ゾーンベースのファイアウォール ルールの管理

ゾーンベースのファイアウォール機能（ゾーンベース ポリシーファイアウォールとも呼ばれる）を使用すると、「ゾーン」と呼ばれるインターフェイスのグループ間でIOSファイアウォールポリシーを一方向に適用できます。つまり、インターフェースはゾーンに割り当てられ、ファイアウォールルールはゾーン間を一方向に移動する特定のタイプのトラフィックに適用されます。Cisco Security Manager 4.16 以降では、サブインターフェイスをゾーンに割り当てることができます。ゾーンベースのファイアウォールは、デフォルトでセキュア ゾーン間ポリシーを強制します。これにより、トラフィックを許可する明示的なポリシーが定義されるまで、トラフィックはセキュリティ ゾーンを通過できません。

「ゾーン」自体は抽象的なものであり、同じまたは類似するセキュリティ要件を持つ、論理的にグループ化できる複数のインターフェイスを指しています。たとえば、ルータインターフェイス Ethernet 0/0 および Ethernet 0/1 が、ローカル LAN に接続されている場合があります。ファイアウォールの観点では、これら 2 つのインターフェイスは内部ネットワークを表す点と、ファイアウォール設定の目的で単一のゾーンにグループ化できる点で同じです。次に、そのゾーンと他のゾーン間にファイアウォール ポリシーを指定できます。ゾーン間ポリシーでは十分な柔軟性と精度が提供されるので、同一のルータ インターフェイスに接続された複数のホスト グループにさまざまな検査ポリシーを適用できます。

（注） ゾーンベースのファイアウォール機能は、12.4(6)T以降を実行するIOSデバイス、および 12.2(33) 以降を実行する ASR デバイスでサポートされています。

単純な例

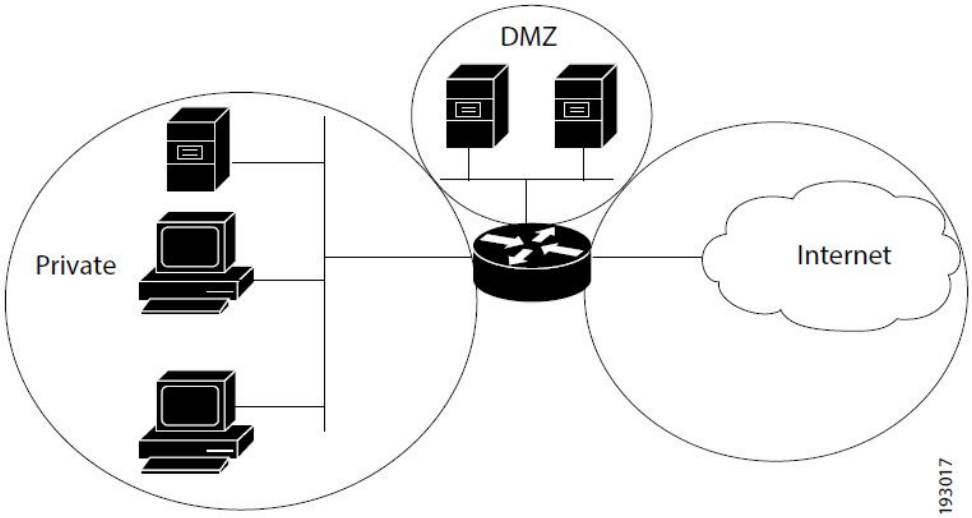
ネットワーク内のセキュリティが類似する領域ごとにセキュリティ ゾーンを設定して、同じゾーンに割り当てられているすべてのインターフェイスが類似するセキュリティ レベルで保護されるようにする必要があります。たとえば、次のように3つのインターフェイスを持つアクセス ルータを考えます。

- 1 つのインターフェイスはパブリック インターネットに接続されています。

- 1 つのインターフェイスは、パブリック インターネットからアクセスできてはいけないプライベート LAN に接続されています。
- 1 つのインターフェイスは、インターネットサービスの「緩衝地帯」（DMZ）に接続されています。ここでは、Web サーバー、

ドメインネームシステム（DNS）サーバーと電子メールサーバーが、公共のインターネットにアクセスできる必要があります。次の図に示すように、このネットワークの各インターフェイスは、独自のゾーンに割り当てられます。

図 *1:* 基本セキュリティ ゾーン トポロジ



この設定例では、通常、以下を定義する 3 つのメインポリシー（ルールセット）があります。

- インターネットへのプライベート ゾーン接続
- DMZ ホストへのプライベート ゾーン接続
- DMZ ホストへのインターネット ゾーン接続

ゾーンベースのファイアウォールは、禁止されたデフォルトのセキュリティ ポスチャの制約を課します。たとえば、DMZ ホストが他のネットワークへのアクセスを特別に許可されていない場合、これらのネットワークは DMZ ホストからの不要な接続から保護されます。同様に、インターネット ホストからプライベート ゾーンへの直接アクセス権が明示的に付与されていないかぎり、プライベート ゾーンのホストはインターネット ホストによる望ましくないアクセスから保護されます。

この単純な例では、各ゾーンにメンバインターフェイスが1つだけあります。たとえば、追加のインターフェイスがプライベートゾーンに追加された場合、その新しいインターフェイスに接続しているホストは、ゾーン内の既存のインターフェイスに接続しているすべてのホストにトラフィックを即時に渡すことができます。また、他のゾーン内のホストへのトラフィックは、既存のプライベート ゾーン ポリシーによって即時に制御されます。

より現実的な例として、DMZ 内の特定のホストへのパブリック インターネットからのさまざまなアクセスを許可する場合、および保護された LAN 内のホストに対するさまざまなアプリケーション使用ポリシーを許可する場合があります。

この章は次のトピックで構成されています。

- ゾーンベースのファイアウォール ルールについて （3 ページ）
- ゾーンベースのファイアウォールルールの Permit/Deny とアクションとの関係について （9 ページ）
- ゾーンベースのファイアウォール ルールの Services と Protocols の関係について （13 ページ）
- ゾーンベースのファイアウォール ルールに対する一般的な推奨事項 （14 ページ）
- ゾーンベースのファイアウォールルールの開発と適用 （15 ページ）
- ゾーンベースのファイアウォールルールの追加 （16 ページ）
- ゾーンベースのファイアウォール ポリシーのインスペクション マップの設定 （19 ページ）
- ゾーンベースのファイアウォール ポリシーのコンテンツ フィルタリング マップの設定 （48 ページ）
- デフォルトのドロップ動作の変更 （66 ページ）
- ゾーンベースのファイアウォール ルールの設定 （67 ページ）
- ゾーンベースのルールと設定のトラブルシューティング （73 ページ）
- [Zone-based Firewall Rules] ページ （78 ページ）

ゾーンベースのファイアウォール ルールについて

ゾーンは、ネットワークのセキュリティ境界を設定します。ゾーンは、トラフィックがネットワークの別の領域に移動するときにインスペクションまたはフィルタリングの対象となる境界を定義します。ゾーン間のデフォルトのゾーンベースのファイアウォールポリシーは、「deny all」です。このため、ゾーンベースのファイアウォールルールが明示的に設定されていない場合、すべてのゾーン間のトラフィックの移動がブロックされます。

ゾーンベースのファイアウォール ルールは、ゾーンのペア間にあるさまざまなタイプの単方向トラフィックに、特定のアクション（Drop、Pass、Inspect、および Content Filter）を適用します。トラフィックの方向は、送信元ゾーンと宛先ゾーンを各ルールの一部として指定することで設定します。

ログ

ゾーンベースのファイアウォール ルールには、syslog、alert、audit-trail のロギング オプションがあります。ほとんどのメッセージは、syslog サーバが設定されていないかぎりルータ コン

ソールに記録されます。syslog ロギングの設定の詳細については、Cisco IOS ルータにおけるロギングを参照してください。

重要なポイント

ゾーンとゾーンベースのファイアウォール ルールについて、次の点に注意してください。

- ゾーンベースのファイアウォール機能は、12.4(6)T 以降を実行する IOS デバイス、および 12.2(33) 以降を実行する ASR デバイスでのみサポートされています。
- ゾーンベースのファイアウォール ルールと IOS インスペクション ルールが同じインターフェイスを使用する場合は、エラーが発生します。

ゾーンベースのファイアウォールモデルと以前のインターフェイスベースのインスペクションルールモデルは、ルータ上で互いに排他的ではありませんが、指定されたインターフェイス上で結合することはできません。つまり、インターフェイスは、インスペクションルールで設定されている場合に、セキュリティゾーンのメンバとして設定できません。さらに、両方のモデルを同時に使用するようにルーターを設定することはお勧めしません。

- インターフェイスは1つのセキュリティゾーンにのみ割り当てることができますが、ゾーンには複数のインターフェイスを含めることができます。インターフェイスが複数のゾーンに割り当てられている場合は、エラーが発生します。
- 特定のインターフェイスとの間のすべてのトラフィックは、インターフェイスがゾーンに割り当てられている場合に暗黙的にブロックされます（同じゾーンの他のインターフェイスとの間で送受信されるトラフィック、およびルータ上の任意のインターフェイスに送信されるトラフィックを除く）。このため、ゾーンメンバ インターフェイスとの間のトラフィックを許可するには、そのゾーンと他の任意のゾーンとの間にトラフィックを許可または検査するルールを 1 つ以上設定する必要があります。
- トラフィックは、同じゾーンのメンバであるインターフェイス間を流れることを暗黙に許可されます。ただし、同じゾーンのメンバ間のトラフィックのインスペクションを要求するルールを定義できます。
- 「Self」ゾーンは、ルータ自体を独立したセキュリティゾーンとして定義するデフォルトのゾーンであり、送信元ゾーンまたは宛先ゾーンとして指定できます。Self ゾーンは、デフォルトの「deny all」ポリシーの唯一の例外です。任意のルータ インターフェイスへのすべてのトラフィックは、明示的に拒否されるまで許可されます。

Self ゾーンを含むゾーンベースのファイアウォール ルールは、ローカル トラフィック（ルータに向けられたトラフィック、またはルータによって生成されたトラフィック）に適用されます。ルータを通過するトラフィックには適用されません。詳細については、Self ゾーン （6 ページ）を参照してください。

- Self ゾーンに適用されるルールでは、検査アクションは許可されません。
- Pass アクションは、一方向でだけトラフィックを許可します。リターン トラフィックのルールは明示的に定義する必要があります。ただし、Inspect アクションでは、リターン トラフィックは確立済みの接続に対して自動的に許可されます。

- トラフィックは、ゾーンメンバインターフェイスと、ゾーン メンバでない任意のインターフェイスとの間を流れることができません。
- ゾーンに割り当てられていないインターフェイスは、依然として従来のルータ ポートとして機能でき、他のタイプのファイアウォール ルールが設定されている場合があります。

ただし、インターフェイスがゾーンベースのファイアウォールポリシーに含まれない場合でも、そのインターフェイスをゾーンに追加し、そのゾーンとゾーン間トラフィックフローが必要な他のゾーンとの間に「pass all」ポリシー（「ダミーポリシー」の一種）を設定する必要がある場合があります。

- ゾーンのメンバーであるインターフェイスに適用されるアクセス制御リスト（ACL）は、ゾーンルールが適用される前に処理されます。したがって、両方のルールタイプの使用を継続するには、インターフェイス ACL を緩和して、特定のトラフィック フローがゾーンベースのルールによって処理されるようにすることが必要な場合があります。
- ゾーン内のすべてのインターフェイスは、同じ Virtual Routing and Forwarding（VRF; 仮想ルーティングおよび転送）インスタンスに属している必要があります。ゾーンベースのルールは、メンバ インターフェイスが別々の VRF にあるゾーン間に設定できます。ただし、トラフィックがこれらの VRF 間を流れることができない場合、これらのルールは実行されません。詳細については、ゾーンと VRF 対応ファイアウォール （8 ページ）を参照してください。
- ゾーンは、インターフェイス ロール オブジェクトを使用して定義されます。ゾーンに使用されているインターフェイスロールの定義を変更した場合は、ゾーンを変更することになり、既存のトラフィック フローに影響することがあります。さらに、インターフェイスロールでワイルドカードを使用してインターフェイス名のパターンを指定すると、ルータで新しいインターフェイスを作成するときに、インターフェイスがゾーンに自動的に追加される可能性があることに注意してください。
- ゾーンベースのファイアウォールルールに、競合するゾーン情報が含まれている場合、テーブルで最初に定義されたルールが優先されます。有効なゾーンを参照しないルールは展開されず、アクティビティ検証警告が表示されます。
- 空のゾーンがあると、特定のデバイスでアクティビティ検証エラーが発生します。次の制約事項リストを参照してください。
- 特定のデバイスでは、送信元ゾーンと宛先ゾーンを同じにできません。次の制約事項リストを参照してください。

（注） バージョン 4.21 以降、Cisco Security Manager では、すべてのアグリゲーション サービス ルータ、統合サービスルータ、埋め込み型サービスルータ、および Cisco IOS ソフトウェアで動作するすべてのデバイスについて、バグ修正または拡張機能のサポートを含むサポート全体が終了します。

関連項目

- Self ゾーン （6 ページ）
- ゾーンベースのファイアウォールポリシーでの VPN の使用 （7 ページ）
- ゾーンと VRF 対応ファイアウォール （8 ページ）
- ゾーンベースのファイアウォール ルールの設定 （67 ページ）
- ゾーンベースのファイアウォールルールの Permit/Deny とアクションとの関係について （9 ページ）
- ゾーンベースのファイアウォール ルールの Services と Protocols の関係について （13 ページ）
- ゾーンベースのファイアウォール ルールに対する一般的な推奨事項 （14 ページ）
- ゾーンベースのファイアウォールルールの開発と適用 （15 ページ）

Self ゾーン

ルータ自体は「**Self**」という固有の名前を持つ独立したセキュリティ ゾーンとして定義されており、IOS ファイアウォールがルータで終端または発信するトラフィック（「ローカル」トラフィックと呼ばれる）の検査をサポート（TCP、UDP および H.323 のみ）しているため、着信および発信ルータトラフィックは、ルーテッドゾーン間トラフィックと同じ方法でルールの対象となります。

インターフェイスがゾーンに割り当てられると、そのインターフェイスに接続されているホストがそのゾーンに含まれます。デフォルトでは、トラフィックは同じゾーンのメンバーであるインターフェイス間のフローを許可されており、デフォルトの「deny-all」ポリシーがゾーン間を移動するトラフィックに適用されます。

