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

次のトピックで、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。

アプリケーション レイヤ プロトコル インスペクション

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』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。

次のトピックで、アプリケーション インスペクションについて詳しく説明します。

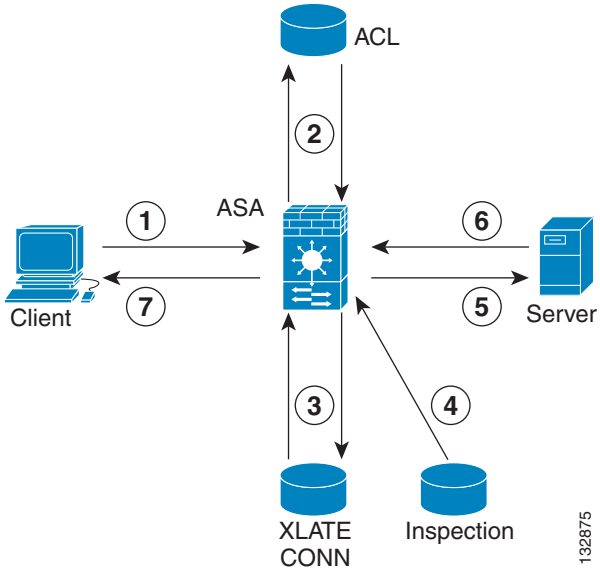
インスペクション エンジンの動作

次の図に示すように、ASA は基本動作を行うために 3 つ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、適応型セキュリティ 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 8-1　　インスペクション エンジンの動作



この図では、動作順に番号が付けられています。

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。既知のポートで初期セッションが使用され、動的に割り当てられたポート番号がネゴシエートされます。

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。

インスペクション ポリシー マップ

*インスペクション ポリシー マップ*を使用して、多くのアプリケーション インスペクションで実行される特別なアクションを設定できます。これらのマップはオプションです。インスペクション ポリシー マップをサポートするプロトコルに関しては、マップを設定しなくてもインスペクションをイネーブルにできます。デフォルトのインスペクション アクション以外のことが必要な場合にのみ、これらのマップが必要になります。

インスペクション ポリシー マップをサポートするアプリケーションのリストについては、「アプリケーション レイヤ プロトコル インスペクションの設定」（P.8-10）を参照してください。

インスペクション ポリシー マップは、次に示す要素の 1 つ以上で構成されています。インスペクション ポリシー マップで使用可能な実際のオプションは、アプリケーションに応じて決まります。

- トラフィック一致基準：アプリケーション トラフィックをそのアプリケーションに固有の基準（URL 文字列など）と照合し、その後アクションをイネーブルにできます。

  一部のトラフィック一致基準では、正規表現を使用してパケット内部のテキストを照合します。ポリシー マップを設定する前に、正規表現クラス マップ内で、正規表現を単独またはグループで作成およびテストしておいてください。

- インスペクション クラス マップ：一部のインスペクション ポリシー マップでは、インスペクション クラス マップを使用して複数のトラフィック一致基準を含めることができます。その後、インスペクション ポリシー マップ内でインスペクション クラス マップを指定し、そのクラス全体でアクションをイネーブルにします。クラス マップを作成することと、インスペクション ポリシー マップ内で直接トラフィック照合を定義することの違いは、より複雑な一致基準を作成できる点と、クラス マップを再使用できる点です。ただし、異なる一致基準に対して異なるアクションを設定することはできません。

- パラメータ：パラメータは、インスペクション エンジンの動作に影響します。

次のトピックで、詳細に説明します。

- 「使用中のインスペクション ポリシー マップの交換」（P.8-4）
- 「複数のトラフィック クラスの処理方法」（P.8-4）

使用中のインスペクション ポリシー マップの交換

サービス ポリシーですでに使用しているインスペクション ポリシー マップを交換する必要がある場合、次の方法を使用してください。

- すべてのインスペクション ポリシー マップ：使用中のインスペクション ポリシー マップを別のマップ名と交換する場合は、そのマップを削除して変更を適用し、新しいインスペクション ポリシー マップをサービス ポリシーに追加する必要があります。
- HTTP インスペクション ポリシー マップ：使用中の HTTP インスペクション ポリシー マップを変更する場合、変更を有効にするにはインスペクション ポリシー マップ アクションを削除し、再適用する必要があります。たとえば、「http-map」インスペクション ポリシー マップを変更する場合、そのインスペクション ポリシー マップを削除して変更を適用し、サービス ポリシーに再度追加する必要があります。

