CHAPTER 1

Cisco ASA の概要

Cisco ASA は、高度なステートフル ファイアウォールと VPN コンセントレータの機能を 1 台のデバイスに集約した製品です。モデルによっては、IPS などのサービス モジュールが統合されています。ASA は多数の高度な機能を備えています。たとえば、マルチ セキュリティ コンテキスト（仮想ファイアウォールに類似）、クラスタリング（複数のファイアウォールを結合して 1 つのファイアウォールにする）、トランスペアレント（レイヤ 2）ファイアウォールまたはルーテッド（レイヤ 3）ファイアウォール動作、高度なインスペクション エンジン、IPsec VPN、SSL VPN、クライアントレス SSL VPN のサポートなどがあります。

この章は、次の項で構成されています。

ハードウェアとソフトウェアの互換性

サポートされているハードウェアおよびソフトウェアの完全なリストについては、『*Cisco ASA Compatibility*』を参照してください。

http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrx.html

VPN 仕様

次の URL にある『*Supported VPN Platforms, Cisco ASA 5500 Series*』を参照してください。

http://www.cisco.com/en/US/docs/security/asa/compatibility/asa-vpn-compatibility.html

新機能

（注）　syslog メッセージ ガイド に、追加、変更、および非推奨化された syslog メッセージを示します。

ASA 9.0(1) の新機能

表 1-1 に ASA バージョン 9.0(1) の新機能を示します。

（注）　8.4(4.x) で追加された機能は、この表で明示されていない限り、9.0(1) には含まれていません。

表 1-1　ASA バージョン 9.0(1) の新機能

機能	説明
ファイアウォール機能	
Cisco TrustSec の統合	Cisco TrustSec は、既存の ID 認証インフラストラクチャを基盤とするアクセス コントロール ソリューションです。ネットワーク デバイス間のデータ機密性保持を目的としており、セキュリティ アクセス サービスを 1 つのプラットフォーム上で統合します。Cisco TrustSec ソリューションでは、実行デバイスはユーザ属性とエンドポイント属性の組み合わせを使用して、ロールベースおよびアイデンティティベースのアクセス コントロールを決定します。 このリリースでは、ASA に Cisco TrustSec が統合されており、セキュリティ グループに基づいてポリシーが適用されます。Cisco TrustSec ドメイン内のアクセス ポリシーは、トポロジには依存しません。ネットワーク IP アドレスではなく、送信元および宛先のデバイスのロールに基づいています。 ASA は、セキュリティ グループに基づくその他のタイプのポリシー（アプリケーション インスペクションなど）に対しても Cisco TrustSec ソリューションを活用できます。たとえば、設定するクラス マップの中に、セキュリティ グループに基づくアクセス ポリシーを入れることができます。 **access-list extended**、**cts sxp enable**、**cts server-group**、**cts sxp default**、**cts sxp retry period**、**cts sxp reconcile period**、**cts sxp connection peer**、**cts import-pac**、**cts refresh environment-data**、**object-group security**、**security-group**、**show running-config cts**、**show running-config object-group**、**clear configure cts**、**clear configure object-group**、**show cts**、**show object-group**、**show conn security-group**、**clear cts**、**debug cts** の各コマンドが導入または変更されました。 次の MIB が導入されました：CISCO-TRUSTSEC-SXP-MIB

表 1-1　ASA バージョン 9.0(1) の新機能 （続き）

機能	説明
Cisco クラウド Web セキュリティ（ScanSafe）	Cisco クラウド Web セキュリティは、Web トラフィックに対してコンテンツスキャンなどのマルウェア防御サービスを実行します。また、ユーザ アイデンティティに基づいて Web トラフィックのリダイレクトと報告を行うこともできます。 （注）　クライアントレス SSL VPN は、クラウド Web セキュリティではサポートされません。クライアントレス SSL VPN トラフィックについては、クラウド Web セキュリティの ASA サービス ポリシーの対象外となっていることを確認してください。 **class-map type inspect scansafe**、**default user group**、**http[s]**（パラメータ）、**inspect scansafe**、**license**、**match user group**、**policy-map type inspect scansafe**、**retry-count**、**scansafe**、**scansafe general-options**、**server {primary | backup}**、**show conn scansafe**、**show scansafe server**、**show scansafe statistics**、**user-identity monitor**、**whitelist** の各コマンドが導入または変更されました。
ICMP コードによって ICMP トラフィックをフィルタリングするための拡張 ACL とオブジェクト機能拡張	ICMP コードに基づいて ICMP トラフィックの許可または拒否ができるようになりました。 **access-list extended**、**service-object**、**service** の各コマンドが導入または変更されました。
ASASM でのユニファイド コミュニケーションのサポート	ASASM は、すべてのユニファイド コミュニケーション機能をサポートするようになりました。
Per-session PAT	Per-session PAT 機能によって PAT のスケーラビリティが向上し、ASA クラスタリングの場合に各メンバ ユニットに独自の PAT 接続を使用できるようになります。Multi-Session PAT 接続は、マスター ユニットに転送してマスター ユニットを所有者とする必要があります。Per-session PAT セッションの終了時に、ASA からリセットが送信され、即座に xlate が削除されます。このリセットによって、エンド ノードは即座に接続を解放し、TIME_WAIT 状態を回避します。対照的に、Multi-Session PAT では、PAT タイムアウトが使用されます（デフォルトでは 30 秒）。「ヒットエンドラン」トラフィック、たとえば HTTP や HTTPS の場合は、Per-session 機能によって、1 アドレスでサポートされる接続率が大幅に増加することがあります。Per-session 機能を使用しない場合は、特定の IP プロトコルに対する 1 アドレスの最大接続率は約 2000/秒です。Per-session 機能を使用する場合は、特定の IP プロトコルに対する 1 アドレスの接続率は 65535/平均ライフタイムです。 デフォルトでは、すべての TCP トラフィックおよび UDP DNS トラフィックが、Per-session PAT xlate を使用します。Multi-Session PAT のメリットを活用できるトラフィック、たとえば H.323、SIP、Skinny に対して Per-session PAT をディセーブルにするには、Per-session 拒否ルールを作成します。 **xlate per-session**、**show nat pool** の各コマンドが導入されました。

