

基本インターネット プロトコルのインスペクション

ここでは、基本インターネット プロトコルのアプリケーション インスペクションについて説明します。特定のプロトコルに関してインスペクションを使用する必要がある理由、およびインスペクションを適用する全体的な方法については、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準備を参照してください。

- DCERPC インスペクション （2 ページ）
- DNS インスペクション （5 ページ）
- FTP インスペクション （9 ページ）
- HTTP インスペクション （15 ページ）
- ICMP インスペクション （19 ページ）
- ICMP エラー インスペクション （20 ページ）
- ILS インスペクション （21 ページ）
- インスタント メッセージ インスペクション （21 ページ）
- IP オプション インスペクション （24 ページ）
- IPsec パススルー インスペクション （26 ページ）
- IPv6 インスペクション （28 ページ）
- NetBIOS インスペクション （30 ページ）
- PPTP インスペクション （30 ページ）
- RSH インスペクション （31 ページ）
- SMTP および拡張 SMTP インスペクション （31 ページ）
- SNMP インスペクション （36 ページ）
- SQL*Net インスペクション （37 ページ）
- Sun RPC インスペクション （38 ページ）
- TFTP インスペクション （39 ページ）
- XDMCP インスペクション （40 ページ）
- VXLAN インスペクション （40 ページ）
- 基本的なインターネット プロトコル インスペクションの履歴 （41 ページ）

DCERPC インスペクション

デフォルトのインスペクション ポリシーでは、DCERPC インスペクションがイネーブルにされていないため、この検査が必要な場合はイネーブルにします。デフォルトのグローバルインスペクション ポリシーを編集するだけで、DCERPC インスペクションを追加できます。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。

次の項では、DCERPC インスペクション エンジンについて説明します。

DCERPC の概要

DCERPC に基づく Microsoft リモート プロシージャ コール（MSRPC）は、Microsoft 分散クライアントおよびサーバー アプリケーションで広く使用されているプロトコルであり、ソフトウェア クライアントがサーバー上のプログラムをリモートで実行できるようにします。

通常、このプロトコルの接続では、クライアントが予約済みポート番号で接続を受け入れるエンドポイント マッパーというサーバーに、必要なサービスについてダイナミックに割り当てられるネットワーク情報を問い合わせます。次に、クライアントは、サービスを提供しているサーバーのインスタンスへのセカンダリ接続をセットアップします。セキュリティ アプライアンスは、適切なポート番号とネットワーク アドレスへのセカンダリ接続を許可し、必要に応じて NAT を適用します。

DCERPC インスペクション エンジンは、EPM とウェルノウン TCP ポート 135 上のクライアントとの間のネイティブ TCP 通信を検査します。クライアント用に EPM のマッピングとルックアップがサポートされています。クライアントとサーバーは、どのセキュリティ ゾーンにあってもかまいません。埋め込まれたサーバーの IP アドレスとポート番号は、EPM からの応答メッセージで受け取ります。クライアントが EPM から返されたサーバーのポートに対して複数の接続を試みる可能性があるので、ピンホールが複数使用でき、ユーザーがそのタイムアウトを設定できるようになっています。

DCE インスペクションは、次の汎用一意識別子（UUID）とメッセージをサポートします。

- エンドポイント マッパー（EPM）UUID。すべての EPM メッセージがサポートされます。
- ISystemMapper UUID（非 EPM）。サポートされるメッセージ タイプは次のとおりです。
  - RemoteCreateInstance opnum4
  - RemoteGetClassObject opnum3
- OxidResolver UUID（非EPM）。サポートされるメッセージは次のとおりです。
  - ServerAlive2 opnum5
- IP アドレスまたはポート情報を含まない任意のメッセージ（これらのメッセージでは検査の必要がないため）。

DCERPC インスペクション ポリシー マップの設定

DCERPC インスペクションの追加のパラメータを指定するには、DCERPC インスペクション ポリシー マップを作成します。作成したインスペクション ポリシー マップは、DCERPC インスペクションをイネーブルにすると適用できます。

トラフィックの一致基準を定義するときに、クラスマップを作成するか、またはポリシーマップにmatchステートメントを直接含めることができます。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、クラスマップを再使用できる点です。次に、インスペクション ポリシー マップの手順について説明していますが、クラスマップで使用可能なトラフィックの一致基準についても説明します。クラス マップを作成するには、**[Configuration]** > **[Firewall]** > **[Objects]** > **[Class Maps]** > **[DCERPC]** の順に選択します。

ヒント　以下で説明する手順に加えて、サービス ポリシーの作成中にインスペクション マップを設定できます。マップの内容は、作成方法に関係なく同じです。

手順

ステップ 1　**[Configuration]** > **[Firewall]** > **[Objects]** > **[Inspect Maps]** > **[DCERPC]** を選択します。

ステップ 2　次のいずれかを実行します。

- [Add] をクリックして、新しいマップを追加します。
- 内容を表示するマップを選択します。セキュリティ レベルを直接変更することも、[Customize]をクリックしてマップを編集することもできます。この後の手順では、マップをカスタマイズまたは追加するものとします。

ステップ 3　新しいマップの場合、名前（最大 40 文字）と説明を入力します。マップを編集するときは、変更できるのは説明のみです。

ステップ 4　[DCERPC Inspect Map] ダイアログボックスの [Security Level] のビューで、希望する設定に一致するレベルを選択します。

プリセット レベルのいずれかが要件と一致する場合、以上で終了です。[OK] をクリックし、残りの手順をとばし、DCERPC インスペクションのサービス ポリシー ルールでマップを使用します。

設定をさらにカスタマイズする必要がある場合は、[Details] をクリックし、手順を続けます。

ヒント　[UUID Filtering] ボタンは、この手順の後半で説明されるメッセージ フィルタリングを設定するショートカットです。

ステップ 5 必要なオプションを設定します。

- [Pinhole Timeout] ：ピンホール タイムアウトを設定します。クライアントが使用するサーバー情報は、複数の接続のエンドポイントマッパーから返される場合があるため、タイムアウト値はクライアントのアプリケーション環境を考慮して設定します。範囲は、0:0:1 ～ 1193:0:0 です。
- [Enforce endpoint-mapper service] ：サービスのトラフィックだけが処理されるよう、バインディング時にエンドポイント マッパー サービスを実行するかどうか設定します。
- [Enable endpoint-mapper service lookup]：エンドポイント マッパー サービスのルックアップ操作をイネーブルにするかどうか設定します。サービス ルックアップのタイムアウトも適用できます。タイムアウトを設定しない場合は、ピンホール タイムアウトが適用されます。

ステップ 6 （任意）[Inspections] タブをクリックして、特定のタイプのメッセージに対して実行するアクションを定義します。

DCERPC クラス マップに基づいて、またはインスペクション マップで一致を直接設定することによって、またはその両方で、トラフィックの一致基準を定義できます。

a) 次のいずれかを実行します。
   - [Add] をクリックして、新しい基準を追加します。
   - 既存の基準を選択し、[Edit] をクリックします。
b) [Single Match] を選択して基準を直接定義するか、または [Multiple Match] を選択して基準を定義する DCERPC クラス マップを選択します。
c) 基準をここで定義した場合は、基準の一致タイプとして [Match] （トラフィックは基準と一致する必要がある）または [No Match] （トラフィックは基準と異なる必要がある）を選択します。次に、希望する UUID を選択します。
   - **ms-rpc-epm**：Microsoft RPC EPM メッセージを照合します。
   - **ms-rpc-isystemactivator**：ISystemMapper メッセージを照合します。
   - **ms-rpc-oxidresolver**：OxidResolver メッセージを照合します。
d) 接続を**リセットする**か、**ログに記録する**かを選択します。接続をリセットすることを選択した場合、ロギングを有効にすることもできます。接続をリセットすると、パケットがドロップされ、接続が閉じられ、サーバーまたはクライアントに TCP リセットが送信されます。
e) [OK] をクリックして、基準を追加します。必要に応じてプロセスを繰り返します。

ステップ 7 [OK] をクリックします。

これで、DCERPC インスペクションのサービス ポリシーで、インスペクション マップを使用できます。

次のタスク

マップを使用するためのインスペクション ポリシーを設定できるようになりました。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 を参照してください。

DNS インスペクション

DNSインスペクションはデフォルトでイネーブルになっています。デフォルト以外の処理が必要な場合にのみ設定する必要があります。ここでは、DNS アプリケーション インスペクションについて説明します。

DNS インスペクションのデフォルト

DNS インスペクションは、次のような preset_dns_map インスペクション クラス マップを使用して、デフォルトでイネーブルになっています。

- 最大 DNS メッセージ長は、512 バイトです。
- DNS over TCP インスペクションは無効です。
- 最大クライアント DNS メッセージ長は、リソース レコードに一致するように自動的に設定されます。
- DNS ガードはイネーブルになり、ASA によって DNS 応答が転送されるとすぐに、ASA は DNS クエリに関連付けられている DNS セッションを切断します。ASA はまた、メッセージ交換をモニターして DNS 応答の ID が DNS クエリの ID と一致することを確認します。
- NAT の設定に基づく DNS レコードの変換はイネーブルです。
- プロトコルの強制はイネーブルであり、DNSメッセージ形式チェックが行われます。ドメイン名の長さが 255 文字以下、ラベルの長さが 63 文字、圧縮、ループ ポインタのチェックなどです。

（注） 毎秒多数のパケットが検査される場合、Cisco ASA で CPU 使用率が上昇する可能性があります。処理されるパケットの数が増えると（特にデバイスがスループットまたは接続キャパシティの最大値に近づいた場合）、CPU 使用率も上昇します。これは、Cisco ASA が毎秒多くの操作を実行する必要があり、CPU リソースの消費が増えるために発生します。

DNS インスペクション ポリシー マップの設定

デフォルトのインスペクション動作がネットワークにとって十分でない場合、DNSインスペクション ポリシー マップを作成して DNS インスペクション アクションをカスタマイズできます。

オプションとして、DNS インスペクション クラス マップを作成し、DNS インスペクションのトラフィック クラスを定義できます。他のオプションとしては、DNS インスペクション ポリシー マップでトラフィック クラスを直接定義することもできます。クラス マップを作成することとインスペクション マップでトラフィックの照合を直接定義することの違いは、クラス マップでは複雑な照合基準を作成でき、クラスマップを再利用できるという点です。この手順ではインスペクションマップについて説明しますが、クラスマップで使用される一致基準は、[Inspection] タブに関する手順で説明されているものと同じです。**[Configuration]** > **[Firewall]** > **[Objects]** > **[Class Maps]** > **[DNS]** を選択するか、またはインスペクション マップの設定時に作成することによって、DNS クラス マップを設定できます。

ヒント 以下で説明する手順に加えて、サービス ポリシーの作成中にインスペクション マップを設定できます。マップの内容は、作成方法に関係なく同じです。

始める前に

一部のトラフィック照合オプションでは、照合のために正規表現を使用します。これらのテクニックの 1 つを使用する場合は、最初に正規表現または正規表現のクラス マップを作成します。

手順

ステップ 1 **[Configuration]** > **[Firewall]** > **[Objects]** > **[Inspect Maps]** > **[DNS]** を選択します。

ステップ 2 次のいずれかを実行します。

- [Add] をクリックして、新しいマップを追加します。
- 内容を表示するマップを選択します。セキュリティ レベルを直接変更することも、[Customize] をクリックしてマップを編集することもできます。この後の手順では、マップをカスタマイズまたは追加するものとします。

