CHAPTER 9

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適用の方法全体については、「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」（P.8-1）を参照してください。

DNS インスペクション

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アクション

DNS インスペクションはデフォルトではイネーブルです。DNS インスペクションをカスタマイズして多くのタスクを実行できます。

- DNS レコードを NAT の設定に基づいて変換します。詳細については、「DNS および NAT」（P.5-32）を参照してください。
- メッセージの長さ、ドメイン名の長さ、ラベルの長さを適用します。
- DNS メッセージに圧縮ポインタが出現した場合、ポインタが参照するドメイン名の整合性を確認します。
- 圧縮ポインタのループが終了するかどうかを確認します。
- DNS のヘッダー、タイプ、クラス、その他に基づいてパケットを検査します。

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、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ります。

- 最大 DNS メッセージ長は、512 バイトです。
- 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して DNS 応答の ID が DNS クエリーの 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。

DNS インスペクションの設定

DNS インスペクションはデフォルトではイネーブルです。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。DNS インスペクションをカスタマイズする場合は、次のプロセスを使用します。

手順

ステップ 1　「DNS インスペクション クラス マップの設定」（P.9-3）

ステップ 2　「DNS インスペクション ポリシー マップの設定」（P.9-4）

ステップ 3　「DNS インスペクション サービス ポリシーの設定」（P.9-6）

DNS インスペクション クラス マップの設定

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 マップでは複雑な一致基準を作成でき、クラス マップを再利用できるという点です。

ヒント　以下で説明する手順に加えて、インスペクション マップまたはサービス ポリシーの作成中にもクラス 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。

はじめる前に

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いずれかを使用する場合は、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] > [Class Maps] > [DNS] を選択します。

ステップ 2　次のどちらかを実行します。

- [Add] をクリックして、新しいクラス 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。マップの編集時には、説明のみを変更できます。

ステップ 4　照合オプションとして [Match All] または [Match Any] を選択します。

[Match All] がデフォルトです。トラフィックがクラス マップと一致するには、すべての基準と一致する必要があることを指定します。[Match Any] は、少なくとも 1 つの基準に一致したトラフィックがクラス マップに一致することを意味します。

ステップ 5　一致テーブルでエントリを追加または編集して、一致基準を設定します。対象トラフィックを定義するために必要な数のエントリを追加します。

a. 基準の一致タイプとして [Match]（トラフィックは基準に一致する必要がある）または [No Match]（トラフィックは基準とは異なっている必要がある）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。

b. 一致基準を選択し、その値を定義します。

- [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）、**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。

c. [OK] をクリックします。

ステップ 6　[DNS Traffic Class 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 ポリシー マップでクラス マップを使用できるようになります。

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。

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もインスペクション 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。

はじめる前に

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いずれかを使用する場合は、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　次のどちらかを実行します。

- [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。マップのセキュリティ レベルは直接変更するか、[Customize] をクリックすることで編集できます。残りの手順は、マップをカスタマイズするか追加することが前提になります。

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。マップの編集時には、説明のみを変更できます。

ステップ 4　[DNS Inspect Map] ダイアログ ボックスの [Security Level] ビューで、目的の設定に最も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 1 つが要件と一致する場合は、これで完了です。[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して DNS 応答の ID が DNS クエリーの 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を行います。
- [Randomize the DNS identifier for DNS query]。
- [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のどちらからのパケットであるかに関係なく、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 DNS メッセージの最大長を設定するか（512 ～ 65535 バイト）、またはリソース 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するか（512 ～ 65535 バイト）、またはリソース 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イネーブル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] タブをクリックして、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。

トラフィック一致基準は、DNS クラス マップをベースにするか、インスペクション マップで一致を直接設定するか、またはこの両方によって定義できます。

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. 基準を直接定義する場合は [Single Match] を選択し、基準を定義する DNS クラス マップを選択する場合は [Multiple Match] を選択します（「DNS インスペクション クラス マップの設定」（P.9-3）を参照）。

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）、**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のどちらにするかを選択します。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。必要に応じてこのプロセスを繰り返します。

ステップ 9　[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。

DNS インスペクション サービス ポリシーの設定

ASA のデフォルトの設定には、すべてのインターフェイスにグローバルに適用されるデフォルト ポートの DNS インスペクションが含まれます。インスペクション設定をカスタマイズするには、デフォルトのグローバル ポリシーをカスタマイズするのが一般的です。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。

手順

ステップ 1　[Configuration] > [Firewall] > [Service Policy] の順に選択し、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、[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。「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、ウィザードを使って [Rules] ページに進みます。
- DNS インスペクション ルールがある場合、または DNS 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。

