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。

（注） ASDM では、多数の ASA バージョンをサポートしています。ASDM のマニュアルおよびオンライン ヘルプには、ASA でサポートされている最新機能がすべて含まれています。古いバージョンの ASA ソフトウェアを実行している場合、ご使用のバージョンでサポートされていない機能がこのマニュアルに含まれている場合があります。同様に、古いメジャー バージョンまたはマイナー バージョンのメンテナンス リリースに機能が追加された場合、この新機能は、以降のすべての ASA リリースで使用できない場合でも、ASDM のマニュアルに含まれています。各章の機能履歴テーブルを参照して、機能がいつ追加されたかを確認してください。各 ASA バージョンの ASDM の最低限のサポートされるバージョンについては、「*Cisco ASA Compatibility*」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。

ASDM クライアントのオペレーティング システムとブラウザの要件

表 1-1 には、ASDM に対応して推奨されるクライアント オペレーティング システムと Java のリストが表示されています。

表 1-1　オペレーティング システムとブラウザの要件

	ブラウザ				
オペレーティング システム	Internet Explorer[InternetExplorer]	Firefox	Safari	Chrome	Java SE プラグイン
Microsoft Windows（英語および日本語）： • 7 • Vista • 2008 サーバ • XP	6.0 以降	1.5 以降	サポートなし	18.0 以降	6.0 以降
Apple Macintosh OS X： • 10.8 • 10.7 • 10.6 • 10.5 • 10.4	サポートなし	1.5 以降	2.0 以降	18.0 以降	6.0 以降
Red Hat Enterprise Linux 5（GNOME または KDE）： • Desktop • Desktop with Workstation	該当なし	1.5 以降	該当なし	18.0 以降	6.0 以降

次の警告を参照してください。

- 以前のバージョンから Java 7 Update 5 にアップグレードした場合、IPv6 アドレスから Java Web Start を使用して ASDM を開くことができない可能性があります。ASDM Launcher をダウンロードするか、http://java.com/en/download/help/clearcache_upgrade.xml で支持される指示される手順に従ってください。
- Java のバグにより、Java 6 では、ASDM は 50 文字を超えるユーザ名をサポートしません。Java 7 では、長いユーザ名は正しく動作します。
- 次の場合には、ASDM は ASA への SSL 接続を必要とします。
  - ブラウザがまず ASA に接続してから、ASDM スプラッシュ画面にアクセスする場合。
  - Launcher または Java Web Start アプリケーションを使用して、ASDM を起動する場合。

  ASA に基本暗号化ライセンス（DES）しかなく、そのため SSL 接続に対する暗号化が弱い場合、スプラッシュ画面にアクセスできなかったり、ASDM 起動できない可能性があります。次の問題を参照してください。
  - ASDM の起動時に Java 7 を使用する場合は、ASA には強力な暗号化ライセンス（3DES/AES）が必要です。基本暗号化ライセンス（DES）のみでは、ASDM を起動できません。ブラウザを ASDM スプラッシュ画面に接続して、Launcher または Web Start アプリケーションをダウンロードできても、ASDM は起動できません。Java 7 をアンインストールし、Java 6 をインストールする必要があります。

  - Java 6 を使用してブラウザのスプラッシュ画面にアクセスする場合、デフォルトでは Windows Vista 以降の Internet Explorer およびすべてのオペレーティング システム上の Firefox は SSL に DES をサポートしません。したがって、強力な暗号化ライセンス（3DES/AES）がない場合は、次の回避策を参照してください。

    可能な場合は、すでにダウンロードした ASDM Launcher または Java Web Start アプリケーションを使用します。ブラウザが動作しなくても、Launcher は Java 6 および脆弱な暗号化と動作します。

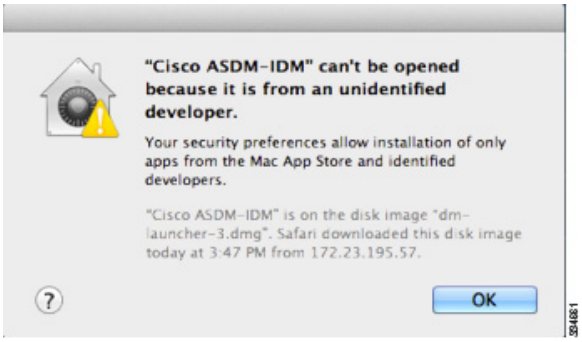
    Windows Internet Explorer の場合は、回避策として DES をイネーブルにすることができます。詳細については、http://support.microsoft.com/kb/929708 を参照してください。

