CHAPTER 24

アプリケーション レイヤ プロトコル検査の設定

この章では、アプリケーション レイヤ プロトコル検査を設定する方法について説明します。検査エンジンは、ユーザのデータ パケット内に IP アドレッシング情報を埋め込むサービスや、ダイナミックに割り当てられるポート上でセカンダリ チャネルを開くサービスに必要です。これらのプロトコルでは、高速パスでパケットを渡すのではなく、セキュリティ アプライアンスが詳細なパケット検査を行う必要があります。そのため、検査エンジンがスループット全体に影響を与えることがあります。

デフォルトでいくつかの一般的な検査エンジンがセキュリティ アプライアンス上でイネーブルになっていますが、ネットワークによっては他の検査エンジンをイネーブルにする必要がある場合があります。この章には、次の項があります。

検査エンジンの概要

ここでは、次の項目について説明します。

アプリケーション プロトコル検査を使用するタイミング

ユーザが接続を確立すると、セキュリティ アプライアンスはアクセスリストと照合してパケットをチェックし、アドレス変換を作成し、高速パスでのセッション用にエントリを作成して、後続のパケットが時間のかかるチェックをバイパスできるようにします。ただし、高速パスは予測可能なポート番号に基づいており、パケット内部のアドレス変換を実行しません。

多くのプロトコルは、セカンダリの TCP ポートまたは UDP ポートを開きます。ウェルノウン ポート上の初期セッションは、ダイナミックに割り当てられたポート番号をネゴシエートするために使用されます。

パケットに IP アドレスを埋め込むアプリケーションもあります。この IP アドレスは送信元アドレスと一致する必要があり、通常、セキュリティ アプライアンスを通過するときに変換されます。

このようなアプリケーションを使用する場合は、アプリケーション検査をイネーブルにする必要があります。

IP アドレスを埋め込むサービスに対してアプリケーション検査をイネーブルにすると、セキュリティ アプライアンスは埋め込まれたアドレスを変換し、チェックサムや変換の影響を受けたその他のフィールドを更新します。

ダイナミックに割り当てられたポートを使用するサービスに対してアプリケーション検査をイネーブルにすると、セキュリティ アプライアンスはセッションを監視してダイナミックに割り当てられたポートを特定し、所定のセッションの間、それらのポートでのデータ交換を許可します。

検査に関する制約事項

アプリケーション プロトコル検査には次の制約事項があります。

- 検査が必要なマルチメディア セッションのステート情報は、ステートフル フェールオーバーのステート リンク経由では渡されません。GTP は例外で、ステート リンクで複製されます。
- 一部の検査エンジンは、PAT、NAT、外部 NAT、または同一セキュリティ インターフェイス間の NAT をサポートしません。NAT サポートの詳細については、「デフォルトの検査ポリシー」を参照してください。

デフォルトの検査ポリシー

デフォルトでは、すべてのデフォルト アプリケーション検査トラフィックを照合するポリシーがコンフィギュレーションに含まれ、すべてのインターフェイス上のトラフィックに検査を適用します（グローバル ポリシー）。デフォルト アプリケーション検査トラフィックには、各プロトコルのデフォルト ポートへのトラフィックが含まれます。適用できるグローバル ポリシーは 1 つだけなので、グローバル ポリシーを変更する場合（標準以外のポートに検査を適用する場合や、デフォルトでイネーブルになっていない検査を追加する場合など）は、デフォルトのポリシーを編集するか、デフォルトのポリシーをディセーブルにして新しいポリシーを適用する必要があります。

表 24-1 に、サポートされているすべての検査、デフォルトのクラスマップで使用されるデフォルトのポート、およびデフォルトでオンになっている検査エンジン（太字）を示します。この表には、NAT に関する制約事項も含まれています。

表 24-1　サポートされているアプリケーション検査エンジン

アプリケーション[1]	デフォルト ポート	NAT の制約事項	標準[2]	コメント
CTIQBE	TCP/2748	—	—	—
DNS over UDP	UDP/53	NAT サポートは、WINS 経由の名前解決では使用できません。	RFC 1123	PTR レコードは変更されません。
FTP	TCP/21	—	RFC 959	—
GTP	UDP/3386 UDP/2123	—	—	特別なライセンスが必要です。
H.323 H.225 および **RAS**	TCP/1720 UDP/1718 UDP (RAS)1718 ～ 1719	同一セキュリティ インターフェイス上の NAT はサポートされません。 スタティック PAT はサポートされません。	ITU-T H.323、H.245、H225.0、Q.931、Q.932	—
HTTP	TCP/80	—	RFC 2616	ActiveX と Java を除去する場合の MTU 制限に注意してください。MTU が小さすぎて Java タグまたは ActiveX タグを 1 つのパケットに収められない場合、除去が行われないことがあります。
ICMP	—	—	—	すべての ICMP トラフィックは、デフォルトのクラスマップで照合されます。
ICMP ERROR	—	—	—	すべての ICMP トラフィックは、デフォルトのクラスマップで照合されます。
ILS（LDAP）	TCP/389	PAT はサポートされません。	—	—
MGCP	UDP/2427、2727	—	RFC 2705bis-05	—
NetBIOS Name Server over IP	UDP/137、138（送信元ポート）	—	—	NetBIOS は、NBNS UDP ポート 137 と NBDS UDP ポート 138 に対するパケットの NAT を行うことでサポートされます。
PPTP	TCP/1723	—	RFC 2637	—
RADIUS Accounting	1646	—	RFC 2865	—
RSH	TCP/514	PAT はサポートされません。	Berkeley UNIX	—
RTSP	TCP/554	PAT はサポートされません。 外部 NAT はサポートされません。	RFC 2326、2327、1889	HTTP クローキングの処理は行われません。

表 24-1　サポートされているアプリケーション検査エンジン（続き）

アプリケーション[1]	デフォルト ポート	NAT の制約事項	標準[2]	コメント
SIP	TCP/5060 UDP/5060	外部 NAT はサポートされません。 同一セキュリティ インターフェイス上の NAT はサポートされません。	RFC 2543	—
SKINNY（SCCP）	TCP/2000	外部 NAT はサポートされません。 同一セキュリティ インターフェイス上の NAT はサポートされません。	—	一定の条件下では、TFTP でアップロードされた Cisco IP Phone コンフィギュレーションの処理は行われません。
SMTP および **ESMTP**	TCP/25	—	RFC 821、1123	—
SNMP	UDP/161、162	NAT および PAT はサポートされません。	RFC 1155、1157、1212、1213、1215	v.2 RFC 1902 ～ 1908、v.3 RFC 2570 ～ 2580
SQL*Net	TCP/1521	—	—	v.1 および v.2
Sun RPC over UDP および TCP	UDP/111	NAT および PAT はサポートされません。	—	デフォルトのルールには UDP ポート 111 が含まれています。TCP ポート 111 の Sun RPC 検査をイネーブルにする場合は、TCP ポート 111 を照合する新しいルールを作成し、Sun RPC 検査を実行する必要があります。
TFTP	UDP/69	—	RFC 1350	ペイロード IP アドレスは変換されません。
XDCMP	UDP/177	NAT および PAT はサポートされません。	—	—

1. デフォルト ポートに対してデフォルトでイネーブルになっている検査エンジンは太字で表記されています。
2. セキュリティ アプライアンスは、これらの標準に準拠していますが、検査対象のパケットには準拠を強制しません。たとえば、各 FTP コマンドは特定の順序である必要がありますが、セキュリティ アプライアンスによってその順序を強制されることはありません。

アプリケーション検査の設定

この機能では、サービス ポリシー ルールを使用します。サービス ポリシーを使用すると、一貫した柔軟な方法でセキュリティ アプライアンスの機能を設定できます。たとえば、サービス ポリシーを使用すると、すべての TCP アプリケーションに適用されるルールではなく、特定の TCP アプリケーションに固有のタイムアウト コンフィギュレーションを作成できます。詳細については、第 23 章「サービス ポリシー ルールの設定」を参照してください。

一部のアプリケーションでは、デフォルトで検査がイネーブルになっています。詳細については、「デフォルトの検査ポリシー」を参照してください。この項を参照して検査ポリシーを変更してください。

アプリケーション検査を設定するには、次の手順を実行します。

ステップ 1　**Configuration > Firewall > Service Policy Rules** をクリックします。

ステップ 2　P.23-5 の「通過トラフィックのサービス ポリシー ルールの追加」を参照して、サービス ポリシー ルールを追加または編集します。

標準以外のポートを照合する場合は、非標準ポート用の新しいルールを作成します。各検査エンジンの標準ポートについては、P.24-3 の「デフォルトの検査ポリシー」を参照してください。必要に応じて同じサービス ポリシー内に複数のルールを組み合せることができるため、照合するトラフィックに応じたルールを作成できます。ただし、トラフィックが検査アクションを含むルールと一致し、その後同様に検査アクションを含む別のルールとも一致した場合、最初に一致したルールだけが使用されます。

ステップ 3　Edit Service Policy Rule > Rule Actions ダイアログボックスで、**Protocol Inspection** タブをクリックします。

新しいルールの場合、Add Service Policy Rule Wizard - Rule Actions というダイアログボックス名が表示されます。

ステップ 4　適用する各検査タイプをオンにします。

ステップ 5　（オプション）一部の検査エンジンでは、トラフィックに検査を適用するときの追加パラメータを制御できます。検査マップを設定するには、各検査タイプの **Configure** をクリックします。

既存のマップを選択することも、新しいマップを作成することもできます。Configuration > Firewall > Objects > Inspect Maps ペインから、検査マップを事前に定義できます。各検査マップ タイプの詳細については、P.24-61 の「検査マップのフィールドの説明」を参照してください。

ステップ 6　必要に応じて、他の Rule Actions タブを使用し、このルールに対して他の機能を設定できます。

ステップ 7　**OK** をクリックします（またはウィザードで **Finish** をクリックします）。

CTIQBE 検査

この項では、CTIQBE アプリケーション検査について説明します。ここでは、次の項目について説明します。

CTIQBE 検査の概要

CTIQBE プロトコル検査では、NAT、PAT、および双方向 NAT がサポートされます。これによって、Cisco IP SoftPhone と他の Cisco TAPI/JTAPI アプリケーションが Cisco CallManager と連動し、セキュリティ アプライアンスを越えてコール セットアップを行うことができるようになります。

TAPI と JTAPI は、多くの Cisco VoIP アプリケーションで使用されます。CTIQBE は、Cisco TSP が Cisco CallManager と通信するために使用されます。

制約事項

CTIQBE アプリケーション検査を使用する場合、次の制約事項が適用されます。

- CTIQBE アプリケーション検査は、**alias** コマンドを使用するコンフィギュレーションをサポートしません。
- CTIQBE コールのステートフル フェールオーバーはサポートされません。
- **debug ctiqbe** コマンドを入力すると、メッセージの伝送が遅れる場合があり、リアルタイム環境のパフォーマンスに影響を与えることがあります。このデバッグまたはロギングをイネーブルにしたことで、Cisco IP SoftPhone がセキュリティ アプライアンスを介したコール セットアップを完了できないと考えられる場合は、Cisco IP SoftPhone が動作するシステムで Cisco TSP 設定のタイムアウト値を増やしてください。

CTIQBE アプリケーション検査を特定のシナリオで使用する場合に、特に注意が必要な考慮事項を次にまとめます。

- 2 つの Cisco IP SoftPhone が異なる Cisco CallManager に登録されていて、各 CallManager がセキュリティ アプライアンスの異なるインターフェイスに接続されている場合、これら 2 つの電話間のコールは失敗します。
- Cisco CallManager が Cisco IP SoftPhone よりもセキュリティの高いインターフェイス上にある状態で、NAT または外部 NAT が Cisco CallManager の IP アドレスに必要な場合、マッピングはスタティックである必要があります。これは、Cisco IP SoftPhone では Cisco CallManager の IP アドレスを PC 上の Cisco TSP コンフィギュレーションで明示的に指定することが必要なためです。
- PAT または外部 PAT を使用しているときに Cisco CallManager の IP アドレスを変換する場合、Cisco IP SoftPhone を正常に登録するには、TCP ポート 2748 を PAT（インターフェイス）アドレスの同一ポートに対してスタティックにマッピングする必要があります。CTIQBE リスニング ポート（TCP 2748）は固定されていて、Cisco CallManager、Cisco IP SoftPhone、Cisco TSP のいずれでもユーザは設定を行うことはできません。

DCERPC 検査

DCERPC は、Microsoft のクライアント / サーバ アプリケーションで広く使われているプロトコルです。このプロトコルによって、ソフトウェア クライアントがサーバにあるプログラムをリモートで実行できるようになります。

通常、このプロトコルの接続では、クライアントがウェルノウン 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のインスタンスへのセカンダリ接続を確立します。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 を行います。

DCERPC 検査マップは、TCP のウェルノウン ポート 135 を経由した、EPM とクライアント間のネイティブ TCP の通信を検査します。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は、どのセキュリティ ゾーンにあってもかまいません。サーバの埋め込まれた 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のポート番号で複数の接続を確立する可能性があるので、ピンホールを複数使用でき、ユーザがそのタイムアウトを設定できるようになっています。

DNS 検査

この項では、DNS アプリケーション検査について説明します。ここでは、次の項目について説明します。

DNS アプリケーション検査の動作

セキュリティ アプライアンスは、DNS 応答を転送するとすぐに DNS クエリーに関連付けられた DNS セッションを切断します。また、メッセージ交換を監視して、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。

DNS 検査をイネーブルにすると（デフォルトはイネーブル）、セキュリティ アプライアンスは次の追加のタスクを実行します。

- NAT ルールを使用して作成されたコンフィギュレーションに基づいて DNS レコードを変換します。変換は、DNS 応答の A レコードにだけ適用されるため、PTR レコードを必要とする逆ルックアップが DNS リライトによって影響を受けることはありません。

（注）　DNS リライトは PAT には適用できません。これは、1 つの A レコードに複数の PAT ルールが適用可能で、使用する PAT ルールがあいまいになるためです。

- 最大 DNS メッセージ長（デフォルトは 512 バイト、最大長は 65535 バイト）を適用します。セキュリティ アプライアンスは必要に応じてリアセンブリを実行し、パケット長が設定されている最大長よりも短いことを確認します。最大長を超えるパケットはドロップされます。
- ドメイン名の長さを 255 バイトに、ラベルの長さを 63 バイトに制限します。
- DNS メッセージ内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存在するかどうか確認します。

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（送信元および宛先 IP アドレス、送信元および宛先ポート、プロトコル）が同じである場合、それらのセッションに対して接続が 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のみであり、リソースの継続使用はできません。ただし、**show conn** コマンドを入力すると、新しい DNS セッションによってリセットされた 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 リライトの動作

DNS 検査がイネーブルの場合、DNS リライトは、任意のインターフェイスから送信された DNS メッセージの NAT を完全にサポートします。

内部ネットワーク上のクライアントが、外部インターフェイス上の DNS サーバから送信される内部アドレスの DNS 解決を要求した場合、DNS A レコードは正しく変換されます。DNS 検査エンジンがディセーブルの場合、A レコードは変換されません。

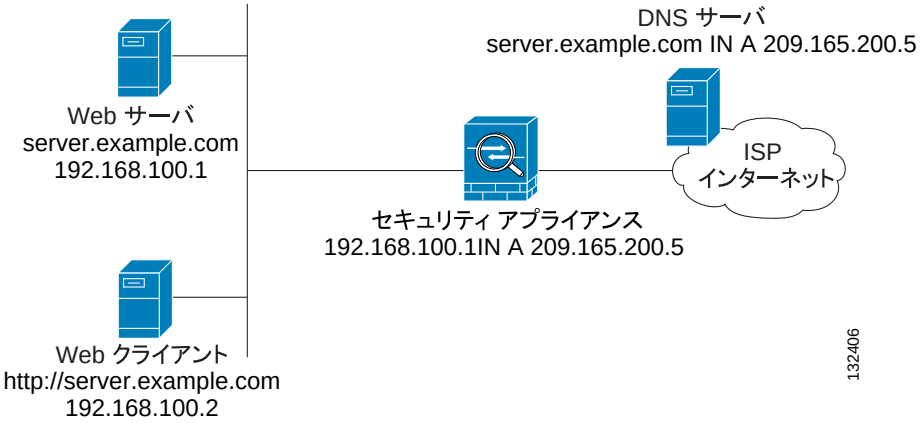
DNS 検査がイネーブルであれば、NAT ルールを使用して DNS リライトを設定できます。

DNS リライトは次の 2 つの機能を実行します。

- DNS クライアントがプライベート インターフェイスにある場合、DNS 応答のパブリック アドレス（ルーティング可能なアドレスまたは「マッピング」アドレス）をプライベート アドレス（「実際の」アドレス）に変換します。
- DNS クライアントがパブリック インターフェイスにある場合、プライベート アドレスをパブリック アドレスに変換します。

図 24-1 では、DNS サーバは外部（ISP）ネットワークにあります。サーバの実際のアドレス（192.168.100.1）は、スタティック NAT ルールを使用して ISP が割り当てるアドレス（209.165.200.5）にマッピングされています。内部インターフェイスの Web クライアントが http://server.example.com という URL を持つ Web サーバにアクセスしようとすると、Web クライアントが動作するホストが、Web サーバの IP アドレスの解決を求める DNS 要求を DNS サーバに送信します。セキュリティ アプライアンスは、IP ヘッダーに含まれるルーティング不可の送信元アドレスを変換し、外部インターフェイスの ISP ネットワークに要求を転送します。DNS 応答が返されると、セキュリティ アプライアンスはアドレス変換を宛先アドレスだけではなく、DNS 応答の A レコードに含まれている、Web サーバの埋め込み IP アドレスにも適用します。結果として、内部ネットワーク上の Web クライアントは、内部ネットワーク上の Web サーバと接続するための正しいアドレスを取得します。

図 24-1　DNS 応答に含まれるアドレスの変換（DNS リライト）



DNS リライトは、DNS 要求を行うクライアントが DMZ ネットワークにあり、DNS サーバが内部インターフェイスにある場合にも機能します。

ESMTP 検査

ESMTP 検査は、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、送受信者およびメール中継のブロックも行います。

FTP 検査

この項では、FTP 検査エンジンについて説明します。ここでは、次の項目について説明します。

FTP 検査の概要

FTP アプリケーション検査は、FTP セッションを検査し、次の 4 つのタスクを実行します。

- ダイナミックなセカンダリ データ接続の準備
- FTP コマンドと応答のシーケンスの追跡
- 監査証跡の生成
- 埋め込み IP アドレスの変換

FTP アプリケーション検査は、FTP データ転送用にセカンダリ チャネルを用意します。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 イベント、ファイル ダウンロード イベント、またはディレクトリ リスト イベントに応答して割り当てられます。

（注） FTP 検査エンジ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 の使用方法

strict オプションにより厳密な 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** をクリックします。

（注） セキュリティ アプライアンスの通過を禁止する FTP コマンドを指定するには、P.24-47 の「FTP Class Map」に従って FTP 検査マップを作成します。

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 検査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、セキュリティ アプライアンスは新しいコマンドを許可しません。
- セキュリティ アプライアンスは、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 コマンドを、エラー文字列に表示されないようにチェックします。

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 応答コマンド内のカンマの数が 5 であるかどうかをチェックします。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し、TCP 接続を閉じます。
- 不正なコマンド：FTP コマンドが、RFC の要求通りに <CR><LF> 文字で終了しているかどうかをチェックします。この文字で終了していない場合は、接続を閉じます。
- RETR コマンドと STOR コマンドのサイズ：固定の定数と照合します。サイズが定数より大きい場合は、エラーメッセージをログに記録し、接続を閉じます。
- 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る必要があります。PORT コマンドがサーバから送信されている場合、TCP 接続を拒否します。
- 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る必要があります。PASV 応答コマンドがクライアントから送信されている場合、TCP 接続を拒否します。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 ホールを予防できます。
- TCP ストリーム編集：セキュリティ アプライアンスは、TCP ストリーム編集を検出した場合に接続を閉じます。
- 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をチェックします。1 ～ 1024 の範囲のポート番号はウェルノウン接続用に予約されているため、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 接続を解放します。
- 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を、定数の 8 と比較します。8 より大きい場合は、TCP 接続を閉じます。
- 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、セキュリティ アプライアンスは、SYST コマンドに対する FTP サーバ応答を連続する X で置き換えます。このデフォルトの動作を無効にするには、FTP マップで Low 設定を使用します。

FTP 検査の確認と監視

FTP アプリケーション検査は、次のログメッセージを生成します。

- An Audit record 302002 is generated for each file that is retrieved or uploaded.
- The FTP command is checked to see if it is RETR or STOR and the retrieve and store commands are logged.
- The username is obtained by looking up a table providing the IP address.
- The username, source IP address, destination IP address, NAT address, and the file operation are logged.
- Audit record 201005 is generated if the secondary dynamic channel preparation failed due to memory shortage.

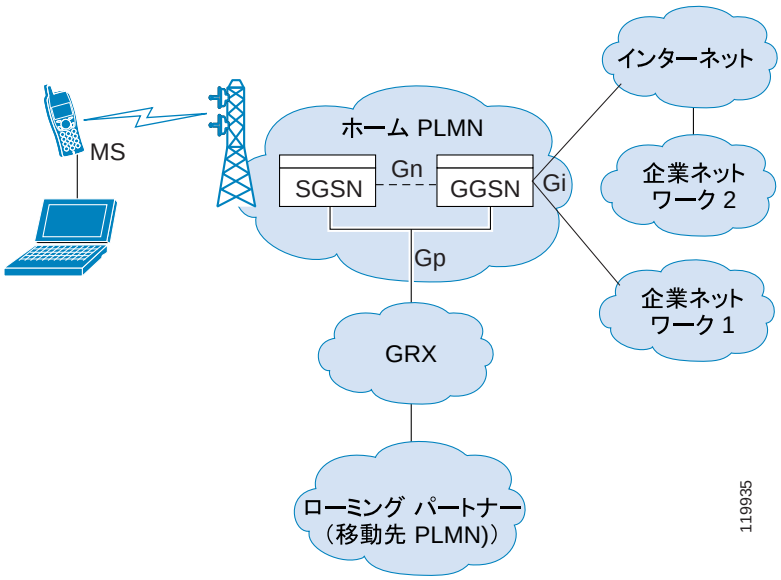
FTP アプリケーション検査は、NAT と連携して、アプリケーション ペイロード内の IP アドレスを変換します。これは、RFC 959 に詳細に記述されています。

GTP 検査

（注）　GTP 検査には、特別なライセンスが必要です。

GPRS は、モバイル加入者に対して、GSM ネットワークと企業ネットワークまたはインターネットとの間で中断のない接続を提供します。GGSN は、GPRS 無線データ ネットワークと他のネットワークとの間のインターフェイスです。SGSN は、モビリティ、データ セッション管理、およびデータ圧縮を実行します（図 24-2 を参照）。

図 24-2　GPRS トンネリング プロトコル



UMTS は、固定回線テレフォニー、モバイル、インターネット、コンピュータ テクノロジーの商用コンバージェンスです。UTRAN は、このシステムで無線ネットワークを実装するためのネットワーキング プロトコルです。GTP を使用すると、GGSN、SGSN、および UTRAN 間の UMTS/GPRS バックボーンで、マルチプロトコル パケットをトンネリングできます。

GTP には固有のセキュリティやユーザ データの暗号化は含まれていませんが、セキュリティ アプライアンスで GTP を使用すると、これらのリスクからネットワークを保護できます。

SGSN は、GTP を使用して GGSN に論理的に接続されます。GTP を使用すると、GSN 間の GPRS バックボーンで、マルチプロトコル パケットをトンネリングできます。GTP は、トンネル制御および管理プロトコルを提供します。このプロトコルによって、SGSN は、トンネルの作成、変更、および削除を行い、モバイル ステーションに GPRS ネットワーク アクセスを提供できます。GTP は、トンネリング メカニズムを使用して、ユーザ データ パケットを伝送するためのサービスを提供します。

（注）　GTP をフェールオーバーと一緒に使用する場合、GTP 接続が確立されて、データがトンネルを通って伝送される前にアクティブ装置に障害が発生すると、GTP データ接続（「j」フラグが設定された状態）は、スタンバイ装置に複製されません。これは、アクティブ装置は初期接続をスタンバイ装置に複製しないためです。

H.323 検査

この項では、H.323 アプリケーション検査について説明します。ここでは、次の項目について説明します。

H.323 検査の概要

H.323 検査は、Cisco CallManager や VocalTec Gatekeeper など、H.323 準拠のアプリケーションをサポートします。H.323 は、International Telecommunication Union（ITU; 国際電気通信連合）によって定義された、LAN を介したマルチメディア会議用のプロトコル群です。セキュリティ アプライアンスは、H.323 v3 機能である同一コール シグナリング チャネルでの複数コールを含む、Version 4 までの H.323 をサポートします。

H.323 検査をイネーブルにすると、セキュリティ アプライアンスは、H.323 Version 3 で導入された機能である、同一コール シグナリング チャネルでの複数コールをサポートします。この機能によってコール セットアップ時間が短縮され、セキュリティ アプライアンスでのポートの使用が減少します。

H.323 検査には、次の 2 つの主要な機能があります。

- H.225 および H.245 メッセージ内の必要な埋め込み IPv4 アドレスに対して NAT を実行します。H.323 メッセージは PER エンコード形式でエンコードされているため、セキュリティ アプライアンスは ASN.1 デコーダを使用して H.323 メッセージをデコードします。
- ネゴシエートされた H.245 と RTP/RTCP 接続をダイナミックに割り当てます。

H.323 の動作

H.323 のプロトコルのコレクションは、合計で最大 2 つの TCP 接続と 4 ～ 6 つの UDP 接続を使用できます。FastConnect は TCP 接続を 1 つだけ使用し、RAS は登録、アドミッション、およびステータス用に UDP 接続を 1 つ使用します。

H.323 クライアントは、最初に TCP ポート 1720 を使用して H.323 サーバへの TCP 接続を確立し、Q.931 コール セットアップを要求する場合があります。H.323 端末は、コール セットアップ プロセスの一部として、H.245 TCP 接続に使用するためのポート番号を 1 つクライアントに供給します。H.323 ゲートキーパーが使用されている環境では、初期パケットは UDP を使用して送信されます。

H.323 検査は、Q.931 TCP 接続を監視して、H.245 ポート番号を決定します。H.323 端末が FastConnect を使用しない場合、セキュリティ アプライアンスが H.225 メッセージの検査に基づいて、H.245 接続をダイナミックに割り当てます。

各 H.245 メッセージ内で、H.323 エンドポイントが、後続の UDP データ ストリームに使用するポート番号を交換します。H.323 検査は、H.245 メッセージを検査してこれらのポートを識別し、メディア交換用の接続をダイナミックに作成します。RTP はネゴシエートされたポート番号を使用し、RTCP はその次に高いポート番号を使用します。

H.323 制御チャネルは、H.225、H.245、および H.323 RAS を処理します。H.323 検査では、次のポートが使用されます。

- 1718：ゲートキーパー検出 UDP ポート
- 1719：RAS UDP ポート
- 1720：TCP 制御ポート

H.225 コール シグナリング用にウェルノウン H.323 ポート 1720 のトラフィックを許可する必要があります。ただし、H.245 シグナリング ポートは、H.225 シグナリングのエンドポイント間でネゴシエートされます。H.323 ゲートキーパーの使用時、セキュリティ アプライアンスは、ACF メッセージの検査に基づいて H.225 接続を開きます。

H.225 メッセージを検査した後、セキュリティ アプライアンスは H.245 チャネルを開き、H.245 チャネルで送信されるトラフィックも検査します。セキュリティ アプライアンスを通過するすべての H.245 メッセージは、H.245 アプリケーション検査を受けます。この検査では、埋め込み IP アドレスが変換され、H.245 メッセージでネゴシエートされたメディア チャネルが開かれます。

H.323 ITU 規格では、メッセージ長を定義する TPKT ヘッダーを最初に送信してから、H.225 と H.245 を信頼できる接続に送信することを要求しています。TPKT ヘッダーは、必ずしも H.225 メッセージや H.245 メッセージと同じ TCP パケット内で送信される必要はないため、セキュリティ アプライアンスは、メッセージを正しく処理してデコードするために TPKT 長を記憶しておく必要があります。セキュリティ アプライアンスは、次のメッセージに備えて、TPKT 長が保存されたレコードを接続ごとに保持します。