表 1-1　ASA バージョン 9.0(1) の新機能 （続き）

機能	説明
ダイナミック ACL からピンホール メカニズムへの SunRPC の変更	これまでは、Sun RPC インスペクションは発信アクセス リストをサポートしません。これは、インスペクション エンジンでセカンダリ接続でなくダイナミック アクセス リストが使用されるためです。 このリリースでは、ASA でダイナミック アクセス リストを設定すると、入力方向のみでサポートされ、ダイナミック ポート宛ての出トラフィックは ASA によってドロップされます。したがって、Sun RPC インスペクションは、ピンホール メカニズムを設定して出力トラフィックをサポートします。Sun RPC インスペクションは、このピンホール メカニズムを使用して発信ダイナミック アクセス リストをサポートします。 *8.4(4.1) でも使用可能です。*
インスペクション リセット アクションの変更	これまでは、インスペクション エンジン ルールに従って ASA によってパケットがドロップされると、ドロップされたパケットのソース デバイスに RST が 1 つのみ送信されました。この動作により、リソースの問題が発生する可能性があります。 このリリースでは、リセット アクションを使用するようにインスペクション エンジンを設定し、パケットによってリセットがトリガーされると、次の条件で ASA によって TCP リセットが送信されます。 • **service resetoutbound** コマンドがイネーブルの場合、ASA は TCP リセットを内部ホストに送信します。（**service resetoutbound** コマンドは、デフォルトでディセーブルです）。 • **service resetinbound** コマンドがイネーブルの場合、ASA は TCP リセットを外部ホストに送信します。（**service resetinbound** コマンドは、デフォルトではディセーブルです）。 詳細については、ASA コマンド リファレンス の **service** コマンドを参照してください。 この動作によって、リセット アクションが ASA および内部サーバの接続をリセットすることが確実になります。したがって、DoS 攻撃を防ぎます。外部ホストの場合、ASA はリセットをデフォルトで送信せず、TCP リセットによって情報が公開されません。 *8.4(4.1) でも使用可能です。*
サービス ポリシー ルールの最大接続数の引き上げ	サービス ポリシー ルールの最大接続数が 65535 から 2000000 に引き上げられました。 **set connection conn-max**、**set connection embryonic-conn-max**、**set connection per-client-embryonic-max**、**set connection per-client-max** の各コマンドが変更されました。
ハイ アベイラビリティとスケーラビリティの機能	

表 1-1　ASA バージョン 9.0(1) の新機能 （続き）

機能	説明
ASA 5580 および 5585-X の ASA クラスタリング	ASA クラスタリングを利用すると、複数の ASA をグループ化して 1 つの論理デバイスとすることができます。クラスタは、単一デバイスのすべての利便性（管理、ネットワークへの統合）を備える一方で、複数デバイスによって高いスループットおよび冗長性を達成します。ASA クラスタリングは、ASA 5580 および ASA 5585-X でサポートされます。1 つのクラスタ内のすべてのユニットが同一モデル、同一ハードウェア仕様であることが必要です。クラスタリングがイネーブルのときにサポートされない機能のリストについては、コンフィギュレーション ガイドを参照してください。 **channel-group**、**clacp system-mac**、**clear cluster info**、**clear configure cluster**、**cluster exec**、**cluster group**、**cluster interface-mode**、**cluster-interface**、**conn-rebalance**、**console-replicate**、**cluster master unit**、**cluster remove unit**、**debug cluster**、**debug lacp cluster**、**enable**（クラスタ グループ）、**health-check**、**ip address**、**ipv6 address**、**key**（クラスタ グループ）、**local-unit**、**mac-address**（インターフェイス）、**mac-address pool**、**mtu cluster-interface**、**port-channel span-cluster**、**priority**（クラスタ グループ）、**prompt cluster-unit**、**show asp cluster counter**、**show asp table cluster chash-table**、**show cluster**、**show cluster info**、**show cluster user-identity**、**show lacp cluster**、**show running-config cluster** の各コマンドが導入または変更されました。
クラスタリングに対する OSPF、EIGRP、マルチキャスト	OSPFv2 および OSPFv3 の場合は、バルク同期、ルート同期、およびスパンド EtherChannel がクラスタリング環境でサポートされます。 EIGRP の場合は、バルク同期、ルート同期、およびスパンド EtherChannel がクラスタリング環境でサポートされます。 マルチキャスト ルーティングは、クラスタリングをサポートします。 **show route cluster**、**debug route cluster**、**show mfib cluster**、**debug mfib cluster** の各コマンドが導入または変更されました。
クラスタリングのパケット キャプチャ	クラスタ全体のトラブルシューティングをサポートするには、**cluster exec capture** コマンドを使用してマスター ユニット上でのクラスタ固有トラフィックのキャプチャをイネーブルにします。これで、クラスタ内のすべてのスレーブ ユニットでも自動的にイネーブルになります。**cluster exec** キーワードは新しいキーワードであり、**capture** コマンドの前に置くとクラスタ全体のキャプチャがイネーブルになります。 **capture**、**show capture** の各コマンドが変更されました。
クラスタリングに対するロギング	クラスタ内の各ユニットは、syslog メッセージを個別に生成します。**logging device-id** コマンドを使用すると、同一または異なるデバイス ID 付きで syslog メッセージを生成することができ、クラスタ内の同一または異なるユニットからのメッセージのように見せることができます。 **logging device-id** コマンドが変更されました。

表 1-1　ASA バージョン 9.0(1) の新機能 （続き）

機能	説明
バルク同期中に接続の複製レートを設定します。	ステートフル フェールオーバーを使用するときに、ASA で接続がスタンバイ装置に複製されるレートを設定できるようになりました。デフォルトでは、スタンバイ装置への接続は、15 秒内で複製されます。ただし、バルク同期が発生したとき（たとえば、最初にフェールオーバーをイネーブルにするとき）、1 秒あたりの最大接続数制限のために、大量の接続を同期するには 15 秒では十分でないことがあります。たとえば、ASA での最大接続数を 800 万とします。800 万の接続を 15 秒間で複製するということは、1 秒あたり約 53.3 万の接続を作成するということです。しかし、1 秒あたりに許可される最大接続数は 30 万です。複製レートが 1 秒あたりの最大接続数以下になるように指定できるようになり、同期期間はすべての接続が同期されるまで調整されます。 **failover replication rate** *rate* コマンドが導入されました。 *8.4(4.1) および 8.5(1.7) でも使用可能です。*
IPv6 の機能	
ASA の外部インターフェイスでの IPv6 サポート（VPN 機能用）。	このリリースの ASA 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。 このリリースの ASA では、内部インターフェイスでの IPv6 VPN トラフィック（SSL プロトコルを使用）がこれまでと同様にサポートされます。このリリースは、内部インターフェイス上での IKEv2/IPsec プロトコルを提供しません。
IPv6 のためのリモート アクセス VPN のサポート： IPv6 アドレス割り当てポリシー	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。 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。 **ipv6-vpn-addr-assig**n、**vpn-framed-ipv6-address** の各コマンドが導入されました。
IPv6 のためのリモート アクセス VPN のサポート： IPv6 アドレスを持つ DNS サーバのグループ ポリシーへの割り当て	DNS サーバを、ASA のネットワーク（クライアント）アクセス内部グループ ポリシー内で定義できます。最大 4 個の DNS サーバ アドレス（最大 2 個の IPv4 アドレスと最大 2 個の IPv6 アドレス）を指定できます。 IPv6 アドレスを持つ DNS サーバに VPN クライアントから到達できるのは、SSL プロトコルを使用するようにクライアントが設定されているときです。この機能は、IKEv2/IPsec プロトコルを使用するように設定されたクライアントではサポートされていません。 **dns-server value** コマンドが変更されました。