ステップ 3 新しいマップの場合、名前（最大 40 文字）と説明を入力します。マップを編集するときは、変更できるのは説明のみです。

ステップ 4 [DNS Inspect Map] ダイアログ ボックスの [Security Level] ビューで、必要なコンフィギュレーションと最もよく一致するレベルを選択します。デフォルトのレベルは [Low] です。

プリセット レベルのいずれかが要件と一致する場合、以上で終了です。[OK] をクリックし、残りの手順をスキップして、DNS インスペクションのサービス ポリシー ルールでマップを使用します。

設定をさらにカスタマイズする必要がある場合は、[Details] をクリックし、手順を続けます。

ステップ 5 [Protocol Conformance] タブをクリックし、必要なオプションを選択します。

- [Enable DNS guard function]： DNS ガードを使用します。ASA によって DNS 応答が転送されるとすぐに、ASA は DNS クエリーに関連付けられている DNS セッションを切断します。ASA はまた、メッセージ交換をモニターして DNS 応答の ID が DNS クエリの ID と一致することを確認します。
- [Enable NAT re-write function] ：DNS レコードを NAT の設定に基づいて変換します。
- [Enable protocol enforcement]： DNS メッセージ形式のチェックをイネーブルにします。ドメイン名の長さが 255 文字以下、ラベルの長さが 63 文字、圧縮、ループ ポインタのチェックなどです。
- [Randomize the DNS identifier for DNS query]。
- [Enable TCP inspection]： DNS over TCP トラフィックのインスペクションを有効にします。DNS/TCP ポート 53 トラフィックが、DNS インスペクションを適用するクラスの一部であることを確認します。インスペクションのデフォルト クラスには、TCP/53 が含まれています。
- [Enforce TSIG resource record to be present in DNS message]： 準拠していないパケットをドロップまたはロギングできます。必要であれば、ドロップされたパケットをロギングできます。

ステップ 6 [Filtering] タブをクリックし、必要なオプションを選択します。

- [Global Settings]：クライアントまたはサーバーのどちらからかに関係なく、指定した最大長を超えるパケットをドロップするかどうかを選択します（512 ～ 65535 バイト）。
- [Server Settings]：[Drop packets that exceed specified maximum length] および [Drop packets sent to server that exceed length indicated by the RR] ：サーバー DNS メッセージの最大長を設定します（512 ～ 65535 バイト）、または、最大長をリソース レコードでの値に設定します。両方の設定をイネーブルにすると、小さい方の値が使用されます。
- [Client Settings]：[Drop packets that exceed specified maximum length] および [Drop packets sent to server that exceed length indicated by the RR] ：クライアント DNS メッセージの最大長を設定します（512 ～ 65535 バイト）、または、最大長をリソース レコードでの値に設定します。両方の設定をイネーブルにすると、小さい方の値が使用されます。

ステップ 7 [Mismatch Rate] タブをクリックして、DNS ID 不一致レートが指定したしきい値を超えた場合のロギングを有効にするかどうかを選択します。たとえば、しきい値を 3 秒あたり 30 個の不一致に設定できます。

ステップ 8 [Inspections] タブをクリックし、トラフィックの特性に基づいて実装する特定のインスペクションを定義します。

DNS クラス マップに基づいて、またはインスペクション マップで一致を直接設定することによって、またはその両方で、トラフィックの一致基準を定義できます。

a) 次のいずれかを実行します。

- [Add] をクリックして、新しい基準を追加します。

- 既存の基準を選択し、[Edit] をクリックします。

b) [Single Match] を選択して基準を直接定義するか、または [Multiple Match] を選択して基準を定義する DNS クラス マップを選択します。

c) 基準をここで定義した場合は、基準の一致タイプとして [Match]（トラフィックは基準と一致する必要がある）または [No Match]（トラフィックは基準と異なる必要がある）を選択します。たとえば、文字列「example.com」で [No Match] を選択した場合、「example.com」を含むトラフィックはすべてクラスマップの対象外になります。次に、基準を以下のように設定します。

- [Header Flag]：フラグが等しい必要があるか、または指定された値を含む必要があるかを選択した後、ヘッダー フラグ名を選択するか、またはヘッダーの 16 進値（0x0 ～ 0xfff）を入力します。複数のヘッダー値を選択する場合、「等しい」はすべてのフラグがパケットに存在する必要があることを示し、「含む」はいずれか 1 つのフラグでもパケットに存在すればよいことを示します。ヘッダー フラグ名は、**AA**（権限応答）、**QR**（クエリー）、**RA**（使用できる再帰）、**RD**（必要な再帰）、**TC**（切り捨て）です。

- [Type]：パケットの DNS タイプ フィールドの名前または値です。フィールド名は、**A**（IPv4 アドレス）、**AXFR**（フルゾーン転送）、**CNAME**（正規の名前）、**IXFR**（増分ゾーン転送）、**NS**（権限ネーム サーバー）、**SOA**（権限ゾーンの開始）、**TSIG**（トランザクション署名）です。値は、DNS タイプ フィールドの 0 ～ 65535 の任意の数字です。特定の値または値の範囲を入力します。

- [Class]：パケットの DNS クラス フィールドの名前または値です。使用可能な唯一のフィールド名は Internet です。値は、DNS クラス フィールドの 0 ～ 65535 の任意の数字です。特定の値または値の範囲を入力します。

- [Question]：DNS メッセージの質問部分です。

- [Resource Record]：DNS のリソース レコードです。追加、応答、権限の各リソース レコード セクションと照合するかどうかを選択します。

d) 一致したトラフィックに対して実行する主要なアクションを選択します。パケットのドロップ、接続の切断、マスク（ヘッダー フラグ一致の場合のみ）、何もしない、のいずれかです。

e) ロギングをイネーブルまたはディセーブルにするかどうかを選択します。TSIG を強制する場合は、ロギングをディセーブルにする必要があります。

f) TSIG リソース レコードの存在を強制するかどうかを選択します。パケットのドロップ、パケットのロギング、またはパケットのドロップとロギングが可能です。通常、TSIG を強制するには [Primary Action] で [None] を選択し、[Log] で [Disable] を選択する必要があります。ただし、ヘッダー フラグ一致の場合は、マスクのプライマリ アクションとともに TSIG を適用できます。

g) [OK] をクリックして、インスペクションを追加します。必要に応じてプロセスを繰り返します。

ステップ 9 [Umbrella Connections] タブをクリックして、クラウドでの Cisco Umbrella への接続を有効にします。

このタブは、**[Configuration]** > **[Firewall]** > **[Objects]** > **[Umbrella]** ページで Cisco Umbrella 接続を設定した場合にのみ機能します。このタブでオプションを設定し、Cisco Umbrella にデバイスを登録して、そのデバイスが DNS ルックアップを Cisco Umbrella にリダイレクトできるようにする必要があります。これを行うと、Cisco Umbrella は FQDN ベースのセキュリティ ポリシーを適用できるようになります。詳細については、Cisco Umbrellaを参照してください。

- [Umbrella]：Cisco Umbrella を有効にします。必要に応じて、デバイスに適用する Cisco Umbrella ポリシーの名前を [Umbrella Tag] フィールドに指定します。ポリシーを指定しない場合は、デフォルトの ACL が適用されます。登録が完了すると、Umbrella のデバイス ID がタグの横に表示されます。
- [Enable Dnscrypt]：DNScrypt を有効にしてデバイスと Cisco Umbrella 間の接続を暗号化します。DNScrypt を有効にすると、Umbrella リゾルバとのキー交換スレッドが開始されます。キー交換スレッドは、1 時間ごとにリゾルバとのハンドシェイクを実行し、新しい秘密鍵でデバイスを更新します。DNScrypt では UDP/443 を使用するため、そのポートが DNS インスペクションに使用するクラス マップに含まれていることを確認する必要があります。デフォルトのインスペクション クラスには DNS インスペクションに UDP/443 がすでに含まれています。
- **フェール オープン**：Umbrella DNS サーバーが使用できない場合に DNS 解決を動作させるには、フェール オープンをイネーブルにします。フェール オープンの状態で Cisco Umbrella DNS サーバーが使用できない場合は、このポリシー マップで Umbrella 自体がディセーブルになり、DNS 要求をシステム上に設定された他の DNS サーバー（存在する場合）に移動できるようになります。Umbrella DNS サーバーが再度使用可能になると、ポリシーマップはそれらの使用を再開します。このオプションを選択しない場合、DNS 要求はアクセスできない Umbrella リゾルバへ移動し続けるので、応答は取得されません。

ステップ 10 [DNS Inspect Map] ダイアログ ボックスの [OK] をクリックします。

DNS インスペクション サービス ポリシーでインスペクション マップを使用できるようになります。

次のタスク

マップを使用するためのインスペクション ポリシーを設定できるようになりました。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 を参照してください。

FTP インスペクション

FTP インスペクションは、デフォルトでイネーブルになっています。デフォルト以外の処理が必要な場合にのみ設定する必要があります。ここでは、FTP インスペクション エンジンについて説明します。

FTP インスペクションの概要

FTP アプリケーション インスペクションは、FTP セッションを検査し、次の 4 つのタスクを実行します。

- FTP データ転送のために動的なセカンダリ データ接続チャネルを準備します。これらのチャネルのポートは、PORT コマンドまたは PASV コマンドを使用してネゴシエートされます。セカンダリ チャネルは、ファイル アップロード、ファイル ダウンロード、またはディレクトリ リスト イベントへの応答で割り当てられます。
- FTP コマンド/応答シーケンスを追跡します。
- 監査証跡を生成します。
  - 取得またはアップロードされたファイルごとに監査レコード 303002 が生成されます。
  - Audit record 201005 is generated if the secondary dynamic channel preparation failed due to memory shortage.
- 埋め込み IP アドレスを変換します。

（注） FTP インスペクションをディセーブルにすると、発信ユーザーはパッシブ モードでしか接続を開始できなくなり、着信 FTP はすべてディセーブルになります。

厳密な FTP

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。厳密な FTP をイネーブルにするには、[Configuration] > [Firewall] > [Service Policy Rules] > [Edit Service Policy Rule] > [Rule Actions] > [Protocol Inspection] タブで、FTP の横にある [Configure] ボタンをクリックします。

厳密な FTP を使用するときは、オプションで FTP インスペクション ポリシー マップを指定して、ASA を通過することが許可されない FTP コマンドを指定できます。

厳密な FTP インスペクションでは、次の動作が強制されます。

- FTP コマンドが確認応答されてからでないと、ASA は新しいコマンドを許可しません。
- ASA は、埋め込みコマンドを送信する接続をドロップします。
- 227 コマンドと PORT コマンドが、エラー文字列に表示されないように確認されます。

注意 厳密な FTP を使用すると、FTP RFC に厳密に準拠していない FTP クライアントは失敗することがあります。さらに、インスペクションを FTP ポートのみに適用する必要があります（通常の FTP ポートは TCP/21 です）。非 FTP トラフィックに厳密な FTP インスペクションを適用すると、（特に HTTP トラフィックで）予期しないトラフィック損失が発生する可能性があります。