ただし、その他のゾーンおよびルータの IP インターフェイス（Self ゾーン）間を直接流れるトラフィックは暗黙的に許可されています。これにより、ゾーンファイアウォール設定がルータに適用される場合に、ルータの管理インターフェイスへの接続が維持されることが保証されます。

つまり、ルータのインターフェイスの IP アドレスへのトラフィックフローおよび IP アドレスからのトラフィックフローは、当初はゾーンポリシーによって制御されていません。ルータインターフェイスと他のゾーンの間を移動するトラフィックを制御する場合は、このローカルトラフィックをブロックまたは許可するルールを適用する必要があります。

Self ゾーンのルールを設定する場合は、次の点を考慮します。

- ルータに設定されているすべての IP アドレスは、インターフェイス ゾーンのメンバーシップに関係なく Self ゾーンに属します。
- 逆に明示的なルールを設定するまで、Self ゾーンとの間のトラフィックは制限されません。

つまり、Self ゾーンを含むゾーンベースのファイアウォールルールを構成すると、Self ゾーンと他のゾーンの間のトラフィックはすぐに両方向で制限されます。たとえば、「プライベート」ゾーンから Self ゾーンへのトラフィックに影響するルールを定義した場合、Self からプライベートへのルールを 1 つ以上定義するまで、ルータはプライベート ゾーンにトラフィックを発信できません。

ルータ自体と、Self ゾーン ルールに含まれない他のゾーンとの間のトラフィックは影響を受けません。

- Self ゾーンに適用されるルールでは、検査アクションは許可されません。

インバウンド Self ゾーン トラフィックに制限を設定する場合は、必要なアウトバウンド トラフィック（ルーティング プロトコルおよびネットワーク管理プロトコルを含む）を検討します。たとえば、あるゾーンからルータ自体へのインバウンド トラフィックを制限した場合、ルーティング プロトコルはそのゾーンに属するすべてのインターフェイスで動作を停止することがあります。

関連項目

- ゾーンベースのファイアウォール ルールについて （3 ページ）

ゾーンベースのファイアウォールポリシーでの VPN の使用

IP Security（IPsec）VPN 実装が最近拡張されて、VPN 接続のファイアウォール ポリシー設定が単純化されました。IPSec Virtual Tunnel Interface（VTI; 仮想トンネル インターフェイス）と GRE+IPSec により、特定のセキュリティ ゾーンにトンネル インターフェイスを配置することで、VPN サイト間接続およびクライアント接続をそのセキュリティ ゾーンに限定できます。接続が特定のポリシーによって制限される必要がある場合は、接続を VPN DMZ 内で隔離できます。または、VPN 接続が暗黙的に信頼されている場合は、VPN 接続をネットワーク内で信頼されているのと同じセキュリティ ゾーンに配置できます。

（トンネル/ループバック/仮想インターフェイスを動的に作成する）動的VPN でゾーンベースのファイアウォール ルールを使用するようにルータを設定するには、次の操作を行います。

- VPN インターフェイス専用のゾーンを定義します。
- [Zone Based Firewall] ページ （68 ページ）の [VPN] タブの [VPNゾーン（VPN Zone）] フィールドに、このゾーンを入力します。
- ゾーンベースのファイアウォール ルールを作成して、VPN トラフィックを適宜許可します。

VTI 以外の IPsec が採用されている場合は、VPN にゾーンベースのファイアウォール ポリシーを設定するときに注意する必要があります。ゾーン ポリシーでは、保護されたホストが暗号化された VPN トラフィックの入力インターフェイスとは異なるゾーンにある場合に、リモート VPN ホストまたはクライアントによるそれらのホストへのアクセスを明示的に許可する必要があります。このアクセス ポリシーは、VPN クライアントの送信元 IP アドレスを列挙するアクセス コントロール リスト（ACL）、および VPN クライアントが到達することを許可されてい

るすべての保護ホストの宛先 IP アドレスを含めることで設定する必要があります。アクセスポリシーが適切に設定されていない場合、ポリシーによって、脆弱なホストが敵対的なトラフィックにさらされる可能性があります。

これらのトピックの詳細については、cisco.com のホワイトペーパー『Using VPN with Zone-Based Policy Firewall』を参照してください。

関連項目

- ゾーンベースのファイアウォール ルールについて （3 ページ）

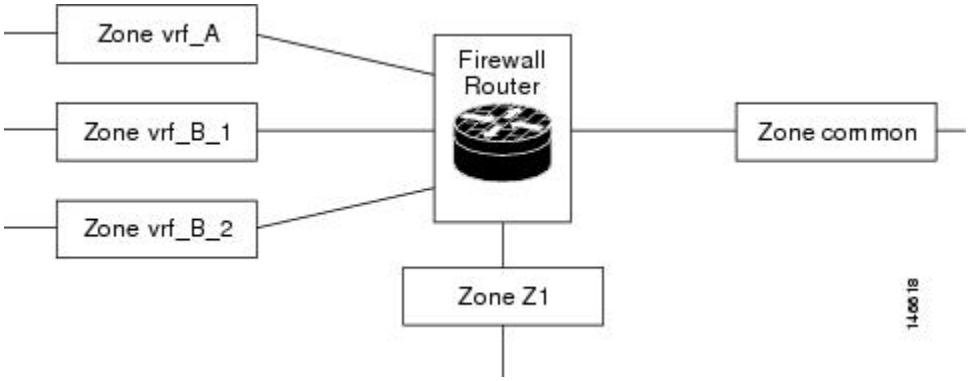
ゾーンと VRF 対応ファイアウォール

Cisco IOS ファイアウォールは Virtual Routing and Forwarding（VRF）に対応しており、異なる VRF 間で重複する IP アドレス、VRF に対する個別のしきい値とタイムアウトなどを管理できます。ゾーンベースのファイアウォール ルールを適用するには、ゾーン内のすべてのインターフェイスが同じ VRF に属している必要があります。

ルータで複数の VRF が設定されていて、あるインターフェイスですべての VRF に共通のサービス（インターネットサービスなど）が提供されている場合は、そのインターフェイスを別のゾーンに配置します。その後、共通ゾーンと他のゾーンとの間のポリシーを定義できます（VRF あたり 1 つ以上のゾーンを設定できます）。

次の図に示すように、異なる VRF を含む 2 つのゾーン間でルールを設定できます。

図 *2:* ゾーンと *VRF*



この図の場合：

- 共通サービスを提供するインターフェイスはゾーン「common」のメンバです。
- すべての VRF A は、単一のゾーン「vrf_A」にあります。
- VRF B には複数のインターフェイスが含まれており、「vrf_B_1」と「vrf_B_2」の 2 つのゾーンに分割されています。
- ゾーン Z1 には VRF インターフェイスがありません。

この設定に基づいて、次の処理を行うことができます。

- これらの各ゾーンと common ゾーンの間にポリシーを指定できます。さらに、VRF ルートエクスポートが設定されていて、トラフィックパターンが適切である場合は、ゾーン vrf_A、vrf_B_n、および Z1 のそれぞれの間でポリシーを指定できます。
- ゾーン vrf_A と vrf_B_1 の間にポリシーを設定できますが、トラフィックがこれらのゾーン間を流れることができることを確認します。
- VRF ごとにグローバルなしきい値とタイマーを指定する必要はありません。その代わりに、パラメータマップによって inspect アクションにパラメータが提供されます。

関連項目

- ゾーンベースのファイアウォール ルールについて （3 ページ）

ゾーンベースのファイアウォールルールの Permit/Deny とアクションとの関係について

ゾーンベースのファイアウォールルールを作成する場合、実行に関連する 2 つの設定を行う必要があります。許可/拒否とアクション（ドロップ、パス、検査、またはコンテンツフィルタ）です。目的の結果を得るには、この 2 つのパラメータ間の関係を明確に理解する必要があります。

- **許可/拒否**：許可/拒否設定は、アクセス制御リスト（ACL）エントリの許可/拒否に対応しているように見えます。ただし、ゾーンベースのファイアウォール ルールでは、標準のアクセス ルールとは異なり、これらのキーワードでトラフィックは許可または拒否されません。代わりに、[Source]、[Destination]、および [Services] フィールドで定義されたトラフィック フローにアクションを適用するかどうかと、それらが関連クラス マップの処理に影響するかどうかを指定します。
  - **許可**：指定したアクションを、[送信元（Source）]、[宛先（Destination）]、および [サービス（Services）]フィールドと一致するトラフィックに適用します（プロトコルが [Protocols] テーブルにリストされている場合、アクションはそれらのプロトコルに限定されます）。

ヒント：ゾーンベースのすべてのルールは基本的に「許可」 ルールである必要があります。これは最も理解しやすい設定です。選択したアクションを適用するトラフィックを識別しているということです。

- - **拒否**：[送信元（Source）]、[宛先（Destination）]、および [サービス（Services）]フィールドで定義されたトラフィックを除外します。（プロトコルが [プロトコル（Protocols）] テーブルにリストされている場合、除外はそれらのプロトコルに限定されます）。つまり、ルールに一致しないトラフィックとして処理します。代わりに、ゾーン ペアの後続のクラス マップ（ゾーン ルールと同じではない）を評価し、トラフィックと一致する後続マップを探します。後続マップがトラフィックと一致し

ない場合は、デフォルトのルールをトラフィックに適用します（デフォルトのドロップ動作の変更 （66 ページ）を参照）。

ゾーン ルールとクラスマップ間には1対1関係がないことに注意してください。したがって、ルール テーブルで参照するだけでは、ルールがクラス マップに変換される方法を判断できません。Deny 規則に一致するトラフィックに適用できる後続規則を確認するには、設定をプレビューする必要があります（設定をプレビューするには、変更を保存し、[ツール（Tools）] > [設定のプレビュー（ Preview Configuration）] を選択します。詳細については、設定のプレビューを参照してください）。

一般的に、拒否ルールを使用して、サブネットに適用する許可ルールからサブネット内の特定の IP アドレスを除外できます。たとえば、10.100.10.0/24 に適用されるルールから 10.100.10.1 を除外します。ただし、特定の IP アドレスの Permit ルールを作成し、目的のアクションを適用して、このルールがゾーンベースのルールテーブルの一般ルールよりも上にリストされるようにする方がはるかに簡単です。

Deny ルールを使用する場合は、ゾーンベースのルールと設定のトラブルシューティング （73 ページ）も参照してください。

- **アクション**：アクションパラメータは、許可ルールに一致するトラフィックに起きることを定義します。どのクラス マップにルールが追加されるかを判断する場合を除き、Deny ルールではこれらのパラメータが無視されます。

Permit ルールを作成する場合、[Source]、[Destination]、[Services]、および [Protocol] フィールドと一致するトラフィックは、選択したアクション（トラフィックをドロップ（さらにオプションでログに記録）、トラフィックを渡す（さらにオプションでログに記録）、トラフィックを検査、またはコンテンツ フィルタリングを適用（Web トラフィックの場合のみ））に従って処理されます。

一部のプロトコルでトラフィックを検査する場合、またはコンテンツ フィルタリングを実行する場合は、詳細インスペクションに使用するポリシー マップを指定するオプションもあります。詳細インスペクション ポリシー マップでは、トラフィックのより詳細な特性に基づくアクションも指定します。この追加のインスペクションは、割り当てたポリシーマップが参照するクラスマップの要件を満たすパケットに適用されます。詳細インスペクションのクラスマップに一致しないパケットは許可されます。このため、詳細インスペクションは、ポリシーマップでそのアクションが指定されている場合に TCP 接続をリセットすることがあります。

次の表に、ゾーンベースのファイアウォール ルールで選択した Permit/Deny とアクションの関係を示します。この表では、TCP サービスを例として使用しますが、全般的な説明は IP サービスにも適用されます。結果は、ルールで指定した [From Zone] と [To Zone] にだけ適用されます。

表 *1 :* ゾーンベースのルールの *Permit/Deny* とアクションとの関係

許可/拒否	サービス	ルール アクション	プロトコル	結果
許可（Permit）	[TCP]	成功（Pass）	（なし）	すべての TCP トラフィックを通過させます。
拒否（Deny）	[TCP]	成功（Pass）	（なし）	ルールをスキップし、次のクラスマップを評価します。Permit ルールを含む次のクラスマップが適用されるか、またはクラスのデフォルト ルールが適用されます。 Pass アクションは無視されます。
許可（Permit）	[TCP]	削除（Drop）	（なし）	すべての TCP トラフィックをドロップします。
拒否（Deny）	[TCP]	削除（Drop）	（なし）	ルールをスキップし、次のクラスマップを評価します。Permit ルールを含む次のクラスマップが適用されるか、またはクラスのデフォルト ルールが適用されます。 Drop アクションは無視されます。
許可（Permit）	[TCP]	成功（Pass）	DNS	DNS トラフィックのみ通過させます。その他の TCP トラフィックは、以降のルールによって処理されます。
許可（Permit）	[TCP]	削除（Drop）	DNS	DNS トラフィックはドロップされます。その他の TCP トラフィックは、以降のルールによって処理されます。
拒否（Deny）	[TCP]	成功（Pass）	DNS	DNS トラフィックのルールをスキップし、次のクラスマップを評価します。Permit ルールを含む次のクラスマップが適用されるか、またはクラスのデフォルト ルールが適用されます。 Pass アクションは無視されます。
拒否（Deny）	[TCP]	削除（Drop）	DNS	DNS トラフィックのルールをスキップし、次のクラスマップを評価します。Permit ルールを含む次のクラスマップが適用されるか、またはクラスのデフォルト ルールが適用されます。 Drop アクションは無視されます。

