CHAPTER 1

Cisco ASA 1000V の概要

ASA 1000V は、VMware vSphere Hypervisor ソフトウェアおよび Cisco Nexus 1000V スイッチで排他的に実行するエッジ ファイアウォール仮想アプライアンスです。これにより、仮想データセンターの仮想マシン（VM）によるインターネットへのセキュアなアクセスを可能にし（テナント間通信を含む）、VM のデフォルト ゲートウェイとして機能して、ネットワークベースの攻撃から守ります。

（注） このマニュアルは、ASDM モードを使用して ASA 1000V を設定する方法について説明します（このモードで、ASA CLI を使用できます）。VNMC モードを使用する場合は、VNMC のマニュアルを参照してください。

この章は、次の項で構成されています。

ASA 1000V バージョン 8.7(1) の新機能

表 1-1 に、ASA 1000V バージョン 8.7(1) の新機能を示します。

表 1-1　ASA 1000V バージョン 8.7(1) の新機能

機能	説明
プラットフォーム機能	
ASA 1000V のサポート	Cisco Nexus 1000V スイッチと ASA 1000V のサポートが導入されました。

表 1-1　ASA 1000V バージョン 8.7(1) の新機能 （続き）

機能	説明
ASA 1000V のクローニング	VM のクローニング方法を使用して、現在の配置に ASA 1000V のインスタンスを 1 つ以上追加できます。
管理機能	
ASDM モード	ASA 1000V 用の単一 GUI ベースのデバイス マネージャである Adaptive Security Device Manager（ASDM）を使用して、ASA 1000V を設定、管理、およびモニタできます。
VNMC モード	複数のテナント用の GUI ベースのマルチデバイス マネージャである Cisco Virtual Network Management Center（VNMC）を使用して、ASA 1000V を設定および管理できます。
XML API	Cisco VNMC によって提供されるアプリケーション プログラムのインターフェイスである XML API を使用して、ASA 1000V を設定および管理できます。この機能は VNMC モードだけで使用できます。
ファイアウォール機能	
Cisco VNMC のアクセスと設定	Cisco VNMC のアクセスと設定では、セキュリティ プロファイルを作成する必要があります。[Configuration] > [Device Setup] > [Interfaces] ペインを使用して Cisco VNMC へのアクセスを設定できます。Cisco VNMC にアクセスするには、ログインのユーザ名とパスワード、ホスト名、および共有秘密を入力します。その後、セキュリティ プロファイルおよびセキュリティ プロファイル インターフェイスを設定します。VNMC モードでは、CLI を使用して、セキュリティ プロファイルを設定します。
セキュリティ プロファイルとセキュリティ プロファイル インターフェイス	セキュリティ プロファイルは、Cisco VNMC で設定され、Cisco Nexus 1000V VSM で割り当てられたエッジ セキュリティ プロファイルに対応するインターフェイスです。通過トラフィックのポリシーは、これらのインターフェイスと外部インターフェイスに割り当てられます。[Configuration] > [Device Setup] > [Interfaces] ペインを使用してセキュリティ プロファイルを追加できます。名前を追加し、サービス インターフェイスを選択することにより、セキュリティ プロファイルを作成します。ASDM は、Cisco VNMC により、セキュリティ プロファイルを生成し、セキュリティ プロファイル ID を割り当ててから自動的に一意のインターフェイスの名前を生成します。インターフェイス名は、セキュリティ ポリシー コンフィギュレーションで使用されます。 次のコマンドを導入または変更しました。**interface security-profile**、**security-profile**、**mtu**、**vpath path-mtu**、**clear interface security-profile**、**clear configure interface security-profile**、**show interface security-profile**、**show running-config interface security-profile**、**show interface ip brief**、**show running-config mtu**、**show vsn ip binding**、**show vsn security-profile**
サービス インターフェイス	サービス インターフェイスは、セキュリティ プロファイル インターフェイスに関連付けられたイーサネット インターフェイスです。内部インターフェイスであることが必要なサービス インターフェイスを 1 つだけ設定できます。 コマンド **service-interface security-profile all** が導入されました。
VNMC ポリシー エージェント	VNMC ポリシー エージェントは ASDM および VNMC モードの両方でポリシー設定をイネーブルにします。HTTPS 経由で Cisco VNMC から XML ベースの要求を受信し、ASA 1000V 設定に変換する Web サーバが含まれます。 次のコマンドが導入されました。**vnmc policy-agent**、**login**、**shared-secret**、**registration host**、**vnmc org**、**show vnmc policy-agent**、**show running-config vnmc policy-agent**、**clear configure vnmc policy-agent**