厳密な FTP インスペクションでは、各 FTP コマンドと応答のシーケンスを追跡し、次の異常なアクティビティがないかをチェックします。

- 切り捨てされたコマンド：PORT コマンドおよび PASV 応答コマンドのカンマの数が 5 であるかどうかが確認されます。カンマの数が 5 でない場合は、PORT コマンドが切り捨てられていると見なされ、TCP 接続は閉じられます。
- 不正なコマンド：FTP コマンドが、RFC の要求どおりに <CR><LF> 文字で終了しているかどうか確認されます。終了していない場合は、接続が閉じられます。
- RETR コマンドと STOR コマンドのサイズ：これらが、固定の定数と比較チェックされます。サイズが定数より大きい場合は、エラーメッセージがロギングされ、接続が閉じられます。
- コマンドスプーフィング：PORT コマンドは、常にクライアントから送信されます。PORT コマンドがサーバーから送信される場合、TCP 接続は拒否されます。
- 応答スプーフィング：PASV 応答コマンド（227）は、常にサーバーから送信されます。PASV 応答コマンドがクライアントから送信される場合、TCP 接続は拒否されます。これにより、ユーザーが「227 xxxxx a1, a2, a3, a4, p1, p2」を実行する場合のセキュリティ ホールが予防できます。
- TCP ストリーム編集：ASA は、TCP ストリーム編集を検出した場合に接続が閉じられます。
- 無効ポート ネゴシエーション：ネゴシエートされたダイナミック ポート値が、1024 未満であるかどうかが調べられます。1 ～ 1024 の範囲のポート番号は、予約済み接続用に指定されているため、ネゴシエートされたポートがこの範囲内であった場合、TCP 接続は解放されます。
- コマンド パイプライン：PORT コマンドと PASV 応答コマンド内のポート番号の後に続く文字数が、定数の 8 と比べられます。8 より大きい場合は、TCP 接続が閉じられます。
- ASA は SYST コマンドに対する FTP サーバーの応答を連続した X で置き換えて、サーバーのシステム タイプが FTP クライアントに知られないようにします。このデフォルトの動作を無効にするには、FTP マップで、**no mask-syst-reply** コマンドを使用します。

FTP インスペクション ポリシー マップの設定

厳密な FTP インスペクションには、セキュリティと制御を向上させるためのコマンド フィルタリングとセキュリティ チェック機能が用意されています。プロトコルとの適合性のインスペクションには、パケットの長さのチェック、デリミタとパケットの形式のチェック、コマンドのターミネータのチェック、およびコマンドの検証が含まれます。

また、ユーザーの値に基づいてFTP接続をブロックできるので、FTPサイトにダウンロード用のファイルを置き、アクセスを特定のユーザーだけに制限できます。ファイルのタイプ、サーバ名、および他の属性に基づいて、FTP 接続をブロックできます。インスペクション時に FTP 接続が拒否されると、システム メッセージのログが作成されます。

FTP インスペクションで FTP サーバーがそのシステム タイプを FTP クライアントに公開することを許可し、許可する FTP コマンドを制限する場合、FTP インスペクション ポリシー マップを作成および設定します。作成したマップは、FTPインスペクションをイネーブルにすると適用できます。

オプションとして、FTP インスペクション クラス マップを作成し、FTP インスペクションのトラフィック クラスを定義できます。他のオプションとしては、FTP インスペクション ポリシー マップでトラフィック クラスを直接定義することもできます。クラス マップを作成することとインスペクション マップでトラフィックの照合を直接定義することの違いは、クラス マップでは複雑な照合基準を作成でき、クラスマップを再利用できるという点です。この手順ではインスペクションマップについて説明しますが、クラスマップで使用される一致基準は、[Inspection] タブに関する手順で説明されているものと同じです。**[Configuration]** > **[Firewall]** > **[Objects]** > **[Class Maps]** > **[FTP]** を選択するか、またはインスペクション マップの設定時に作成することによって、DNS クラス マップを設定できます。

ヒント　以下で説明する手順に加えて、サービス ポリシーの作成中にインスペクション マップを設定できます。マップの内容は、作成方法に関係なく同じです。

始める前に

一部のトラフィック照合オプションでは、照合のために正規表現を使用します。これらのテクニックの 1 つを使用する場合は、最初に正規表現または正規表現のクラス マップを作成します。

手順

ステップ 1　**[Configuration]** > **[Firewall]** > **[Objects]** > **[Inspect Maps]** > **[FTP]** を選択します。

ステップ 2　次のいずれかを実行します。

- [Add] をクリックして、新しいマップを追加します。

- 内容を表示するマップを選択します。セキュリティ レベルを直接変更することも、[Customize] をクリックしてマップを編集することもできます。この後の手順では、マップをカスタマイズまたは追加するものとします。

ステップ 3 新しいマップの場合、名前（最大 40 文字）と説明を入力します。マップを編集するときは、変更できるのは説明のみです。

ステップ 4 [FTP Inspect Map] ダイアログ ボックスの [Security Level] ビューで、必要なコンフィギュレーションと最もよく一致するレベルを選択します。デフォルトのレベルは [High] です。

プリセット レベルのいずれかが要件と一致する場合、以上で終了です。[OK] をクリックし、残りの手順をスキップして、FTP インスペクションのサービス ポリシー ルールでマップを使用します。

設定をさらにカスタマイズする必要がある場合は、[Details] をクリックし、手順を続けます。

ヒント [File Type Filtering] ボタンはファイル メディアまたは MIME タイプのインスペクションを設定するためのショートカットです。これについては後で説明します。

ステップ 5 [Parameters] タブをクリックし、サーバーからの接続時バナーをマスクするかどうか、または SYST コマンドへの応答をマスクするかどうかを選択します。

これらの項目をマスクすることによって、クライアントは攻撃を利する可能性のあるサーバー情報の検出を防ぐことができます。

ステップ 6 [Inspections] タブをクリックし、トラフィックの特性に基づいて実装する特定のインスペクションを定義します。

FTP クラス マップに基づいて、またはインスペクション マップで一致を直接設定することによって、またはその両方で、トラフィックの一致基準を定義できます。

a) 次のいずれかを実行します。

- [Add] をクリックして、新しい基準を追加します。
- 既存の基準を選択し、[Edit] をクリックします。

b) [Single Match] を選択して基準を直接定義するか、または [Multiple Match] を選択して基準を定義する FTP クラス マップを選択します。

c) 基準をここで定義した場合は、基準の一致タイプとして [Match]（トラフィックは基準と一致する必要がある）または [No Match]（トラフィックは基準と異なる必要がある）を選択します。たとえば、文字列「example.com」で [No Match] を選択した場合、「example.com」を含むトラフィックはすべてクラスマップの対象外になります。次に、基準を以下のように設定します。

- [File Name]：転送されるファイルの名前を、選択した正規表現または正規表現クラスと照合します。

- [File Type]：転送されるファイルの MIME またはメディア タイプを、選択した正規表現または正規表現クラスと照合します。
- [Server]：FTP サーバーの名前を、選択した正規表現または正規表現クラスと照合します。
- [User]：ログイン ユーザーの名前を、選択した正規表現または正規表現クラスと照合します。
- [Request Command]：パケットで使用される FTP コマンドです。以下の任意の組み合わせです。
  - **APPE**：ファイルに追加します。
  - **CDUP**：現在の作業ディレクトリの親ディレクトリに変更します。
  - **DELE**：サーバーのファイルを削除します。
  - **GET**：サーバーからファイルを取得します。
  - **HELP**：ヘルプ情報を提供します。
  - **MKD**：サーバーにディレクトリを作成します。
  - **PUT**：ファイルをサーバーに送信します。
  - **RMD**：サーバーのディレクトリを削除します。
  - **RNFR**：「変更前の」ファイル名を指定します。
  - **RNTO**：「変更後の」ファイル名を指定します。
  - **SITE**：サーバー固有のコマンドの指定に使用されます。通常、これはリモート管理に使用されます。
  - **STOU**：一義的なファイル名を使用してファイルを保存します。

d) ロギングをイネーブルまたはディセーブルにするかどうかを選択します。アクションは常に接続をリセットします。パケットをドロップして接続を閉じ、サーバーまたはクライアントに TCP リセットを送信します。

e) [OK] をクリックして、インスペクションを追加します。必要に応じてプロセスを繰り返します。

ステップ 7 [FTP Inspect Map] ダイアログ ボックスの [OK] をクリックします。

FTP インスペクション サービス ポリシーでインスペクション マップを使用できるようになります。

次のタスク

マップを使用するためのインスペクション ポリシーを設定できるようになりました。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 を参照してください。

HTTP インスペクション

HTTP インスペクションはデフォルトのインスペクション ポリシーではイネーブルにされないため、このインスペクションが必要な場合はイネーブルにする必要があります。ただし、デフォルトの inspect クラスにはデフォルトの HTTP ポートが含まれているので、デフォルトのグローバル インスペクション ポリシーを編集するだけで HTTP インスペクションを追加できます。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。

ここでは、HTTP インスペクション エンジンについて説明します。

HTTP インスペクションの概要

HTTP インスペクション エンジンを使用して、HTTP トラフィックに関係する特定の攻撃やその他の脅威から保護します。

HTTP アプリケーション インスペクションで HTTP のヘッダーと本文をスキャンし、さまざまなデータ チェックができます。これらのチェックで、HTTP 構築、コンテンツ タイプ、トンネル プロトコル、メッセージ プロトコルなどがセキュリティ アプライアンスを通過することを防止します。

拡張 HTTP インスペクション機能はアプリケーション ファイアウォールとも呼ばれ、HTTP インスペクション ポリシーマップを設定するときに使用できます。これによって、攻撃者がネットワーク セキュリティ ポリシーに従わない HTTP メッセージを使用できないようにします。

HTTP アプリケーション インスペクションでトンネル アプリケーションと ASCII 以外の文字を含む HTTP 要求や応答をブロックして、悪意のあるコンテンツが Web サーバに到達することを防ぎます。HTTP 要求や応答ヘッダーのさまざまな要素のサイズ制限、URL のブロッキング、HTTP サーバ ヘッダー タイプのスプーフィングもサポートされています。

拡張 HTTP インスペクションは、すべての HTTP メッセージについて次の点を確認します。

- RFC 2616 への準拠
- RFC で定義された方式だけを使用していること
- 追加の基準への準拠

HTTP インスペクション ポリシー マップの設定

メッセージがパラメータに違反したときのアクションを指定するには、HTTP インスペクション ポリシー マップを作成します。作成したインスペクション ポリシー マップは、HTTP インスペクションをイネーブルにすると適用できます。

オプションとして、HTTP インスペクション クラス マップを作成し、HTTP インスペクションのトラフィック クラスを定義できます。他のオプションとしては、HTTP インスペクション ポリシー マップでトラフィック クラスを直接定義することもできます。クラス マップを作成することとインスペクション マップでトラフィックの照合を直接定義することの違いは、クラス マップでは複雑な照合基準を作成でき、クラス マップを再利用できるという点です。この手順ではインスペクション マップについて説明しますが、クラス マップで使用される一致基準は、[Inspection] タブに関する手順で説明されているものと同じです。**[Configuration]** > **[Firewall]** > **[Objects]** > **[Class Maps]** > **[HTTP]** を選択するか、またはインスペクション マップの設定時に作成することによって、HTTP クラス マップを設定できます。

ヒント　以下で説明する手順に加えて、サービス ポリシーの作成中にインスペクション マップを設定できます。マップの内容は、作成方法に関係なく同じです。

始める前に

一部のトラフィック照合オプションでは、照合のために正規表現を使用します。これらのテクニックの 1 つを使用する場合は、最初に正規表現または正規表現のクラス マップを作成します。

手順

ステップ 1　**[Configuration]** > **[Firewall]** > **[Objects]** > **[Inspect Maps]** > **[HTTP]** を選択します。