セキュリティ アプライアンスでメッセージ内の IP アドレスに NAT を行う必要がある場合、チェックサム、UUIE 長、および TPKT（H.225 メッセージが入っている TCP パケットに含まれている場合）は変更されます。TPKT が別の TCP パケットで送信される場合、セキュリティ アプライアンスがその TPKT へのプロキシ ACK を実行し、新しい TPKT を新しい長さで H.245 メッセージに追加します。

（注） セキュリティ アプライアンスは、TPKT に対するプロキシ ACK では TCP オプションをサポートしていません。

H.323 検査を受けるパケットが通る各 UDP 接続は、H.323 接続としてマークされ、Configuration > Firewall > Advanced > Global Timeouts ペインで設定された H.323 タイムアウト値でタイムアウトします。

制約事項

H.323 アプリケーション検査を使用する場合、次の既知の問題および制約事項があります。

- スタティック PAT は、H.323 メッセージのオプション フィールドに埋め込まれた IP アドレスを正しく変換できないことがあります。この種の問題が発生した場合は、H.323 でスタティック PAT を使用しないでください。
- H.323 アプリケーション検査は、同一セキュリティ レベルのインターフェイス間の NAT ではサポートされていません。
- NetMeeting クライアントが H.323 ゲートキーパーに登録し、同じく H.323 ゲートキーパーに登録されている H.323 ゲートウェイを呼び出そうとすると、接続は確立されますが、どちらの方向でも音声が聞こえません。この問題は、セキュリティ アプライアンスの問題ではありません。
- ネットワーク スタティック アドレスを設定した場合、このネットワーク スタティック アドレスが第三者のネットマスクおよびアドレスと同じであると、すべての発信 H.323 接続が失敗します。

HTTP 検査

HTTP 検査エンジンを使用して、特定の攻撃、および HTTP トラフィックに関係している可能性があるその他の脅威から保護します。HTTP 検査は、次の機能を実行します。

- 拡張 HTTP 検査
- N2H2 または Websense を使用した URL スクリーニング
- Java および ActiveX のフィルタリング

2 つ目と 3 つ目の機能は、フィルタ ルールと共に設定します。

拡張 HTTP 検査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 検査マップを設定すると使用できます（P.24-51 の「HTTP Class Map」を参照）。この機能を使用すると、攻撃者が HTTP メッセージを使用してネットワーク セキュリティ ポリシーを回避することを阻止できます。この機能は、すべての HTTP メッセージの次の点について確認します。

- 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

インスタント メッセージ検査

インスタント メッセージ（IM）検査エンジンを使用すると、IM アプリケーションの制御を細かく調整して、ネットワークの使用を制御し、機密情報の漏洩やワームの繁殖など企業のネットワークへの脅威を阻止できます。

ICMP 検査

ICMP 検査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できるようになります。ICMP 検査エンジンを使用しない場合、アクセスリストで ICMP にセキュリティ アプライアンスの通過を許可しないことをお勧めします。ステートフル検査を実行しないと、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 検査エンジンは、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。

ICMP エラー検査

この機能がイネーブルの場合、セキュリティ アプライアンスは、NAT コンフィギュレーションに基づいて 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。セキュリティ アプライアンスは、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、セキュリティ アプライアンスは、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。内部ホストとセキュリティ アプライアンス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セキュリティ アプライアンスの内部にある宛先までのホップをトレースする場合、これは望ましくありません。セキュリティ アプライアンス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 アドレスと共に表示されます。

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 エラー検査エンジンは、ICMP パケットに対して次の変更を加えます。

- IP ヘッダー内で、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。

ILS 検査

ILS 検査エンジンは、LDAP を使用してディレクトリ情報を ILS サーバと交換する 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。

セキュリティ アプライアンスは ILS に対して NAT をサポートします。NAT は、ILS または SiteServer Directory のエンドポイントの登録および検索で使用されます。LDAP データベースには IP アドレスだけが保存されるため、PAT はサポートされません。

LDAP サーバが外部にある場合、内部ピアが外部 LDAP サーバ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 を行うことを検討してください。このような検索応答では、最初に xlate が検索され、次に DNAT エントリが検索されて正しいアドレスが取得されます。これらの検索が両方とも失敗した場合、アドレスは変更されません。NAT 0（NAT なし）を使用していて、DNAT の相互作用を想定していないサイトの場合は、パフォーマンスを向上させるために検査エンジンをオフにすることをお勧めします。

ILS サーバがセキュリティ アプライアンス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、指定されたポート（通常は TCP 389）の LDAP サーバに外部クライアントがアクセスするためのホールが必要となります。

ILS トラフィックはセカンダリ UDP チャネルだけで発生するため、TCP 接続は一定の間隔で TCP アクティビティがなければ切断されます。デフォルトでは、この間隔は 60 分です。この値は、Configuration > Firewall > Advanced > Global Timeouts ペインで設定できます。

ILS/LDAP はクライアント / サーバ モデルに従っており、セッションは 1 つの TCP 接続で処理されます。クライアントのアクションに応じて、このようなセッションがいくつか作成されることがあります。

接続ネゴシエーション時間中、クライアントからサーバに BIND PDU が送信されます。成功を示す BIND RESPONSE をサーバから受信すると、ILS Directory に対する操作を実行するためのその他の操作メッセージ（ADD、DEL、SEARCH、MODIFY など）が交換される場合があります。ADD REQUEST PDU および SEARCH RESPONSE PDU には、NetMeeting セッションを確立するために H.323（SETUP および CONNECT メッセージ）によって使用される、NetMeeting ピアの IP アドレスが含まれている場合があります。Microsoft NetMeeting v2.X および v3.X は、ILS をサポートしています。

ILS 検査では、次の操作が実行されます。

- BER デコード機能を使用して LDAP REQUEST PDU/RESPONSE PDU をデコードする。
- LDAP パケットを解析する。
- IP アドレスを抽出する。
- 必要に応じて IP アドレスを変換する。
- BER エンコード機能を使用して、変換されたアドレスが含まれる PDU をエンコードする。
- 新しくエンコードされた PDU を元の TCP パケットにコピーする。
- TCP チェックサムとシーケンス番号の増分を調整する。

ILS 検査には、次の制約事項があります。

- 参照要求および応答はサポートされません。
- 複数のディレクトリ内のユーザは統合されません。
- 1 人のユーザが複数のディレクトリで複数の ID を持つ場合、NAT はそのユーザを認識できません。

（注）　H225 コール シグナリング トラフィックはセカンダリ UDP チャネルだけで発生するため、Configuration > Firewall > Advanced > Global Timeouts ペインの TCP オプションで指定された間隔が経過すると、TCP 接続は切断されます。デフォルトでは、この間隔は 60 分に設定されています。

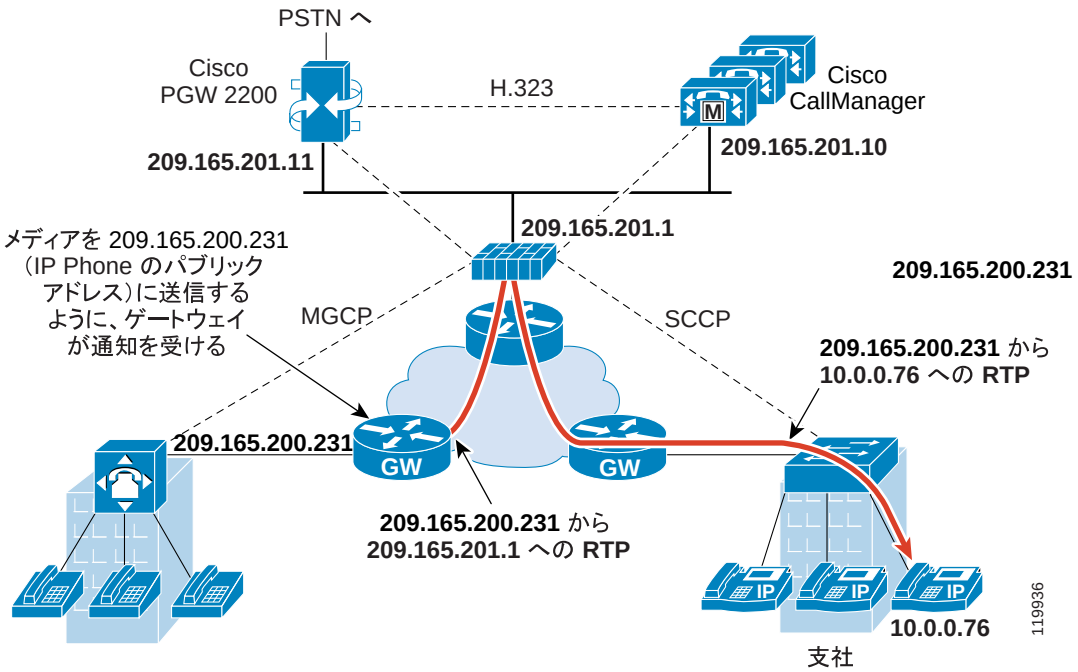
MGCP 検査

MGCP は、メディア ゲートウェイ コントローラまたはコール エージェントと呼ばれる外部のコール制御要素からメディア ゲートウェイを制御するために使用されるマスター/スレーブ プロトコルです。メディア ゲートウェイは一般に、電話回線を通じた音声信号と、インターネットまたは他のパケット ネットワークを通じたデータ パケットとの間の変換を行うネットワーク要素です。NAT および PAT を MGCP と一緒に使用すると、限られた外部（グローバル）アドレスのセットで、内部ネットワークにある多くのデバイスをサポートできます。メディア ゲートウェイには、次のものがあります。

- トランキング ゲートウェイ。電話ネットワークと Voice over IP ネットワークとの間のインターフェイスです。このようなゲートウェイは通常、大量のデジタル回線を管理します。
- 住宅用ゲートウェイ。従来のアナログ（RJ11）インターフェイスを Voice over IP ネットワークに提供します。住宅用ゲートウェイの例としては、ケーブル モデムやケーブル セットトップ ボックス、xDSL デバイス、ブロードバンド無線デバイスなどがあります。
- ビジネス ゲートウェイ。従来のデジタル PBX インターフェイスまたは統合 soft PBX インターフェイスを Voice over IP ネットワークに提供します。

MGCP メッセージは UDP を介して送信されます。応答はコマンドの送信元アドレス（IP アドレスと UDP ポート番号）に返送されますが、コマンド送信先と同じアドレスからの応答は到達しない場合があります。これは、複数のコール エージェントがフェールオーバー コンフィギュレーションで使用されているときに、コマンドを受信したコール エージェントが制御をバックアップ コール エージェントに引き渡し、バックアップ コール エージェントが応答を送信する場合に起こる可能性があります。図 24-3 に、MGCP でどのように NAT が使用されるかを示します。

図 24-3　MGCP での NAT の使用方法



MGCP エンドポイントは、物理または仮想のデータ送信元および宛先です。メディア ゲートウェイには、他のマルチメディア エンドポイントとのメディア セッションを確立して制御するために、コール エージェントが接続を作成、変更、および削除できるエンドポイントが含まれています。また、コール エージェントは、特定のイベントを検出してシグナルを生成するようにエンドポイントに指示できます。エンドポイントは、サービス状態の変化を自動的にコール エージェントに伝達します。

MGCP トランザクションは、コマンドと必須応答で構成されます。次の 8 種類のコマンドがあります。

- CreateConnection
- ModifyConnection
- DeleteConnection
- NotificationRequest
- Notify
- AuditEndpoint
- AuditConnection
- RestartInProgress

最初の 4 つのコマンドは、コール エージェントからゲートウェイに送信されます。Notify コマンドは、ゲートウェイからコール エージェントに送信されます。ゲートウェイは DeleteConnection を送信することもあります。 MGCP ゲートウェイをコール エージェントに登録するには、RestartInProgress コマンドを使用します。AuditEndpoint コマンドと AuditConnection コマンドは、コール エージェントからゲートウェイに送信されます。

すべてのコマンドは、コマンド ヘッダーと、その後に続くオプションのセッション記述で構成されます。すべての応答は、応答ヘッダーと、その後に続くオプションのセッション記述で構成されます。

- ゲートウェイがコール エージェントからのコマンドを受信するポート。通常、ゲートウェイは UDP ポート 2427 をリスンします。
- コール エージェントがゲートウェイからのコマンドを受信するポート。通常、コールエージェントは UDP ポート 2727 をリスンします。

（注） MGCP 検査では、MGCP シグナリングと RTP データで異なる IP アドレスを使用することはサポートされていません。一般的かつ推奨される方法は、ループバック IP アドレスや仮想 IP アドレスなどの回復力のある IP アドレスから RTP データを送信することです。ただし、セキュリティ アプライアンスは、MGCP シグナリングと同じアドレスから RTP データを受信する必要があります。

NetBIOS 検査

NetBIOS 検査はデフォルトでイネーブルになっています。NetBios 検査エンジンは、セキュリティ アプライアンスの NAT コンフィギュレーションに基づいて、NetBios Name Service（NBNS; NetBios ネーム サービス）パケット内の IP アドレスを変換します。

PPTP 検査

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 アプリケーション検査は、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。RFC 2637 で定義されているバージョン 1 だけがサポートされます。

PAT は、PPTP TCP 制御チャネル上で修正バージョンの GRE（RFC 2637）がネゴシエートされたときに、その GRE に対してのみ実行されます。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。

具体的には、セキュリティ アプライアンスは、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の後の検査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 検査エンジンは、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 に対してのみ実行されます。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。

RFC 2637 で定義されているように、PPTP プロトコルは主に、モデム バンク PPTP Access Concentrator（PAC; PPTP アクセス コンセントレータ）から開始されたヘッドエンド PPTP Network Server（PNS; PPTP ネットワーク サーバ）への PPP セッションのトンネリングに使用されます。このように使用された場合、PAC がリモート クライアントで PNS がサーバです。

ただし、Windows によって VPN で使用された場合、この関係は逆になります。PNS は、中央のネットワークにアクセスするためにヘッドエンド PAC への接続を開始する、リモートの単一ユーザ PC です。

RADIUS アカウンティング検査

RADIUS アカウンティング検査の詳細については、P.23-14 の「Select RADIUS Accounting Map」を参照してください。

RSH 検査

RSH 検査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 サーバへの TCP 接続を使用します。クライアントとサーバは、クライアントが STDERR 出力ストリームをリスンする TCP ポート番号をネゴシエートします。RSH 検査は、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。

RTSP 検査

この項では、RTSP アプリケーション検査について説明します。ここでは、次の項目について説明します。

RTSP 検査の概要

RTSP 検査エンジンを使用することにより、セキュリティ アプライアンスは RTSP パケットを通過させることができます。RTSP は、RealAudio、RealNetworks、Apple QuickTime 4、RealPlayer、および Cisco IP/TV 接続で使用されます。

（注）　Cisco IP/TV には、RTSP TCP ポート 554 と TCP 8554 を使用してください。

RTSP アプリケーションは、制御チャネルとして TCP（まれに UDP）でウェルノウン ポート 554 を使用します。セキュリティ アプライアンスは、RFC 2326 に準拠して、TCP だけをサポートします。この TCP 制御チャネルは、クライアント上に設定されている転送モードに応じて、音声 / ビデオ トラフィックの送信に使用されるデータ チャネルのネゴシエーションに使用されます。

サポートされている RDT 転送は、rtp/avp、rtp/avp/udp、x-real-rdt、x-real-rdt/udp、x-pn-tng/udp です。

セキュリティ アプライアンスは、ステータス コード 200 の Setup 応答メッセージを解析します。応答メッセージが着信である場合、サーバはセキュリティ アプライアンスから見て外部に存在することになるため、サーバから着信する接続に対してダイナミック チャネルを開く必要があります。この応答メッセージが発信である場合、セキュリティ アプライアンスがダイナミック チャネルを開く必要はありません。

RFC 2326 では、クライアント ポートとサーバ ポートが SETUP 応答メッセージに含まれていることが必須ではないため、セキュリティ アプライアンスは、状態を保持し、SETUP メッセージ内のクライアント ポートを記憶します。QuickTime が、SETUP メッセージ内にクライアント ポートを設定すると、サーバはサーバ ポートだけで応答します。

RTSP 検査は、PAT またはデュアル NAT をサポートしていません。また、セキュリティ アプライアンスは、RTSP メッセージが HTTP メッセージ内に隠される HTTP クローキングを認識できません。

RealPlayer の使用方法

RealPlayer を使用する場合は、転送モードを正しく設定することが重要です。セキュリティ アプライアンスの場合、サーバからクライアントに、またはその逆にアクセス ルールを追加します。RealPlayer の場合、**Options** > **Preferences** > **Transport** > **RTSP Settings** をクリックして転送モードを変更します。

RealPlayer で TCP モードを使用する場合は、**Use TCP to Connect to Server** チェックボックスおよび **Attempt to use TCP for all content** チェックボックスをオンにします。セキュリティ アプライアンス上に検査エンジンを設定する必要はありません。

RealPlayer で UDP モードを使用する場合、**Use TCP to Connect to Server** チェックボックスおよび **Attempt to use UDP for static content, and for live content not available via Multicast** チェックボックスをオンにします。セキュリティ アプライアンスで、**inspect rtsp** *port* コマンドを追加します。

制約事項

RTSP 検査には、次の制約事項が適用されます。

- セキュリティ アプライアンスは、マルチキャスト RTSP または UDP 経由の RTSP メッセージをサポートしません。
- PAT はサポートされていません。
- セキュリティ アプライアンスは、RTSP メッセージが HTTP メッセージ内に隠されている HTTP クローキングを認識できません。
- 埋め込み IP アドレスが HTTP メッセージまたは RTSP メッセージの一部として SDP ファイル内に含まれているため、セキュリティ アプライアンスは、RTSP メッセージに NAT を実行できません。パケットはフラグメント化する可能性があり、セキュリティ アプライアンスはフラグメント化されたパケットに対して NAT を実行できません。
- Cisco IP/TV では、メッセージの SDP 部分に対してセキュリティ アプライアンスが実行する変換の数は、Content Manager にあるプログラム リストの数に比例します（各プログラム リストには、少なくとも 6 個の埋め込み IP アドレスを含めることができます）。
- Apple QuickTime 4 または RealPlayer に NAT を設定できます。Cisco IP/TV は、ビューアと Content Manager が外部ネットワークにあり、サーバが内部ネットワークにあるときだけ NAT を使用できます。

SIP 検査

この項では、SIP アプリケーション検査について説明します。ここでは、次の項目について説明します。

SIP 検査の概要

SIP は、IETF で定義されているように、特に 2 者間の音声会議などのコール処理セッション、つまり「コール」を使用できるようにします。SIP は、コール シグナリング用の SDP で動作します。SDP は、メディア ストリーム用のポートを指定します。SIP を使用することにより、セキュリティ アプライアンスは SIP VoIP ゲートウェイおよび VoIP プロキシ サーバをサポートできます。SIP と SDP は、次の RFC で定義されています。

- SIP：Session Initiation Protocol、RFC 2543
- SDP：Session Description Protocol、RFC 2327

セキュリティ アプライアンスを通過する SIP コールをサポートするには、メディア接続アドレスのシグナリング メッセージ、メディア ポート、およびメディアの初期接続を検査する必要があります。これは、シグナリングがウェルノウン宛先ポート（UDP/TCP 5060）経由で送信される一方で、メディア ストリームはダイナミックに割り当てられるためです。また、SIP は、IP パケットのユーザ データ部分に IP アドレスを埋め込みます。SIP 検査は、それらの埋め込み IP アドレスに NAT を適用します。

PAT を SIP で使用する場合、次の制約事項が適用されます。

- セキュリティ アプライアンスで保護されているネットワークの SIP プロキシにリモート エンドポイントを登録しようとすると、次のようなきわめて限定された条件では登録が失敗します。
  - PAT がリモート エンドポイント用に設定されている。
  - SIP レジストラ サーバが外部ネットワークにある。
  - エンドポイントからプロキシ サーバに送信された REGISTER メッセージの接続先フィールドにポートが設定されていない。
- SDP 部分の所有者 / 作成者フィールド（o=）の IP アドレスが接続フィールド（c=）の IP アドレスと異なるパケットを SIP デバイスが送信すると、o= フィールドの IP アドレスが正しく変換されない場合があります。これは、o= フィールドでポート値を提供しないという SIP プロトコルの制限によるものです。

SIP インスタント メッセージ

インスタント メッセージとは、ほぼリアルタイムにユーザ間でメッセージを転送することです。SIP は、Windows Messenger RTC Client バージョン 4.7.0105 を使用する Windows XP のチャット機能のみをサポートします。次の RFC で定義されているように、MESSAGE/INFO 方式および 202 Accept 応答を使用して IM をサポートします。

- Session Initiation Protocol（SIP）：Specific Event Notification、RFC 3265
- Session Initiation Protocol（SIP）：Extension for Instant Messaging、RFC 3428

MESSAGE/INFO 要求は、登録または加入の後であれば、いつでも受け取ることができます。たとえば、2 人のユーザはいつでもオンラインになる可能性がありますが、何時間もチャットをすることはありません。そのため、SIP 検査エンジンは、設定されている SIP タイムアウト値に従ってタイムアウトするピンホールを開きます。この値は、加入継続時間よりも 5 分以上長く設定する必要があります。加入継続時間は Contact Expires 値で定義され、通常 30 分です。

MESSAGE/INFO 要求は、通常、ポート 5060 以外のダイナミックに割り当てられたポートを使用して送信されるため、SIP 検査エンジンを通過する必要があります。

（注）　現在は、チャット機能のみがサポートされています。ホワイトボード、ファイル転送、アプリケーション共有はサポートされていません。RTC Client 5.0 はサポートされていません。

SIP 検査は、テキストベースの SIP メッセージを変換し、メッセージの SDP 部分の内容長を再計算した後、パケット長とチェックサムを再計算します。また、SIP メッセージの SDP 部分に、エンドポイントがリスンすべきアドレスまたはポートとして指定されたポートに対するメディア接続をダイナミックに開きます。

SIP 検査では、SIP ペイロードから取得したインデックス CALL_ID/FROM/TO を持つデータベースが使用されます。これらのインデックスにより、コール、送信元、宛先が識別されます。このデータベースには、SDP のメディア情報フィールド内で見つかったメディア アドレスとメディア ポート、およびメディア タイプが格納されています。1 つのセッションに対して、複数のメディア アドレスとポートを設定できます。セキュリティ アプライアンスは、これらのメディア アドレス / ポートを使用して、2 つのエンドポイント間に RTP/RTCP 接続を開きます。

初期コール セットアップ（INVITE）メッセージでは、ウェルノウン ポート 5060 を使用する必要があります。ただし、後続のメッセージにはこのポート番号がない場合もあります。SIP 検査エンジンはシグナリング接続のピンホールを開き、それらの接続を SIP 接続としてマークします。これは、SIP アプリケーションに到達した変換対象のメッセージに対して行われます。

コールがセットアップされるとき、SIP セッションは、着信側エンドポイントから応答メッセージでメディア アドレスとメディア ポートを受信し、着信側エンドポイントがリスンする RTP ポートを知らされるまで、「一時的な」状態にあります。1 分以内に応答メッセージを受信できないと、シグナリング接続は切断されます。

最終的なハンドシェイクが行われると、コール状態はアクティブに移行し、シグナリング接続は、BYE メッセージを受信するまで継続されます。

内部エンドポイントが外部エンドポイントへのコールを開始した場合、メディア ホールが外部インターフェイスに対して開き、内部エンドポイントからの INVITE メッセージで指定された内部エンドポイントのメディア アドレスとメディア ポートに RTP/RTCP UDP パケットが流れることが可能になります。要求していないのに内部インターフェイスに送信される RTP/RTCP UDP パケットは、セキュリティ アプライアンスのコンフィギュレーションで特に許可されていない限り、セキュリティ アプライアンスを通過できません。

Skinny（SCCP）検査

この項では、SCCP アプリケーション検査について説明します。ここでは、次の項目について説明します。

SCCP 検査の概要

Skinny（SCCP）は、VoIP ネットワークで使用される簡易プロトコルです。SCCP を使用する Cisco IP Phone は、H.323 環境内で共存できます。Cisco CallManager と併用すると、SCCP クライアントは H.323 準拠端末と相互運用できます。セキュリティ アプライアンスのアプリケーション レイヤ機能は、SCCP バージョン 3.3 を認識します。SCCP プロトコルには、5 つのバージョン（2.4、3.0.4、3.1.1、3.2、3.3.2）があります。セキュリティ アプライアンスは、バージョン 3.3.2 までのすべてのバージョンをサポートします。

セキュリティ アプライアンスは、SCCP に対して PAT と NAT をサポートします。IP 電話で使用できるグローバル IP アドレスよりも IP 電話が多い場合は、PAT が必要です。Skinny アプリケーション検査は、SCCP シグナリング パケットの NAT と PAT をサポートすることで、すべての SCCP シグナリングとメディア パケットがセキュリティ アプライアンスを通過できるようにします。

Cisco CallManager と Cisco IP Phones 間の通常のトラフィックは SCCP を使用しており、特別な設定をしなくても SCCP 検査によって処理されます。セキュリティ アプライアンスは、TFTP サーバの場所を Cisco IP Phone とその他の DHCP クライアントに送信することで、DHCP オプション 150 および 66 もサポートします。Cisco IP Phone では、デフォルト ルートを設定する DHCP オプション 3 を要求に含めることもできます。

Cisco IP Phone のサポート

Cisco CallManager が Cisco IP Phone よりもセキュリティの高いインターフェイスにあるトポロジでは、NAT が Cisco CallManager の IP アドレスに必要な場合、マッピングは**スタティック**である必要があります。これは、Cisco IP Phone では Cisco CallManager の IP アドレスをコンフィギュレーションで明示的に指定する必要があるためです。スタティック アイデンティティ エントリを使用すると、セキュリティが高いインターフェイス上にある Cisco CallManager が Cisco IP Phone からの登録を受け付けるようにできます。

Cisco IP Phone では、TFTP サーバにアクセスして、Cisco CallManager サーバに接続するために必要なコンフィギュレーション情報をダウンロードする必要があります。

Cisco IP Phone が TFTP サーバよりもセキュリティの低いインターフェイス上にある場合は、アクセスリストを使用し、保護された TFTP サーバに UDP ポート 69 で接続する必要があります。TFTP サーバにはスタティック エントリが必要ですが、アイデンティティ スタティック エントリである必要はありません。NAT を使用する場合、アイデンティティ スタティック エントリは同じ IP アドレスにマッピングされます。PAT を使用する場合は、同じ IP アドレスとポートにマッピングされます。

Cisco IP Phone が TFTP サーバおよび Cisco CallManager よりもセキュリティの高いインターフェイス上にある場合、Cisco IP Phone が接続を開始できるようにするためには、アクセスリストもスタティック エントリも必要ありません。

制約事項

SCCP に対する現在のバージョンの PAT および NAT のサポートには、次の制約事項が適用されます。

- PAT は、**alias** コマンドを含むコンフィギュレーションでは動作しません。
- 外部 NAT および PAT はサポートされません。

内部の Cisco CallManager のアドレスが NAT または PAT 用に別の IP アドレスまたはポートに設定されている場合、外部の Cisco IP Phone 用の登録は失敗します。これは、現在セキュリティ アプライアンスが、TFTP 経由で転送するファイルの内容に対する NAT または PAT をサポートしていないためです。セキュリティ アプライアンスは TFTP メッセージの NAT をサポートし、TFTP ファイル用にピンホールを開きますが、電話の登録中に TFTP によって転送された Cisco IP Phone のコンフィギュレーション ファイルに埋め込まれた Cisco CallManager の IP アドレスとポートを変換することはできません。

（注）　セキュリティ アプライアンスは、コール セットアップ中のコールを除き、SCCP コールのステートフル フェールオーバーをサポートします。

SMTP および拡張 SMTP 検査

拡張 SMTP（ESMTP）アプリケーション検査を使用すると、セキュリティ アプライアンスを通過できる SMTP コマンドのタイプを制限し、モニタリング機能を追加することによって、SMTP ベースの攻撃に対する保護を強化できます。

ESMTP は SMTP プロトコルの拡張版で、ほとんどの点で 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検査プロセスは、SMTP アプリケーション検査に似ており、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より多くのオプションを使用できます。

拡張 SMTP アプリケーション検査では、AUTH、EHLO、ETRN、HELP、SAML、SEND、SOML、VRFY の 8 つの拡張 SMTP コマンドのサポートが追加されます。セキュリティ アプライアンスは、7 つの RFC 821 コマンド（DATA、HELO、MAIL、NOOP、QUIT、RCPT、RSET）をサポートすると共に、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、STARTLS、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 X に変換され、内部サーバにより拒否されます。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、廃棄されます。