Cisco ASA 1000V でサポートされる機能およびサポートされていない機能

ASA 1000V では、ASA の機能のサブセットがサポートされます。表 1-2 に、ASA 1000V で主にサポートされる機能を示します。

表 1-2　ASA 1000V で主にサポートされる機能

機能	説明
管理アクセス用の AAA	第 17 章「管理アクセスの設定」を参照してください。
アクセル ルール	第 16 章「アクセス ルールの設定」を参照してください。
DHCP サーバ、DHCP クライアント、および DHCP リレー	第 6 章「DHCP の設定」を参照してください。
名前解決のための DNS サーバ	第 5 章「ホスト名、ドメイン名、パスワードなどの基本的な設定」を参照してください。
フェールオーバー	アクティブ/スタンバイのみ。第 3 章「アクティブ/スタンバイ フェールオーバーの設定」を参照してください。
インスペクション エンジン	GTP と IM インスペクション マップ（ディープ パケット インスペクション）を除く。第 19 章「アプリケーション レイヤ プロトコル インスペクションの準備」、第 20 章「基本インターネット プロトコルのインスペクションの設定」、第 21 章「音声とビデオのプロトコルのインスペクションの設定」、および第 23 章「管理アプリケーション プロトコルのインスペクションの設定」を参照してください。
IP 監査	第 25 章「保護ツールの使用」を参照してください。
IPsec サイトツーサイト VPN	スタティック トンネルのみ。第 28 章「LAN-to-LAN IPsec VPN の設定」を参照してください。
NAT	第 11 章「NAT に関する情報」、第 12 章「ネットワーク オブジェクト NAT の設定」、および第 13 章「Twice NAT の設定」を参照してください。
NTP および時間帯	第 5 章「ホスト名、ドメイン名、パスワードなどの基本的な設定」を参照してください。
SNMP MIB およびトラップ	第 30 章「SNMP の設定」を参照してください。
SSH および Telnet	第 17 章「管理アクセスの設定」を参照してください。
syslog メッセージ（TCP および UDP）	syslog メッセージ ガイドおよび第 29 章「ロギングの設定」を参照してください。
TCP 代行受信	第 24 章「接続の設定」を参照してください。

表 1-3 に、ASA 1000V でサポートされていない機能を示します。

（注）　サポートされていない機能に関連付けられたコマンドは、CLI ではサポートされません。

表 1-3　ASA 1000V でサポートされていない機能

機能	説明
ネットワーク アクセス用の AAA	サポートされていません。
アクティブ/アクティブ フェールオーバーとサブセカンド フェールオーバー	サポートされていません。
証明書を使用する認証	サポートされていません。
ボットネット トラフィック フィルタ	サポートされていません。
ダイナミック DNS	サポートされていません。
ダイナミック ルーティング	サポートされていません。
GTP/GTPRS（モバイル サービス プロバイダー）	サポートされていません。
ディープ パケット インスペクション用の HTTP インスペクション マップ	サポートされていません。
アイデンティティ ファイアウォール	サポートされていません。
受信 PAT	サポートされていません。
IPS および CSC モジュール	サポートされていません。
IPv6	サポートされていません。
マルチ コンテキスト	サポートされていません。
NetFlow	サポートされていません。
PPPoE/VPDN	サポートされていません。
QoS	サポートされていません。
冗長インターフェイス、EtherChannel インターフェイスおよびサブインターフェイス	サポートされていません。
shun	サポートされていません。
脅威の検出	サポートされていません。
トランスペアレント モード	サポートされていません。
ユニファイド コミュニケーション	サポートされていません。（TLS プロキシ、電話プロキシ、プロキシの制限と IME を含む）。
URL フィルタリング	サポートされていません。
VPN リモート アクセス	サポートされていません。（リモート アクセス、クライアントレス（SSL）アクセス、マルチサイト（SSL）アクセス、ASA 5505 上の Easy VPN、VPN Phone、AnyConnect Essentials および AnyConnect Mobile を含む）。
WCCP	サポートされていません。

