



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。

- [DNS インスペクション \(1 ページ\)](#)
- [FTP インスペクション \(5 ページ\)](#)
- [HTTP インスペクション \(10 ページ\)](#)
- [ICMP インスペクション \(15 ページ\)](#)
- [ICMP エラー インスペクション \(16 ページ\)](#)
- [インスタントメッセージ インスペクション \(16 ページ\)](#)
- [IP オプション インスペクション \(18 ページ\)](#)
- [IPsec パススルー インスペクション \(20 ページ\)](#)
- [IPv6 インスペクション \(22 ページ\)](#)
- [NetBIOS インスペクション \(24 ページ\)](#)
- [PPTP インスペクション \(25 ページ\)](#)
- [SMTP および拡張 SMTP インスペクション \(25 ページ\)](#)
- [TFTP インスペクション \(30 ページ\)](#)

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。
- 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。

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です。
- [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 [不一致レート (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グ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 ~ 0xffff) 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) ログイ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、ログイ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、パケットのログイング、またはパケットのドロップとログイングが可能です。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 [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 データ接続チャンネルを準備します。これらのチャンネルのポートは、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 チャンネルは、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。
- 監査証拠を生成します。

- 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。
- メモリ不足のためにセカンダリ ダイナミック チャネルの準備に失敗した場合、監査レコード 201005 が生成されます。
- 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。

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。

- 切り捨てられたコマンド：PORT コマンドおよび PASV 応答コマンドのカンマの数が 5 であるかどうかを確認されます。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 サーバの応答を連続した X で置き換えて、サーバのシステム 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。

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、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。
 - **RMD** : サーバ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) ログイン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

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は、ASA に HTTP インスペクションを手動で設定できます。

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。



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。

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



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 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 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

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 を通過すること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。

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。

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。

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。

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。

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選択します。

[End of Options List]、[No Operation]、および [Router Alert] オプションを許可できます。

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。パケットにサポートされていないオプションが含まれている場合は、それもドロップされます。

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 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。

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 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を確認できます。

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 チャンネルと通常2つの PPTP GRE トンネルで構成されます。TCP チャンネルは、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ンネルです。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 制御チャン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せん。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 エンジンには、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 制御チャン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。

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。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 (空白に変更されます)、「<」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。

- サーババナーはマスクされます。ESMTP インスペクション エンジンでは、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。
- 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つまたは複数指定できます。auth、data、ehlo、etn、helo、help、mail、noop、quit、rcpt、rset、saml、somi、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つまたは複数指定できます。8bitmime、auth、binaryname、checkpoint、dsn、etn、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。

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。

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](#)を参照してください。