ESMTP 検査エンジンは、サーバの SMTP バナーの文字（「2」、「0」、「0」を除く）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 検査がイネーブルの場合、SMTP コマンドは 4 文字以上にし、復帰と改行で終了し、応答がくるまで待ってから次の応答を発行するという規則に従わないと、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 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 アプリケーション検査は、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 検査は、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 コマンドと応答のシーケンスを監視します。
- 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 検査では、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監視します。

- コマンドの切り捨て。
- コマンドの不正な終了（<CR><LF> で終了していない）。
- MAIL コマンドと RCPT コマンドは、メールの送信者と受信者を指定します。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。パイプライン文字（|）は削除（空白に変更）され、「<」および「>」は、メール アドレスの定義に使用される場合だけ許可されます（「<」、「>」の順に使用されている必要があります）。
- SMTP サーバによる予期しない移行。
- 不明なコマンドがあると、セキュリティ アプライアンス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、サーバは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ているため、TCP チェックサムを再計算または調整する必要があります。
- TCP ストリーム編集。
- コマンドのパイプライン処理。

SNMP 検査

SNMP アプリケーション検査では、SNMP トラフィックを特定のバージョンの SNMP に制限できます。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。セキュリティ アプライアンスは、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、SNMP マップを作成して制御します。

SQL*Net 検査

SQL*Net 検査はデフォルトでイネーブルになっています。

SQL*Net プロトコルは、さまざまなパケットタイプで構成されています。セキュリティ アプライアンスはこれらのパケットを処理して、セキュリティ アプライアンスのどちらの側の Oracle アプリケーションにも一貫性のあるデータ ストリームが表示されるようにします。

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、Structured Query Language（SQL; 構造化照会言語）の IANA ポート割り当てとは一致しません。SQL*Net 検査を一連のポート番号に適用するには、**class-map** コマンドを使用します。

セキュリティ アプライアンスはすべてのアドレスを変換し、パケットを調べて、SQL*Net バージョン 1 用に開くすべての埋め込みポートを見つけます。

SQL*Net バージョン 2 の場合、データ長ゼロの REDIRECT パケットの直後に続くすべての DATA パケットまたは REDIRECT パケットはフィックスアップされます。

フィックスアップが必要なパケットには、埋め込みホスト アドレスおよびポート アドレスが次の形式で含まれています。

```
(ADDRESS=(PROTOCOL=tcp)(DEV=6)(HOST=a.b.c.d)(PORT=a))
```

SQL*Net バージョン 2 の各 TNSFrame タイプ（Connect、Accept、Refuse、Resend、Marker）は、NAT 対象のアドレスがあるかどうかがスキャンされず、パケット内に埋め込まれたポート用にダイナミック接続も開かれません。

SQL*Net バージョン 2 の TNSFrame、Redirect パケット、および Data パケットは、ペイロードのデータ長がゼロの REDIRECT TNSFrame タイプの後に続く場合、開くポートおよび NAT 対象のアドレスがあるかどうかスキャンされます。データ長ゼロの Redirect メッセージがセキュリティ アプライアンスを通過すると、フラグが接続データ構造に設定されます。このフラグでは、この後に続く Data メッセージまたは Redirect メッセージが変換され、ポートがダイナミックに開かれることを想定します。先行するパラグラフの TNS フレームのいずれかが Redirect メッセージの後に到着した場合、フラグはリセットされます。

SQL*Net 検査エンジンは、チェックサムを再計算し、IP および TCP の長さを変更し、新旧のメッセージの長さの差を使用してシーケンス番号と確認応答番号を再調整します。

SQL*Net バージョン 1 では、その他のすべての場合を想定しています。TNSFrame タイプ（Connect、Accept、Refuse、Resend、Marker、Redirect、Data）とすべてのパケットは、ポートおよびアドレスがあるかどうかスキャンされます。アドレスが変換され、ポート接続が開かれます。

Sun RPC 検査

この項では、Sun RPC アプリケーション検査について説明します。ここでは、次の項目について説明します。

Sun RPC 検査の概要

Sun RPC 検査エンジンは、Sun RPC プロトコルのアプリケーション検査をイネーブルまたはディセーブルにします。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、ウェルノウン 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 クエリーをサーバに送信します。サーバが応答すると、セキュリティ アプライアンス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。

（注）　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。

SUNRPC Server

Configuration > Firewall > Advanced > **SUNRPC Server** ペインには、セキュリティ アプライアンスを通過できる SunRPC サービスと、その固有のタイムアウト値がサーバ単位で表示されます。

フィールド

- **Interface**：SunRPC サーバが常駐するインターフェイスを表示します。
- **IP address**：SunRPC サーバの IP アドレスを表示します。
- **Mask**：SunRPC サーバの IP アドレスのサブネット マスクを表示します。
- **Service ID**：セキュリティ アプライアンスを通過することを許可する、SunRPC プログラム番号、またはサービス ID を表示します。
- **Protocol**：SunRPC 転送プロトコル（TCP または UDP）を表示します。
- **Port**：SunRPC プロトコルのポート範囲を表示します。
- **Timeout**：SunRPC サービス トラフィックへのアクセスが閉じられるまでのアイドル時間を表示します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit SUNRPC Service

Configuration > Firewall > Advanced > **SUNRPC Server > Add/Edit SUNRPC Service** ダイアログボックスでは、セキュリティ アプライアンスを通過することを許可する SunRPC サービス、およびそれらの固有タイムアウトをサーバ単位で指定できます。

フィールド

- **Interface Name**：SunRPC サーバが常駐するインターフェイスを指定します。
- **Protocol**：SunRPC 転送プロトコル（TCP または UDP）を指定します。
- **IP address**：SunRPC サーバの IP アドレスを指定します。
- **Port**：SunRPC プロトコルのポート範囲を指定します。
- **Mask**：SunRPC サーバの IP アドレスのサブネット マスクを指定します。
- **Timeout**：SunRPC サービス トラフィックへのアクセスが閉じられるまでのアイドル時間を指定します。形式は、HH:MM:SS です。
- **Service ID**：セキュリティ アプライアンスを通過することを許可する、SunRPC プログラム番号、またはサービス ID を指定します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

TFTP 検査

TFTP 検査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。

セキュリティ アプライアンスは、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、検査エンジンは 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 検査をイネーブルにする必要があります。

XDMCP 検査

XDMCP 検査はデフォルトでイネーブルになっていますが、**established** コマンドが適切に構成されていないと、XDMCP 検査エンジンは使用できません。

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には、セキュリティ アプライアンスは、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、セキュリティ アプライアンスで **established** コマンドを使用します。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るかどうか確認されます。