許可/拒否	サービス	ルール アクション	プロトコル	結果
許可（Permit）	[TCP]	検査（Inspect）	HTTP	HTTP トラフィックを許可して検査します。より詳細な検査用のポリシーマップを指定すると、ポリシーマップのアクションは、より詳細な検査パラメータに一致するすべてのパケットに適用されます（プロトコル違反の接続のリセットなど）。
拒否（Deny）	[TCP]	検査（Inspect）	HTTP	HTTP トラフィックのルールをスキップし、次のクラスマップを評価します。Permit ルールを含む次のクラスマップが適用されるか、またはクラスのデフォルト ルールが適用されます。 検査アクションは無視されます。 **ヒント** 後続のルールまたはクラス デフォルトが検査なしでトラフィックを通過させる場合、HTTP 接続のリターン トラフィックを許可するために、もう一方の方向に Permit/Pass ルール（またはアクセス ルール）を作成する必要があります。HTTP接続を禁止する場合は、拒否/検査ルールの代わりに許可/ドロップルールを作成します。
許可（Permit）	[TCP]	コンテンツ フィルタ	HTTP	HTTP トラフィックを許可して検査し、URL フィルタリング マップを適用して、要求された Web サイトに基づいて Web 接続を選択的に許可または拒否します。 より詳細な検査用のポリシー マップを指定すると、ポリシーマップのアクションは、より詳細な検査パラメータに一致するすべてのパケットに適用されます（プロトコル違反の接続のリセットなど）。 このため、Webサイトがブラックリストに追加されたか、HTTP パケットが詳細インスペクション ルールに違反したため、トラフィックがドロップされることがあります。

許可/拒否	サービス	ルール アクション	プロトコル	結果
拒否（Deny）	[TCP]	コンテンツ フィルタ	HTTP	HTTP トラフィックのルールをスキップし、次のクラスマップを評価します。Permit ルールを含む次のクラスマップが適用されるか、またはクラスのデフォルト ルールが適用されます。 コンテンツ フィルタ アクションは無視されます。 **ヒント** このタイプのルールでは、トラフィックをドロップまたはコンテンツ フィルタリングを適用する後続のクラス マップがない場合に、指定した送信元/宛先をコンテンツ フィルタリングから免除できます。ただし、このトラフィックに対して HTTP 接続を許可する場合は、トラフィックの Permit/Inspect ルールを作成する必要があります。

ゾーンベースのファイアウォール ルールの Services と Protocols の関係について

ゾーンベースのファイアウォールを作成する場合、ターゲット トラフィックの特性の識別に役立つ、一見すると同じような 2 つのパラメータ（Services と Protocols）があります。これらのフィールドのエントリは非常によく似た情報を提供する場合がありますが、デバイス設定でゾーンベースのファイアウォール ポリシーを構築するときに異なる方法で使用されます。ここでは、これらのフィールドの推奨される使用方法について説明します。

- [サービス（Services）] : [サービス（Services）] フィールドは、アクセス制御リスト（ACL）エントリのトラフィック プロトコルの定義に使用されます。この ACL エントリは、指定された送信元と宛先とともに、ポリシーを適用するトラフィックを定義するためにクラスマップによって使用されます。ただし、標準のアクセス ルールとは異なり、このサービス情報はトラフィック プロトコルを識別する主要な手段ではありません。ACL ではエントリごとにサービスを指定する必要があるため、サービス情報が必要となります。

一般に、[プロトコル（Protocol）] テーブルを使用して Drop、Pass、または Inspect の対象とする特定のプロトコルを識別するため、すべてのゾーンベースのファイアウォール ルールの [サービス（Services）] フィールドはデフォルト エントリ（IP）のままにできます。

[Service] に IP 以外を指定する場合は、[Protocol] テーブルにリストされているプロトコルと競合しないように選択してください。たとえば、[サービス（Services）] フィールドで UDP を指定せずに、テーブルに TCP ベースのプロトコルをリストします。一般に、特定のルールに対して、[Services] フィールドに特定のサービスを指定する場合は、[Protocol] テーブルにプロトコルを入力しないでください。

- [プロトコル（Protocol）]：[ゾーンベースのルールの追加（Add Zone Based Rule）] ダイアログボックスと [ゾーンベースのルールの編集（Edit Zone Based Rule）] ダイアログボックスの [アクション（Action）] 領域にある [プロトコル（Protocol）] テーブルは、1 つ以上のプロトコルの選択、カスタム ポート アプリケーション マッピングの追加（デフォルト以外のポートを指定した場合）、およびディープ インスペクション ポリシー マップの適用に使用されます。DNS などの非常に特定的なプロトコル、TCP や UDP などの一般プロトコル、さらに特殊なアプリケーションに使用するポートを識別するカスタムプロトコルを指定できます。

原則として、[Services] は [IP] に設定したままにし、[Protocol] テーブルを使用して、Drop、Pass、Inspect アクションのすべてのゾーンベース ルールに対するプロトコル（これもサービスです）を指定します（コンテンツ フィルタ アクションは、HTTP プロトコルを自動的に使用します。これを設定することはできますが、変更はできません。）このアプローチに従うと、可能な限り「クリーン」で、解釈（およびトラブルシューティング）が容易な設定が作成されます。

デバイス コンフィギュレーションを生成するときにこれらのフィールドがどのように使用されるかの詳細については、ゾーンベースのルールと設定のトラブルシューティング （73 ページ）を参照してください。

ゾーンベースのファイアウォール ルールに対する一般的な推奨事項

ゾーンベースのファイアウォール ルールでは、さまざまな設定が可能です。標準のアクセス ルール、インスペクション ルール、および Web フィルタ ルールの代わりにゾーンベースのルールを使用できるため、非常に複雑で分析が難しい一連のルールをすばやく生成できます。

ゾーンベースのルールを定義する際は、それらをできるだけ単純明快なものにするように努めてください。ゾーンベースのファイアウォール ポリシーの簡略性を維持するために、次の推奨事項を考慮してください。

- **許可**ルールのみを使用します。選択したアクションによって、一致したトラフィックに対する処理が決定されます。**拒否**ルールは解析が困難です。詳細については、ゾーンベースのファイアウォール ルールの Permit/Deny とアクションとの関係について （9 ページ）を参照してください。
- **ドロップ**ルールと**パス**ルールは、標準のインターフェイス アクセス ルールと同等ですが、指定されたゾーンペアに適用されます。[サービス（Services）] フィールドまたは [プロトコル（Protocol）] テーブルのいずれかを使用してトラフィックのタイプを識別できますが、[プロトコル（Protocol）] テーブルのみを使用することをお勧めします。トラフィックをドロップするには、アクション [ドロップ（Drop）] とともに [許可（Permit）] を指定します。
- 最初のトラフィックを検査する前に、それを通過させる必要はありません。たとえば、ゾーン間の HTTP トラフィックを許可する場合、必要な許可/インスペクション ルールは 1 つだけです。最初に許可/パス ルールを作成する必要はありません。Pass ルールを使用す

る場合で、リターン トラフィックを許可する場合には、リターン方向の Pass ルールも作成する必要があることに注意してください。実際には、通常、インスペクションルールのみを使用して、パスルールの作成を避けることができます。

- 許可/パスルールと許可/ドロップルールを使用して、標準のアクセスルールと同じ機能を実行できます。このため、アクセス ルール ポリシーを排除し、ゾーンベースのファイアウォール ルールだけを使用できます。

ただし、インターフェイス アクセス ルールの解析に使用できるツールは複数あり、Security Manager ではゾーンベース ルールとアクセス ルールに同じインターフェイス ロールを使用できるため、ゾーン ルール テーブルではなくアクセス ルール テーブルに Pass/Drop ポリシー（標準アクセス ルールの Permit/Deny）を作成する方が便利な場合があります。ゾーン ルール テーブルは、主にゾーンベースの Inspection および Content Filter ルールに使用します。

- セクションを使用して、各ゾーンペアのルールを編成します。セクションを使用すると、ペアのすべてのルールを簡単に参照できます。これは、ルールに順序の依存関係がある場合に重要になることがあります。セクションでの作業の詳細については、セクションを使用したルール テーブルの編成を参照してください。

ゾーンベースのファイアウォールルールの開発と適用

次に、ゾーンベースのファイアウォールルールを作成してネットワークに適用する方法の概要を示します。

- セキュリティ ゾーンに関してネットワークとそのサブネットワークを検討します。さまざまなゾーンのセキュリティ要件について考えます。一般的なガイドラインとして、セキュリティの観点から見たときに類似するルータ インターフェイスをグループ化します。
- あるゾーンから別のゾーンに移動するときに検査されるトラフィックのタイプを決定し、それぞれのタイプをどのように検査し、処理するかを決定します。
- これらの決定を実行するゾーンベースのファイアウォールルールを定義します。このプロセスには、ルール自体を定義する前に実行できる、またはルールの定義中に必要に応じて実行できる次の手順の一部またはすべてが含まれる場合があります。
  - 名前付きインターフェイス ロール オブジェクトを作成し、適切なインターフェイスとインターフェイス パターンをそれらのオブジェクトに割り当てることで、ゾーンを定義します。
  - 特定のレイヤ 4 プロトコルとポート、およびオプションで特定のネットワークとホストの Port Application Mapping（PAM; ポート アプリケーション マッピング）設定を定義/編集します。
  - レイヤ 7 プロトコル（HTTP、IMAP、インスタントメッセージング（IM）、ピアツーピア（P2P））のディープ パケット インスペクション（DPI）ポリシーを設定します。
  - プロトコル情報パラメータ マップを設定します。これらのパラメータ マップは IM アプリケーションと対話する DNS サーバを定義します。

- 検査アクションの接続、タイムアウト、およびその他の設定を定義する検査パラメータマップを設定します。
- URL ベース コンテンツ フィルタリングの WebFilter パラメータまたは WebFilter ポリシー マップを定義します。

ここでは、これらの手順に関する追加情報を提供します。

- マップ オブジェクトについて
- ゾーンベースのファイアウォール ポリシーのコンテンツ フィルタリング マップの設定（48 ページ）
- ゾーンベースのファイアウォール ポリシーのインスペクション マップの設定 （19 ページ）

ゾーンベースのファイアウォールルールの追加

この手順では、Security Manager でゾーンベースのファイアウォール ルールを設定する方法について説明します。

関連項目

- ゾーンベースのファイアウォール ルールについて （3 ページ）
- ゾーンベースのファイアウォール ルールの設定 （67 ページ）
- マップ オブジェクトについて
- ルールのイネーブル化とディセーブル化
- ルールの追加および削除
- ルールの移動とルール順序の重要性

ステップ 1 [Zone-based Firewall Rules] ページ （78 ページ）へのアクセス方法を次に示します。

- （デバイスビュー）IOS ルータを選択し、ポリシーセレクタから **[ファイアウォール（Firewall）] > [ゾーンベースのファイアウォールルール（Zone Based Firewall Rules）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[ファイアウォール（Firewall）] > [ゾーンベースのファイアウォールルール（Zone Based Firewall Rules）]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

ステップ 2 ルールテーブルの下にある [行の追加（Add Row）] ボタンをクリックするか、テーブル内の任意の場所を右クリックして [行の追加（Add Row）] を選択し、[ゾーンベースのファイアウォールルールの追加（Add Zone Based Firewall Rule）] ダイアログボックスを開きます。

このダイアログボックスの詳細な説明については、ゾーンベースのファイアウォール ルールの追加と編集（82 ページ）を参照してください。

ステップ 3 このルールの基本トラフィック フローを定義します。

（注） [Permit/Deny]、[Sources]、[Destinations]、および [Services] オプションは、詳細なアクション関連ポリシーを適用することで拡張でき、特定のゾーンのペア間の特定の方向に制限される単純なアクセス ルールの定義と考えることができます。

a) [Permit] または [Deny] で、このルールに一致するトラフィックをさらに処理するかどうかを選択します。詳細については、ゾーンベースのファイアウォールルールの Permit/Deny とアクションとの関係について （9 ページ）を参照してください。

b) 必要に応じて、送信元と宛先のホスト/ネットワークまたはセキュリティグループ（IOS 15.2(2)T+ および IOS-XE 3.5.x(15.2(1)S)+ のみ）を指定します。

デフォルトでは、トラフィック定義には、「any」（任意）の送信元から「any」（任意）の宛先へのパケットが含まれます。これらのフィールドを使用して、1 つ以上の送信元および宛先ホスト/ネットワークを指定することにより、この基本トラフィック定義を改良できます（詳細については、ネットワーク/ホストオブジェクトについておよびネットワーク/ホストオブジェクトについてを参照してください）。

c) IP や TCP など、トラフィックのタイプを示す 1 つ以上のサービス（プロトコル）を指定します。

複数のサービスを指定できますが、IP は通常、単独で使用されます（サービスとサービス オブジェクトおよびポート リスト オブジェクトの理解と指定 を参照。）

d) [From Zone] を指定します。このゾーンから発信したトラフィックだけが一致します。

e) [To Zone] を指定します。このゾーンに流れるトラフィックだけが一致します。

ゾーン/インターフェイス オブジェクトの詳細については、インターフェイス ロール オブジェクトについてを参照してください。

（注） [開始ゾーン（From Zone）] と [終了ゾーン（To Zone）] は、「ゾーンペア」と呼ばれるものを構成します。

f) [Advanced] ボタンをクリックして時間範囲を追加するか、このゾーンベースのファイアウォール ルールに packet-fragment または established-connection 制限を適用します。

これらのオプションの詳細については、ゾーンベースのファイアウォール ルール：[Advanced Options] ダイアログボックス （87 ページ）を参照してください。

ステップ 4 ベースアクションを選択し、必要に応じて追加のパラメータを指定することにより、この定義に一致するトラフィックに適用されるアクションを指定します。

a) ベースアクションを選択します。

- [ドロップ（Drop）]：一致するトラフィックはサイレントにドロップされます。ドロップの通知は発信元ホストに送信されません。
- [ドロップして記録（Drop and Log）]：一致するトラフィックはドロップされ、syslog メッセージが生成されます。ドロップの通知は発信元ホストに送信されません。

- [通過（Pass）]：トラフィックは転送されます。 このアクションは単方向です。[Pass] では、指定した方向のトラフィックだけが許可されます。
- [通過させて記録（Pass and Log）]：トラフィックは転送され、syslog メッセージが生成されます。

（注） [通過（Pass）] アクションは、トラフィック内の接続またはセッションの状態を追跡しません。[通過（Pass）] は、一方向のトラフィックのみを許可します。リターン トラフィックを許可するには、対応するルールを定義する必要があります。Pass アクションは、IPSec ESP、IPSec AH、ISAKMP、およびその他の動作が予測可能なセキュアなプロトコルに役立ちます。ただし、ほとんどのアプリケーション トラフィックは、Inspect アクションを指定したゾーンベースのファイアウォール ルールでより適切に処理されます。

- [検査（Inspect）]：このオプションは、状態に基づくトラフィック制御を提供します。デバイスは TCP および UDP トラフィックに関する接続またはセッション情報を維持するため、接続要求に対するリターントラフィックが許可されます。