ステップ 2　[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 3　（使用中のポリシーを変更する場合）使用中のポリシーを編集して別の DNS インスペクション ポリシー マップを使用する場合は、DNS インスペクションをディセーブルにしてから、新しい DNS 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する必要があります。

a. [DNS] チェックボックスの選択を解除します。

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 4　[DNS] を選択します

ステップ 5　デフォルト以外のインスペクションが必要な場合は、[Configure] をクリックし、次の操作を実行します。

a. デフォルト マップを使用するか、設定した DNS インスペクション ポリシー マップを使用するかを選択します。この時点でマップを作成できます。詳細については、「DNS インスペクション ポリシー マップの設定」（P.9-4）を参照してください。

b. 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。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（必要な場合は [Manage] をクリックして作成します）。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。

c. [Select DNS Inspect Map] ダイアログ ボックスの [OK] をクリックします。

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。

DNS インスペクションのモニタリング

現在の DNS 接続に関する情報を表示するには、[Tools] > [Command Line Interface] で次のコマンドを入力するか、または [Monitoring] > [Properties] > [Connections] を使用します。

```
hostname# show conn
```

DNS サーバを使用する接続の場合、show conn コマンドの出力で、接続の送信元ポートが DNS サーバの IP アドレスに置き換えられることがあります。

複数の DNS セッションが同じ 2 つのホスト間で発生し、それらのセッションの 5 つのタプル（送信元/宛先 IP アドレス、送信元/宛先ポート、およびプロトコル）が同じものである場合、それらのセッションに対しては接続が 1 つだけ作成されます。DNS ID は app_id で追跡され、各 app_id のアイドル タイマーは独立して実行されます。

app_id の有効期限はそれぞれ独立して満了するため、正当な DNS 応答がセキュリティ アプライアンスを通過できるのは、限られた期間内だけであり、リソースの継続使用はできません。ただし、**show conn** コマンドを入力した場合、新しい DNS セッションによってリセットされている DNS 接続のアイドル タイマーが表示されます。これは共有 DNS 接続の性質によるものであり、仕様です。

DNS アプリケーション インスペクションの統計情報を表示するには、**show service-policy** コマンドを入力します。次に、**show service-policy** コマンドの出力例を示します。

```
hostname# show service-policy
Interface outside:
Service-policy: sample_policy
    Class-map: dns_port
      Inspect: dns maximum-length 1500, packet 0, drop 0, reset-drop 0
```

FTP インスペクション

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。

- ダイナミックな二次的データ接続の準備
- FTP コマンド応答シーケンスの追跡
- 監査証跡の生成
- 埋め込み IP アドレスの変換

FTP アプリケーション インスペクションによって、FTP データ転送用にセカンダリ チャネルが用意されます。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。

（注）　**no inspect ftp** コマンドを使用して、FTP インスペクション エンジンをディセーブルにすると、アウトバウンド ユーザはパッシブ モードだけで接続を開始でき、インバウンド 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。

インターフェイスに対して **strict** オプションをオンにすると、FTP インスペクションによって次の動作が適用されます。

- 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　**strict** オプションを使用すると、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。

strict オプションがイネーブルの場合、各 FTP コマンドと応答シーケンスが追跡され、次の異常なアクティビティがないか確認されます。

- 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 サーバ応答を X の連続に置き換えることで、FTP クライアントがサーバのシステム タイプを取得できないようにします。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 インスペクションの設定

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。FTP インスペクションをカスタマイズする場合は、次のプロセスを使用します。

手順

ステップ 1　「FTP インスペクション クラス マップの設定」（P.9-10）
ステップ 2　「FTP インスペクション ポリシー マップの設定」（P.9-11）
ステップ 3　「FTP インスペクション サービス ポリシーの設定」（P.9-13）

FTP インスペクション クラス マップの設定

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 マップでは複雑な一致基準を作成でき、クラス マップを再利用できるという点です。

ヒント　以下で説明する手順に加えて、インスペクション マップまたはサービス ポリシーの作成中にもクラス 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。

はじめる前に

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いずれかを使用する場合は、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] > [Class Maps] > [FTP] を選択します。
ステップ 2　次のどちらかを実行します。

- [Add] をクリックして、新しいクラス 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。マップの編集時には、説明のみを変更できます。
ステップ 4　照合オプションとして [Match All] または [Match Any] を選択します。

[Match All] がデフォルトです。トラフィックがクラス マップと一致するには、すべての基準と一致する必要があることを指定します。[Match Any] は、少なくとも 1 つの基準に一致したトラフィックがクラス マップに一致することを意味します。