XWindows セッション中、マネージャはウェルノウン 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
```

ここでは、*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 アドレスには、セキュリティ アプライアンスが必要に応じて NAT を行うことができます。XDCMP 検査では、PAT はサポートされません。

サービス ポリシーのフィールドの説明

この項では、各プロトコル検査ダイアログボックスのフィールドについて説明します。次の項目を取り上げます。

Rule Actions > Protocol Inspection タブ

フィールド

- **CTIQBE**：CTIQBE プロトコルでのアプリケーション検査をイネーブルにします。
- **DCERPC**：DCERPC プロトコルでのアプリケーション検査をイネーブルにします。
  - Configure：**Select** DCERPC **Map** ダイアログボックスを表示します。このダイアログボックスでは、このプロトコルで使用するマップ名を選択できます。
- **DNS**：DNS プロトコルでのアプリケーション検査をイネーブルにします。
  - Configure：**Select DNS Map** ダイアログボックスを表示します。このダイアログボックスでは、このプロトコルで使用するマップ名を選択できます。
- **ESMTP**：ESMTP プロトコルでのアプリケーション検査をイネーブルにします。
  - Configure：**Select ESMTP Map** ダイアログボックスを表示します。このダイアログボックスでは、このプロトコルで使用するマップ名を選択できます。
- **FTP**：FTP プロトコルでのアプリケーション検査をイネーブルにします。
  - Configure：**Select FTP Map** ダイアログボックスを表示します。このダイアログボックスでは、このプロトコルで使用するマップ名を選択できます。
- **GTP**：GTP プロトコルでのアプリケーション検査をイネーブルにします。
  - Configure：**Select GTP Map** ダイアログボックスを表示します。このダイアログボックスでは、このプロトコルで使用するマップ名を選択できます。

（注）　GTP 検査には、特別なライセンスが必要です。

- **H323 H225：**H323 H225 プロトコルでのアプリケーション検査をイネーブルにします。
  - Configure：**Select** H323 H225 **Map** ダイアログボックスを表示します。このダイアログボックスでは、このプロトコルで使用するマップ名を選択できます。
- **H323 RAS：**H323 RAS プロトコルでのアプリケーション検査をイネーブルにします。
  - Configure：**Select** H323 RAS **Map** ダイアログボックスを表示します。このダイアログボックスでは、このプロトコルで使用するマップ名を選択できます。
- **HTTP：**HTTP プロトコルでのアプリケーション検査をイネーブルにします。
  - Configure：**Select HTTP Map** ダイアログボックスを表示します。このダイアログボックスでは、このプロトコルで使用するマップ名を選択できます。
- **ICMP：**ICMP プロトコルでのアプリケーション検査をイネーブルにします。
- **ICMP Error：**ICMP Error プロトコルでのアプリケーション検査をイネーブルにします。
- **ILS：**ILS プロトコルでのアプリケーション検査をイネーブルにします。
- **IM：**IM プロトコルでのアプリケーション検査をイネーブルにします。
  - Configure：**Select IM Map** ダイアログボックスを表示します。このダイアログボックスでは、このプロトコルで使用するマップ名を選択できます。
- **IPSec-Pass-Thru：**IPSec プロトコルでのアプリケーション検査をイネーブルにします。
  - Configure：**Select IPSec Map** ダイアログボックスを表示します。このダイアログボックスでは、このプロトコルで使用するマップ名を選択できます。
- **MGCP：**MGCP プロトコルでのアプリケーション検査をイネーブルにします。
  - Configure：**Select MGCP Map** ダイアログボックスを表示します。このダイアログボックスでは、このプロトコルで使用するマップ名を選択できます。
- **NETBIOS：**NetBIOS プロトコルでのアプリケーション検査をイネーブルにします。
  - Configure：**Select NETBIOS Map** ダイアログボックスを表示します。このダイアログボックスでは、このプロトコルで使用するマップ名を選択できます。
- **PPTP：**PPTP プロトコルでのアプリケーション検査をイネーブルにします。
- **RSH：**RSH プロトコルでのアプリケーション検査をイネーブルにします。
- **RTSP：**RTSP プロトコルでのアプリケーション検査をイネーブルにします。
- **SCCP SKINNY：**Skinny プロトコルでのアプリケーション検査をイネーブルにします。
  - Configure：**Select SCCP (Skinny) Map** ダイアログボックスを表示します。このダイアログボックスでは、このプロトコルで使用するマップ名を選択できます。
- **SIP：**SIP プロトコルでのアプリケーション検査をイネーブルにします。
  - Configure：**Select SIP Map** ダイアログボックスを表示します。このダイアログボックスでは、このプロトコルで使用するマップ名を選択できます。
- **SNMP：**SNMP プロトコルでのアプリケーション検査をイネーブルにします。
  - Configure：**Select SNMP Map** ダイアログボックスを表示します。このダイアログボックスでは、このプロトコルで使用するマップ名を選択できます。
- **SQLNET：**SQLNET プロトコルでのアプリケーション検査をイネーブルにします。
- **SUNRPC：**SunRPC プロトコルでのアプリケーション検査をイネーブルにします。
- **TFTP：**TFTP プロトコルでのアプリケーション検査をイネーブルにします。
- **XDMCP：**XDMCP プロトコルでのアプリケーション検査をイネーブルにします。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

詳細情報

検査マップのフィールドの説明（P. 24-61）

『*Cisco Security Appliance Command Reference*』にあるプロトコルごとの **Inspect** コマンド ページ

Select DCERPC Map

Select DCERPC Map ダイアログボックスでは、**DCERPC** マップを選択または新しく作成できます。**DCERPC** マップにより、**DCERPC** アプリケーション検査で使用されるコンフィギュレーションの値を変更できます。**Select DCERPC Map** テーブルには、アプリケーション検査で選択可能な事前に設定されたマップのリストが表示されます。

フィールド

- **Use the default DCERPC inspection map**：デフォルトの DCERPC マップの使用を指定します。
- **Select a DCERPC map for fine control over inspection**：定義済みのアプリケーション検査マップを選択するか、新しいマップを追加できます。
- Add：その検査の Add Policy Map ダイアログボックスを開きます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Select DNS Map

Select DNS Map ダイアログボックスでは、**DNS** マップを選択または新しく作成できます。**DNS** マップにより、**DNS** アプリケーション検査で使用されるコンフィギュレーションの値を変更できます。**Select DNS Map** テーブルには、アプリケーション検査で選択可能な事前に設定されたマップのリストが表示されます。

フィールド

- **Use the default DNS inspection map**：デフォルトの **DNS** マップの使用を指定します。
- **Select a DNS map for fine control over inspection**：定義済みのアプリケーション検査マップを選択するか、新しいマップを追加できます。
- Add：その検査の Add Policy Map ダイアログボックスを開きます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Select ESMTP Map

Select ESMTP Map ダイアログボックスでは、**ESMTP** マップを選択または新しく作成できます。**ESMTP** マップにより、**ESMTP** アプリケーション検査で使用されるコンフィギュレーションの値を変更できます。**Select ESMTP Map** テーブルには、アプリケーション検査で選択可能な事前に設定されたマップのリストが表示されます。

フィールド

- **Use the default ESMTP inspection map**：デフォルトの **ESMTP** マップの使用を指定します。
- **Select an ESMTP map for fine control over inspection**：定義済みのアプリケーション検査マップを選択するか、新しいマップを追加できます。
- Add：その検査の Add Policy Map ダイアログボックスを開きます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Select FTP Map

Select FTP Map ダイアログボックスでは、厳密な FTP アプリケーション検査のイネーブル化、FTP マップの選択、または新しい FTP マップの作成を行うことができます。FTP マップにより、FTP アプリケーション検査で使用されるコンフィギュレーションの値を変更できます。**Select FTP Map** テーブルには、アプリケーション検査で選択可能な事前に設定されたマップのリストが表示されます。

フィールド

- **FTP Strict (prevent web browsers from sending embedded commands in FTP requests) :** 厳密な FTP アプリケーション検査をイネーブルにします。これによってセキュリティ アプライアンスは、埋め込みコマンドが FTP 要求に含まれている場合には接続をドロップします。
- **Use the default FTP inspection map**：デフォルトの FTP マップの使用を指定します。
- **Select an FTP map for fine control over inspection**：定義済みのアプリケーション検査マップを選択するか、新しいマップを追加できます。
- Add：その検査の Add Policy Map ダイアログボックスを開きます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Select GTP Map

Select GTP Map ダイアログボックスでは、GTP マップを選択または新しく作成できます。GTP マップにより、GTP アプリケーション検査で使用されるコンフィギュレーションの値を変更できます。Select GTP Map テーブルには、アプリケーション検査で選択可能な事前に設定されたマップのリストが表示されます。

（注） GTP 検査には、特別なライセンスが必要です。必要なライセンスがないときにセキュリティ アプライアンスで GTP アプリケーション検査のイネーブル化を試みると、セキュリティ アプライアンスはエラー メッセージを表示します。

フィールド

- **Use the default GTP inspection map**：デフォルトの GTP マップの使用を指定します。
- **Select an GTP map for fine control over inspection**：定義済みのアプリケーション検査マップを選択するか、新しいマップを追加できます。
- Add：その検査の Add Policy Map ダイアログボックスを開きます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Select H.323 Map

Select H.323 Map ダイアログボックスでは、**H.323** マップを選択または新しく作成できます。**H.323** マップにより、**H.323** アプリケーション検査で使用されるコンフィギュレーションの値を変更できます。Select **H.323** Map テーブルには、アプリケーション検査で選択可能な事前に設定されたマップのリストが表示されます。

フィールド

- **Use the default H.323 inspection map**：デフォルトの **H.323** マップの使用を指定します。
- **Select an H.323 map for fine control over inspection**：定義済みのアプリケーション検査マップを選択するか、新しいマップを追加できます。
- Add：その検査の Add Policy Map ダイアログボックスを開きます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Select HTTP Map

Select HTTP Map ダイアログボックスでは、HTTP マップを選択または新しく作成できます。HTTP マップにより、HTTP アプリケーション検査で使用されるコンフィギュレーションの値を変更できます。Select HTTP Map テーブルには、アプリケーション検査で選択可能な事前に設定されたマップのリストが表示されます。

フィールド

- **Use the default HTTP inspection map**：デフォルトの HTTP マップの使用を指定します。
- **Select an HTTP map for fine control over inspection**：定義済みのアプリケーション検査マップを選択するか、新しいマップを追加できます。
- Add：その検査の Add Policy Map ダイアログボックスを開きます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Select IM Map

Select IM Map ダイアログボックスでは、**IM** マップを選択または新しく作成できます。**IM** マップにより、**IM** アプリケーション検査で使用されるコンフィギュレーションの値を変更できます。Select **IM** Map テーブルには、アプリケーション検査で選択可能な事前に設定されたマップのリストが表示されます。

フィールド

- Add：その検査の Add Policy Map ダイアログボックスを開きます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Select IPSec-Pass-Thru Map

Select IPSec-Pass-Thru ダイアログボックスでは、**IPSec** マップを選択または新しく作成できます。**IPSec** マップにより、**IPSec** アプリケーション検査で使用されるコンフィギュレーションの値を変更できます。Select **IPSec** Map テーブルには、アプリケーション検査で選択可能な事前に設定されたマップのリストが表示されます。

フィールド

- **Use the default IPSec inspection map**：デフォルトの **IPSec** マップの使用を指定します。
- **Select an IPSec map for fine control over inspection**：定義済みのアプリケーション検査マップを選択するか、新しいマップを追加できます。
- Add：その検査の Add Policy Map ダイアログボックスを開きます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Select MGCP Map

Select MGCP Map ダイアログボックスでは、MGCP マップを選択または新しく作成できます。MGCP マップにより、MGCP アプリケーション検査で使用されるコンフィギュレーションの値を変更できます。**Select MGCP Map** テーブルには、アプリケーション検査で選択可能な事前に設定されたマップのリストが表示されます。

フィールド

- **Use the default MGCP inspection map**：デフォルトの **MGCP** マップの使用を指定します。
- **Select an MGCP map for fine control over inspection**：定義済みのアプリケーション検査マップを選択するか、新しいマップを追加できます。
- Add：その検査の Add Policy Map ダイアログボックスを開きます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Select NETBIOS Map

Select NETBIOS Map ダイアログボックスでは、**NetBIOS** マップを選択または新しく作成できます。**NetBIOS** マップにより、**NetBIOS** アプリケーション検査で使用されるコンフィギュレーションの値を変更できます。Select **NetBIOS** Map テーブルには、アプリケーション検査で選択可能な事前に設定されたマップのリストが表示されます。

フィールド

- **Use the default NetBIOS inspection map**：デフォルトの **NetBIOS** マップの使用を指定します。
- **Select a NetBIOS map for fine control over inspection**：定義済みのアプリケーション検査マップを選択するか、新しいマップを追加できます。
- Add：その検査の Add Policy Map ダイアログボックスを開きます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Select RTSP Map

Select RTSP Map ダイアログボックスでは、**RTSP** マップを選択または新しく作成できます。RTSP マップにより、**RTSP** アプリケーション検査で使用されるコンフィギュレーションの値を変更できます。Select **RTSP** Map テーブルには、アプリケーション検査で選択可能な事前に設定されたマップのリストが表示されます。

フィールド

- **Use the default RTSP inspection map**：デフォルトの RTSP 検査マップの使用を指定します。
- **Select a RTSP inspect map for fine control over inspection**：定義済みのアプリケーション検査マップを選択するか、新しいマップを追加できます。
- Add：その検査の Add Policy Map ダイアログボックスを開きます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Select SCCP (Skinny) Map

Select SCCP (Skinny) Map ダイアログボックスでは、**SCCP (Skinny)** マップを選択または新しく作成できます。**SCCP (Skinny)** マップにより、**SCCP (Skinny)** アプリケーション検査で使用されるコンフィギュレーションの値を変更できます。Select **SCCP (Skinny)** Map テーブルには、アプリケーション検査で選択可能な事前に設定されたマップのリストが表示されます。

フィールド

- **Use the default SCCP (Skinny) inspection map**：デフォルトの **SCCP (Skinny)** マップの使用を指定します。
- **Select an SCCP (Skinny) map for fine control over inspection**：定義済みのアプリケーション検査マップを選択するか、新しいマップを追加できます。
- Add：その検査の Add Policy Map ダイアログボックスを開きます。
- TLS Proxy：検査マップの TLS プロキシ設定を指定できます。
  - Use TLS Proxy to enable inspection of encrypted traffic：TLS プロキシを使用して、暗号化されたトラフィックの検査をイネーブルにすることを指定します。

    TLS Proxy Name：既存の TLS プロキシの名前。

    New：TLS プロキシを追加するための Add TLS Proxy ダイアログボックスを開きます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Select SIP Map

Select SIP Map ダイアログボックスでは、**SIP** マップを選択または新しく作成できます。**SIP** マップにより、**SIP** アプリケーション検査で使用されるコンフィギュレーションの値を変更できます。Select **SIP** Map テーブルには、アプリケーション検査で選択可能な事前に設定されたマップのリストが表示されます。

フィールド

- **Use the default SIP inspection map**：デフォルトの **SIP** マップの使用を指定します。
- **Select a SIP map for fine control over inspection**：定義済みのアプリケーション検査マップを選択するか、新しいマップを追加できます。
- Add：その検査の Add Policy Map ダイアログボックスを開きます。
- TLS Proxy：検査マップの TLS プロキシ設定を指定できます。
  - Use TLS Proxy to enable inspection of encrypted traffic：TLS プロキシを使用して、暗号化されたトラフィックの検査をイネーブルにすることを指定します。

    TLS Proxy Name：既存の TLS プロキシの名前。

    New：TLS プロキシを追加するための Add TLS Proxy ダイアログボックスを開きます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Select SNMP Map

Select SNMP Map ダイアログボックスでは、SNMP マップを選択または新しく作成できます。SNMP マップにより、SNMP アプリケーション検査で使用されるコンフィギュレーションの値を変更できます。Select SNMP Map テーブルには、アプリケーション検査で選択可能な事前に設定されたマップのリストが表示されます。

フィールド

- **Use the default SNMP inspection map**：デフォルトの **SNMP** マップの使用を指定します。
- **Select an SNMP map for fine control over inspection**：定義済みのアプリケーション検査マップを選択するか、新しいマップを追加できます。
- Add：その検査の Add Policy Map ダイアログボックスを開きます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

クラスマップのフィールドの説明

検査クラスマップで、アプリケーションのトラフィックを、URL 文字列などアプリケーション固有の基準と照合します。次に、クラスマップを検査マップから特定して、アクションをイネーブルにします。クラスマップを作成することと検査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。検査クラスマップは DNS、FTP、H.323、HTTP、IM、SIP のアプリケーションでサポートされます。

この項では、検査クラスマップを設定する方法について説明します。次の項目を取り上げます。

DNS Class Map

DNS Class Map パネルでは、DNS 検査のクラスマップを設定できます。

検査クラスマップで、アプリケーションのトラフィックをアプリケーション固有の基準と照合します。次に、クラスマップを検査マップから特定して、アクションをイネーブルにします。クラスマップを作成することと検査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。検査クラスマップは DNS、FTP、H.323、HTTP、IM、SIP のアプリケーションでサポートされます。

フィールド

- Name：DNS クラスマップの名前を示します。
- Match Conditions：クラスマップに設定されているタイプ、照合基準、値を示します。
  - Match Type：一致タイプを示します。肯定一致と否定一致があります。
  - Criterion：DNS クラスマップの基準を示します。
  - Value：DNS クラスマップで照合する値を示します。
- Description：クラスマップの説明を示します。
- Add：DNS クラスマップの照合条件を追加します。
- Edit：DNS クラスマップの照合条件を編集します。
- Delete：DNS クラスマップの照合条件を削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit DNS Traffic Class Map

Add/Edit DNS Traffic Class Map ダイアログボックスでは、DNS クラスマップを定義できます。

フィールド

- Name：DNS クラスマップの名前を 40 文字以内で入力します。
- Description：DNS クラスマップの説明を入力します。
- Add：DNS クラスマップを追加します。
- Edit：DNS クラスマップを編集します。
- Delete：DNS クラスマップを削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit DNS Match Criterion

Add/Edit DNS Match Criterion ダイアログボックスでは、DNS クラスマップの照合基準と値を定義できます。

フィールド

- Match Type：基準に一致したトラフィックをクラスマップに含めるか、または一致しないトラフィックを含めるか指定します。

  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。
- Criterion：DNS トラフィックに適用する照合基準を指定します。
  - Header Flag：ヘッダーの DNS フラグを照合します。
  - Type：DNS クエリーまたはリソース レコードのタイプを照合します。
  - Class：DNS クエリーまたはリソース レコードのクラスを照合します。
  - Question：DNS の問い合せを照合します。
  - Resource Record：DNS リソース レコードを照合します。
  - Domain Name：DNS クエリーやリソース レコードのドメイン名を照合します。
- Header Flag Criterion Values：DNS ヘッダー フラグの照合値の詳細を指定します。
  - Match Option：完全一致または全ビット一致（ビット マスク一致）のどちらかを指定します。
  - Match Value：ヘッダー フラグについて名前と値のどちらを照合するか指定します。

    Header Flag Name：照合するヘッダー フラグ名を 1 つ以上選択できます。AA（authoritative answer）、QR（query）、RA（recursion available）、RD（recursion denied）、TC（truncation）のフラグ ビットがあります。

    Header Flag Value：任意の 16 ビットの値を 16 進数で入力して照合できます。
- Type Criterion Values：DNS タイプの照合値の詳細を指定します。
  - DNS Type Field Name：選択する DNS タイプを一覧表示します。

    A：IPv4 アドレス

    NS：信頼できるネーム サーバ

CNAME：正規名

SOA：信頼ゾーンの開始

TSIG：トランザクション シグニチャ

IXFR：差分（ゾーン）転送

AXFR：完全（ゾーン）転送

- DNS Type Field Value：DNS タイプ フィールドについて値と範囲のどちらを照合するか指定します。

  Value：0 ～ 65535 の範囲の値を入力して照合できます。

  Range：範囲を入力して照合します。両方とも 0 ～ 65535 の範囲の値を指定します。

- Class Criterion Values：DNS クラスの照合値の詳細を指定します。
  - DNS Class Field Name：インターネットで照合する DNS クラス フィールド名を指定します。
  - DNS Class Field Value：DNS クラス フィールドについて値と範囲のどちらを照合するか指定します。

    Value：0 ～ 65535 の範囲の値を入力して照合できます。

    Range：範囲を入力して照合します。両方とも 0 ～ 65535 の範囲の値を指定します。
- Question Criterion Values：DNS の問い合せセクションの照合方法を指定します。
- Resource Record Criterion Values：DNS リソース レコードのセクションの照合方法を指定します。
  - Resource Record：照合対象セクションを一覧表示します。

    Additional：DNS 追加リソース レコード

    Answer：DNS 応答リソース レコード

    Authority：DNS 認証リソース レコード
- Domain Name Criterion Values：DNS ドメイン名の照合方法を指定します。
  - Regular Expression：照合する定義された正規表現を一覧表示します。
  - Manage：Manage Regular Expressions ダイアログボックスが開き、正規表現を設定できます。
  - Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。
  - Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップを設定できます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Manage Regular Expressions

Manage Regular Expressions ダイアログボックスでは、Regular Expressions を設定し、パターン照合で使用できます。「_default」で始まる正規表現はデフォルトの正規表現です。変更または削除はできません。

フィールド

- Name：正規表現の名前を示します。
- Value：正規表現の定義値を示します。
- Add：正規表現を追加します。

- Edit：正規表現を編集します。
- Delete：正規表現を削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Manage Regular Expression Class Maps

Manage Regular Expression Class Maps ダイアログボックスでは、正規表現クラスマップを設定できます。詳細については、「Regular Expressions」を参照してください。

フィールド

- Name：正規表現クラスマップの名前を示します。
- Match Conditions：クラスマップの照合タイプと正規表現を示します。
  - Match Type：照合タイプを示します。正規表現の場合、常に基準の肯定一致タイプ（等号（=）を表示したアイコン）になります。また、検査クラスマップで否定一致（赤丸を表示したアイコン）の作成もできます。クラスマップに正規表現が複数ある場合は、照合タイプ アイコンの隣にそれぞれ「OR」を表示し、「match any」クラスマップになっていることを示します。正規表現のいずれか 1 つと一致するだけで、トラフィックがクラスマップに一致します。
  - Regular Expression：クラスマップごとに登録されている正規表現を一覧表示します。
- Description：クラスマップの説明を示します。
- Add：正規表現クラスマップを追加します。
- Edit：正規表現クラスマップを編集します。
- Delete：正規表現クラスマップを削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

FTP Class Map

FTP Class Map パネルでは、FTP 検査のクラスマップを設定できます。

検査クラスマップで、アプリケーションのトラフィックをアプリケーション固有の基準と照合します。次に、クラスマップを検査マップから特定して、アクションをイネーブルにします。クラスマップを作成することと検査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。検査クラスマップは DNS、FTP、H.323、HTTP、IM、SIP のアプリケーションでサポートされます。

フィールド

- Name：FTP クラスマップの名前を示します。
- Match Conditions：クラスマップに設定されているタイプ、照合基準、値を示します。
  - Match Type：一致タイプを示します。肯定一致と否定一致があります。
  - Criterion：FTP クラスマップの基準を示します。
  - Value：FTP クラスマップで照合する値を示します。
- Description：クラスマップの説明を示します。
- Add：FTP クラスマップを追加します。
- Edit：FTP クラスマップを編集します。
- Delete：FTP クラスマップを削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit FTP Traffic Class Map

Add/Edit FTP Traffic Class Map ダイアログボックスでは、FTP クラスマップを定義できます。

フィールド

- Name：FTP クラスマップの名前を 40 文字以内で入力します。
- Description：FTP クラスマップの説明を入力します。
- Add：FTP クラスマップを追加します。
- Edit：FTP クラスマップを編集します。
- Delete：FTP クラスマップを削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit FTP Match Criterion

Add/Edit FTP Match Criterion ダイアログボックスでは、FTP クラスマップの照合基準と値を定義できます。

フィールド

- Match Type：基準に一致したトラフィックをクラスマップに含めるか、または一致しないトラフィックを含めるか指定します。

  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。
- Criterion：FTP トラフィックに適用する照合基準を指定します。
  - Request-Command：FTP 要求コマンドを照合します。
  - File Name：FTP 転送のファイル名を照合します。
  - File Type：FTP 転送のファイル タイプを照合します。
  - Server：FTP サーバを照合します。
  - User Name：FTP ユーザを照合します。
- Request-Command Criterion Values：FTP 要求コマンドの照合値の詳細を指定します。
  - Request Command：照合する要求コマンドを 1 つ以上選択できます。

    APPE：ファイルに追加します。

    CDUP：現在のディレクトリから親ディレクトリへ移動します。

    DELE：サーバ サイトのファイルを削除します。

    GET：retr（retrieve a file）コマンドの FTP クライアント コマンドです。

    HELP：サーバのヘルプ情報です。

    MKD：ディレクトリを作成します。

    PUT：stor（store a file）コマンドの FTP クライアント コマンドです。

    RMD：ディレクトリを削除します。

    RNFR：この名前からリネームします。

    RNTO：この名前にリネームします。

    SITE：サーバ固有のコマンドを指定します。

    STOU：ファイルに一意の名前をつけて保存します。
- File Name Criterion Values：FTP 転送のファイル名の照合方法を指定します。
  - Regular Expression：照合する定義された正規表現を一覧表示します。
  - Manage : Manage Regular Expressions ダイアログボックスが開き、正規表現を設定できます。
  - Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。
  - Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップを設定できます。
- File Type Criterion Values：FTP 転送のファイル タイプの照合方法を指定します。
  - Regular Expression：照合する定義された正規表現を一覧表示します。
  - Manage : Manage Regular Expressions ダイアログボックスが開き、正規表現を設定できます。
  - Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。
  - Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップを設定できます。
- Server Criterion Values：FTP サーバの照合方法を指定します。
  - Regular Expression：照合する定義された正規表現を一覧表示します。
  - Manage : Manage Regular Expressions ダイアログボックスが開き、正規表現を設定できます。
  - Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。

- Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップを設定できます。

- User Name Criterion Values：FTP ユーザの照合方法を指定します。
  - Regular Expression：照合する定義された正規表現を一覧表示します。
  - Manage : Manage Regular Expressions ダイアログボックスが開き、正規表現を設定できます。
  - Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。
  - Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップを設定できます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

H.323 Class Map

H.323 Class Map パネルでは、H.323 検査のクラスマップを設定できます。

検査クラスマップで、アプリケーションのトラフィックをアプリケーション固有の基準と照合します。次に、クラスマップを検査マップから特定して、アクションをイネーブルにします。クラスマップを作成することと検査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。検査クラスマップは DNS、FTP、H.323、HTTP、IM、SIP のアプリケーションでサポートされます。

フィールド

- Name：H.323 クラスマップの名前を示します。
- Match Conditions：クラスマップに設定されているタイプ、照合基準、値を示します。
  - Match Type：一致タイプを示します。肯定一致と否定一致があります。
  - Criterion：H.323 クラスマップの基準を示します。
  - Value：H.323 クラスマップで照合する値を示します。
- Description：クラスマップの説明を示します。
- Add：H.323 クラスマップを追加します。
- Edit：H.323 クラスマップを編集します。
- Delete：H.323 クラスマップを削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit H.323 Traffic Class Map

Add/Edit H.323 Traffic Class Map ダイアログボックスでは、H.323 クラスマップを定義できます。

フィールド

- Name：H.323 クラスマップの名前を 40 文字以内で入力します。
- Description：H.323 クラスマップの説明を入力します。
- Add：H.323 クラスマップを追加します。
- Edit：H.323 クラスマップを編集します。
- Delete：H.323 クラスマップを削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit H.323 Match Criterion

Add/Edit H.323 Match Criterion ダイアログボックスでは、H.323 クラスマップの照合基準と値を定義できます。

フィールド

- Match Type：基準に一致したトラフィックをクラスマップに含めるか、または一致しないトラフィックを含めるか指定します。

  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。
- Criterion：H.323 トラフィックに適用する照合基準を指定します。
  - Called Party：受信側を照合します。
  - Calling Party：発信元を照合します。
  - Media Type：メディア タイプを照合します。
- Called Party Criterion Values：H.323 受信側の照合方法を指定します。
  - Regular Expression：照合する定義された正規表現を一覧表示します。
  - Manage : Manage Regular Expressions ダイアログボックスが開き、正規表現を設定できます。
  - Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。
  - Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップを設定できます。
- Calling Party Criterion Values：H.323 発信元の照合方法を指定します。
  - Regular Expression：照合する定義された正規表現を一覧表示します。
  - Manage : Manage Regular Expressions ダイアログボックスが開き、正規表現を設定できます。
  - Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。
  - Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップを設定できます。
- Media Type Criterion Values：照合するメディア タイプを指定します。

- Audio：音声タイプを照合します。
- Video：ビデオ タイプを照合します。
- Data：データ タイプを照合します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

HTTP Class Map

HTTP Class Map パネルでは、HTTP 検査のクラスマップを設定できます。

検査クラスマップで、アプリケーションのトラフィックをアプリケーション固有の基準と照合します。次に、クラスマップを検査マップから特定して、アクションをイネーブルにします。クラスマップを作成することと検査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。検査クラスマップは DNS、FTP、H.323、HTTP、IM、SIP のアプリケーションでサポートされます。

フィールド

- Name：HTTP クラスマップの名前を示します。
- Match Conditions：クラスマップに設定されているタイプ、照合基準、値を示します。
  - Match Type：一致タイプを示します。肯定一致と否定一致があります。
  - Criterion：HTTP クラスマップの基準を示します。
  - Value：HTTP クラスマップで照合する値を示します。
- Description：クラスマップの説明を示します。
- Add：HTTP クラスマップを追加します。
- Edit：HTTP クラスマップを編集します。
- Delete：HTTP クラスマップを削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit HTTP Traffic Class Map

Add/Edit HTTP Traffic Class Map ダイアログボックスでは、HTTP クラスマップを定義できます。

フィールド

- Name：HTTP クラスマップの名前を 40 文字以内で入力します。
- Description：HTTP クラスマップの説明を入力します。
- Add：HTTP クラスマップを追加します。
- Edit：HTTP クラスマップを編集します。
- Delete：HTTP クラスマップを削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit HTTP Match Criterion

Add/Edit HTTP Match Criterion ダイアログボックスでは、HTTP クラスマップの照合基準と値を定義できます。

フィールド

- Match Type：基準に一致したトラフィックをクラスマップに含めるか、または一致しないトラフィックを含めるか指定します。

  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。
- Criterion：HTTP トラフィックに適用する照合基準を指定します。
  - Request/Response Content Type Mismatch : 応答のコンテンツ タイプを、要求の accept フィールドの MIME タイプの 1 つに一致させるかどうかを指定します。
  - Request Arguments：要求の引数を正規表現で照合します。

    Regular Expression：照合する定義された正規表現を一覧表示します。

    Manage : Manage Regular Expressions ダイアログボックスが開き、正規表現を設定できます。

    Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。

    Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップを設定できます。
  - Request Body Length：要求の本文に指定したバイト数より長いフィールドがある場合、正規表現で照合します。

    Greater Than Length : 要求フィールドの長さと照合するフィールドの値をバイト単位で入力します。
  - Request Body：要求の本文を正規表現で照合します。

    Regular Expression：照合する定義された正規表現を一覧表示します。

    Manage : Manage Regular Expressions ダイアログボックスが開き、正規表現を設定できます。

    Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。

    Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップを設定できます。

- Request Header Field Count：要求ヘッダーのフィールド数が最大値の場合、正規表現で照合します。

