコル交換についての詳しい実務知識が必要です。

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。

次の図は、後述する SSO 認証手順を示しています。

図 *9 : HTTP Form* を使用した *SSO* 認証



1. クライアントレス SSL VPN のユーザは、最初に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。
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する Web サーバに転送します。
3. 認証する 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。
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。
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。

ユーザ名やパスワードなどの POST データを ASA によって含めるようにフォーム パラメータを設定しても、Web サーバに必要な非表示のパラメータが追加されたことに、当初、ユーザは気づ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、ASA を仲介役のプロキシとして使用せずに、ブラウザから Web サーバに直接認証要求を行うことによって、認証 Web サーバに必要な非表示のパラメータを見つけることができます。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 サーバは非表示のパラメータのデータを必要とする場合、そのデータが省略されている認証 POST 要求をすべて拒否します。ヘッダーアナライザは非表示のパラメータが必須であるかオプションであるかを示さないため、必須パラメータを判別できるまでは、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 プロトコルを使用する SSO を設定するには、以下を実行する必要があります。

- フォーム データ（**action-uri**）を受信して処理するために、認証 Web サーバにユニフォーム 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 サーバが必要とするあらゆる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。

手順

ステップ 1 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。

aaa-server-host

ステップ 2 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。

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
```

この例では、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。

ステップ 3 認証 Web サーバ上の認証プログラムの URI を指定します。

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&SMAGENTNA
ME=$SM$5FZmjnk3DRNwNjk2KcqVCFbIrNT9%2bJ0H0KPshFtg6rB1UV2PxkHqLw%3d%3d&TARGET=https%3A%2F%2F
auth.example.com
```

この action 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=$SM$5FZmjnk
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
```

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 HTTP POST 要求の userid ユーザ名パラメータを設定します。

user-parameter

例：

```
hostname(config-aaa-server-host)# user-parameter userid
```

ステップ 5 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。

password-parameter

例：

```
hostname(config-aaa-server-host)# password-parameter user_password
```

ステップ 6 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。

hidden-parameter

例：

```
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
```

この例では、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、値は https%3A%2F%2Fwww.example.com%2Femco%2Fappdir%2FAreaRoot.do。
- %3FEMCOPageCode%3DENG。
- smauthreason、値は 0。

ステップ 7 認証クッキーの名前を指定します。

auth-cookie-name *cookie-name*

例：

```
hostname(config-aaa-server-host)# auth-cookie-name SsoAuthCookie
```

この例では、SsoAuthCookie の認証クッキー名を指定します。

ステップ 8 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。

tunnel-group general-attributes

ステップ 9 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。

authentication-server-group

例：

```
hostname(config)# tunnel-group testgroup general-attributes
hostname(config-tunnel-general)#authentication-server-group testgrp1
```

この例では、/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 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。

aaa-server-host

ステップ 11 認証クッキーの名前を指定します。

auth-cookie-name *cookie-name*

例：

```
hostname(config-aaa-server-host)# auth-cookie-name SsoAuthCookie
```

この例では、SsoAuthCookie の認証クッキー名を指定します。

ステップ 12 トンネル グループ一般属性モードに切り替えます。

tunnel-group general-attributes

ステップ 13 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。

authentication-server-group group

例：

```
hostname(config)# tunnel-group testgroup general-attributes
hostname(config-tunnel-general)#authentication-server-group testgrp1
```

この例では、/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。

始める前に

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

ステップ 1 ブラウザと HTTP ヘッダー アナライザを起動し、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
-ac05-83846dc90034&GUID=&SMAUTHREASON=0&METHOD=GET&SMAGENTNAME=$SM$5FZmjnk3DRNwNjk
2KcqVCFbIrNT9%2bJ0H0KPshFtg6rB1UV2PxkHqLw%3d%3d&TARGET=https%3A%2F%2Fwww.example.c
om%2Femco%2Fmyemco%2FHTTP/1.1

Host: www.example.com

(BODY)

SMENC=ISO-8859-1&SMLOCALE=US-EN&USERID=Anyuser&USER_PASSWORD=XXXXXX&target=https
%3A%2F%2Fwww.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。

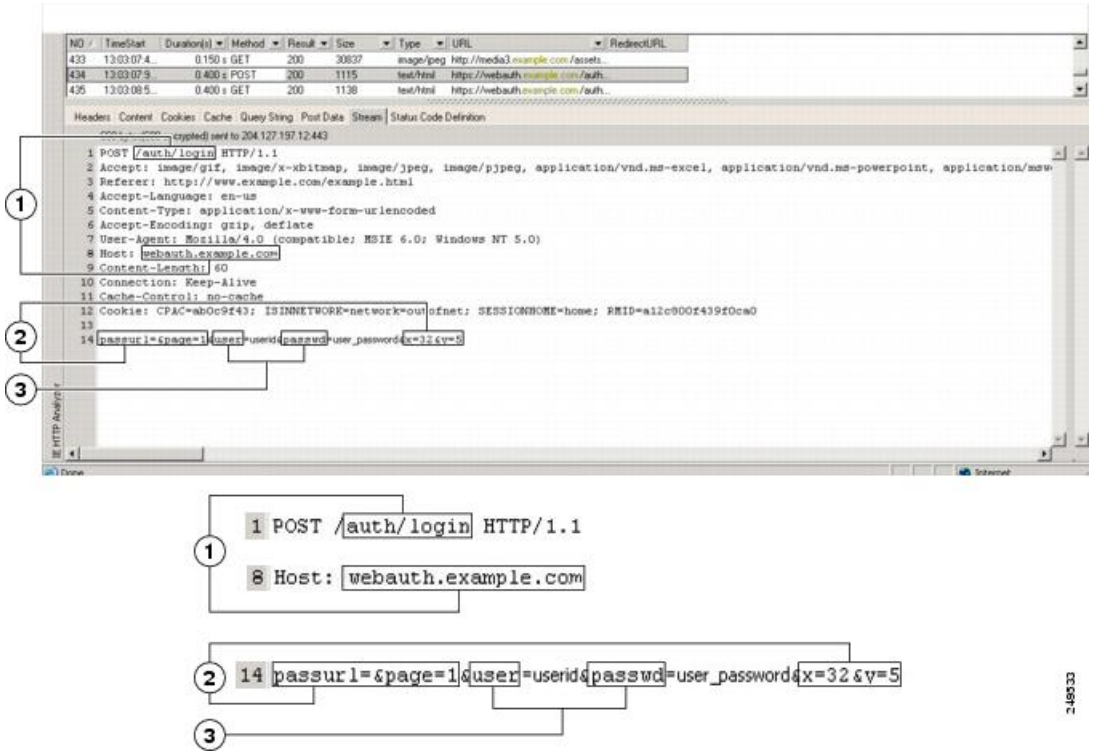
c) 非表示パラメータ。

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%2
Femco%2Fmyemco%2F&smauthreason=0
```