ASA 1000V に関する詳細については、次の URL を参照してください。
http://www.cisco.com/en/US/products/ps12233/index.html

ASA 1000V の VMware 機能のサポート

表 1-4 に、ASA 1000V の VMware 機能のサポートを示します。

表 1-4　ASA 1000V の VMware 機能のサポート

機能	説明	サポート（Yes/No）	コメント
コールド クローン	クローニング前に VM の電源がオフになります。	Yes	—
DRS	動的リソースのスケジューリングおよび分散電源管理に使用されます。	Yes	—
ホット クローン	クローニング中に VM が動作しています。	No	—
スナップショット	VM を数秒間フリーズします。トラフィックが緩和される場合があります。フェールオーバーが発生することがあります。	コメントを参照してください。	使用には注意が必要です。
VM の移行	VM の移行に使用されます。	Yes	—
vMotion	VM のライブ マイグレーションに使用されます。	Yes	—
VMware FT	VM の HA に使用されます。	No	ASA 1000V VM の障害に対して ASA 1000V のフェールオーバーを使用します。
VMware HA	ESX およびサーバ障害に使用されます。	Yes	ASA 1000V VM の障害に対して ASA 1000V のフェールオーバーを使用します。
VM ハートビートの VMware HA	VM 障害に使用されます。	No	ASA 1000V VM の障害に対して ASA 1000V のフェールオーバーを使用します。

ASA 1000V 設定のタスク フロー

表 1-5 に、ASA 1000V の設定に関する主なタスクを示します。このマニュアルでは、次の表にリストされていない他のオプション機能も含まれます。

表 1-5　ASA 1000V 設定のタスク フロー

作業	参照先
1. VSN の設定。	『*Cisco Nexus 1000V Interface Configuration Guide*』を参照してください。
2. ASA 1000V の配置。	『*Cisco ASA 1000V Getting Started Guide*』を参照してください。
3. ASA 1000V ユーザ インターフェイスへの接続。	第 2 章「スタートアップ ガイド」を参照してください。
4. アクティブ/スタンバイ フェールオーバーの設定。	第 3 章「アクティブ/スタンバイ フェールオーバーの設定」を参照してください。
5. インターフェイスの設定。	第 4 章「インターフェイスの設定」を参照してください。

表 1-5　ASA 1000V 設定のタスク フロー （続き）

作業	参照先
6. ルーティングの設定。	第 7 章「スタティック ルートおよびデフォルト ルートの設定」を参照してください。
7. サービス ポリシーの設定。	第 14 章「モジュラ ポリシー フレームワークを使用したサービス ポリシーの設定」を参照してください。
8. アクセス ルールの設定。	第 16 章「アクセス ルールの設定」を参照してください。

ASA 1000V のクローニング

ASA 1000V の複数のインスタンスを展開できます。次の方法のいずれかを使用して、現在の配置に ASA 1000V のインスタンスを 1 つ以上追加することができます。

- 出荷時の OVA テンプレート：この方法では、さまざまな OVF 展開パラメータ セットを使用して、ASA 1000V の複数のインスタンスをクローニングすることができます。ASA 1000V のコンフィギュレーションはブランクで、インスタンスごとに OVF 展開パラメータから必要なコンフィギュレーション設定を取得します。
- 設定済み OVA テンプレート：この方法では、事前に設定された OVA テンプレートのクローンを可能にします。ASA 1000V にはすでにコンフィギュレーションが適用されていて、現在の OVF パラメータを再適用するだけです。その結果、必要なコンフィギュレーションが適用された、すぐに使用できる ASA 1000V のインスタンスを複数クローニングできます。
- VMware vSphere API：この方法では、アプリケーション プログラムのインターフェイスを使用して、既存の ASA 1000V をクローニングし、新しい ASA 1000V インスタンスごとに現在のコンフィギュレーション パラメータを変更できます。

