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

この章では、アプリケーション レイヤ プロトコル インスペクションを設定する方法について説明します。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では、高速パスでパケットを渡すのではなく、ASA で詳細なパケット インスペクションを行う必要があります（高速パスの詳細については、一般的な操作のコンフィギュレーション ガイドの“Stateful Inspection Overview” section on page 1-20 を参照してください）。そのため、インスペクション エンジンがスループット全体に影響を与えることがあります。ASA では、デフォルトでいくつかの一般的なインスペクション エンジンがイネーブルになっていますが、ネットワークによっては他のインスペクション エンジンをイネーブルにしなければならない場合があります。

この章は、次の項で構成されています。

アプリケーション レイヤ プロトコル インスペクションに関する情報

この項は、次の内容で構成されています。

インスペクション エンジンの動作

図 9-1 に示されているように、ASA は基本動作に 3 種類のデータベースを使用します。

- ACL：特定のネットワーク、ホスト、およびサービス（TCP/UDP ポート番号）に基づく接続の認証と許可のために使用されます。
- インスペクション：事前定義済みの一連のスタティックなアプリケーションレベルのインスペクション機能を含みます。

- 接続（XLATE および CONN テーブル）：確立済みの各接続についての状態および他の情報を保持します。この情報は、確立済みのセッション内でトラフィックを効率的に転送するため、アダプティブ セキュリティ アルゴリズムおよびカットスルー プロキシによって使用されます。

図 9-1　　インスペクション エンジンの動作

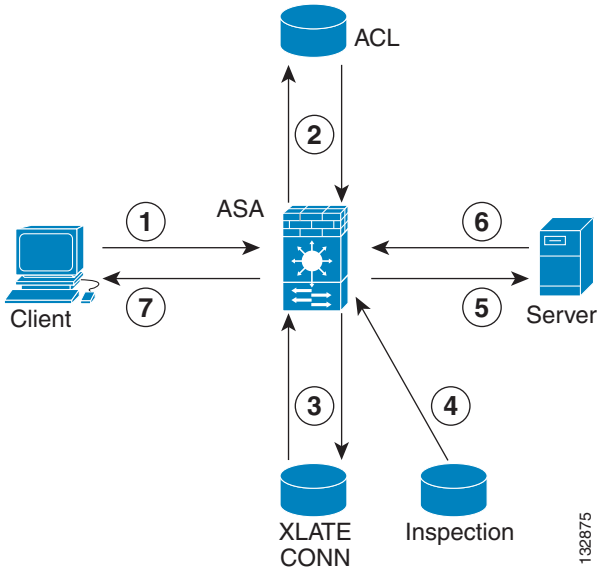

図 9-1 では、動作にはその発生順に番号が付けられており、次でその動作について説明します。

1. TCP SYN パケットが ASA に到着して、新しい接続を確立します。
2. ASA は ACL データベースをチェックして、接続が許可されるかどうかを判定します。
3. ASA は接続データベース（XLATE および CONN テーブル）に新しいエントリを作成します。
4. ASA はインスペクション データベースをチェックして、接続にアプリケーションレベルのインスペクションが必要かどうかを判定します。
5. アプリケーション インスペクション エンジンがパケットに必要な処理を完了した後、ASA はパケットを宛先システムに転送します。
6. 宛先システムは初期要求に応答します。
7. ASA は応答パケットを受信し、接続データベースで接続を検索して、確立済みのセッションに属しているのでパケットを転送します。

ASA のデフォルト コンフィギュレーションには、サポートされるプロトコルを特定の TCP または UDP ポート番号と関連付けて、必要とされる特殊な処理を識別する、一連のアプリケーション インスペクション エントリが含まれます。

アプリケーション プロトコル インスペクションを使用するタイミング

ユーザが接続を確立すると、ASA は ACL と照合してパケットをチェックし、アドレス変換を作成し、高速パスでのセッション用にエントリを作成して、後続のパケットが時間のかかるチェックをバイパスできるようにします。ただし、高速パスは予測可能なポート番号に基づいており、パケット内部のアドレス変換を実行しません。