複数のトラフィック クラスの処理方法

インスペクション ポリシー マップには、複数のインスペクション クラス マップや直接照合を指定できます。

1 つのパケットが複数の異なる照合と一致する場合、ASA がアクションを適用する順序は、インスペクション ポリシー マップにアクションが追加された順序ではなく、ASA の内部ルールによって決まります。内部ルールは、アプリケーションのタイプとパケット解析の論理的進捗によって決まり、ユーザが設定することはできません。HTTP トラフィックの場合、Request Method フィールドの解析が Header Host Length フィールドの解析よりも先に行われ、Request Method フィールドに対するアクションは Header Host Length フィールドに対するアクションより先に行われます。

アクションがパケットをドロップすると、インスペクション ポリシー マップではそれ以降のアクションは実行されません。たとえば、最初のアクションが接続のリセットである場合、それ以降の一致基準との照合は行われません。最初のアクションがパケットのログへの記録である場合、接続のリセットなどの 2 番目のアクションは実行されます。

パケットが、同じ複数の一致基準と照合される場合は、ポリシー マップ内のそれらのコマンドの順序に従って照合されます。

クラス マップは、そのクラス マップ内で重要度が最低の照合オプション（重要度は、内部ルールに基づきます）に基づいて、別のクラス マップまたは直接照合のと同じタイプであると判断されます。クラス マップに、別のクラス マップと同じタイプの重要度が最低の照合オプションがある場合、それらのクラス マップはポリシー マップに追加された順序で照合されます。クラス マップごとに最低重要度の照合が異なる場合は、最高重要度の照合オプションを持つクラス マップが最初に照合されます。

アプリケーション インスペクションのガイドライン

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。ステート リンク経由で複製される GTP および SIP は例外です。

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
- SCCP（Skinny）
- 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 インスペクションと NAT に関する制限事項」（P.8-6）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、ASA 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。
- ASA（インターフェイス）に送信される TCP/UDP トラフィックはデフォルトで検査されます。ただし、インターフェイスに送信される ICMP トラフィックは、ICMP インスペクションをイネーブルにした場合でも検査されません。したがって、ASA がバックアップ デフォルト ルートを介して到達できる送信元からエコー要求が送信された場合など、特定の状況下では、インターフェイスへの ping（エコー要求）が失敗する可能性があります。

アプリケーション インスペクションのデフォルト

次のトピックで、アプリケーション インスペクションのデフォルトの動作について説明します。

- 「デフォルト インスペクションと NAT に関する制限事項」（P.8-6）
- 「デフォルトのインスペクション ポリシー マップ」（P.8-10）

デフォルト インスペクションと NAT に関する制限事項

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。

次の表に、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 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。この表の見方は次のとおりです。

- 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。
- ASA は、これらの指定された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。

表 8-1　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	デフォルト ポート	NAT に関する制限事項	Standards	注
CTIQBE	TCP/2748	拡張 PAT はサポートされません。 NAT64 なし。 （クラスタリング）スタティック PAT はサポートされません。	—	—
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	—
FTP	TCP/21	（クラスタリング）スタティック PAT はサポートされません。	RFC 959	—
GTP	UDP/3386 UDP/2123	拡張 PAT はサポートされません。 NAT なし。	—	特別なライセンスが必要です。

表 8-1　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	デフォルト ポート	NAT に関する制限事項	Standards	注
H.323 H.225 および **RAS**	TCP/1720 UDP/1718 UDP (RAS) 1718-1719	ダイナミック NAT または PAT はサポートされません。 スタティック PAT は機能しない可能性があります。 （クラスタリング）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。 Per-Session PAT 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。 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	—	—	—	ASA インターフェイスに送信される ICMP トラフィックは検査されません。
ICMP ERROR	—	—	—	—
ILS（LDAP）	TCP/389	拡張 PAT はサポートされません。 NAT64 なし。	—	—
インスタント メッセージング（IM）	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	—
IPsec パススルー	UDP/500	PAT はサポートされません。 NAT64 なし。	—	—
IPv6	—	NAT64 なし。	RFC 2460	—