クローニング要件

ここでは、次の内容について説明します。

- 「マスター ASA 1000V の準備」（P.1-6）
- 「マスターのクローニング」（P.1-7）

マスター ASA 1000V の準備

マスター ASA 1000V を準備するには、次の手順を実行します。

1. ASA 1000V を配置し、管理ルート、SSH アクセス、ユーザ名とパスワード、および ASDM アクセスを設定します。
2. 『*Cisco ASA 1000V Getting Stated Guide*』に示された手順を使用して、VNMC を登録します。
3. **write memory** コマンドを使用して、スタートアップ コンフィギュレーションに実行コンフィギュレーションを保存します。
4. ASA 1000V の電源を切ることが*重要です*。

（注）　電源がオンの ASA 1000V をクローニングした場合、クローニングの完了直後すぐに元の ASA 1000V がまれにクラッシュする可能性があります。

マスターのクローニング

マスター ASA 1000V をクローニングするには、次の手順を実行します。

1. vSphere クライアント GUI または他の同等な方法を使用して OVA テンプレートに ASA 1000V マスターをエクスポートします。たとえば、次のように、VMware の ovftool を使用できます。

```
ovftool vi://sample-vc50.example.com/performance-testbed/vm/ASA_1000V asa_master.ova
```

（注）　VSphere 4.x を使用して OVA テンプレートを作成すると、マスターで設定された vApp プロパティが削除されます。これは、ステップ 2 でクローンを展開する場合に、すべての vApp プロパティを指定する必要があることを意味します。

2. VSphere クライアント GUI または他の同等な方法を使用してクローニングされた ASA 1000V インスタンスを作成します。たとえば、次のように、VMware の ovftool を使用できます。

```
ovftool --acceptAllEulas --datastore="datastore1 (1)" "--net:VM Network=525-net-vm"
"--net:425-net-vm=60-net" "--net:60-net=425-net-vm" --prop:ManagementIPv4=2.2.2.5
--prop:ManagementIPv4Gateway=2.2.2.2 --prop:ManagementIPv4Subnet=255.255.0.0 --name="ASA
Clone 2 "  asa_master.ova
vi://sample-vc50.example.com/performance-testbed/host/sample-esxhost.example.com/
```

個別のインスタンスになるようにクローンの管理インターフェイスの IP アドレスを変更することが重要です。そのようにしないと、IP アドレスの競合が発生します。他のすべての vApp プロパティは、異なるパラメータを設定する必要がある場合に変更できます。OVA テンプレートが VSphere 4.x を使用して作成される場合、すべての vApp パラメータをクローンで指定する必要があることに注意してください。これらのパラメータはテンプレートに保存されないためです。

（注）　ovftool は ESXi 4.1 の配置を使用している場合はデフォルト値をエクスポートしません。ただし、ESXi 5.0 の配置はデフォルト値のエクスポートをサポートします。

次は、VMware から ovftool を使用して、プロパティをすべて設定する例です。

```
ovftool --acceptAllEulas --datastore="datastore1 (1)" "--net:VM Network=525-net-vm"
"--net:425-net-vm=60-net" "--net:60-net=425-net-vm" --prop:ManagementIPv4=2.2.2.5
--prop:ManagementIPv4Gateway=2.2.2.2 --prop:ManagementIPv4Subnet=255.255.0.0
--prop:ASDMIPv4=0.0.0.0 --prop:HAActiveIPv4=0.0.0.0 --prop:HASubnetIPv4=0.0.0.0
--prop:HAStandbyIPv4=0.0.0.0 --prop:ManagementStandbyIPv4=0.0.0.0 --prop:VNMCIPv4=0.0.0.0
--name="ASA Clone 2 "  asa_master.ova
vi://sample-vc50.example.com/performance-testbed/host/sample-esxhost.example.com/.
```