    すべてのオペレーティング システムでの Firefox の場合は、回避策として security.ssl3.dhe_dss_des_sha 設定をイネーブルにすることができます。非表示のコンフィギュレーション プリファレンスを変更する方法については、http://kb.mozillazine.org/About:config を参照してください。

- ASA が自己署名証明書または信頼できない証明書を使用する場合、Firefox 4 以降と Safari では、IPv6 を介した HTTPS を使用して参照する場合にはセキュリティ例外を追加することはできません。https://bugzilla.mozilla.org/show_bug.cgi?id=633001 を参照してください。この警告は、Firefox または Safari から ASA に発信されるすべての SSL 接続に影響します（ASDM 接続を含む）。この警告を回避するには、信頼できる認証局が ASA に対して発行した適切な証明書を設定します。
- RC4-MD5 および RC4-SHA1 アルゴリズム（これらのアルゴリズムはデフォルトでイネーブル）の両方を除外するために ASA の SSL 暗号化を変更した場合、Chrome の「SSL false start」機能のために Chrome は ASDM を起動できません。これらのアルゴリズムの 1 つを再度イネーブルにすることを推奨します（[Configuration] > [Device Management] > [Advanced] > [SSL Settings] ペインを参照）。または http://www.chromium.org/developers/how-tos/run-chromium-with-flags に従って **--disable-sslfalse-start** フラグを使用して Chrome の SSL false start をディセーブルにすることができます。
- サーバの Internet Explorer 9.0 に対しては、[Do not save encrypted pages to disk] オプションがデフォルトでイネーブルです（[Tools] > [Internet Options] > [Advanced] を参照）。このオプションでは、最初の ASDM のダウンロードは失敗します。ASDM でダウンロードを行うには、このオプションを確実にディセーブルにしてください。
- MacOS では、ASDM の初回実行時に、Java のインストールを要求される場合があります。必要に応じて、プロンプトに従います。インストールの完了後に ASDM が起動します。
- MacOS では、ASDM Launcher を開くと、次のエラー メッセージが表示される場合があります。

  ```
  Cannot launch Cisco ASDM-IDM.No compatible version of Java 1.5+ is available.
  ```

  この場合は、Java 7 が現在優先する Java のバージョンになっており、優先する Java のバージョンを Java 6 に変更する必要があります。[Java Preferences] アプリケーション（[Applications] > [Utilities] に続き）を開き、優先する Java のバージョンを選択して、テーブルの最初の行にドラッグします。
- MacOS 10.8 以降では、Apple Developer ID で署名されていないアプリケーションを許可する必要があります。セキュリティの設定を変更しないと、エラー画面が表示されます。



a. セキュリティ設定を変更するには、[System Preference] を開き、[Security & Prfivacy] をクリックします。

b. [Allow applications downloaded from] 下の [General] タブで、[Anywhere] をクリックします。

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 の互換性

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 9.1（2）/ASDM 7.1（3）の新機能

表 1-2 に、ASA バージョン 9.1（2）/ASDM バージョン 7.1（3）の新機能を一覧表示します。

（注） 8.4（6）で追加された機能は、このテーブルに明示的に示されていない限り、9.1（2）には含まれません。

表 1-2　ASA バージョン 9.1（2）/ASDM バージョン 7.1（3）の新機能

機能	説明
暗号化機能	
フェールオーバー リンクおよびステート リンクの通信を暗号化する IPSec LAN-to-LAN トンネルのサポート	フェールオーバー キーに独自の暗号化を使用する代わりに、フェールオーバー リンクおよびステート リンクの暗号化に IPSec LAN-to-LAN トンネルが使用できるようになりました。 **（注）** フェールオーバー LAN-to-LAN トンネルは、IPSec（他の VPN）ライセンスには適用されません。 次の画面が変更になりました。[Configuration] > [Device Management] > [High Availability] > [Failover] > [Setup]。