ステップ 5　一致テーブルでエントリを追加または編集して、一致基準を設定します。対象トラフィックを定義するために必要な数のエントリを追加します。

a. 基準の一致タイプとして [Match]（トラフィックは基準に一致する必要がある）または [No Match]（トラフィックは基準とは異なっている必要がある）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。
b. 一致基準を選択し、その値を定義します。
   - [File Name]：選択した正規表現または正規表現クラスに対して転送されるファイルの名前と照合します。

- [File Type]：選択した正規表現または正規表現クラスに対して転送されるファイルの MIME またはメディア タイプと照合します。
- [Server]：選択した正規表現または正規表現クラスに対する FTP サーバの名前と照合します。
- [User]：選択した正規表現または正規表現クラスに対するログイン ユーザの名前と照合します。
- [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移動します。

  DELE：サーバのファイルを削除します。

  GET：サーバ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：サーバにディレクトリを作成します。

  PUT：ファイルをサーバに送信します。

  MKD：サーバのディレクトリを削除します。

  RNFR：「変更元」ファイル名を指定します。

  RNTO：「変更先」ファイル名を指定します。

  SITE：サーバ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：一意のファイル名を使用してファイルを保存します。

c. [OK] をクリックします。

ステップ 6　[FTP Traffic Class 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 ポリシー マップでクラス マップを使用できるようになります。

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。

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もインスペクション 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。

はじめる前に

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いずれかを使用する場合は、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　次のどちらかを実行します。

- [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。マップのセキュリティ レベルは直接変更するか、[Customize] をクリックすることで編集できます。残りの手順は、マップをカスタマイズするか追加することが前提になります。

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。マップの編集時には、説明のみを変更できます。

ステップ 4　[FTP Inspect Map] ダイアログ ボックスの [Security Level] ビューで、目的の設定に最も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 1 つが要件と一致する場合は、これで完了です。[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] タブをクリックして、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。

トラフィック一致基準は、FTP クラス マップをベースにするか、インスペクション マップで一致を直接設定するか、またはこの両方によって定義できます。

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. 基準を直接定義する場合は [Single Match] を選択し、基準を定義する FTP クラス マップを選択する場合は [Multiple Match] を選択します（「FTP インスペクション クラス マップの設定」（P.9-10）を参照）。

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、「FTP インスペクション クラス マップの設定」（P.9-10）の説明に従って基準を設定します。

d. ロギングをイネーブルまたはディセーブルのどちらにするかを選択します。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。必要に応じてこの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。

FTP インスペクション サービス ポリシーの設定

ASA のデフォルトの設定には、すべてのインターフェイスにグローバルに適用されるデフォルト ポートの FTP インスペクションが含まれます。インスペクション設定をカスタマイズするには、デフォルトのグローバル ポリシーをカスタマイズするのが一般的です。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。

手順

ステップ 1　[Configuration] > [Firewall] > [Service Policy] の順に選択し、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、[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。「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、ウィザードを使って [Rules] ページに進みます。
- FTP インスペクション ルールがある場合、または FTP 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。

ステップ 2　[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 3　（使用中のポリシーを変更する場合）使用中のポリシーを編集して別の FTP インスペクション ポリシー マップを使用する場合は、FTP インスペクションをディセーブルにしてから、新しい FTP 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する必要があります。

a. [FTP] チェックボックスの選択を解除します。

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 4　[FTP] を選択します。

ステップ 5　デフォルト以外のインスペクションが必要な場合は、[Configure] をクリックし、次の操作を実行します。

a. [Use Strict FTP] を選択します。

b. デフォルト マップを使用するか、またはユーザが設定した FTP インスペクション ポリシー マップを使用するかを選択します。この時点でマップを作成できます。詳細については、「FTP インスペクション ポリシー マップの設定」（P.9-11）を参照してください。

c. [Select FTP Inspect Map] ダイアログ ボックスの [OK] をクリックします。

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。

FTP インスペクションの確認とモニタリング

FTP アプリケーション インスペクションでは、次のログ メッセージが生成されます。

- 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。
- FTP コマンドが RETR または STOR であるかがチェックされ、取得コマンドおよび保存コマンドがログに記録されます。
- IP アドレスを提供するテーブルを検索してユーザ名が取得されます。
- ユーザ名、接続元の IP アドレス、接続先の IP アドレス、NAT アドレス、およびファイル操作がログに記録されます。
- メモリ不足によって動的なセカンダリ チャネルの準備に失敗した場合は、監査レコード 201005 が生成されます。

NAT と連携することにより、FTP アプリケーション インスペクションでは、アプリケーション ペイロード内の IP アドレスが変換されます。これは、RFC 959 に詳細に記述されています。

HTTP インスペクション

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」（P.9-14）
- 「HTTP インスペクションの設定」（P.9-15）