0.0.0.0 値でマークされたフィールドを使用する場合は正しく設定する必要があります。そうでない場合、0.0.0.0 として設定できます。

3. クローンの電源を入れます。

（注）　クローニングされた ASA 1000V がデフォルトの RSA キー ペアを同じ設定で再生成し、その他すべてのキーを削除します。

ASA 1000V のライセンスの強制

Nexus 1000V 仮想サービス モジュール（VSM）には、ASA 1000V で使用される各仮想イーサネット モジュール（VEM）の CPU ソケットの数を制御するライセンスが必要です。VSM に十分なライセンスがなく、ライセンスのサポートなしで ASA 1000V を配置する場合、トラフィックは ASA 1000V を通過できません。これは次のことを意味します。

- 内部から外部へのトラフィックの場合、トラフィックは、ASA 1000V に到達しません。詳細については、syslog 4450002 を参照してください。
- 外部から内部へのトラフィックの場合、ASA 1000V が初期パケットの通過を許可しますが、Nexus 1000V の vPath モジュールはパケットを拒否し、ASA 1000V でフローが削除されます。詳細については、syslog 4450002 を参照してください。

ASA 1000V の設定例

特定の機能の設定例は、『*Cisco ASA 1000V Getting Started Guide*』で説明しています。

ASA 1000V のモニタリング

SSH、Telnet、コンソールの他、ASDM モードおよび VNMC モードの両方で（読み取り専用ビューの ASDM のモニタリング ペインにアクセスして）ASA 1000V をモニタできます。このプラットフォーム用に導入または変更した ASA 1000V のコマンドは、このマニュアルのそれぞれの機能の章の最後にある機能履歴の表に記載されています。

ファイアウォール機能の概要

ファイアウォールは、外部ネットワーク上のユーザによる不正アクセスから内部ネットワークを保護します。ファイアウォールは、特定のアドレスだけを外部へ許可することによって、内部ユーザが外部ネットワークにアクセスするときの（たとえば、インターネットへのアクセス）制御を可能にします。

ファイアウォールに接続するネットワークを説明する場合、*外部*ネットワークはファイアウォールの前にあり、*内部*ネットワークはファイアウォールの背後で保護されます。ASA 1000V は、内部 1 つと外部 1 つの 2 つのデータ インターフェイスを許可します。さらに管理インターフェイスとフェールオーバー用のインターフェイスを使用できます。ASA 1000V では、複数のセキュリティ プロファイル インターフェイスを作成でき、内部インターフェイス上の仮想マシン（VM）が外部にアクセスするときに各種セキュリティ ポリシーを提供できます。（VM 間のトラフィックは、Cisco VSG を使用して制御されます）。

ASA 1000V で許容される同時ファイアウォール接続の最大数は 200,000 です。

この項は、次の内容で構成されています。

セキュリティ ポリシーの概要

他のネットワークにアクセスするために、ファイアウォールを通過することが許可されるトラフィックがセキュリティ ポリシーによって決められます。デフォルトでは、ASA 1000V は、内部ネットワーク（高セキュリティ レベル）のセキュリティ プロファイル インターフェイスから外部ネットワーク（低セキュリティ レベル）にトラフィックを自由に通過させます。トラフィックにアクションを適用してセキュリティ ポリシーをカスタマイズすることができます。

この項は、次の内容で構成されています。

アクセス リストによるトラフィックの許可または拒否（ルール）

アクセス ルールを適用して、内部のセキュリティ プロファイルから外部へのトラフィックを制限したり、外部から内部のセキュリティ プロファイルへのトラフィックを許可したりできます。

NAT の適用

NAT の利点のいくつかを次に示します。

- 内部ネットワークでプライベート アドレスを使用できます。プライベート アドレスは、インターネットにルーティングできません。
- NAT はローカル アドレスを他のネットワークから隠蔽するため、攻撃者はホストの実際のアドレスを取得できません。
- NAT は、重複 IP アドレスをサポートすることで、IP ルーティングの問題を解決できます。