  Predefined：要求のヘッダー フィールドを次の中から指定します。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。

  Regular Expression：照合する定義された正規表現を一覧表示します。

  Manage : Manage Regular Expressions ダイアログボックスが開き、正規表現を設定できます。

  Greater Than Count：ヘッダー フィールド数の最大値を入力します。

- Request Header Field Length：要求ヘッダーに指定したバイト数より長いフィールドがある場合、正規表現で照合します。

  Predefined：要求のヘッダー フィールドを次の中から指定します。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。

  Regular Expression：照合する定義された正規表現を一覧表示します。

  Manage : Manage Regular Expressions ダイアログボックスが開き、正規表現を設定できます。

  Greater Than Length : 要求フィールドの長さと照合するフィールドの値をバイト単位で入力します。

- Request Header Field：要求ヘッダーを正規表現で照合します。

  Predefined：要求のヘッダー フィールドを次の中から指定します。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。

  Regular Expression：照合する定義された正規表現を一覧表示します。

  Manage : Manage Regular Expressions ダイアログボックスが開き、正規表現を設定できます。

  Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。

  Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップを設定できます。

- Request Header Count：要求ヘッダー数が最大値の場合、正規表現で照合します。

  Greater Than Count：ヘッダー数の最大値を入力します。

- Request Header Length : 要求ヘッダーが指定したバイト数より長い場合、正規表現で照合します。

  Greater Than Length：ヘッダーの長さをバイト単位で入力します。

- Request Header non-ASCII：要求ヘッダーに含まれる ASCII 以外の文字を照合します。

- Request Method：要求の方式を正規表現で照合します。

  Method：照合する要求方式を次の中から指定します。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。

  Regular Expression：正規表現の照合方法を指定します。

  Regular Expression：照合する定義された正規表現を一覧表示します。

  Manage : Manage Regular Expressions ダイアログボックスが開き、正規表現を設定できます。

  Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。

Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップを設定できます。

- Request URI Length：要求の URI が指定したバイト数より長い場合、正規表現で照合します。

  Greater Than Length：URI の長さをバイト単位で入力します。

- Request URI：要求の URI を正規表現で照合します。

  Regular Expression：照合する定義された正規表現を一覧表示します。

  Manage：Manage Regular Expressions ダイアログボックスが開き、正規表現を設定できます。

  Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。

  Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップを設定できます。

- Response Body：要求の本文を regex で照合します。

  ActiveX：ActiveX の照合方法を指定します。

  Java Applet：Java アプレットの照合方法を指定します。

  Regular Expression：正規表現の照合方法を指定します。

  Regular Expression：照合する定義された正規表現を一覧表示します。

  Manage：Manage Regular Expressions ダイアログボックスが開き、正規表現を設定できます。

  Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。

  Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップを設定できます。

- Response Body Length：応答の本文に指定したバイト数より長いフィールドがある場合、正規表現で照合します。

  Greater Than Length：応答フィールドの長さと照合するフィールドの値をバイト単位で入力します。

- Response Header Field Count：応答ヘッダーのフィールド数が最大値の場合、正規表現で照合します。

  Predefined：応答のヘッダー フィールドを次の中から指定します。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。

  Regular Expression：照合する定義された正規表現を一覧表示します。

  Manage：Manage Regular Expressions ダイアログボックスが開き、正規表現を設定できます。

  Greater Than Count：ヘッダー フィールド数の最大値を入力します。

- Response Header Field Length：応答ヘッダーに指定したバイト数より長いフィールドがある場合、正規表現で照合します。

  Predefined：応答のヘッダー フィールドを次の中から指定します。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。

  Regular Expression：照合する定義された正規表現を一覧表示します。

  Manage：Manage Regular Expressions ダイアログボックスが開き、正規表現を設定できます。

  Greater Than Length：応答フィールドの長さと照合するフィールドの値をバイト単位で入力します。

- Response Header Field：応答ヘッダーを正規表現で照合します。

  Predefined：応答のヘッダー フィールドを次の中から指定します。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。

Regular Expression：照合する定義された正規表現を一覧表示します。

Manage : Manage Regular Expressions ダイアログボックスが開き、正規表現を設定できます。

Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。

Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップを設定できます。

- Response Header Count：応答ヘッダー数が最大値の場合、正規表現で照合します。

  Greater Than Count：ヘッダー数の最大値を入力します。

- Response Header Length：応答ヘッダーが指定したバイト数より長い場合、正規表現で照合します。

  Greater Than Length：ヘッダーの長さをバイト単位で入力します。

- Response Header non-ASCII：応答ヘッダーに含まれる ASCII 以外の文字を照合します。
- Response Status Line：ステータス行を正規表現で照合します。

  Regular Expression：照合する定義された正規表現を一覧表示します。

  Manage : Manage Regular Expressions ダイアログボックスが開き、正規表現を設定できます。

  Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。

  Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップを設定できます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

IM Class Map

IM Class Map パネルでは、IM 検査のクラスマップを設定できます。

検査クラスマップで、アプリケーションのトラフィックをアプリケーション固有の基準と照合します。次に、クラスマップを検査マップから特定して、アクションをイネーブルにします。クラスマップを作成することと検査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。検査クラスマップは DNS、FTP、H.323、HTTP、IM、SIP のアプリケーションでサポートされます。

フィールド

- Name：IM クラスマップの名前を示します。
- Match Conditions：クラスマップに設定されているタイプ、照合基準、値を示します。
  - Match Type：一致タイプを示します。肯定一致と否定一致があります。
  - Criterion：IM クラスマップの基準を示します。
  - Value：IM クラスマップで照合する値を示します。
- Description：クラスマップの説明を示します。
- Add：IM クラスマップを追加します。
- Edit：IM クラスマップを編集します。
- Delete：IM クラスマップを削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit IM Traffic Class Map

Add/Edit IM Traffic Class Map ダイアログボックスでは、IM クラスマップを定義できます。

フィールド

- Name：IM クラスマップの名前を 40 文字以内で入力します。
- Description：IM クラスマップの説明を入力します。
- Add：IM クラスマップを追加します。
- Edit：IM クラスマップを編集します。
- Delete：IM クラスマップを削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit IM Match Criterion

Add/Edit IM Match Criterion ダイアログボックスでは、IM クラスマップの照合基準と値を定義できます。

フィールド

- Match Type：基準に一致したトラフィックをクラスマップに含めるか、または一致しないトラフィックを含めるか指定します。

  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。
- Criterion：IM トラフィックに適用する照合基準を指定します。
  - Protocol：IM プロトコルを照合します。
  - Service：IM サービスを照合します。
  - Version：IM ファイル転送のサービス バージョンを照合します。
  - Client Login Name：IM サービスのクライアント ログイン名を照合します。
  - Client Peer Login Name：IM サービスのクライアントのピア ログイン名を照合します。
  - Source IP Address：送信元 IP アドレスを照合します。
  - Destination IP Address：宛先 IP アドレスを照合します。

  - Filename：IM ファイル転送サービスのファイル名を照合します。
- Protocol Criterion Values：照合する IM プロトコルを指定します。
  - Yahoo! Messenger：Yahoo! Messenger のインスタント メッセージを照合します。
  - MSN Messenger：MSN Messenger のインスタント メッセージを照合します。
- Service Criterion Values：照合する IM サービスを指定します。
  - Chat：IM メッセージ チャット サービスを照合します。
  - Conference：IM コンファレンス サービスを照合します。
  - File Transfer：IM ファイル転送サービスを照合します。
  - Games：IM ゲーム サービスを照合します。
  - Voice Chat：IM 音声チャット サービスを照合します（Yahoo の IM は対象外です）。
  - Web Cam：IM Web カメラ サービスを照合します。
- Version Criterion Values：IM ファイル転送サービスで照合するバージョンを指定します。正規表現で照合します。
  - Regular Expression：照合する定義された正規表現を一覧表示します。
  - Manage：Manage Regular Expressions ダイアログボックスが開き、正規表現を設定できます。
  - Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。
  - Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップを設定できます。
- Client Login Name Criterion Values：IM サービスで照合するクライアント ログイン名を指定します。正規表現で照合します。
  - Regular Expression：照合する定義された正規表現を一覧表示します。
  - Manage：Manage Regular Expressions ダイアログボックスが開き、正規表現を設定できます。
  - Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。
  - Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップを設定できます。
- Client Peer Login Name Criterion Values：IM サービスで照合するクライアントのピア ログイン名を指定します。正規表現で照合します。
  - Regular Expression：照合する定義された正規表現を一覧表示します。
  - Manage：Manage Regular Expressions ダイアログボックスが開き、正規表現を設定できます。
  - Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。
  - Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップを設定できます。
- Source IP Address Criterion Values：IM サービスで照合する送信元 IP アドレスを指定します。
  - IP Address：IM サービスの送信元 IP アドレスを入力します。
  - IP Mask：送信元 IP アドレスのマスクです。
- Destination IP Address Criterion Values：IM サービスで照合する宛先 IP アドレスを指定します。
  - IP Address：IM サービスの宛先 IP アドレスを入力します。
  - IP Mask：宛先 IP アドレスのマスクです。
- Filename Criterion Values：IM ファイル転送サービスで照合するファイル名を指定します。正規表現で照合します。
  - Regular Expression：照合する定義された正規表現を一覧表示します。
  - Manage：Manage Regular Expressions ダイアログボックスが開き、正規表現を設定できます。
  - Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。
  - Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップを設定できます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

SIP Class Map

SIP Class Map パネルでは、SIP 検査のクラスマップを設定できます。

検査クラスマップで、アプリケーションのトラフィックをアプリケーション固有の基準と照合します。次に、クラスマップを検査マップから特定して、アクションをイネーブルにします。クラスマップを作成することと検査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。検査クラスマップは DNS、FTP、H.323、HTTP、IM、SIP のアプリケーションでサポートされます。

フィールド

- Name：SIP クラスマップの名前を示します。
- Match Conditions：クラスマップに設定されているタイプ、照合基準、値を示します。
  - Match Type：一致タイプを示します。肯定一致と否定一致があります。
  - Criterion：SIP クラスマップの基準を示します。
  - Value：SIP クラスマップで照合する値を示します。
- Description：クラスマップの説明を示します。
- Add：SIP クラスマップを追加します。
- Edit：SIP クラスマップを編集します。
- Delete：SIP クラスマップを削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit SIP Traffic Class Map

Add/Edit SIP Traffic Class Map ダイアログボックスでは、SIP クラスマップを定義できます。

フィールド

- Name：SIP クラスマップの名前を 40 文字以内で入力します。
- Description：SIP クラスマップの説明を入力します。
- Add：SIP クラスマップを追加します。
- Edit：SIP クラスマップを編集します。
- Delete：SIP クラスマップを削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit SIP Match Criterion

Add/Edit SIP Match Criterion ダイアログボックスでは、SIP クラスマップの照合基準と値を定義できます。

フィールド

- Match Type：基準に一致したトラフィックをクラスマップに含めるか、または一致しないトラフィックを含めるか指定します。

  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。
- Criterion：SIP トラフィックに適用する照合基準を指定します。
  - Called Party：To ヘッダーに指定された受信側を照合します。
  - Calling Party：From ヘッダーに指定された発信元を照合します。
  - Content Length：ヘッダーのコンテンツの長さを照合します。0 ～ 65536 の範囲の値です。
  - Content Type：ヘッダーのコンテンツ タイプを照合します。
  - IM Subscriber：SIP IM の加入者を照合します。
  - Message Path：SIP の Via ヘッダーを照合します。
  - Request Method：SIP の要求方式を照合します。
  - Third-Party Registration：サード パーティの登録要求者を照合します。
  - URI Length：SIP ヘッダーにある URI を照合します。0 ～ 65536 の範囲の値です。
- Called Party Criterion Values：照合する受信側を指定します。正規表現で照合します。
  - Regular Expression：照合する定義された正規表現を一覧表示します。
  - Manage : Manage Regular Expressions ダイアログボックスが開き、正規表現を設定できます。
  - Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。
  - Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップを設定できます。
- Calling Party Criterion Values：照合する発信元を指定します。正規表現で照合します。
  - Regular Expression：照合する定義された正規表現を一覧表示します。
  - Manage : Manage Regular Expressions ダイアログボックスが開き、正規表現を設定できます。
  - Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。
  - Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップを設定できます。
- Content Length Criterion Values：指定値より長い SIP コンテンツ ヘッダーを照合します。
  - Greater Than Length：ヘッダーの長さをバイト単位で入力します。
- Content Type Criterion Values：照合する SIP コンテンツ ヘッダーのタイプを指定します。
  - SDP：SDP タイプの SIP コンテンツ ヘッダーを照合します。
  - Regular Expression：正規表現を照合します。

Regular Expression：照合する定義された正規表現を一覧表示します。

Manage : Manage Regular Expressions ダイアログボックスが開き、正規表現を設定できます。

Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。

Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップを設定できます。

- IM Subscriber Criterion Values：照合する IM 登録者を指定します。正規表現で照合します。
  - Regular Expression：照合する定義された正規表現を一覧表示します。
  - Manage : Manage Regular Expressions ダイアログボックスが開き、正規表現を設定できます。
  - Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。
  - Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップを設定できます。
- Message Path Criterion Values : 照合する SIP の Via ヘッダーを指定します。正規表現で照合します。
  - Regular Expression：照合する定義された正規表現を一覧表示します。
  - Manage : Manage Regular Expressions ダイアログボックスが開き、正規表現を設定できます。
  - Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。
  - Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップを設定できます。
- Request Method Criterion Values：照合する SIP 要求方式を指定します。
  - Request Method : 次の中から要求方式を指定します。ack、bye、cancel、info、invite、message、notify、options、prack、refer、register、subscribe、unknown、update。
- Third-Party Registration Criterion Values : 照合するサード パーティの登録要求者を指定します。正規表現で照合します。
  - Regular Expression：照合する定義された正規表現を一覧表示します。
  - Manage : Manage Regular Expressions ダイアログボックスが開き、正規表現を設定できます。
  - Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。
  - Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップを設定できます。
- URI Length Criterion Values：SIP ヘッダーで指定した値より長い、選択したタイプの URI を照合します。
  - URI type：SIP URI または TEL URI を指定して照合します。
  - Greater Than Length：長さをバイト単位で指定します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

検査マップのフィールドの説明

この項では、検査マップを設定する方法について説明します。次の項目を取り上げます。

（注）　RADIUS 検査マップの詳細については、P.23-9 の「管理トラフィックのサービス ポリシー ルールの追加」を参照してください。

セキュリティ アプライアンスのステートフル アプリケーション検査にアルゴリズムを適用して、アプリケーションのセキュリティとサービスを保証します。アプリケーションの中には特別な処理を必要とするものがあり、専用の検査エンジンでそのような場合に対応します。専用の検査エンジンが必要なアプリケーションとは、ユーザのデータ パケットの中に IP アドレッシング情報を埋め込むサービスや、ダイナミック割り当てポートでセカンダリ チャネルを開くサービスなどです。

アプリケーション検査エンジンは NAT と連携し、アドレッシング情報が埋め込まれている場所の識別をサポートします。これによって、このような埋め込みアドレスを NAT で変換したり、変換の影響を受けるチェックサムやその他のフィールドをアップデートしたりできます。

各アプリケーション検査エンジンはセッションを監視して、セカンダリ チャネルのポート番号も確認します。多くのプロトコルは、パフォーマンスを向上させるために、TCP または UDP のセカンダリ ポートを開きます。ウェルノウン ポート上の初期セッションは、ダイナミックに割り当てられたポート番号をネゴシエートするために使用されます。アプリケーション検査エンジンは、この初期セッションを監視し、ダイナミックに割り当てられたポートを特定し、所定のセッションの間、それらのポート上でのデータ交換を許可します。

また、ステートフル アプリケーション検査により、検査中のプロトコルの過程で発行されたコマンドと応答の有効性を監査します。セキュリティ アプライアンスは攻撃を確実に防御するため、トラフィックが検査されるプロトコルごとに RFC 仕様に準拠しているかどうかチェックします。

検査マップ機能で、専用のプロトコル検査エンジンを作成できます。検査マップを利用して、プロトコル検査エンジンのコンフィギュレーションを保存します。それから、グローバル セキュリティ ポリシーや特定のインターフェイスのセキュリティ ポリシーを使用して特定のトラフィック タイプにマップを関連付け、検査マップのコンフィギュレーション設定をイネーブルにします。

Security Policy ペインの Service Policy Rules タブから検査マップをトラフィックに適用すると、サービス ポリシーで指定した基準に従って照合が行われます。サービス ポリシーは、セキュリティ アプライアンスの特定のインターフェイスまたはすべてのインターフェイスに適用することができます。

DCERPC	DCERPC 検査で、DCERPC 検査マップを作成、表示、管理します。DCERPC マップでクライアントとエンドポイント マッパーの間で送受される DCERPC メッセージを検査し、必要に応じてセカンダリ接続に NAT を適用します。DCERPC はリモート プロシージャ コール メカニズムの仕様です。
DNS	DNS 検査で、DNS 検査マップを作成、表示、管理します。このマップを使用して DNS メッセージをより詳細に制御し、DNS スプーフィングとキャッシュ ポイズニングを保護できます。DNS は、IP アドレスやメール サーバなどのドメイン名の情報を解決します。
ESMTP	ESMTP 検査で、ESMTP 検査マップを作成、表示、管理します。ESMTP マップを使用してアプリケーションのセキュリティおよびプロトコル準拠性を検査し、攻撃の防御、送信者や受信者のブロック、メール中継のブロックができます。ESMTP（Extended SMTP）は SMTP 規格のプロトコル拡張を定義します。
FTP	FTP 検査で、FTP 検査マップを作成、表示、管理します。インターネットなど、TCP/IP ネットワークを介してファイルを転送する通信プロトコルです。FTP マップを使用して、セキュリティ アプライアンスを通過したり FTP サーバに到達したりする FTP PUT などの、特定の FTP プロトコル方式をブロックできます。
GTP	GTP 検査で、GTP 検査マップを作成、表示、管理します。GTP は比較的新しいプロトコルで、インターネットなど TCP/IP ネットワークと無線接続する場合のセキュリティを提供します。GTP マップを使用して、タイムアウト値、メッセージ サイズ、トンネル数、セキュリティ アプライアンスを通過する GTP バージョンを制御できます。
H.323	H.323 検査で、H.323 検査マップを作成、表示、管理します。H.323 マップを使用して、RAS、H.225、H.245 の VoIP プロトコルを検査し、ステートのトラッキングとフィルタリングができます。
HTTP	HTTP 検査で、HTTP 検査マップを作成、表示、管理します。HTTP はワールドワイド ウェブのクライアントとサーバ間の通信で使用されるプロトコルです。HTTP マップを使用して、RFC 準拠の HTTP ペイロード コンテンツ タイプを設定できます。また、特定の HTTP 方式をブロックし、一部のトンネル アプリケーションによる HTTP 転送を防止できます。
IM	IM 検査で、IM 検査マップを作成、表示、管理します。IM マップを使用してネットワークの使用を制御し、IM アプリケーションによる機密情報の漏洩や他のネットワークの脅威を防止できます。
IPSec Pass Through	IPSec パススルー検査で、IPSec パススルーの検査マップを作成、表示、管理します。IPSec パススルー マップを使用すると、アクセスリストを参照しなくても、特定のフローを許可できます。
MGCP	MGCP 検査で、MGCP 検査マップを作成、表示、管理します。MGCP マップを使用して、VoIP デバイスと MGCP コール エージェント間の接続を管理できます。
NetBIOS	NetBIOS 検査で、NetBIOS 検査マップを作成、表示、管理します。NetBIOS マップを使用して、NetBIOS プロトコルに確実に準拠し、フィールドの数と長さの整合性やメッセージなどをチェックできます。
RADIUS Accounting	RADIUS Accounting 検査で、RADIUS Accounting 検査マップを作成、表示、管理します。RADIUS マップを使用すると、過剰請求攻撃を防御できます。

RTSP	RTSP 検査で、RTSP 検査マップを作成、表示、管理できます。RTSP マップを使用して、RTSP PAT を含む RTSP トラフィックを保護できます。
SCCP（Skinny）	SCCP（Skinny）検査で、SCCP（Skinny）の検査マップを作成、表示、管理します。SCCP マップを使用して、プロトコル準拠チェックと基本的なステート トラッキングができます。
SIP	SIP 検査で、SIP の検査マップを作成、表示、管理します。SIP マップを使用して、アプリケーションのセキュリティとプロトコル準拠をチェックし、SIP を利用した攻撃を防御できます。SIP は、インターネット会議、テレフォニー、プレゼンス、イベント通知、インスタント メッセージ機能で幅広く利用されているプロトコルです。
SNMP	SNMP 検査で、SNMP の検査マップを作成、表示、管理します。SNMP は、ネットワーク管理デバイスとネットワーク管理ステーション間の通信に利用されるプロトコルです。SNMP マップを使用して、SNMP v1、2、2c、3 など特定の SNMP バージョンをブロックできます。

DCERPC Inspect Map

DCERPC ペインでは、DCERPC アプリケーションの事前に設定された検査マップを表示できます。DCERPC マップでは、DCERPC アプリケーション検査のデフォルト設定値を変更できます。

DCERPC は、Microsoft のクライアント / サーバ アプリケーションで広く使われているプロトコルです。このプロトコルによって、ソフトウェア クライアントがサーバにあるプログラムをリモートで実行できるようになります。

通常、このプロトコルの接続では、クライアントがウェルノウン 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（EPM）というサーバに、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のインスタンスへのセカンダリ接続を確立します。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 を行います。

DCERPC 検査マップは、TCP のウェルノウン ポート 135 を経由した、EPM とクライアント間のネイティブ TCP の通信を検査します。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は、どのセキュリティ ゾーンにあってもかまいません。サーバの埋め込まれた 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のポート番号で複数の接続を確立する可能性があるので、ピンホールを複数使用でき、ユーザがそのタイムアウトを設定できるようになっています。

フィールド

- DCERPC Inspect Maps：定義されている DCERPC 検査マップを一覧表示するテーブルです。
- Add：新しい DCERPC 検査マップを設定します。DCERPC 検査マップを編集するには、DCERPC Inspect Maps テーブルで DCERPC のエントリを選択し、Customize をクリックします。
- Delete：DCERPC Inspect Maps テーブルで選択した検査マップを削除します。
- Security Level：セキュリティ レベル（High、Medium、Low）を選択します。
  - Low

    ピンホールのタイムアウト：00:02:00

    エンドポイント マッパー サービス：適用強制しない

    エンドポイント マッパー サービス ルックアップ：イネーブル

    エンドポイント マッパー サービス ルックアップのタイムアウト：00:05:00
  - Medium：デフォルト

    ピンホールのタイムアウト：00:01:00

    エンドポイント マッパー サービス：適用強制しない

エンドポイント マッパー サービス ルックアップ：ディセーブル

- High

  ピンホールのタイムアウト：00:01:00

  エンドポイント マッパー サービス：適用強制する

  エンドポイント マッパー サービス ルックアップ：ディセーブル

- Customize：Add/Edit DCERPC Policy Map ダイアログボックスを開き、追加の設定を行います。
- Default Level：セキュリティ レベルをデフォルトの Medium レベルに戻します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit DCERPC Policy Map

Add/Edit DCERPC Policy Map ペインでは、DCERPC アプリケーション検査マップのセキュリティ レベルとパラメータを設定できます。

フィールド

- Name：DCERPC マップの追加時に DCERPC マップの名前を入力します。DCERPC マップの編集時には、事前に設定した DCERPC マップの名前が表示されます。
- Description：DCERPC マップの説明を 200 文字以内で入力します。
- Security Level：セキュリティ レベル（High、Medium、Low）を選択します。
  - Low

    ピンホールのタイムアウト：00:02:00

    エンドポイント マッパー サービス：適用強制しない

    エンドポイント マッパー サービス ルックアップ：イネーブル

    エンドポイント マッパー サービス ルックアップのタイムアウト：00:05:00

  - Medium：デフォルト

    ピンホールのタイムアウト：00:01:00

    エンドポイント マッパー サービス：適用強制しない

    エンドポイント マッパー サービス ルックアップ：ディセーブル

  - High

    ピンホールのタイムアウト：00:01:00

    エンドポイント マッパー サービス：適用強制する

    エンドポイント マッパー サービス ルックアップ：ディセーブル

  - Default Level：セキュリティ レベルをデフォルトの Medium レベルに戻します。
- Details：詳細な設定を行うためのパラメータを表示します。
  - 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。0:0:1 ～ 1193:0:0 の範囲で指定します。デフォルト値は 2 分です。

- Enforce endpoint-mapper service：バインディング中にエンドポイント マッパー サービスを適用します。
- 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をイネーブルにします。ディセーブルの場合、ピンホール タイムアウトが適用されます。

  Enforce Service Lookup Timeout：指定されたサービス ルックアップ タイムアウトを適用します。

  Service Lookup Timeout：ルックアップでピンホールした場合のタイムアウトを設定します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

DNS Inspect Map

DNS ペインでは、DNS アプリケーションの事前に設定された検査マップを表示できます。DNS マップでは、DNS アプリケーション検査のデフォルト設定値を変更できます。

DNS アプリケーション検査は、DNS スプーフィングとキャッシュ ポイズニングを防ぐための DNS メッセージの管理機能をサポートしています。ユーザが設定できるルールを使用して、特定の DNS タイプを許可、ドロップ、ロギングし、他の DNS タイプをブロックすることができます。たとえば、ゾーン転送をこの機能のあるサーバ間だけに制限します。

公開サーバが特定の内部ゾーンだけをサポートしている場合に、DNS パケットのヘッダーにある Recursion Desired フラグと Recursion Available フラグをマスクして、サーバを攻撃から守ることができます。また、DNS のランダム化をイネーブルにすると、ランダム化をサポートしていないサーバや強度の低い擬似乱数ジェネレータを使用するサーバのスプーフィングやキャッシュ ポイズニングを回避できます。照会できるドメイン名を制限することにより、公開サーバの保護がさらに確実になります。

DNS の不一致の応答数が増える（キャッシュ ポイズニング攻撃を示す可能性があります）と、DNS の不一致のアラートを設定して通知されるようします。さらに、DNS のすべてのメッセージに Transaction Signature（TSIG; トランザクション シグニチャ）を付け、メッセージをチェックする設定も行えます。

フィールド

- DNS Inspect Maps：定義されている DNS 検査マップを一覧表示するテーブルです。
- Add：新しい DNS 検査マップを設定します。DNS 検査マップを編集するには、DNS Inspect Maps テーブルで DNS のエントリを選択し、Customize をクリックします。
- Delete：DNS Inspect Maps テーブルで選択した検査マップを削除します。
- Security Level：セキュリティ レベル（High、Medium、Low）を選択します。
  - Low：デフォルト

    DNS Guard：イネーブル

    NAT のリライト：イネーブル

    プロトコル適用：イネーブル

    ID のランダム化：ディセーブル

    メッセージの長さのチェック：イネーブル

メッセージの最大長：512
不一致レートのロギング：ディセーブル
TSIG リソース レコード：適用強制しない

- Medium

DNS Guard：イネーブル
NAT のリライト：イネーブル
プロトコル適用：イネーブル
ID のランダム化：イネーブル
メッセージの長さのチェック：イネーブル
メッセージの最大長：512
不一致レートのロギング：イネーブル
TSIG リソース レコード：適用強制しない

- High

DNS Guard：イネーブル
NAT のリライト：イネーブル
プロトコル適用：イネーブル
ID のランダム化：イネーブル
メッセージの長さのチェック：イネーブル
メッセージの最大長：512
不一致レートのロギング：イネーブル
TSIG リソース レコード：適用強制する

- Customize：Add/Edit DNS Policy Map ダイアログボックスを開き、追加の設定を行います。
- Default Level：セキュリティ レベルをデフォルトの Low レベルに戻します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit DNS Policy Map（セキュリティ レベル）

Add/Edit DNS Policy Map ペインでは、DNS アプリケーション検査マップのセキュリティ レベルと追加の設定値を設定できます。

フィールド

- Name：DNS マップの追加時に DNS マップの名前を入力します。DNS マップの編集時には、事前に設定した DNS マップの名前が表示されます。
- Description：DNS マップの説明を 200 文字以内で入力します。
- Security Level：セキュリティ レベル（High、Medium、Low）を選択します。

- Low：デフォルト

DNS Guard：イネーブル
NAT のリライト：イネーブル

プロトコル適用：イネーブル
ID のランダム化：ディセーブル
メッセージの長さのチェック：イネーブル
メッセージの最大長：512
不一致レートのロギング：ディセーブル
TSIG リソース レコード：適用強制しない

- Medium

DNS Guard：イネーブル
NAT のリライト：イネーブル
プロトコル適用：イネーブル
ID のランダム化：イネーブル
メッセージの長さのチェック：イネーブル
メッセージの最大長：512
不一致レートのロギング：イネーブル
TSIG リソース レコード：適用強制しない

- High

DNS Guard：イネーブル
NAT のリライト：イネーブル
プロトコル適用：イネーブル
ID のランダム化：イネーブル
メッセージの長さのチェック：イネーブル
メッセージの最大長：512
不一致レートのロギング：イネーブル
TSIG リソース レコード：適用強制する

- Default Level：セキュリティ レベルをデフォルトの Low レベルに戻します。

- Details：詳細な設定を行うための Protocol Conformance タブ、Filtering タブ、Mismatch Rate タブ、および Inspection タブを表示します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit DNS Policy Map（詳細）

Add/Edit DNS Policy Map ペインでは、DNS アプリケーション検査マップのセキュリティ レベルと追加の設定値を設定できます。

フィールド

- Name：DNS マップの追加時に DNS マップの名前を入力します。DNS マップの編集時には、事前に設定した DNS マップの名前が表示されます。
- Description：DNS マップの説明を 200 文字以内で入力します。
- Security Level：設定するセキュリティ レベルを表示します。

- Protocol Conformance：このタブで DNS のプロトコル準拠を設定します。
  - Enable DNS guard function：DNS ヘッダーの識別フィールドを使用して、DNS クエリーと応答の不一致のチェックを行います。1 つのクエリーに対して 1 つの応答がセキュリティアプライアンスを通過できます。
  - Enable NAT re-write function：DNS 応答の A レコードにある IP アドレスの変換をイネーブルにします。
  - Enable protocol enforcement：DNS メッセージの形式チェックをイネーブルにします。ドメイン名、ラベルの長さ、圧縮、ループしたポインタなどをチェックします。
  - Randomize the DNS identifier for DNS query：DNS クエリー メッセージの DNS 識別子をランダム化します。
  - Enforce TSIG resource record to be present in DNS message：TSIG リソース レコードが DNS トランザクションに存在する必要があります。TSIG を強制的に適用すると、次のアクションが実行されます。

    Drop packet：パケットをドロップします（ロギングはイネーブルまたはディセーブルに指定できます）。

    Log：ロギングをイネーブルにします。
- Filtering：このタブで DNS のフィルタリングを設定します。
  - Global Settings：設定がグローバルに適用されます。

    Drop packets that exceed specified maximum length (global)：最大長（バイト）を超えるパケットをドロップします。

    Maximum Packet Length：パケットの最大長をバイト単位で入力します。
  - Server Settings：サーバの設定だけを適用します。

    Drop packets that exceed specified maximum length：最大長（バイト）を超えるパケットをドロップします。

    Maximum Packet Length：パケットの最大長をバイト単位で入力します。

    Drop packets sent to server that exceed length indicated by the RR：Resource Record で指定された長さを超えるパケットがサーバに送信された場合はドロップします。
  - Client Settings：クライアントの設定だけを適用します。

    Drop packets that exceed specified maximum length：最大長（バイト）を超えるパケットをドロップします。

    Maximum Packet Length：パケットの最大長をバイト単位で入力します。

    Drop packets sent to client that exceed length indicated by the RR：Resource Record で指定された長さを超えるパケットがクライアントに送信された場合はドロップします。
- Mismatch Rate：このタブで DNS の ID 不一致レートを設定します。
  - Enable Logging when DNS ID mismatch rate exceeds specified rate：DNS 識別子の不一致が多く発生した場合にレポートを表示します。

    Mismatch Instance Threshold：不一致のインスタンスの最大数を入力します。この値を超えると、システム メッセージ ログに出力されます。

    Time Interval：監視間隔時間（秒単位）を入力します。
- Inspections：このタブで DNS 検査のコンフィギュレーションを表示して、追加や編集ができます。
  - Match Type：一致タイプを示します。肯定一致と否定一致があります。
  - Criterion：DNS 検査の基準を示します。
  - Value：DNS 検査で照合する値を示します。
  - Action：照合条件が一致したときのアクションを示します。
  - Log：ログの状態を示します。