表 8-1　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	デフォルト ポート	NAT に関する制限事項	Standards	注
MGCP	UDP/2427、2727	拡張 PAT はサポートされません。 NAT64 なし。 （クラスタリング）スタティック PAT はサポートされません。	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。 （クラスタリング）スタティック PAT はサポートされません。	RFC 2637	—
RADIUS アカウンティング	1646	NAT64 なし。	RFC 2865	—
RSH	TCP/514	PAT はサポートされません。 NAT64 なし。 （クラスタリング）スタティック PAT はサポートされません。	Berkeley UNIX	—
RTSP	TCP/554	拡張 PAT はサポートされません。 NAT64 なし。 （クラスタリング）スタティック PAT はサポートされません。	RFC 2326、2327、1889	HTTP クローキングは処理しません。
ScanSafe（クラウド Web セキュリティ）	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。

表 8-1　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	デフォルト ポート	NAT に関する制限事項	Standards	注
SIP	TCP/5060 UDP/5060	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。 Per-Session PAT はサポートされません。 NAT64 または NAT46 はなし。 （クラスタリング）スタティック PAT はサポートされません。	RFC 2543	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。
SKINNY（SCCP）	TCP/2000	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。 Per-Session PAT はサポートされません。 NAT64、NAT46、または NAT66 はなし。 （クラスタリング）スタティック PAT はサポートされません。	—	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。 （クラスタリング）スタティック PAT はサポートされません。	—	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 8-1　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	デフォルト ポート	NAT に関する制限事項	Standards	注
TFTP	UDP/69	NAT64 なし。 （クラスタリング）スタティック PAT はサポートされません。	RFC 1350	ペイロード IP アドレスは変換されません。
WAAS	TCP/1- 65535	拡張 PAT はサポートされません。 NAT64 なし。	—	—
XDMCP	UDP/177	拡張 PAT はサポートされません。 NAT64 なし。 （クラスタリング）スタティック PAT はサポートされません。	—	—

デフォルトのインスペクション ポリシー マップ

一部のインスペクション タイプは、非表示のデフォルト ポリシー マップを使用します。たとえば、マップを指定しないで ESMTP インスペクションをイネーブルにした場合、_default_esmtp_map が使用されます。

デフォルトのインスペクションは、各インスペクション タイプについて説明しているセクションで説明されています。これらのデフォルト マップは、[show running-config all policy-map] コマンドを使用して表示できます。[Tools] > [Command Line Interface] を使用します。

DNS インスペクションは、明示的に設定されたデフォルト マップ preset_dns_map を使用する唯一のインスペクションです。

アプリケーション レイヤ プロトコル インスペクションの設定

サービス ポリシーにアプリケーション インスペクションを設定します。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。アプリケーションによっては、インスペクションをイネーブルにすると特別なアクションを実行できるものがあります。サービス ポリシーに関する一般的な情報については、第 1 章「サービス ポリシー」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 インスペクションと NAT に関する制限事項」（P.8-6）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

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.1-11）に従ってサービス ポリシー ルールを追加または編集し、[Rule Action] ページに進みます。

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 インスペクションと NAT に関する制限事項」（P.8-6）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。

RADIUS アカウンティング インスペクションを実装している場合、「管理トラフィックのサービス ポリシー ルールの追加」（P.1-14）に従って管理サービス ポリシー ルールを作成します。