表 1-2　ASA バージョン 9.1（2）/ASDM バージョン 7.1（3）の新機能 （続き）

機能	説明
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。 • 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。 次の画面が変更されました。[Configuration] > [Device Management] > [Advanced] > [SSL Settings]。 *8.4(4.1) でも使用可能です。*
管理機能	
ローカル データベースを使用する場合の管理者パスワード ポリシーのサポート	ローカル データベースを使用して CLI または ASDM アクセスの認証を設定する場合は、指定期間を過ぎるとユーザにパスワードの変更を要求し、パスワードの最短長と最低変更文字数などのパスワード標準に従うことを要求するパスワード ポリシーを設定することができます。 次の画面が導入されました。[Configuration] > [Device Management] > [Users/AAA] > [Password Policy]。 *8.4(4.1) でも使用可能です。*
SSH 公開キー認証のサポート	ASA への SSH 接続の公開キー認証がユーザ単位でイネーブルにできるようになりました。公開キー ファイル（PKF）でフォーマットされたキーまたは Base64 キーを指定できます。PKF キーは、4096 ビットまで使用できます。Base64 形式（最大 2048 ビット）の ASA サポートには大きすぎるキーには、PKF 形式を使用します。 次の画面が導入されました。 [Configuration] > [Device Management] > [Users/AAA] > [User Accounts] > [Edit User Account] > [Public Key Authentication] [Configuration] > [Device Management] > [Users/AAA] > [User Accounts] > [Edit User Account] > [Public Key Using PKF] *8.4(4.1) でも使用可能。PKF キー形式は 9.1(2) でのみサポートされます。*
SSH の AES-CTR 暗号化	ASA での SSH サーバの実装が、AES-CTR モードの暗号化をサポートするようになりました。
SSH キー再生成間隔の改善	SSH 接続は、接続時間 60 分間またはデータ トラフィック 1 GB ごとに再生成されます。

表 1-2　ASA バージョン 9.1（2）/ASDM バージョン 7.1（3）の新機能 （続き）

機能	説明
SSH キー交換の Diffie-Hellman グループ 14 のサポート	SSH キー交換に Diffie-Hellman グループ 14 が追加されました。これまでは、グループ 1 だけがサポートされていました。 次の画面が変更されました。[Configuration] > [Device Management] > [Management Access] > [ASDM/HTTPS/Telnet/SSH]。 *8.4(4.1) でも使用可能です。*
管理セッションの最大数のサポート	同時 ASDM、SSH、Telnet セッションの最大数を設定することができます。 次の画面が導入されました。[Configuration] > [Device Management] > [Management Access] > [Management Session Quota]。 *8.4(4.1) でも使用可能です。*
ASDM のプリログイン バナーのサポート	管理者は、ユーザが管理アクセスのために ASDM にログインする前に表示するメッセージを定義できます。このカスタマイズ可能コンテンツはプリログイン バナーと呼ばれ、特別な要件や重要な情報をユーザに通知することができます。
デフォルトの Telnet パスワードが削除されました	ASA への管理アクセスのセキュリティ向上のために、Telnet のデフォルト ログイン パスワードが削除されました。Telnet を使用してログインする前に、パスワードを手動で設定する必要があります。**注** : Telnet ユーザ認証を設定していない場合、ログイン パスワードは Telnet 接続にのみ使用されます。 以前はパスワードをクリアすると、ASA がデフォルト「cisco」をリストアしていました。今ではパスワードをクリアすると、パスワードは削除されるようになりました。 ログイン パスワードは、スイッチから ASASM への Telnet セッションでも使用されます（**session** コマンドを参照）。最初 ASASM のアクセスでは、ログイン パスワードを設定するまで、**service-module session** コマンドを使用します。 変更された ASDM 画面はありません。 *9.0（2）でも使用可能です。*
プラットフォーム機能	
電源投入時自己診断テスト（POST）のサポート	ASA は、FIPS 140 2 準拠モードで実行されていない場合でも、起動時の電源投入時自己診断テストを実行します。 AES-GCM/GMAC アルゴリズム、ECDSA アルゴリズム、PRNG、Deterministic Random Bit Generator Validation System（DRBGVS）の変更に対応するために、POST が追加されました。
疑似乱数生成（PRNG）の改善	X9.31 の実装がアップグレードされ、シングルコアの ASA での Network Device Protection Profile（NDPP）に対応するために、トリプル DES 暗号化の代わりに AES-256 の暗号化を使用するようになりました。
イメージ検証のサポート	SHA-512 イメージ整合性チェックのサポートが追加されました。 変更された ASDM 画面はありません。 *8.4(4.1) でも使用可能です。*
ASA サービス モジュールでのプライベート VLAN のサポート	ASASM では、プライベート VLAN を使用できます。ASASM にプライマリ VLAN を割り当てると、ASASM は自動的にセカンダリ VLAN トラフィックを処理します。この機能は、ASASM 上での設定は必要ありません。詳細については、スイッチのコンフィギュレーション ガイドを参照してください。