表 1-1　ASA バージョン 9.0(1) の新機能 （続き）

機能	説明
IPv6 のためのリモート アクセス VPN のサポート： スプリット トンネリング	スプリット トンネリングを使用すると、一部のネットワーク トラフィックを VPN トンネルを介して（暗号化あり）ルーティングし、それ以外のネットワーク トラフィックを VPN トンネルの外部で（暗号化なし、つまりクリアテキストとして）ルーティングすることができます。IPv6 ネットワーク トラフィックに対してスプリット トンネリングを実行できるようになりました。このようにするには、IPv6 ポリシーを定義し、この中で統合アクセス コントロール ルールを指定します。 IPv6 スプリット トンネリングは、Smart Call Home 機能によって送信されるテレメトリ データで報告されます。IPv4 または IPv6 スプリット トンネリングがイネーブルの場合は、Smart Call Home はスプリット トンネリングを「イネーブル」として報告します。テレメトリ データについては、VPN セッション データベースに表示される IPv6 データは一般的に、セッション管理で報告されます。 SSL プロトコルを使用するように設定された VPN クライアント用の VPN トンネルについて、IPv6 トラフィックを含めるか除外するかを指定できます。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。 ipv6-split-tunnel-policy コマンドが導入されました。
IPv6 のためのリモート アクセス VPN のサポート： AnyConnect クライアント ファイアウォール ルール	クライアント ファイアウォール用のアクセス コントロール ルールは、IPv4 と IPv6 の両方のアドレスのアクセス リスト エントリをサポートします。 IPv6 アドレスが含まれている ACL は、SSL プロトコルを使用するように設定されたクライアントに適用できます。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。 **anyconnect firewall-rule** コマンドが変更されました。

表 1-1　ASA バージョン 9.0(1) の新機能 （続き）

機能	説明
IPv6 のためのリモート アクセス VPN のサポート： クライアント プロトコル バイパス	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、ASA が AnyConnect 接続に IPv4 アドレスだけを割り当てたが、そのエンドポイントがデュアル スタックであるとします。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。 この機能は、クライアントが SSL と IKEv2/IPsec プロトコルのどちらを使用するように設定されていても使用できます。 **client-bypass-protocol** コマンドが導入されました。
IPv6 のためのリモート アクセス VPN のサポート： IPv6 インターフェイス ID とプレフィックス	ローカル VPN ユーザに対して専用の IPv6 アドレスを指定できるようになりました。 この機能の利点を活用できるのは、ユーザが SSL プロトコルを使用するように設定されている場合です。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。 **vpn-framed-ipv6-address** コマンドが導入されました。
IPv6 のためのリモート アクセス VPN のサポート： AnyConnect クライアントへの ASA FQDN の送信	AnyConnect クライアントに ASA の FQDN を返すことができます。これは、ロード バランシングおよびセッション ローミングに役立ちます。 この機能は、クライアントが SSL と IKEv2/IPsec プロトコルのどちらを使用するように設定されていても使用できます。 **gateway-fqdn** コマンドが導入されました。

表 1-1　ASA バージョン 9.0(1) の新機能 （続き）

機能	説明
IPv6 のためのリモート アクセス VPN のサポート： ASA VPN ロード バランシング	IPv6 アドレスを持つクライアントは、AnyConnect 接続を行うときに、ASA クラスタのパブリック向け IPv6 アドレスを経由することも、GSS サーバを経由することもできます。同様に、IPv6 アドレスを持つクライアントは、AnyConnect VPN 接続を行うときに、ASA クラスタのパブリック向け IPv4 アドレスを経由することも、GSS サーバを経由することもできます。どちらのタイプの接続も、ASA クラスタ内でロード バランシングすることができます。 IPv6 アドレスを持つクライアントが ASA のパブリック向け IPv4 アドレスに接続できるようにするには、IPv6 から IPv4 へのネットワーク アドレス変換を実行できるデバイスがネットワーク上に存在する必要があります。 この機能は、クライアントが SSL と IKEv2/IPsec プロトコルのどちらを使用するように設定されていても使用できます。 **show run vpn load-balancing** コマンドが変更されました。
IPv6 のためのリモート アクセス VPN のサポート： ダイナミック アクセス ポリシーでの IPv6 属性のサポート	ASA 9.0 以降を ASDM 6.8 以降とともに使用するときに、次の属性をダイナミック アクセス ポリシー（DAP）の一部として指定できるようになりました。 • IPv6 アドレス（Cisco AAA 属性として） • IPv6 TCP および UDP ポート（デバイスのエンドポイント属性の一部として） • ネットワーク ACL フィルタ（クライアント） この機能は、クライアントが SSL と IKEv2/IPsec プロトコルのどちらを使用するように設定されていても使用できます。
IPv6 のためのリモート アクセス VPN のサポート： セッション管理	セッション管理の出力の Public/Assigned アドレス フィールドに IPv6 アドレスが表示されるのは、AnyConnect 接続、サイトツーサイト VPN 接続、およびクライアントレス SSL VPN 接続の場合です。新しいフィルタ キーワードを追加して出力をフィルタリングし、IPv6（外部または内部）接続だけを表示することができます。IPv6 ユーザ フィルタに対する変更はありません。 この機能を使用できるのは、クライアントが SSL プロトコルを使用するように設定されている場合です。この機能では、IKEv2/IPsec プロトコルはサポートされません。 **show vpn-sessiondb** コマンドが変更されました。
IPv6 用の NAT のサポート	NAT が IPv6 トラフィックをサポートするようになり、IPv4 と IPv6 の間の変換（NAT64）もサポートされます。IPv4 と IPv6 の間の変換は、トランスペアレント モードではサポートされません。 **nat**（グローバルおよびオブジェクト ネットワーク コンフィギュレーション モード）、**show conn**、**show nat**、**show nat pool**、**show xlate** の各コマンドが変更されました。

表 1-1　ASA バージョン 9.0(1) の新機能 （続き）

機能	説明
DHCPv6 リレー	DHCP リレーが IPv6 に対してサポートされます。 **ipv6 dhcprelay server**、**ipv6 dhcprelay enable**、**ipv6 dhcprelay timeout**、**clear config ipv6 dhcprelay**、**ipv6 nd managed-config-flag**、**ipv6 nd other-config-flag**、**debug ipv6 dhcp**、**debug ipv6 dhcprelay**、**show ipv6 dhcprelay binding**、**clear ipv6 dhcprelay binding**、**show ipv6 dhcprelay statistics**、**clear ipv6 dhcprelay statistics** の各コマンドが導入されました。