選択したレイヤ 4（TCP、UDP）プロトコルおよびレイヤ 7（HTTP、IMAP、インスタント メッセージング、およびピアツーピア）プロトコルに基づいたパケット インスペクションを適用する場合、このオプションを選択します。選択したプロトコルのポート アプリケーション マッピング（PAM）も編集でき、ディープ パケット インスペクション（DPI）を設定して、レイヤ 7 プロトコルの追加のプロトコル関連情報を指定できます。

- [コンテンツフィルタ（Content Filter）]：WebFilter パラメータマップまたは WebFilter ポリシーマップに基づいて HTTP コンテンツインスペクション（URL フィルタリング）を設定します。このアクションは一般に Web フィルタ ルールと同等ですが、ゾーンベースのファイアウォール ルールでは、HTTP ディープ パケット インスペクション（DPI）などの追加の詳細オプションがサポートされます。

ルータが HTTP 要求を代行受信し、プロトコル関連の検査を実行します。また、任意で、要求を許可するかブロックするかを決定するためにサードパーティ製サーバに接続します。WebFilter パラメータ マップを提供できます。このマップにより、ローカル URL リスト、および外部 SmartFilter（以前の N2H2）や Websense サーバからの情報に基づくフィルタリングを定義します。または、ローカル、N2H2、Websense、または Trend Micro フィルタリング データにアクセスする WebFilter ポリシー マップを提供できます。

b) コンテンツフィルタ以外のアクションについては、考慮される特定のトラフィックプロトコルを選択および編集できます。

[プロトコル（Protocol）] テーブルの横にある [選択（Select）] をクリックして [Protocol Selector] ダイアログボックス （89 ページ）を開きます。1 つ以上のプロトコルを選択し、[>>] をクリックしてそれらを [選択済みのプロトコル（Selected Protocols）] リストに追加します。選択したプロトコルの [Port Application Mapping (PAM)] 設定を編集できます。詳細については、[Configure Protocol] ダイアログボックス （90 ページ）を参照してください。

インスタント メッセージングおよび Stun-ice プロトコルでは、プロトコル情報パラメータ マップを選択できます。また、アクションとして [Inspect] が選択されている場合、一部のプロトコルでは詳細インスペクション ポリシー マップを選択できます。

詳細については、ゾーンベースのファイアウォール ポリシーのインスペクション マップの設定 （19 ページ）および プロトコル情報パラメータ マップの設定 （43 ページ）を参照してください。

（注） [ドロップ（Drop）]、[ドロップして記録（Drop and Log）]、[通過（Pass）]、[通過させて記録（Pass and Log）] アクションのプロトコルを指定する必要はありません。[Protocol] テーブルを空のままにして、[送信元（Sources）]、[宛先（Destinations）]、および[サービス（Services）] パラメータに基づいてトラフィックを渡すかドロップできます。

c) 選択したアクションが [Content Filter] の場合は、URL フィルタリングを設定します。

1. [Protocol] フィールドの横の [Configure] をクリックして HTTP PAM 設定をカスタマイズし、HTTP 詳細インスペクション ポリシー マップを適用します。詳細については、[Configure Protocol] ダイアログボックス （90 ページ）を参照してください。
2. [WebFilter Parameter Map] または [WebFilter Policy Map] を選択し、適切な WebFilter マップの名前を入力または選択します。詳細については、ゾーンベースのファイアウォール ポリシーのコンテンツ フィルタリング マップの設定 （48 ページ）を参照してください。

d) 選択したアクションが [Inspect] または [Content Filter] の場合は、カスタマイズした接続、タイムアウト、およびその他の設定のセットに適用するインスペクション パラメータ マップの名前を入力または選択します。詳細については、インスペクション パラメータ マップの設定 （40 ページ）を参照してください。

ステップ 5 （任意）ルールの識別に役立つ説明を入力します。

ステップ 6 （任意）[Category] の下で、ルール テーブルでこのルールを識別するために使用するカテゴリを選択します。カテゴリ オブジェクトの使用を参照してください。

ステップ 7 [OK] をクリックして [ゾーンベースのファイアウォールルールの追加（Add Zone Based Firewall Rule）] ダイアログボックスを終了し、[ゾーンベースのファイアウォールルール（Zone Based Firewall Rules）] テーブルに戻ります。

新しいルールがテーブルにリストされます。

ゾーンベースのファイアウォール ポリシーのインスペクション マップの設定

ルータのゾーンベースのファイアウォール ポリシーを設定する場合は、ルールのアクションとして [Inspect] を選択することで、トラフィックを検査するルールを定義できます。続いて、検査する特定のプロトコルを選択できます。

一部のプロトコルでは、ポリシーマップを選択して、基準に一致するパケットに対して詳細インスペクションを実行できます。これらのマップは、ルールの定義時に [ポリシーオブジェクトセレクタ（Policy Object Selector）] ダイアログボックスから設定するか、[Policy Object Manager] ウィンドウでいつでも設定できます（[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択）。ポリシー マップに加えて、インスペクションに対して設定できるパラメータ マップがいくつかあります。

- 詳細インスペクションを許可するプロトコルでは、関連ポリシーマップを選択できます。ポリシー マップには、ターゲットのトラフィックの一致条件を定義するクラス マップが含まれます。これらのポリシーマップを [Policy Object Manager] で作成するには、[マップ（Maps）]>[ポリシーマップ（Policy Maps）]>[検査（Inspect）] フォルダから、次の表に一覧表示されている使用可能なマップタイプの 1 つを選択し、ゾーンベースのファイアウォール ポリシーのポリシー マップの設定 （45 ページ）に記載の詳細な使用方法情報を確認します。

詳細インスペクション ポリシー マップで使用するクラス マップの作成については、次の表の一致基準ダイアログボックスと、ゾーンベースのファイアウォール ポリシーのクラス マップの設定 （23 ページ）を参照してください。これらのクラスマップは、[Policy Object Manager] の [マップ（Maps）]>[クラスマップ（Class Maps）]>[検査（Inspect）] フォルダにあります。

- アクションとして [Inspect]（または [Content Filter]）が選択されている場合は、ゾーンベースのファイアウォール ルールの追加と編集 （82 ページ）のインスペクション パラメータ マップも適用できます。ゾーンベースのファイアウォール インスペクションには、いくつかの一般設定が含まれ、そのすべてに、ほとんどのネットワークに適切なデフォルト値があります。これらの設定のいずれかを調整する場合は、検査パラメータマップを作成する必要があります。[Policy Object Manager] で、[マップ（Maps）]>[パラメータマップ（Parameter Maps）]>[検査（Inspect）]>[検査パラメータ（Inspect Parameters）] を選択し、インスペクション パラメータ マップの設定 （40 ページ）の詳細な使用状況情報を確認します。

表 *2:* ゾーンベースのファイアウォール インスペクション ルールのポリシー オブジェクト

プロトコル	IOS ソフトウェアの最小バージョン	ポリシーマップ	クラスマップ	パラメータマップ	説明および一致基準の参照
インスタントメッセージング：AOL、ICQ、MSN Messenger、Windows Messenger、Yahoo Messenger	12.4(9)T	IM（ゾーンベースの IOS）	AOL ICQ MSN Messenger Windows Messenger Yahoo Messenger	Protocol Info	サービスのタイプ（テキストチャットまたはその他）に基づいてトラフィックを検査します。ゾーンベースのファイアウォールの IM アプリケーション クラス マップ：[Add Match Condition]/[Edit Match Condition] ダイアログボックス （26 ページ）を参照してください。 プロトコル情報パラメータ マップを選択して、検査しているトラフィックで使用されている DNS サーバも定義する必要があります。プロトコル情報パラメータ マップの設定 （43 ページ）を参照してください。

プロトコル	IOS ソフトウェアの最小バージョン	ポリシーマップ	クラスマップ	パラメータマップ	説明および一致基準の参照
Peer-to-peer（P2P; ピアツーピア）：eDonkey、FastTrack、Gnutella、Kazaa2	12.4(9)T	P2P	eDonkey FastTrack Gnutella Kazaa2	なし（None）	ファイル名に基づいてトラフィックを検査します。ゾーンベースのファイアウォールの P2P アプリケーション クラス マップ：[Add Match Condition]/[Edit Match Condition] ダイアログボックス （27 ページ）を参照してください。
H.323	12.4(6)T	H.323（IOS）	H.323（IOS）	なし（None）	H.323 メッセージ タイプに基づいてトラフィックを検査します。H.323（IOS）クラス マップの [Add Match Criterion]/[Edit Match Criterion] ダイアログボックス （28 ページ）を参照してください。
HTTP	12.4(6)T	HTTP（Zone ベースの IOS）	HTTP（IOS）	なし（None）	ヘッダーや本文の内容、ポートの誤用、トラフィックに Java アプレットが含まれているかどうかなど、広範な基準に基づいてトラフィックを検査します。HTTP（IOS）クラスの [Add Match Criterion]/[Edit Match Criterion] ダイアログボックス （28 ページ）を参照してください。
Internet Message Access Protocol（IMAP） Post Office Protocol 3（POP3）	12.4(6)T	IMAP POP3	IMAP POP3	なし（None）	無効なコマンドまたはクリアテキスト ログインに基づいてトラフィックを検査します。IMAP および POP3 クラス マップの [Add Match Criterion]/[Edit Match Criterion] ダイアログボックス （32 ページ）を参照してください。
SIP（Session Initiation Protocol）	12.4(6)T	SIP（IOS）	SIP（IOS）	なし（None）	広範な基準に基づいてトラフィックを検査します。SIP（IOS）クラスの [Add Match Criterion]/[Edit Match Criterion] ダイアログボックス （32 ページ）を参照してください。

プロトコル	IOS ソフトウェアの最小バージョン	ポリシーマップ	クラスマップ	パラメータマップ	説明および一致基準の参照
SMTP（Simple Mail Transfer Protocol）	12.4(6)T	SMTP	SMTP	なし（None）	データ長に基づいてトラフィックを検査します。 SMTP クラス マップの [Add Match Criterion]/[Edit Match Criterion] ダイアログボックス （34 ページ）を参照してください。
Stun-ice	12.4(9)T	なし	なし	Protocol Info	プロトコル情報パラメータマップを選択して、検査しているトラフィックで使用されている DNS サーバーを定義する必要があります。 プロトコル情報パラメータ マップの設定 （43 ページ）を参照してください。
Sun Remote Procedure Call（RPC; リモート プロシージャ コール）	12.4(6)T	Sun RPC	Sun RPC	なし（None）	RPC プロトコル番号に基づいてトラフィックを検査します。 Sun RPC クラス マップの [Add Match Criterion]/[Edit Match Criterion] ダイアログボックス （38 ページ）を参照してください。
SCTP（Stream Control Transmission Protocol）	12.4(6)T	SCTP	なし	なし	PPID 一致基準に基づいてトラフィックを検査します。SCTP ポリシーマップの [一致条件とアクションの追加または編集（Add or Edit Match Condition and Action] ダイアログボックスを参照してください。
Diameter プロトコル	12.4(6)T	Diameter	Diameter	なし（None）	アプリケーション ID、コマンドコード、および AVP に基づいてトラフィックを検査します。Diameter クラスとポリシーマップの [一致条件（とアクション）の追加または編集（Add or Edit Match Condition (and Action)] ダイアログボックスを参照してください。
LISP（Locator and ID Separation Protocol）	12.4(6)T	LISP	なし	なし	アプリケーション ID、コマンドコード、および AVP に基づいてトラフィックを検査します。

関連項目

- ゾーンベースのファイアウォール ルールについて （3 ページ）
- [Zone-based Firewall Rules] ページ （78 ページ）
- ポリシー オブジェクトの作成
- マップ オブジェクトについて

ゾーンベースのファイアウォール ポリシーのクラス マップの設定

[Add Class Map]/[Edit Class Map] ダイアログボックスを使用すると、同じタイプのポリシー マップで使用するクラスマップを定義できます。ダイアログボックスの名前は、作成するマップのタイプを示します。

クラス マップでは、アプリケーション固有の基準に基づいてトラフィックを定義します。次に、対応するポリシー マップ内のクラス マップを選択し、選択したトラフィックに適用するアクションを設定します。したがって、各クラスマップには、同じ方法（許可する、ドロップするなど）で処理するトラフィックを含める必要があります。

Cisco IOS ソフトウェアを実行しているデバイスのゾーンベースのファイアウォール ルールを設定する場合は、次の目的でクラス マップを作成できます。

- 12.4(6)T 以降では、H.323、HTTP、IMAP、POP3、SIP、SMTP、および Sun RPC タイプのトラフィックのインスペクション用のクラスを作成できます。Local、N2H2（SmartFilter）、WebSense のクラス タイプを使用して、Web フィルタリングのクラスを作成できます。一致基準の詳細については、次の項を参照してください。
  - H.323（IOS）クラス マップの [Add Match Criterion]/[Edit Match Criterion] ダイアログボックス （28 ページ）
  - HTTP（IOS）クラスの [Add Match Criterion]/[Edit Match Criterion] ダイアログボックス （28 ページ）
  - IMAP および POP3 クラス マップの [Add Match Criterion]/[Edit Match Criterion] ダイアログボックス （32 ページ）
  - SIP（IOS）クラスの [Add Match Criterion]/[Edit Match Criterion] ダイアログボックス （32 ページ）
  - SMTP クラス マップの [Add Match Criterion]/[Edit Match Criterion] ダイアログボックス （34 ページ）
  - Sun RPC クラス マップの [Add Match Criterion]/[Edit Match Criterion] ダイアログボックス （38 ページ）
  - ローカル Web フィルタ クラスの [Add Match Criterion]/[Edit Match Criterion] ダイアログボックス （38 ページ）
  - N2H2 および Websense クラスの [Add Match Criterion]/[Edit Match Criterion] ダイアログボックス （39 ページ）

- 12.4(9)T 以降では、AOL、eDonkey、FastTrack、Gnutella、ICQ、Kazaa2、MSN Messenger、Windows Messenger、および Yahoo Messenger タイプのトラフィックのインスペクション用のクラスを作成できます。一致基準の詳細については、次の項を参照してください。
  - ゾーンベースのファイアウォールの IM アプリケーション クラス マップ：[Add Match Condition]/[Edit Match Condition] ダイアログボックス （26 ページ）
  - ゾーンベースのファイアウォールの P2P アプリケーション クラス マップ：[Add Match Condition]/[Edit Match Condition] ダイアログボックス （27 ページ）
- 12.4(20)T 以降では、トレンドポリシーオブジェクトを使用して Web フィルタリングのクラスを作成できます。Trend コンテンツ フィルタ クラス マップの一致基準については、次の表で説明します。