次の図は、HTTP アナライザの出力例におけるアクション 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ています。これは一例にすぎません。出力は Web サイトに応じて大きく異なります。

図 *10*：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



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に成功したら、HTTP ヘッダー アナライザを使用してサーバの応答を検証し、サーバによってブラウザに設定されたセッション クッキーの名前を探します。これは **auth-cookie-name** パラメータです。

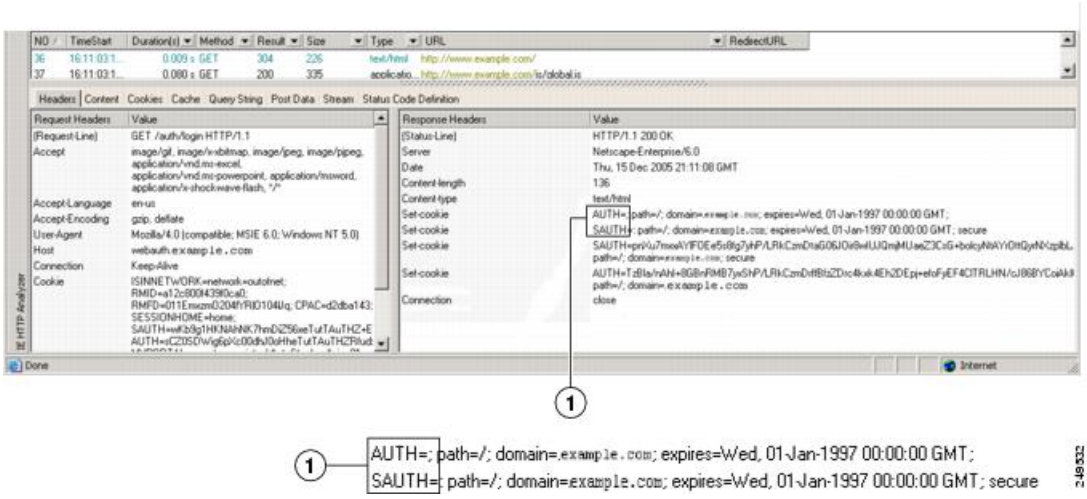
次のサーバ応答ヘッダーでは、SMSESSION がセッションのクッキーの名前です。必要なのはこの名前だけです。値は不要です。

```
Set-Cookie:
SMSESSION=yN4Yp5hHVNDgs4FT8dn7+Rwev41hsE49XlKc+1twie0gqnjbhkTkUnR8XWP3hvDH6PZ
PbHIHtWLDKTa8ngDB/lbYTjIxrbDx8WPWwaG3CxVa3adOxHFR8yjD55GevK3ZF4ujgU1lhO6fta0d
SSOSepWvnsCb7IFxCw+MGiw0o88uHa2t4l+SillqfJvcpuXfiIAO06D/gtDF40Ow5YKHEl2KhDEvv
+yQzxwfEz2cl7Ef5iMr8LgGcDK7qvMcvrgUqx68JQOK2+RSwtHQ15bCZmsDU5vQVCvSQWC8OMHNGw
pS253XwRLvd/h6S/tM0k98QMv+i3N8oOdj1V7flBqecH7+kVrU01F6oFzr0zM1kMyLr5HhlVDh7B0
```

```
k9wp0dUFZiAzaf43jupD5f6CEkuLeudYW1xgNzsR8eqtPK6t1gFJyOn0s7QdNQ7q9knsPJsekRAH9
hrLBhWBLTU/3B1QS94wEGD2YTuiW36TiP14hYwOlCAYRj2/bY3+lYzVu7EmzMQ+UefYxh4cF2gYD8
RZL2RwmP9JV5148I3XBFPNUw/3V5jf7nRuLr/CdfK3OO8+Pa3V6/nNhokErSgyxjzMd88DVzM41Lx
xaUDhbcmkoHT9ImzBvKzJX0J+o7FoUDFOxEdIqlAN4GNqk49cpi2sXDbIarALp6Bl3+tbB4MlHGH+
0CPscZXqoi/kon9YmGauHyRs+0m6wthdlAmCnvlJCDfDoXtn8DpabgiW6VDTrvl3SGPyQtUv7Wdah
uq5SxbUzjY2JxQnrUtwB977NCzYu2sOtN+dsEReWJ6ueyJBbMzKyzUB4L3i5uSYN50B4PCv1w5KdR
Ka5p3N0Nfq6RM6dfipMEJw0Ny1sZ7ohz3fbvQ/YZ7lw/k7ods/8VbaR15ivkE8dSCzuf/AInHtCzu
Q6wApzEp9CUoG8/dapWriHjNoi4llJOgCst33wEhxFxcWy2UWxs4EZSjsI5GyBnefSQTPVfma5dc/
emWor9vWr0HnTQaHP5rg5dTNqunkDEdMIHfbeP3F90cZejVzihM6igiS6P/CEJAjE;Domain=.exa
mple.com;Path=/
```

