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。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。

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ションされます。

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。

- トラフィック照合基準：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照合基準では、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照合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、異なる照合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

サービス ポリシーのポリシー マップでインスペクションが有効になっている場合、ポリシーマップの交換は2つのステップからなるプロセスです。まず、サービス ポリシーからインスペクションを削除し、変更を適用する必要があります。次に、再度追加し、新しいポリシーマップ名を選択して、再度変更を適用します。

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クラスまたはダイレクト マッチに一致する場合、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、それ以降の照合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、同一の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 match 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 マップまたはダイレクト マッチ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 match 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。各クラス マップの重要度が最低の照合が異なる場合、重要度が高い match 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

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、M3UA、および SIP は例外です。ステートフル フェールオーバーを取得するために、M3UA インスペクションで厳密なアプリケーション サーバ プロセス（ASP）のステート チェックを設定する必要があります。

クラスタ

次のインスペクションはクラスタリングではサポートされていません。

- CTIQBE
- H323、H225、および RAS
- IPsec パススルー
- MGCP
- MMP
- RTSP
- SCCP（Skinny）
- WAAS

IPv6

IPv6 は次のインスペクションでサポートされています。

- Diameter
- DNS over UDP
- FTP
- GTP
- HTTP
- ICMP
- IPSec パススルー
- IPv6
- M3UA
- SCCP（Skinny）
- SCTP
- SIP
- SMTP
- VXLAN

NAT64 は次のインスペクションでサポートされています。

- DNS over UDP
- FTP
- HTTP
- ICMP
- SCTP

その他のガイドライン

- 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 （5 ページ）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。
- TCP接続にインスペクションが必要であるとシステムが判断した場合、システムはそれらのインスペクションの前に、パケット上でMSSおよび選択的確認応答（SACK）オプションを除き、すべての TCP オプションをクリアします。その他のオプションは、接続に適用されている TCP マップで許可されているとしてもクリアされます。
- 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

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 *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 プロトコル、ポート	NAT に関する制限事項	標準	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。	—	—
Diameter	TCP/3868 TCP/5868（TCP/TLS 用） SCTP/3868	NAT/PAT なし。	RFC 6733	キャリアライセンスが必要です。
DNS over UDP DNS over TCP	UDP/53 UDP/443 TCP/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	DNS over TCP を検査するには、DNS インスペクション ポリシーマップで DNS/TCP インスペクションを有効にする必要があります。 UDP/443 は、Cisco Umbrella DNScrypt セッションのみに使用されます。
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（GTPv0） UDP/2123（GTPv1+）	拡張 PAT はサポートされません。 NAT なし。	—	キャリアライセンスが必要です。

アプリケーション	デフォルト プロトコル、ポート	NAT に関する制限事項	標準	注
H.323 H.225 および **RAS**	TCP/1720 UDP/1718 UDP（RAS）1718～1719	（クラスタリング）スタティック PAT なし。 拡張 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	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	ICMP	—	—	—
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	RSVP	NAT64 なし。	RFC 791、RFC 2113	—
IPsec Pass Through	UDP/500	PAT はサポートされません。 NAT64 なし。	—	—
IPv6	—	NAT64 なし。	RFC 2460	—
LISP	—	NAT および PAT はサポートされません。	—	—

アプリケーション	デフォルト プロトコル、ポート	NAT に関する制限事項	標準	注
M3UA	SCTP/2905	埋め込まれたアドレスに対する NAT または PAT はなし。	RFC 4666	キャリアライセンスが必要です。
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	UDP/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。

アプリケーション	デフォルト プロトコル、ポート	NAT に関する制限事項	標準	注
SCTP	SCTP	—	RFC 4960	キャリアライセンスが必要です。 SCTP トラフィックでスタティック ネットワーク オブジェクト NAT を実行できますが（ダイナミック NAT/PAT なし）、インスペクション エンジンは NAT には使用されません。
SIP モード（SIP	TCP/5060 UDP/5060	セキュリティ レベルが同じインターフェイス、または低セキュリティ レベルから高セキュリティ レベルに至るインターフェイス上の NAT/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 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。 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 FXOS も実行するプラットフォーム上の UDP/4161。	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