ステップ 2　次のいずれかを実行します。

- [Add] をクリックして、新しいマップを追加します。
- 内容を表示するマップを選択します。セキュリティ レベルを直接変更することも、[Customize] をクリックしてマップを編集することもできます。この後の手順では、マップをカスタマイズまたは追加するものとします。

ステップ 3　新しいマップの場合、名前（最大 40 文字）と説明を入力します。マップを編集するときは、変更できるのは説明のみです。

ステップ 4　[HTTP Inspect Map] ダイアログ ボックスの [Security Level] ビューで、必要なコンフィギュレーションと最もよく一致するレベルを選択します。デフォルトのレベルは [Low] です。

プリセット レベルのいずれかが要件と一致する場合、以上で終了です。[OK] をクリックし、残りの手順をスキップして、HTTP インスペクションのサービス ポリシー ルールでマップを使用します。

設定をさらにカスタマイズする必要がある場合は、[Details] をクリックし、手順を続けます。

ヒント [URI Filtering] ボタンは要求 URI のインスペクションを設定するためのショートカットです。これについては後で説明します。

ステップ 5 [Parameters] タブをクリックし、必要なオプションを設定します。

- [Body Match Maximum] ：HTTP メッセージの本文照合時に検索される、最大文字数です。デフォルトは 200 バイトです。大きな値を指定すると、パフォーマンスに大きな影響を与えます。
- [Check for protocol violations]： パケットが HTTP プロトコルに準拠しているかどうかを確認します。違反している場合、接続のドロップ、リセット、またはログへの記録を行うことができます。ドロップまたはリセットする場合は、ロギングをイネーブルにすることもできます。
- [Spoof server string]：サーバー HTTP ヘッダーの値を指定した文字列に置き換えます。最大 82 文字です。

ステップ 6 [Inspections] タブをクリックし、トラフィックの特性に基づいて実装する特定のインスペクションを定義します。

HTTP クラスマップに基づいて、またはインスペクションマップで一致を直接設定することによって、またはその両方で、トラフィックの一致基準を定義できます。

a) 次のいずれかを実行します。
   - [Add] をクリックして、新しい基準を追加します。
   - 既存の基準を選択し、[Edit] をクリックします。

b) [Single Match] を選択して基準を直接定義するか、または [Multiple Match] を選択して基準を定義する HTTP クラス マップを選択します。

c) 基準をここで定義した場合は、基準の一致タイプとして [Match] （トラフィックは基準と一致する必要がある）または [No Match] （トラフィックは基準と異なる必要がある）を選択します。たとえば、文字列「example.com」で [No Match] を選択した場合、「example.com」を含むトラフィックはすべてクラスマップの対象外になります。次に、基準を以下のように設定します。
   - [Request/Response Content Type Mismatch]：応答のコンテンツ タイプが要求の accept フィールドの MIME タイプの 1 つと一致しないパケットを照合します。
   - [Request Arguments]：要求の引数を、選択した正規表現または正規表現クラスと照合します。
   - [Request Body Length]：要求の本文が指定したバイト数より大きいパケットを照合します。
   - [Request Body]：要求の本文を、選択した正規表現または正規表現クラスと照合します。

- [Request Header Field Count]：要求のヘッダー フィールドの数が指定した数より多いパケットを照合します。フィールドのヘッダータイプを正規表現または定義済みのタイプと照合できます。定義済みのタイプは次のとおりです。accept、accept-charset、accept-encoding、accept-language、allow、authorization、cache-control、connection、content-encoding、content-language、content-length、content-location、content-md5、content-range、content-type、cookie、date、expect、expires、from、host、if-match、if-modified-since、if-none-match、if-range、if-unmodified-since、last-modified、max-forwards、pragma、proxy-authorization、range、referer、te、trailer、transfer-encoding、upgrade、user-agent、via、warning。
- [Request Header Field Length]：要求のヘッダー フィールドの長さが指定したバイト数より大きいパケットを照合します。フィールドのヘッダータイプを正規表現または定義済みのタイプと照合できます。定義済みのタイプは、上の [Request Header Field Count] に対する一覧と同じです。
- [Request Header Field]：要求の選択したヘッダー フィールドの内容を、選択した正規表現または正規表現クラスと照合します。事前定義されたヘッダータイプを指定するか、または正規表現を使用してヘッダーを選択できます。
- [Request Header Count]：要求のヘッダーの数が指定した数より多いパケットを照合します。
- [Request Header Length]：要求のヘッダーの長さが指定したバイト数より大きいパケットを照合します。
- [Request Header Non-ASCII]：要求のヘッダーに ASCII 以外の文字が含まれるパケットを照合します。
- [Request Method]：要求メソッドが定義済みのタイプまたは選択した正規表現もしくは正規表現クラスと一致するパケットを照合します。定義済みのタイプは次のとおりです。bcopy、bdelete、bmove、bpropfind、bproppatch、connect、copy、delete、edit、get、getattribute、getattributenames、getproperties、head、index、lock、mkcol、mkdir、move、notify、options、poll、post、propfind、proppatch、put、revadd、revlabel、revlog、revnum、save、search、setattribute、startrev、stoprev、subscribe、trace、unedit、unlock、unsubscribe。
- [Request URI Length]：要求の URI の長さが指定したバイト数より大きいパケットを照合します。
- [Request URI]：要求の URI の内容を、選択した正規表現または正規表現クラスと照合します。
- [Request Body]：要求の本文を、選択した正規表現または正規表現クラスあるいは ActiveX または Java アプレットの内容と照合します。
- [Response Body Length]：応答の本文の長さが指定したバイト数より大きいパケットを照合します。
- [Response Header Field Count]：応答のヘッダー フィールドの数が指定した数より多いパケットを照合します。フィールドのヘッダータイプを正規表現または定義済みのタ

イプと照合できます。定義済みのタイプは次のとおりです。accept-ranges、age、allow、cache-control、connection、content-encoding、content-language、content-length、content-location、content-md5、content-range、content-type、date、etag、expires、last-modified、location、pragma、proxy-authenticate、retry-after、server、set-cookie、trailer、transfer-encoding、upgrade、vary、via、warning、www-authenticate。

- [Response Header Field Length]：応答のヘッダー フィールドの長さが指定したバイト数より大きいパケットを照合します。フィールドのヘッダータイプを正規表現または定義済みのタイプと照合できます。定義済みのタイプは、上の [Response Header Field Count] に対する一覧と同じです。
- [Response Header Field]：応答の選択したヘッダー フィールドの内容を、選択した正規表現または正規表現クラスと照合します。事前定義されたヘッダータイプを指定するか、または正規表現を使用してヘッダーを選択できます。
- [Response Header Count]：応答のヘッダーの数が指定した数より多いパケットを照合します。
- [Response Header Length]：応答のヘッダーの長さが指定したバイト数より大きいパケットを照合します。
- [Response Header Non-ASCII]：応答のヘッダーに ASCII 以外の文字が含まれるパケットを照合します。
- [Response Status Line]：応答のステータス行の内容を、選択した正規表現または正規表現クラスと照合します。

d) 接続のドロップ、リセット、またはログへの記録を行うかどうか選択します。接続のドロップまたはリセットの場合は、ロギングをイネーブルまたはディセーブルにできます。

e) [OK] をクリックして、インスペクションを追加します。必要に応じてプロセスを繰り返します。

ステップ 7 [HTTP Inspect Map] ダイアログ ボックスの [OK] をクリックします。

HTTP インスペクション サービス ポリシーでインスペクション マップを使用できるようになります。

次のタスク

マップを使用するためのインスペクション ポリシーを設定できるようになりました。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 を参照してください。

ICMP インスペクション

ICMP インスペクション エンジンを使用すると、ICMP トラフィックが「セッション」を持つようになるため、TCP トラフィックや UDP トラフィックのように検査することが可能になり

ます。ICMP インスペクション エンジンを使用しない場合は、ACL で ICMP が ASA を通過するのを禁止することを推奨します。ステートフル インスペクションを実行しないと、ICMP がネットワーク攻撃に利用される可能性があります。ICMP インスペクション エンジンは、要求ごとに応答が 1 つだけであること、シーケンス番号が正しいことを確認します。

ただし、ASA 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。

（注） NAT は、ICMP インスペクションを無効にしても、パケットを変換するときに ICMP インスペクションを使用します。

ICMP インスペクションをイネーブルにする方法については、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を参照してください。

ICMP エラー インスペクション

ICMP エラー インスペクションをイネーブルにすると、ASA は NAT の設定に基づいて、ICMP エラー メッセージを送信する中間ホップ用の変換セッションを作成します。ASA は、変換後の IP アドレスでパケットを上書きします。

ディセーブルの場合、ASA は、ICMP エラー メッセージを生成する中間ノード用の変換セッションを作成しません。内部ホストと ASA の間にある中間ノードによって生成された ICMP エラー メッセージは、NAT リソースをそれ以上消費することなく、外部ホストに到達します。外部ホストが traceroute コマンドを使用して ASA の内部にある宛先までのホップをトレースする場合、これは適切ではありません。ASA が中間ホップを変換しない場合、すべての中間ホップは、マッピングされた宛先 IP アドレスとともに表示されます。

（注） NAT が ICMP パケットで使用される可能性がある場合は、常に ICMP エラー インスペクションを有効にする必要があります。NAT は、ICMP インスペクションを無効にしていても ICMP パケットに対して ICMP インスペクションを自動的に実行するため、マッピングされた宛先アドレスを送信元アドレスとして使用すると、スキャナーがネットワークを検査しているように見える可能性があります。たとえば、ICMP エラー インスペクションも有効になっていない場合、ICMP タイム超過応答に埋め込まれたエコー要求パケットの宛先が変換されると、タイム超過要求の外部ヘッダーでは、変換された宛先が送信元アドレスとして使用されます。ICMP エラー インスペクションを有効にすると、タイム超過になった送信元アドレスに正しい値が設定されます。

ICMP エラー インスペクションをイネーブルにする方法については、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を参照してください。

ILS インスペクション

Internet Locator Service（ILS）インスペクション エンジンは、LDAP を使用してディレクトリ情報を ILS サーバーと交換する Microsoft NetMeeting、SiteServer、および Active Directory の各製品に対して NAT をサポートします。LDAP データベースには IP アドレスだけが保存されるため、ILS インスペクションで PAT は使用できません。

LDAP サーバーが外部にある場合、内部ピアが外部 LDAP サーバーに登録された状態でローカルに通信できるように、検索応答に対して NAT を使用することを検討してください。NAT を使用する必要がなければ、パフォーマンスを向上させるためにインスペクション エンジンをオフにすることを推奨します。

ILS サーバーが ASA 境界の内部にある場合は、さらに設定が必要なことがあります。この場合、外部クライアントが指定されたポート（通常は TCP 389）の LDAP サーバーにアクセスするためのホールが必要となります。

（注） ILS トラフィック（H225 コール シグナリング）はセカンダリ UDP チャネルだけで発生するため、TCP 接続は TCP 非アクティブ間隔の後に切断されます。デフォルトでは、この間隔は 60 分です。この値は、TCP timeout コマンドを使用して調整できます。ASDM では、これは [Configuration] > [Firewall] > [Advanced] > [Global Timeouts] ペインにあります。

ILS インスペクションには、次の制限事項があります。

- 照会要求や応答はサポートされません。
- 複数のディレクトリのユーザーは統合されません。
- 複数のディレクトリに複数の ID を持っている単一のユーザーは NAT には認識されません。

ILSインスペクションをイネーブルにする方法については、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を参照してください。