次の図は、HTTP アナライザの出力における許可クッキーの例を示しています。これは一例にすぎません。出力は Web サイトに応じて大きく異なります。

図 *11 : HTTP* アナライザの出力例における認可クッキー



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 ～ 6 を繰り返し、「失敗した」クッキーと「成功した」クッキーを比較します。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 データを用意できました。

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。Active Directory での LDAP 属性マッピングの例については、次の URL 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 *21 : 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。Active Directory での LDAP 属性マッピングの例については、次の URL 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。

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件

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。次の表に、クライアントレス SSL VPN ユーザが理解し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。

ログイン ユーザ名/パスワードのタイプ		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
Internet Service Provider：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
File Server	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 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リソース）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SSLVPNの機能を使用するためのリモート システムの設定

この項では、クライアントレス SSL VPN を使用するようにリモート システム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 について （466 ページ）

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 について

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 がサポートしている Web ブラウザのリストについては、サポート対象の VPN プラットフォーム、Cisco ASA 5500 シリーズ を参照してください。

クライアントレス SSL VPN の前提条件

- 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* 形式の https アドレスでなければなりません。*address* は、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://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。

（注） 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、クライアントレス SSL VPN セッションの終了を求めるメッセージが ASA によって表示されます。

ヒント テキスト フィールドにテキストを貼り付けるには、Ctrl+V を使用します（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）。

（注） 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 ヒントの通知 （465 ページ）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 ホーム 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 ホーム 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
  - 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。

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 ホーム ページ上にリンクとして表示されるものに限られる

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 ホーム 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**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。

重要なポイントは次のとおりです。

- 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。

（注） 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。

（注） この機能を使用するには、ユーザのマシンに Oracle Java ランタイム環境（JRE）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。

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。

  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て、[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て、[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

ポート フォワーディングを使用するには、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。

- アプリケーションを使用した後、ユーザは [Close]**Close**アイコンをクリックして必ず [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。

始める前に

- 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、ホスト 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 Runtime Environment（JRE）をインストールしておく必要があります。

  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、ユーザに対して使用可能なサイトが示されます。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。
  3. Java のインスタンスをすべて閉じます。
  4. 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。デフォルトでは有効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。

手順

ステップ 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。

ステップ 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。

ステップ 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。

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。

Microsoft Outlook Express バージョン 5.5 および 6.0 はテスト済みです。

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

（注） Web ベースの電子メール製品がインストールされており、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する必要がありますが、検証されていません。

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 （387 ページ）」を参照してください。

はじめる前に

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。

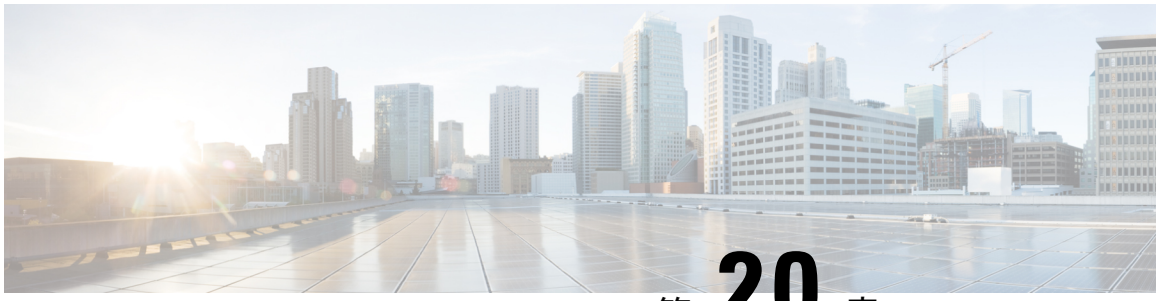
その他の SSL 対応クライアントも動作しますが、動作確認は行っていません。

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。

- スマート トンネルを使用する場合、Windows では ActiveX または JRE、Mac OS X では Java Web Start が必要です。
- ブラウザで Cookie 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。
- 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。
- サポートされているオペレーティング システムとブラウザだけを使用してください。
- 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。



第 20 章

モバイル デバイスでのクライアントレス SSL VPN

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

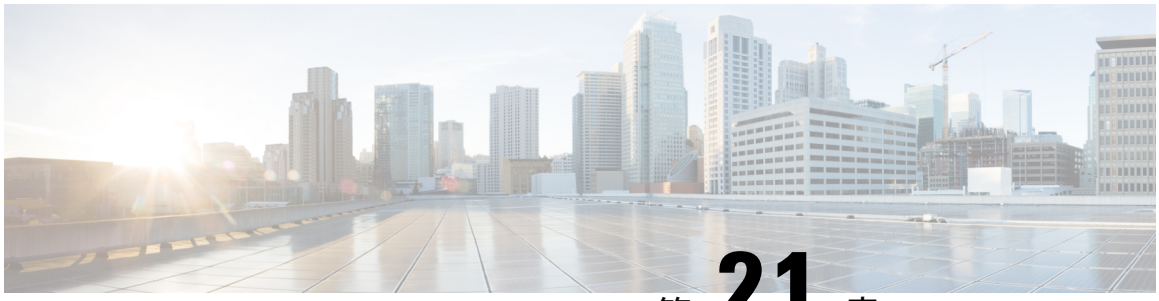
クライアントレス SSL VPN のモバイル デバイス バージョンに応じて、次のような相違点があります。