表 1-2　ASA バージョン 9.1（2）/ASDM バージョン 7.1（3）の新機能 （続き）

機能	説明
CPU プロファイルの拡張機能	**cpu profile activate** コマンドが、以下をサポートするようになりました。 • トリガーされるまでのプロファイラの開始の遅延（グローバルまたは特定スレッド CPU%） • シングル スレッドのサンプリング 変更された ASDM 画面はありません。 *8.4(6) でも使用可能です。*
DHCP の機能	
インターフェイスごとの DHCP リレー サーバ（IPv4 のみ）	DHCP リレー サーバをインターフェイスごとに設定できるようになったため、特定のインターフェイスを入力する要求は、そのインターフェイス用に指定されたサーバに対してのみリレーされます。インターフェイス単位の DHCP リレーでは、IPv6 はサポートされません。 次の画面が変更されました。[Configuration] > [Device Management] > [DHCP] > [DHCP Relay]。
DHCP の信頼できるインターフェイス	DHCP Option 82 を維持するために、信頼できるインターフェイスとしてインターフェイスを設定できるようになりました。DHCP Option 82 は、DHCP スヌーピングおよび IP ソースガードのために、ダウンストリーム スイッチおよびルータによって使用されます。通常、ASA DHCP リレー エージェントがすでに設定されている Option 82 で DHCP パケットを受信すると、giaddr フィールド（サーバにパケットを転送する前にリレー エージェントによって設定された DHCP リレー エージェント アドレスを指定するフィールド）が 0 に設定されている場合は、ASA がそのパケットをデフォルトで削除します。インターフェイスを信頼できるインターフェイスとして指定することで、Option 82 を維持したままパケットを転送できるようになりました。 次の画面が変更されました。[Configuration] > [Device Management] > [DHCP] > [DHCP Relay]。
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。 次の画面が導入されました。 [Home] > [ASA CX Status] [Wizards] > [Startup Wizard] > [ASA CX Basic Configuration] [Configuration] > [Firewall > Service Policy Rules] > [Add Service Policy Rule] > [Rule Actions] > [ASA CX Inspection] *8.4(4.1) でも使用可能です。*

表 1-2　ASA バージョン 9.1（2）/ASDM バージョン 7.1（3）の新機能 （続き）

機能	説明
ASA 5585-X のネットワーク モジュール サポート	ASA 5585-X が、スロット 1 でネットワーク モジュール上の追加インターフェイスをサポートするようになりました。次のオプション ネットワーク モジュールの 1 つまたは 2 つをインストールできます。 • ASA 4 ポート 10G ネットワーク モジュール • ASA 8 ポート 10G ネットワーク モジュール • ASA 20 ポート 1G ネットワーク モジュール *8.4(4.1) でも使用可能です。*
ASA 5585-X DC 電源サポート	ASA 5585-X DC 電源のサポートが追加されました。 *8.4(5) でも使用可能です。*
デモンストレーション用モニタリング専用モードのサポート	デモンストレーション目的でのみ、サービス ポリシー用のモニタリング専用モードをイネーブルにすることができ、元のトラフィックに影響を与えずに、トラフィックのコピーを ASA CX モジュールに転送することができます。 デモンストレーション用のもう 1 つのオプションは、モニタリング専用モードでのサービス ポリシーの代わりにトラフィック転送インターフェイスを設定することです。トラフィック転送インターフェイスは、ASA をバイパスして、ASA CX モジュールにすべてのトラフィックを直接送信します。 次の画面が変更されました。[Configuration] > [Firewall] > [Service Policy Rules] > [Add Service Policy Rule] > [Rule Actions] > [ASA CX Inspection]。 トラフィック転送機能は CLI のみでサポートされます。
ASA CX モジュールおよび NAT 64 のサポート	ASA CX モジュールに加えて NAT 64 が使用できるようになりました。 変更された ASDM 画面はありません。
ファイアウォール機能	
EtherType ACL による IS-IS トラフィック（トランスペアレント ファイアウォール モード）のサポート	トランスペアレント ファイアウォール モードでは、ASA が EtherType ACL を使用して IS-IS トラフィックを渡すことができるようになりました。 次の画面が変更されました。[Configuration] > [Device Management] > [Management Access] > [EtherType Rules]。 *8.4(5) でも使用可能です。*
ハーフ クローズ タイムアウト最小値を 30 秒に削減	グローバル タイムアウトおよび接続タイムアウトの両方のハーフ クローズド タイムアウトの最小値が 5 分から 30 秒に短縮され、DoS 保護が向上しました。 次の画面が変更されました。 [Configuration] > [Firewall] > [Service Policy Rules] > [Connection Settings] [Configuration] > [Firewall] > [Advanced] > [Global Timeouts]。
リモート アクセス機能	