IP フラグメントからの保護

ASA 1000V は IP フラグメント保護を提供します。この機能は、すべての ICMP エラー メッセージの完全リアセンブリ、および ASA 1000V を介してルーティングされる残りの IP フラグメントの仮想リアセンブリを実行します。セキュリティ チェックに失敗したフラグメントは、ドロップされログに記録されます。仮想リアセンブリはディセーブルにできません。

アプリケーション インスペクションの適用

インスペクション エンジンは、ユーザのデータ パケット内に IP アドレッシング情報を埋め込むサービスや、ダイナミックに割り当てられるポート上でセカンダリ チャネルを開くサービスに必要です。

接続の制限と TCP 正規化の適用

TCP 接続、UDP 接続、および初期接続を制限することができます。接続と初期接続の数を制限することで、DoS 攻撃（サービス拒絶攻撃）から保護されます。ASA 1000V では、初期接続制限を利用して TCP 代行受信をトリガーします。代行受信によって、TCP SYN パケットを使用してインターフェイスをフラッディングすることにより行われる DoS 攻撃から内部システムを保護します。初期接続とは、送信元と宛先の間で必要になるハンドシェイクを完了していない接続要求のことです。

TCP 正規化は、正常に見えないパケットをドロップするように設計された高度な TCP 接続設定で構成される機能です。

フェールオーバーの概要

ハイ アベイラビリティを設定するには、専用のステートフル フェールオーバー リンクで相互に接続されている 2 台の同じ ASA 1000V が必要です。フェールオーバー ペアの 2 台の ASA 1000V は、フェールオーバー リンク経由で常に通信して、それぞれの動作ステータスを確認します。アクティブ インターフェイスの状態がモニタされて、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別されます。所定の条件に一致すると、フェールオーバーが行われます。

フェールオーバー リンクとして ASA 1000V 上の GigabitEthernet 0/2 インターフェイスを使用できます。フェールオーバー リンク インターフェイスは、通常のネットワーク インターフェイスとしては設定されません。フェールオーバー通信のためにだけ存在します。このインターフェイスは、フェールオーバー リンク（および、オプションでステートフル フェールオーバー リンク）専用とする必要があります。

ASA 1000V はアクティブ/スタンバイ フェールオーバーだけをサポートします。1 つの ASA 1000V でトラフィックを渡し、もう 1 つの ASA 1000V はスタンバイ状態で待機します。

ファイアウォール モードの概要

ASA 1000V はルーテッド ファイアウォール モードでしか稼働せず、ネットワークのルータ ホップと見なされます。

ステートフル インスペクションの概要

ASA 1000V を通過するトラフィックはすべて、アダプティブ セキュリティ アルゴリズムを使用して検査され、通過が許可されるか、またはドロップされます。単純なパケット フィルタは、送信元アドレス、宛先アドレス、およびポートが正しいかどうかはチェックできますが、パケット シーケンスまたはフラグが正しいかどうかはチェックしません。また、フィルタはすべてのパケットをフィルタと照合してチェックするため、処理が低速になる場合があります。

（注）　TCP ステート バイパス機能を使用すると、パケット フローをカスタマイズできます。「TCP ステート バイパス」（P.24-3）を参照してください。

ただし、ASA 1000V のようなステートフル ファイアウォールは、パケットの次のようなステートについて検討します。

- 新規の接続かどうか。

新規の接続の場合、ASA 1000Vは、パケットをアクセス リストと照合してチェックする必要があり、これ以外の各種のタスクを実行してパケットの許可または拒否を決定する必要があります。このチェックを行うために、セッションの最初のパケットはセッション管理パスを通過しますが、トラフィックのタイプに応じて、コントロール プレーン パスも通過する場合があります。