  - Add：Add DNS Inspect ダイアログボックスが開き、DNS 検査を追加できます。
  - Edit：Edit DNS Inspect ダイアログボックスが開き、DNS 検査を編集できます。

- Delete：DNS 検査を削除します。
- Move Up：検査をリストの上に移動します。
- Move Down：検査をリストの下に移動します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit DNS Inspect

Add/Edit DNS Inspect ダイアログボックスでは、DNS 検査マップの照合基準と値を定義できます。

フィールド

- Single Match：DNS 検査に照合文が 1 つだけの場合に指定します。
- Match Type：トラフィックと値を一致させるかどうかを指定します。

  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。
- Criterion：DNS トラフィックに適用する照合基準を指定します。
  - Header Flag：ヘッダーの DNS フラグを照合します。
  - Type：DNS クエリーまたはリソース レコードのタイプを照合します。
  - Class：DNS クエリーまたはリソース レコードのクラスを照合します。
  - Question：DNS の問い合せを照合します。
  - Resource Record：DNS リソース レコードを照合します。
  - Domain Name：DNS クエリーやリソース レコードのドメイン名を照合します。
- Header Flag Criterion Values：DNS ヘッダー フラグの照合値の詳細を指定します。
  - Match Option：完全一致または全ビット一致（ビット マスク一致）のどちらかを指定します。
  - Match Value：ヘッダー フラグについて名前と値のどちらを照合するか指定します。

    Header Flag Name：照合するヘッダー フラグ名を 1 つ以上選択できます。AA（authoritative answer）、QR（query）、RA（recursion available）、RD（recursion denied）、TC（truncation）のフラグ ビットがあります。

    Header Flag Value：任意の 16 ビットの値を 16 進数で入力して照合できます。
- Type Criterion Values：DNS タイプの照合値の詳細を指定します。
  - DNS Type Field Name：選択する DNS タイプを一覧表示します。

    A：IPv4 アドレス

    NS：信頼できるネーム サーバ

    CNAME：正規名

    SOA：信頼ゾーンの開始

    TSIG：トランザクション シグニチャ

    IXFR：差分（ゾーン）転送

    AXFR：完全（ゾーン）転送

  - DNS Type Field Value：DNS タイプ フィールドについて値と範囲のどちらを照合するか指定します。

    Value：0 ～ 65535 の範囲の値を入力して照合できます。

    Range：範囲を入力して照合します。両方とも 0 ～ 65535 の範囲の値を指定します。
- Class Criterion Values：DNS クラスの照合値の詳細を指定します。
  - DNS Class Field Name：インターネットで照合する DNS クラス フィールド名を指定します。
  - DNS Class Field Value：DNS クラス フィールドについて値と範囲のどちらを照合するか指定します。

    Value：0 ～ 65535 の範囲の値を入力して照合できます。

    Range：範囲を入力して照合します。両方とも 0 ～ 65535 の範囲の値を指定します。
- Question Criterion Values：DNS の問い合せセクションの照合方法を指定します。
- Resource Record Criterion Values：DNS リソース レコードのセクションの照合方法を指定します。
  - Resource Record：照合対象セクションを一覧表示します。

    Additional：DNS 追加リソース レコード

    Answer：DNS 応答リソース レコード

    Authority：DNS 認証リソース レコード
- Domain Name Criterion Values：DNS ドメイン名の照合方法を指定します。
  - Regular Expression：照合する定義された正規表現を一覧表示します。
  - Manage：Manage Regular Expressions ダイアログボックスが開き、正規表現を設定できます。
  - Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。
  - Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップを設定できます。
- Multiple Matches：DNS 検査の複数の照合文を指定します。
  - DNS Traffic Class：DNS トラフィック クラスを照合します。
  - Manage：Manage DNS Class Maps ダイアログボックスが開き、DNS クラスマップの追加、編集、削除ができます。
- Actions：プライマリ アクションおよびログを設定します。
  - Primary Action：マスク、パケットをドロップ、接続をドロップ、なし。
  - Log：イネーブルまたはディセーブルにします。
  - Enforce TSIG：適用強制しない、パケットをドロップ、ログに出力、パケットをドロップしてログに出力。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Manage Class Maps

Manage Class Map ダイアログボックスでは、検査のクラスマップを設定できます。

検査クラスマップで、アプリケーションのトラフィックをアプリケーション固有の基準と照合します。次に、クラスマップを検査マップから特定して、アクションをイネーブルにします。クラスマップを作成することと検査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。検査クラスマップは DNS、FTP、H.323、HTTP、インスタント メッセージ（IM）、SIP のアプリケーションでサポートされます。

フィールド

- Name：クラスマップの名前を示します。
- Match Conditions：クラスマップに設定されているタイプ、照合基準、値を示します。
  - Match Type：一致タイプを示します。肯定一致と否定一致があります。
  - Criterion：クラスマップの基準を示します。
  - Value：クラスマップで照合する値を示します。
- Description：クラスマップの説明を示します。
- Add：クラスマップの照合条件を追加します。
- Edit：クラスマップの照合条件を編集します。
- Delete：クラスマップの照合条件を削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

ESMTP Inspect Map

ESMTP ペインでは、ESMTP アプリケーションの事前に設定された検査マップを表示できます。ESMTP マップでは、ESMTP アプリケーション検査のデフォルト設定値を変更できます。

スパム、フィッシング、不正な形式のメッセージ、バッファ オーバーフロー / アンダーフローなどの攻撃の大部分は ESMTP トラフィックから発生するので、ESMTP トラフィックのパケットを詳細に検査して制御します。アプリケーション セキュリティとプロトコルで正常な ESMTP メッセージだけを通し、各種の攻撃の検出、送受信者およびメール中継のブロックも行います。

フィールド

- ESMTP Inspect Maps：定義されている ESMTP 検査マップを一覧表示するテーブルです。
- Add：新しい ESMTP 検査マップを設定します。ESMTP 検査マップを編集するには、ESMTP Inspect Maps テーブルで ESMTP のエントリを選択し、Customize をクリックします。
- Delete：ESMTP Inspect Maps テーブルで選択した検査マップを削除します。
- Security Level：セキュリティ レベル（High、Medium、Low）を選択します。
  - Low：デフォルト
    コマンドラインの長さが 512 を超える場合、ログを出力
    コマンドの宛先の数が 100 を超える場合、ログを出力

本文の行の長さが 1000 を超える場合、ログを出力
送信者のアドレスの長さが 320 を超える場合、ログを出力
MIME ファイル名の長さが 255 を超える場合、ログを出力

- Medium

  サーバ バナーを難読化
  コマンドラインの長さが 512 を超える場合、接続をドロップ
  コマンドの宛先の数が 100 を超える場合、接続をドロップ
  本文の行の長さが 1000 を超える場合、接続をドロップ
  送信者のアドレスの長さが 320 を超える場合、接続をドロップ
  MIME ファイル名の長さが 255 を超える場合、接続をドロップ

- High

  サーバ バナーを難読化
  コマンドラインの長さが 512 を超える場合、接続をドロップ
  コマンドの宛先の数が 100 を超える場合、接続をドロップ
  本文の行の長さが 1000 を超える場合、接続をドロップ
  送信者のアドレスの長さが 320 を超える場合、接続をドロップしてログを出力
  MIME ファイル名の長さが 255 を超える場合、接続をドロップしてログを出力

- MIME File Type Filtering : MIME Type Filtering ダイアログボックスを開き、MIME ファイル タイプのフィルタを設定します。
- Customize : Add/Edit ESMTP Policy Map ダイアログボックスを開き、追加の設定を行います。
- Default Level：セキュリティ レベルをデフォルトの Low レベルに戻します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

MIME File Type Filtering

MIME File Type Filtering ダイアログボックスでは、MIME ファイル タイプのフィルタを設定できます。

フィールド

- Match Type：一致タイプを示します。肯定一致と否定一致があります。
- Criterion：検査の基準を示します。
- Value：検査で照合する値を示します。
- Action：照合条件が一致したときのアクションを示します。
- Log：ログの状態を示します。
- Add : Add MIME File Type Filter ダイアログボックスが開き、MIME ファイル タイプのフィルタを追加できます。
- Edit : Edit MIME File Type Filter ダイアログボックスが開き、MIME ファイル タイプのフィルタを編集できます。
- Delete：MIME ファイル タイプのフィルタを削除します。

- Move Up：エントリをリストの上に移動します。
- Move Down：エントリをリストの下に移動します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit ESMTP Policy Map（セキュリティ レベル）

Add/Edit ESMTP Policy Map ペインでは、ESMTP アプリケーション検査マップのセキュリティ レベルと追加の設定値を設定できます。

フィールド

- Name：ESMTP マップの追加時に ESMTP マップの名前を入力します。ESMTP マップの編集時には、事前に設定した ESMTP マップの名前が表示されます。
- Description：ESMTP マップの説明を 200 文字以内で入力します。
- Security Level：セキュリティ レベル（High、Medium、Low）を選択します。
  - Low：デフォルト

    コマンドラインの長さが 512 を超える場合、ログを出力

    コマンドの宛先の数が 100 を超える場合、ログを出力

    本文の行の長さが 1000 を超える場合、ログを出力

    送信者のアドレスの長さが 320 を超える場合、ログを出力

    MIME ファイル名の長さが 255 を超える場合、ログを出力
  - Medium

    サーバ バナーを難読化

    コマンドラインの長さが 512 を超える場合、接続をドロップ

    コマンドの宛先の数が 100 を超える場合、接続をドロップ

    本文の行の長さが 1000 を超える場合、接続をドロップ

    送信者のアドレスの長さが 320 を超える場合、接続をドロップ

    MIME ファイル名の長さが 255 を超える場合、接続をドロップ
  - High

    サーバ バナーを難読化

    コマンドラインの長さが 512 を超える場合、接続をドロップ

    コマンドの宛先の数が 100 を超える場合、接続をドロップ

    本文の行の長さが 1000 を超える場合、接続をドロップ

    送信者のアドレスの長さが 320 を超える場合、接続をドロップしてログを出力

    MIME ファイル名の長さが 255 を超える場合、接続をドロップしてログを出力
  - MIME File Type Filtering : MIME Type Filtering ダイアログボックスを開き、MIME ファイル タイプのフィルタを設定します。
  - Default Level：セキュリティ レベルをデフォルトの Low レベルに戻します。
- Details：詳細な設定を行うための Parameters タブと Inspections タブを表示します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit ESMTP Policy Map（詳細）

Add/Edit ESMTP Policy Map ペインでは、ESMTP アプリケーション検査マップのセキュリティ レベルと追加の設定値を設定できます。

フィールド

- Name：ESMTP マップの追加時に ESMTP マップの名前を入力します。ESMTP マップの編集時には、事前に設定した ESMTP マップの名前が表示されます。
- Description：ESMTP マップの説明を 200 文字以内で入力します。
- Security Level：設定するセキュリティ レベルと MIME ファイル タイプ フィルタリング設定を表示します。
- Parameters：このタブで ESMTP 検査マップのパラメータを設定します。
  - Mask server banner：バナーを難読化します。
  - Configure Mail Relay：ESMTP のメール中継をイネーブルにします。

    Domain Name：ローカル ドメインを指定します。

    Action：接続をドロップまたはログに出力します。

    Log：イネーブルまたはディセーブルにします。
- Inspections：このタブで ESMTP 検査のコンフィギュレーションを表示して、追加や編集ができます。
  - Match Type：一致タイプを示します。肯定一致と否定一致があります。
  - Criterion：ESMTP 検査の基準を示します。
  - Value：ESMTP 検査で照合する値を示します。
  - Action：照合条件が一致したときのアクションを示します。
  - Log：ログの状態を示します。
  - Add：Add ESMTP Inspect ダイアログボックスが開き、ESMTP 検査を追加できます。
  - Edit：Edit ESMTP Inspect ダイアログボックスが開き、ESMTP 検査を編集できます。
  - Delete：ESMTP 検査を削除します。
  - Move Up：検査をリストの上に移動します。
  - Move Down：検査をリストの下に移動します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit ESMTP Inspect

Add/Edit ESMTP Inspect ダイアログボックスでは、ESMTP 検査マップの照合基準と値を定義できます。

フィールド

- Match Type：トラフィックと値を一致させるかどうかを指定します。

  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。
- Criterion：ESMTP トラフィックに適用する照合基準を指定します。
  - Body Length：本文の長さと指定した長さをバイト単位で照合します。
  - Body Line Length：本文の行の長さと指定した長さをバイト単位で照合します。
  - Commands：ESMTP プロトコルで交換されるコマンドを照合します。
  - Command Recipient Count：コマンド宛先の数が指定した数より大きい場合に照合します。
  - Command Line Length：コマンドラインが指定した長さより長い場合に、バイト単位で照合します。
  - EHLO Reply Parameters：ESMTP の EHLO 応答パラメータを照合します。
  - Header Length：ヘッダーの長さと指定した長さをバイト単位で照合します。
  - Header To Fields Count：ヘッダーの To フィールドの数が指定した数より大きい場合に照合します。
  - Invalid Recipients Count：無効な宛先の数が指定した数より大きい場合に照合します。
  - MIME File Type：MIME ファイル タイプを照合します。
  - MIME Filename Length：MIME ファイル名を照合します。
  - MIME Encoding：MIME の符号化を照合します。
  - Sender Address：送信者の電子メール アドレスを照合します。
  - Sender Address Length：送信者の電子メール アドレスの長さを照合します。
- Body Length Criterion Values：本文の長さの照合値に関する詳細を指定します。
  - Greater Than Length：本文の長さをバイト単位で指定します。
  - Action：リセット、接続をドロップ、またはログに出力します。
  - Log：イネーブルまたはディセーブルにします。
- Body Line Length Criterion Values：本文の行の長さの照合値に関する詳細を指定します。
  - Greater Than Length：本文の行の長さをバイト単位で指定します。
  - Action：リセット、接続をドロップ、またはログに出力します。
  - Log：イネーブルまたはディセーブルにします。
- Commands Criterion Values：コマンドの照合値の詳細を指定します。
  - Available Commands テーブル

    AUTH

    DATA

    EHLO

    ETRN

    HELO

    HELP

    MAIL

    NOOP

    QUIT

    RCPT

RSET
SAML
SOML
VRFY

- Add : Available Commands テーブルで選択したコマンドを Selected Commands テーブルに追加します。
- Remove：選択したコマンドを Selected Commands テーブルから削除します。
- Primary Action：Mask、Reset、Drop Connection、None、Limit Rate (pps)。
- Log：イネーブルまたはディセーブルにします。
- Rate Limit：Do not limit rate、Limit Rate (pps)。

- Command Recipient Count Criterion Values：コマンド宛先の数の照合値に関する詳細を指定します。
  - Greater Than Count：コマンド宛先の数を指定します。
  - Action：リセット、接続をドロップ、またはログに出力します。
  - Log：イネーブルまたはディセーブルにします。
- Command Line Length Criterion Values：コマンドラインの長さの値に関する詳細を指定します。
  - Greater Than Length：コマンドラインの長さをバイト単位で指定します。
  - Action：リセット、接続をドロップ、またはログに出力します。
  - Log：イネーブルまたはディセーブルにします。
- EHLO Reply Parameters Criterion Values：EHLO 応答パラメータの照合値の詳細を指定します。
  - Available Parameters テーブル

    8bitmime
    auth
    binarymime
    checkpoint
    dsn
    ecode
    etrn
    others
    pipelining
    size
    vrfy
  - Add : Available Parameters テーブルで選択したパラメータを Selected Parameters テーブルに追加します。
  - Remove：選択したコマンドを Selected Commands テーブルから削除します。
  - Action：Reset、Drop Connection、Mask、Log。
  - Log：イネーブルまたはディセーブルにします。
- Header Length Criterion Values：ヘッダーの長さの照合値に関する詳細を指定します。
  - Greater Than Length：ヘッダーの長さをバイト単位で指定します。
  - Action：Reset、Drop Connection、Mask、Log。
  - Log：イネーブルまたはディセーブルにします。
- Header To Fields Count Criterion Values：ヘッダーの To フィールド数の照合値に関する詳細を指定します。
  - Greater Than Count：コマンド宛先の数を指定します。
  - Action：リセット、接続をドロップ、またはログに出力します。

- Log：イネーブルまたはディセーブルにします。

- Invalid Recipients Count Criterion Values：無効な宛先の数の照合値に関する詳細を指定します。
  - Greater Than Count：コマンド宛先の数を指定します。
  - Action：リセット、接続をドロップ、またはログに出力します。
  - Log：イネーブルまたはディセーブルにします。
- MIME File Type Criterion Values：MIME ファイル タイプの照合値の詳細を指定します。
  - Regular Expression：照合する定義された正規表現を一覧表示します。
  - Manage : Manage Regular Expressions ダイアログボックスが開き、正規表現を設定できます。
  - Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。
  - Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップを設定できます。
  - Action：リセット、接続をドロップ、またはログに出力します。
  - Log：イネーブルまたはディセーブルにします。
- MIME Filename Length Criterion Values：MIME ファイル名の長さの照合値に関する詳細を指定します。
  - Greater Than Length：MIME ファイル名の長さをバイト単位で指定します。
  - Action：Reset、Drop Connection、Log。
  - Log：イネーブルまたはディセーブルにします。
- MIME Encoding Criterion Values：MIME の符号化の照合値に関する詳細を指定します。
  - Available Encodings テーブル

    7bit

    8bit

    base64

    binary

    others

    quoted-printable
  - Add：Available Encodings テーブルで選択したパラメータを Selected Encodings テーブルに追加します。
  - Remove：選択したコマンドを Selected Commands テーブルから削除します。
  - Action：Reset、Drop Connection、Log。
  - Log：イネーブルまたはディセーブルにします。
- Sender Address Criterion Values：送信者アドレスの照合値の詳細を指定します。
  - Regular Expression：照合する定義された正規表現を一覧表示します。
  - Manage : Manage Regular Expressions ダイアログボックスが開き、正規表現を設定できます。
  - Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。
  - Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップを設定できます。
  - Action：Reset、Drop Connection、Log。
  - Log：イネーブルまたはディセーブルにします。
- Sender Address Length Criterion Values : 送信者アドレスの長さの照合値に関する詳細を指定します。
  - Greater Than Length：送信者アドレスの長さをバイト単位で指定します。
  - Action：Reset、Drop Connection、Log。
  - Log：イネーブルまたはディセーブルにします。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

FTP Inspect Map

FTP ペインでは、FTP アプリケーションの事前に設定された検査マップを表示できます。FTP マップでは、FTP アプリケーション検査のデフォルト設定値を変更できます。

厳密な FTP 検査には、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検査には、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。ファイル名、サーバ名、および他のアトリビュートに基づいて、FTP 接続をブロックできます。検査時に 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。

フィールド

- FTP Inspect Maps：定義されている FTP 検査マップを一覧表示するテーブルです。
- Add：新しい FTP 検査マップを設定します。FTP 検査マップを編集するには、FTP Inspect Maps テーブルで FTP のエントリを選択し、Customize をクリックします。
- Delete：FTP Inspect Maps テーブルで選択した検査マップを削除します。
- Security Level：セキュリティ レベル（Medium または Low）を選択します。
  - Low

    Mask Banner：ディセーブル

    Mask Reply：ディセーブル
  - Medium：デフォルト

    Mask Banner：イネーブル

    Mask Reply：イネーブル
  - File Type Filtering：Type Filtering ダイアログボックスを開き、ファイル タイプのフィルタを設定します。
  - Customize：Add/Edit FTP Policy Map ダイアログボックスを開き、追加の設定を行います。
  - Default Level：セキュリティ レベルをデフォルトの Medium レベルに戻します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

File Type Filtering

File Type Filtering ダイアログボックスでは、ファイル タイプ フィルタを設定できます。

フィールド

- Match Type：一致タイプを示します。肯定一致と否定一致があります。
- Criterion：検査の基準を示します。
- Value：検査で照合する値を示します。
- Action：照合条件が一致したときのアクションを示します。
- Log：ログの状態を示します。
- Add：Add File Type Filter ダイアログボックスが開き、ファイル タイプのフィルタを追加できます。
- Edit：Edit File Type Filter ダイアログボックスが開き、ファイル タイプのフィルタを編集できます。
- Delete：ファイル タイプのフィルタを削除します。
- Move Up：エントリをリストの上に移動します。
- Move Down：エントリをリストの下に移動します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit FTP Policy Map（セキュリティ レベル）

Add/Edit FTP Policy Map ペインでは、FTP アプリケーション検査マップのセキュリティ レベルと追加の設定値を設定できます。

フィールド

- Name：FTP マップの追加時に FTP マップの名前を入力します。FTP マップの編集時には、事前に設定した FTP マップの名前が表示されます。
- Description：FTP マップの説明を 200 文字以内で入力します。
- Security Level：セキュリティ レベル（Medium または Low）を選択します。
  - Low

    Mask Banner：ディセーブル

    Mask Reply：ディセーブル
  - Medium：デフォルト

    Mask Banner：イネーブル

    Mask Reply：イネーブル
  - File Type Filtering：Type Filtering ダイアログボックスを開き、ファイル タイプのフィルタを設定します。
  - Default Level：セキュリティ レベルをデフォルトの Medium レベルに戻します。
- Details：詳細な設定を行うための Parameters タブと Inspections タブを表示します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit FTP Policy Map（詳細）

Add/Edit FTP Policy Map ペインでは、FTP アプリケーション検査マップのセキュリティ レベルと追加の設定値を設定できます。

フィールド

- Name : FTP マップの追加時に FTP マップの名前を入力します。FTP マップの編集時には、事前に設定した FTP マップの名前が表示されます。
- Description：FTP マップの説明を 200 文字以内で入力します。
- Security Level：設定するセキュリティ レベルとファイル タイプ フィルタリング設定を表示します。
- Parameters：このタブで FTP 検査マップのパラメータを設定します。
  - Mask greeting banner from the server：FTP サーバとの接続時に表示されるバナーをマスクし、クライアントに対するサーバ情報の公開を防止します。
  - Mask reply to SYST command : syst コマンドに対する応答をマスクし、クライアントに対するサーバ情報の公開を防止します。
- Inspections：このタブで FTP 検査のコンフィギュレーションを表示して、追加や編集ができます。
  - Match Type：一致タイプを示します。肯定一致と否定一致があります。
  - Criterion：FTP 検査の基準を示します。
  - Value：FTP 検査で照合する値を示します。
  - Action：照合条件が一致したときのアクションを示します。
  - Log：ログの状態を示します。
  - Add：Add FTP Inspect ダイアログボックスが開き、FTP 検査を追加できます。
  - Edit：Edit FTP Inspect ダイアログボックスが開き、FTP 検査を編集できます。
  - Delete：FTP 検査を削除します。
  - Move Up：検査をリストの上に移動します。
  - Move Down：検査をリストの下に移動します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit FTP Map

Add/Edit FTP Inspect ダイアログボックスでは、FTP 検査マップの照合基準と値を定義できます。

フィールド

- Single Match：FTP 検査に照合文が 1 つだけの場合に指定します。
- Match Type：トラフィックと値を一致させるかどうかを指定します。

  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。
- Criterion：FTP トラフィックに適用する照合基準を指定します。
  - Request Command：FTP 要求コマンドを照合します。
  - File Name：FTP 転送のファイル名を照合します。
  - File Type：FTP 転送のファイル タイプを照合します。
  - Server：FTP サーバを照合します。
  - User Name：FTP ユーザを照合します。
- Request Command Criterion Values：FTP 要求コマンドの照合値の詳細を指定します。
  - 要求コマンド

    APPE：ファイルに追加するコマンド

    CDUP：現在の作業ディレクトリの親ディレクトリに移動するコマンド

    DELE：ファイルを削除するコマンド

    GET：ファイルを取得するコマンド

    HELP：ヘルプ情報を提供するコマンド

    MKD：ディレクトリを作成するコマンド

    PUT：ファイルを送信するコマンド

    RMD：ディレクトリを削除するコマンド

    RNFR：変更元ファイル名を指定するコマンド

    RNTO：変更先ファイル名を指定するコマンド

    SITE：サーバ システム固有のコマンド。通常、リモート管理に使用します。

    STOU：一意のファイル名を使用してファイル名を保存するコマンド
- File Name Criterion Values：FTP ファイル名の照合値の詳細を指定します。
  - Regular Expression：照合する定義された正規表現を一覧表示します。
  - Manage : Manage Regular Expressions ダイアログボックスが開き、正規表現を設定できます。
  - Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。
  - Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップを設定できます。
- File Type Criterion Values：FTP ファイル タイプの照合値の詳細を指定します。
  - Regular Expression：照合する定義された正規表現を一覧表示します。
  - Manage : Manage Regular Expressions ダイアログボックスが開き、正規表現を設定できます。
  - Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。
  - Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップを設定できます。
- Server Criterion Values：FTP サーバの照合値の詳細を指定します。
  - Regular Expression：照合する定義された正規表現を一覧表示します。
  - Manage : Manage Regular Expressions ダイアログボックスが開き、正規表現を設定できます。
  - Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。

  - Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップを設定できます。
- User Name Criterion Values：FTP ユーザ名の照合値の詳細を指定します。
  - Regular Expression：照合する定義された正規表現を一覧表示します。
  - Manage : Manage Regular Expressions ダイアログボックスが開き、正規表現を設定できます。
  - Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。
  - Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップを設定できます。
- Multiple Matches：FTP 検査の複数の照合文を指定します。
  - FTP Traffic Class：FTP トラフィック クラスを照合します。
  - Manage : Manage FTP Class Maps ダイアログボックスが開き、FTP クラスマップの追加、編集、削除ができます。
- Action：リセットします。
- Log：イネーブルまたはディセーブルにします。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

GTP Inspect Map

GTP ペインでは、GTP アプリケーションの事前に設定された検査マップを表示できます。GTP マップでは、GTP アプリケーション検査のデフォルト設定値を変更できます。

GTP は比較的新しいプロトコルで、インターネットなど TCP/IP ネットワークと無線接続する場合のセキュリティを提供します。GTP マップを使用して、タイムアウト値、メッセージ サイズ、トンネル数、セキュリティ アプライアンスを通過する GTP バージョンを制御できます。

（注） GTP 検査には、特別なライセンスが必要です。

フィールド

- GTP Inspect Maps：定義されている GTP 検査マップを一覧表示するテーブルです。
- Add : 新しい GTP 検査マップを設定します。GTP 検査マップを編集するには、GTP Inspect Maps テーブルで GTP のエントリを選択し、Customize をクリックします。
- Delete：GTP Inspect Maps テーブルで選択した検査マップを削除します。
- Security Level：セキュリティ レベルは常に Low です。
  - エラーを許可しない
  - トンネルの最大数：500
  - GSN タイムアウト：00:30:00
  - PDP コンテキスト タイムアウト：00:30:00
  - 要求タイムアウト：00:01:00

- シグナリング タイムアウト：00:30:00
- トンネル タイムアウト：01:00:00
- T3 応答タイムアウト：00:00:20
- 未知のメッセージ ID をドロップしてログを出力

- IMSI Prefix Filtering：IMSI Prefix Filtering ダイアログボックスを開き、IMSI プレフィックス フィルタを設定します。
- Customize：Add/Edit GTP Policy Map ダイアログボックスを開き、追加の設定を行います。
- Default Level：セキュリティ レベルをデフォルトに戻します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

IMSI Prefix Filtering

IMSI Prefix タブでは、GTP 要求の中で使用できるように IMSI プレフィックスを定義できます。

フィールド

- Mobile Country Code：0 以外の 3 桁の値でモバイル カントリ コードを定義します。1 桁または 2 桁の値を指定すると、先頭に 0 が付加されて 3 桁になります。
- Mobile Network Code：2 桁または 3 桁の数字でネットワーク コードを定義します。
- Add：指定したカントリ コードとネットワーク コードを IMSI Prefix テーブルに追加します。
- Delete：指定したカントリ コードとネットワーク コードを IMSI Prefix テーブルから削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit GTP Policy Map（セキュリティ レベル）

Add/Edit GTP Policy Map ペインでは、GTP アプリケーション検査マップのセキュリティ レベルと追加の設定値を設定できます。

フィールド

- Name：GTP マップの追加時に GTP マップの名前を入力します。GTP マップの編集時には、事前に設定した GTP マップの名前が表示されます。
- Description：GTP マップの説明を 200 文字以内で入力します。

- Security Level：セキュリティ レベルは常に Low です。

  エラーを許可しない

  トンネルの最大数：500

  GSN タイムアウト：00:30:00

  PDP コンテキスト タイムアウト：00:30:00

  要求タイムアウト：00:01:00

  シグナリング タイムアウト：00:30:00

  トンネル タイムアウト：01:00:00

  T3 応答タイムアウト：00:00:20

  未知のメッセージ ID をドロップしてログを出力

  - IMSI Prefix Filtering：IMSI Prefix Filtering ダイアログボックスを開き、IMSI プレフィックス フィルタを設定します。
  - Default Level：セキュリティ レベルをデフォルトに戻します。
- Details：詳細な設定を行うための Parameters タブ、IMSI Prefix Filtering タブ、および Inspections タブを表示します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit GTP Policy Map（詳細）

Add/Edit GTP Policy Map ペインでは、GTP アプリケーション検査マップのセキュリティ レベルと追加の設定値を設定できます。

フィールド

- Name：GTP マップの追加時に GTP マップの名前を入力します。GTP マップの編集時には、事前に設定した GTP マップの名前が表示されます。
- Description：GTP マップの説明を 200 文字以内で入力します。
- Security Level：設定するセキュリティ レベルと IMSI プレフィックス フィルタリング設定を表示します。
- Permit Parameters：このタブで GTP 検査マップの許可パラメータを設定します。
  - Object Groups to Add

    From object group：オブジェクト グループを指定して、または Browse ボタンをクリックして、Add Network Object Group ダイアログボックスを開きます。

    To object group：オブジェクト グループを指定して、または Browse ボタンをクリックして、Add Network Object Group ダイアログボックスを開きます。
  - Add：指定したカントリ コードとネットワーク コードを IMSI Prefix テーブルに追加します。
  - Delete：指定したカントリ コードとネットワーク コードを IMSI Prefix テーブルから削除します。
  - Permit Errors：無効なパケットや検査時にエラーが見つかったパケットを、ドロップしないでセキュリティ アプライアンスから送信します。デフォルトでは、無効なパケットや解析中に失敗したパケットはドロップされます。

- General Parameters：このタブで GTP 検査マップの一般パラメータを設定します。
  - Maximum Number of Requests：許容される要求キュー サイズのデフォルト最大値を変更できます。要求キュー サイズのデフォルト最大値は 200 です。キューで応答待ちができる GTP 要求数の最大値を指定します。1 ～ 9999999 の範囲で指定できます。
  - Maximum Number of Tunnels：許容されるトンネル数のデフォルト最大値を変更できます。デフォルトのトンネル制限値は 500 です。許容するトンネル数の最大値を指定します。グローバルなトンネル全体の制限値を 1 ～ 9999999 の範囲で指定できます。
  - Timeouts

    GSN timeout : GSN を削除するまでの、非アクティブ期間のデフォルト最大値を変更できます。デフォルトは 30 分です。タイムアウト値を *hh*:*mm*:*ss* 形式で指定します。ここで *hh* は時間、*mm* は分、*ss* は秒です。値 0 は、切断しないことを意味します。

    PDP-Context timeout：GTP セッションで PDP コンテキストを受け取るまでの、非アクティブ期間のデフォルト最大値を変更できます。デフォルトは 30 分です。タイムアウト値を *hh*:*mm*:*ss* 形式で指定します。ここで *hh* は時間、*mm* は分、*ss* は秒です。値 0 は、切断しないことを意味します。

    Request Queue：GTP セッション中に GTP メッセージを受け取るまでの、非アクティブ期間のデフォルト最大値を変更できます。デフォルトは 1 分です。タイムアウト値を *hh*:*mm*:*ss* 形式で指定します。ここで *hh* は時間、*mm* は分、*ss* は秒です。値 0 は、切断しないことを意味します。

    Signaling：GTP シグナリングを削除するまでの、非アクティブ期間のデフォルト最大値を変更できます。デフォルトは 30 分です。タイムアウト値を *hh*:*mm*:*ss* 形式で指定します。ここで *hh* は時間、*mm* は分、*ss* は秒です。値 0 は、切断しないことを意味します。

    Tunnel：GTP トンネルの非アクティブ期間のデフォルト最大値を変更できます。デフォルトは 1 時間です。タイムアウト値を *hh*:*mm*:*ss* 形式で指定します。ここで *hh* は時間、*mm* は分、*ss* は秒です。値 0 は切断しないことを意味します。

    Request timeout：GTP 要求のアイドル タイムアウト値を指定します。

    T3-Response timeout：接続を削除するまでの、応答待ち時間の最大値を指定します。
- IMSI Prefix Filtering：このタブで GTP 検査マップの IMSI プレフィックス フィルタリングを設定します。
  - Mobile Country Code：0 以外の 3 桁の値でモバイル カントリ コードを定義します。1 桁または 2 桁の値を指定すると、先頭に 0 が付加されて 3 桁になります。
  - Mobile Network Code：2 桁または 3 桁の数字でネットワーク コードを定義します。
  - Add：指定したカントリ コードとネットワーク コードを IMSI Prefix テーブルに追加します。
  - Delete：指定したカントリ コードとネットワーク コードを IMSI Prefix テーブルから削除します。
- Inspections：このタブで GTP 検査マップを設定します。
  - Match Type：一致タイプを示します。肯定一致と否定一致があります。
  - Criterion：GTP 検査の基準を示します。
  - Value：GTP 検査で照合する値を示します。
  - Action：照合条件が一致したときのアクションを示します。
  - Log：ログの状態を示します。
  - Add：Add GTP Inspect ダイアログボックスが開き、GTP 検査を追加できます。
  - Edit：Edit GTP Inspect ダイアログボックスが開き、GTP 検査を編集できます。
  - Delete：GTP 検査を削除します。
  - Move Up：検査をリストの上に移動します。
  - Move Down：検査をリストの下に移動します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit GTP Map

Add/Edit GTP Inspect ダイアログボックスでは、GTP 検査マップの照合基準と値を定義できます。

フィールド

- Match Type：トラフィックと値を一致させるかどうかを指定します。

  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。
- Criterion：GTP トラフィックに適用する照合基準を指定します。