アプリケーション	デフォルト プロトコル、ポート	NAT に関する制限事項	標準	注
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
STUN	TCP/3478 UDP/3478	（WebRTC）スタティック NAT/PAT44 のみ。 （Cisco Spark）スタティック NAT/PAT44 と 64、およびダイナミック NAT/PAT。	RFC 5245、5389	—
Sun RPC	TCP/111 UDP/111	拡張 PAT はサポートされません。 NAT64 なし。	—	—
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。	—	—
VXLAN	UDP/4789	N/A	RFC 7348	Virtual Extensible Local Area Network。

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。

インスペクションは、一部のアプリケーションの標準のポートとプロトコルに関しては、デフォルトですべてのインターフェイスでグローバルに有効になっています。デフォルトのインスペクションの詳細については、デフォルト インスペクションと NAT に関する制限事項 （5 ページ） を参照してください。インスペクションの設定をカスタマイズする一般的な方法は、デフォルトのグローバル ポリシーをカスタマイズすることです。または、たとえばインターフェイス固有のポリシーなど、必要に応じて新しいサービス ポリシーを作成することもできます。

始める前に

一部のアプリケーションでは、インスペクション ポリシー マップを設定することで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ます。この手順の後半の表に、インスペクション ポリシー マップを使用できるプロトコルを示します。また、それらの設定手順へのポインタも記載しています。これらの拡張機能を設定する場合は、インスペクションを設定する前にマップを作成します。

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 ルールを開きます。

- デフォルトのグローバル ポリシーを編集するには、[Global] フォルダの「inspection_default」ルールを選択して、[Edit] をクリックします。
- 新しいルールを作成するには、[Add] > [Add Service Policy Rule] をクリックします。ウィザードの [Rules] ページまで進みます。
- 別のインスペクション ルールがある場合、またはインスペクションを追加しているルールがある場合は、それを選択して、[Edit] をクリックします。

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 インスペクションと NAT に関する制限事項 （5 ページ）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は、代わりに管理サービス ポリシー ルールを作成します。RADIUS アカウンティング インスペクションの設定を参照してください。

ステップ 3 [Rule Actions] ウィザード ページまたはタブで、[Protocol Inspection] タブを選択します。

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ンにします。
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 マップおよび他のオプションを設定するには、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 *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	なし	なし	CTIQBE インスペクションを参照してください。
DCERPC	対応	対応	DCERPC インスペクションを参照してください。

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
Diameter	対応	対応	Diameter インスペクションを参照してください。 暗号化された Diameter トラフィックを検査する場合は、[Enable encrypted traffic inspection] を選択し、TLS プロキシを選択します（必要であれば、[Manage] をクリックして作成します）。
DNS	対応	対応	DNS インスペクションを参照してください。 ボットネット トラフィック フィルタを使用している場合は、[Enable DNS snooping] を選択します。DNS スヌーピングは、外部 DNS 要求が送信されるインターフェイスでだけイネーブルにすることを推奨します。すべての UDP DNS トラフィック（内部 DNS サーバへの送信トラフィックを含む）に対して DNS スヌーピングをイネーブルにすると、ASA で不要な負荷が発生します。たとえば、DNS サーバが外部インターフェイスに存在する場合は、外部インターフェイスのすべての UDP DNS トラフィックに対して DNS インスペクションとスヌーピングをイネーブルにする必要があります。
ESMTP	対応	非対応	SMTP および拡張 SMTP インスペクションを参照してください。
FTP	対応	対応	FTP インスペクションを参照してください。 [Use Strict FTP] を選択して、インスペクション ポリシー マップを選択します。厳密な FTP を使用すると、Web ブラウザが FTP 要求内の埋め込みコマンドを送信できなくなるため、保護されたネットワークのセキュリティが強化されます。
GTP	対応	非対応	GTP インスペクションの概要を参照してください。
H.323 H.225	対応	対応	H.323 インスペクションを参照してください。
H.323 RAS	対応	対応	H.323 インスペクションを参照してください。