表 1-2　ASA バージョン 9.1（2）/ASDM バージョン 7.1（3）の新機能 （続き）

機能	説明
IKE セキュリティとパフォーマンスの改善	IKE v2 に加えて IKE v1 に対して、IPSec-IKE セキュリティ アソシエーション（SA）を制限できます。 次の画面が変更されました。[Configuration] > [Site-to-Site VPN] > [Advanced] > [IKE Parameter]。
	IKE v2 ナンスのサイズが 64 バイトに増加しました。 ASDM 画面または CLI に変更はありません。
	サイト間 IKE v2 では、新しいアルゴリズムは、子の IPsec SA によって使用される暗号化アルゴリズムが親の IKE より強力でないことを保障します。強力アルゴリズムが IKE レベルに下げられます。 この新しいアルゴリズムはデフォルトでイネーブルです。この機能をディセーブルにしないことを推奨します。 変更された ASDM 画面はありません。
	サイト間の場合は、IPSec データ ベースの再調整をディセーブルにできます。 次の画面が変更されました。[Configuration] > [Site-to-Site] > [IKE Parameter]。
ホスト スキャンおよび ASA 相互運用性の改善	ホスト スキャンおよび ASA のプロセスが改善され、クライアントから ASA にポスチャ属性が転送できます。つまり、クライアントとの VPN 接続を確立し、ダイナミック アクセス ポリシーを適用するために、ASA はより長い時間を割くことができます。 *8.4(5) でも使用可能です。*
クライアントレス SSL VPN： Windows 8 のサポート	このリリースでは、Windows 8 x86（32 ビット）および Windows 8 x64（64 ビット）オペレーティング システムのサポートが追加されました。 Windows 8 では次のブラウザのみがサポートされます。 • Internet Explorer 10（デスクトップのみ） • Firefox（すべての Windows 8 バージョンをサポート） • Chrome（すべての Windows 8 バージョンをサポート） 次の制限事項を確認してください。 • Internet Explorer 10 – Modern（別名 Metro）ブラウザはサポートされません。 – 拡張保護モードをイネーブルにする場合は、信頼できるゾーンに ASA を追加することを推奨します。 – 拡張保護モードがイネーブルの場合は、スマート トンネルおよびポート転送はサポートされません。 • Windows 8 PC への Java Remote Desktop Protocol (RDP) プラグイン接続は、サポートされません。 *9.0（2）でも使用可能です。*
Cisco Secure Desktop Windows 8 のサポート	CSD 3.6.6215 がアップデートされ、プリログイン ポリシーのオペレーティング システムのチェックで Windows 8 が選択できるようになりました。 次の制限事項を確認してください。 • Secure Desktop（Vault）は Windows 8 ではサポートされません。 *9.0（2）でも使用可能です。*

表 1-2　ASA バージョン 9.1（2）/ASDM バージョン 7.1（3）の新機能 （続き）

機能	説明
ダイナミック アクセス ポリシー Windows 8 のサポート	ASDM がアップデートされ、DAP オペレーティング システム属性で Windows 8 が選択できるようになりました。 *9.0（2）でも使用可能です。*
モニタ機能	
Xlate カウントへのポーリング可能にする NAT-MIB cnatAddrBindNumberOfEntries および cnatAddrBindSessionCount OID。	SNMP の xlate_count および max_xlate_count に、NAT-MIB cnatAddrBindNumberOfEntries および cnatAddrBindSessionCount OID がサポートされるようになりました。 このデータは、**show xlate count** コマンドと同等です。 変更された ASDM 画面はありません。 *8.4(5) でも使用可能です。*
NSEL	フロー トラフィックの定期的なバイト カウンタを提供するために flow-update イベントが導入されました。flow-update イベントが NetFlow コレクタに送信される時間間隔を変更できます。flow-update レコードを送信するコレクタをフィルタリングできます。 次の画面が変更されました。 [Configuration] > [Device Management] > [Logging] > [NetFlow]。 [Configuration] > [Firewall] > [Service Policy Rules] > [Add Service Policy Rule Wizard - Rule Actions] > [NetFlow] > [Add Flow Event] *8.4(5) でも使用可能です。*

