

シナリオ : サイトツーサイト VPN の設定

この章では、適応型セキュリティアプライアンスを使用したサイトツーサイト VPNの作成方法について説明します。

適応型セキュリティアプライアンスが提供するサイトツーサイト VPN 機能を使 用すると、ネットワーク セキュリティを維持しながら、低コストな公衆インター ネット接続で、ビジネス ネットワークを世界中のビジネス パートナー、および リモート オフィスに拡張できます。VPN 接続を使用すると、あるロケーション から別のロケーションに、セキュアな接続(トンネル)でデータを送信できま す。まず、接続の両端が認証され、次に、2 つのサイト間で送信されるすべての データが自動的に暗号化されます。

この章には、次の項があります。

- サイトツーサイト VPN ネットワーク トポロジの例 (P.8-2)
- サイトツーサイトのシナリオの実装 (P.8-3)
- VPN 接続の反対側の設定(P.8-14)
- 次の手順 (P.8-15)

サイトツーサイト VPN ネットワーク トポロジの例

サイトツーサイト VPN ネットワーク トポロジの例

図 8-1 で、2 つの適応型セキュリティ アプライアンス間の、VPN トンネルの例を 示します。

図 8-1 サイトツーサイト VPN の設定シナリオのネットワーク レイアウト



図 8-1 で示すような VPN サイトツーサイト配置の作成では、接続のそれぞれの 端で1つずつ、合計2つの適応型セキュリティ アプライアンスを設定する必要 があります。

サイトツーサイトのシナリオの実装

この項では、図 8-1 で示したリモートアクセスのシナリオのパラメータ例を使用 して、サイトツーサイト VPN 配置で適応型セキュリティ アプライアンスを設定 する方法を示します。

この項では次のトピックを取り上げます。

- 必要な情報(P.8-3)
- サイトツーサイト VPN の設定 (P.8-3)

必要な情報

設定手順を開始する前に、次の情報を収集します。

- リモート適応型セキュリティアプライアンスピアの IP アドレス
- トンネルを使用してリモート サイトのリソースと通信できるローカル ホス トおよびネットワークの IP アドレス
- トンネルを使用してローカル リソースと通信できるリモート ホストおよび ネットワークの IP アドレス

サイトツーサイト VPN の設定

この項では、ASDM VPN Wizard を使用してサイトツーサイト VPN 用に適応型セキュリティアプライアンスを設定する方法について説明します。

次のトピックについて取り上げます。

- ASDM の起動 (P.8-4)
- ローカル サイトでのセキュリティ アプライアンスの設定 (P.8-5)
- リモート VPN ピアに関する情報の入力 (P.8-7)
- IKE ポリシーの設定 (P.8-8)
- IPSec 暗号化および認証パラメータの設定(P.8-10)
- ホストおよびネットワークの指定(P.8-11)
- VPN アトリビュートの確認とウィザードの完了 (P.8-12)

次の項では、各設定手順の実行方法について詳しく説明します。

Cisco ASA 5550 スタートアップ ガイド ▮

ASDM の起動

Web ブラウザで ASDM を実行するには、アドレスフィールドに、工場出荷時の デフォルトの IP アドレス https://192.168.1.1/admin/ を入力します。



E)「s」を追加して「https」にすることに注意してください。追加しないと、 接続が失敗します。HTTPS(HTTP over SSL)は、ブラウザと適応型セ キュリティアプライアンスとの間でセキュアな接続を提供します。

ASDM のメイン ウィンドウが表示されます。



ローカル サイトでのセキュリティ アプライアンスの設定

(注)

E) 以後、最初のサイトの適応型セキュリティアプライアンスを、セキュリティア プライアンス1と呼びます。

セキュリティアプライアンス1を設定するには、次の手順を実行します。

ステップ1 ASDM のメイン ウィンドウの Wizards ドロップダウン リストで、VPN Wizard オ プションを選択します。最初の VPN Wizard 画面が表示されます。

VPN Wizard の Step 1 で、次の手順を実行します。

a. Site-to-Site VPN オプション ボタンをクリックします。



- Site-to-Site VPN オプションは、2 つの IPsec セキュリティ ゲートウェ イを接続します。これには、適応型セキュリティ アプライアンス、 VPN コンセントレータ、またはサイトツーサイト IPsec 接続をサポー トするその他のデバイスが含まれます。
- **b.** ドロップダウンリストで、現在の VPN トンネルに対してイネーブルにする インターフェイスとして outside を選択します。