HTTP インスペクションの概要

ヒント　アプリケーションおよび URL のフィルタリングを実行するサービス モジュールをインストールできます。これには、ASA CX や ASA FirePOWER などの HTTP インスペクションが含まれます。ASA 上で実行される HTTP インスペクションは、これらのモジュールと互換性がありません。HTTP インスペクション ポリシー マップを使用して ASA 上で手作業による設定を試みるより、専用のモジュールを使用してアプリケーション フィルタリングを設定する方がはるかに簡単であることに注意してください。

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 インスペクションの設定

HTTP インスペクションはデフォルトではイネーブルになりません。ASA CX や ASA FirePOWER などの HTTP インスペクションおよびアプリケーション フィルタリングに専用のモジュールを使用していない場合、以下の方法を使用して、ASA に HTTP インスペクションを手動で設定できます。

ヒント　サービス モジュールと ASA の両方で HTTP インスペクションを設定しないでください。インスペクションの互換性はありません。

手順

ステップ 1　「HTTP インスペクション クラス マップの設定」（P.9-15）
ステップ 2　「HTTP インスペクション ポリシー マップの設定」（P.9-18）
ステップ 3　「HTTP インスペクション サービス ポリシーの設定」（P.9-19）

HTTP インスペクション クラス マップの設定

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 マップでは複雑な一致基準を作成でき、クラス マップを再利用できるという点です。

ヒント　以下で説明する手順に加えて、インスペクション マップまたはサービス ポリシーの作成中にもクラス 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。

はじめる前に

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いずれかを使用する場合は、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] > [Class Maps] > [HTTP] を選択します。

ステップ 2　次のどちらかを実行します。

- [Add] をクリックして、新しいクラス 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。マップの編集時には、説明のみを変更できます。

ステップ 4　照合オプションとして [Match All] または [Match Any] を選択します。

[Match All] がデフォルトです。トラフィックがクラス マップと一致するには、すべての基準と一致する必要があることを指定します。[Match Any] は、少なくとも 1 つの基準に一致したトラフィックがクラス マップに一致することを意味します。

ステップ 5　一致テーブルでエントリを追加または編集して、一致基準を設定します。対象トラフィックを定義するために必要な数のエントリを追加します。

a. 基準の一致タイプとして [Match]（トラフィックは基準に一致する必要がある）または [No Match]（トラフィックは基準とは異なっている必要がある）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。

b. 一致基準を選択し、その値を定義します。

- [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。

c. [OK] をクリックします。

ステップ 6　[HTTP Traffic Class 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 ポリシー マップでクラス マップを使用できるようになります。

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。

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もインスペクション 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。

はじめる前に

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いずれかを使用する場合は、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　次のどちらかを実行します。

- [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。マップのセキュリティ レベルは直接変更するか、[Customize] をクリックすることで編集できます。残りの手順は、マップをカスタマイズするか追加することが前提になります。

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。マップの編集時には、説明のみを変更できます。

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 1 つが要件と一致する場合は、これで完了です。[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 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] タブをクリックして、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。

トラフィック一致基準は、HTTP クラス マップをベースにするか、インスペクション マップで一致を直接設定するか、またはこの両方によって定義できます。

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. 基準を直接定義する場合は [Single Match] を選択し、基準を定義する HTTP クラス マップを選択する場合は [Multiple Match] を選択します（「HTTP インスペクション クラス マップの設定」（P.9-15）を参照）。

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、「HTTP インスペクション クラス マップの設定」（P.9-15）の説明に従って基準を設定します。

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を選択します。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。必要に応じてこの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。

HTTP インスペクション サービス ポリシーの設定

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。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。

手順

ステップ 1　[Configuration] > [Firewall] > [Service Policy] の順に選択し、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、[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。「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、ウィザードを使って [Rules] ページに進みます。
- HTTP インスペクション ルールがある場合、または HTTP 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。

ステップ 2　[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 3　（使用中のポリシーを変更する場合）使用中のポリシーを編集して別の HTTP インスペクション ポリシー マップを使用する場合は、HTTP インスペクションをディセーブルにしてから、新しい HTTP 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する必要があります。

a. [HTTP] チェックボックスの選択を解除します。

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 4　[HTTP] を選択します。

ステップ 5　デフォルト以外のインスペクションが必要な場合は、[Configure] をクリックし、次の操作を実行します。

a. デフォルト マップを使用するか、設定した HTTP インスペクション ポリシー マップを使用するかを選択します。この時点でマップを作成できます。詳細については、「HTTP インスペクション ポリシー マップの設定」（P.9-18）を参照してください。

b. [Select HTTP Inspect Map] ダイアログ ボックスの [OK] をクリックします。

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。

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 によるASAの通過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られる 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。

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」（P.8-10）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。