ステップ 3　ルールのアクションで、[Protocol Inspection] タブをクリックします。

ステップ 4　（使用中のポリシーを変更）異なるインスペクション ポリシー マップを使用するために使用中のポリシーを編集する場合は、インスペクションをディセーブルにし、新しいインスペクション ポリシー マップ名で再度イネーブルにします。

a.　プロトコルのチェックボックスをオフにします。

b.　[OK] をクリックします。

c.　[Apply] をクリックします。

d.　この手順を繰り返して [Protocol Inspections] タブに戻ります。

ステップ 5　適用したいインスペクション タイプを選択します。

デフォルトのインスペクション トラフィック クラスに対してのみ、複数のオプションを選択できます。

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 ポリシー マップを設定するには、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] リストから、インスペクション ポリシー マップを事前に定義できます。

次の表に、検査可能なプロトコル、インスペクション ポリシー マップまたはインスペクション クラス マップを使用できるかどうか、さらにインスペクションに関する詳細情報へのポインタを示します。

表 8-2　インスペクション プロトコル

プロトコル	インスペクション ポリシー マップのサポート	インスペクション クラス マップのサポート	注意
CTIQBE	No	No	「CTIQBE インスペクション」（P.10-1）を参照してください。
クラウド Web セキュリティ	Yes	Yes	ScanSafe（クラウド Web セキュリティ）をイネーブルにしたい場合、この手順ではなく、次のトピック、「クラウド Web セキュリティにトラフィックを送信するサービス ポリシーの方法」（P.16-10）で説明している手順を使用してください。前述の手順では、ポリシー インスペクション マップの設定方法を含む、完全なポリシー設定について説明しています。

表 8-2　インスペクション プロトコル（続き）

プロトコル	インスペクション ポリシー マップのサポート	インスペクション クラス マップのサポート	注意
DCERPC	Yes	No	「DCERPC インスペクション」（P.12-1）を参照してください。
DNS	Yes	Yes	「DNS インスペクション」（P.9-1）を参照してください。
ESMTP	Yes	No	「SMTP および拡張 SMTP 検査」（P.9-34）を参照してください。
FTP	Yes	Yes	「FTP インスペクション」（P.9-8）を参照してください。
GTP	Yes	No	「GTP インスペクション」（P.12-4）を参照してください。
H.323 H.225	Yes	Yes	「H.323 インスペクション」（P.10-2）を参照してください。
H.323 RAS	Yes	Yes	「H.323 インスペクション」（P.10-2）を参照してください。
HTTP	Yes	Yes	「HTTP インスペクション」（P.9-14）を参照してください。
ICMP	No	No	「ICMP インスペクション」（P.9-20）を参照してください。
ICMP Error	No	No	「ICMP エラー インスペクション」（P.9-20）を参照してください。
ILS	No	No	「ILS インスペクション」（P.11-1）を参照してください。
IM	Yes	Yes	「インスタント メッセージ インスペクション」（P.9-21）を参照してください。
IP-Options	Yes	No	「IP オプション インスペクション」（P.9-24）を参照してください。
IPSec パススルー	Yes	No	「IPsec パススルー インスペクション」（P.9-27）を参照してください。
IPv6	Yes	No	「IPv6 インスペクション」（P.9-30）を参照してください。
MGCP	Yes	No	「MGCP インスペクション」（P.10-9）を参照してください。
NetBIOS	Yes	No	「NETBIOS インスペクション」（P.9-32）を参照してください。
PPTP	No	No	「PPTP インスペクション」（P.9-34）を参照してください。

表 8-2　インスペクション プロトコル（続き）

プロトコル	インスペクション ポリシー マップのサポート	インスペクション クラス マップのサポート	注意
RADIUS アカウンティング	Yes	No	「RADIUS アカウンティング インスペクション」（P.12-9）を参照してください。 RADIUS アカウンティング インスペクションは管理サービス ポリシーでのみ使用可能です。このインスペクションを実装するには、ポリシー マップを選択する必要があります。
RSH	No	No	「RSH インスペクション」（P.12-12）を参照してください。
RTSP	Yes	No	「RTSP インスペクション」（P.10-13）を参照してください。
SCCP（Skinny）		No	「Skinny（SCCP）インスペクション」（P.10-25）を参照してください。
SIP	Yes	Yes	「SIP インスペクション」（P.10-17）を参照してください。
SNMP	Yes	No	「SNMP インスペクション」（P.12-12）を参照してください。
SQLNET	No	No	「SQL*Net インスペクション」（P.11-2）を参照してください。
SUNRPC	No	No	「Sun RPC インスペクション」（P.11-3）を参照してください。 デフォルトのクラス マップには 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には、TCP ポート 111 を照合する新しいクラス マップを作成し、クラスをポリシーに追加してから、そのクラスに **inspect sunrpc** コマンドを適用する必要があります。
TFTP	No	No	「TFTP インスペクション」（P.9-39）を参照してください。
WAAS	No	No	TCP オプション 33 解析をイネーブルにします。Cisco Wide Area Application Services 製品を導入するときに使用します。
XDMCP	No	No	「XDMCP インスペクション」（P.12-13）を参照してください。