  - Access Point Name：アクセス ポイント名を照合します。
  - Message ID：メッセージ ID を照合します。
  - Message Length：メッセージの長さを照合します。
  - Version：バージョンを照合します。
- Access Point Name Criterion Values：照合するアクセス ポイント名を指定します。デフォルトでは、有効な APN のメッセージをすべて検査します。すべての APN が指定できます。
  - Regular Expression：照合する定義された正規表現を一覧表示します。
  - Manage : Manage Regular Expressions ダイアログボックスが開き、正規表現を設定できます。
  - Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。
  - Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップを設定できます。
  - Action：Drop。
  - Log：イネーブルまたはディセーブルにします。
- Message ID Criterion Values：照合するメッセージの数値識別子を指定します。有効な指定範囲は 1 ～ 255 です。デフォルトでは、すべての有効なメッセージ ID が対象です。
  - Value：値を完全一致で照合するか、範囲で照合するかを指定します。

    Equals：値を入力します。

    Range：値の範囲を入力します。
  - Action：Drop packet または limit rate (pps)。
  - Log：イネーブルまたはディセーブルにします。
- Message Length Criterion Values：許可される UDP ペイロードの、メッセージの長さのデフォルト最大値を変更できます。
  - Minimum value : UDP ペイロードの最小バイト数を指定します。1 ～ 65536 の範囲の値を指定できます。
  - Maximum value：UDP ペイロードの最大バイト数を指定します。1 ～ 65536 の範囲の値を指定できます。
  - Action：Drop packet。
  - Log：イネーブルまたはディセーブルにします。

- Version Criterion Values : 照合するメッセージの GTP バージョンを指定します。有効な指定範囲は 0 ～ 255 です。0 は Version 0、1 は Version 1 を示します。GTP の Version 0 はポート 3386 を使用し、Version 1 はポート 2123 を使用します。デフォルトでは、すべての GTP バージョンが対象です。
  - Value：値を完全一致で照合するか、範囲で照合するかを指定します。

    Equals：値を入力します。

    Range：値の範囲を入力します。
  - Action：Drop packet。
  - Log：イネーブルまたはディセーブルにします。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

H.323 Inspect Map

H.323 ペインでは、H.323 アプリケーションの事前に設定された検査マップを表示できます。H.323 マップでは、H.323 アプリケーション検査のデフォルト設定値を変更できます。

H.323 検査は RAS、H.225、H.245 をサポートし、埋め込まれた IP アドレスとポートをすべて変換する機能を備えています。ステートのトラッキングとフィルタリングを実行し、検査機能のアクティベーションをカスケードできます。H.323 検査は、電話番号のフィルタリング、T.120 のダイナミック制御、H.245 のトンネル機能制御、HSI グループ、プロトコルのステート トラッキング、H.323 通話時間制限の適用、音声 / ビデオ制御をサポートします。

フィールド

- H.323 Inspect Maps：定義されている H.323 検査マップを一覧表示するテーブルです。
- Add：新しい H.323 検査マップを設定します。H.323 検査マップを編集するには、H.323 Inspect Maps テーブルで H.323 のエントリを選択し、Customize をクリックします。
- Delete：H.323 Inspect Maps テーブルで選択した検査マップを削除します。
- Security Level：セキュリティ レベル（High、Medium、Low）を選択します。
  - Low：デフォルト

    H.225 状態確認：ディセーブル

    RAS 状態確認：ディセーブル

    発信側の番号：ディセーブル

    通話制限時間：ディセーブル

    RTP 準拠：適用強制しない
  - Medium

    H.225 状態確認：イネーブル

    RAS 状態確認：イネーブル

    発信側の番号：ディセーブル

    通話制限時間：ディセーブル

    RTP 準拠：適用強制する

ペイロードを音声またはビデオに限定してシグナリング交換を適用：しない

- High

  H.225 状態確認：イネーブル

  RAS 状態確認：イネーブル

  発信側の番号：イネーブル

  通話制限時間：1:00:00

  RTP 準拠：適用強制する

  ペイロードを音声またはビデオに限定してシグナリング交換を適用：する

- Phone Number Filtering：Phone Number Filtering ダイアログボックスが開き、電話番号フィルタを設定できます。
- Customize：Add/Edit H.323 Policy Map ダイアログボックスを開き、追加の設定を行います。
- Default Level：セキュリティ レベルをデフォルトの Medium レベルに戻します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Phone Number Filtering

Phone Number Filtering ダイアログボックスでは、電話番号のフィルタを設定できます。

フィールド

- Match Type：一致タイプを示します。肯定一致と否定一致があります。
- Criterion：検査の基準を示します。
- Value：検査で照合する値を示します。
- Action：照合条件が一致したときのアクションを示します。
- Log：ログの状態を示します。
- Add：Add Phone Number Filter ダイアログボックスが開き、電話番号のフィルタを追加できます。
- Edit：Edit Phone Number Filter ダイアログボックスが開き、電話番号を編集できます。
- Delete：電話番号のフィルタを削除します。
- Move Up：エントリをリストの上に移動します。
- Move Down：エントリをリストの下に移動します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit H.323 Policy Map（セキュリティ レベル）

Add/Edit H.323 Policy Map ペインでは、H.323 アプリケーション検査マップのセキュリティ レベルと追加の設定値を設定できます。

フィールド

- Name：H.323 マップの追加時に H.323 マップの名前を入力します。H.323 マップの編集時には、事前に設定した H.323 マップの名前が表示されます。
- Description：H.323 マップの説明を 200 文字以内で入力します。
- Security Level：セキュリティ レベル（High、Medium、Low）を選択します。
  - Low：デフォルト

    H.225 状態確認：ディセーブル

    RAS 状態確認：ディセーブル

    発信側の番号：ディセーブル

    通話制限時間：ディセーブル

    RTP 準拠：適用強制しない
  - Medium

    H.225 状態確認：イネーブル

    RAS 状態確認：イネーブル

    発信側の番号：ディセーブル

    通話制限時間：ディセーブル

    RTP 準拠：適用強制する

    ペイロードを音声またはビデオに限定してシグナリング交換を適用：しない
  - High

    H.225 状態確認：イネーブル

    RAS 状態確認：イネーブル

    発信側の番号：イネーブル

    通話制限時間：1:00:00

    RTP 準拠：適用強制する

    ペイロードを音声またはビデオに限定してシグナリング交換を適用：する
  - Phone Number Filtering : Phone Number Filtering ダイアログボックスが開き、電話番号のフィルタを設定できます。
  - Default Level：セキュリティ レベルをデフォルトに戻します。
- Details : 詳細な設定を行うための State Checking タブ、Call Attributes タブ、Tunneling and Protocol Conformance タブ、HSI Group Parameters タブ、および Inspections タブを表示します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit H.323 Policy Map（詳細）

Add/Edit H.323 Policy Map ペインでは、H.323 アプリケーション検査マップのセキュリティ レベルと追加の設定値を設定できます。

フィールド

- Name：H.323 マップの追加時に H.323 マップの名前を入力します。H.323 マップの編集時には、事前に設定した H.323 マップの名前が表示されます。
- Description：H.323 マップの説明を 200 文字以内で入力します。
- Security Level：設定するセキュリティ レベルと電話番号フィルタリング設定を表示します。
- State Checking：このタブで H.323 検査マップの状態確認パラメータを設定します。
  - Check state transition of H.225 messages：H.323 の状態確認を H.225 メッセージに適用します。
  - Check state transition of RAS messages：H.323 の状態確認を RAS メッセージに適用します。
- Call Attributes：このタブで H.323 検査マップのコール アトリビュート パラメータを設定します。
  - Enforce call duration limit：通話を一定の時間で制限します。

    Call Duration Limit：通話制限時間（hh:mm:ss）。
  - Enforce presence of calling and called party numbers：通話設定時に、強制的に発信側の番号を送信します。
- Tunneling and Protocol Conformance：このタブで H.323 検査マップのトンネリングとプロトコル準拠パラメータを設定します。
  - Check for H.245 tunneling：H.245 のトンネリングを許可します。

    Action：接続をドロップまたはログに出力します。
  - Check RTP packets for protocol conformance：ピンホールの RTP/RTCP パケットがプロトコルに準拠しているかどうかをチェックします。

    Limit payload to audio or video, based on the signaling exchange：ペイロード タイプを強制的に音声やビデオにして、シグナリング交換を適用します。
- HSI Group Parameters：このタブで HSI グループを設定します。
  - HSI Group ID：HSI グループの ID を示します。
  - IP Address：HSI グループの IP アドレスを示します。
  - Endpoints：HSI グループのエンドポイントを示します。
  - Add：Add HSI Group ダイアログボックスが開き、HSI グループを追加できます。
  - Edit：Edit HSI Group ダイアログボックスが開き、HSI グループを編集できます。
  - Delete：HSI グループを削除します。
- Inspections：このタブで H.323 検査のコンフィギュレーションを表示して、追加や編集ができます。
  - Match Type：一致タイプを示します。肯定一致と否定一致があります。
  - Criterion：H.323 検査の基準を示します。
  - Value：H.323 検査で照合する値を示します。
  - Action：照合条件が一致したときのアクションを示します。
  - Log：ログの状態を示します。
  - Add：Add H.323 Inspect ダイアログボックスが開き、H.323 検査を追加できます。
  - Edit：Edit H.323 Inspect ダイアログボックスが開き、H.323 検査を編集できます。
  - Delete：H.323 検査を削除します。
  - Move Up：検査をリストの上に移動します。
  - Move Down：検査をリストの下に移動します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit HSI Group

Add/Edit HSI Group ダイアログボックスでは、HSI グループを設定できます。

フィールド

- Group ID：HSI のグループ ID を入力します。
- IP Address：HSI の IP アドレスを入力します。
- Endpoints：エンドポイントの IP アドレスとインターフェイスを設定します。
  - IP Address：エンドポイントの IP アドレスを入力します。
  - Interface：エンドポイントのインターフェイスを指定します。
- Add：定義された HSI グループを追加します。
- Delete：選択した HSI グループを削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit H.323 Map

Add/Edit H.323 Inspect ダイアログボックスでは、H.323 検査マップの照合基準と値を定義できます。

フィールド

- Single Match：H.323 検査に照合文が 1 つだけの場合に指定します。
- Match Type：トラフィックと値を一致させるかどうかを指定します。

  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。
- Criterion：H.323 トラフィックに適用する照合基準を指定します。
  - Called Party：受信側を照合します。
  - Calling Party：発信元を照合します。
  - Media Type：メディア タイプを照合します。
- Called Party Criterion Values：H.323 受信側の照合方法を指定します。
  - Regular Expression：照合する定義された正規表現を一覧表示します。
  - Manage : Manage Regular Expressions ダイアログボックスが開き、正規表現を設定できます。

  - Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。
  - Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップを設定できます。
- Calling Party Criterion Values：H.323 発信元の照合方法を指定します。
  - Regular Expression：照合する定義された正規表現を一覧表示します。
  - Manage : Manage Regular Expressions ダイアログボックスが開き、正規表現を設定できます。
  - Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。
  - Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップを設定できます。
- Media Type Criterion Values：照合するメディア タイプを指定します。
  - Audio：音声タイプを照合します。
  - Video：ビデオ タイプを照合します。
  - Data：データ タイプを照合します。
- Multiple Matches：H.323 検査の複数の照合文を指定します。
  - H323 Traffic Class：H.323 トラフィック クラスを照合します。
  - Manage : Manage H.323 Class Maps ダイアログボックスが開き、H.323 クラスマップの追加、編集、削除ができます。
- Action：Drop Packet、Drop Connection、Reset。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

HTTP Inspect Map

HTTP ペインでは、HTTP アプリケーションの事前に設定された検査マップを表示できます。HTTP マップでは、HTTP アプリケーション検査のデフォルト設定値を変更できます。

HTTP アプリケーション検査で 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。

HTTP アプリケーション検査でトンネル 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。

フィールド

- HTTP Inspect Maps：定義されている HTTP 検査マップを一覧表示するテーブルです。
- Add：新しい HTTP 検査マップを設定します。HTTP 検査マップを編集するには、HTTP Inspect Maps テーブルで HTTP のエントリを選択し、Customize をクリックします。
- Delete：HTTP Inspect Maps テーブルで選択した検査マップを削除します。
- Security Level：セキュリティ レベル（High、Medium、Low）を選択します。
  - Low：デフォルト

プロトコル違反時のアクション：Drop Connection
安全でない方式の接続ドロップ：ディセーブル
要求のヘッダーに ASCII 以外の文字が含まれる場合の接続ドロップ：ディセーブル
URI フィルタリング：設定しない
高度な検査：設定しない

- Medium

  プロトコル違反時のアクション：Drop Connection
  安全でない方式の接続ドロップ：GET、HEAD、POST だけを許可
  要求のヘッダーに ASCII 以外の文字が含まれる場合の接続ドロップ：ディセーブル
  URI フィルタリング：設定しない
  高度な検査：設定しない

- High

  プロトコル違反時のアクション：Drop Connection と Log
  安全でない方式の接続ドロップ：GET、HEAD だけを許可
  要求のヘッダーに ASCII 以外の文字が含まれる場合の接続ドロップ：イネーブル
  URI フィルタリング：設定しない
  高度な検査：設定しない

- URI Filtering：URI Filtering ダイアログボックスが開き、URI フィルタを設定できます。
- Customize：Edit HTTP Policy Map ダイアログボックスを開き、追加の設定を行います。
- Default Level：セキュリティ レベルをデフォルトの Medium レベルに戻します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

URI Filtering

URI Filtering ダイアログボックスでは、URI フィルタを設定できます。

フィールド

- Match Type：一致タイプを示します。肯定一致と否定一致があります。
- Criterion：検査の基準を示します。
- Value：検査で照合する値を示します。
- Action：照合条件が一致したときのアクションを示します。
- Log：ログの状態を示します。
- Add：Add URI Filtering ダイアログボックスが開き、URI フィルタを追加できます。
- Edit：Edit URI Filtering ダイアログボックスが開き、URI フィルタを編集できます。
- Delete：URI フィルタを削除します。
- Move Up：エントリをリストの上に移動します。
- Move Down：エントリをリストの下に移動します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit HTTP Policy Map（セキュリティ レベル）

Add/Edit HTTP Policy Map ペインでは、HTTP アプリケーション検査マップのセキュリティ レベルと追加の設定値を設定できます。

フィールド

- Name : HTTP マップの追加時に HTTP マップの名前を入力します。HTTP マップの編集時には、事前に設定した HTTP マップの名前が表示されます。
- Description：HTTP マップの説明を 200 文字以内で入力します。
- Security Level：セキュリティ レベル（High、Medium、Low）を選択します。
  - Low：デフォルト

    プロトコル違反時のアクション：Drop Connection

    安全でない方式の接続ドロップ：ディセーブル

    要求のヘッダーに ASCII 以外の文字が含まれる場合の接続ドロップ：ディセーブル

    URI フィルタリング：設定しない

    高度な検査：設定しない
  - Medium

    プロトコル違反時のアクション：Drop Connection

    安全でない方式の接続ドロップ：GET、HEAD、POST だけを許可

    要求のヘッダーに ASCII 以外の文字が含まれる場合の接続ドロップ：ディセーブル

    URI フィルタリング：設定しない

    高度な検査：設定しない
  - High

    プロトコル違反時のアクション：Drop Connection と Log

    安全でない方式の接続ドロップ：GET、HEAD だけを許可

    要求のヘッダーに ASCII 以外の文字が含まれる場合の接続ドロップ：イネーブル

    URI フィルタリング：設定しない

    高度な検査：設定しない
  - URI Filtering：URI Filtering ダイアログボックスが開き、URI フィルタを設定します。
  - Default Level：セキュリティ レベルをデフォルトに戻します。
- Details：詳細な設定を行うための Parameters タブと Inspections タブを表示します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit HTTP Policy Map（詳細）

Add/Edit HTTP Policy Map ペインでは、HTTP アプリケーション検査マップのセキュリティ レベルと追加の設定値を設定できます。

フィールド

- Name : HTTP マップの追加時に HTTP マップの名前を入力します。HTTP マップの編集時には、事前に設定した HTTP マップの名前が表示されます。
- Description：HTTP マップの説明を 200 文字以内で入力します。
- Security Level：設定するセキュリティ レベルと URI フィルタリング設定を表示します。
- Parameters：このタブで HTTP 検査マップのパラメータを設定します。
  - Check for protocol violations：HTTP プロトコル違反の有無をチェックします。

    Action：Drop Connection、Reset、Log。

    Log：イネーブルまたはディセーブルにします。
  - Spoof server string：サーバの HTTP ヘッダーの値を指定の文字列で置き換えます。

    Spoof String：サーバのヘッダー フィールドと置き換える文字列を入力します。最大 82 文字まで入力できます。
  - 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。
- Inspections：このタブで HTTP 検査のコンフィギュレーションを表示して、追加や編集ができます。
  - Match Type：一致タイプを示します。肯定一致と否定一致があります。
  - Criterion：HTTP 検査の基準を示します。
  - Value：HTTP 検査で照合する値を示します。
  - Action：照合条件が一致したときのアクションを示します。
  - Log：ログの状態を示します。
  - Add：Add HTTP Inspect ダイアログボックスが開き、HTTP 検査を追加できます。
  - Edit：Edit HTTP Inspect ダイアログボックスが開き、HTTP 検査を編集できます。
  - Delete：HTTP 検査を削除します。
  - Move Up：検査をリストの上に移動します。
  - Move Down：検査をリストの下に移動します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit HTTP Map

Add/Edit HTTP Inspect ダイアログボックスでは、HTTP 検査マップの照合基準と値を定義できます。

フィールド

- Single Match：HTTP 検査に照合文が 1 つだけの場合に指定します。
- Match Type：トラフィックと値を一致させるかどうかを指定します。

  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。
- Criterion：HTTP トラフィックに適用する照合基準を指定します。
  - Request/Response Content Type Mismatch : 応答のコンテンツ タイプを、要求の accept フィールドの MIME タイプの 1 つに一致させるかどうかを指定します。
  - Request Arguments：要求の引数を正規表現で照合します。

    Regular Expression：照合する定義された正規表現を一覧表示します。

    Manage : Manage Regular Expressions ダイアログボックスが開き、正規表現を設定できます。

    Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。

    Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップを設定できます。
  - Request Body Length：要求の本文に指定したバイト数より長いフィールドがある場合、正規表現で照合します。

    Greater Than Length : 要求フィールドの長さと照合するフィールドの値をバイト単位で入力します。
  - Request Body：要求の本文を正規表現で照合します。

    Regular Expression：照合する定義された正規表現を一覧表示します。

    Manage : Manage Regular Expressions ダイアログボックスが開き、正規表現を設定できます。

    Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。

    Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップを設定できます。
  - Request Header Field Count : 要求ヘッダーのフィールド数が最大値の場合、正規表現で照合します。

    Predefined：要求のヘッダー フィールドを次の中から指定します。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。

    Regular Expression：照合する定義された正規表現を一覧表示します。

    Manage : Manage Regular Expressions ダイアログボックスが開き、正規表現を設定できます。

    Greater Than Count：ヘッダー フィールド数の最大値を入力します。

- Request Header Field Length：要求ヘッダーに指定したバイト数より長いフィールドがある場合、正規表現で照合します。

  Predefined：要求のヘッダー フィールドを次の中から指定します。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。

  Regular Expression：照合する定義された正規表現を一覧表示します。

  Manage : Manage Regular Expressions ダイアログボックスが開き、正規表現を設定できます。

  Greater Than Length : 要求フィールドの長さと照合するフィールドの値をバイト単位で入力します。

- Request Header Field：要求ヘッダーを正規表現で照合します。

  Predefined：要求のヘッダー フィールドを次の中から指定します。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。

  Regular Expression：照合する定義された正規表現を一覧表示します。

  Manage : Manage Regular Expressions ダイアログボックスが開き、正規表現を設定できます。

  Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。

  Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップを設定できます。

- Request Header Count：要求ヘッダー数が最大値の場合、正規表現で照合します。

  Greater Than Count：ヘッダー数の最大値を入力します。

- Request Header Length : 要求ヘッダーが指定したバイト数より長い場合、正規表現で照合します。

  Greater Than Length：ヘッダーの長さをバイト単位で入力します。

- Request Header non-ASCII：要求ヘッダーに含まれる ASCII 以外の文字を照合します。

- Request Method：要求の方式を正規表現で照合します。

  Method：照合する要求方式を次の中から指定します。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。

  Regular Expression：正規表現の照合方法を指定します。

  Regular Expression：照合する定義された正規表現を一覧表示します。

  Manage : Manage Regular Expressions ダイアログボックスが開き、正規表現を設定できます。

  Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。

  Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップを設定できます。

- Request URI Length : 要求の URI が指定したバイト数より長い場合、正規表現で照合します。

  Greater Than Length：URI の長さをバイト単位で入力します。

- Request URI：要求の URI を正規表現で照合します。

  Regular Expression：照合する定義された正規表現を一覧表示します。

  Manage : Manage Regular Expressions ダイアログボックスが開き、正規表現を設定できます。

  Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。

  Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップを設定できます。

- Response Body：要求の本文を regex で照合します。

  ActiveX：ActiveX の照合方法を指定します。

  Java Applet：Java アプレットの照合方法を指定します。

  Regular Expression：正規表現の照合方法を指定します。

  Regular Expression：照合する定義された正規表現を一覧表示します。

  Manage : Manage Regular Expressions ダイアログボックスが開き、正規表現を設定できます。

  Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。

  Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップを設定できます。

- Response Body Length : 応答の本文に指定したバイト数より長いフィールドがある場合、正規表現で照合します。

  Greater Than Length : 応答フィールドの長さと照合するフィールドの値をバイト単位で入力します。

- Response Header Field Count：応答ヘッダーのフィールド数が最大値の場合、正規表現で照合します。

  Predefined : 応答のヘッダー フィールドを次の中から指定します。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。

  Regular Expression：照合する定義された正規表現を一覧表示します。

  Manage : Manage Regular Expressions ダイアログボックスが開き、正規表現を設定できます。

  Greater Than Count：ヘッダー フィールド数の最大値を入力します。

- Response Header Field Length : 応答ヘッダーに指定したバイト数より長いフィールドがある場合、正規表現で照合します。

  Predefined : 応答のヘッダー フィールドを次の中から指定します。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。

  Regular Expression：照合する定義された正規表現を一覧表示します。

  Manage : Manage Regular Expressions ダイアログボックスが開き、正規表現を設定できます。

  Greater Than Length : 応答フィールドの長さと照合するフィールドの値をバイト単位で入力します。

- Response Header Field：応答ヘッダーを正規表現で照合します。

  Predefined : 応答のヘッダー フィールドを次の中から指定します。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。

  Regular Expression：照合する定義された正規表現を一覧表示します。

  Manage : Manage Regular Expressions ダイアログボックスが開き、正規表現を設定できます。

  Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。

  Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップを設定できます。

- Response Header Count：応答ヘッダー数が最大値の場合、正規表現で照合します。

  Greater Than Count：ヘッダー数の最大値を入力します。

- Response Header Length：応答ヘッダーが指定したバイト数より長い場合、正規表現で照合します。

  Greater Than Length：ヘッダーの長さをバイト単位で入力します。

- Response Header non-ASCII：応答ヘッダーに含まれる ASCII 以外の文字を照合します。
- Response Status Line：ステータス行を正規表現で照合します。

  Regular Expression：照合する定義された正規表現を一覧表示します。

  Manage : Manage Regular Expressions ダイアログボックスが開き、正規表現を設定できます。

  Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。

  Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップを設定できます。

- Multiple Matches：HTTP 検査の複数の照合文を指定します。
  - H323 Traffic Class：HTTP トラフィック クラスを照合します。
  - Manage : Manage HTTP Class Maps ダイアログボックスが開き、HTTP クラスマップの追加、編集、削除ができます。
- Action：Drop Connection、Reset、Log。
- Log：イネーブルまたはディセーブルにします。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Instant Messaging (IM) Inspect Map

IM ペインでは、インスタント メッセージ（IM）アプリケーションの事前に設定された検査マップを表示できます。インスタント メッセージ（IM）マップでは、インスタント メッセージ（IM）アプリケーション検査のデフォルト設定値を変更できます。

インスタント メッセージ（IM）アプリケーション検査で、ネットワーク アクセスの使用量を詳細に制御できます。また、機密情報の漏洩やその他の攻撃からネットワークを守ります。正規表現データベースのさまざまな検索パターンを使って、インスタント メッセージ（IM）をフィルタできます。フローが認識されない場合は、syslog が生成されます。

スコープを限定するには、アクセスリストから検査するトラフィック ストリームを指定します。UDP メッセージの場合、対応する UDP ポート番号も設定できます。Yahoo! Messenger および MSN Messenger のインスタント メッセージの検査もサポートされています。

フィールド

- Name：検査マップの名前を 40 文字以内で入力します。
- Description：検査マップの説明を 200 文字以内で入力します。
- IM Inspect Maps：定義されている IM 検査マップを一覧表示するテーブルです。
- Add：新しい IM 検査マップを設定します。
- Edit：IM Inspect Maps テーブルで選択した IM のエントリを編集します。
- Delete：IM Inspect Maps テーブルで選択した検査マップを削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit Instant Messaging (IM) Policy Map

Add/Edit Instant Messaging (IM) Policy Map ペインでは、IM アプリケーション検査マップのセキュリティ レベルと追加の設定値を設定できます。

フィールド

- Name：IM マップの追加時に IM マップの名前を入力します。IM マップの編集時には、事前に設定した IM マップの名前が表示されます。
- Description：IM マップの説明を 200 文字以内で入力します。
- Match Type：一致タイプを示します。肯定一致と否定一致があります。
- Criterion：IM 検査の基準を示します。
- Value：IM 検査で照合する値を示します。
- Action：照合条件が一致したときのアクションを示します。
- Log：ログの状態を示します。
- Add：Add IM Inspect ダイアログボックスが開き、IM 検査を追加できます。
- Edit：Edit IM Inspect ダイアログボックスが開き、IM 検査を編集できます。
- Delete：IM 検査を削除します。
- Move Up：検査をリストの上に移動します。
- Move Down：検査をリストの下に移動します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit IM Map

Add/Edit IM Inspect ダイアログボックスでは、IM 検査マップの照合基準と値を定義できます。

フィールド

- Single Match：IM 検査に照合文が 1 つだけの場合に指定します。
- Match Type：トラフィックと値を一致させるかどうかを指定します。

  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。

- Criterion：IM トラフィックに適用する照合基準を指定します。
  - Protocol：IM プロトコルを照合します。
  - Service：IM サービスを照合します。
  - Source IP Address：送信元 IP アドレスを照合します。
  - Destination IP Address：宛先 IP アドレスを照合します。
  - Version：IM ファイル転送のサービス バージョンを照合します。
  - Client Login Name：IM サービスのクライアント ログイン名を照合します。
  - Client Peer Login Name：IM サービスのクライアントのピア ログイン名を照合します。
  - Filename：IM ファイル転送サービスのファイル名を照合します。
- Protocol Criterion Values：照合する IM プロトコルを指定します。
  - Yahoo! Messenger：Yahoo! Messenger のインスタント メッセージを照合します。
  - MSN Messenger：MSN Messenger のインスタント メッセージを照合します。
- Service Criterion Values：照合する IM サービスを指定します。
  - Chat：IM メッセージ チャット サービスを照合します。
  - Conference：IM コンファレンス サービスを照合します。
  - File Transfer：IM ファイル転送サービスを照合します。
  - Games：IM ゲーム サービスを照合します。
  - Voice Chat：IM 音声チャット サービスを照合します（Yahoo の IM は対象外です）。
  - Web Cam：IM Web カメラ サービスを照合します。
- Source IP Address Criterion Values：IM サービスで照合する送信元 IP アドレスを指定します。
  - IP Address：IM サービスの送信元 IP アドレスを入力します。
  - IP Mask：送信元 IP アドレスのマスクです。
- Destination IP Address Criterion Values：IM サービスで照合する宛先 IP アドレスを指定します。
  - IP Address：IM サービスの宛先 IP アドレスを入力します。
  - IP Mask：宛先 IP アドレスのマスクです。
- Version Criterion Values：IM ファイル転送サービスで照合するバージョンを指定します。正規表現で照合します。
  - Regular Expression：照合する定義された正規表現を一覧表示します。
  - Manage：Manage Regular Expressions ダイアログボックスが開き、正規表現を設定できます。
  - Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。
  - Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップを設定できます。
- Client Login Name Criterion Values：IM サービスで照合するクライアント ログイン名を指定します。正規表現で照合します。
  - Regular Expression：照合する定義された正規表現を一覧表示します。
  - Manage：Manage Regular Expressions ダイアログボックスが開き、正規表現を設定できます。
  - Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。
  - Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップを設定できます。
- Client Peer Login Name Criterion Values：IM サービスで照合するクライアントのピア ログイン名を指定します。正規表現で照合します。
  - Regular Expression：照合する定義された正規表現を一覧表示します。
  - Manage：Manage Regular Expressions ダイアログボックスが開き、正規表現を設定できます。
  - Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。

  - Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップを設定できます。
- Filename Criterion Values：IM ファイル転送サービスで照合するファイル名を指定します。正規表現で照合します。
  - Regular Expression：照合する定義された正規表現を一覧表示します。
  - Manage : Manage Regular Expressions ダイアログボックスが開き、正規表現を設定できます。
  - Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。
  - Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップを設定できます。
- Multiple Matches：IM 検査の複数の照合文を指定します。
  - IM Traffic Class：IM トラフィック クラスを照合します。
  - Manage：Manage IM Class Maps ダイアログボックスが開き、IM クラスマップの追加、編集、削除ができます。
- Action：Drop Connection、Reset、Log。
- Log：イネーブルまたはディセーブルにします。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

IPSec Pass Through Inspect Map

IPSec Pass Through ペインでは、IPSec パススルー アプリケーションの事前に設定された検査マップを表示できます。IPSec パススルー マップでは、IPSec パススルー アプリケーション検査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、アクセスリストを参照しなくても、特定のフローを許可できます。

フィールド

- IPSec Pass Through Inspect Maps：定義されている IPSec パススルー検査マップを一覧表示するテーブルです。
- Add：新しい IPSec パススルー検査マップを設定します。IPSec パススルー検査マップを編集するには、IPSec Pass Through Inspect Maps テーブルで IPSec パススルーのエントリを選択し、Customize をクリックします。
- Delete：IPSec Pass Through Inspect Maps テーブルで選択した検査マップを削除します。
- Security Level：セキュリティ レベル（High または Low）を選択します。
  - Low：デフォルト

    クライアントごとの最大 ESP フロー：制限なし

    ESP アイドル タイムアウト：00:10:00

    クライアントごとの最大 AH フロー：制限なし

    AH アイドル タイムアウト：00:10:00
  - High

    クライアントごとの最大 ESP フロー：10

    ESP アイドル タイムアウト：00:00:30

クライアントごとの最大 AH フロー：10

AH アイドル タイムアウト：00:00:30

- Customize：Add/Edit IPSec Pass Thru Policy Map ダイアログボックスを開き、追加の設定を行います。
- Default Level：セキュリティ レベルをデフォルトの Low レベルに戻します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit IPSec Pass Thru Policy Map（セキュリティ レベル）

Add/Edit IPSec Pass Thru Policy Map ペインでは、IPSec パススルー アプリケーション検査マップのセキュリティ レベルと追加の設定値を設定できます。

フィールド