ICMP ペイロードがスキャンされて、元のパケットから 5 つのタプルが取得されます。取得した 5 つのタプルを使用してルックアップを実行し、クライアントの元のアドレスを判別します。ICMP エラー インスペクション エンジンは、ICMP パケットに対して次の変更を加えます。

- IP ヘッダー内のマッピング IP を実際の IP（宛先アドレス）に変更し、IP チェックサムを修正する。
- ICMP パケットに変更を加えたため、ICMP ヘッダー内の ICMP チェックサムを修正する。
- ペイロードに次の変更を加える。
  - 元のパケットのマッピング IP を実際の IP に変更する。
  - 元のパケットのマッピング ポートを実際のポートに変更する。
  - 元のパケットの IP チェックサムを再計算する。

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」（P.8-10）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ではイネーブルになりません。IM インスペクションが必要な場合は設定する必要があります。

手順

ステップ 1　「インスタント メッセージ インスペクション ポリシー マップの設定」（P.9-21）

ステップ 2　「IM インスペクション サービス ポリシーの設定」（P.9-23）

インスタント メッセージ 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、IM 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、IM 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、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 マップでは複雑な一致基準を作成でき、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もインスペクション 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。

はじめる前に

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いずれかを使用する場合は、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　次のどちらかを実行します。

- [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。マップの編集時には、説明のみを変更できます。

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。

トラフィック一致基準は、IM クラス マップをベースにするか、インスペクション マップで一致を直接設定するか、またはこの両方によって定義できます。

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. 基準を直接定義する場合は [Single Match] を選択し、基準を定義する HTTP クラス マップを選択する場合は [Multiple Match] 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を選択します。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。必要に応じてこの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。

IM インスペクション サービス ポリシーの設定

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。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。

手順

ステップ 1　[Configuration] > [Firewall] > [Service Policy] の順に選択し、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、[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。「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、ウィザードを使って [Rules] ページに進みます。
- IM インスペクション ルールがある場合、または IM 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。

ステップ 2　[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 3　（使用中のポリシーを変更する場合）使用中のポリシーを編集して別の IM インスペクション ポリシー マップを使用する場合は、IM インスペクションをディセーブルにしてから、新しい IM 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する必要があります。

a.　[IM] チェックボックスの選択を解除します。

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 4　[IM] を選択します。

ステップ 5　デフォルト以外のインスペクションが必要な場合は、[Configure] をクリックし、次の操作を実行します。

a.　デフォルト マップを使用するか、設定した IM インスペクション ポリシー マップを使用するかを選択します。この時点でマップを作成できます。詳細については、「インスタント メッセージ インスペクション ポリシー マップの設定」（P.9-21）を参照してください。

b.　[Select IM Inspect Map] ダイアログ ボックスの [OK] をクリックします。

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。

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、どの IP パケットが所定の IP オプションを持ち、ASAを通過できるかを制御できます。このインスペクションを設定することで、パケットの転送許可や、指定した IP オプションのクリアがASAに指示され、パケットの転送が可能になります。

ここでは、IP オプション インスペクション エンジ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概要

各 IP パケットには、Options フィールドのある IP ヘッダーが含まれています。Options フィールドは、通常は IP オプションと呼ばれ、制御機能を提供します。特定の状況で必要になりますが、一般的な通信では必要ありません。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 インスペクションを設定して、どの IP パケットが所定の IP オプションを持ち、ASAを通過できるかを制御できます。このインスペクションを設定することで、パケットの転送許可や、指定した IP オプションのクリアがASAに指示され、パケットの転送が可能になります。

オプションをクリアしたときの結果

IP オプション インスペクション ポリシー マップを設定する場合、各オプション タイプを許可またはクリアするかどうかを指定できます。オプション タイプを指定しないと、そのオプションを含むパケットはドロップされます。

オプションを単に許可すると、そのオプションを含むパケットは未変更で渡されます。

IP ヘッダーからオプションをクリアするように指定すると、IP ヘッダーは次のように変更されます。

- オプションがヘッダーから除去されます。
- Options フィールドは、32 ビット境界で終了するようにパディングされます。
- パケット内のインターネット ヘッダー長（IHL）が変更されます。
- パケット全体の長さが変更されます。
- チェックサムが再計算されます。

インスペクションでサポートされる IP オプション

IP オプション インスペクションでは、パケット内の次の IP オプションをチェックできます。IP ヘッダーにこれら以外のオプションがさらに含まれている場合、これらのオプションを許可するように ASA が設定されているかどうかに関係なく、ASA はそのパケットをドロップします。