サイトツーサイトのシナリオの実装



C. Next をクリックして続行します。

リモート VPN ピアに関する情報の入力

VPN ピアは、設定している接続の反対側にあるシステムで、通常、リモート サイトにあります。

(注)

このシナリオでは、以後、リモート VPN ピアをセキュリティ アプライアンス 2 と呼びます。

VPN Wizard の Step 2 で、次の手順を実行します。

- **ステップ1** Peer IP Address (セキュリティアプライアンス 2 の IP アドレス。このシナリオ では 209.165.200.236) と、Tunnel Group Name (「Cisco」など)を入力します。
- **ステップ2** 次の手順のいずれかを実行して、使用する認証の種類を指定します。
 - 認証にスタティックな事前共有キーを使用するには、Pre-Shared Key オプションボタンをクリックし、事前共有キー(「Cisco」など)を入力します。このキーは、適応型セキュリティアプライアンス間の IPsec ネゴシエーションで使用されます。



リモート サイトでセキュリティ アプライアンス 2 を設定するとき、 VPN ピアはセキュリティ アプライアンス 1 になります。ここで使用 するものと同じ事前共有キー(Cisco)を入力してください。

- Challenge/Response Authentication オプションボタンをクリックすると、この方法で認証されます。
- 認証にデジタル証明書を使用するには、Certificate オプション ボタンをク リックし、ドロップダウン リストで Certificate Signing Algorithm を選択し、 次のドロップダウン リストで事前設定されたトラスト ポイント名を選択し ます。

デジタル証明書を認証に使用するがトラストポイント名をまだ設定してい ない場合は、他の2つのオプションのいずれかを使用して Wizard を続行で きます。認証方式の設定は、標準の ASDM 画面を使用して後で変更できま す。

🖆 VPN Wizard		×
VPN Wizard	Remote Site Peer (Step 2 of 6)	
VPN Wizard	Remote Site Peer (Step 2 of 6) Configure the IP address of the peer device, authentication method and the tunnel group for this site-to-site tunnel. Peer IP Address: 209.165.200.236 Authentication Method • Pre-shared key Pre-Shared Key: Cisco Certificate Certificate Signing Algorithm: rsa-sig Trustpoint Name: ✓ Challenge/response authentication (CRACK) Tunnel Group For site-to-site connections with pre-shared key authentication, the tunnel group name must be the same as either the peer IP address or the peer hostname, whichever is used as the peer's identity.	
	Tunnel Group Name: 209.165.200.236	
	< Back Next > Finish Cancel Help]

ステップ3 Next をクリックして続行します。

IKE ポリシーの設定

IKE は、暗号化方式を含むネゴシエーションプロトコルで、データを保護し、機 密性を保証します。また、ピアのアイデンティティも保証する認証方式でもあり ます。ほとんどの場合、ASDM のデフォルト値で、2 つのピア間でセキュアな VPN トンネルを確立できます。

VPN Wizard の Step 3 で、次の手順を実行します。

ステップ1 IKE セキュリティ アソシエーションで、適応型セキュリティ アプライアンスが 使用する暗号化アルゴリズム (DES、3DES、または AES) 、認証アルゴリズム (MD5 または SHA)、および Diffie-Hellman グループ(1、2、または 5) をクリッ クします。

🖆 VPN Wizard		×	
VPN Wizard	IKE Policy (Step 3 of 6)		
Branch ISP Home Home	Select the encryption algorithm, authentication algorithm, and Diffie-Hellman group for the devices to use to negotiate an Internet Key Exchange (IKE) security association between them. Configurations on both sides of the connection must match exactly.		
Corpork	Encryption: 3DES		
	Authentication: SHA		
	DH Group: 2		
	< Back Next > Finish Cancel Hel	•	

<u>》</u> (注)

セキュリティアプライアンス2を設定するときは、セキュリティアプラ イアンス1で選択した各オプションの値を正確に入力する必要がありま す。暗号化の不一致は、VPNトンネル障害のよくある原因で、設定プロ セスを遅らせる原因になります。

ステップ2 Next をクリックして続行します。

IPSec 暗号化および認証パラメータの設定

VPN Wizard の Step 4 で、次の手順を実行します。

ステップ1 暗号化アルゴリズム (DES、3DES、または AES) および認証アルゴリズム (MD5 または SHA) をそれぞれのドロップダウン リストから選択します。

💕 VPN Wizard	X
VPN Wizard	IPSec Encryption and Authentication (Step 4 of 6)
Corporate Network	Select the encryption and authentication algorithms for this IPSec VPN tunnel. Configurations on both sides of the connection must match exactly. Encryption: 3DES Authentication: SHA
	< Back Next > Finish Cancel Help