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）。

正規表現の設定

正規表現は、テキスト文字列のパターン照合を定義します。一部のプロトコル インスペクション マップでは、正規表現を使用して、URL や特定のヘッダー フィールドのコンテンツなどの文字列に基づいてパケットを照合できます。

- 「正規表現の作成」（P.8-14）
- 「正規表現クラス マップの作成」（P.8-17）

正規表現の作成

正規表現は、ストリングそのものとしてテキスト ストリングと文字どおりに照合することも、*メタ文字*を使用してテキスト ストリングの複数のバリアントと照合することもできます。正規表現を使用して特定のアプリケーション トラフィックの内容と照合できます。たとえば、HTTP パケット内部の URL 文字列と照合できます。

はじめる前に

正規表現をパケットと照合する場合のパフォーマンスへの影響については、コマンド リファレンスの **regex** コマンドを参照してください。一般的に、長い入力文字列と照合したり、多くの正規表現と照合しようとすると、システム パフォーマンスが低下します。

(注)　最適化のために、ASA では、難読化解除された URL が検索されます。難読化解除では、複数のスラッシュ（/）が単一のスラッシュに圧縮されます。通常、「http://」のようなダブル スラッシュが使用される文字列では、代わりに「http:/」を検索してください。

次の表に、特別な意味を持つメタ文字を示します。

表 8-3　正規表現のメタ文字

文字	説明	注意
.	ドット	任意の単一文字と一致します。たとえば、**d.g** は、dog、dag、dtg、およびこれらの文字を含む任意の単語（doggonnit など）に一致します。
(*exp*)	サブ表現	サブ表現は、文字を周囲の文字から分離して、サブ表現に他のメタ文字を使用できるようにします。たとえば、**d(o|a)g** は dog および dag に一致しますが、**do|ag** は do および ag に一致します。また、サブ表現を繰り返し限定作用素とともに使用して、繰り返す文字を区別できます。たとえば、**ab(xy){3}z** は、abxyxyxyz に一致します。
|	代替	このメタ文字によって区切られている複数の表現のいずれかと一致します。たとえば、**dog|cat** は、dog または cat に一致します。
?	疑問符	直前の表現が 0 または 1 個存在することを示す修飾子。たとえば、**lo?se** は、lse または lose に一致します。
*	アスタリスク	直前の表現が 0、1、または任意の個数存在することを示す修飾子。たとえば、**lo*se** は、lse、lose、loose などに一致します。