- End of Options List（EOOL）または IP Option 0：このオプションにはゼロ バイトが 1 つだけ含まれており、オプションのリストの終わりを示すために、すべてのオプションの末尾に表示されます。これは、ヘッダー長に基づくヘッダーの末尾とは一致しない場合があります。
- No Operation（NOP）または IP Option 1：IP ヘッダーの Options 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、これがフィールド変数全体の長さになります。ただし、IP ヘッダーは 32 ビットの倍数である必要があります。すべてのオプションのビット数が 32 ビットの倍数でない場合、NOP オプションは、オプションを 32 ビット境界上に揃えるために、「内部パディング」として使用されます。
- Router Alert（RTRALT）または IP Option 20：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。

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、デフォルトでイネーブルになります。

- Router Alert オプションは許可されます。
- 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。これには、サポートされていないオプションを含むパケットが含まれます。

IP オプション インスペクションの設定

IP オプション 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 マップで許可されているもの以外の追加オプションが必要な場合にのみ、設定する必要があります。

手順

ステップ 1　「IP オプション インスペクション ポリシー マップの設定」（P.9-25）

ステップ 2　「IP オプション インスペクション サービス ポリシーの設定」（P.9-26）

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、サポートされる各オプション 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もインスペクション 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　次のどちらかを実行します。

- [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。マップの編集時には、説明のみを変更できます。

ステップ 4　許可するオプションを選択します。各オプション タイプの説明については、「インスペクションでサポートされる IP オプション」（P.9-24）を参照してください。

選択していないオプションを含むパケットはドロップされます。

ステップ 5　許可する各オプションについて、パケットを許可する前にオプションをクリアするかどうかを選択します。

オプションをクリアすると、インスペクションは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除去します。

ステップ 6　**[OK]** をクリックします。

これで、このインスペクション マップを IP オプション インスペクションのサービス ポリシーで使用できるようになります。

IP オプション インスペクション サービス ポリシーの設定

ASA のデフォルトのコンフィギュレーションには、すべてのインターフェイスにグローバルに適用される IP オプション インスペクションが含まれます。インスペクション設定をカスタマイズするには、デフォルトのグローバル ポリシーをカスタマイズするのが一般的です。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。

手順

ステップ 1　[Configuration] > [Firewall] > [Service Policy] の順に選択し、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、[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。「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、ウィザードを使って [Rules] ページに進みます。
- IP オプション インスペクション ルールがある場合、または IP オプション 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。

ステップ 2　[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 3　（使用中のポリシーを変更する場合）使用中のポリシーを編集して別の IP オプション インスペクション ポリシー マップを使用する場合は、IP オプション インスペクションをディセーブルにしてから、新しい IP オプション 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する必要があります。

a. [IP Options] 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 4　[IP Options] を選択します。

ステップ 5　デフォルト以外のインスペクションが必要な場合は、[Configure] をクリックし、次の操作を実行します。

a. デフォルト マップを使用するか、設定した IP オプション インスペクション ポリシー マップを使用するかを選択します。この時点でマップを作成できます。詳細については、「IP オプション インスペクション ポリシー マップの設定」（P.9-25）を参照してください。

b. [Select IP Options Inspect Map] ダイアログ ボックスの [OK] をクリックします。

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。

IP オプション インスペクションのモニタリング

以下の方法を使用して IP オプション インスペクションの結果をモニタリングできます。

- 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。

IPsec パススルー インスペクション

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」（P.9-27）
- 「IPsec パススルー インスペクションの設定」（P.9-28）

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 ユーザまたはサーバなど）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 インスペクションの設定

IPsec パススルー インスペクションはデフォルトではイネーブルになりません。IPsec パススルー インスペクションが必要な場合は設定する必要があります。

手順

ステップ 1　「IPsec パススルー インスペクション ポリシー マップの設定」（P.9-28）

ステップ 2　「IPsec パススルー インスペクション サービス ポリシーの設定」（P.9-29）

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もインスペクション 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　次のどちらかを実行します。

- [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。マップのセキュリティ レベルは直接変更するか、[Customize] をクリックすることで編集できます。残りの手順は、マップをカスタマイズするか追加することが前提になります。

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。マップの編集時には、説明のみを変更できます。

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 1 つが要件と一致する場合は、これで完了です。[OK] をクリックし、残りの手順はスキップして、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。

これで、このインスペクション マップを IPsec パススルー インスペクション サービス ポリシーで使用できるようになります。

IPsec パススルー インスペクション サービス ポリシーの設定

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。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。

手順

ステップ 1　[Configuration] > [Firewall] > [Service Policy] の順に選択し、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、[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。「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、ウィザードを使って [Rules] ページに進みます。
- IPsec パススルー インスペクション ルールがある場合、または IPsec パススルー 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。

ステップ 2　[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 3　（使用中のポリシーを変更する場合）使用中のポリシーを編集して別のインスペクション ポリシー マップを使用する場合は、IPsec パススルー インスペクションをディセーブルにしてから、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する必要があります。

a.　[IPsec Pass Through] 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 4　[IPsec Pass Through] を選択します。