表 1-1　ASA バージョン 9.0(1) の新機能 （続き）

機能	説明
OSPFv3	OSPFv3 ルーティングが IPv6 に対してサポートされます。OSPFv2 および OSPFv3 に関する次の追加のガイドラインと制限事項に注意してください。 **クラスタリング** • OSPFv2 および OSPFv3 は、クラスタリングをサポートします。 • クラスタリングが設定されているときは、OSPFv3 暗号化はサポートされません。クラスタリング環境で OSPFv3 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。 • 個々のインターフェイスを使用するときに、必ずマスターおよびスレーブ ユニットを OSPFv2 または OSPFv3 のネイバーとして確立します。 • 個々のインターフェイスを使用するときに、OSPFv2 隣接関係を確立できるのは、マスター ユニットの共有インターフェイス上の 2 つのコンテキスト間のみです。スタティック ネイバーの設定がサポートされるのは、ポイントツーポイント リンク上のみです。したがって、1 つのインターフェイス上では 1 つのネイバー ステートメントだけが許可されます。 **その他** • OSPFv2 および OSPFv3 は 1 つのインターフェイス上での複数インスタンスをサポートしています。 • ESP および AH プロトコルが OSPFv3 認証に対してサポートされます。 • OSPFv3 は非ペイロード暗号化をサポートします。 **ipv6 ospf cost**、**ipv6 ospf database-filter all out**、**ipv6 ospf dead-interval**、**ipv6 ospf hello-interval**、**ipv6 ospf mtu-ignore**、**ipv6 ospf neighbor**、**ipv6 ospf network**、**ipv6 ospf priority**、**ipv6 ospf retransmit-interval**、**ipv6 ospf transmit-delay**、**ipv6 router ospf**、**ipv6 router ospf area**、**ipv6 router ospf default**、**ipv6 router ospf default-information**、**ipv6 router ospf distance**、**ipv6 router ospf exit**、**ipv6 router ospf ignore**、**ipv6 router ospf log-adjacency-changes**、**ipv6 router ospf no**、**ipv6 router ospf redistribute**、**ipv6 router ospf router-id**、**ipv6 router ospf summary-prefix**、**ipv6 router ospf timers**、**area range**、**area virtual-link**、**default**、**default-information originate**、**distance**、**ignore lsa mospf**、**log-adjacency-changes**、**redistribute**、**router-id**、**summary-prefix**、**timers lsa arrival**、**timers pacing flood**、**timers pacing lsa-group**、**timers pacing retransmission**、**show ipv6 ospf**、**show ipv6 ospf border-routers**、**show ipv6 ospf database-filter**、**show ipv6 ospf flood-list**、**show ipv6 ospf interface**、**show ipv6 ospf neighbor**、**show ipv6 ospf request-list**、**show ipv6 ospf retransmission-list**、**show ipv6 ospf summary-prefix**、**show ipv6 ospf virtual-links**、**show ospf**、**show run ipv6 router**、**clear ipv6 ospf**、**clear configure ipv6 router**、**debug ospfv3** の各コマンドが導入または変更されました。

表 1-1　ASA バージョン 9.0(1) の新機能 （続き）

機能	説明
IPv4 および IPv6 の統合 ACL	ACL で IPv4 および IPv6 アドレスがサポートされるようになりました。送信元および宛先に対して IPv4 および IPv6 アドレスの組み合わせも指定できます。IPv6 固有の ACL は非推奨です。既存の IPv6 ACL は拡張 ACL に移行されます。 IPv6 アドレスが含まれている ACL は、SSL プロトコルを使用するように設定されたクライアントに適用できます。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。 **access-list extended**、**access-list webtype** の各コマンドが変更されました。 **ipv6 access-list**、**ipv6 access-list webtype**、**ipv6-vpn-filter** の各コマンドが削除されました。
IPv4 および IPv6 の混合オブジェクト グループ	以前は、ネットワーク オブジェクト グループに含まれているのは、すべて IPv4 アドレスであるか、すべて IPv6 アドレスでなければなりませんでした。現在では、ネットワーク オブジェクト グループが、IPv4 と IPv6 の両方のアドレスの混合をサポートするようになりました。 **（注）**　混合オブジェクト グループを NAT に使用することはできません。 **object-group network** コマンドが変更されました。
ネットワーク オブジェクトの IPv6 アドレスの範囲	ネットワーク オブジェクトの IPv6 アドレス範囲を設定できるようになりました。 **range** コマンドが変更されました。
IPv6 および NAT64 のインスペクションのサポート	IPv6 トラフィックの DNS インスペクションがサポートされるようになりました。 また、次のインスペクションについて、IPv4 と IPv6 の間の変換がサポートされます。 • DNS • FTP • HTTP • ICMP また、サポートされていないインスペクションが IPv6 トラフィックを受信してドロップしたときに syslog メッセージ（767001）を生成するように、サービス ポリシーを設定できます。 **service-policy fail-close** コマンドが変更されました。
リモート アクセス機能	

表 1-1　ASA バージョン 9.0(1) の新機能 （続き）

機能	説明
クライアントレス SSL VPN： 追加のサポート	次のブラウザ、オペレーティング システム、Web テクノロジー、およびアプリケーションのサポートが追加されました。 **インターネット ブラウザのサポート**：Microsoft Internet Explorer 9、Firefox 4、5、6、7、および 8 **オペレーティング システムのサポート**：Mac OS X 10.7 **Web テクノロジーのサポート**：HTML 5 **アプリケーションのサポート**：SharePoint 2010
クライアントレス SSL VPN： リライタ エンジンの品質の向上	クライアントレス SSL VPN リライタ エンジンの品質と有効性が大きく向上しました。その結果、クライアントレス SSL VPN ユーザのエンドユーザ エクスペリエンスも向上が期待できます。 この機能に関して、追加または変更されたコマンドはありません。 *8.4(4.1) でも使用可能です。*
クライアントレス SSL VPN： Citrix Mobile Receiver	これは、モバイル デバイス上で実行される Citrix Receiver アプリケーションから XenApp および XenDesktop VDI サーバへの、ASA 経由のセキュア リモート アクセスを実現するための機能です。 ASA が Citrix Receiver と Citrix サーバとの間のプロキシとなる場合は、ユーザが Citrix 仮想化リソースへの接続を試みるときに、Citrix サーバのアドレスとクレデンシャルの代わりに、ユーザは ASA の SSL VPN IP アドレスとクレデンシャルを入力します。 **vdi** コマンドが変更されました。
クライアントレス SSL VPN： 自動サインオン機能の拡張	この機能は、認証にダイナミック パラメータを必要とする Web アプリケーションのサポートを強化します。
クライアントレス SSL VPN： クライアントレス Java リライタ プロキシ サポート	この機能は、クライアントレス Java プラグインのためのプロキシ サポートを行います（クライアント マシンのブラウザでプロキシが設定されているとき）。 この機能に関して、追加または変更されたコマンドはありません。
クライアントレス SSL VPN： Remote File Explorer	Remote File Explorer は、企業ネットワークを Web ブラウザからブラウズするための機能です。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、アプレットがユーザのシステムで起動され、リモート ファイル システムがツリーとフォルダ形式で表示されます。 この機能に関して、追加または変更されたコマンドはありません。
クライアントレス SSL VPN： サーバ証明書の検証	この機能は、クライアントレス SSL VPN のサポートを拡張します。リモート HTTPS サイトの SSL サーバ証明書を、信頼済み CA 証明書のリストと比較して検証することができます。 **ssl-server-check**、**crypto**、**crypto ca trustpool**、**crl**、**certificate**、**revocation-check** の各コマンドが変更されました。