多くのプロトコルは、セカンダリの TCP ポートまたは UDP ポートを開きます。予約済みポートでの初期セッションは、ダイナミックに割り当てられるポート番号のネゴシエーションに使用されます。

パケットに IP アドレスを埋め込むアプリケーションもあります。この IP アドレスは送信元アドレスと一致する必要があり、通常、ASA を通過するときに変換されます。

これらのアプリケーションを使用する場合は、アプリケーション インスペクションをイネーブルにする必要があります。

IP アドレスを埋め込むサービスに対してアプリケーション インスペクションをイネーブルにすると、ASA は埋め込まれたアドレスを変換し、チェックサムや変換の影響を受けたその他のフィールドを更新します。

ダイナミックに割り当てられたポートを使用するサービスに対してアプリケーション インスペクションをイネーブルにすると、ASA はセッションをモニタしてダイナミックに割り当てられたポートを特定し、所定のセッションの間、それらのポートでのデータ交換を許可します。

ガイドラインと制限事項

この項では、この機能のガイドラインと制限事項について説明します。

コンテキスト モードのガイドライン

シングル コンテキスト モードとマルチ コンテキスト モードでサポートされています。

ファイアウォール モードのガイドライン

ルーテッド ファイアウォール モードとトランスペアレント ファイアウォール モードでサポートされています。

フェールオーバーのガイドライン

インスペクションが必要なマルチメディア セッションのステート情報は、ステートフル フェールオーバーのステート リンク経由では渡されません。GTP は例外で、ステート リンクで複製されます。

IPv6 のガイドライン

IPv6 は次のインスペクションでサポートされています。

- DNS
- FTP
- HTTP
- ICMP
- SIP
- SMTP
- IPSec パススルー
- IPv6

NAT64 は次のインスペクションでサポートされています。

- DNS
- FTP
- HTTP
- ICMP

その他のガイドラインと制限事項

一部のインスペクション エンジンは、PAT、NAT、外部 NAT、または同一セキュリティ インターフェイス間の NAT をサポートしません。NAT サポートの詳細については、「デフォルト設定」を参照してください。

すべてのアプリケーション インスペクションについて、適応型セキュリティ アプライアンスはアクティブな同時データ接続の数を 200 接続に制限します。たとえば、FTP クライアントが複数のセカンダリ接続を開く場合、FTP インスペクション エンジンはアクティブな接続を 200 だけ許可して 201 番目の接続からはドロップし、適応型セキュリティ アプライアンスはシステム エラー メッセージを生成します。

検査対象のプロトコルは高度な TCP ステート トラッキングの対象となり、これらの接続の TCP ステートは自動的には複製されません。スタンバイ装置への接続は複製されますが、TCP ステートを再確立するベスト エフォート型の試行が行われます。

デフォルト設定

デフォルトでは、すべてのデフォルト アプリケーション インスペクション トラフィックに一致するポリシーがコンフィギュレーションに含まれ、すべてのインスペクションがすべてのインターフェイスのトラフィックに適用されます（グローバル ポリシー）。デフォルト アプリケーション インスペクション トラフィックには、各プロトコルのデフォルト ポートへのトラフィックが含まれます。適用できるグローバル ポリシーは 1 つだけなので、グローバル ポリシーを変更する（標準以外のポートにインスペクションを適用する場合や、デフォルトでイネーブルになっていないインスペクションを追加する場合など）には、デフォルトのポリシーを編集するか、デフォルトのポリシーをディセーブルにして新しいポリシーを適用する必要があります。

表 9-1 にサポートされているすべてのインスペクション、デフォルトのクラス マップで使用されるデフォルトのポート、およびデフォルトでオンになっているインスペクション エンジン（太字）を示します。この表には、NAT に関する制限事項も含まれています。