ASA 8.4(6)/ASDM 7.1(2.102) の新機能

表 1-3 に、ASA バージョン 8.4(6)/ASDM バージョン 7.1(2.102) の新機能を示します。

表 1-3　ASA バージョン 8.4(6)/ASDM バージョン 7.1(2.102) の新機能

機能	説明
モニタ機能	
メモリの上位 10 ユーザの表示機能	上位割り当て済み bin サイズと割り当て済みの bin サイズごとの上位 10 PC を表示することができます。以前は、この情報を見るためには、複数のコマンド（**show memory detail** コマンドと **show memory binsize** コマンド）の入力が必要でした。新しいコマンドにより、メモリの問題の迅速な分析が可能です。 ASDM の変更はありません。 *この機能は、8.5（1）、8.6（1）、8.7（1）、9.0（1）、9.1（1）では、利用できません。*
CPU プロファイルの拡張機能	**cpu profile activate** コマンドが、以下をサポートするようになりました。 • トリガーされるまでのプロファイラの開始の遅延（グローバルまたは特定スレッド CPU%） • シングル スレッドのサンプリング ASDM の変更はありません。 *この機能は、8.5（1）、8.6（1）、8.7（1）、9.0（1）、9.1（1）では、利用できません。*

表 1-3　ASA バージョン 8.4(6)/ASDM バージョン 7.1(2.102) の新機能 （続き）

機能	説明
リモート アクセス機能	
user-storage value コマンドのパスワードの **show** コマンドでの暗号化	**show running-config** コマンドを入力すると、**user-storage value** コマンドのパスワードは暗号化されます。 次の画面が変更されました。[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Group Policies] > [More Options] > [Session Settings]。 *この機能は、8.5（1）、8.6（1）、8.7（1）、9.0（1）、9.1（1）では、利用できません。*

ASA 9.0(2)/ASDM 7.1(2) の新機能

表 1-4 に、ASA バージョン 9.0(2)/ASDM バージョン 7.1(2) の新機能を示します。

（注）　8.4（4.x）、8.4（5）、8.4（6）にない機能は、9.0（1）機能テーブルにない限り 9.0（2）にもありません。

表 1-4　ASA バージョン 9.0（2）/ASDM バージョン 7.1（2）の新機能

機能	説明
リモート アクセス機能	
クライアントレス SSL VPN： Windows 8 のサポート	このリリースでは、Windows 8 x86（32 ビット）および Windows 8 x64（64 ビット）オペレーティング システムのサポートが追加されました。 Windows 8 では次のブラウザのみがサポートされます。 • Internet Explorer 10（デスクトップのみ） • Firefox（すべての Windows 8 バージョンをサポート） • Chrome（すべての Windows 8 バージョンをサポート） 次の制限事項を確認してください。 • Internet Explorer 10 – Modern（別名 Metro）ブラウザはサポートされません。 – 拡張保護モードをイネーブルにする場合は、信頼できるゾーンに ASA を追加することを推奨します。 – 拡張保護モードがイネーブルの場合は、スマート トンネルおよびポート転送はサポートされません。 • Windows 8 PC への Java Remote Desktop Protocol (RDP) プラグイン接続は、サポートされません。
Cisco Secure Desktop Windows 8 のサポート	CSD 3.6.6215 がアップデートされ、プリログイン ポリシーのオペレーティング システムのチェックで Windows 8 が選択できるようになりました。 次の制限事項を確認してください。 • Secure Desktop（Vault）は Windows 8 ではサポートされません。