表 1-1　ASA バージョン 9.0(1) の新機能 （続き）

機能	説明
AnyConnect のパフォーマンスの向上	この機能は、マルチコア プラットフォームでの AnyConnect TLS/DTLS トラフィックのスループット パフォーマンスを高めます。これは SSL VPN データパスを高速化し、AnyConnect、スマート トンネル、およびポート フォワーディングに関して、ユーザが認識可能なパフォーマンス向上を実現します。 **crypto engine accelerator-bias**、**show crypto accelerator** の各コマンドが変更されました。
カスタム属性	カスタム属性は、まだ ASDM に追加されていない AnyConnect 機能を定義し、設定します。カスタム属性をグループ ポリシーに追加し、その属性の値を定義します。 AnyConnect 3.1 については、カスタム属性は、AnyConnect Deferred Upgrade をサポートするために使用できます。 カスタム属性の利点は、AnyConnect クライアントが IKEv2/IPsec と SSL のどちらのプロトコルを使用するように設定されていても活用できます。 **anyconnect-custom-attr** コマンドが追加されました。

表 1-1　ASA バージョン 9.0(1) の新機能 （続き）

機能	説明
次世代暗号化	National Standards Association（NSA）は、暗号化強度に関する米国連邦規格に従うためにデバイスがサポートする必要がある、一連の暗号化アルゴリズムを定めています。RFC 6379 で Suite B 暗号化スイートが定義されています。NSA Suite B として定義されるアルゴリズムのセットは、全体で 1 つの標準になりつつあるため、AnyConnect IPSec VPN（IKEv2 のみ）および公開キー インフラストラクチャ（PKI）サブシステムでサポートされるようになりました。次世代暗号化（NGE）には、このセットよりも大きなスーパーセットが含まれており、IPsec V3 VPN のための暗号化アルゴリズムが追加されるほか、IKEv2 に対する Diffie-Hellman グループ 14 および 24、および DTLS と IKEv2 に対する RSA 証明書（4096 ビット キー）が追加されています。 次の機能は、Suite B のアルゴリズムをサポートするために ASA に追加されました。 • AES-GCM/GMAC のサポート（128、192、256 ビット キー） – IKEv2 ペイロード暗号化と認証 – ESP パケット暗号化と認証 – マルチコア プラットフォームでのみサポートされているハードウェア • SHA-2 サポート（256、384、512 ビット ハッシュ） – ESP パケット認証 – マルチコア プラットフォームでのみサポートされているハードウェアおよびソフトウェア • ECDH サポート（グループ 19、20、および 21） – IKEv2 キー交換 – IKEv2 PFS – 単一またはマルチコアのプラットフォームでのみサポートされるソフトウェア • ECDSA サポート（256、384、521 ビット楕円曲線） – IKEv2 ユーザ認証 – PKI 証明書登録 – PKI 証明書の生成および検証 – 単一またはマルチコアのプラットフォームでのみサポートされるソフトウェア 新しい暗号化アルゴリズムが IPsecV3 に対して追加されました。 **（注）** Suite B のアルゴリズムをサポートするには、AnyConnect Premium ライセンスが IKEv2 リモート アクセス接続用に必要ですが、他の接続または目的（たとえば PKI）のために Suite B を使用する場合は、制限はありません。IPsecV3 にはライセンスに関する制限はありません。 **crypto ikev2 policy**、**crypto ipsec ikev2 ipsec-proposal**、**crypto key generate**、**crypto key zeroize**、**show crypto key mypubkey**、**show vpn-sessiondb** の各コマンドが導入または変更されました。

表 1-1　ASA バージョン 9.0(1) の新機能 （続き）

機能	説明
ASASM での VPN のサポート	ASASM は、すべての VPN 機能をサポートするようになりました。
SSL 暗号化用の追加のエフェメラル Diffie-Hellman 暗号	ASA で次のエフェメラル Diffie-Hellman（DHE）SSL 暗号スイートがサポートされるようになりました。 • DHE-AES128-SHA1 • DHE-AES256-SHA1 これらの暗号スイートは、RFC 3268『*Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)*』で指定されています。 DHE では完全転送秘密が提供されるため、クライアントでサポートされている場合、DHE は推奨される暗号です。次の制限事項を確認してください。 • DHE は SSL 3.0 接続ではサポートされないため、SSL サーバの TLS 1.0 もイネーブルにしてください。 `!!set server version` `hostname(config)# ssl server-version tlsv1 sslv3` `!!set client version` `hostname(config) # ssl client-version any` • 一部の一般的なアプリケーションで DHE はサポートされないため、SSL クライアントとサーバの両方に共通の暗号スイートを使用できるように、他の SSL 暗号化方式を少なくとも 1 つ含めます。 • 一部のクライアントで DHE はサポートされない場合があります。AnyConnect 2.5 および 3.0、Cisco Secure Desktop、Internet Explorer 9.0 などです。 **ssl encryption** コマンドが変更されました。 *8.4(4.1) でも使用可能です。*
マルチ コンテキスト モード機能	
マルチ コンテキスト モードのサイトツーサイト VPN	サイトツーサイト VPN トンネルが、マルチ コンテキスト モードでサポートされるようになりました。
サイトツーサイト VPN トンネルのための新しいリソース タイプ	新しいリソース タイプ vpn other と vpn burst other が作成されました。これは、各コンテキストでのサイトツーサイト VPN トンネルの最大数を設定するためです。 **limit-resource**、**show resource types**、**show resource usage**、**show resource allocation** の各コマンドが変更されました。
セキュリティ コンテキストでのダイナミック ルーティング	EIGRP と OSPFv2 ダイナミック ルーティング プロトコルが、マルチ コンテキスト モードでサポートされるようになりました。OSPFv3、RIP、およびマルチキャスト ルーティングはサポートされません。
ルーティング テーブル エントリのための新しいリソース タイプ	新規リソース クラス routes が作成されました。これは、各コンテキストでのルーティング テーブル エントリの最大数を設定するためです。 **limit-resource**、**show resource types**、**show resource usage**、**show resource allocation** の各コマンドが変更されました。

