このマニュアルについて

このマニュアルでは、適用型セキュリティ アプライアンスにおける ASDM による VPN 機能の設定手順について説明します。

対象読者

このマニュアルは、Adaptive Security Device Manager を使用し、バーチャル プライベート ネットワークの ASA のセットアップや設定を行うシステムエンジニア（SE）および ネットワーク管理者を対象としています。読者は、ネットワーク機器、基本的なネットワークの概念、およびバーチャル プライベート ネットワークについて理解している必要があります。

マニュアルの構成

このマニュアルの構成は、次の通りです。

章番号	説明
第 1 章「デジタル証明書の登録」	デジタル証明書の登録、鍵ペアの生成、トラストポイントの生成、および証明書を取得する SCEP の使用について説明しています。
第 2 章「グループ ポリシーの設定」	グループ ポリシーの設定について説明しています。グループ ポリシーとトンネル グループ および ユーザの関連について説明しています。
第 3 章「SVC の設定」	VPN トンネル テクノロジーである SVC の設定について説明しています。これによって、ネットワーク管理者がリモート コンピュータへの IPSec VPN クライアントをインストールして設定しなくても、リモート ユーザは IPSec VPN クライアントの利点を利用できます。
第 4 章「Windows クライアントと VPN 3002　クライアントのクライアント アップデートの設定」	クライアント アップデートの設定方法について説明しています。これによって、中心的な場所にいる管理者が、VPN クライアント ユーザに VPN クライアント ソフトウェア および VPN 3002 ハードウェア クライアント イメージをアップデートする時期にあることを自動的に通知することができます。
第 5 章「DDNS アップデートの設定」	ダイナミック DNS リソース レコードをアップデートする DHCP サーバの設定方法について説明しています。
第 6 章「LDAP AAA サーバの設定」	セキュリティ アプライアンスと同じ内部ネットワークにある Microsoft Active Directory Server（LDAP）を使用して、セキュリティ アプライアンスのユーザ認証および認可を設定する手順の例を紹介しています。
第 7 章「Citrix MetaFrame サービスの設定」	Citrix MetaFrame サービスをサポートするセキュリティ アプライアンスの設定について説明しています。この場合の証明書の設定方法も示しています。
第 8 章「WebVPN に対する SSO の設定」	SSO について説明しています。これによって、WebVPN ユーザは、ユーザ名とパスワードを一度だけ入力して複数の保護されたサービスおよび Web サーバにアクセスできます。Siteminder SSO および HTTP Form プロトコルを設定する手順についても説明しています。
第 9 章「ネットワーク アドミッション コントロールの設定」	Network Admission Control（NAC; ネットワーク アドミッション コントロール）の設定について説明しています。これによって、実稼働環境でのネットワーク アクセスの条件として、エンドポイントの準拠性と脆弱性のチェックを実行し、ワーム、ウイルス、および不正アプリケーションによる侵入や感染から企業ネットワークを保護します。
第 10 章「L2TP over IPSec の設定」	セキュリティ アプライアンスの設定について説明します。これによって、リモート Windows クライアントが、Layer 2 Tunneling Protocol（L2TP）を使用して、パブリック IP ネットワークへアクセスし、プライベートおよび会社のネットワーク サーバと安全に通信できます。

章番号	説明
第 11 章「ロード バランシングの設定」	ロード バランシングの概念および ASA 5520 以降のモデルへのロード バランシングの設定方法について説明しています。
第 12 章「ASA 5505 での Easy VPN Services の設定」	ASA 5505 における VPN サービスの設定方法について説明しています。これによって、ハードウェア クライアントまたはヘッドエンドとして実行できますが、両方同時には実行できません。