- 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。

モバイルでのクライアントレス SSL VPN の制限

- 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）



第 21 章

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、およびリモート 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。

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 パネルから構成されています。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、ログイン画面です。

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、このクライアントレス SSL

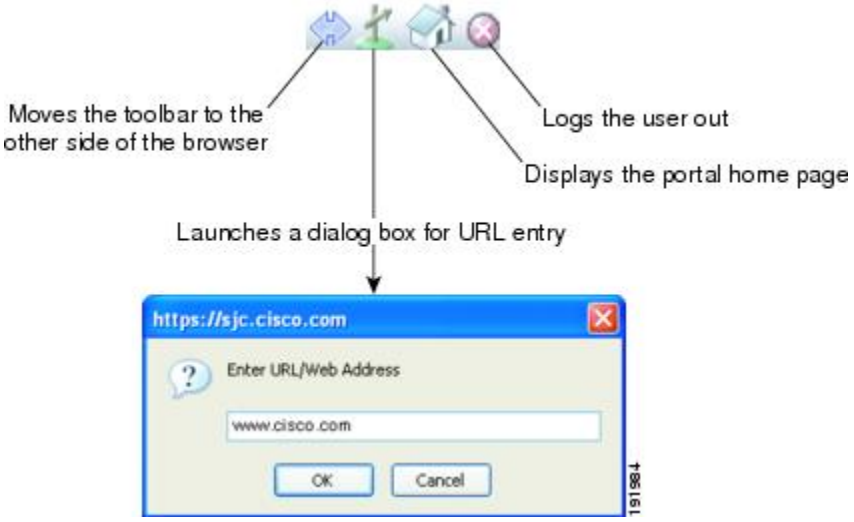
VPN 接続用に設定された TCP アプリケーションが表示されます。このパネルを開いたままでアプリケーションを使用する場合は、通常の方法でアプリケーションを起動します。

（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

次の図のフローティング ツールバーには、現在のクライアントレス SSL VPN セッションが示されます。

図 *12*：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、クライアントレス SSL VPN セッションの終了を求めるメッセージが ASA によって表示されます。

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承認後に表示される [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 をリロードするまで、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ついて

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、新しいカスタマイゼーション オブジェクトとして再び 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、エクスポートして編集し、新しいカスタマイゼーション オブジェクトとして再び 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、エクスポートして編集し、新しいカスタマイゼーション オブジェクトとして再び ASA にインポートできます。

手順

ステップ 1 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 タグを変更します。

export webvpn customization

ステップ 2 ファイルを新しいオブジェクトとしてインポートします。

import webvpn customization

例：

次の例では、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。

```
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#
```

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。

```
<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>(Chinese)</text>
        </language>
        <language>
```

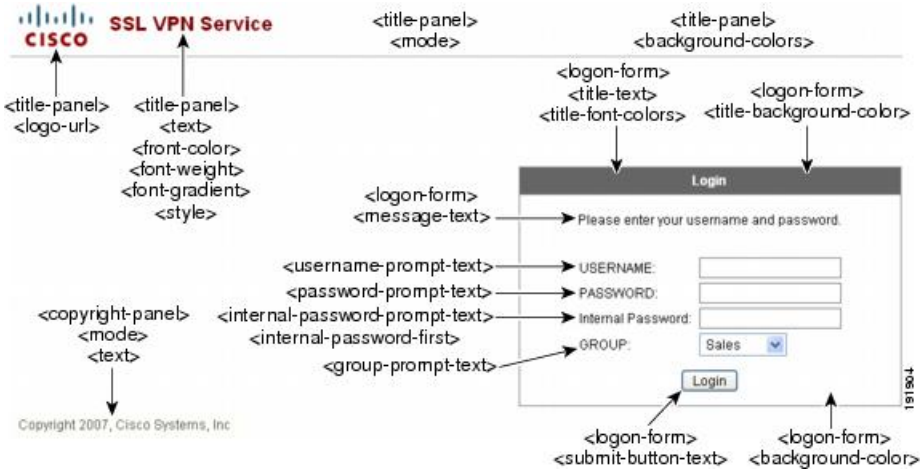
```
            <code>ja</code>
            <text>(Japanese)</text>
          </language>
          <language>
            <code>ru</code>
            <text>(Russian)</text>
          </language>
          <language>
            <code>ua</code>
            <text>(Ukrainian)</text>
          </language>
      </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>
            <username-prompt-text l10n="yes"></username-prompt-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>
```

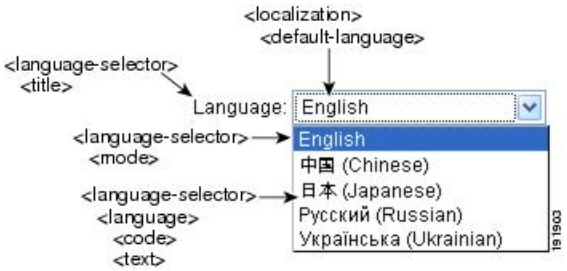
次の図に、[Login] ページとページをカスタマイズする XML タグを示します。これらのタグはすべて、上位レベルのタグ <auth-page> にネストされています。

図 *13 : [Login]* ページと関連 *XML* タグ



次の図に、[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 *14 : [Login]* 画面の言語セレクタと関連 *XML* タグ