表 1-4　ASA バージョン 9.0（2）/ASDM バージョン 7.1（2）の新機能 （続き）

機能	説明
ダイナミック アクセス ポリシー Windows 8 のサポート	ASDM がアップデートされ、DAP オペレーティング システム属性で Windows 8 が選択できるようになりました。
管理機能	
デフォルトの Telnet パスワードが削除されました	ASA への管理アクセスのセキュリティ向上のために、Telnet のデフォルト ログイン パスワードが削除されました。Telnet を使用してログインする前に、パスワードを手動で設定する必要があります。**注** : Telnet ユーザ認証を設定していない場合、ログイン パスワードは Telnet 接続にのみ使用されます。 以前はパスワードをクリアすると、ASA がデフォルト「cisco」をリストアしていました。今ではパスワードをクリアすると、パスワードは削除されるようになりました。 ログイン パスワードは、スイッチから ASASM への Telnet セッションでも使用されます（**session** コマンドを参照）。最初 ASASM のアクセスでは、ログイン パスワードを設定するまで、**service-module session** コマンドを使用します。 変更された ASDM 画面はありません。

ASA 9.1(1)/ASDM 7.1(1) の新機能

表 1-5 に、ASA バージョン 9.1(1)/ASDM バージョン 7.1(1) の新機能を示します。

（注）　8.4（4.x）、8.4（5）、8.4（6）、9.0（2）にない機能は、9.0（1）機能テーブルにない限り 9.1（1）にもありません。

表 1-5　ASA バージョン 9.1(1)/ASDM バージョン 7.1(1) の新機能

機能	説明
モジュール機能	
ASA 5512-X ～ ASA 5555-X に対する ASA CX SSP のサポート	ASA 5512-X、ASA 5515-X、ASA 5525-X、ASA 5545-X、および ASA 5555-X に対する ASA CX SSP ソフトウェア モジュールのサポートが導入されました。ASA CX ソフトウェア モジュールを使用するには、ASA 上に Cisco ソリッド ステート ドライブ（SSD）が必要です。SSD の詳細については、ASA 5500-X のハードウェア ガイドを参照してください。 変更された画面はありません。

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 シリーズおよび Cisco 7600 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。

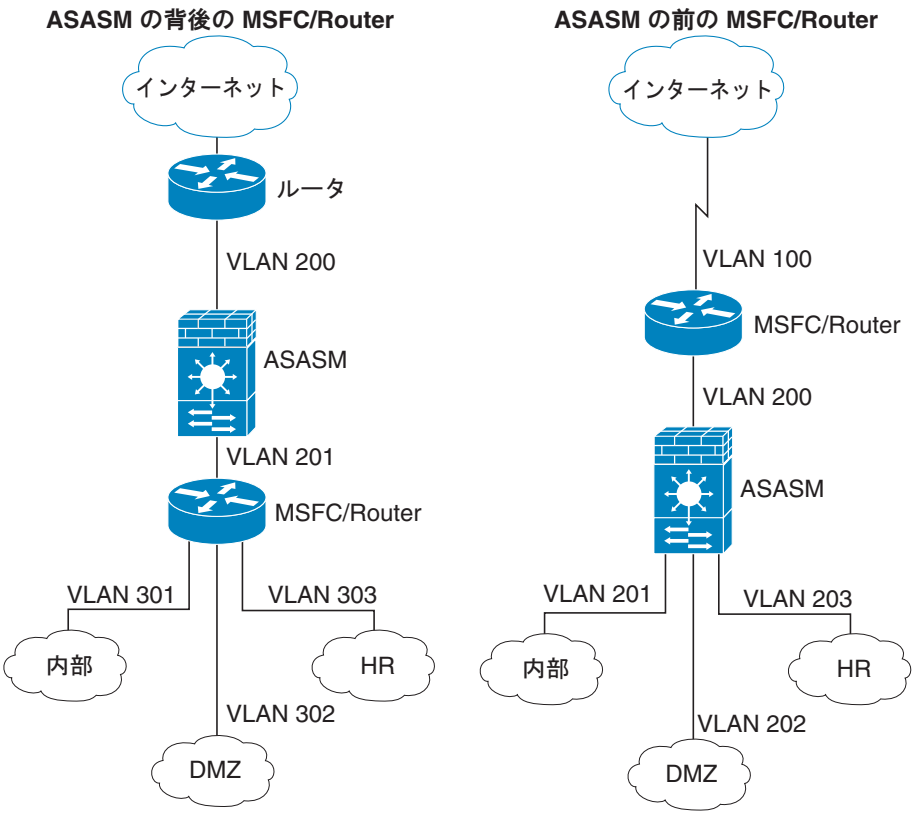
スイッチにはスイッチング プロセッサ（スーパーバイザ）とルータ（MSFC）が組み込まれています。MSFC はシステムの一部として必要ですが、使用しなくてもかまいません。使用することを選択する場合、MSFC に 1 つまたは複数の VLAN インターフェイスを割り当てることができます。MSFC の代わりに外部ルータを使用できます。