表 1-1　ASA バージョン 9.0(1) の新機能 （続き）

機能	説明
マルチ コンテキスト モードのファイア ウォール モードの混合がサポートされます。	セキュリティ コンテキスごとに個別のファイアウォール モードを設定できます。したがってその一部をトランスペアレント モードで実行し、その他をルーテッド モードで実行することができます。 **firewall transparent** コマンドが変更されました。 *バージョン 8.5(1) でも使用可能です。*
モジュール機能	
ASA CX SSP-10 と -20 に対する ASA 5585-X サポート	ASA CX モジュールを使用すると、特定の状況の完全なコンテキストに基づいてセキュリティを強制することができます。このコンテキストには、ユーザのアイデンティティ（誰が）、ユーザがアクセスを試みているアプリケーションまたは Web サイト（何を）、アクセス試行の発生元（どこで）、アクセス試行の時間（いつ）、およびアクセスに使用されているデバイスのプロパティ（どのように）が含まれます。ASA CX モジュールを使用すると、フローの完全なコンテキストを抽出して、細分化したポリシーを適用することができます。たとえば、Facebook へのアクセスを許可するが Facebook でのゲームへのアクセスは禁止する、あるいは企業の機密データベースへのアクセスを財務担当者に許可するが他の社員には禁止するといったことが可能です。 **capture**、**cxsc**、**cxsc auth-proxy**、**debug cxsc**、**hw-module module password-reset**、**hw-module module reload**、**hw-module module reset**、**hw-module module shutdown**、**session do setup host ip**、**session do get-config**、**session do password-reset**、**show asp table classify domain cxsc**、**show asp table classify domain cxsc-auth-proxy**、**show capture**、**show conn**、**show module**、**show service-policy** の各コマンドが導入または変更されました。 *8.4(4.1) でも使用可能です。*
SSP-10 および SSP-20 に対する ASA 5585-X デュアル SSP サポート（SSP-40 および SSP-60 に加えて）、デュアル SSP に対する VPN サポート	ASA 5585-X は、すべての SSP モデルでデュアル SSP をサポートするようになりました（同一シャーシ内で同じレベルの SSP を 2 つ使用できます）。デュアル SSP を使用するときに VPN がサポートされるようになりました。 変更されたコマンドはありません。

スイッチにおける ASA サービス モジュール の動作

Cisco IOS ソフトウェアを搭載した Catalyst 6500 シリーズ スイッチで、スイッチのスーパーバイザおよび統合型 MSFC の両方に ASASM をインストールできます。

（注）　Catalyst オペレーティング システム（OS）はサポートされていません。

ASA は独自のオペレーティング システムで動作します。

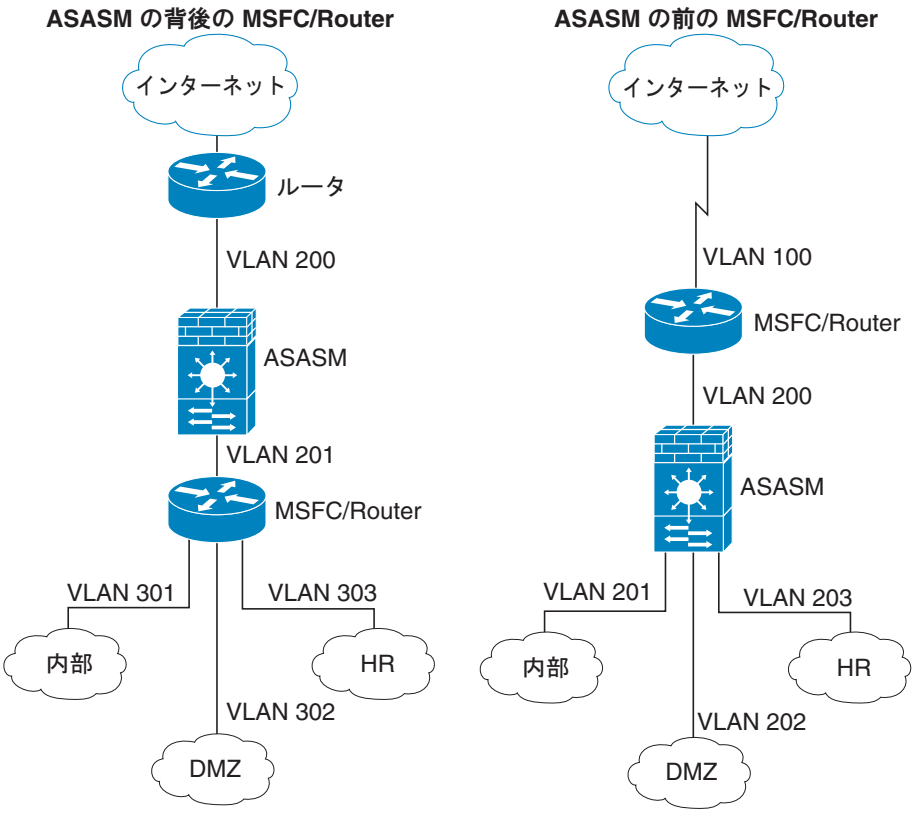
スイッチにはスイッチング プロセッサ（スーパーバイザ）とルータ（MSFC）が組み込まれています。MSFC はシステムの一部として必要ですが、使用しなくてもかまいません。使用することを選択する場合、MSFC に 1 つまたは複数の VLAN インターフェイスを割り当てることができます。MSFC の代わりに外部ルータを使用できます。

シングル コンテキスト モードでは、ファイアウォールの向こう側にルータを配置することも、ファイアウォールより手前に配置することもできます（図 1-1 を参照）。

ルータの位置は、割り当てる VLAN によって決まります。たとえば、図 1-1 の左側の例では、ASASM の内部インターフェイスに VLAN 201 を割り当てているので、ルータはファイアウォールより手前になります。図 1-1 の右側の例では、ASASM の外部インターフェイスに VLAN 200 を割り当てているので、ルータはファイアウォールの向こう側になります。