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
HTTP	対応	対応	HTTP インスペクションを参照してください。
ICMP	なし	なし	ICMP インスペクションを参照してください。
ICMP Error	なし	なし	ICMP エラー インスペクションを参照してください。
ILS	なし	なし	ILS インスペクションを参照してください。
IM	対応	対応	インスタント メッセージ インスペクションを参照してください。
IP-Options	対応	非対応	IP オプション インスペクションを参照してください。
IPSec パススルー	対応	非対応	IPsec パススルー インスペクションを参照してください。
IPv6	対応	非対応	IPv6 インスペクションを参照してください。
LISP	対応	非対応	インスペクションなどの LISP を設定する詳細については、全般設定ガイドのクラスタリングの章を参照してください。
M3UA	対応	非対応	M3UA インスペクションを参照してください。
MGCP	対応	非対応	MGCP インスペクションを参照してください。
NetBIOS	対応	非対応	NetBIOS インスペクションを参照してください。
PPTP	なし	なし	PPTP インスペクションを参照してください。
RADIUS Accounting	対応	非対応	RADIUS アカウンティング インスペクションの概要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	なし	なし	RSH インスペクションを参照してください。
RTSP	対応	非対応	RTSP インスペクションを参照してください。

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
SCCP（Skinny）	対応	非対応	Skinny（SCCP）インスペクションを参照してください。
SCTP	対応	非対応	SCTP アプリケーション レイヤのインスペクションを参照してください。
SIP	対応	対応	SIP インスペクションを参照してください。 暗号化された SIP トラフィックを検査する場合は、[Enable encrypted traffic inspection] を選択し、TLS プロキシを選択します（必要であれば、[Manage]をクリックして作成します）。
SNMP	対応	非対応	SNMPインスペクションを参照してください。
SQLNET	なし	なし	SQL*Net インスペクションを参照してください。
STUN	なし	なし	STUNインスペクションを参照してください。
SUNRPC	なし	なし	Sun RPC インスペクション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 SUNRPC インスペクションを適用する必要があります。
TFTP	なし	なし	TFTPインスペクションを参照してください。
WAAS	なし	なし	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	なし	なし	XDMCP インスペクションを参照してください。
VXLAN	なし	なし	VXLAN インスペクションを参照してください。

ステップ 6 [OK] または [Finish] をクリックして、サービス ポリシー ルールを保存します。

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

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。

始める前に

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 リファレンスで 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 *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。

文字	説明	注意
(*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。
+	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、大文字以外の任意の 1 文字に一致します。

文字	説明	注意
[*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] をクリックしてサポート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通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」と入力した場合、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) （任意）[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。

インスペクション ポリシーのモニタリング

インスペクション サービス ポリシーをモニタするには、次のコマンドを入力します。コマンドを入力するには、**[Tools]** > **[Command Line Interface]** を選択します。構文の詳細と例については、Cisco.com のコマンド リファレンスを参照してください。

- **show service-policy inspect** *protocol*

  インスペクション サービス ポリシーの統計情報を表示します。*protocol* は、**dns** などの inspect コマンドからのプロトコルです。ただし、すべてのインスペクション プロトコルでこのコマンドを使用して統計情報が表示されるわけではありません。次に例を示します。

```
asa# show service-policy inspect dns

Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
      Inspect: dns preset_dns_map, packet 0, lock fail 0, drop 0, reset-drop 0,
5-min-pkt-rate 0 pkts/sec, v6-fail-close 0
        message-length maximum client auto, drop 0
        message-length maximum 512, drop 0
        dns-guard, count 0
        protocol-enforcement, drop 0
        nat-rewrite, count 0
asa#
```

- **show conn**

デバイスを通過するトラフィックの現在の接続を示します。さまざまなプロトコルに関する情報を取得できるように、このコマンドにはさまざまなキーワードがあります。

- 特定の検査対象プロトコルの追加コマンドは次のとおりです。
  - **show ctiqbe**

    CTIQBEインスペクションエンジンによって割り当てられたメディア接続に関する情報を表示します。
  - **show h225**

    H.225 セッションの情報を表示します。
  - **show h245**

    スロースタートを使用しているエンドポイントによって確立されたH.245セッションの情報を表示します。
  - **show h323 ras**

    ゲートキーパーとその H.323 エンドポイントの間に確立されている H.323 RAS セッションの接続情報を表示します。
  - **show mgcp** {**commands** | **sessions** }

    コマンド キュー内の MGCP コマンドの数、または既存の MGCP セッションの数を表示します。
  - **show sip**

    SIP セッションの情報を表示します。
  - **show skinny**

    Skinny（SCCP）セッションに関する情報を表示します。
  - **show sunrpc-server active**

    Sun RPC サービス用に開けられているピンホールを表示します。

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。

機能名	リリース	説明
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。