- Name：IPSec パススルー マップの追加時に IPSec パススルー マップの名前を入力します。IPSec パススルー マップの編集時には、事前に設定した IPSec パススルー マップの名前が表示されます。
- Security Level：セキュリティ レベル（High または Low）を選択します。
  - Low：デフォルト

    クライアントごとの最大 ESP フロー：制限なし

    ESP アイドル タイムアウト：00:10:00

    クライアントごとの最大 AH フロー：制限なし

    AH アイドル タイムアウト：00:10:00
  - High

    クライアントごとの最大 ESP フロー：10

    ESP アイドル タイムアウト：00:00:30

    クライアントごとの最大 AH フロー：10

    AH アイドル タイムアウト：00:00:30
  - Default Level：セキュリティ レベルをデフォルトの Low レベルに戻します。
- Details：追加の設定を行うパラメータを表示します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit IPSec Pass Thru Policy Map（詳細）

Add/Edit IPSec Pass Thru Policy Map ペインでは、IPSec パススルー アプリケーション検査マップのセキュリティ レベルと追加の設定値を設定できます。

フィールド

- Name：IPSec パススルー マップの追加時に IPSec パススルー マップの名前を入力します。IPSec パススルー マップの編集時には、事前に設定した IPSec パススルー マップの名前が表示されます。
- Description：IPSec パススルー検査マップの説明を 200 文字以内で入力します。
- Security Level：設定するセキュリティ レベルを表示します。
- Parameters：ESP および AH パラメータを設定します。
  - Limit ESP flows per client：クライアントごとの ESP フローを制限します。
    Maximum：最大限度を指定します。
  - Apply ESP idle timeout：ESP アイドル タイムアウトを適用します。
    Timeout：タイムアウト値を指定します。
  - Limit AH flows per client：クライアントごとの AH フローを制限します。
    Maximum：最大限度を指定します。
  - Apply AH idle timeout：AH アイドル タイムアウトを適用します。
    Timeout：タイムアウト値を指定します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

MGCP Inspect Map

MGCP ペインでは、MGCP アプリケーションの事前に設定された検査マップを表示できます。MGCP マップでは、MGCP アプリケーション検査のデフォルト設定値を変更できます。MGCP マップを使用して、VoIP デバイスと MGCP コール エージェント間の接続を管理できます。

フィールド

- MGCP Inspect Maps：定義されている MGCP 検査マップを一覧表示するテーブルです。
- Add：新しい MGCP 検査マップを設定します。
- Edit：MGCP Inspect Maps テーブルで選択した MGCP のエントリを編集します。
- Delete：MGCP Inspect Maps テーブルで選択した検査マップを削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Gateways and Call Agents

Gateways and Call Agents ダイアログボックスでは、ゲートウェイとコール エージェントのグループをマップに設定できます。

フィールド

- Group ID：コール エージェント グループの ID を識別します。コール エージェント グループで、1 つ以上のコール エージェントを 1 つ以上の MGCP メディア ゲートウェイと関連付けます。ゲートウェイの IP アドレスは、1 つのグループ ID だけに関連付けできます。同じゲートウェイを別のグループ ID で使用できません。1 ～ 2147483647 の範囲の値を指定できます。
- Criterion：検査の基準を示します。
- Gateways：関連付けられたコール エージェントによって制御されるメディア ゲートウェイの IP アドレスを識別します。メディア ゲートウェイは一般に、電話回線を通じた音声信号と、インターネットまたは他のパケット ネットワークを通じたデータ パケットとの間の変換を行うネットワーク要素です。通常、ゲートウェイはコマンドを、コール エージェントのデフォルト MGCP ポート（2727）に送信します。
- Call Agents：コール エージェント グループの MGCP メディア ゲートウェイを制御するコール エージェントの IP アドレスを識別します。通常、コール エージェントはコマンドを、ゲートウェイのデフォルト MGCP ポート（2427）に送信します。
- Add：Add MGCP ダイアログボックスが表示され、新規のアプリケーション検査マップを定義できます。
- Edit：Edit MGCP ダイアログボックスが表示され、アプリケーション検査マップ テーブルで選択した検査マップを修正できます。
- Delete：アプリケーション検査マップ テーブルで選択した検査マップを削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit MGCP Policy Map

Add/Edit MGCP Policy Map ペインでは、MGCP アプリケーション検査マップのコマンド キュー、ゲートウェイ、およびコール エージェントの設定値を設定できます。

フィールド

- Name：MGCP マップの追加時に MGCP マップの名前を入力します。MGCP マップの編集時には、事前に設定した MGCP マップの名前が表示されます。
- Description：MGCP マップの説明を 200 文字以内で入力します。
- Command Queue：このタブで MGCP コマンドの許容キュー サイズを指定します。
  - Command Queue Size：キューに入れるコマンドの最大数を指定します。1 ～ 2147483647 の範囲の値を指定できます。
- Gateways and Call Agents : このタブでゲートウェイとコール エージェント グループをマップに設定します。
  - Group ID : コール エージェント グループの ID を識別します。コール エージェント グループで、1 つ以上のコール エージェントを 1 つ以上の MGCP メディア ゲートウェイと関連付けます。ゲートウェイの IP アドレスは、1 つのグループ ID だけに関連付けできます。同じゲートウェイを別のグループ ID で使用できません。1 ～ 2147483647 の範囲の値を指定できます。
  - Criterion：検査の基準を示します。
  - Gateways : 関連付けられたコール エージェントによって制御されるメディア ゲートウェイの IP アドレスを識別します。メディア ゲートウェイは一般に、電話回線を通じた音声信号と、インターネットまたは他のパケット ネットワークを通じたデータ パケットとの間の変換を行うネットワーク要素です。通常、ゲートウェイはコマンドを、コール エージェントのデフォルト MGCP ポート（2727）に送信します。
  - Call Agents : コール エージェント グループの MGCP メディア ゲートウェイを制御するコール エージェントの IP アドレスを識別します。通常、コール エージェントはコマンドを、ゲートウェイのデフォルト MGCP ポート（2427）に送信します。
  - Add：Add MGCP Group ダイアログボックスが表示され、ゲートウェイとコール エージェントの新規の MGCP グループを定義できます。
  - Edit : Edit MGCP ダイアログボックスが表示され、Gateways and Call Agents テーブルで選択した MGCP グループを修正できます。
  - Delete：Gateways and Call Agents テーブルで選択した MGCP グループを削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit MGCP Group

Add/Edit MGCP Group ダイアログボックスでは、MGCP アプリケーション検査がイネーブルのときに使用される MGCP グループのコンフィギュレーションを定義できます。

フィールド

- Group ID：コール エージェント グループの ID を指定します。コール エージェント グループで、1 つ以上のコール エージェントを 1 つ以上の MGCP メディア ゲートウェイと関連付けます。0 ～ 2147483647 の範囲の値を指定できます。
- Gateways エリア
  - Gateway to Be Added：関連付けられたコール エージェントによって制御されるメディア ゲートウェイの IP アドレスを指定します。メディア ゲートウェイは一般に、電話回線を通じた音声信号と、インターネットまたは他のパケット ネットワークを通じたデータ パケットとの間の変換を行うネットワーク要素です。通常、ゲートウェイはコマンドを、コール エージェントのデフォルト MGCP ポート（2727）に送信します。
  - Add：指定した IP アドレスを IP アドレス テーブルに追加します。
  - Delete：選択した IP アドレスを IP アドレス テーブルから削除します。
  - IP Address：コール エージェント グループに設定されているゲートウェイの IP アドレスを一覧表示します。
- Call Agents
  - Call Agent to Be Added：コール エージェント グループの MGCP メディア ゲートウェイを制御するコール エージェントの IP アドレスを指定します。通常、コール エージェントはコマンドを、ゲートウェイのデフォルト MGCP ポート（2427）に送信します。
  - Add：指定した IP アドレスを IP アドレス テーブルに追加します。
  - Delete：選択した IP アドレスを IP アドレス テーブルから削除します。
  - IP Address：コール エージェント グループに設定されているコール エージェントの IP アドレスを一覧表示します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

NetBIOS Inspect Map

NetBIOS ペインでは、NetBIOS アプリケーションの事前に設定された検査マップを表示できます。NetBIOS マップでは、NetBIOS アプリケーション検査のデフォルト設定値を変更できます。

NetBIOS アプリケーション検査では、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。

フィールド

- NetBIOS Inspect Maps：定義されている NetBIOS 検査マップを一覧表示するテーブルです。
- Add：新しい NetBIOS 検査マップを設定します。
- Edit：NetBIOS Inspect Maps テーブルで選択した NetBIOS のエントリを編集します。

- Delete：NetBIOS Inspect Maps テーブルで選択した検査マップを削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit NetBIOS Policy Map

Add/Edit NetBIOS Policy Map ペインでは、NetBIOS アプリケーション検査マップのプロトコル違反の設定値を設定できます。

フィールド

- Name : NetBIOS マップの追加時に NetBIOS マップの名前を入力します。NetBIOS マップの編集時には、事前に設定した NetBIOS マップの名前が表示されます。
- Description：NetBIOS マップの説明を 200 文字以内で入力します。
- Check for protocol violations：プロトコル違反の有無をチェックして、指定したアクションを実行します。
  - Action：Drop packet または Log。
  - Log：イネーブルまたはディセーブルにします。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

RTSP Inspect Map

RTSP ペインでは、RTSP アプリケーションの事前に設定された検査マップを表示できます。RTSP マップでは、RTSP アプリケーション検査のデフォルト設定値を変更できます。RTSP マップを使用して、RTSP トラフィックを保護できます。

フィールド

- RTSP Inspect Maps：定義されている RTSP 検査マップを一覧表示するテーブルです。
- Add：新しい RTSP 検査マップを設定します。
- Edit：RTSP Inspect Maps テーブルで選択した RTSP のエントリを編集します。
- Delete：RTSP Inspect Maps テーブルで選択した検査マップを削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit RTSP Policy Map

Add/Edit RTSP Policy Map ペインでは、RTSP アプリケーション検査マップのパラメータと検査設定値を設定できます。

フィールド

- Name：RTSP マップの追加時に RTSP マップの名前を入力します。RTSP マップの編集時には、事前に設定した RTSP マップの名前が表示されます。
- Description：RTSP マップの説明を 200 文字以内で入力します。
- Parameters：このタブで、メディア ポート ネゴシエーション中の予約済みポートの使用を制限し、URL の長さ制限を設定できます。
  - Enforce Reserve Port Protection : メディア ポート ネゴシエーション中の予約済みポートの使用を制限できます。
  - Maximum URL Length：メッセージで許容される URL の最大長を指定します。6000 以下の値を指定します。
- Inspections : このタブで RTSP 検査のコンフィギュレーションを表示して、追加や編集ができます。
  - Match Type：一致タイプを示します。肯定一致と否定一致があります。
  - Criterion：RTSP 検査の基準を示します。
  - Value：RTSP 検査で照合する値を示します。
  - Action：照合条件が一致したときのアクションを示します。
  - Log：ログの状態を示します。
  - Add：Add RTSP Inspect ダイアログボックスを開き、RTSP 検査を追加します。
  - Edit：Edit RTSP Inspect ダイアログボックスを開き、RTSP 検査を編集します。
  - Delete：RTSP 検査を削除します。
  - Move Up：検査をリストの上に移動します。
  - Move Down：検査をリストの下に移動します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit RTSP Inspect

Add/Edit RTSP Inspect ダイアログボックスでは、RTSP 検査マップの照合基準、値、およびアクションを定義できます。

フィールド

- Match Type：トラフィックと値を一致させるかどうかを指定します。

  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。
- Criterion：RTSP トラフィックに適用する照合基準を指定します。
  - URL Filter：URL フィルタリングを照合します。
  - Request Method：RTSP の要求方式を照合します。
- URL Filter Criterion Values：URL フィルタリングを照合するために指定します。正規表現で照合します。
  - Regular Expression：照合する定義された正規表現を一覧表示します。
  - Manage : Manage Regular Expressions ダイアログボックスが開き、正規表現を設定できます。
  - Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。
  - Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップを設定できます。
- URL Filter Actions：プライマリ アクションおよびログを設定します。
  - Action：接続をドロップまたはログに出力します。
  - Log：イネーブルまたはディセーブルにします。
- Request Method Criterion Values：照合する RTSP 要求方式を指定します。
  - Request Method : 要求方式を announce、describe、get_parameter、options、pause、play、record、redirect、setup、set_parameters、teardown のいずれかから指定します。
- Request Method Actions：プライマリ アクションを設定します。
  - Action：Limit rate (pps)。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

SCCP (Skinny) Inspect Map

SCCP (Skinny) ペインでは、SCCP（Skinny）アプリケーションの事前に設定された検査マップを表示できます。SCCP (Skinny) マップでは、SCCP (Skinny) アプリケーション検査のデフォルト設定値を変更できます。

Skinny アプリケーション検査では、パケット データ、ピンホールの動的開放に埋め込まれている IP アドレスとポート番号を変換します。また、追加のプロトコル準拠チェックと基本的なステートフルトラッキングも行います。

フィールド

- SCCP (Skinny) Inspect Maps：定義されている SCCP (Skinny) 検査マップを一覧表示するテーブルです。
- Add：新しい SCCP (Skinny) 検査マップを設定します。SCCP (Skinny) 検査マップを編集するには、SCCP (Skinny) Inspect Maps テーブルで SCCP (Skinny) のエントリを選択し、Customize をクリックします。
- Delete：SCCP (Skinny) Inspect Maps テーブルで選択した検査マップを削除します。
- Security Level：セキュリティ レベル（High または Low）を選択します。
  - Low：デフォルト

    登録：適用強制しない

    メッセージの最大 ID：0x181

    プレフィックスの長さの最小値：4

    メディア タイムアウト：00:05:00

    シグナリング タイムアウト：01:00:00

    RTP 準拠：適用強制しない
  - Medium

    登録：適用強制しない

    メッセージの最大 ID：0x141

    プレフィックスの長さの最小値：4

    メディア タイムアウト：00:01:00

    シグナリング タイムアウト：00:05:00

    RTP 準拠：適用強制する

    ペイロードを音声またはビデオに限定してシグナリング交換を適用：しない
  - High

    登録：適用強制する

    メッセージの最大 ID：0x141

    プレフィックスの長さの最小値：4

    プレフィックスの長さの最大値：65536

    メディア タイムアウト：00:01:00

    シグナリング タイムアウト：00:05:00

    RTP 準拠：適用強制する

    ペイロードを音声またはビデオに限定してシグナリング交換を適用：する
  - Message ID Filtering : Messaging ID Filtering ダイアログボックスが開き、メッセージ ID フィルタを設定できます。
  - Customize : Add/Edit SCCP (Skinny) Policy Map ダイアログボックスを開き、追加の設定を行います。
  - Default Level：セキュリティ レベルをデフォルトの Low レベルに戻します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Message ID Filtering

Message ID Filtering ダイアログボックスでは、メッセージ ID のフィルタを設定できます。

フィールド

- Match Type：一致タイプを示します。肯定一致と否定一致があります。
- Criterion：検査の基準を示します。
- Value：検査で照合する値を示します。
- Action：照合条件が一致したときのアクションを示します。
- Log：ログの状態を示します。
- Add：Add Message ID Filtering ダイアログボックスが開き、メッセージ ID のフィルタを追加できます。
- Edit：Edit Message ID Filtering ダイアログボックスが開き、メッセージ ID のフィルタを編集できます。
- Delete：メッセージ ID のフィルタを削除します。
- Move Up：エントリをリストの上に移動します。
- Move Down：エントリをリストの下に移動します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit SCCP (Skinny) Policy Map（セキュリティ レベル）

Add/Edit SCCP (Skinny) Policy Map ペインでは、SCCP (Skinny) アプリケーション検査マップのセキュリティ レベルと追加の設定値を設定できます。

フィールド

- Name：SCCP（Skinny）マップの追加時に SCCP（Skinny）マップの名前を入力します。SCCP (Skinny) マップの編集時には、事前に設定した SCCP (Skinny) マップの名前が表示されます。
- Description：SCCP (Skinny) マップの説明を 200 文字以内で入力します。
- Security Level：セキュリティ レベル（High または Low）を選択します。
  - Low：デフォルト

    登録：適用強制しない

    メッセージの最大 ID：0x181

    プレフィックスの長さの最小値：4

    メディア タイムアウト：00:05:00

    シグナリング タイムアウト：01:00:00

    RTP 準拠：適用強制しない
  - Medium

    登録：適用強制しない

    メッセージの最大 ID：0x141

プレフィックスの長さの最小値：4
メディア タイムアウト：00:01:00
シグナリング タイムアウト：00:05:00
RTP 準拠：適用強制する
ペイロードを音声またはビデオに限定してシグナリング交換を適用：しない

- High

登録：適用強制する
メッセージの最大 ID：0x141
プレフィックスの長さの最小値：4
プレフィックスの長さの最大値：65536
メディア タイムアウト：00:01:00
シグナリング タイムアウト：00:05:00
RTP 準拠：適用強制する
ペイロードを音声またはビデオに限定してシグナリング交換を適用：する

- Message ID Filtering : Messaging ID Filtering ダイアログボックスが開き、メッセージ ID フィルタを設定できます。
- Default Level：セキュリティ レベルをデフォルトに戻します。

- Details：追加の設定を行うパラメータ、RTP 準拠、メッセージ ID のフィルタリング設定値を表示します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit SCCP (Skinny) Policy Map（詳細）

Add/Edit SCCP (Skinny) Policy Map ペインでは、SCCP (Skinny) アプリケーション検査マップのセキュリティ レベルと追加の設定値を設定できます。

フィールド

- Name：SCCP (Skinny) マップの追加時に SCCP (Skinny) マップの名前を入力します。SCCP (Skinny) マップの編集時には、事前に設定した SCCP (Skinny) マップの名前が表示されます。
- Description：DNS マップの説明を 200 文字以内で入力します。
- Security Level：設定するセキュリティ レベルとメッセージ ID のフィルタリング設定を表示します。
- Parameters：このタブで SCCP (Skinny) のパラメータを設定します。

Enforce endpoint registration：Skinny エンドポイントを登録してから通話を受発信します。
Maximum Message ID：SCCP メッセージ ID に使用できる最大値を指定します。

- SCCP Prefix Length：Skinny メッセージのプレフィックスの長さを指定します。

Minimum Prefix Length：SCCP プレフィックスの長さの許容最小値を指定します。
Maximum Prefix Length：SCCP プレフィックスの長さの許容最大値を指定します。

- Media Timeout：メディア接続時のタイムアウト値を指定します。

- Signaling Timeout：シグナリング接続時のタイムアウト値を指定します。

- RTP Conformance：このタブで SCCP (Skinny) の RTP 準拠を設定します。
  - Check RTP packets for protocol conformance : ピンホールをフローする RTP/RTCP パケットがプロトコルに準拠しているかどうかをチェックします。

    Limit payload to audio or video, based on the signaling exchange : ペイロード タイプを強制的に音声やビデオにして、シグナリング交換を適用します。
- Message ID Filtering : このタブで SCCP (Skinny) のメッセージ ID フィルタリングを設定します。
  - Match Type：一致タイプを示します。肯定一致と否定一致があります。
  - Criterion：検査の基準を示します。
  - Value：検査で照合する値を示します。
  - Action：照合条件が一致したときのアクションを示します。
  - Log：ログの状態を示します。
  - Add：Add Message ID Filtering ダイアログボックスが開き、メッセージ ID のフィルタを追加できます。
  - Edit：Edit Message ID Filtering ダイアログボックスが開き、メッセージ ID のフィルタを編集できます。
  - Delete：メッセージ ID のフィルタを削除します。
  - Move Up：エントリをリストの上に移動します。
  - Move Down：エントリをリストの下に移動します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit Message ID Filter

Add Message ID Filter ダイアログボックスでは、メッセージ ID のフィルタを設定できます。

フィールド

- Match Type：トラフィックと値を一致させるかどうかを指定します。

  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。
- Criterion：SCCP (Skinny) トラフィックに適用する照合基準を指定します。
  - Message ID：指定したメッセージ ID を照合します。

    Message ID：SCCP メッセージ ID に使用できる最大値を指定します。
  - Message ID Range：指定範囲のメッセージ ID を照合します。

    Lower Message ID：SCCP メッセージ ID に使用できる下限値を指定します。

    Upper Message ID：SCCP メッセージ ID に使用できる上限値を指定します。
- Action：Drop packet。
- Log：イネーブルまたはディセーブルにします。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

SIP Inspect Map

SIP ペインでは、SIP アプリケーションの事前に設定された検査マップを表示できます。SIP マップでは、SIP アプリケーション検査のデフォルト設定値を変更できます。

SIP は、インターネット会議、テレフォニー、プレゼンス、イベント通知、インスタント メッセージ機能で幅広く利用されているプロトコルです。もともとテキスト ベースで自由に操作できるこのプロトコルに原因の一端があり、SIP ネットワークのセキュリティは数多くの脅威にさらされています。

SIP アプリケーション検査では、メッセージのヘッダーと本文、ポートの動的開放でアドレス変換を行い、基本的な正常性チェックを行います。また、アプリケーションのセキュリティとプロトコル準拠をサポートし、SIP メッセージの正常性を保つと同時に SIP 関連の脅威を検出します。

フィールド

- SIP Inspect Maps：定義されている SIP 検査マップを一覧表示するテーブルです。
- Add：新しい SIP 検査マップを設定します。SIP 検査マップを編集するには、SIP Inspect Maps テーブルで SIP のエントリを選択し、Customize をクリックします。
- Delete：SIP Inspect Maps テーブルで選択した検査マップを削除します。
- Security Level：セキュリティ レベル（High または Low）を選択します。
  - Low：デフォルト

    SIP インスタント メッセージ（IM）の拡張機能：イネーブル

    SIP トラフィック以外の SIP ポート使用：許可

    サーバとエンドポイントの IP アドレスを非表示：ディセーブル

    ソフトウェアのバージョンと SIP 以外の URI をマスク：ディセーブル

    1 以上の宛先ホップ数を保証：イネーブル

    RTP 準拠：適用強制しない

    SIP 準拠：ステート チェックとヘッダー検証を実行しない
  - Medium

    SIP インスタント メッセージ（IM）の拡張機能：イネーブル

    SIP トラフィック以外の SIP ポート使用：許可

    サーバとエンドポイントの IP アドレスを非表示：ディセーブル

    ソフトウェアのバージョンと SIP 以外の URI をマスク：ディセーブル

    1 以上の宛先ホップ数を保証：イネーブル

    RTP 準拠：適用強制する

    ペイロードを音声やビデオに限定してシグナリング交換を適用：しない

    SIP 準拠：ステート チェックで失敗したパケットをドロップ
  - High

    SIP インスタント メッセージ（IM）の拡張機能：イネーブル

SIP トラフィック以外の SIP ポート使用：禁止
サーバとエンドポイントの IP アドレスを非表示：ディセーブル
ソフトウェアのバージョンと SIP 以外の URI をマスク：イネーブル
1 以上の宛先ホップ数を保証：イネーブル
RTP 準拠：適用強制する
ペイロードを音声やビデオに限定してシグナリング交換を適用：する
SIP 準拠：ステート チェックとヘッダー検証で失敗したパケットをドロップ

- Customize：Add/Edit SIP Policy Map ダイアログボックスを開き、追加の設定を行います。
- Default Level：セキュリティ レベルをデフォルトの Low レベルに戻します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit SIP Policy Map（セキュリティ レベル）

Add/Edit SIP Policy Map ペインでは、SIP アプリケーション検査マップのセキュリティ レベルと追加の設定値を設定できます。

フィールド

- Name：SIP の追加時に SIP マップの名前を入力します。SIP マップの編集時には、事前に設定した SIP マップの名前が表示されます。
- Description：SIP マップの説明を 200 文字以内で入力します。
- Security Level：セキュリティ レベル（High または Low）を選択します。
  - Low：デフォルト

    SIP インスタント メッセージ（IM）の拡張機能：イネーブル
    SIP トラフィック以外の SIP ポート使用：許可
    サーバとエンドポイントの IP アドレスを非表示：ディセーブル
    ソフトウェアのバージョンと SIP 以外の URI をマスク：ディセーブル
    1 以上の宛先ホップ数を保証：イネーブル
    RTP 準拠：適用強制しない
    SIP 準拠：ステート チェックとヘッダー検証を実行しない
  - Medium

    SIP インスタント メッセージ（IM）の拡張機能：イネーブル
    SIP トラフィック以外の SIP ポート使用：許可
    サーバとエンドポイントの IP アドレスを非表示：ディセーブル
    ソフトウェアのバージョンと SIP 以外の URI をマスク：ディセーブル
    1 以上の宛先ホップ数を保証：イネーブル
    RTP 準拠：適用強制する
    ペイロードを音声やビデオに限定してシグナリング交換を適用：しない
    SIP 準拠：ステート チェックで失敗したパケットをドロップ

- High

  SIP インスタント メッセージ（IM）の拡張機能：イネーブル

  SIP トラフィック以外の SIP ポート使用：禁止

  サーバとエンドポイントの IP アドレスを非表示：ディセーブル

  ソフトウェアのバージョンと SIP 以外の URI をマスク：イネーブル

  1 以上の宛先ホップ数を保証：イネーブル

  RTP 準拠：適用強制する

  ペイロードを音声やビデオに限定してシグナリング交換を適用：する

  SIP 準拠：ステート チェックとヘッダー検証で失敗したパケットをドロップ

- Default Level：セキュリティ レベルをデフォルトに戻します。

• Details：追加の設定を行うフィルタリング、IP アドレスのプライバシー、ホップ カウント、RTP 準拠、SIP 準拠、フィールド マスク、および検査の設定値を表示します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit SIP Policy Map（詳細）

Add/Edit SIP Policy Map ペインでは、SIP アプリケーション検査マップのセキュリティ レベルと追加の設定値を設定できます。

フィールド

- Name：SIP の追加時に SIP マップの名前を入力します。SIP マップの編集時には、事前に設定した SIP マップの名前が表示されます。
- Description：SIP マップの説明を 200 文字以内で入力します。
- Security Level：設定するセキュリティ レベルを表示します。
- Filtering：このタブで SIP のフィルタリングを設定します。
  - Enable SIP instant messaging (IM) extensions：インスタント メッセージの拡張機能をイネーブルにします。デフォルトはイネーブルです。
  - Permit non-SIP traffic on SIP port：SIP トラフィック以外に SIP ポートの使用を許可します。デフォルトは許可です。
- IP Address Privacy：このタブで SIP の IP アドレスのプライバシーを設定します。
  - Hide server's and endpoint's IP addresses：IP アドレスのプライバシーをイネーブルにします。デフォルトはディセーブルです。
- Hop Count：このタブで SIP のホップ数を設定します。
  - Ensure that number of hops to destination is greater than 0：Max-Forwards ヘッダーの値が 0 かどうかのチェックをイネーブルにします。

    Action：Drop packet、Drop Connection、Reset、Log。

    Log：イネーブルまたはディセーブルにします。

- RTP Conformance：このタブで SIP の RTP 準拠を設定します。
  - Check RTP packets for protocol conformance：ピンホールをフローする RTP/RTCP パケットがプロトコルに準拠しているかどうかをチェックします。

    Limit payload to audio or video, based on the signaling exchange：ペイロード タイプを強制的に音声やビデオにして、シグナリング交換を適用します。
- SIP Conformance：このタブで SIP の SIP 準拠を設定します。
  - Enable state transition checking：SIP のステート チェックをイネーブルにします。

    Action：Drop packet、Drop Connection、Reset、Log。

    Log：イネーブルまたはディセーブルにします。
  - Enable strict validation of header fields：SIP ヘッダー フィールドの検証をイネーブルにします。

    Action：Drop packet、Drop Connection、Reset、Log。

    Log：イネーブルまたはディセーブルにします。
- Field Masking：このタブで SIP のフィールド マスクを設定します。
  - Inspect non-SIP URIs：Alert-Info と Call-Info ヘッダーに含まれる SIP 以外の URI 検査をイネーブルにします。

    Action：Mask または Log。

    Log：イネーブルまたはディセーブルにします。
  - Inspect server's and endpoint's software version：User-Agent と Server ヘッダーに含まれる SIP エンドポイントのソフトウェア バージョンを検査します。

    Action：Mask または Log。

    Log：イネーブルまたはディセーブルにします。
- Inspections：このタブで SIP 検査のコンフィギュレーションを表示して、追加や編集ができます。
  - Match Type：一致タイプを示します。肯定一致と否定一致があります。
  - Criterion：SIP 検査の基準を示します。
  - Value：SIP 検査で照合する値を示します。
  - Action：照合条件が一致したときのアクションを示します。
  - Log：ログの状態を示します。
  - Add：Add SIP Inspect ダイアログボックスが開き、SIP 検査を追加できます。
  - Edit：Edit SIP Inspect ダイアログボックスが開き、SIP 検査を編集できます。
  - Delete：SIP 検査を削除します。
  - Move Up：検査をリストの上に移動します。
  - Move Down：検査をリストの下に移動します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit SIP Inspect

Add/Edit SIP Inspect ダイアログボックスでは、SIP 検査マップの照合基準と値を定義できます。

フィールド

- Single Match：SIP 検査に照合文が 1 つだけの場合に指定します。
- Match Type：トラフィックと値を一致させるかどうかを指定します。

  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。
- Criterion：SIP トラフィックに適用する照合基準を指定します。
  - Called Party：To ヘッダーに指定された受信側を照合します。
  - Calling Party：From ヘッダーに指定された発信元を照合します。
  - Content Length：ヘッダーのコンテンツの長さを照合します。
  - Content Type：ヘッダーのコンテンツ タイプを照合します。
  - IM Subscriber：SIP IM の加入者を照合します。
  - Message Path：SIP の Via ヘッダーを照合します。
  - Request Method：SIP の要求方式を照合します。
  - Third-Party Registration：サード パーティの登録要求者を照合します。
  - URI Length：SIP ヘッダーの URI を照合します。
- Called Party Criterion Values：照合する受信側を指定します。正規表現で照合します。
  - Regular Expression：照合する定義された正規表現を一覧表示します。
  - Manage : Manage Regular Expressions ダイアログボックスが開き、正規表現を設定できます。
  - Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。
  - Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップを設定できます。
- Calling Party Criterion Values：照合する発信元を指定します。正規表現で照合します。
  - Regular Expression：照合する定義された正規表現を一覧表示します。
  - Manage : Manage Regular Expressions ダイアログボックスが開き、正規表現を設定できます。
  - Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。
  - Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップを設定できます。
- Content Length Criterion Values：指定値より長い SIP コンテンツ ヘッダーを照合します。
  - Greater Than Length：ヘッダーの長さをバイト単位で入力します。
- Content Type Criterion Values：照合する SIP コンテンツ ヘッダーのタイプを指定します。
  - SDP：SDP タイプの SIP コンテンツ ヘッダーを照合します。
  - Regular Expression：正規表現を照合します。

    Regular Expression：照合する定義された正規表現を一覧表示します。

    Manage : Manage Regular Expressions ダイアログボックスが開き、正規表現を設定できます。

    Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。

    Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップを設定できます。
- IM Subscriber Criterion Values：照合する IM 登録者を指定します。正規表現で照合します。
  - Regular Expression：照合する定義された正規表現を一覧表示します。
  - Manage : Manage Regular Expressions ダイアログボックスが開き、正規表現を設定できます。
  - Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。

  - Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップを設定できます。
- Message Path Criterion Values：照合する SIP の Via ヘッダーを指定します。正規表現で照合します。
  - Regular Expression：照合する定義された正規表現を一覧表示します。
  - Manage：Manage Regular Expressions ダイアログボックスが開き、正規表現を設定できます。
  - Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。
  - Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップを設定できます。
- Request Method Criterion Values：照合する SIP 要求方式を指定します。
  - Request Method：次の中から要求方式を指定します。ack、bye、cancel、info、invite、message、notify、options、prack、refer、register、subscribe、unknown、update。
- Third-Party Registration Criterion Values：照合するサード パーティの登録要求者を指定します。正規表現で照合します。
  - Regular Expression：照合する定義された正規表現を一覧表示します。
  - Manage：Manage Regular Expressions ダイアログボックスが開き、正規表現を設定できます。
  - Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。
  - Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップを設定できます。
- URI Length Criterion Values：指定値より長い SIP ヘッダーの URI を指定して照合します。
  - URI type：SIP URI または TEL URI を指定して照合します。
  - Greater Than Length：長さをバイト単位で指定します。
- Multiple Matches：SIP 検査の複数の照合文を指定します。
  - SIP Traffic Class：SIP トラフィック クラスを照合します。
  - Manage：Manage SIP Class Maps ダイアログボックスが開き、SIP クラスマップの追加、編集、削除ができます。
- Actions：プライマリ アクションおよびログを設定します。
  - Action：Drop Packet、Drop Connection、Reset、Log。注：要求方式が invite か register の場合は、Limit rate (pps) アクションを使用できます。
  - Log：イネーブルまたはディセーブルにします。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

SNMP Inspect Map

SNMP ペインでは、SNMP アプリケーションの事前に設定された検査マップを表示できます。SNMP マップでは、SNMP アプリケーション検査のデフォルト設定値を変更できます。

フィールド

- Map　Name：すでに設定されているアプリケーション検査マップを一覧表示します。マップのチェックボックスをオンにし、**Edit** をクリックして、既存のマップの表示または変更ができます。
- Add：新しい SNMP 検査マップを設定します。
- Edit：SNMP Inspect Maps テーブルで選択した SNMP のエントリを編集します。
- Delete：SNMP Inspect Maps テーブルで選択した検査マップを削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit SNMP Map

Add/Edit SNMP Map ダイアログボックスでは、SNMP のアプリケーション検査を制御する SNMP マップを新規作成できます。

フィールド

- SNMP Map Name：アプリケーション検査マップの名前を定義します。
- SNMP version 1：SNMP バージョン 1 のアプリケーション検査をイネーブルにします。
- SNMP version 2 (party based)：SNMP バージョン 2 のアプリケーション検査をイネーブルにします。
- SNMP version 2c (community based)：SNMP バージョン 2c のアプリケーション検査をイネーブルにします。
- SNMP version 3：SNMP バージョン 3 のアプリケーション検査をイネーブルにします。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—