インスタント メッセージ インスペクション

インスタントメッセージ（IM）インスペクションエンジンを使用すると、IMのネットワーク使用を制御し、機密情報の漏洩、ワームの送信、および企業ネットワークへのその他の脅威を停止できます。

IM インスペクションはデフォルトのインスペクション ポリシーではイネーブルにされないため、このインスペクションが必要な場合はイネーブルにする必要があります。ただし、デフォルトの inspect クラスにはデフォルトの IM ポートが含まれているので、デフォルトのグローバル インスペクション ポリシーを編集するだけで IM インスペクションを追加できます。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。

IM インスペクションを実装する場合は、メッセージがパラメータに違反した場合のアクションを指定する IM インスペクション ポリシー マップを設定することもできます。次の手順では、IM インスペクション ポリシー マップについて説明します。

オプションとして、IM インスペクション クラス マップを作成し、IM インスペクションのトラフィック クラスを定義できます。他のオプションとしては、IM インスペクション ポリシー マップでトラフィック クラスを直接定義することもできます。クラス マップを作成することとインスペクション マップでトラフィックの照合を直接定義することの違いは、クラス マップでは複雑な照合基準を作成でき、クラスマップを再利用できるという点です。この手順ではインスペクションマップについて説明しますが、トラフィック照合のアクションを指定しないことを除き、クラス マップは基本的に同じです。[Configuration] > [Firewall] > [Objects] > [Class Maps] > [Instant Messaging (IM)] の順に選択することによって、IM クラス マップを設定できます。

ヒント 以下で説明する手順に加えて、サービス ポリシーの作成中にインスペクション マップを設定できます。マップの内容は、作成方法に関係なく同じです。

始める前に

一部のトラフィック照合オプションでは、照合のために正規表現を使用します。これらのテクニックの 1 つを使用する場合は、最初に正規表現または正規表現のクラス マップを作成します。

手順

ステップ 1 **[Configuration]** > **[Firewall]** > **[Objects]** > **[Inspect Maps]** > **[Instant Messaging (IM)]** の順に選択します。

ステップ 2 次のいずれかを実行します。

- [Add] をクリックして、新しいマップを追加します。
- マップを選択して [Edit] をクリックします。

ステップ 3 新しいマップの場合、名前（最大 40 文字）と説明を入力します。マップを編集するときは、変更できるのは説明のみです。

ステップ 4 トラフィックの特性に基づいて実装する特定のインスペクションを定義します。

IM クラス マップに基づいて、またはインスペクション マップで一致を直接設定することによって、またはその両方で、トラフィックの一致基準を定義できます。

a) 次のいずれかを実行します。

- [Add] をクリックして、新しい基準を追加します。
- 既存の基準を選択し、[Edit] をクリックします。

b) [Single Match] を選択して基準を直接定義するか、または [Multiple Match] を選択して基準を定義する IM クラス マップを選択します。[Manage] をクリックして、新しいクラス マップを作成します。

c) 基準をここで定義した場合は、基準の一致タイプとして [Match]（トラフィックは基準と一致する必要がある）または [No Match]（トラフィックは基準と異なる必要がある）を選択します。たとえば、文字列「example.com」で [No Match] を選択した場合、「example.com」を含むトラフィックはすべてクラス マップの対象外になります。次に、基準を設定します。

- [Protocol]：特定の IM プロトコル（Yahoo Messenger や MSN Messenger など）のトラフィックを照合します。
- [Service]：特定の IM サービス（チャット、ファイル転送、Web カメラ、音声チャット、会議、ゲームなど）を照合します。
- [Version]：IM メッセージのバージョンを、選択した正規表現または正規表現クラスと照合します。
- [Client Login Name]：選択した正規表現または正規表現クラスと IM メッセージの送信元クライアントのログイン名を照合します。
- [Client Peer Login Name]：選択した正規表現または正規表現クラスと IM メッセージの宛先ピアのログイン名を照合します。
- [Source IP Address]：送信元の IP アドレスおよびマスクを照合します。
- [Destination IP Address]：宛先の IP アドレスおよびマスクを照合します。
- [Filename]：IM メッセージのファイル名を、選択した正規表現または正規表現クラスと照合します。

d) 接続のドロップ、リセット、またはログへの記録を行うかどうか選択します。接続のドロップまたはリセットの場合は、ロギングをイネーブルまたはディセーブルにできます。

e) [OK] をクリックして、インスペクションを追加します。必要に応じてプロセスを繰り返します。

ステップ 5 [IM Inspect Map] ダイアログ ボックスの [OK] をクリックします。

IM インスペクション サービス ポリシーでインスペクション マップを使用できるようになります。

次のタスク

マップを使用するためのインスペクション ポリシーを設定できるようになりました。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 を参照してください。

IP オプション インスペクション

IP オプション インスペクションを設定して、パケット ヘッダーの [IP Options] フィールドのコンテンツに基づいてどの IP パケットを許可するかについて制御できます。望ましくないオプションがあるパケットをドロップしたり、オプションをクリア（してパケットを許可）したり、変更なしでパケットを許可したりできます。

IP オプションで提供される制御機能は、一部の状況では必須ですが、ほとんどの一般的な状況では不要です。具体的には、IP オプションにはタイムスタンプ、セキュリティ、および特殊なルーティングの規定が含まれています。IP オプションの使用は任意であり、このフィールドにはオプションを 0 個、1 個、またはそれ以上含めることができます。

IP オプションおよび関連する RFC の参照のリストについては、IANA のページ（http://www.iana.org/assignments/ip-parameters/ip-parameters.xhtml）を参照してください。

IP オプションのインスペクションはデフォルトで有効になっていますが、RSVP トラフィックに対してのみとなっています。デフォルトのマップが許可しているもの以外に追加のオプションを許可するか、またはデフォルト以外のインスペクション トラフィック クラス マップを使用することによって他のタイプのトラフィックに適用する場合にのみ、これを設定する必要があります。

（注） IP オプション インスペクションは、フラグメント化されたパケットでは動作しません。たとえば、オプションはフラグメントからクリアされません。

次の項では、IP オプション インスペクションについて説明します。

IP オプション インスペクションのデフォルト

IP オプション インスペクションは、_default_ip_options_map インスペクション ポリシー マップを使用して、RSVP トラフィックのデフォルトのみで有効になります。

- Router Alert オプションは許可されます。

  このオプションは、中継ルータに対し、パケットの宛先がそのルータでない場合でも、パケットのコンテンツを検査するよう通知します。このインスペクションは、RSVP を実装している場合に役に立ちます。同様のプロトコルは、パケットの配信パス上にあるルータでの比較的複雑な処理を必要とします。Router Alert オプションが含まれた RSVP パケットをドロップすると、VoIP の実装で問題が生じることがあります。

- その他のオプションを含むパケットはドロップされます。

  インスペクションによってパケットがドロップされるたびに、syslog 106012 が発行されます。メッセージではドロップの原因になったオプションが示されます。show service-policy inspect ip-options コマンドを使用して、各オプションの統計情報を表示します。

IP オプション インスペクション ポリシー マップの設定

デフォルト以外の IP オプション インスペクションを実行する場合は、IP オプション インスペクション ポリシー マップを作成して、各オプション タイプの処理方法を指定します。

ヒント　以下で説明する手順に加えて、サービス ポリシーの作成中にインスペクション マップを設定できます。マップの内容は、作成方法に関係なく同じです。

手順

ステップ 1　**[Configuration]** > **[Firewall]** > **[Objects]** > **[Inspect Maps]** > **[IP Options]** を選択します。

ステップ 2　次のいずれかを実行します。

- [Add] をクリックして、新しいマップを追加します。
- マップを選択して [Edit] をクリックします。

ステップ 3　新しいマップの場合、名前（最大 40 文字）と説明を入力します。マップを編集するときは、変更できるのは説明のみです。

ステップ 4　許可するオプションを [Drop] リストから [Allow] リストに移動して選択します。

次のヒントを考慮してください。

- 「デフォルト」オプションでは、マップに含まれていないオプションのデフォルトの動作が設定されます。これを [Allowed] リストに移動した場合は、[Drop] リストに表示されているオプションも許可されます。
- 許可するオプションでは、[Clear] ボックスをオンにすることで、パケットを送信する前にパケット ヘッダーからオプションを削除できます。
- 一部のオプションは、オプション タイプ番号別にリストされます。番号は全オプション タイプのオクテット（コピー、クラス、およびオプション番号）で、オクテットのオプションの番号部分だけではありません。これらのオプション タイプは、実際のオプションに表示されない可能性があります。非標準オプションは、インターネット プロトコル RFC 791、http://tools.ietf.org/html/rfc791 で定義された予測されるタイプ/長さ/値の形式である必要があります。
- パケットに複数のオプション タイプが含まれている場合、それらのタイプのいずれかに対するアクションがパケットをドロップすることであれば、そのパケットはドロップされます。

IP オプションおよび関連する RFC の参照のリストについては、IANA のページ（http://www.iana.org/assignments/ip-parameters/ip-parameters.xhtml）を参照してください。

ステップ 5　[OK] をクリックします。

IP オプション インスペクション サービス ポリシーでインスペクション マップを使用できるようになります。

次のタスク

マップを使用するためのインスペクション ポリシーを設定できるようになりました。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 を参照してください。

IPsec パススルー インスペクション

IPsec パススルー インスペクションはデフォルトのインスペクション ポリシーではイネーブルにされないため、このインスペクションが必要な場合はイネーブルにする必要があります。ただし、デフォルトの inspect クラスにはデフォルトの IPsec ポートが含まれているので、デフォルトのグローバル インスペクション ポリシーを編集するだけで IPsec インスペクションを追加できます。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。

ここでは、IPsec パススルー インスペクション エンジンについて説明します。

IPsec パス スルー インスペクションの概要

Internet Protocol Security（IPsec）は、データ ストリームの各 IP パケットを認証および暗号化することによって、IP 通信をセキュリティで保護するためのプロトコル スイートです。IPsec には、セッションの開始時、およびセッション中に使用される暗号キーのネゴシエーションの開始時に、エージェント間の相互認証を確立するためのプロトコルも含まれています。IPsec を使用して、ホスト（コンピュータ ユーザーまたはサーバーなど）のペア間、セキュリティ ゲートウェイ（ルータやファイアウォールなど）のペア間、またはセキュリティ ゲートウェイとホスト間のデータ フローを保護できます。

IPsec パススルー アプリケーション インスペクションは、IKE UDP ポート 500 接続に関連付けられた ESP（IP プロトコル 50）および AH（IP プロトコル 51）トラフィックを簡単に横断できます。このインスペクションは、冗長な ACL コンフィギュレーションを回避して ESP および AH トラフィックを許可し、タイムアウトと最大接続数を使用してセキュリティも確保します。

ESP または AH トラフィックの制限を指定するには、IPsec パススルーのポリシー マップを設定します。クライアントあたりの最大接続数と、アイドル タイムアウトを設定できます。

NAT および非 NAT トラフィックは許可されます。ただし、PAT はサポートされません。

IPsec パススルー インスペクション ポリシー マップの設定

IPsec パススルー マップでは、IPsec パススルー アプリケーション インスペクションのデフォルト設定値を変更できます。IPsec パススルー マップを使用すると、アクセス リストを使用しなくても、特定のフローを許可できます。

コンフィギュレーションに含まれるデフォルト マップ _default_ipsec_passthru_map では、ESP 接続に対するクライアントごとの最大数は制限なしに設定され、ESP アイドル タイムアウトは 10 分に設定されます。異なる値が必要な場合、または AH 値を設定する必要がある場合にのみ、インスペクション ポリシー マップを設定する必要があります。