表 8-3　正規表現のメタ文字 （続き）

文字	説明	注意
+	プラス	直前の表現が少なくとも 1 個存在することを示す修飾子。たとえば、**lo+se** は、lose および loose に一致しますが、lse には一致しません。
{*x***}** または **{***x***,}**	最小繰り返し限定作用素	少なくとも *x* 回繰り返します。たとえば、**ab(xy){2,}z** は、abxyxyz や abxyxyxyz などに一致します。
[*abc***]**	文字クラス	カッコ内の任意の文字と一致します。たとえば、**[abc]** は、a、b、または c に一致します。
[^*abc***]**	否定文字クラス	角カッコに含まれていない単一文字と一致します。たとえば、**[^abc]** は、a、b、c 以外の任意の文字に一致します。**[^A-Z]** は、大文字のアルファベット文字以外の任意の単一の文字に一致します。
[*a-c***]**	文字範囲クラス	範囲内の任意の文字と一致します。**[a-z]** は、任意の小文字のアルファベット文字に一致します。文字と範囲を組み合わせて使用することもできます。**[abcq-z]** および **[a-cq-z]** は、a、b、c、q、r、s、t、u、v、w、x、y、z に一致します。 ダッシュ（-）文字は、角カッコ内の最初の文字または最後の文字である場合にのみリテラルとなります（**[abc-]** や **[-abc]**）。
「」	引用符	文字列の末尾または先頭のスペースを保持します。たとえば、**" test"** は、一致を検索する場合に先頭のスペースを保持します。
^	キャレット	行の先頭を指定します。
****	エスケープ文字	メタ文字とともに使用すると、リテラル文字と一致します。たとえば、**\[** は左角カッコに一致します。
char	文字	文字がメタ文字でない場合は、リテラル文字と一致します。
\r	復帰	復帰 0x0d と一致します。
\n	改行	改行 0x0a と一致します。
\t	タブ	タブ 0x09 と一致します。
\f	改ページ	フォーム フィード 0x0c と一致します。
\x*NN*	エスケープされた 16 進数	16 進数（厳密に 2 桁）を使用した ASCII 文字と一致します。
*****NNN*	エスケープされた 8 進数	8 進数（厳密に 3 桁）としての ASCII 文字と一致します。たとえば、文字 040 はスペースを表します。

手順

ステップ 1　[Configuration] > [Firewall] > [Objects] > [Regular Expressions] を選択します。

ステップ 2　[Regular Expressions] 領域で、次のいずれかを実行します。

- [Add] を選択し、新しいオブジェクトを追加します。名前を入力し、任意で説明を入力します。

- 既存のオブジェクトを選択し、[Edit] をクリックします。

ステップ 3　[Value] フィールドに正規表現を入力するか、[Build] をクリックしてヘルプを利用しながら表現を作成します。

正規表現の長さは 100 文字までに制限されています。

[Build] をクリックした場合、次のプロセスを使用して表現を作成します。

a. [Build Snippet] 領域で、次のオプションを使用して表現のコンポーネントを作成します。作成中の表現を表示するには、この項の終わりにある [Snippet Preview] 領域を確認してください。

- [Starts at the beginning of the line (^)]：部分式は行頭から開始し、開始場所はメタ文字のカレット（^）で示します。このオプションを使用して作成した部分式は、正規表現の先頭に挿入してください。
- [Specify Character String]：単語やフレーズなどの特定の文字列を照合しようとしている場合、その文字列を入力します。

  テキスト文字列の中に文字どおりに使用したいメタ文字がある場合、[Escape Special Characters] を選択し、そのメタ文字の前にエスケープ文字のバックスラッシュ（\）を追加します。たとえば、「example.com」と入力すると、このオプションによって「example\.com」に変換されます。

  大文字および小文字を照合したい場合は、[Ignore Case] を選択します。たとえば、「cats」は「[cC][aA][tT][sS]」に変換されます。
- [Specify Character]：特定のフレーズではなく、特定タイプの文字や文字の組み合わせを照合しようとしている場合は、このオプションを選択し、次のオプションを使用して文字を特定します。

  [Negate the character]：識別した文字を照合の対象外に指定します。

  [Any character (.)]：すべての文字と一致させる、メタ文字のピリオド（.）を挿入します。たとえば、**d.g** は、dog、dag、dtg、およびこれらの文字を含む任意の単語（doggonnit など）に一致します。

  [Character set]：文字セットを挿入します。テキストをこのセットに含まれるすべての文字と照合します。たとえば、[0-9A-Za-z] の場合、部分式は 0 ～ 9 の数字と A ～ Z の大文字および小文字と照合します。[\n\f\r\t] セットは、改行、改ページ、復帰、タブと一致します。

  [Special character]：エスケープが必要な文字（\、?、*、+、|、.、[、(、^ など）を挿入します。エスケープ文字はバックスラッシュ（\）で、このオプションを選択すると自動的に入力されます。