関連マニュアル

このマニュアルは、次のユーザ ガイドと一緒に利用することができます。

- *Cisco ASA 5500 Series Release Notes*
- *Cisco ASDM Release Notes*
- *Regulatory Compliance and Safety Information for the Cisco ASA 5500 Series*
- *Cisco ASA 5500 Series Hardware Installation Guide*
- *Cisco ASA 5500 Series Quick Start Guide*
- *Cisco Security Appliance Command Line Configuration Guide*
- *Cisco Security Appliance Command Reference*
- *Migrating to ASA 7.1(1) from the VPN 3000 Series Concentrator*
- *Release Notes for Cisco Secure Desktop*
- *Cisco Security Appliance Logging Configuration and System Log Messages*

表記法

このマニュアルは、次の表記法を使用しています。

表記法	説明
太字	ユーザアクションおよびコマンドは、太字で示しています。
イタリック体	ユーザが値を指定する引数は、イタリック体で示しています。
screen フォント	システムが表示する端末セッションおよび情報は、screen フォントで示しています。
太字の **screen** フォント	入力する必要のある情報は、コマンド ライン インターフェイスの **boldface screen** フォントで示しています（たとえば、**vpnclient stat**）。

（注）は、次の表記法を使用しています。

（注） 「注釈」です。役立つ情報や、このマニュアル以外の参照資料などを紹介しています。

注意は、次の表記法を使用しています。

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。

システムを設定および管理する際、指示がある場合を除き、次のようにデータを入力してください。

データのタイプ	形式
IP アドレス	IP アドレスの表記には、4 バイトのドット付き 10 進法による表記法（たとえば、192.168.12.34）を使用してください。例で示すように、先頭の 0 を省略することができます。
サブネット マスクおよびワイルドカード マスク	サブネット マスクは、4 バイトのドット付き 10 進法による表記法（たとえば、255.255.255.0）を使用します。ワイルドカード マスクも、同じ表記法を使用します（たとえば、0.0.0.255）。例で示すように、先頭の 0 を省略することができます。
MAC アドレス	MAC アドレスは、6 バイトの 16 進数による表記法（たとえば、0001.03cf.0238）を使用します。
ホスト名	ホスト名は、正当なネットワーク ホスト名または、エンドシステム名による表記法（たとえば、VPN01）を使用します。スペースは、使用できません。ホスト名は、ネットワーク上の特定のシステムを一意に識別する必要があります。
文字列	文字列は、大文字および小文字の英数字を使用します。ほとんどの文字列は、大文字と小文字を区別します（たとえば、simon および Simon は、異なるユーザ名を示します）。通常、文字列の最大長は 48 文字です。
ポート番号	ポート番号は、0 から 65535 の 10 進数を使用します。番号中に、カンマやスペースは使用できません。

技術情報の入手方法

シスコの製品マニュアルやその他の資料は、Cisco.com でご利用いただけます。また、テクニカルサポートおよびその他のリソースを、さまざまな方法で入手することができます。ここでは、シスコ製品に関する技術情報を入手する方法について説明します。

Cisco.com

シスコの最新のマニュアルには、次の URL からアクセスできます。

http://www.cisco.com/univercd/home/home.htm

シスコの Web サイトには、次の URL からアクセスしてください。

http://www.cisco.com

また、シスコの Web サイトの各国語版へは、次の URL からアクセスできます。

http://www.cisco.com/public/countries_languages.shtml

シスコ製品の最新資料の日本語版は、次の URL からアクセスしてください。

http://www.cisco.com/jp

マニュアルの発注方法（英語版）

英文マニュアルの発注方法については、次の URL にアクセスしてください。

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

シスコ製品の英文マニュアルは、次の方法で発注できます。

- Cisco.com 登録ユーザ（Cisco Direct Customers）の場合、Ordering ツールからシスコ製品の英文マニュアルを発注できます。次の URL にアクセスしてください。
  http://www.cisco.com/en/US/partner/ordering/index.shtml
- Cisco.com に登録されていない場合、製品を購入された代理店へお問い合せください。