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。

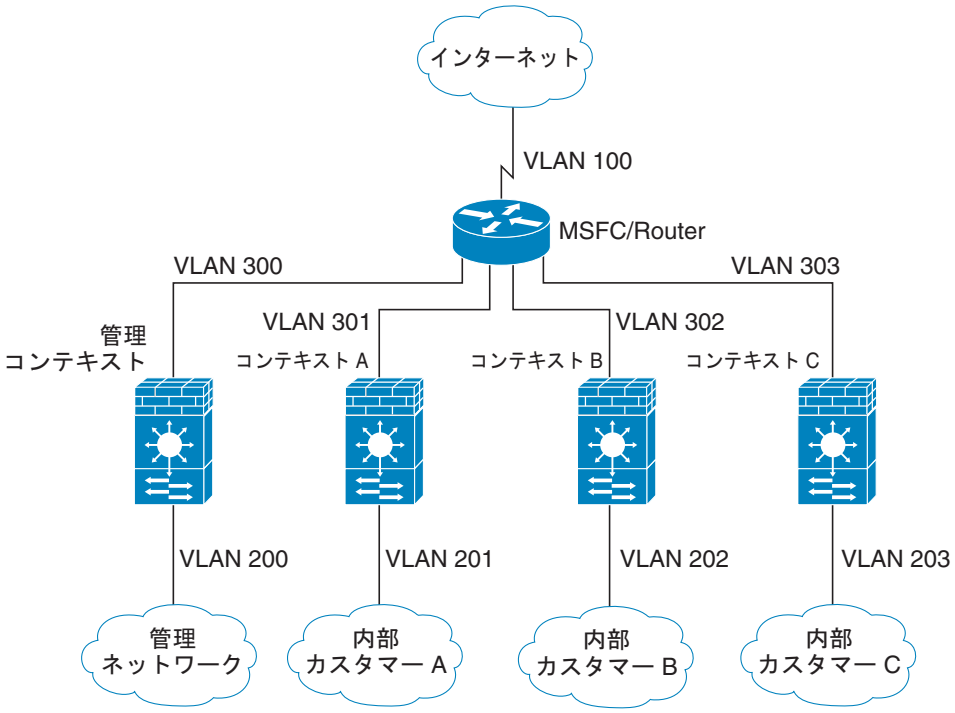
図 1-1　MSFC/Router の配置



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。

- 「ステートフル インスペクションの概要」（P.1-19）

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 ルールによるトラフィックの許可または拒否」（P.1-16）
- 「NAT の適用」（P.1-16）
- 「IP フラグメントからの保護」（P.1-17）
- 「通過トラフィックに対する AAA の使用」（P.1-17）
- 「HTTP、HTTPS、または FTP フィルタリングの適用」（P.1-17）
- 「アプリケーション インスペクションの適用」（P.1-17）
- 「IPS モジュールへのトラフィックの送信」（P.1-17）
- 「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」（P.1-17）
- 「QoS ポリシーの適用」（P.1-18）
- 「接続の制限と TCP 正規化の適用」（P.1-18）
- 「脅威検出のイネーブル化」（P.1-18）
- 「ボットネット トラフィック フィルタのイネーブル化」（P.1-18）
- 「Cisco Unified Communications の設定」（P.1-18）

アクセス ルールによるトラフィックの許可または拒否

アクセス ルールは、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。ファイアウォール コンフィギュレーション ガイドの “TCP State Bypass” section on page 61-3 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

ASA は、TCP トラフィックのファスト パスに転送フローとリバース フローを作成します。ASA は、高速パスも使用できるように、UDP、ICMP（ICMP インスペクションがイネーブルの場合）などのコネクションレス型プロトコルの接続状態の情報も作成するので、これらのプロトコルもファスト パスを使用できます。

（注）　SCTP などの他の IP プロトコルの場合、ASA はリバース パス フローを作成しません。そのため、これらの接続を参照する ICMP エラー パケットはドロップされます。

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

  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。