ステップ 5　デフォルト以外のインスペクションが必要な場合は、[Configure] をクリックし、次の操作を実行します。

a.　デフォルト マップを使用するか、設定した IPsec パススルー インスペクション ポリシー マップを使用するかを選択します。この時点でマップを作成できます。詳細については、「IPsec パススルー インスペクション ポリシー マップの設定」（P.9-28）を参照してください。

b.　[Select IPsec Pass Through Inspect Map] ダイアログ ボックスの [OK] をクリックします。

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。

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 インスペクションのデフォルト」（P.9-30）
- 「IPv6 インスペクションの設定」（P.9-30）

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 インスペクションの設定

IPv6 インスペクションはデフォルトではイネーブルになりません。IPv6 インスペクションが必要な場合は設定する必要があります。

手順

ステップ 1　「IPv6 インスペクション ポリシー マップの設定」（P.9-30）

ステップ 2　「IPv6 インスペクション サービス ポリシーの設定」（P.9-31）

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　次のどちらかを実行します。

- [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。マップの編集時には、説明のみを変更できます。

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　（オプション）[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。必要に応じてこの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。

これで、このインスペクション マップを IPv6 インスペクション サービス ポリシーで使用できるようになります。

IPv6 インスペクション サービス ポリシーの設定

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。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。

手順

ステップ 1　[Configuration] > [Firewall] > [Service Policy] の順に選択し、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、[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。「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、ウィザードを使って [Rules] ページに進みます。
- IPv6 インスペクション ルールがある場合、または IPv6 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。

ステップ 2　[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 3　（使用中のポリシーを変更する場合）使用中のポリシーを編集して別の IPv6 インスペクション ポリシー マップを使用する場合は、IPv6 インスペクションをディセーブルにしてから、新しい IPv6 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する必要があります。

a.　[IPv6] 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 4　[IPv6] を選択します。

ステップ 5　デフォルト以外のインスペクションが必要な場合は、[Configure] をクリックし、次の操作を実行します。

a.　デフォルト マップを使用するか、設定した IPv6 インスペクション ポリシー マップを使用するかを選択します。この時点でマップを作成できます。詳細については、「IPv6 インスペクション ポリシー マップの設定」（P.9-30）を参照してください。

b.　[Select IPv6 Inspect Map] ダイアログ ボックスの [OK] をクリックします。

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。

NETBIOS インスペクション

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。NetBIOS インスペクション エンジンは、ASAの NAT コンフィギュレーションに基づいて、NetBIOS ネーム サービス（NBNS）パケット内の IP アドレスを変換します。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。

手順

ステップ 1　「インスペクション制御を追加するための NetBIOS インスペクション ポリシー マップの設定」（P.9-33）

ステップ 2　「NetBIOS インスペクション サービス ポリシーの設定」（P.9-33）

インスペクション制御を追加するための NetBIOS インスペクション ポリシー マップの設定

プロトコル違反のアクションを指定するには、NetBIOS 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、NETBIOS インスペクションをイネーブルにすると適用できます。

手順

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

ステップ 2　次のどちらかを実行します。

- [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。マップの編集時には、説明のみを変更できます。

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。

NetBIOS インスペクション サービス ポリシーの設定

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 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。

ASA のデフォルトの設定には、すべてのインターフェイスにグローバルに適用されるデフォルト ポートの NetBIOS インスペクションが含まれます。インスペクション設定をカスタマイズするには、デフォルトのグローバル ポリシーをカスタマイズするのが一般的です。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。

手順

ステップ 1　[Configuration] > [Firewall] > [Service Policy] の順に選択し、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、[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。「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、ウィザードを使って [Rules] ページに進みます。
- NetBIOS インスペクション ルールがある場合、または NetBIOS 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。

ステップ 2　[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 3　[NetBIOS] を選択します。

ステップ 4　デフォルト以外のインスペクションが必要な場合は、[Configure] をクリックし、デフォルト マップを使用するか、またはユーザが設定した NetBIOS インスペクション ポリシー マップを使用するかを選択します。この時点でマップを作成できます。詳細については、「インスペクション制御を追加するための NetBIOS インスペクション ポリシー マップの設定」（P.9-33）を参照してください。

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

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。

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。接続と xlate は、後続のセカンダリ 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」（P.8-10）を参照してください。

SMTP および拡張 SMTP 検査

ESMTP インスペクションは、スパム、フィッシング、不正な形式のメッセージによる攻撃、バッファ オーバーフロー /アンダーフロー攻撃を検出します。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、各種の攻撃の検出や送受信者およびメール中継のブロックも行います。