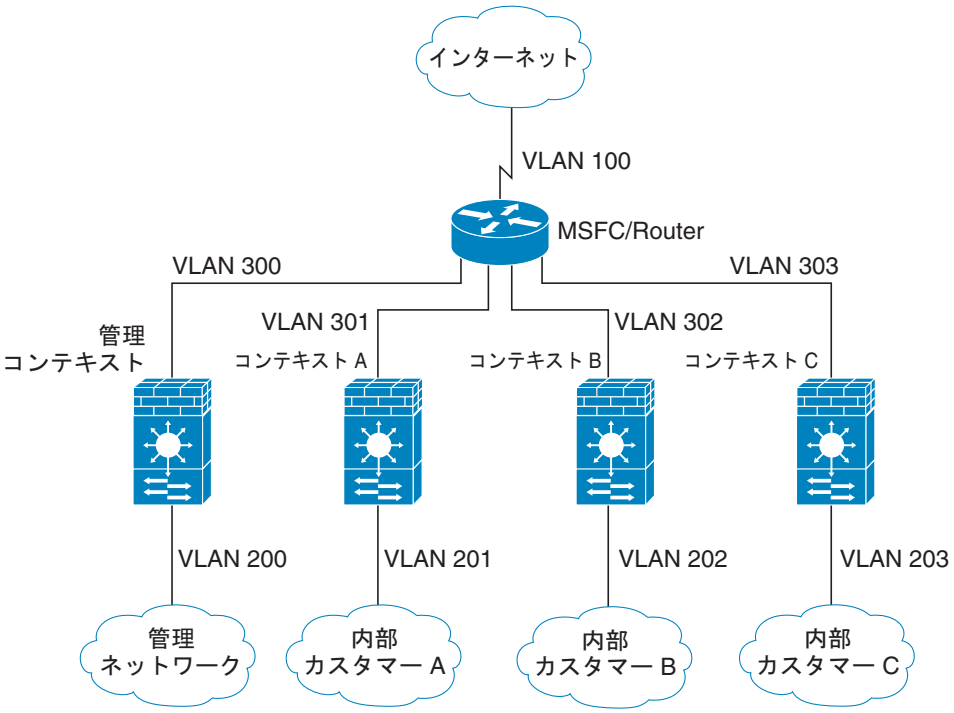
左側の例では、MSFC またはルータは VLAN 201、301、302、および 303 の間をルーティングします。宛先がインターネットの場合以外、内部トラフィックは ASASM を通過しません。右側の例では、ASASM は内部 VLAN 201、202、および 203 間のすべてのトラフィックを処理して保護します。

図 1-1　MSFC/Router の配置



マルチコンテキスト モードでは、ASASM より手前にルータを配置した場合、1 つのコンテキストに限定して接続する必要があります。ルータを複数のコンテキストに接続すると、ルータはコンテキスト間をルーティングすることになり、意図に反する可能性があります。複数のコンテキストの一般的なシナリオでは、インターネットとスイッチド ネットワーク間でルーティングするためにすべてのコンテキストの前にルータを使用します（図 1-2 を参照）。

図 1-2　マルチコンテキストの場合の MSFC/Router の配置



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。また、ファイアウォールは、人事部門ネットワークをユーザ ネットワークから分離するなど、内部ネットワーク同士の保護も行います。Web サーバまたは FTP サーバなど、外部のユーザが使用できるようにする必要のあるネットワーク リソースがあれば、ファイアウォールで保護された別のネットワーク（*Demiliterized Zone*（DMZ; 非武装地帯）と呼ばれる）上に配置します。ファイアウォールによって DMZ へのアクセスを制限できますが、DMZ には公開サーバしかないため、この地帯が攻撃されても影響を受けるのは公開サーバに限定され、他の内部ネットワークに影響が及ぶことはありません。また、特定アドレスだけに許可する、認証または許可を義務づける、または外部の URL フィルタリング サーバと協調するといった手段によって、内部ユーザが外部ネットワーク（インターネットなど）にアクセスする機会を制御することもできます。

ファイアウォールに接続されているネットワークに言及する場合、*外部*ネットワークはファイアウォールの手前にあるネットワーク、*内部*ネットワークはファイアウォールの背後にある保護されているネットワーク、そして *DMZ* はファイアウォールの背後にあるが、外部ユーザに制限付きのアクセスが許されているネットワークです。ASA を使用すると、数多くのインターフェイスに対してさまざまなセキュリティ ポリシーが設定できます。このインターフェイスには、多数の内部インターフェイス、多数の DMZ、および必要に応じて多数の外部インターフェイスが含まれるため、ここでは、このインターフェイスの区分は一般的な意味で使用するだけです。

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、内部ネットワーク（高セキュリティ レベル）から外部ネットワーク（低セキュリティ レベル）へのトラフィックは、自由に流れることが ASA によって許可されます。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

アクセスリストは、内部から外部へのトラフィックを制限するため、または外部から内部へのトラフィックを許可するために使用できます。トランスペアレント ファイアウォール モードでは、非 IP トラフィックを許可するための EtherType アクセス リストも適用できます。

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 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 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。

通過トラフィックに対する AAA の使用

HTTP など特定のタイプのトラフィックに対して、認証と許可のいずれかまたは両方を要求することができます。ASA は、RADIUS サーバまたは TACACS+ サーバにアカウンティング情報を送信することもあります。

HTTP、HTTPS、または FTP フィルタリングの適用

アクセス リストを使用して、特定の Web サイトまたは FTP サーバへの発信アクセスを禁止できますが、このような方法で Web サイトの使用方法を設定し管理することは、インターネットの規模とダイナミックな特性から、実用的とはいえません。ASA を、次のインターネット フィルタリング製品のいずれかを実行している別のサーバと連携させて使用することをお勧めします。

- Websense Enterprise
- Secure Computing SmartFilter

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。これらのプロトコルは、ASA が詳細なパケット インスペクションを行うことを要求します。

IPS モジュールへのトラフィックの送信

使用しているモデルが侵入防御用の IPS モジュールをサポートしている場合、トラフィックをモジュールに送信して検査することができます。IPS モジュールは、多数の埋め込み型シグニチャ ライブラリに基づいて異常や悪用を探索することでネットワーク トラフィックのモニタおよびリアルタイム分析を行います。システムで不正なアクティビティが検出されると、侵入防御サービス機能は、該当する接続を終了して攻撃元のホストを永続的にブロックし、この事象をログに記録し、さらにアラートを Device Manager に送信します。その他の正規の接続は、中断することなく独立した動作を継続します。詳細については、IPS モジュールのマニュアルを参照してください。

コンテンツ セキュリティおよび制御モジュールへのトラフィックの送信

使用しているモデルでサポートされていれば、CSC SSM により、ウイルス、スパイウェア、スパム、およびその他の不要トラフィックから保護されます。これは、FTP、HTTP、POP3、および SMTP トラフィックをスキャンすることで実現されます。そのためには、これらのトラフィックを CSC SSM に送信するようにASA を設定しておきます。

QoS ポリシーの適用

音声やストリーミング ビデオなどのネットワーク トラフィックでは、長時間の遅延は許容されません。QoS は、この種のトラフィックにプライオリティを設定するネットワーク機能です。QoS とは、選択したネットワーク トラフィックによりよいサービスを提供するネットワークの機能です。

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 では、初期接続の制限を利用して TCP 代行受信を発生させます。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 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。

脅威検出のイネーブル化

スキャン脅威検出と基本脅威検出、さらに統計情報を使用して脅威を分析する方法を設定できます。

基本脅威検出は、DoS 攻撃などの攻撃に関係している可能性のあるアクティビティを検出し、自動的にシステム ログ メッセージを送信します。

典型的なスキャン攻撃では、あるホストがサブネット内の IP アドレスにアクセスできるかどうかを 1 つずつ試します（サブネット内の複数のホストすべてを順にスキャンするか、1 つのホストまたはサブネットの複数のポートすべてを順にスイープする）。スキャン脅威検出機能は、いつホストがスキャンを実行するかを判別します。トラフィック署名に基づく IPS スキャン検出とは異なり、ASA のスキャンによる脅威の検出機能では、広範なデータベースが保持され、これに含まれるホスト統計情報をスキャン アクティビティに関する分析に使用できます。