ナビゲーション パス

[管理（Manage）]>[ポリシーオブジェクト（Policy Objects）]を選択し、コンテンツテーブルの**[マップ（Maps）]>[クラスマップ（Class Maps）]**フォルダ内のフォルダにある任意のゾーンベースのクラスマップオブジェクトを選択します。作業領域内を右クリックしてから [新規オブジェクト(New Object] を選択するか、行を右クリックしてから [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- マップ オブジェクトについて
- ゾーンベースのファイアウォール ポリシーのインスペクション マップの設定 （19 ページ）
- ゾーンベースのファイアウォール ポリシーのコンテンツ フィルタリング マップの設定 （48 ページ）
- ゾーンベースのファイアウォール ルールについて （3 ページ）

フィールド リファレンス

表 3： ゾーンベースのファイアウォール ポリシーの ***[Add Class Maps]/[Edit Class Maps]*** ダイアログボックス

要素	説明
名前	ポリシー オブジェクトの名前。最大 40 文字を使用できます。
説明	ポリシー オブジェクトの説明。最大 200 文字を使用できます。

要素	説明
[Match] テーブル 一致タイプ（Match Type） （Trend コンテンツ フィルタ クラス マップを除く）	[Match] テーブルには、クラス マップに含まれている基準が表示されます。各行には、各基準に一致する、または一致しないトラフィックを検査で検索するかどうか、および検査される基準と値が示されます。 テーブルの名前は、クラスに一致するためにトラフィックがすべての基準を満たす必要があるか（[Match All]）、またはリストされているいずれかの基準との一致で十分か（[Match Any]）を示します。HTTP（IOS）および SMTP クラスの場合は、すべて一致といずれか一致のどちらかを選択できます。[Match All] テーブルを使用しているときに、複数の基準を追加する場合は、いずれのトラフィックとも一致しない特性のセットを定義しないようにしてください。 ヒント [完全一致（Match All）] は、Cisco IOS Software バージョン 12.4(20)T 以降を実行しているデバイスでだけ動作します。 • 基準を追加するには、[Add] ボタンをクリックし、[Match Criterion] ダイアログボックスに入力します。詳細については、上記で示している項を参照してください。 • 基準を編集するには、基準を選択し、[Edit] ボタンをクリックします。 • 基準を削除するには、基準を選択し、[Delete] ボタンをクリックします。
Trend コンテンツ フィルター一致基準	Trend コンテンツ フィルタ クラス マップの一致基準は、他のどのクラス マップとも異なります。テーブルに項目を追加する代わりに、リストから目的の項目を選択します。次のタブにある Trend-Micro 分類のいずれかの [Enable] チェックボックスをオンにします。トラフィックは、いずれかの選択項目と一致する場合にクラスと一致します。 • [Productivity Categories]：トラフィックを URL が属するカテゴリと照合します。たとえば、ギャンブルやポルノに関連するトラフィックをターゲットにできます。 • [Security Ratings]：トラフィックを、Trend-Micro によって割り当てられたセキュリティ レーティングと照合します。たとえば、広告に関連するトラフィックであるアドウェアをターゲットにできます。 これらのカテゴリまたはセキュリティ分類の詳細については、Trend-Micro のマニュアルを参照してください。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用を参照してください。

要素	説明
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可および個々のデバイスのポリシー オブジェクト オーバーライドについてを参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

ゾーンベースのファイアウォールの IM アプリケーション クラス マップ：[Add Match Condition]/[Edit Match Condition] ダイアログボックス

ゾーンベースのファイアウォール ポリシーで使用するさまざまな Instant Messenger（IM; インスタント メッセンジャ）アプリケーション クラス用の [Add Match Criterion]/[Edit Match Criterion] ダイアログボックスを使用して、クラス マップの一致基準と値を定義します。

次のタイプのトラフィックに対して一致を定義できます。

- [Any]：テキスト チャット トラフィックを除く、アプリケーションからの任意のタイプのトラフィック。
- [Text-chat]：テキスト チャット トラフィック。

ナビゲーション パス

AOL、ICQ、MSN Messenger、Windows Messenger、または Yahoo Messenger クラスの [クラスマップの追加（Add Class Maps）]/[クラスマップの編集（Edit Class Maps）] ダイアログボックスで、テーブル内を右クリックして [行の追加（Add Row）] を選択するか、行を右クリックして [行の編集（Edit Row）] を選択します。ゾーンベースのファイアウォール ポリシーのクラス マップの設定 （23 ページ） を参照してください。

関連項目

- マップ オブジェクトについて
- ゾーンベースのファイアウォール ポリシーのインスペクション マップの設定 （19 ページ）
- ゾーンベースのファイアウォール ルールについて （3 ページ）

ゾーンベースのファイアウォールの P2P アプリケーション クラス マップ：[Add Match Condition]/[Edit Match Condition] ダイアログボックス

ゾーンベースのファイアウォール ポリシーで使用するさまざまな Peer-to-Peer（P2P; ピアツーピア）アプリケーション クラスの [Add Match Criterion]/[Edit Match Criterion] ダイアログボックスを使用して、クラス マップの一致基準と値を定義します。

ナビゲーション パス

eDonkey、FastTrack、Gnutella、または Kazaa2 クラスの [クラスマップの追加（Add Class Maps）]/[クラスマップの編集（Edit Class Maps）] ダイアログボックスで、テーブル内を右クリックして [行の追加（Add Row）] を選択するか、行を右クリックして [行の編集（Edit Row）] を選択します。 ゾーンベースのファイアウォール ポリシーのクラス マップの設定 （23 ページ） を参照してください。

関連項目

- マップ オブジェクトについて
- ゾーンベースのファイアウォール ポリシーのインスペクション マップの設定 （19 ページ）
- ゾーンベースのファイアウォール ルールについて （3 ページ）

フィールド リファレンス

表 *4 :* ゾーンベースのファイアウォールの *P2P* アプリケーション クラス マップの *[Add Match Condition]/[Edit Match Condition]* ダイアログボックス

要素	説明
基準	照合の基準を選択します。 • [File Transfer]：ファイル転送トラフィックを照合します。 • [Search Filename]：ユーザが検索しているファイルの名前を照合します。この基準を使用して、ユーザが eDonkey を使用して特定のファイルを検索できないようにできます。 • [Text Chat]：eDonkey テキスト チャット トラフィックを照合します。
タイプ（Type）	基準に一致するトラフィックをマップに含めることを指定します。
ファイル名	トラフィックに関連付けられているファイルの名前。正規表現を使用して、名前のパターンを指定できます。正規表現の作成に使用できるメタ文字の詳細については、正規表現の作成に使用されるメタ文字を参照してください。 **ヒント**　eDonkey にはファイル名は不要です。

H.323（IOS）クラス マップの [Add Match Criterion]/[Edit Match Criterion] ダイアログボックス

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IOS の機能をサポートしていますが、拡張機能はサポートしていません。

ゾーンベースのファイアウォール ポリシーで使用する H.323（IOS）クラスの [Add Match Criterion]/[Edit Match Criterion] ダイアログボックスを使用して、クラス マップの一致基準と値を定義します。H.323 プロトコル メッセージ タイプに基づいてトラフィックを照合できます。照合するメッセージを選択します。

ナビゲーション パス

H.323（IOS）クラスの [クラスマップの追加（Add Class Maps）]/[クラスマップの編集（Edit Class Maps）] ダイアログボックスで、テーブル内を右クリックして [行の追加（Add Row）] を選択するか、行を右クリックして [行の編集（Edit Row）] を選択します。ゾーンベースのファイアウォール ポリシーのクラス マップの設定 （23 ページ） を参照してください。

関連項目

- マップ オブジェクトについて
- ゾーンベースのファイアウォール ポリシーのインスペクション マップの設定 （19 ページ）
- ゾーンベースのファイアウォール ルールについて （3 ページ）

HTTP（IOS）クラスの [Add Match Criterion]/[Edit Match Criterion] ダイアログボックス

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IOS の機能をサポートしていますが、拡張機能はサポートしていません。

ゾーンベースのファイアウォール ポリシーで使用する HTTP（IOS）クラスの [Add Match Criterion]/[Edit Match Criterion] ダイアログボックスを使用して、クラス マップの一致基準と値を定義します。

このダイアログボックスのフィールドは、選択した基準によって変わります。次の基準を使用できます。

- [Request/Response Body Length]、[Request Body Length]、[Response Body Length]：要求、応答、またはその両方の本文の長さが指定した数よりも小さいまたは大きいことを指定します。これにより、最小または最大のメッセージ長を設定できます。

- [Request/Response Body]、[Request Body]、[Response Body]：要求、応答、またはその両方の本文の照合に正規表現を適用します。
- [Request/Response Header]、[Request Header]、[Response Header]：ヘッダーと正規表現の照合、繰り返しフィールドのテスト、コンテンツ タイプのチェック、またはヘッダー内のレコードの合計の長さまたはレコード数のチェックを行うことができます。
- [Request/Response Protocol Violation]：非準拠 HTTP トラフィックを照合します。
- [Request Argument]、[Request URI]：要求メッセージ内の引数（パラメータ）または Uniform Resource Identifier（URI）の長さやコンテンツ（正規表現）を照合します。
- [Request Port Misuse]：特定のタイプのアプリケーションによるポートの誤使用を照合します。
- [Response Body Java Applet]：HTTP 接続の Java アプレットを照合します。
- [Response Header Status Line]：ヘッダー内のステータス行のコンテンツの照合に正規表現を適用します。

ナビゲーション パス

HTTP（IOS）クラスの [クラスマップの追加（Add Class Maps）]/[クラスマップの編集（Edit Class Maps）] ダイアログボックスで、テーブル内を右クリックして [行の追加（Add Row）] を選択するか、行を右クリックして [行の編集（Edit Row）] を選択します。ゾーンベースのファイアウォール ポリシーのクラス マップの設定 （23 ページ） を参照してください。

関連項目

- マップ オブジェクトについて
- ゾーンベースのファイアウォール ポリシーのインスペクション マップの設定 （19 ページ）
- ゾーンベースのファイアウォール ポリシーのコンテンツ フィルタリング マップの設定 （48 ページ）
- ゾーンベースのファイアウォール ルールについて （3 ページ）

フィールド リファレンス

表 *5 : HTTP（IOS）クラスの [Add Match Criterion]/[Edit Match Criterion] ダイアログボックス*

要素	説明
基準	照合する HTTP トラフィック基準を指定します。基準については、上記で説明しています。
タイプ（Type）	基準に一致するトラフィックをマップに含めることを指定します。

要素	説明
可変フィールド 次のフィールドは、[Criterion] フィールドでの選択内容によって変わります。このリストは、表示されると想定されるフィールドのスーパーセットです。	
最小長	評価されるフィールドの最小長（バイト単位）。指定した数値よりも長さが小さい場合は、条件が一致します。
最大長	評価されるフィールドの最大長（バイト単位）。指定した数値よりも長さが大きい場合は、条件が一致します。
ヘッダーオプション	ヘッダー レコードのタイプ。レコード タイプを選択しない場合は、ヘッダー内のすべてのレコードにカウントまたは表現が適用されます。レコード タイプを選択した場合、それらの選択は選択したタイプのレコードにだけ適用されます。コンテンツ タイプまたは転送の符号化を選択した場合は、それらのタイプに関連する追加の選択を行うことができます。
要求メソッド	照合する要求メソッド。
値（コンテンツタイプ）	[Header Option] フィールドでコンテンツ タイプを選択した場合、次のタイプを選択できます。 • [Mismatch]：要求メッセージの受け入れフィールド値に照らして応答メッセージのコンテンツ タイプを検証します。 • [Unknown]：コンテンツ タイプは不明です。既知のすべての MIME タイプに照らして項目を評価する場合は、[Unknown] を選択します。 • [Violation]：コンテンツ タイプ定義と実際の本文のコンテンツ タイプが一致しません。

要素	説明
エンコード タイプ	[Header Option] フィールドで転送の符号化を選択した場合、次のタイプを選択できます。 • [All]：すべての転送符号化タイプ。 • [Chunked]：メッセージ本文は一連のチャンクとして転送され、各チャンクに固有のサイズ インジケータが含まれます。 • [圧縮（Compress）]：メッセージ本文は、UNIX ファイル圧縮を使用して転送されます。 • [Deflate]：メッセージ本文は、zlib 形式（RFC 1950）および deflate 圧縮（RFC 1951）を使用して転送されます。 • [GZIP]：メッセージ本文は、GNU zip（RFC 1952）を使用して転送されます。 • [Identity]：転送の符号化は実行されません。
Greater Than Count	ヘッダーで使用できるレコードの最大数。特定のヘッダー オプションを選択した場合、カウントはそれらのタイプのレコードに適用されます。特定のヘッダー オプションを選択しない場合、カウントはタイプにかかわらずヘッダー内のレコードの総数に適用されます。
正規表現	パターンマッチングに使用する正規表現を定義する、正規表現オブジェクト。オブジェクトの名前を入力します。[選択（Select）] をクリックして既存のオブジェクトのリストからオブジェクトを選択するか、または新しい正規表現オブジェクトを作成できます。
ポート誤使用	照合する要求ポート誤使用のタイプ。選択できるオプションは、次のとおりです。 • [Any]：リストされている誤使用タイプのいずれか。 • [IM]：インスペクションの対象となるインスタント メッセージング プロトコル アプリケーション。 • [P2P]：インスペクションの対象となるピアツーピア プロトコル アプリケーション。 • [Tunneling]：インスペクションの対象となるトンネリング アプリケーション（HTTPPort/HTTPHost）。

IMAP および POP3 クラス マップの [Add Match Criterion]/[Edit Match Criterion] ダイアログボックス

ゾーンベースのファイアウォール ポリシーで使用する Internet Message Access Protocol（IMAP）および Post Office Protocol 3（POP3）クラスの [Add Match Criterion]/[Edit Match Criterion] ダイアログボックスを使用して、クラス マップの一致基準と値を定義します。

照合するトラフィックを識別するために次の基準を選択できます。

- [Invalid Command]：POP3 サーバまたは IMAP 接続で有効でないコマンドを照合します。
- [Login Clear Text]：パスワードがクリア テキストで提供されるセキュアでないログインを照合します。