ヒント 以下で説明する手順に加えて、サービス ポリシーの作成中にインスペクション マップを設定できます。マップの内容は、作成方法に関係なく同じです。

手順

ステップ 1 **[Configuration]** > **[Firewall]** > **[Objects]** > **[Inspect Maps]** > **[IPsec Pass Through]** を選択します。

ステップ 2 次のいずれかを実行します。

- [Add] をクリックして、新しいマップを追加します。
- 内容を表示するマップを選択します。セキュリティ レベルを直接変更することも、[Customize] をクリックしてマップを編集することもできます。この後の手順では、マップをカスタマイズまたは追加するものとします。

ステップ 3 新しいマップの場合、名前（最大 40 文字）と説明を入力します。マップを編集するときは、変更できるのは説明のみです。

ステップ 4 [IPsec Pass Through Inspect Map] ダイアログ ボックスの [Security Level] ビューで、必要なコンフィギュレーションと最もよく一致するレベルを選択します。

プリセット レベルのいずれかが要件と一致する場合、以上で終了です。[OK] をクリックし、残りの手順をスキップして、IPsec パススルー インスペクションのサービス ポリシー ルールでマップを使用します。

設定をさらにカスタマイズする必要がある場合は、[Details] をクリックし、手順を続けます。

ステップ 5 ESP および AH トンネルを許可するかどうかを選択します。

プロトコルごとに、各クライアントに許可される最大接続数およびアイドル タイムアウトも設定できます。

ステップ 6 [OK] をクリックします。

IPsec パススルー オプション インスペクション サービス ポリシーでインスペクション マップを使用できるようになります。

IPv6 インスペクション

IPv6 インスペクションを使用すると、拡張ヘッダーに基づいて IPv6 トラフィックを選択的にログに記録したりドロップしたりできます。さらに、IPv6 インスペクションでは、IPv6 パケット内の拡張ヘッダーのタイプと順序が RFC 2460 に準拠しているかどうかも確認できます。

IPv6 インスペクションはデフォルトのインスペクション ポリシーではイネーブルにされないため、このインスペクションが必要な場合はイネーブルにする必要があります。デフォルトのグローバル インスペクション ポリシーを編集して IPv6 インスペクションを追加できます。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。

IPv6 インスペクションのデフォルト

IPv6 インスペクションをイネーブルにし、インスペクション ポリシー マップを指定しないと、デフォルトの IPv6 インスペクション ポリシー マップが使用され、次のアクションが実行されます。

- 既知の IPv6 拡張ヘッダーのみを許可します。準拠しないパケットはドロップされ、ログに記録されます。
- RFC 2460 仕様で定義されている IPv6 拡張ヘッダーの順序を適用します。準拠しないパケットはドロップされ、ログに記録されます。
- ルーティング タイプ ヘッダーを含むパケットをドロップします。

IPv6 インスペクション ポリシー マップの設定

ドロップまたはロギングする拡張ヘッダーを指定するには、またはパケットの検証をディセーブルにするには、サービス ポリシーで使用される IPv6 インスペクション ポリシー マップを作成します。

手順

ステップ 1 **[Configuration]** > **[Firewall]** > **[Objects]** > **[Inspect Maps]** > **[IPv6]** を選択します。

ステップ 2 次のいずれかを実行します。

- [Add] をクリックして、新しいマップを追加します。

- マップを選択して [Edit] をクリックします。

ステップ 3 新しいマップの場合、名前（最大 40 文字）と説明を入力します。マップを編集するときは、変更できるのは説明のみです。

ステップ 4 [Enforcement] タブをクリックし、既知の IPv6 拡張ヘッダーだけを許可するかどうか、または RFC 2460 で定義されている IPv6 拡張ヘッダーの順序を適用するかどうかを選択します。準拠しないパケットはドロップされ、ログに記録されます。

ステップ 5 （任意）[Header Matches] タブをクリックし、IPv6 メッセージのヘッダーに基づいてドロップまたはログに記録するトラフィックを指定します。

a) 次のいずれかを実行します。

- [Add] をクリックして、新しい基準を追加します。
- 既存の基準を選択し、[Edit] をクリックします。

b) 一致する IPv6 拡張ヘッダーを選択します。

- 認証（AH）認証ヘッダー。
- 宛先オプション ヘッダー。
- カプセル化セキュリティ ペイロード（ESP）ヘッダー。
- フラグメント ヘッダー。
- ホップバイホップ オプション ヘッダー。
- [Routing header]：1 つのヘッダー タイプ番号または番号の範囲を指定します。
- [Header Count]：パケットをドロップまたはログに記録しないで許可する拡張ヘッダーの最大数を指定します。
- [Routing header address count]：パケットをドロップまたはログに記録しないで許可するタイプ 0 ルーティング ヘッダー内のアドレスの最大数を指定します。

c) パケットをドロップするか、ログに記録するかを選択します。パケットをドロップする場合は、ロギングをイネーブルにすることもできます。

d) [OK] をクリックして、インスペクションを追加します。必要に応じてプロセスを繰り返します。

ステップ 6 [IPv6 Inspect Map] ダイアログ ボックスの [OK] をクリックします。

IPv6 インスペクション サービス ポリシーでインスペクション マップを使用できるようになります。

次のタスク

マップを使用するためのインスペクション ポリシーを設定できるようになりました。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 を参照してください。

NetBIOS インスペクション

NetBIOS アプリケーション インスペクションでは、NetBIOS ネーム サービス（NBNS）パケットおよび NetBIOS データグラム サービス パケットに埋め込まれている IP アドレスで NAT を実行します。また、プロトコル準拠チェックを行って、さまざまなフィールドの数や長さの整合性を確認します。

NETBIOSインスペクションはデフォルトでイネーブルになっています。必要に応じて、NetBIOS プロトコル違反をドロップまたはログに記録するポリシー マップを作成できます。次の手順で、NetBIOS インスペクション ポリシー マップを設定する方法について説明します。

手順

ステップ 1 **[Configuration]** > **[Firewall]** > **[Objects]** > **[Inspect Maps]** > **[NetBIOS]** を選択します。

ステップ 2 次のいずれかを実行します。

- [Add] をクリックして、新しいマップを追加します。
- マップを選択して [Edit] をクリックします。

ステップ 3 新しいマップの場合、名前（最大 40 文字）と説明を入力します。マップを編集するときは、変更できるのは説明のみです。

ステップ 4 [Check for Protocol Violations] を選択します。このオプションを選択しない場合、マップを作成する理由はありません。

ステップ 5 実行するアクションは、パケットのドロップまたはログ記録から選択します。パケットをドロップする場合は、ロギングをイネーブルにすることもできます。

ステップ 6 [OK] をクリックします。

NetBIOS インスペクション サービス ポリシーでインスペクション マップを使用できるようになります。

次のタスク

マップを使用するためのインスペクション ポリシーを設定できるようになりました。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 を参照してください。

PPTP インスペクション

PPTP は、PPP トラフィックのトンネリングに使用されるプロトコルです。PPTP セッションは、1 つの TCP チャネルと通常 2 つの PPTP GRE トンネルで構成されます。TCP チャネルは、

PPTP GRE トンネルのネゴシエートと管理に使用される制御チャネルです。GRE トンネルは、2 つのホスト間の PPP セッションを伝送します。

PPTP アプリケーション インスペクションは、イネーブルになると、PPTP プロトコル パケットを検査し、PPTP トラフィックを許可するために必要な GRE 接続と xlate をダイナミックに作成します。

具体的には、ASA は、PPTP のバージョン通知と発信コールの要求/応答シーケンスを検査します。RFC 2637 で定義されている PPTP バージョン 1 だけが検査されます。どちらかの側から通知されたバージョンがバージョン 1 でない場合、TCP 制御チャネルでのそれ以降のインスペクションはディセーブルになります。また、発信コールの要求と応答のシーケンスは追跡されます。接続および xlate は、以降のセカンダリ GRE データ トラフィックを許可するために、必要に応じて、ダイナミックに割り当てられます。

PPTP インスペクション エンジンは、PPTP トラフィックを PAT で変換できるように、イネーブルにする必要があります。また、PAT は、PPTP TCP 制御チャネルで修正バージョンの GRE（RFC 2637）がネゴシエートされた場合に限り、その GRE に対してだけ実行されます。PAT は、未修正バージョンの GRE（RFC 1701、RFC 1702）には実行されません。

PPTP インスペクションをイネーブルにする方法については、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を参照してください。

RSH インスペクション

RSH インスペクションはデフォルトでイネーブルになっています。RSH プロトコルは、TCP ポート 514 で RSH クライアントから RSH サーバーへの TCP 接続を使用します。クライアントとサーバーは、クライアントが STDERR 出力ストリームを受信する TCP ポート番号をネゴシエートします。RSH インスペクションは、必要に応じて、ネゴシエートされたポート番号の NAT をサポートします。

RSH インスペクションのイネーブル化の詳細については、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を参照してください。

SMTP および拡張 SMTP インスペクション

ESMTP インスペクションでは、スパム、フィッシング、不正形式メッセージ攻撃、バッファオーバーフロー/アンダーフロー攻撃などの攻撃を検出します。また、アプリケーションセキュリティとプロトコル準拠により、正常な ESMTP メッセージだけを通し、送受信者およびメール中継のブロックも行います。

ESMTP インスペクションはデフォルトでイネーブルになっています。デフォルト インスペクション マップとは異なる処理が必要な場合にのみ、設定する必要があります。

ここでは、ESMTP インスペクション エンジンについて説明します。

SMTP および ESMTP インスペクションの概要

拡張 SMTP（ESMTP）アプリケーション インスペクションを使用すると、ASA を通過できる SMTP コマンドの種類を制限し、モニター機能を追加することによって、SMTP ベースの攻撃からより強固に保護できます。ESMTP は SMTP プロトコルの拡張で、ほとんどの観点で SMTP に似ています。

ESMTP アプリケーション インスペクションは、ユーザーが使用できるコマンドとサーバーが返送するメッセージを制御し、その数を減らします。ESMTP インスペクションは、次の 3 つの主要なタスクを実行します。

- SMTP 要求を 7 つの基本 SMTP コマンドと 8 つの拡張コマンドに制限します。サポートされるコマンドは次のとおりです。
  - 拡張 SMTP：AUTH、EHLO、ETRN、HELP、SAML、SEND、SOML、STARTTLS、および VRFY。
  - SMTP（RFC 821）：DATA、HELO、MAIL、NOOP、QUIT、RCPT、RSET。
- SMTP コマンド応答シーケンスをモニターします。
- 監査証跡の生成：メールアドレス内に埋め込まれている無効な文字が置き換えられたときに、監査レコード 108002 を生成します。詳細については、RFC 821 を参照してください。

ESMTP インスペクションでは、次の異常なシグニチャがないかどうか、コマンドと応答のシーケンスをモニターします。

- 切り捨てられたコマンド
- 不正なコマンド終端（<CR><LR> で終了していない）
- MAIL コマンドと RCPT コマンドでは、メールの送信者と受信者が指定されます。異常な文字がないか、メール アドレスがスキャンされます。縦棒（|）は削除され（ブランクに変更されます）、「<」および「>」はメール アドレスを定義する場合にのみ許可されます（「>」より前に「<」がある必要があります）。
- SMTP サーバーによる不意の移行
- 未知またはサポート対象外のコマンドに対し、インスペクション エンジンは、パケット内のすべての文字を X に変更し、それらは内部サーバーによって拒否されます。この結果は、「500 Command unknown: 'XXX'」のようなメッセージで表示されます。不完全なコマンドは、破棄されます。