シスコシステムズマニュアルセンター

シスコシステムズマニュアルセンターでは、シスコ製品の日本語マニュアルの最新版を PDF 形式で公開しています。また、日本語マニュアル、および日本語マニュアル CD-ROM もオンラインで発注可能です。ご希望の方は、次の URL にアクセスしてください。

http://www2.hipri.com/cisco/

また、シスコシステムズマニュアルセンターでは、日本語マニュアル中の誤記、誤植に関するコメントをお受けしています。次の URL の「製品マニュアル内容不良報告」をクリックすると、コメント入力画面が表示されます。

http://www2.hipri.com/cisco/

なお、技術内容に関するお問い合せは、この Web サイトではお受けできませんので、製品を購入された各代理店へお問い合せください。

テクニカル サポート

シスコと正式なサービス契約を交わしているすべてのお客様、パートナー、および代理店は、Cisco Technical Support で 24 時間テクニカル サポートを利用することができます。Cisco.com の Cisco Technical Support Web サイトでは、多数のサポート リソースをオンラインで提供しています。また、Cisco Technical Assistance Center（TAC）のエンジニアが電話でのサポートにも対応します。シスコと正式なサービス契約を交わしていない場合は、代理店にお問い合せください。

Cisco Technical Support Web サイト

Cisco Technical Support Web サイトでは、シスコ製品やシスコの技術に関するトラブルシューティングにお役立ていただけるように、オンラインでマニュアルやツールを提供しています。この Web サイトは、24 時間 365 日、いつでも利用可能です。URL は次のとおりです。

http://www.cisco.com/techsupport

Cisco Technical Support Web サイトのツールにアクセスするには、Cisco.com のユーザ ID とパスワードが必要です。サービス契約が有効で、ユーザ ID またはパスワードを取得していない場合は、次の URL にアクセスして登録手続きを行ってください。

http://tools.cisco.com/RPF/register/register.do

（注） Web または電話でサービス リクエストを発行する前に、Cisco Product Identification（CPI）ツールを使用して製品のシリアル番号を確認してください。CPI ツールには、Cisco Technical Support Web サイトから、Documentation & Tools の下の **Tools & Resources** リンクをクリックするとアクセスできます。アルファベット順の索引ドロップダウン リストから **Cisco Product Identification Tool** を選択するか、Alerts & RMAs の下の **Cisco Product Identification Tool** リンクをクリックします。CPI ツールには、3 つの検索オプションがあります。製品 ID またはモデル名による検索、ツリー表示による検索、**show** コマンド出力のコピー アンド ペーストによる特定製品の検索です。検索結果では、製品が図示され、シリアル番号ラベルの位置が強調表示されます。ご使用の製品でシリアル番号ラベルを確認し、その情報を記録してからサービス コールをかけてください。

Japan TAC Web サイト

Japan TAC Web サイトでは、利用頻度の高い TAC Web サイト（http://www.cisco.com/tac）のドキュメントを日本語で提供しています。Japan TAC Web サイトには、次の URL からアクセスしてください。

http://www.cisco.com/jp/go/tac

サポート契約を結んでいない方は、「ゲスト」としてご登録いただくだけで、Japan TAC Web サイトのドキュメントにアクセスできます。Japan TAC Web サイトにアクセスするには、Cisco.com のログイン ID とパスワードが必要です。ログイン ID とパスワードを取得していない場合は、次の URL にアクセスして登録手続きを行ってください。

http://www.cisco.com/jp/register

サービス リクエストの発行

オンラインの TAC Service Request Tool を使用すると、S3 と S4 のサービス リクエストを短時間でオープンできます（S3：ネットワークに軽微な障害が発生した、S4：製品情報が必要である）。状況を入力すると、その状況を解決するための推奨手段が検索されます。これらの推奨手段で問題を解決できない場合は、シスコの TAC エンジニアが対応します。TAC Service Request Tool には、次の URL からアクセスできます。

http://www.cisco.com/techsupport/servicerequest

S1 または S2 のサービス リクエストの場合、またはインターネットにアクセスできない場合は、Cisco TAC に電話でお問い合せください（S1：ネットワークがダウンした、S2：ネットワークの機能が著しく低下した）。S1 および S2 のサービス リクエストには、Cisco TAC のエンジニアがすぐに割り当てられ、業務を円滑に継続できるようサポートします。