ナビゲーション パス

IMAP または POP3 クラスの [クラスマップの追加（Add Class Maps）]/[クラスマップの編集（Edit Class Maps）] ダイアログボックスで、テーブル内を右クリックして [行の追加（Add Row）] を選択するか、行を右クリックして [行の編集（Edit Row）] を選択します。ゾーンベースのファイアウォール ポリシーのクラス マップの設定 （23 ページ） を参照してください。

関連項目

- マップ オブジェクトについて
- ゾーンベースのファイアウォール ポリシーのインスペクション マップの設定 （19 ページ）
- ゾーンベースのファイアウォール ルールについて （3 ページ）

SIP（IOS）クラスの [Add Match Criterion]/[Edit Match Criterion] ダイアログボックス

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IOS の機能をサポートしていますが、拡張機能はサポートしていません。

ゾーンベースのファイアウォール ポリシーで使用する SIP（IOS）クラスの [Add Match Criterion]/[Edit Match Criterion] ダイアログボックスを使用して、クラス マップの一致基準と値を定義します。

このダイアログボックスのフィールドは、選択した基準によって変わります。

ナビゲーション パス

SIP（IOS）クラスの [クラスマップの追加（Add Class Maps）]/[クラスマップの編集（Edit Class Maps）] ダイアログボックスで、テーブル内を右クリックして [行の追加（Add Row）] を選択するか、行を右クリックして [行の編集（Edit Row）] を選択します。ゾーンベースのファイアウォール ポリシーのクラス マップの設定 （23 ページ） を参照してください。

関連項目

- マップ オブジェクトについて
- ゾーンベースのファイアウォール ポリシーのインスペクション マップの設定 （19 ページ）
- ゾーンベースのファイアウォール ルールについて （3 ページ）

フィールド リファレンス

表 *6 : SIP（IOS）クラスの [Add Match Criterion]/[Edit Match Criterion] ダイアログボックス*

要素	説明
基準	照合するトラフィック基準を指定します。次の中から選択できます。 • [Protocol Violation]：プロトコルに違反するトラフィックを照合します。 • [Request/Response Header Options]：選択した要求または応答ヘッダー フィールドと正規表現を照合します。 • [Request Options]：選択した要求ヘッダー フィールドと要求メソッドを照合するか、正規表現を照合します。 • [Response Options]：選択した応答ヘッダー フィールドまたはステータス メッセージと正規表現を照合します。
タイプ（Type）	基準に一致するトラフィックをマップに含めることを指定します。
可変フィールド 次のフィールドは、[Criterion] フィールドでの選択内容によって変わります。このリストは、表示されると想定されるフィールドのスーパーセットです。	
ヘッダー	要求または応答メッセージのヘッダーのタイプ。正規表現は、選択したタイプのヘッダーの内容と照合されます。

要素	説明
方法	検査する要求メソッドを次に示します。 • [ack]：前のメッセージが有効で受け入れられることを確認応答します。 • [bye]：コールを終了することを示します。 • [cancel]：保留中の要求を終了します。 • [info]：コールのシグナリング パスを経由する中間セッション シグナリング情報を伝えます。 • [invite]：コールをセットアップします。 • [message]：インスタント メッセージを送信します。 • [notify]：状態変更を加入者に通知します。 • [options]：別のユーザ エージェントまたはプロキシ サーバの容量を問い合わせます。 • [prack]：暫定応答メッセージの信頼性の高い転送を提供します。 • [refer]：受信者が要求で提供されている連絡先情報を使用してサードパーティに連絡する必要があることを示します。 • [register]：レコードのアドレスの SIP 要求の転送先とする連絡先アドレスを含みます。 • [subscribe]：1 つのイベントまたは一連のイベントに関する通知をあとで受け取ることを要求します。 • [update]：セッションのパラメータを更新することをクライアントに許可しますが、ダイアログの状態に影響はありません。
ステータス	正規表現が応答内のステータス行と照合されます。
正規表現	パターン マッチングに使用する正規表現を定義する、正規表現オブジェクト。オブジェクトの名前を入力します。[選択（Select）] をクリックして既存のオブジェクトのリストからオブジェクトを選択するか、または新しい正規表現オブジェクトを作成できます。

SMTP クラス マップの [Add Match Criterion]/[Edit Match Criterion] ダイアログボックス

ゾーンベースのファイアウォール ポリシーで使用する SMTP クラスの [Add Match Criterion]/[Edit Match Criterion] ダイアログボックスを使用して、クラス マップの一致基準と値を定義します。

ヒント　12.4(20)T よりも前の Cisco IOS ソフトウェアを実行しているルータでは、[Data Length] 基準だけを使用できます。

このダイアログボックスのフィールドは、選択した基準によって変わります。次の基準を使用できます。

- [Data Length]：トラフィックのデータ長が指定した数値よりも大きいことを指定します。トラフィックのデータ長を照合して、SMTP 接続で転送されるデータが指定したバイト数を超えているかどうかを判断できます。デフォルトでは、インスペクションはデータ長を 20 未満に維持します。
- [Body Regular Expression]：正規表現を適用して、電子メール メッセージの本文のテキストおよび HTML のコンテンツ タイプおよびコンテンツ符号化タイプを照合します。7 ビットまたは 8 ビット符号化を使用するテキストまたは HTML だけがチェックされます。正規表現は、別の符号化タイプ（base64 や Zip ファイルなど）を使用するメッセージではスキャンできません。
- [Command Line Length]：指定した数値以下の ESMTP コマンドラインの長さを指定します。この基準を使用して、Denial of Service（DoS; サービス拒絶）攻撃を阻止します。
- [コマンドVerb（Command Verb）]：選択した SMTP または ESMTP コマンドに検査を制限します。SMTP の検査を設定すると、制限しない限り、すべてのコマンドが検査されます。
- [Header Length]：SMTP ヘッダーの長さが指定した数値よりも大きいことを指定します。この基準を使用して、ヘッダーの使用可能サイズを制限することで DoS 攻撃を阻止します。
- [Header Regular Expression]：正規表現を適用して、電子メール メッセージのヘッダーのコンテンツを照合します。たとえば、この基準を使用して件名、差出人、または宛先フィールドの特定のパターンをテストできます。
- [MIMEコンテンツタイプの正規表現（Mime Content-Type Regular Expression）]：正規表現を適用して、電子メール添付ファイルの Multipurpose Internet Message Exchange（MIME）コンテンツタイプと照合します。この基準を使用して、望ましくないタイプの添付ファイルの送信を防ぎます。
- [Mime Encoding]：検査する電子メール添付ファイルの MIME 符号化タイプを指定します。この基準を使用して、送信を制限する不明または非標準の符号化を識別します。
- [Recipient Address]：正規表現を適用して、SMTP RCPT コマンドの電子メール メッセージの受信者を照合します。この基準を使用して、存在しない受信者を検索します。これは、スパムの送信元の識別に役立つ場合があります。
- [Recipient Count]：電子メール メッセージの受信者数が指定した数を超えられないことを指定します。この基準を使用して、スパムの発信者が多数のユーザに電子メールを送信することを防ぎます。

- [無効な受信者数（Recipient Invalid Count）]：電子メールメッセージの無効な受信者の数が指定した数を超えられないことを指定します。これを使用して、スパマーが多数の一般的な名前に電子メールを送信し、実際のアドレスを狙っているのを防ぎます。SMTP は通常、アドレスが無効な場合に「no such address」メッセージを返信します。無効なアドレスの数を制限することで、これらのスパム発信者への応答を防ぐことができます。
- [Reply EHLO]：EHLO サーバ応答のサービス拡張パラメータを指定します。この基準を使用して、クライアントが特定のサービス拡張を使用することを防ぎます。
- [Sender Address]：正規表現を適用して、電子メール メッセージの送信者を照合します。この基準を使用して、既知のスパム発信者などの特定の送信者がデバイスを介して電子メール メッセージを送信することをブロックします。

ナビゲーション パス

SMTP クラスの [クラスマップの追加（Add Class Maps）]/[クラスマップの編集（Edit Class Maps）] ダイアログボックスで、テーブル内を右クリックして [行の追加（Add Row）] を選択するか、行を右クリックして [行の編集（Edit Row）] を選択します。ゾーンベースのファイアウォール ポリシーのクラス マップの設定 （23 ページ） を参照してください。

関連項目

- マップ オブジェクトについて
- ゾーンベースのファイアウォール ポリシーのインスペクション マップの設定 （19 ページ）
- ゾーンベースのファイアウォール ルールについて （3 ページ）

フィールド リファレンス

表 *7: SMTP* クラスの *[Add Match Criterion]/[Edit Match Criterion]* ダイアログボックス

要素	説明
基準	照合する SMTP トラフィック基準を指定します。基準については、上記で説明しています。
タイプ（Type）	基準に一致するトラフィックをマップに含めることを指定します。
可変フィールド 次のフィールドは、[Criterion] フィールドでの選択内容によって変わります。このリストは、表示されると想定されるフィールドのスーパーセットです。	
最大長	評価されるフィールドの最大長（バイト単位）。指定した数値よりも長さが大きい場合は、条件が一致します。

要素	説明
Greater Than Count	電子メール メッセージで許可される受信者または無効な受信者の最大数。指定した数値よりも数が大きい場合は、条件が一致します。
Verb Option User Defined Format （[Command Verb] 基準のみ）	検査する SMTP または ESMTP コマンド。[User Defined] を選択した場合は、電子メール メッセージの本文の単語に対応するテキスト文字列を入力する必要があります。単語には、スペースまたは特殊文字は使用できません。使用できるのは英数字だけです。
Service Extension Parameter User Defined Format （[EHLO応答（Reply EHLO）] 基準の場合）	検査する EHLO サーバ応答のサービス拡張パラメータ。よく知られたパラメータの 1 つを選択するか、[User Defined] を選択して [User Defined Format] フィールドでプライベート拡張を指定します。
Encoding Format User Defined Format	テストする MIME 符号化フォーマット。エンコーディングタイプは次のとおりです。 • [7-bit]：ASCII 符号化。 • [8-bit]：7 ビット ASCII の範囲外のオクテットを含む電子メール メッセージの交換に使用されます。 • [base64]：数値として扱い、base 64 表現に変換することでバイナリ データを符号化します。 • [quoted-printable]：印刷可能文字を使用して 8 ビット データを 7 ビット データ パス上に送信する符号化。 • [binary]：0 と 1 だけを使用した符号化。 • [unknown]：符号化タイプは不明です。 • [x-uuencode]：非標準の符号化。 • [user defined]：定義する符号化タイプ。[User Defined] を選択した場合は、探している符号化タイプを定義するテキスト文字列を入力する必要があります。
正規表現	パターン マッチングに使用する正規表現を定義する、正規表現オブジェクト。オブジェクトの名前を入力します。[選択（Select）] をクリックして既存のオブジェクトのリストからオブジェクトを選択するか、または新しい正規表現オブジェクトを作成できます。

Sun RPC クラス マップの [Add Match Criterion]/[Edit Match Criterion] ダイアログボックス

ゾーンベースのファイアウォールポリシーで使用するSunリモートプロシージャコール（RPC）クラスの [Add Match Criterion]/[Edit Match Criterion] ダイアログボックスを使用して、クラスマップの一致基準と値を定義します。照合する RPC プロトコル番号を入力できます。プロトコル番号の詳細については、Sun RPC のマニュアルを参照してください。

ナビゲーション パス

Sun RPC クラスの [クラスマップの追加（Add Class Maps）]/[クラスマップの編集（Edit Class Maps）] ダイアログボックスで、テーブル内を右クリックして [行の追加（Add Row）] を選択するか、行を右クリックして [行の編集（Edit Row）] を選択します。ゾーンベースのファイアウォール ポリシーのクラス マップの設定 （23 ページ） を参照してください。

関連項目

- マップ オブジェクトについて
- ゾーンベースのファイアウォール ポリシーのインスペクション マップの設定 （19 ページ）
- ゾーンベースのファイアウォール ルールについて （3 ページ）

ローカル Web フィルタ クラスの [Add Match Criterion]/[Edit Match Criterion] ダイアログボックス

ローカル Web フィルタ クラスの [Add Match Criterion]/[Edit Match Criterion] ダイアログボックスを使用して、クラス マップの一致基準と値を定義します。

ナビゲーション パス

ローカル Web フィルタクラスの [クラスマップの追加（Add Class Maps）]/[クラスマップの編集（Edit Class Maps）] ダイアログボックスで、テーブル内を右クリックして [行の追加（Add Row）] を選択するか、行を右クリックして [行の編集（Edit Row）] を選択します。ゾーンベースのファイアウォール ポリシーのクラス マップの設定 （23 ページ） を参照してください。

関連項目

- マップ オブジェクトについて
- ゾーンベースのファイアウォール ポリシーのコンテンツ フィルタリング マップの設定 （48 ページ）
- ゾーンベースのファイアウォール ルールについて （3 ページ）

フィールド リファレンス

表 8 : ローカル *Web* フィルタ クラスの *[Add Match Criterion]/[Edit Match Criterion]* ダイアログボックス

要素	説明
基準	照合するトラフィック基準を指定します。次の中から選択できます。 • [Server Domain]：サーバの名前に基づいてトラフィックを照合します。選択する URLF Glob パラメータ マップでは、*.cisco.com や www.cisco.com などのサーバ ドメイン名を指定する必要があります。 • [URL Keyword]：URL 内のキーワードに基づいてトラフィックを照合します。キーワードは、URL 内の / 文字の間に出現する完結した文字列です。たとえば、URL セグメント www.cisco.com/en/US では、en と US がキーワードの例です。
タイプ（Type）	基準に一致するトラフィックをマップに含めることを指定します。
URLF Globパラメータマップ（URLF Glob Parameter Map）	照合する URL パターンを定義する URLF Glob パラメータ マップ オブジェクト。選択したオブジェクトに、選択した照合タイプに適したコンテンツがあることを確認します。 オブジェクトの名前を入力します。[選択（Select）] をクリックして既存のオブジェクトのリストからオブジェクトを選択するか、または新しいオブジェクトを作成できます。

N2H2 および Websense クラスの [Add Match Criterion]/[Edit Match Criterion] ダイアログボックス

N2H2（SmartFilter）および Websense Web フィルタ クラスの [Add Match Criterion]/[Edit Match Criterion] ダイアログボックスを使用して、クラス マップの一致基準と値を定義します。使用可能な一致基準は、SmartFilter または Websense サーバからの応答の照合だけです。