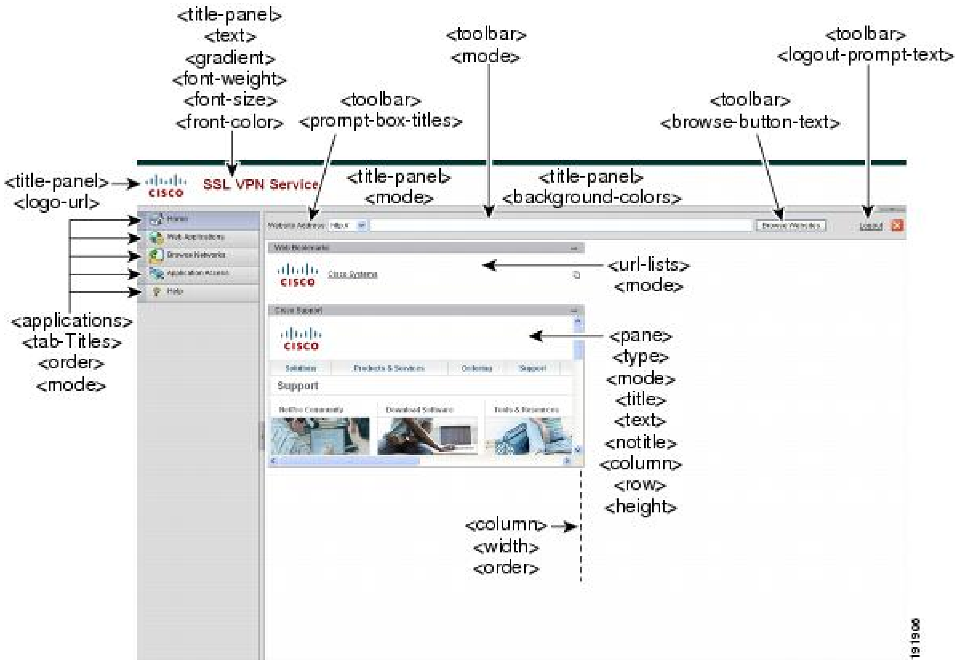


次の図に、[Login] ページで使用できる Information Panel とこの機能をカスタマイズするための XML タグを示します。この情報は [Login] ボックスの左側または右側に表示されます。これらのタグは、上位レベルの <auth-page> タグにネストされています。

図 *15 : [Login]* 画面の *[Information Panel]* と関連 *XML* タグ

次の図に、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 16 : [Portal] ページと関連 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ら、ASA のキャッシュ メモリにインポートします。カスタマイゼーション オブジェクトをインポートするとき、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。

import webvpn customization

次の例では、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。

```
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)
```

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。

手順

ステップ 1 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。

webvpn

ステップ 2 トンネル グループ、グループ ポリシー、または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。

tunnel-group webvpn または **group-policy webvpn** または **username webvpn**

ステップ 3 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。

customization *name*

または、カスタマイゼーションをグループまたはユーザに適用します。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、グループまたはユーザのカスタマイゼーションの名前です。

例：

次の例では、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。

```
hostname(config)# tunnel-group cisco_telecommuters webvpn-attributes
hostname(tunnel-group-webvpn)# customization cisco
```

次の例では、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。

```
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
```

次の例では、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。

```
hostname(config)# username cisco_employee attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)#customization value cisco
```

ステップ 4 （任意）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。

[**no**] **customization** *name*

ステップ 5 （任意） コンフィギュレーションからコマンドを削除して、デフォルトに戻します。

[**no**] **customization** {**none** | **value** *name*}

ステップ 6 既存のカスタマイゼーションのリストを表示します。

customization ?

ログイン画面の高度なカスタマイゼーション

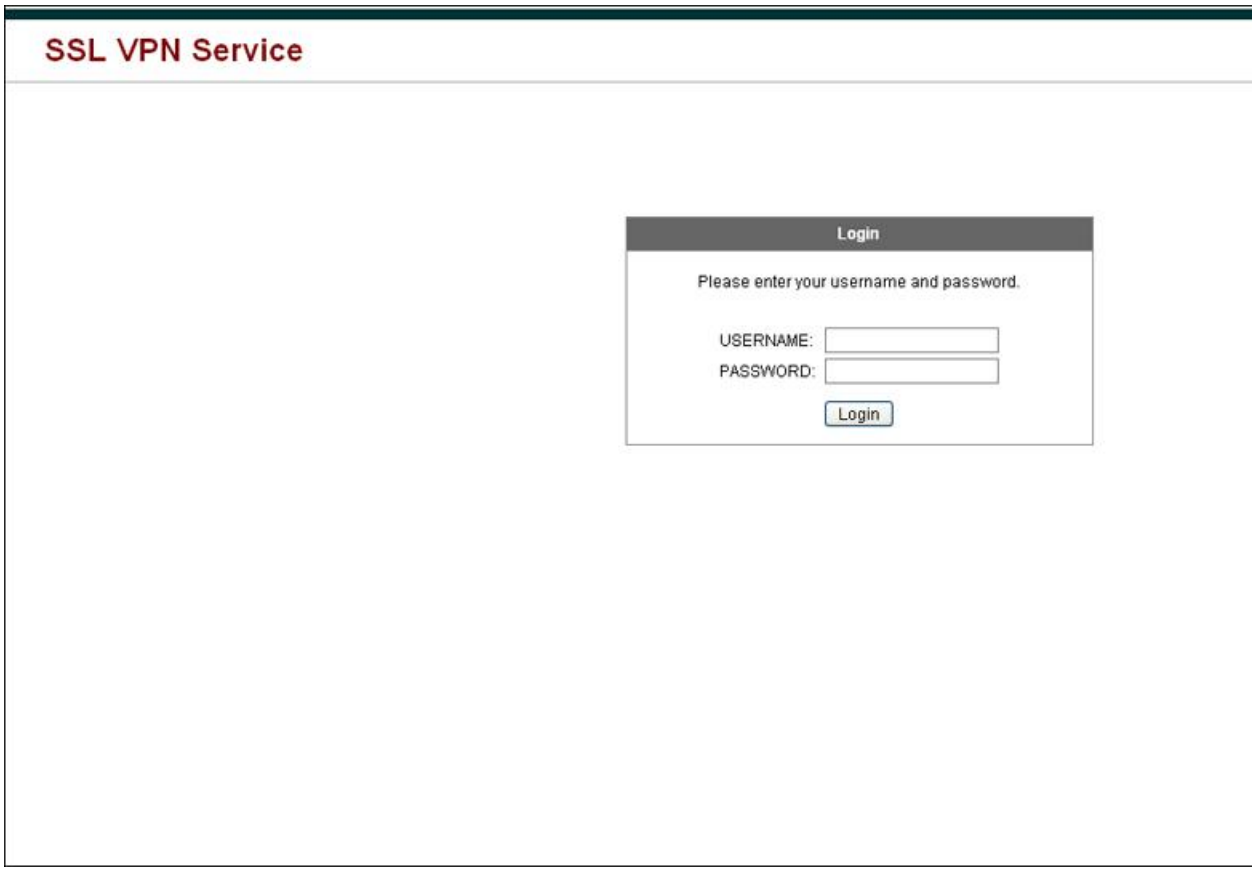
提供されるログイン画面の特定の画面要素を変更するのではなく、独自のカスタムログイン画面を使用する場合は、フル カスタマイゼーション機能を使用してこの高度なカスタマイゼーションを実行できます。