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 および拡張 SMTP（ESMTP）のインスペクションの概要

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。便宜上、このマニュアルでは、SMTP という用語を SMTP と ESMTP の両方に使用します。拡張 SMTP に対するアプリケーション インスペクション処理は、SMTP アプリケーション インスペクションに似ており、SMTP セッションのサポートが含まれています。拡張 SMTP セッションで使用するほとんどのコマンドは、SMTP セッションで使用するコマンドと同じですが、ESMTP セッションの方が大幅に高速で、配信ステータス通知など信頼性およびセキュリティに関するオプションが増えています。

拡張 SMTP アプリケーション インスペクションでは、AUTH、EHLO、ETRN、HELP、SAML、SEND、SOML、STARTTLS、および VRFY を含む拡張 SMTP コマンドに対するサポートが追加されています。ASAは、7 つの RFC 821 コマンド（DATA、HELO、MAIL、NOOP、QUIT、RCPT、RSET）をサポートするとともに、合計 15 の SMTP コマンドをサポートします。

その他の拡張 SMTP コマンド（ATRN、ONEX、VERB、CHUNKING など）、およびプライベート拡張はサポートされません。サポートされないコマンドは、内部サーバにより拒否される X に変換されます。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、廃棄されます。

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。

SMTP 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。

SMTP サーバは、数値の応答コード、およびオプションの可読文字列でクライアント要求に応答します。SMTP アプリケーション インスペクションは、ユーザが使用できるコマンドとサーバが返送するメッセージを制御し、その数を減らします。SMTP 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。
- SMTP コマンド応答シーケンスをモニタします。
- 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。

SMTP インスペクションでは、次の異常な署名がないかどうか、コマンドと応答のシーケンスをモニタします。

- 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 サーバによる不意の移行
- 未知のコマンドに対しては、ASA はパケット内のすべての文字を X に変更します。この場合、サーバがクライアントに対してエラー コードを生成します。パケット内が変更されるため、TCP チェックサムの再計算または調整が必要になります。

- TCP ストリーム編集
- コマンド パイプライン

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、デフォルトでイネーブルになります。

- サーバ バナーはマスクされます。
- 暗号化されたトラフィックが検査されます。
- 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 インスペクションの設定

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 マップとは異なるプロセスが必要な場合にのみ、設定する必要があります。

手順

ステップ 1　「ESMTP インスペクション ポリシー マップの設定」（P.9-36）

ステップ 2　「ESMTP インスペクション サービス ポリシーの設定」（P.9-38）

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。

はじめる前に

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いずれかを使用する場合は、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　次のどちらかを実行します。

- [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。マップのセキュリティ レベルは直接変更するか、[Customize] をクリックすることで編集できます。残りの手順は、マップをカスタマイズするか追加することが前提になります。

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。マップの編集時には、説明のみを変更できます。

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 1 つが要件と一致する場合は、これで完了です。[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。

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] タブをクリックして、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に一致する必要がある）または [No Match]（トラフィックは基準とは異なっている必要がある）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]：メッセージ内のコマンド動詞と一致します。次のコマンドの 1 つ以上を指定できます。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 つ以上を指定できます。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 以上を指定できます。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を選択します。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 応答パラメータの一致の場合、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。必要に応じてこの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。

ESMTP インスペクション サービス ポリシーの設定

ASA のデフォルトのコンフィギュレーションには、すべてのインターフェイスにグローバルに適用される ESMTP インスペクションが含まれます。インスペクション設定をカスタマイズするには、デフォルトのグローバル ポリシーをカスタマイズするのが一般的です。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。

手順

ステップ 1　[Configuration] > [Firewall] > [Service Policy] の順に選択し、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、[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。「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、ウィザードを使って [Rules] ページに進みます。
- ESMTP インスペクション ルールがある場合、または ESMTP 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。

ステップ 2　[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 3　（使用中のポリシーを変更する場合）使用中のポリシーを編集して別のインスペクション ポリシー マップを使用する場合は、ESMTP インスペクションをディセーブルにしてから、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する必要があります。

a. [ESMTP] 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 4　[ESMTP] を選択します。

ステップ 5　デフォルト以外のインスペクションが必要な場合は、[Configure] をクリックし、次の操作を実行します。

a. デフォルト マップを使用するか、設定した ESMTP インスペクション ポリシー マップを使用するかを選択します。この時点でマップを作成できます。詳細については、「ESMTP インスペクション ポリシー マップの設定」（P.9-36）を参照してください。
b. [Select ESMTP Inspect Map] ダイアログ ボックスの [OK] をクリックします。

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。

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。

ASAは、TFTP トラフィックを検査し、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の間のファイル転送を許可します。具体的には、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」（P.8-10）を参照してください。