  サポート対象外の ESMTP コマンドは ATRN、ONEX、VERB、CHUNKING で、プライベート拡張子です。
- TCP ストリーム編集
- コマンド パイプライン

（注） ESMTPインスペクションをイネーブルにする場合、次のルールに従わないと、対話型のSMTPに使用する Telnet セッションが停止することがあります。SMTP コマンドの長さは 4 文字以上にする必要があります。復帰と改行で終了する必要があります。次の応答を発行する前に現在の応答を待機する必要があります。

ESMTP インスペクションのデフォルト

ESMTP インスペクションは、_default_esmtp_map インスペクション ポリシー マップを使用して、デフォルトで有効になります。

- サーバー バナーはマスクされます。ESMTP インスペクション エンジンは、文字「2」、「0」、「0」を除くサーバーの SMTP バナーの文字をアスタリスクに変更します。復帰（CR）、および改行（LF）は無視されます。
- 暗号化接続が可能ですが、検査されません。
- 送信側と受信側のアドレスの特殊文字は認識されず、アクションは実行されません。
- コマンド行の長さが 512 より大きい接続は、ドロップされてログに記録されます。
- 受信者が 100 より多い接続は、ドロップされてログに記録されます。
- 本文の長さが 998 バイトより大きいメッセージはログに記録されます。
- ヘッダー行の長さが 998 より大きい接続は、ドロップされてログに記録されます。
- MIME ファイル名が 255 文字より長いメッセージは、ドロップされてログに記録されます。
- 「others」に一致する EHLO 応答パラメータはマスクされます。

ESMTP インスペクション ポリシー マップの設定

メッセージがパラメータに違反したときのアクションを指定するには、ESMTPインスペクション ポリシー マップを作成します。作成したインスペクション ポリシー マップは、ESMTP インスペクションをイネーブルにすると適用できます。

始める前に

一部のトラフィック照合オプションでは、照合のために正規表現を使用します。これらのテクニックの 1 つを使用する場合は、最初に正規表現または正規表現のクラス マップを作成します。

手順

ステップ 1 **[Configuration]** > **[Firewall]** > **[Objects]** > **[Inspect Maps]** > **[ESMTP]** を選択します。

ステップ 2 次のいずれかを実行します。

- [Add] をクリックして、新しいマップを追加します。
- 内容を表示するマップを選択します。セキュリティ レベルを直接変更することも、[Customize] をクリックしてマップを編集することもできます。この後の手順では、マップをカスタマイズまたは追加するものとします。

ステップ 3 新しいマップの場合、名前（最大 40 文字）と説明を入力します。マップを編集するときは、変更できるのは説明のみです。

ステップ 4 [ESMTP Inspect Map] ダイアログ ボックスの [Security Level] ビューで、必要なコンフィギュレーションと最もよく一致するレベルを選択します。

プリセット レベルのいずれかが要件と一致する場合、以上で終了です。[OK] をクリックし、残りの手順をスキップして、ESMTP インスペクションのサービス ポリシー ルールでマップを使用します。

設定をさらにカスタマイズする必要がある場合は、[Details] をクリックし、手順を続けます。

ヒント [MIME File Type Filtering] ボタンはファイル タイプのインスペクションを設定するためのショートカットです。これについては後で説明します。

ステップ 5 [Parameters] タブをクリックし、必要なオプションを設定します。

- [Mask Server Banner] ：ESMTP サーバーからのバナーをマスクするかどうか。
- [Encrypted Packet Inspection] ：インスペクションなしで ESMTP over TLS（暗号化された接続）を許可するかどうか。必要に応じて、暗号化された接続をログに記録できます。デフォルトでは、インスペクションのない TLS セッションを許可します。このオプションの選択を解除すると、システムは暗号化セッション接続試行から STARTTLS インジケータを削除し、強制的にプレーンテキスト接続を行います。

ステップ 6 [Filtering] タブをクリックし、必要なオプションを設定します。

- [Configure mail relay] ：メール中継のドメイン名を指定します。接続をドロップし、必要に応じてログに記録できます。または、ログへの記録だけを行うこともできます。
- [Check for special characters] ：電子メールの送信者または受信者アドレスに特殊文字パイプ（|）、バック クォート、NUL が含まれるメッセージに対して実行するアクションを指定します。接続をドロップし、必要に応じてログに記録できます。または、ログへの記録だけを行うこともできます。

ステップ 7 [Inspections] タブをクリックし、トラフィックの特性に基づいて実装する特定のインスペクションを定義します。

a) 次のいずれかを実行します。

- [Add] をクリックして、新しい基準を追加します。
- 既存の基準を選択し、[Edit] をクリックします。

b) 基準の一致タイプとして、[Match]（トラフィックは基準と一致する必要がある）または [No Match]（トラフィックは基準と異なる必要がある）を選択します。たとえば、文字列「example.com」で [No Match] を選択した場合、「example.com」を含むトラフィックはすべてクラス マップの対象外になります。次に、基準を設定します。

- [Body Length]： ESMTP 本文メッセージの長さが指定したバイト数より大きいメッセージと一致します。
- [Body Line Length] ：ESMTP 本文メッセージの行の長さが指定したバイト数より大きいメッセージと一致します。
- [Commands]：メッセージのコマンド動詞と一致します。 次のコマンドの 1 つまたは複数を指定できます。auth、data、ehlo、etrn、helo、help、mail、noop、quit、rcpt、rset、saml、soml、vrfy。
- [Command Recipient Count]： 受信者の数が指定した値より大きいメッセージと一致します。
- [Command Line Length] ：コマンド動詞の行の長さが指定したバイト数より大きいメッセージと一致します。
- [EHLO Reply Parameters] ：ESMTP EHLO 応答パラメータと一致します。次のパラメータの 1 つまたは複数を指定できます。8bitmime、auth、binaryname、checkpoint、dsn、etrn、others、pipelining、size、vrfy。
- [Header Length] ：ESMTP ヘッダーの長さが指定したバイト数より大きいメッセージと一致します。
- [Header Line Length] ：ESMTP ヘッダーの行の長さが指定したバイト数より大きいメッセージと一致します。
- [Header To: Fields Count] ：ヘッダーの To フィールドの数が指定した値より大きいメッセージと一致します。
- [Invalid Recipients Count] ：無効な受信者の数が指定した値より大きいメッセージと一致します。
- [MIME File Type] ：MIME またはメディア ファイル タイプを、指定した正規表現または正規表現クラスと照合します。
- [MIME Filename Length] ：ファイル名が指定したバイト数より大きいメッセージと一致します。

- [MIME Encoding] ：MIME エンコーディング タイプと一致します。次のタイプの 1 つまたは複数を指定できます。7bit、8bit、base64、binary、others、quoted-printable。
- [Sender Address] ：送信者の電子メール アドレスを、指定した正規表現または正規表現クラスと照合します。
- [Sender Address Length] ：送信者のアドレスが指定したバイト数より大きいメッセージと一致します。

c) 接続のドロップ、リセット、またはログへの記録を行うかどうか選択します。接続のドロップまたはリセットの場合は、ロギングをイネーブルまたはディセーブルにできます。コマンドおよびEHLO応答パラメータの場合、コマンドをマスクすることもできます。コマンドの一致の場合、1 秒間のパケット数制限を適用することもできます。

d) [OK]をクリックして、インスペクションを追加します。必要に応じてプロセスを繰り返します。

ステップ 8 [ESMTP Inspect Map] ダイアログ ボックスの [OK] をクリックします。

ESMTP インスペクション サービス ポリシーでインスペクション マップを使用できるようになります。

次のタスク

マップを使用するためのインスペクション ポリシーを設定できるようになりました。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 を参照してください。

SNMP インスペクション

SNMP アプリケーション インスペクションは、デバイスへのトラフィックとデバイス経由のトラフィックの両方に適用されます。このインスペクションは、ユーザーが特定の SNMP ホストに制限される SNMP v3 を設定する場合に必要です。インスペクションなしの場合、定義された v3 ユーザーは任意の許可されたホストからデバイスをポーリングできます。SNMP インスペクションはデフォルトポートではデフォルトで有効になっているため、デフォルト以外のポートを使用する場合にのみ設定する必要があります。デフォルトポートは UDP/161、162 であり（すべてのデバイスタイプ）、FXOS は UDP/161 でリッスンするため、FXOS も実行するデバイスでは UDP/4161 です。

デフォルトでは、SNMP インスペクションはポーリングを構成されたバージョンに制限します。

（注） FXOS も実行しているデバイスで SNMP を設定する場合、SNMP インスペクションは必須であり、無効にすると再度有効になります。SNMP インスペクションは、ポート UDP/4161 を含むトラフィック クラスマップで有効になります。

必要に応じて、SNMP トラフィックを特定のバージョンの SNMP に制限することもできます。以前のバージョンの SNMP は安全性が低いため、セキュリティ ポリシーを使用して特定の SNMP バージョンを拒否する必要が生じる場合もあります。システムは、SNMP バージョン 1、2、2c、または 3 を拒否できます。許可するバージョンは、以下に説明するように、SNMP マップを作成して制御します。バージョンを制御する必要がない場合は、マップなしで SNMP インスペクションを有効にします。

手順

ステップ 1 **[Configuration]** > **[Firewall]** > **[Objects]** > **[Inspect Maps]** > **[SNMP]** を選択します。

ステップ 2 [Add] をクリックするか、マップを選択し、[Edit] をクリックします。マップの追加時にマップ名を入力します。

ステップ 3 拒否する SNMP のバージョンを選択します。

ステップ 4 [OK] をクリックします。

次のタスク

マップを使用するためのインスペクション ポリシーを設定できるようになりました。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 を参照してください。

SQL*Net インスペクション

SQL*Net インスペクションはデフォルトでイネーブルになっています。インスペクション エンジンは、SQL*Net バージョン 1 および 2 をサポートしていますが、形式は Transparent Network Substrate（TNS）のみです。インスペクションでは、表形式データ ストリーム（TDS）形式をサポートしていません。SQL*Net メッセージは、埋め込まれたアドレスとポートについてスキャンされ、必要に応じて NAT の書き換えが適用されます。

SQL*Net のデフォルトのポート割り当ては 1521 です。これは、Oracle が SQL*Net 用に使用している値ですが、構造化照会言語（SQL）の IANA ポート割り当てとは一致しません。アプリケーションが別のポートを使用する場合は、そのポートを含むトラフィック クラスに SQL*Net インスペクションを適用します。

次の場合は、SQL*Net インスペクションを無効にします。

- SQL 制御 TCP ポート 1521 と同じポートで SQL データ転送が行われます。SQL*Net インスペクションがイネーブルになっていると、セキュリティ アプライアンスはプロキシとして機能し、クライアントのウィンドウ サイズを 65000 から約 16000 に減らすため、データ転送の問題が発生します。
- 高レートの SQL 通信のインスペクションにより、CPU 使用率の許容できないスパイクが発生します。

SQL*Net インスペクションを無効にした後、 **clear conn port 1521** コマンドを使用して、インスペクションなしで接続を再構築できるようにします。

SQL*Net インスペクションをイネーブルにする方法については、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を参照してください。

Sun RPC インスペクション

この項では、Sun RPC アプリケーション インスペクションについて説明します。

Sun RPC インスペクションの概要

Sun RPC プロトコル インスペクションはデフォルトではイネーブルです。Sun RPC サーバー テーブルを管理するだけで、ファイアウォールの通過を許可されているサービスを識別できます。ただし、NFS のピンホール化は、サーバー テーブルの設定がなくても各サーバーで実行されます。