フル カスタマイゼーション機能を使用して、独自のログイン画面に HTML を配置し、ASA で関数を呼び出す Cisco HTML コードを挿入します。これにより、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、および ASA でユーザ独自のコードを使用するために設定する必要があるタスクについて説明します。

次の図に、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 *17* : 標準の *Cisco [Login]* ページ

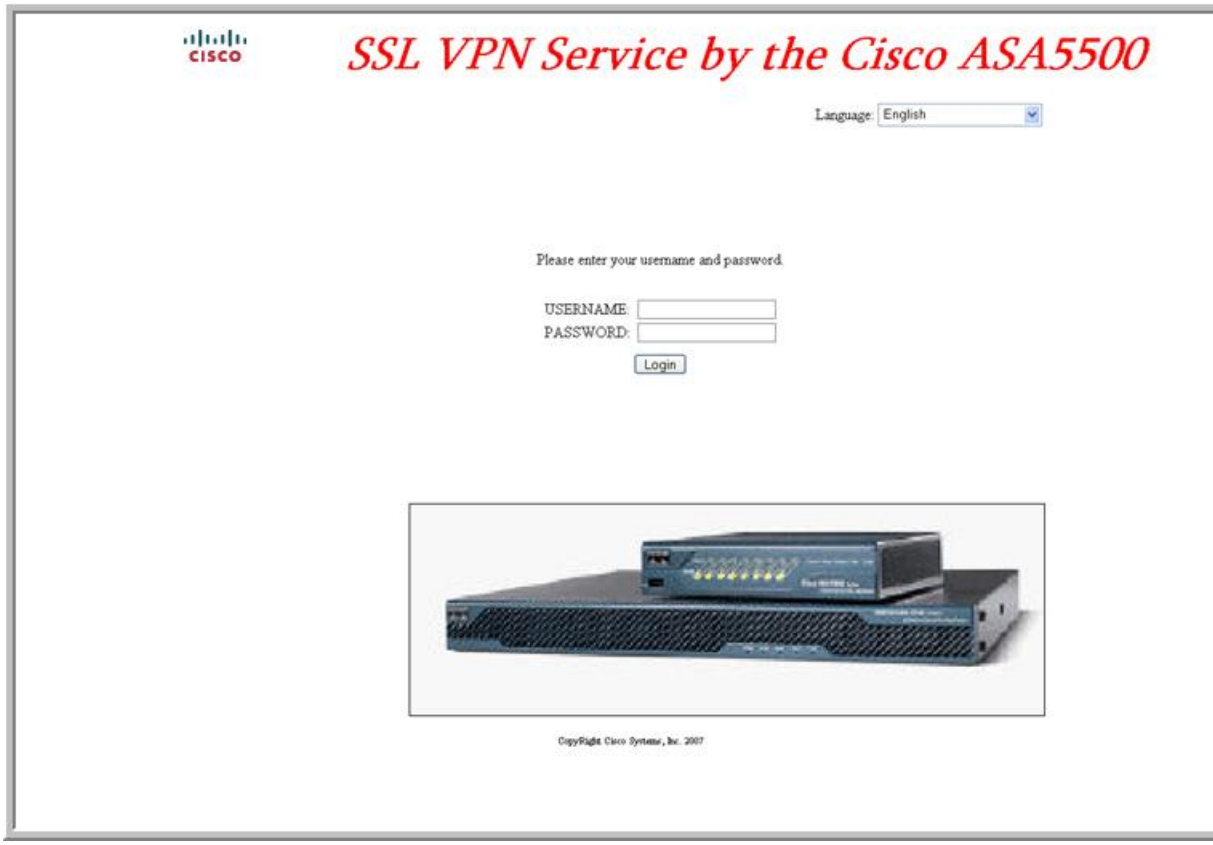


次の図に、[Language Selector]ドロップダウン リストを示します。この機能は、クライアントレス SSL VPN ユーザにはオプションとなっており、ログイン画面の HTML コード内の関数によっても呼び出されます。