ステップ2 Next をクリックして続行します。

ホストおよびネットワークの指定

この IPsec トンネルを使用してリモートサイト ピアと通信できるローカル サイ トのホストおよびネットワークを指定しますホストおよびネットワークを動的 に追加または削除するには、それぞれ、Add または Delete をクリックします。現 在のシナリオでは、Network A(10.10.10.0)からのトラフィックはセキュリティ アプライアンス 1 で暗号化され、VPN トンネルを使用して送信されます。

さらに、この IPsec トンネルを使用してローカル ホストおよびネットワークにア クセスできるリモート サイトのホストおよびネットワークを指定します。ホス トおよびネットワークを動的に追加または削除するには、それぞれ、Add または Delete をクリックします。このシナリオでは、セキュリティ アプライアンス 1の リモート ネットワークは Network B (10.20.20.0) なので、このネットワークか らの暗号化されたトラフィックは、トンネルを使用できます。

VPN Wizard の Step 5 で、次の手順を実行します。

- ステップ1 Source 領域の Type ドロップダウン リストで、IP Address を選択します。
- **ステップ2** ローカル IP アドレスとネットマスクを IP Address と Netmask の各フィールドに 入力します。
- **ステップ3** Destination 領域の Type ドロップダウン リストで、IP Address を選択します。
- **ステップ4** リモートホストまたはネットワークの IP アドレスおよびネットマスクを入力します。

サイトツーサイトのシナリオの実装

🖆 VPN Wizard	
VPN Wizard	Hosts and Networks (Step 5 of 6)
Branch Branch ISP Home Corporate Network	An IPSec tunnel protects data exchanged by selected hosts and networks at the local and remote sites. Please identify hosts and networks to be used in the IPSec tunnel. Host/Network Interface: outside Source Type: IP Address IP Address: 10.10.10.0 IP Address: 209.136.200.236 IP Address: 200.236 IP Address
	Netmask: 255.255.255.0 Image: Constraint of the state o

ステップ5 Next をクリックして続行します。

VPN アトリビュートの確認とウィザードの完了

VPN Wizard の Step 6 で、ここで作成した VPN トンネルの設定リストを確認しま す。設定が正しいことを確認したら、Finish をクリックし、設定の変更を適応型 セキュリティ アプライアンスに適用します。



設定の変更をスタートアップ設定に保存して、デバイスを次回に起動したときに この変更が適用されるようにする場合は、File メニューの Save をクリックしま す。

あるいは、ASDMの終了時に、設定の変更を保存するかどうか確認を求めるメッ セージが表示されます。

設定の変更を保存しないと、次回にデバイスを起動したときに、以前の設定が有 効になります。

これで、セキュリティアプライアンス1の設定プロセスは終わりです。

VPN 接続の反対側の設定

これで、ローカルな適応型セキュリティ アプライアンスが設定されました。次 に、リモート サイトの適応型セキュリティ アプライアンスを設定する必要があ ります。

リモート サイトでは、VPN ピアとして機能するように、2 番目の適応型セキュ リティ アプライアンスを設定します。ローカルな適応型セキュリティ アプライ アンスの設定手順のうち、P.8-5 の「ローカル サイトでのセキュリティ アプライ アンスの設定」から P.8-12 の「VPN アトリビュートの確認とウィザードの完了」 までを使用します。

(注)

セキュリティアプライアンス 2を設定するときは、セキュリティアプライアンス 1 で選択した各オプションと同じ値を、正確に入力する必要があります。不一致は、VPN トンネル設定エラーのよくある原因です。

次の手順

サイトツーサイト VPN 環境に、適応型セキュリティ アプライアンスを配置する だけの場合は、これで初期設定は終わりです。このほかに、次の手順について、 実行する必要があるかどうかを検討してください。

	参照先
設定の調整およびオプション機能	Cisco Security Appliance Command Line
と高度な機能の設定	Configuration Guide
	Cisco Security Appliance Command Reference
	Cisco Security Appliance Logging Configuration and System Log Messages

適応型セキュリティアプライアンスは、複数のアプリケーション用に設定できます。次の項で、その他の一般的なアプリケーション用に適応型セキュリティアプライアンスを設定する手順を説明します。

作業内容	参照先
DMZ内のWebサーバを保護する適	第6章「シナリオ:DMZの設定」
応型セキュリティ アプライアンス	
の設定	
リモートアクセス VPN の設定	第7章「シナリオ:リモートアクセス VPN
	の設定」