ホスト データベースは、不審なアクティビティを追跡します。このようなアクティビティには、戻りアクティビティのない接続、閉じているサービス ポートへのアクセス、脆弱な TCP 動作（非ランダム IPID など）、およびその他の多くの動作が含まれます。

攻撃者に関するシステム ログ メッセージを送信するように ASA を設定したり、自動的にホストを回避したりできます。

ボットネット トラフィック フィルタのイネーブル化

マルウェアとは、知らないうちにホストにインストールされている悪意のあるソフトウェアです。個人情報（パスワード、クレジット カード番号、キー ストローク、または独自データ）の送信などのネットワーク アクティビティを試みるマルウェアは、マルウェアが既知の不正な IP アドレスへの接続を開始したときにボットネット トラフィック フィルタによって検出できます。ボットネット トラフィック フィルタは、着信と発信の接続を既知の不正なドメイン名と IP アドレス（ブラックリスト）のダイナミック データベースと照合して確認し、不審なアクティビティのログを記録します。マルウェア アクティビティに関する syslog メッセージを確認すると、ホストを切り離して感染を解決するための手順を実行できます。

Cisco Unified Communications の設定

Cisco ASA 5500 シリーズは、統合された通信構成にプロキシの機能を提供する戦略的なプラットフォームです。プロキシの目的は、クライアントとサーバ間の接続を終端し、再発信することです。プロキシは、トラフィック インスペクション、プロトコルとの適合性、ポリシー制御など幅広いセキュ

リティ機能を提供し、内部ネットワークのセキュリティを保証します。プロキシの機能として広く普及しているのが、暗号化された接続を終端して、接続の機密性を維持しながらセキュリティ ポリシーを適用する機能です。

ファイアウォール モードの概要

ASA は、次の 2 つのファイアウォール モードで動作します。

- ルーテッド
- 透過

ルーテッド モードでは、ASA は、ネットワークのルータ ホップと見なされます。

トランスペアレント モードでは、ASA は「Bump In The Wire」または「ステルス ファイアウォール」のように動作し、ルータ ホップとは見なされません。ASA では、内部インターフェイスと外部インターフェイスに同じネットワークが接続されます。

トランスペアレント ファイアウォールは、ネットワーク コンフィギュレーションを簡単にするために使用できます。トランスペアレント モードは、攻撃者からファイアウォールが見えないようにする場合にも有効です。トランスペアレント ファイアウォールは、他の場合にはルーテッド モードでブロックされるトラフィックにも使用できます。たとえば、トランスペアレント ファイアウォールでは、EtherType アクセス リストを使用するマルチキャスト ストリームが許可されます。

ステートフル インスペクションの概要

ASA 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.57-3）を参照してください。

ただし、ASA 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 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
  - 「ファスト パス」でのセッション確立

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 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 チェックサム検証
  - セッション ルックアップ
  - TCP シーケンス番号のチェック
  - 既存セッションに基づく NAT 変換
  - レイヤ 3 ヘッダー調整およびレイヤ 4 ヘッダー調整

  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 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。

VPN 機能の概要

VPN は、TCP/IP ネットワーク（インターネットなど）上のセキュアな接続で、プライベートな接続として表示されます。このセキュアな接続はトンネルと呼ばれます。ASA は、トンネリング プロトコルを使用して、セキュリティ パラメータのネゴシエート、トンネルの作成および管理、パケットのカプセル化、トンネルを通したパケットの送信または受信、パケットのカプセル化の解除を行います。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。たとえば、プレーン パケットを受信してカプセル化し、それをトンネルのもう一方の側に送信することができます。そのエンドポイントで、パケットはカプセル化が解除され、最終的な宛先に送信されます。また、セキュリティ アプライアンスは、カプセル化されたパケットを受信してカプセル化を解除し、それを最終的な宛先に送信することもできます。ASA は、これらの機能を実行するためにさまざまな標準プロトコルを起動します。

ASA が実行する機能は次のとおりです。

- トンネルの確立
- トンネル パラメータのネゴシエーション
- ユーザの認証
- ユーザ アドレスの割り当て
- データの暗号化と復号化
- セキュリティ キーの管理
- トンネルを通したデータ転送の管理

- トンネル エンドポイントまたはルータとしての着信データと発信データの転送の管理

ASA は、これらの機能を実行するためにさまざまな標準プロトコルを起動します。

セキュリティ コンテキストの概要

1 台の ASA を、セキュリティ コンテキストと呼ばれる複数の仮想デバイスに分割することができます。各コンテキストは、独自のセキュリティ ポリシー、インターフェイス、および管理者を持つ独立したデバイスです。マルチ コンテキストは、複数のスタンドアロン デバイスを使用することに似ています。マルチ コンテキスト モードでは、ルーティング テーブル、ファイアウォール機能、IPS、管理など、多くの機能がサポートされます。VPN、ダイナミック ルーティング プロトコルなど、いくつかの機能はサポートされません。

マルチ コンテキスト モードの場合、ASA には、セキュリティ ポリシー、インターフェイス、およびスタンドアロン デバイスで設定できるほとんどのオプションを識別するコンテキストごとのコンフィギュレーションが含まれます。システム管理者がコンテキストを追加および管理するには、コンテキストをシステム コンフィギュレーションに設定します。これが、シングル モード設定と同じく、スタートアップ コンフィギュレーションとなります。システム コンフィギュレーションは、ASA の基本設定を識別します。システム コンフィギュレーションには、ネットワーク インターフェイスやネットワーク設定は含まれません。その代わりに、ネットワーク リソースにアクセスする必要が生じたときに(サーバからコンテキストをダウンロードするなど)、システムは管理コンテキストとして指定されているコンテキストのいずれかを使用します。

管理コンテキストは、他のコンテキストとまったく同じです。ただし、ユーザが管理コンテキストにログインすると、システム管理者権限を持つので、システム コンテキストおよび他のすべてのコンテキストにアクセス可能になる点が異なります。

ASA クラスタリングの概要

ASA クラスタリングを利用すると、複数の ASA をグループ化して 1 つの論理デバイスとすることができます。クラスタは、単一デバイスのすべての利便性（管理、ネットワークへの統合）を備える一方で、複数デバイスによって高いスループットおよび冗長性を達成します。

すべてのコンフィギュレーション作業（ブートストラップ コンフィギュレーションを除く）は、マスター ユニット上でのみ実行します。コンフィギュレーションは、メンバ ユニットに複製されます。