表 9-1　サポートされているアプリケーション インスペクション エンジン

アプリケーション[1]	デフォルト ポート	NAT に関する制限事項	標準[2]	コメント
CTIQBE	TCP/2748	拡張 PAT はサポートされません。 NAT64 なし。	—	—
DCERPC	TCP/135	NAT64 なし。	—	—
DNS over UDP	UDP/53	NAT サポートは、WINS 経由の名前解決では使用できません。	RFC 1123	PTR レコードは変更されません。
FTP	TCP/21	—	RFC 959	—
GTP	UDP/3386 UDP/2123	拡張 PAT はサポートされません。 NAT64 なし。	—	特別なライセンスが必要です。

表 9-1　サポートされているアプリケーション インスペクション エンジン （続き）

アプリケーション[1]	デフォルト ポート	NAT に関する制限事項	標準[2]	コメント
H.323 H.225 および **RAS**	TCP/1720 UDP/1718 UDP (RAS) 1718-1719	同一セキュリティのインターフェイス上の NAT はサポートされません。 スタティック PAT はサポートされません。 拡張 PAT はサポートされません。 NAT64 なし。	ITU-T H.323、H.245、H225.0、Q.931、Q.932	—
HTTP	TCP/80	—	RFC 2616	ActiveX と Java を除去する場合の MTU 制限に注意してください。MTU が小さすぎて Java タグまたは ActiveX タグを 1 つのパケットに納められない場合は、除去の処理は行われません。
ICMP	—	—	—	すべての ICMP トラフィックは、デフォルトのクラス マップで照合されます。
ICMP ERROR	—	—	—	すべての ICMP トラフィックは、デフォルトのクラス マップで照合されます。
ILS（LDAP）	TCP/389	拡張 PAT はサポートされません。 NAT64 なし。	—	—
Instant Messaging（IM; インスタント メッセージ）	クライアントにより異なる	拡張 PAT はサポートされません。 NAT64 なし。	RFC 3860	—
IP オプション	—	NAT64 なし。	RFC 791、RFC 2113	すべての IP オプション トラフィックは、デフォルトのクラス マップで照合されます。
MGCP	UDP/2427、2727	拡張 PAT はサポートされません。 NAT64 なし。	RFC 2705bis-05	—
MMP	TCP 5443	拡張 PAT はサポートされません。 NAT64 なし。	—	—
NetBIOS Name Server over IP	UDP/137、138（送信元ポート）	拡張 PAT はサポートされません。 NAT64 なし。	—	NetBIOS は、NBNS UDP ポート 137 および NBDS UDP ポート 138 に対してパケットの NAT 処理を実行することでサポートされます。
PPTP	TCP/1723	NAT64 なし。	RFC 2637	—
RADIUS Accounting	1646	NAT64 なし。	RFC 2865	—

表 9-1　サポートされているアプリケーション インスペクション エンジン （続き）

アプリケーション[1]	デフォルト ポート	NAT に関する制限事項	標準[2]	コメント
RSH	TCP/514	PAT はサポートされません。 NAT64 なし。	Berkeley UNIX	—
RTSP	TCP/554	拡張 PAT はサポートされません。 外部 NAT はサポートされません。 NAT64 なし。	RFC 2326、2327、1889	HTTP クローキングは処理しません。
ScanSafe	TCP/80 TCP/413	—	—	これらのポートは、ScanSafe インスペクションの default-inspection-traffic クラスには含まれません。
SIP	TCP/5060 UDP/5060	外部 NAT はサポートされません。 同一セキュリティのインターフェイス上の NAT はサポートされません。 拡張 PAT はサポートされません。 NAT64 なし。	RFC 2543	—
SKINNY（SCCP）	TCP/2000	外部 NAT はサポートされません。 同一セキュリティのインターフェイス上の NAT はサポートされません。 拡張 PAT はサポートされません。 NAT64 なし。	—	一定の条件下で、Cisco IP Phone 設定をアップロード済みの TFTP は処理しません。
SMTP および **ESMTP**	TCP/25	NAT64 なし。	RFC 821、1123	—
SNMP	UDP/161、162	NAT および PAT はサポートされません。	RFC 1155、1157、1212、1213、1215	v.2 RFC 1902 ～ 1908、v.3 RFC 2570 ～ 2580
SQL*Net	TCP/1521	拡張 PAT はサポートされません。 NAT64 なし。	—	v.1 および v.2
Sun RPC over UDP および TCP	UDP/111	拡張 PAT はサポートされません。 NAT64 なし。	—	デフォルトのルールには UDP ポート 111 が含まれています。TCP ポート 111 の Sun RPC インスペクションをイネーブルにする場合は、TCP ポート 111 を照合する新しいルールを作成し、Sun RPC インスペクションを実行する必要があります。