セッション管理パスで行われるタスクは次のとおりです。

- アクセス リストとの照合チェック
- ルート ルックアップ
- NAT 変換（xlates）の割り当て
- 高速パスでのセッションの確立

レイヤ 7 インスペクションが必要なパケット（パケットのペイロードの検査または変更が必要）は、コントロール プレーン パスに渡されます。レイヤ 7 インスペクション エンジンは、2 つ以上のチャネルを持つプロトコルで必要です。2 つ以上のチャネルの 1 つは周知のポート番号を使用するデータ チャネルで、その他はセッションごとに異なるポート番号を使用するコントロール チャネルです。このようなプロトコルには、FTP、H.323、および SNMP があります。

- 確立済みの接続かどうか。

  接続がすでに確立されている場合は、ASA 1000V でパケットの再チェックを行う必要はありません。一致するパケットの大部分は、両方向で高速パスを通過できます。高速パスで行われるタスクは次のとおりです。

  - IP チェックサムの確認
  - セッション ルックアップの実行
  - TCP シーケンス番号のチェック
  - 既存のセッションに基づく NAT 変換の割り当て
  - レイヤ 3 およびレイヤ 4 ヘッダーの調整

  UDP プロトコルまたは他のコネクションレス型プロトコルに対して、ASA 1000Vはコネクション ステート情報を作成して、高速パスも使用できるようにします。

  レイヤ 7 インスペクションを必要とするプロトコルに合致するデータ パケットも高速パスを通過できます。

  確立済みセッション パケットの中には、セッション管理パスまたはコントロール プレーン パスを引き続き通過しなければならないものがあります。セッション管理パスを通過するパケットには、インスペクションまたはコンテンツ フィルタリングを必要とする HTTP パケットが含まれます。コントロール プレーン パスを通過するパケットには、レイヤ 7 インスペクションを必要とするプロトコルのコントロール パケットが含まれます。

IPsec サイトツーサイト VPN の機能概要

サイトツーサイト（LAN-to-LAN VPN）は、地理的に異なる場所にネットワークを接続します。ASA 1000V は、2 つのピアに IPv4 の内部および外部インターフェイスがある場合、シスコまたはサードパーティのピアへの IPsec サイトツーサイト接続（トンネルと呼ばれます）をサポートします。IPsec トンネル モードは、トラフィックが中間の非信頼ネットワークを通る場合、異なるネットワーク間のトラフィックを保護するために役立ちます。

IPsec サイトツーサイト トンネルでサポートされるプロトコルは、事前共有キーだけを使用する IKEv1 と IKEv2 です。事前共有キーまたは共有秘密は VPN が他のクレデンシャルの前に受信を待機するテキストの文字列です（ユーザ名やパスワードなど）。スプリット トンネルもサポートされ、どのトラフィックをクライアントが VPN トンネルを通じて渡すか、どのトラフィックをインターネットへ通過させるか（非トンネル）、ネットワーク管理者が決定できます。

サポートされるトンネル モードは、カプセル化セキュリティ ペイロード（ESP）単独、および ESP と認証ヘッダー（AH）の組み合わせです。AH トンネル モードは、AH と IP ヘッダーを含む IP パケットをカプセル化し、整合性と認証用にパケット全体に署名します。ESP トンネル モードは、ESP と IP ヘッダーを含む IP パケット、および ESP 認証トレーラをカプセル化します。トンネリングの際、ESP と AH は連結できるため、トンネリングされた IP パケットのセキュリティ、およびパケット全体の整合性と認証の両方を提供します。

さらに、NAT 通過は、IPsec サイトツーサイト VPN クライアントでサポートおよび使用されて、ESP パケットが NAT を通過できるようになります。

その他の参考資料

ASA 1000V を構成する個々のコンポーネントの詳細については、次のマニュアルを参照してください。

- ASA 1000V
  http://www.cisco.com/en/US/products/ps12233/tsd_products_support_series_home.html
- ASDM
  http://www.cisco.com/en/US/products/ps6120/products_installation_and_configuration_guides_list.html
- Cisco Nexus 1000V
  http://www.cisco.com/en/US/products/ps9902/tsd_products_support_series_home.html
- Cisco VNMC および Cisco VSG
  http://www.cisco.com/en/US/products/ps11213/tsd_products_support_series_home.html
- VMware
  http://www.vmware.com/support/pubs/