Cisco TAC の連絡先については、次の URL を参照してください。

http://www.cisco.com/techsupport/servicerequest

サービス リクエストのシビラティの定義

シスコでは、報告されるサービス リクエストを標準化するために、シビラティを定義しています。

シビラティ 1（S1）：ネットワークが「ダウン」した状態か、業務に致命的な損害が発生した場合。お客様およびシスコが、24 時間体制でこの問題を解決する必要があると判断した場合。

シビラティ 2（S2）：既存のネットワーク動作が著しく低下したか、シスコ製品が十分に機能しないため、業務に重大な影響を及ぼした場合。お客様およびシスコが、通常の業務中の全時間を費やして、この問題を解決する必要があると判断した場合。

シビラティ 3（S3）：ネットワークの動作パフォーマンスが低下しているが、ほとんどの業務運用は継続できる場合。お客様およびシスコが、業務時間中にサービスを十分なレベルにまで復旧させる必要があると判断した場合。

シビラティ 4（S4）：シスコ製品の機能、インストレーション、コンフィギュレーションについて、情報または支援が必要な場合。業務の運用には、ほとんど影響がありません。

その他の資料および情報の入手方法

シスコの製品、テクノロジー、およびネットワーク ソリューションに関する情報について、さまざまな資料をオンラインおよび印刷物で入手できます。

- Cisco Marketplace では、シスコの書籍やリファレンス ガイド、ロゴ製品を数多く提供しています。購入を希望される場合は、次の URL にアクセスしてください。

  http://www.cisco.com/go/marketplace/

- 『*Cisco Product Catalog*』には、シスコシステムズが提供するネットワーキング製品のほか、発注方法やカスタマー サポート サービスについての情報が記載されています。『*Cisco Product Catalog*』には、次の URL からアクセスしてください。

  http://cisco.com/univercd/cc/td/doc/pcat/

- Cisco Press では、ネットワーク全般、トレーニング、および認定資格に関する出版物を幅広く発行しています。これらの出版物は、初級者にも上級者にも役立ちます。Cisco Press の最新のオンライン情報などについては、次の URL からアクセスしてください。

  http://www.ciscopress.com

- 『*Packet*』はシスコシステムズが発行する技術者向けの雑誌で、インターネットやネットワークへの投資を最大限に活用するために役立ちます。本誌は季刊誌として発行され、業界の最先端トレンド、最新テクノロジー、シスコ製品やソリューション情報が記載されています。また、ネットワーク構成およびトラブルシューティングに関するヒント、コンフィギュレーション例、カスタマー ケース スタディ、認定情報とトレーニング情報、および充実したオンラインサービスへのリンクの内容が含まれます。『*Packet*』には、次の URL からアクセスしてください。

  http://www.cisco.com/packet

  日本語版『*Packet*』は、米国版『*Packet*』と日本版のオリジナル記事で構成されています。日本語版『*Packet*』には、次の URL からアクセスしてください。

  http://www.cisco.com/japanese/warp/public/3/jp/news/packet

- 『*iQ Magazine*』はシスコシステムズの季刊誌で、成長企業が収益を上げ、業務を効率化し、サービスを拡大するためには技術をどのように利用したらよいかを学べるように構成されています。本誌では、実例とビジネス戦略を挙げて、成長企業が直面する問題とそれを解決するための技術を紹介し、読者が技術への投資に関して適切な決定を下せるよう配慮しています。『*iQ Magazine*』には、次の URL からアクセスしてください。

  http://www.cisco.com/go/iqmagazine

- 『*Internet Protocol Journal*』は、インターネットおよびイントラネットの設計、開発、運用を担当するエンジニア向けに、シスコが発行する季刊誌です。『*Internet Protocol Journal*』には、次の URL からアクセスしてください。

  http://www.cisco.com/ipj

- シスコは、国際的なレベルのネットワーク関連トレーニングを実施しています。最新情報については、次の URL からアクセスしてください。

  http://www.cisco.com/en/US/learning/index.html