図 *18* : 言語セレクタ ドロップダウン リスト

次の図に、フル カスタマイゼーション機能によって有効化される簡単なカスタム ログイン画面の例を示します。

図 *19 :* 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。

```
<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

ステップ 1 ファイルに login.inc という名前を付けます。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を変更して、/+CSCOU+/ を含めます。

認証前にリモートユーザに表示するファイルは、パス /+CSCOU+/ で表される ASA キャッシュメモリの特定の領域に配置する必要があります。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、選択され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。次の表に、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 *22 : VPN* アプリケーションのヘルプ ファイル

Application Type	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
規格	Application Access	/+CSCOE+/help/*language*/app_access_hlp.inc	Yes
規格	Browse Networks	/+CSCOE+/help/*language*/file_access_hlp.inc	Yes
規格	AnyConnect Client	/+CSCOE+/help/*language*/net_access_hlp.inc	Yes
規格	Web Access	/+CSCOE+/help/*language*/web_access_hlp.inc	Yes
プラグイン	MetaFrame Access	/+CSCOE+/help/*language*/ica_hlp.inc	No
プラグイン	Terminal Servers	/+CSCOE+/help/*language*/rdp_hlp.inc	Yes
プラグイン	Telnet/SSH Servers	/+CSCOE+/help/*language*/telnet_hlp.inc	Yes
プラグイン	VNC Connections	/+CSCOE+/help/*language*/vnc_hlp.inc	Yes

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。

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

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。

import webvpn webcontent *destination_url source_url*

- *destination_url* は、「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

次の例では、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。

```
hostname# import webvpn webcontent /+CSCOE+/help/en/app-access-hlp.inc
tftp://209.165.200.225/app-access-hlp.inc
```

フラッシュ メモリにインポートされているヘルプ ファイルのエクスポート

手順

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。

export webvpn webcontent *source_url destination_url*

- *source_url* は、「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、**the target 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

次の例では、[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。

```
hostname# export webvpn webcontent /+CSCOE+/help/en/file-access-hlp.inc
tftp://209.165.200.225/file-access-hlp.inc
```

言語変換について

ASA は、クライアントレス SSL VPN セッション全体に対する言語変換機能を備えています。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。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。次の表に、変換ドメインおよび、変換される機能領域を示します。

言語変換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。
バナー	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。

変換ドメイン	変換される機能エリア
カスタマイゼーション	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 フォワーディング 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。

一部のテンプレートはスタティックですが、ASA の設定に基づいて変化するテンプレートもあります。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、URL ブックマークはカスタマイズが可能なため、ASA は **ASA generates the 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

ステップ 1 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。

export webvpn translation-table

例：

次の例では、使用可能な変換テーブル テンプレートを示し、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す customization ドメインのテンプレートをエクスポートします。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。

```
hostname# show import webvpn translation-table
Translation Tables' Templates:
customization
AnyConnect

PortForwarder
url-list
webvpn
Citrix-plugin
RPC-plugin
Telnet-SSH-plugin
VNC-plugin

Translation Tables:

hostname#  export webvpn translation-table customization template
tftp://209.165.200.225/portal
```

ステップ 2 変換テーブルの XML ファイルを編集します。

例：

次の例は、*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ています。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。

```
# 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 ""
```

ステップ 3 変換テーブルをインポートします。

import webvpn translation-table

例：

次の例では、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。

```
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

customization
keepout
url-list
webvpn
Citrix-plugin
RPC-plugin
Telnet-SSH-plugin
VNC-plugin

Translation Tables:
es-us customization
```

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。

始める前に

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

ステップ 1 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。

export webvpn customization template

次の例では、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。

```
hostname# export webvpn customization template tftp://209.165.200.225/sales
```

ステップ 2 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。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。

次の例では、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> タグによって、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。

```
<localization>
      <languages>en,ja,zh,ru,ua</languages>
      <default-language>en</default-language>
   </localization>
```

次の例は、言語セレクタの表示に影響を与え、<language selector> タグとそれに関連する <language> タグにより、言語セレクタをイネーブルにして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。

```
<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>
```

ステップ 3 変更を行った後ファイルを保存します。

ステップ 4 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。

import webvpn customization

例：

ステップ 5 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。

show import webvpn customization

例：

```
hostname# import webvpn customization sales tftp://209.165.200.225/sales
hostname# !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