Sun RPC は、NFS および NIS で使用されます。Sun RPC サービスはどのポート上でも実行できます。サーバー上の Sun RPC サービスにアクセスしようとするクライアントは、そのサービスが実行されているポートを知る必要があります。そのためには、予約済みポート 111 でポート マッパー プロセス（通常は rpcbind）に照会します。

クライアントがサービスの Sun RPC プログラム番号を送信すると、ポート マッパー プロセスはサービスのポート番号を応答します。クライアントは、ポート マッパー プロセスによって特定されたポートを指定して、Sun RPC クエリーをサーバーに送信します。サーバーが応答すると、ASA はこのパケットを代行受信し、そのポートで TCP と UDP の両方の初期接続を開きます。

Sun RPC ペイロード情報の NAT または PAT はサポートされていません。

Sun RPC サービスの管理

Sun RPC サービス テーブルを使用して、確立された Sun RPC セッションに基づいて Sun RPC トラフィックを制御します。

手順

ステップ 1 **[Configuration]** > **[Firewall]** > **[Advanced]** > **[SUNRPC Server]** を選択します。

ステップ 2 次のいずれかを実行します。

- [Add] をクリックして新しいサーバーを追加します。
- サーバーを選択して [Edit] をクリックします。

ステップ 3 サービス プロパティを設定します。

- [Interface Name] ：サーバーへのトラフィックが伝送されるインターフェイス。
- [IP Address/Mask] ：Sun RPC サーバーのアドレス。
- [Service ID] ：サーバーのサービス タイプ。サービス タイプ（100003 など）を判定するには、Sun RPC サーバー マシンの UNIX または Linux コマンドラインで、sunrpcinfo コマンドを使用します。
- [Protocol]：サービスがプロトコルとして使用する TCP または UDP。
- [Port/Port Range] ：サービスによって使用されているポートまたはポートの範囲。
- [Timeout]：Sun RPC インスペクションによって接続のために開かれたピンホールのアイドル タイムアウト。

ステップ 4 [OK] をクリックします。

ステップ 5 （オプション）これらのサービス用に作成されたピンホールをモニターします。

Sun RPC サービスで開かれているピンホールを表示するには、**show sunrpc-server active** 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。次に例を示します。

```
hostname# show sunrpc-server active
LOCAL FOREIGN SERVICE TIMEOUT
-------------------------------------------------
1 209.165.200.5/0 192.168.100.2/2049 100003 0:30:00
2 209.165.200.5/0 192.168.100.2/2049 100003 0:30:00
3 209.165.200.5/0 192.168.100.2/647 100005 0:30:00
4 209.165.200.5/0 192.168.100.2/650 100005 0:30:00
```

LOCAL カラムのエントリは、内部インターフェイスのクライアントまたはサーバーの IP アドレスを示します。FOREIGN カラムの値は、外部インターフェイスのクライアントまたはサーバーの IP アドレスを示します。

必要に応じ、次のコマンドを使用してこれらのサービスをクリアすることができます。 **clear sunrpc-server active**

TFTP インスペクション

TFTP インスペクションはデフォルトでイネーブルになっています。

TFTP は、RFC 1350 に記述されているように、TFTP サーバーとクライアントの間のファイルの読み書きを行うための簡易プロトコルです。

インスペクションエンジンは、TFTP 読み取り要求（RRQ）、書き込み要求（WRQ）、およびエラー通知（ERROR）を検査し、必要に応じてダイナミックに接続と変換を作成し、TFTP クライアントとサーバーの間のファイル転送を許可します。

有効な読み取り要求（RRQ）または書き込み要求（WRQ）を受信すると、必要に応じて、ダイナミックなセカンダリ チャネルと PAT 変換が割り当てられます。このセカンダリ チャネルは、これ以降 TFTP によってファイル転送またはエラー通知用に使用されます。

TFTP サーバーだけがセカンダリ チャネル経由のトラフィックを開始できます。また、TFTP クライアントとサーバーの間に存在できる不完全なセカンダリ チャネルは1つまでです。サーバーからのエラー通知があると、セカンダリ チャネルは閉じます。

TFTP トラフィックのリダイレクトにスタティック PAT が使用されている場合は、TFTP インスペクションをイネーブルにする必要があります。

TFTPインスペクションをイネーブルにする方法については、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を参照してください。

XDMCP インスペクション

XDMCP は、UDP ポート 177 を使用して X セッションをネゴシエートするプロトコルです。X セッションは確立時に TCP を使用します。

XWindows セッションを正常にネゴシエートして開始するために、ASA は、Xhosted コンピュータからの TCP 戻り接続を許可する必要があります。戻り接続を許可するには、TCP ポートを許可するアクセス ルールを使用できます。または、ASA で **established** コマンドを使用できます。XDMCP がディスプレイを送信するポートをネゴシエートすると、**established** コマンドが参照され、この戻り接続を許可すべきかどうかが確認されます。

XWindows セッション中、マネージャは予約済みポート 6000 | n 上でディスプレイ Xserver と通信します。次の端末設定を行うと、各ディスプレイは別々に Xserver と接続します。

```
setenv DISPLAY Xserver:n
```

n はディスプレイ番号です。

XDMCP が使用されている場合、ディスプレイは IP アドレスを使用してネゴシエートされます。IP アドレスは、ASA が必要に応じて NAT を行うことができます。XDCMP インスペクションでは、PAT はサポートされません。

XDMCP インスペクションのイネーブル化の詳細については、 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 を参照してください。

VXLAN インスペクション

Virtual Extensible Local Area Network （VXLAN）インスペクションは、ASA を通過する VXLAN のカプセル化されたトラフィックで機能します。VXLAN ヘッダーフォーマットが標準に準拠し、不正な形式のパケットをドロップすることを確認します。VXLAN インスペクションは、ASA が VXLAN トンネル エンドポイント（VTEP）または VXLAN ゲートウェイとして機能するトラフィックでは行われません。これは、それらのチェックが VXLAN パケットの通常の非カプセル化の一部として行われるためです。

VXLAN パケットは通常、ポート 4789 の UDP です。このポートは、default-inspection-traffic クラスの一部であるため、inspection_default サービス ポリシー ルールに VXLAN インスペクションを追加するだけです。または、それに対してポートまたは ACL マッチングを使用してクラスを作成することもできます。

基本的なインターネット プロトコル インスペクションの履歴

機能名	リリース	機能情報
DCERPC インスペクションで ISystemMapper UUID メッセージ RemoteGetClassObject opnum3 をサポート。	9.4(1)	ASA は、リリース 8.3 で EPM 以外の DCERPC メッセージのサポートを開始し、ISystemMapper UUID メッセージ RemoteCreateInstance opnum4 をサポートしています。この変更により、RemoteGetClassObject opnum3 メッセージまでサポートが拡張されます。 変更された ASDM 画面はありません。
VXLAN パケット インスペクション	9.4(1)	ASA は、標準形式に準拠するために VXLAN ヘッダーを検査できます。 次の画面が変更されました。[Configuration] > [Firewall] > [Service Policy Rules] > [Add Service Policy Rule] > [Rule Actions] > [Protocol Inspection]。
ESMTP インスペクションの TLS セッションでのデフォルトの動作の変更。	9.4(1)	ESMTP インスペクションのデフォルトが、検査されない、TLS セッションを許可するように変更されました。ただし、このデフォルトは新しい、または再イメージングされたシステムに適用されます。**no allow-tls** を含むシステムをアップグレードする場合、このコマンドは変更されません。 デフォルトの動作の変更は、古いバージョンでも行われました：8.4（7.25）、8.5（1.23）、8.6（1.16）、8.7（1.15）、9.0（4.28）、9.1（6.1）、9.2（3.2）、9.3（1.2）、9.3（2.2）。

機能名	リリース	機能情報
IP オプション インスペクションの改善	9.5(1)	IP オプション インスペクションは、すべての有効な IP オプションをサポートするようになりました。まだ定義されていないオプションを含む、標準または試行的なオプションを許可、クリア、またはドロップするようにインスペクションを調整できます。また、IP オプション インスペクション マップで明示的に定義されていないオプションのデフォルトの動作を設定できます。 追加のオプションを含めるように [IP Options Inspect Map] ダイアログボックスが変更されました。許可およびオプションでクリアするオプションを選択するようになりました。
DCERPC インスペクションの改善および UUID フィルタリング	9.5(2)	DCERPC インスペクションは、OxidResolver ServerAlive2 opnum5 メッセージに対して NAT をサポートするようになりました。また、DCERPC メッセージの汎用一意識別子（UUID）でフィルタリングし、特定のメッセージ タイプをリセットするかログに記録できるようになりました。UUID フィルタリング用の新しい DCERPC インスペクション クラス マップがあります。 **[Configuration]** > **[Firewall]** > **[Objects]** > **[Class Maps]** > **[DCERPC]** の画面が追加されました。次の画面が変更されました。**[Configuration]** > **[Firewall]** > **[Objects]** > **[Inspect Maps]** > **[DCERPC]**。
DNS over TCP インスペクション。	9.6(2)	DNS over TCP トラフィック（TCP/53）を検査できるようになりました。 次のページが変更されました：**[Configuration]** > **[Firewall]** > **[Objects]** > **[Inspection Maps]** > **[DNS]**[Add/Edit] ダイアログボックス
Cisco Umbrella サポート。	9.10(1)	Cisco Umbrella で定義されている エンタープライズ セキュリティ ポリシーをユーザー接続に適用できるように DNS 要求を Cisco Umbrella へリダイレクトするようにデバイスを設定できます。FQDN に基づいて接続を許可またはブロックできます。または、疑わしい FQDN の場合は Cisco Umbrella インテリジェント プロキシにユーザーをリダイレクトして URL フィルタリングを実行できます。Umbrella の設定は、DNS インスペクション ポリシーに含まれています。 次の画面を追加または変更しました。 **[Configuration]** > **[Firewall]** > **[Objects]** > **[Umbrella]**、**[Configuration]** > **[Firewall]** > **[Objects]** > **[Inspect Maps]** > **DNS**.

機能名	リリース	機能情報
Cisco Umbrella の強化	9.12(1)	Cisco Umbrella をバイパスする必要があるローカル ドメイン名を特定できるようになりました。これらのドメインの DNS 要求は、Umbrella を処理せず DNS サーバーに直接送信されます。また、DNS 要求の解決に使用する Umbrella サーバーも特定できるようになりました。さらに、Umbrella サーバーを使用できない場合は、DNS 要求がブロックされないように、Umbrella インスペクション ポリシーをフェール オープンに定義することができます。 次の画面が変更されました。**[Configuration]** > **[Firewall]** > **[Objects]** > **[Umbrella]**、**[Configuration]** > **[Firewall]** > **[Objects]** > **[Inspect Maps]** > **[DNS]**。
新規インストールでは、デフォルトでXDMCP インスペクションが無効になっています。	9.15(1)	以前は、すべてのトラフィックに対して XDMCP インスペクションがデフォルトで有効になっていました。新しいシステムと再イメージ化されたシステムを含む新規インストールでは、XDMCP はデフォルトで無効になっています。このインスペクションが必要な場合は、有効にしてください。アップグレードでは、デフォルトのインスペクション設定を使用して XDMCP インスペクションを有効にしただけでも、XDMCP インスペクションの現在の設定は保持されます。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。