表 9-1　サポートされているアプリケーション インスペクション エンジン （続き）

アプリケーション[1]	デフォルト ポート	NAT に関する制限事項	標準[2]	コメント
TFTP	UDP/69	NAT64 なし。	RFC 1350	ペイロード IP アドレスは変換されません。
WAAS	—	拡張 PAT はサポートされません。 NAT64 なし。	—	—
XDCMP	UDP/177	拡張 PAT はサポートされません。 NAT64 なし。	—	—

1. デフォルト ポートに対してデフォルトでイネーブルになっているインスペクション エンジンは太字で表記されています。
2. ASA は、これらの標準に準拠していますが、検査対象のパケットには準拠を強制しません。たとえば、各 FTP コマンドは特定の順序である必要がありますが、ASA によってその順序を強制されることはありません。

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設定

この機能は、セキュリティ ポリシー ルールを使用してサービス ポリシーを作成します。サービス ポリシーでは、一貫性と柔軟性を備えた方法で ASA 機能を設定できます。たとえば、サービス ポリシーを使用すると、すべての TCP アプリケーションに適用されるタイムアウト コンフィギュレーションではなく、特定の TCP アプリケーションに固有のタイムアウト コンフィギュレーションを作成できます。詳細については、第 1 章「サービス ポリシーの設定」を参照してください。

一部のアプリケーションでは、デフォルトでインスペクションがイネーブルになっています。詳細については、「デフォルト設定」を参照してください。この項を参照してインスペクション ポリシーを変更してください。

手順の詳細

ステップ 1　[Configuration] > [Firewall] > [Service Policy Rules] の順に選択します。

ステップ 2　「通過トラフィックのサービス ポリシー ルールの追加」（P.1-9）を参照して、サービス ポリシー ルールを追加または編集します。

標準以外のポートを照合する場合は、非標準ポート用の新しいルールを作成します。各インスペクション エンジンの標準ポートについては、「デフォルト設定」（P.9-4）を参照してください。必要に応じて同じサービス ポリシー内に複数のルールを組み合わせることができるため、照合するトラフィックに応じたルールを作成できます。ただし、トラフィックがインスペクション アクションを含むルールと一致し、その後同様にインスペクション アクションを含む別のルールとも一致した場合、最初に一致したルールだけが使用されます。

ステップ 3　[Edit Service Policy Rule] > [Rule Actions] ダイアログボックスで、[Protocol Inspection] タブをクリックします。

新しいルールの場合、[Add Service Policy Rule Wizard - Rule Actions] というダイアログボックス名が表示されます。

ステップ 4　適用する各インスペクション タイプを選択します。

ステップ 5　（任意）一部のインスペクション エンジンでは、トラフィックにインスペクションを適用するときの追加パラメータを制御できます。インスペクション マップを設定するには、各インスペクション タイプの [Configure] をクリックします。

既存のマップを選択することも、新しいマップを作成することもできます。[Configuration] > [Firewall] > [Objects] > [Inspect Maps] ペインから、インスペクション マップを事前に定義できます。

ステップ 6　必要に応じて、他の [Rule Actions] タブを使用し、このルールに対して他の機能を設定できます。

ステップ 7　[OK] をクリックします（またはウィザードで [Finish] をクリックします）。