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

ステップ 1 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。

webvpn

ステップ 2 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。

group-policy webvpn

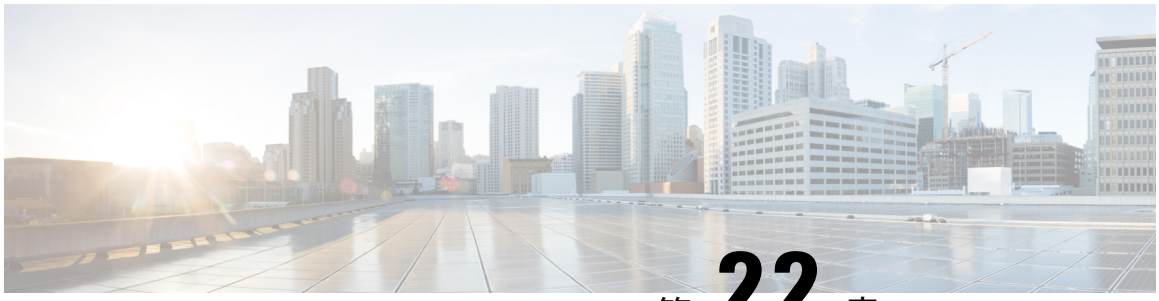
ステップ 3 カスタマイゼーション オブジェクトをイネーブルにします。

customization

例

次の例は、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ています。

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# customization value sales
```



第 22 章

クライアントレス SSL VPN のトラブルシューティング

Application Access 使用時の hosts ファイル エラーからの回復

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 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 が異常終了した場合は、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。

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 ファイルには、IP アドレスとホスト名がマッピングされています。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。

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

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。

[Applications Access] リンクをクリックします。

ステップ 2 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

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

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\sysem32\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。

ステップ 6 [Application Access] リンクをクリックします。

WebVPN 条件付きデバッグ

リモート アクセス VPN 上で複数のセッションを実行すると、ログのサイズを考慮するとトラブルシューティングが困難になることがあります。**debug webvpn condition** コマンドを使用して、デバッグ プロセスをより正確に絞り込むためのフィルタを設定できます。

debug webvpn condition {**group** *name* | **p-ipaddress** *ip_address* [{**subnet** *subnet_mask* | **prefix** *length*}] | **reset** | **user** *name*}

それぞれの説明は次のとおりです。

- **group** *name* は、グループ ポリシー（トンネル グループまたは接続プロファイルではない）でフィルタ処理を行います。
- **p-ipaddress** *ip_address* [{**subnet** *subnet_mask* | **prefix** *length*}] は、クライアントのパブリック IP アドレスでフィルタ処理を行います。サブネット マスク（IPv4）またはプレフィックス（IPv6）はオプションです。

- **reset** はすべてのフィルタをリセットします。**no debug webvpn condition** コマンドを使用して、特定のフィルタをオフにできます。
- **user** *name* は、ユーザ名でフィルタ処理を行います。

複数の条件を設定すると、条件が結合（AND で連結）され、すべての条件が満たされた場合にのみデバッグが表示されます。

条件フィルタを設定したら、基本の **debug webvpn** コマンドを使用してデバッグをオンにします。条件を設定するだけではデバッグは有効になりません。デバッグの現在の状態を表示するには、**show debug** および **show webvpn debug-condition** コマンドを使用します。

ASA VPN で複数のセッションが実行されている場合、単一のユーザー セッションをトラブルシューティングすることが煩わしくなります。条件付きデバッグを使用すると、フィルタ条件のセットに基づいて特定のセッションのログを検証できます。条件付きデバッグをサポートするモジュールは、SAML、WebVPN 要求および応答、Anyconnect です。

（注） IPv4 および IPv6 サブネットの「any, any」のサポートが提供されます。

次に、ユーザ jdoe で条件付きデバッグを有効にする例を示します。

```
asa3(config)# debug webvpn condition user jdoe

asa3(config)# show webvpn debug-condition
INFO: Webvpn conditional debug is turned ON
INFO: User name filters:
INFO: jdoe

asa3(config)# debug webvpn
INFO: debug webvpn  enabled at level 1.

asa3(config)# show debug
debug webvpn  enabled at level 1
INFO: Webvpn conditional debug is turned ON
INFO: User name filters:
INFO: jdoe
```

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。

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

ステップ 1 クライアントレス SSL VPN 用のキャプチャ ユーティリティを開始して、user2 のトラフィックをファイルにキャプチャする hr という名前のキャプチャを作成します。

capture capture_name type webvpn user webvpn_username

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。

例：

```
hostname# capture hr type webvpn user user2
WebVPN capture started.
   capture name   hr
   user name      user2
hostname# no capture hr
```

ステップ 2 （任意） ユーザがログインしてクライアントレス SSL VPN セッションを開始したら、キャプチャ ユーティリティによるパケットの取得を停止します。キャプチャ ユーティリティが *capture_name.zip* ファイルを作成します。このファイルはパスワード **koleso** で暗号化されます。

no capture capture_name

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。

ブラウザによるキャプチャ データの表示

手順

ステップ 1 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 capture_name type webvpn user webvpn_username

- *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 （任意） ユーザがログインしてクライアントレス SSL VPN セッションを開始したら、キャプチャ ユーティリティによるパケットの取得を停止します。

no capture capture_name

ステップ 3 ブラウザを開いて、hr という名前のキャプチャをスニファ形式で表示します。

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
```

クライアントレス SSL VPN セッション クッキーの保護

Flash アプリケーションや Java アプレットなどの組み込みオブジェクト、および外部アプリケーションは、通常は既存のセッションのクッキーに依存してサーバと連携しています。これらの組み込みオブジェクトは、初期化時にいくつかの Javascript を使用してブラウザからクッキーを取得します。クライアントレス SSL VPN セッション クッキーに httponly フラグを追加すると、セッションクッキーがブラウザのみで認識され、クライアント側のスクリプトでは認識されなくなり、セッションの共有は不可能になります。

始める前に

- VPN セッションのクッキー設定は、アクティブなクライアントレス SSL VPN セッションがない場合にだけ変更してください。
- クライアントレス SSL VPN セッションのステータスを確認するには、show vpn-sessiondb webvpn コマンドを使用します。
- vpn-sessiondb logoff webvpn コマンドを使用して、すべてのクライアントレス SSL VPN セッションからログアウトします。
- 次のクライアントレス SSL VPN 機能は、http-only-cookie コマンドがイネーブルの場合に動作しません。
  - Java プラグイン
  - Java リライタ
  - ポート フォワーディング。
  - ファイル ブラウザ
  - デスクトップ アプリケーション（Microsoft Office アプリケーションなど）を必要とする Sharepoint 機能

- AnyConnect Web 起動
- Citrix Receiver、XenDesktop、および Xenon
- その他の非ブラウザ ベース アプリケーションおよびブラウザ プラグイン ベースのアプリケーション

クライアントレス SSL VPN セッション Cookie が JavaScript などのクライアント側のスクリプトを介してサードパーティからアクセスされないようにするには、次の手順を実行します。

手順

クライアントレス SSL VPN セッションのクッキーで httponly フラグを有効にします。この設定はデフォルトでイネーブルになっています。

http-only-cookie

例：

```
hostname(config)# webvpn
hostname(config-webvpn)# http-only-cookie
```

（注） このコマンドは、Cisco TAC から使用を推奨された場合のみ使用してください。このコマンドをイネーブルにすると、「ガイドライン」に記載されているクライアントレス SSL VPN 機能が警告なしで動作しなくなるため、セキュリティ上のリスクが発生します。