ナビゲーション パス

N2H2 または Websense Web フィルタクラスの [クラスマップの追加（Add Class Maps）]/[クラスマップの編集（Edit Class Maps）] ダイアログボックスで、テーブル内を右クリックして [行の追加（Add Row）] を選択するか、行を右クリックして [行の編集（Edit Row）] を選択します。ゾーンベースのファイアウォール ポリシーのクラス マップの設定 （23 ページ） を参照してください。

関連項目

- マップ オブジェクトについて
- ゾーンベースのファイアウォール ポリシーのコンテンツ フィルタリング マップの設定（48 ページ）

- ゾーンベースのファイアウォール ルールについて （3 ページ）

インスペクション パラメータ マップの設定

[Add Inspect Parameter Map]/[Edit Inspect Parameter Map] ダイアログボックスを使用して、ルータのゾーンベースのファイアウォール ポリシーのインスペクション用のパラメータ マップを定義します。ゾーンベースのファイアウォール ポリシールールのアクションを [Inspect] または [Content Filter] に設定する場合は、インスペクション パラメータ マップを選択して、インスペクション アクションの接続、タイムアウト、およびその他の設定を定義できます。ゾーンベースのファイアウォールルールのインスペクション パラメータ マップを選択しない場合は、これらの設定にデフォルト値が使用されます。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、コンテンツテーブルから [マップ（Maps）] > [パラメータマップ（Parameter Maps）] > [検査（Inspect）] > [パラメータの検査（Inspect Parameters）] を選択します。作業領域内を右クリックして [新規オブジェクト（New Object）] を選択するか、行を右クリックして [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- マップ オブジェクトについて
- ゾーンベースのファイアウォール ポリシーのインスペクション マップの設定 （19 ページ）
- ゾーンベースのファイアウォール ポリシーのコンテンツ フィルタリング マップの設定 （48 ページ）
- ゾーンベースのファイアウォール ルールについて （3 ページ）

フィールド リファレンス

表 9 : [Add Inspect Parameter Map]/[Edit Inspect Parameter Map] ダイアログボックス

要素	説明
名前	ポリシー オブジェクトの名前。最大 40 文字を使用できます。
説明	ポリシー オブジェクトの説明。最大 200 文字を使用できます。
DNS Timeout	アクティビティがないときに DNS ルックアップ セッションが管理される時間の長さ（秒単位）。
ICMP Timeout	非アクティブな Internet Control Message Protocol（ICMP; インターネット制御メッセージプロトコル）セッションが維持される時間の長さ（秒単位）。

要素	説明
Max Incomplete Low Max Incomplete High	既存のハーフオープンセッションの数。これにより、ソフトウェアは、ハーフオープン状態のセッションの削除を開始（上限しきい値に達したとき）および停止（下限しきい値に達したとき）します。 [低（Low）]フィールドには、必ず[高（High）]フィールドに入力した数値よりも小さい数値を入力してください（たとえば、400 と 500 など）。デフォルトでは、ハーフオープン セッションは無制限です。
One Minute Low One Minute High	新しい未確立セッションの数。これにより、システムは、ハーフオープン状態のセッションの削除を開始および停止します。[Low]フィールドには、[High]フィールドに入力した数値よりも小さい数値を必ず入力してください。デフォルトは無制限です。
最大セッション数（Max Sessions）	ゾーン ペア上のインスペクション セッションの最大数（200 など）。デフォルトは無制限です。
TCP FINWAIT Timeout	ファイアウォールが FIN 交換を検出したあと、TCP セッション状態情報を保持する時間の長さ（秒単位）。TCP セッションを閉じる準備が整うと、FIN 交換が発生します。
TCP SYNWAIT Timeout	セッションをドロップする前に、TCP セッションが設定された状態に到達するのを待機する時間の長さ（秒単位）。
TCP Idle Timeout	セッションでアクティビティがない間、TCP セッションを維持する時間の長さ（秒単位）。

要素	説明
TCP Max Incomplete Hosts TCP Max Incomplete Block Time	TCP ホスト固有の Denial of Service（DoS; サービス拒絶攻撃）の検出と防止のしきい値とブロッキング時間（分単位）。 最大不完全ホストは、ソフトウェアがホストへのハーフオープン セッションの削除を開始する前に同時に存在できる、同じホスト宛先アドレスを持つハーフオープン TCP セッションの数です。同じ宛先ホストアドレスを持つハーフオープン セッションの数が異常に多い場合は、ホストに対して DoS 攻撃が起動されていることを示している可能性があります。 しきい値を超えた場合、ハーフオープン セッションは、最大不完全ブロック時間に基づいてドロップされます。 • ブロック時間が 0 の場合、ソフトウェアは、ホストへの新規接続要求のたびに、ホストの最も古い既存のハーフオープン セッションを削除します。これにより、ホストに対するハーフオープン セッション数がしきい値を超えないことが保証されます。 • ブロック時間が 0 よりも大きい場合、ソフトウェアはホストのすべての既存のハーフオープン セッションを削除し、ホストに対するすべての新規接続要求をブロックします。ソフトウェアは、ブロック時間が経過するまですべての新規接続要求のブロックを継続します。 ソフトウェアは、指定されたしきい値を超えるたびに、またホストへの接続開始のブロッキングが開始または終了したときに、syslog メッセージを送信します。
UDP Idle Timeout	セッションでアクティビティがない間、UDP セッションを維持する時間の長さ（秒単位）。 ソフトウェアは、有効な UDP パケットを検出すると、新しい UDP セッションの状態情報を確立します。UDP はコネクションレス型サービスであるため、実際のセッションは存在しません。したがって、ソフトウェアは、パケット内の情報を調べることでセッションを見積もり、そのパケットが他の UDP パケットと似ているかどうか（類似の送信元アドレスまたは宛先アドレスを持っているなど）、および別の類似 UDP パケットの直後にそのパケットが検出されたかどうかを判断します。 ソフトウェアが、UDP アイドル タイムアウトで定義されている期間中に UDP セッションの UDP パケットを検出しなかった場合、ソフトウェアは、そのセッションの状態情報の管理を継続しません。
Enable Alert	ステートフル パケット インスペクションのアラート メッセージをコンソールで生成するかどうか。
Enable Audit Trail	監査証跡メッセージを syslog サーバまたはルータに記録するかどうか。

要素	説明
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用を参照してください。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可および個々のデバイスのポリシー オブジェクト オーバーライドについてを参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

プロトコル情報パラメータ マップの設定

[Add Protocol Info Parameter Map]/[Edit Protocol Info Parameter Map] ダイアログボックスを使用して、ルータ上のゾーンベースのファイアウォール ポリシーの Instant Messaging（IM; インスタント メッセージング）アプリケーションまたは Stun-ice プロトコルのインスペクション用のパラメータ マップを定義します。ゾーンベースのファイアウォール ポリシー ルールのアクションを [Inspect] に設定した場合は、AOL、ICQ、MSN Messenger、Windows Messenger、Yahoo Messenger、Stun-ice のいずれかのアプリケーションを設定するときにプロトコル情報パラメータ マップを選択する必要があります。プロトコル情報パラメータ マップでは、これらのアプリケーションと対話する DNS サーバを定義します。これにより、インスタント メッセンジャ アプリケーション エンジンは、インスタント メッセンジャ トラフィックを認識し、そのインスタント メッセンジャ アプリケーションに対して設定済みポリシーを適用できます。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、目次から **[マップ（Maps）] > [パラメータマップ（Parameter Maps）] > [検査（Inspect）] > [プロトコル情報パラメータ（Protocol Info Parameters）]** を選択します。作業領域内を右クリックして [新規オブジェクト（New Object）] を選択するか、行を右クリックして [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- マップ オブジェクトについて
- ゾーンベースのファイアウォール ポリシーのインスペクション マップの設定 （19 ページ）
- ゾーンベースのファイアウォール ルールについて （3 ページ）

フィールド リファレンス

表 10 : [Add Protocol Info Parameter Map]/[Edit Protocol Info Parameter Map] ダイアログボックス

要素	説明
名前	ポリシー オブジェクトの名前。最大 40 文字を使用できます。
説明	ポリシー オブジェクトの説明。最大 200 文字を使用できます。
DNS Server Table	トラフィックが許可（および検査）または拒否される DNS サーバ。 • サーバを追加するには、[Add] ボタンをクリックし、[Add Server] ダイアログボックスに入力します（プロトコル情報パラメータの [Add DNS Server]/[Edit DNS Server] ダイアログボックス （44 ページ）を参照）。 • サーバを編集するには、サーバを選択し、[Edit] ボタンをクリックします。 • サーバを削除するには、サーバを選択し、[Delete]ボタンをクリックします。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用を参照してください。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可および個々のデバイスのポリシー オブジェクト オーバーライドについてを参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

プロトコル情報パラメータの [Add DNS Server]/[Edit DNS Server] ダイアログボックス

[Add DNS Server]/[Edit DNS Server] ダイアログボックスを使用して、トラフィックが許可（および検査）または拒否される DNS サーバを識別します。これらのサーバは、ゾーンベースのファイアウォール ポリシーでこれらのサーバを必要とするプロトコルのインスペクションに使用するプロトコル情報パラメータ マップで定義されます。

次のいずれかのタイプを使用して、サーバを識別できます。

- [Server Name]：DNS サーバの名前。アスタリスク（*）をワイルドカードとして使用して、1 文字以上を照合できます。たとえば、cisco.com ドメイン上のすべての DNS サーバを識別する場合は、*.cisco.com を指定できます。

- [IP Address]：単一の DNS サーバの IP アドレス。
- [IPアドレス範囲（IP Address Range）]：開始アドレスと終了アドレスの間にある DNS サーバーを識別する IP アドレスの範囲。

ナビゲーション パス

[プロトコル情報パラメータマップの追加（Add Protocol Info Parameter Map）]/[プロトコル情報パラメータマップの編集（Edit Protocol Info Parameter Map）] ダイアログボックスで、サーバーテーブルの下にある [追加（Add）] ボタンをクリックするか、サーバーを選択して [編集（Edit）] ボタンをクリックします。プロトコル情報パラメータ マップの設定 （43 ページ） を参照してください。

ゾーンベースのファイアウォール ポリシーのポリシー マップの設定

ゾーンベースのファイアウォール ポリシーの [Add Policy Map]/[Edit Policy Map] ダイアログボックスを使用して、Cisco IOS ルータのゾーンベースのファイアウォール ポリシーで使用するインスペクション マップの一致基準と値を定義します。H.323（IOS）、HTTP（ゾーン ベース IOS）、IM（ゾーン ベース IOS）、IMAP、P2P、POP3、SIP（IOS）、SMTP、および Sun RPC インスペクションのポリシー インスペクション マップを作成できます。ダイアログボックスの名前は、作成しているマップのタイプを示します。

インスペクション マップを定義するときに、同じタイプのクラス マップを選択し、一致するトラフィックに対して実行するアクションを定義します。ポリシーマップを作成する前、またはポリシー マップの作成時に、必要なクラス マップを設定できます。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、コンテンツテーブルの **[マップ（Maps）] > [ポリシーマップ（Policy Maps）] > [検査（Inspect）]** フォルダで、[H.323 (IOS)]、[HTTP (Zone based IOS)]、[IM (Zone based IOS)]、[IMAP]、[P2P]、[POP3]、[SIP (IOS)]、[SMTP]、[Sun RPC] のいずれかの項目を選択します。作業領域内を右クリックして [新規オブジェクト（New Object）] を選択するか、行を右クリックして [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- マップ オブジェクトについて
- ゾーンベースのファイアウォール ルールについて （3 ページ）
- ゾーンベースのファイアウォール ポリシーのインスペクション マップの設定 （19 ページ）
- ゾーンベースのファイアウォール ポリシーのコンテンツ フィルタリング マップの設定 （48 ページ）

フィールド リファレンス

表 *11* : ゾーンベースのファイアウォール ポリシーの *[Add Policy Maps]/[Edit Policy Maps]* ダイアログボックス

要素	説明
名前	ポリシー オブジェクトの名前。最大 40 文字を使用できます。
説明	ポリシー オブジェクトの説明。最大 200 文字を使用できます。
[Match All] テーブル	[Match All] テーブルには、ポリシー マップに含まれているクラス マップ、およびこのクラスに一致するトラフィックに適用するアクションが表示されます。トラフィックがこのクラスと照合される場合、選択したクラスマップで定義されているすべての基準を満たす必要があります。 • 基準を追加するには、[Add] ボタンをクリックし、[Match Condition and Action] ダイアログボックスに入力します（ゾーンベースのファイアウォール ポリシーおよび Web フィルタ ポリシーの [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス （46 ページ）を参照）。 • 基準を編集するには、基準を選択し、[Edit] ボタンをクリックします。 • 基準を削除するには、基準を選択し、[Delete] ボタンをクリックします。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用を参照してください。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可および個々のデバイスのポリシー オブジェクト オーバーライドについてを参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

ゾーンベースのファイアウォール ポリシーおよび Web フィルタ ポリシーの [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス

ゾーンベースのファイアウォール ポリシーおよび Web フィルタ ポリシーの [Add Match Condition and Action]、[Edit Match Condition and Action] ダイアログボックスを使用して、インスペクションのクラスマップを選択し、クラスに一致するトラフィックに対して実行するアクションを定義します。このダイアログボックスは、H.323（IOS）、HTTP（ゾーンベース IOS）、IM（ゾー

ン ベース IOS）、IMAP、P2P、POP3、SIP（IOS）、SMTP、Sun RPC、Web フィルタのタイプのポリシー マップに使用されます。

このダイアログボックスのフィールドは、定義しているポリシーマップのタイプによって若干異なります。

ナビゲーション パス

ゾーンベースのファイアウォールポリシーの [ポリシーマップの追加（Add Policy Maps）]/[ポリシーマップの編集（Edit Policy Maps）] ダイアログボックスで、一致テーブル内を右クリックして [行の追加（Add Row）] を選択するか、行を右クリックして [行の編集（Edit Row）] を選択します。ゾーンベースのファイアウォール ポリシーのポリシー マップの設定 （45 ページ） を参照してください。

関連項目

- マップ オブジェクトについて
- ゾーンベースのファイアウォール ポリシーのインスペクション マップの設定 （19 ページ）
- ゾーンベースのファイアウォール ポリシーのコンテンツ フィルタリング マップの設定 （48 ページ）
- ゾーンベースのファイアウォール ルールについて （3 ページ）