  [Whitespace character]：空白スペースには \n（改行）、\f（改ページ）、\r（復帰）、\t（タブ）があります。

  [Three digit octal number]：8 進数を使用する ASCII 文字（3 桁まで）と一致します。たとえば、\040 はスペースを意味します。バックスラッシュ（\）は自動的に入力されます。

  [Two digit hexadecimal number]：16 進数を使用する ASCII 文字（厳密に 2 桁）と一致します。バックスラッシュ（\）は自動的に入力されます。

  [Specified character]：任意の 1 文字を入力します。

b. 次のいずれかのボタンを使用して、正規表現ボックスに部分式を追加します。正規表現ボックスに直接入力できることにも注意してください。

- [Append Snippet]：部分式を正規表現の最後に追加します。

- [Append Snippet as Alternate]：部分式をパイプ記号（|）で区切って、正規表現の最後に追加します。区切られた表現の一方と照合します。たとえば、**dog|cat** は、dog または cat に一致します。
- [Insert Snippet at Cursor]：部分式をカーソル位置に挿入します。

c. 表現が完了するまで、部分式を追加するプロセスを繰り返します。

d. （オプション）[Selection Occurrences] では、表現またはその一部を、一致すると考えられるテキストとどれくらいの頻度で照合する必要があるかを選択します。[Regular Expression] フィールドでテキストを選択し、次のいずれかのオプションをクリックしてから [Apply to Selection] をクリックします。たとえば、正規表現が「test me」であり、「me」を選択して [One or more times] を適用する場合、正規表現は「test (me)+」に変更されます。

- [Zero or one times (?)]：直前の表現が 0 または 1 個存在します。たとえば、**lo?se** は、lse または lose に一致します。
- [One or more times (+)]：直前の表現が少なくとも 1 個存在します。たとえば、**lo+se** は、lose および loose に一致しますが、lse には一致しません。
- [Any number of times (*)]：直前の表現が 0、1、または任意の個数あります。たとえば、**lo*se** は、lse、lose、loose などに一致します。
- [At least]：少なくとも *x* 回繰り返します。たとえば、**ab(xy){2,}z** は、abxyxyz や abxyxyxyz などに一致します。
- [Exactly]：*x* 回だけ繰り返します。たとえば、**ab(xy){3}z** は、abxyxyxyz に一致します。

e. 表現が意図したテキストに一致することを検証するには、[Test] をクリックします。テストが失敗した場合は、[Test] ダイアログボックスで編集を試みるか、表現ビルダーに戻ることができます。テキスト ダイアログの表現を編集し、[OK] をクリックすると、編集内容が保存され、表現ビルダーに反映されます。

f. [OK] をクリックします。

正規表現クラス マップの作成

正規表現クラス マップは、1 つ以上の正規表現を特定します。正規表現クラス マップは、正規表現オブジェクトを集めているにすぎません。多くの場合、正規表現オブジェクトの代わりに正規表現クラス マップを使用できます。

手順

ステップ 1　[Configuration] > [Firewall] > [Objects] > [Regular Expressions] を選択します。

ステップ 2　[Regular Expressions Classes] 領域で、次のいずれかを実行します。

- [Add] を選択して、新しいクラス マップを追加します。名前を入力し、任意で説明を入力します。
- 既存のクラス マップを選択し、[Edit] をクリックします。

ステップ 3　マップに含めたい表現を選択し、[Add] をクリックします。不要なものを削除します。

ステップ 4　[OK] をクリックします。

アプリケーション インスペクションの履歴

機能名	リリース	説明
インスペクション ポリシー マップ	7.2(1)	インスペクション ポリシー マップが導入されました。**class-map type inspect** コマンドが導入されました。
正規表現およびポリシー マップ	7.2(1)	インスペクション ポリシー マップで使用される正規表現およびポリシー マップが導入されました。**class-map type regex** コマンド、**regex** コマンド、および**match regex** コマンドが導入されました。
インスペクション ポリシー マップの match any	8.0(2)	インスペクション ポリシー マップで使用される **match any** キーワードが導入されました。トラフィックを 1 つ以上の基準に照合してクラス マップに一致させることができます。以前は、**match all** だけが使用可能でした。