フィールド リファレンス

表 *12* : ゾーンベースのファイアウォール ポリシーの *[Add Match Condition and Action]*、*[Edit Match Condition and Action]* ダイアログボックス

要素	説明
一致タイプ（Match Type）	クラスマップを選択していることを指定します。ゾーンベースのファイアウォール ポリシーのポリシー マップを作成する場合は、クラスマップを定義する必要があります。
クラスマップ P2P、IM、および Web フィルタ クラスマップ タイプ	作成しているポリシーマップ タイプのクラスマップの名前です。[選択（Select）] をクリックしてリストからマップを選択するか、新しいクラスマップオブジェクトを作成します。 P2P、IM、および Web フィルタ ポリシー マップの場合は、作成しているポリシーマップのタイプも選択する必要があります。たとえば、P2P マップでは、[eDonkey]、[FastTrack]、[Gnutella]、[Kazaa2] から選択する必要があります。IM（ゾーン ベース IOS）マップでは、[AOL]、[MSN Messenger]、[Yahoo Messenger]、[Windows Messenger]、[ICQ] から選択する必要があります。Web フィルタ マップでは、[Local]、[N2H2]、[WebSense]、[Trend] から選択する必要があります。

要素	説明
操作	選択したクラスに一致するトラフィックに対してデバイスが適用するアクション。

ゾーンベースのファイアウォールポリシーのコンテンツフィルタリング マップの設定

ルータのゾーンベースのファイアウォールポリシーを設定する場合は、ルールのアクションとして [Content Filter] を選択することで、Web コンテンツをフィルタリングするルールを定義できます。

Web コンテンツをフィルタリングするには、特定のマップオブジェクトを設定する必要があります。マップオブジェクトは、ルールを定義しているときに [ポリシーオブジェクトセレクタ（policy object selector）] ダイアログボックスから設定するか、[Policy Object Manager] ウィンドウ（[管理（Manage）]> [ポリシーオブジェクト（Policy Objects）] を選択） でいつでも設定できます。

必要なマップのタイプは、コンテンツのフィルタリングに使用している手法と、使用している Cisco IOS ソフトウェア バージョンによって異なります。デバイスにローカルに定義されている URL リストに基づいてコンテンツをフィルタリングするか、SmartFilter（N2H2）、Websense、Trend Micro などの外部フィルタリング サーバを使用できます。

ヒント　外部サーバを使用する場合は、選択したサーバ タイプ用のマニュアルに基づいて、サーバを適切に設定する必要があります。Trend Micro サーバを使用する場合は、[Zone Based Firewall] ページ（[Firewall] > [Settings] > [Zone Based Firewall] を選択）の [Content Filtering] タブで、サーバの詳細を指定し、製品を登録して証明書をダウンロードする必要があります。[Zone-based Firewall Rules] ページ （78 ページ）を参照してください。

次に、ゾーンベースのコンテンツ フィルタリングに使用されるマップ オブジェクトの要件を示します。

- 12.4(20)T よりも前のリリースを実行しているデバイスでは、URL フィルタ パラメータ マップを作成する必要があります。[Policy Object Manager] で、[マップ（Maps）] > [パラメータマップ（Parameter Maps）] > [ウェブフィルタ（Web Filter）] > [URLフィルタ（URL Filter）] を選択し、URL フィルタ パラメータ マップの設定 （57 ページ）の詳細な使用状況情報を確認します。
  - 許可されるホストのリスト（許可リストの一部）および拒否されるホストのリスト（ブロックリストの一部）を使用して、ルータでローカルフィルタリングを実行するには、[ローカルフィルタリング（Local Filtering）] タブでリストを作成します。最初に Web アクセス要求がこれらのリストと比較されてから、要求が外部フィルタリング サーバに送信されます（外部フィルタリング サーバを設定している場合）。これらのリストには、完全なドメイン名（www.cisco.com など）、または部分的な名前

（cisco.comなど）が含まれますが、パスやページ名は含まれず、ワイルドカードは使用できません。

- SmartFilter（N2H2）または Websense サーバを使用するには、使用しているサーバのタイプとそのアドレス情報を [External Filter] タブで設定します。サーバとの通信を制御するその他の設定も設定できます。URL フィルタ パラメータ マップを使用して Trend Micro サーバを設定することはできません。

- リリース 12.4(20)T 以降を実行しているデバイスでは、Web フィルタポリシーマップを使用するアプローチが推奨されます。Web フィルタ ポリシー マップはより複雑ですが、柔軟性が向上し、Trend Micro フィルタリング サーバにアクセスできます。[Policy Object Manager] で、[マップ（Maps）]>[ポリシーマップ（Policy Maps）]>[ウェブフィルタ（Web Filter）]>[ウェブフィルタ（Web Filter）] を選択し、Web フィルタ マップの設定 （64 ページ）の詳細な使用状況情報を確認します。

Web フィルタ ポリシー マップには、他のタイプのマップが組み込まれます。ポリシー マップを作成するには、次のマップ タイプの 1 つ以上が必要です。

- - パラメータ マップ：デフォルト設定を使用しない場合は、[Add Web Filter Map]/[Edit Web Filter Map] ダイアログボックスの [Parameters] タブで、さまざまなタイプの Web フィルタリングのパラメータ マップを選択できます。SmartFilter（N2H2）または Websense を使用している場合は、パラメータ マップがこれらのサーバを識別するため、マップを選択する必要があります。ローカル フィルタリングおよび Trend Micro フィルタリングでは、パラメータマップでいくつかの一般設定を設定します。その中で最も重要な設定は、URL がブロックされるときにメッセージまたは Web ページを表示するかどうかです。[Policy Object Manager] の [マップ（Maps）]>[パラメータマップ（Parameter Maps）]>[ウェブフィルタ（Web Filter）] フォルダで、ローカル、N2H2、Trend、および Websense のパラメータマップを検索できます。詳細な使用方法については、ローカル Web フィルタ パラメータ マップの設定 （51 ページ）、N2H2 または WebSense パラメータ マップの設定 （52 ページ）、またはTrend パラメータ マップの設定 （56 ページ）を参照してください。

（注） Trend Micro サーバ情報は、[Zone Based Firewall] ページ（[Firewall]>[Settings]>[Zone Based Firewall] を選択）の [Content Filtering] タブで設定します。[Zone-based Firewall Rules] ページ （78 ページ）を参照してください。

- - 一致条件のクラスマップ：これらのクラスマップでは、ターゲットとするトラフィックのタイプを定義し、実行するアクションを指定します。フィルタリングのタイプ（[Local]、[SmartFilter/N2H2]、[Websense]、または [Trend Micro]）を選択し、ターゲットのトラフィックを識別するクラスマップを指定し、そのトラフィックに対して実行するアクション（[Allow]、[Reset] など）を選択します。[Policy Object Manager] の [マップ（Maps）]>[クラスマップ（Class Maps）]>[ウェブフィルタ（Web Filter）] フォルダで、ローカル、N2H2、Trend、および Websense のクラスマップを検索できます。

これらのクラスマップ設定は、フィルタリングのタイプによって異なります。

[Local Filtering]：Local WebFilter クラスマップは、ターゲットにするドメイン名または URL キーワードを指定する 1 つ以上の URLF Glob パラメータのリストです。URL キーワードは、URL 内のスラッシュ（/）文字で囲まれた任意のテキスト文字列です。これらのクラスマップは、Web フィルタポリシーで許可する URL リスト（許可リストの一部）と拒否する URL リスト（ブロックリストの一部）を定義するのに役立ちます。リストごとに別々のマップを作成します。詳細な使用方法については、ゾーンベースのファイアウォール ポリシーのクラス マップの設定 （23 ページ）、ローカル Web フィルタ クラスの [Add Match Criterion]/[Edit Match Criterion] ダイアログボックス （38 ページ）、および URLF Glob パラメータ マップの設定 （61 ページ）を参照してください。

[SmartFilter (N2H2)] または [Websense Filtering]：N2H2 および Websense のクラスマップでは、任意のサーバー応答を一致基準として定義します。詳細な使用方法については、ゾーンベースのファイアウォール ポリシーのクラス マップの設定 （23 ページ）を参照してください。

[Trend Micro Filtering]：Trend クラスマップでは、Trend Micro によって定義されている、ターゲットにするさまざまなプロダクティビティカテゴリおよびセキュリティレーティングを選択できます。詳細な使用方法については、ゾーンベースのファイアウォール ポリシーのクラス マップの設定 （23 ページ）を参照してください。

コンテンツ フィルタリングの定義に使用されるマップ以外に、コンテンツ フィルタ ルールの次のマップも設定できます。

- インスペクション パラメータ マップ：ゾーンベースのファイアウォール インスペクションには、いくつかの一般設定が含まれ、そのすべてに、ほとんどのネットワークに適切なデフォルト値があります。これらの設定のいずれかを調整する場合は、インスペクション パラメータ マップを作成できます。[Policy Object Manager] で、[マップ（Maps）] > [パラメータマップ（Parameter Maps）] > [検査（Inspect）] > [検査パラメータ（Inspect Parameters）] を選択し、インスペクション パラメータ マップの設定 （40 ページ）の詳細な使用状況情報を確認します。
- HTTP ポリシーマップ：Web フィルタリングに加えて個々の HTTP パケットに詳細インスペクションを使用する場合は、ゾーンベースのファイアウォール ルールの追加と編集 （82 ページ）の [アクション（Action）] セクションの [プロトコル（Protocol）] フィールドの横にある [設定（Configure）] をクリックして、HTTP ポリシーマップを設定できます。HTTP ポリシーマップには、照合するトラフィックのタイプを定義し、実行するアクションを定義する HTTP クラスマップが組み込まれます。たとえば、Java アプレットを含むトラフィックをターゲットにできます。[Policy Object Manager] で、[マップ（Maps）] > [ポリシーマップ（Policy Maps）] > [検査（Inspect））] > [HTTP（ゾーンベースのIOS）（HTTP (Zone Based IOS)）] を選択し、ゾーンベースのファイアウォール ポリシーのポリシーマップの設定 （45 ページ）、HTTP（IOS）クラスの [Add Match Criterion]/[Edit Match Criterion] ダイアログボックス （28 ページ）、および ゾーンベースのファイアウォール ポリシーのクラス マップの設定 （23 ページ）の詳細な使用状況情報を確認します。

関連項目

- ゾーンベースのファイアウォール ルールについて （3 ページ）

- [Zone-based Firewall Rules] ページ （78 ページ）
- ポリシー オブジェクトの作成
- マップ オブジェクトについて

ローカル Web フィルタ パラメータ マップの設定

[Add Local Parameter Map]/[Edit Local Parameter Map] ダイアログボックスを使用して、ルータのゾーンベースのファイアウォール ポリシーのローカル Web フィルタリング用のパラメータ マップを定義します。ゾーンベースのファイアウォール ポリシー ルールのアクションを [Content Filter] に設定する場合は、（[Parameter] タブでパラメータ タイプに [Local] を選択するときに）ローカル Web フィルタ パラメータ マップを組み込む Web フィルタ ポリシー マップを選択できます。Web フィルタ ポリシー マップの詳細については、Web フィルタ マップの設定 （64 ページ）を参照してください。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、次にコンテンツテーブルから **[マップ（Maps）] > [パラメータマップ（Parameter Maps）] > [Webフィルタ（Web Filter）] > [ローカル（Local）]** を選択します。作業領域内を右クリックして [新規オブジェクト（New Object）] を選択するか、行を右クリックして [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- マップ オブジェクトについて
- ゾーンベースのファイアウォール ポリシーのコンテンツ フィルタリング マップの設定 （48 ページ）
- ゾーンベースのファイアウォール ルールについて （3 ページ）

フィールド リファレンス

表 13 : [Add Local Web Filter Parameter Map]/[Edit Local Web Filter Parameter Map] ダイアログボックス

要素	説明
名前	ポリシー オブジェクトの名前。最大 40 文字を使用できます。
説明	ポリシー オブジェクトの説明。最大 200 文字を使用できます。
Enable Alert	ステートフル パケット インスペクションのアラート メッセージをコンソールで生成するかどうか。

要素	説明
Enable Allow Mode	URL フィルタリング プロセスが URL フィルタリング データベースに接続していない場合に、URL 要求を許可するかまたはブロックするか。許可モードがオンの場合、一致しないすべての URL 要求が許可され、オフの場合は、一致しないすべての URL 要求がブロックされます。
Block Page	ブロックしているページにユーザがアクセスしようとした場合に、ユーザに表示する Web ページ。次の中から選択できます。 • [None]：ユーザには何の情報も示されません。 • [Message]：編集ボックスに入力したテキスト メッセージがユーザに表示されます。 • [リダイレクトURL（Redirect URL）]：編集ボックスに入力した URL にユーザーがリダイレクトされます。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用を参照してください。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）]ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可および個々のデバイスのポリシー オブジェクト オーバーライドについてを参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）]ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

N2H2 または WebSense パラメータ マップの設定

[Add N2H2 Parameter Map]/[Edit N2H2 Parameter Map] または [Add Websense Parameter Map]/[Edit Websense Parameter Map] ダイアログボックスを使用して、ルータのゾーンベースのファイアウォール ポリシーの Smartfilter（N2H2）または Websense Web フィルタリング用のパラメータ マップを定義します。ゾーンベースのファイアウォール ポリシー ルールのアクションを [Content Filter] に設定する場合は、（[Parameter] タブでパラメータ タイプに [N2H2] または [Websense] を選択するときに）N2H2 または Websense Web フィルタ パラメータ マップを組み込む Web フィルタ ポリシー マップを選択できます。Web フィルタ ポリシー マップの詳細については、Web フィルタ マップの設定 （64 ページ）を参照してください。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、次にコンテンツテーブルの [マップ（Maps）] > [パラメータマップ（Parameter Maps）] > [Webフィルタ（Web Filter）] フォルダから [N2H2] または [WebSense] を選択します。作業領域内を右クリックして [新規オブジェクト（New Object）] を選択するか、行を右クリックして [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- マップ オブジェクトについて
- ゾーンベースのファイアウォール ポリシーのコンテンツ フィルタリング マップの設定（48 ページ）
- ゾーンベースのファイアウォール ルールについて （3 ページ）

フィールド リファレンス

表 14 : [Add N2H2 Parameter Map]/[Edit N2H2 Parameter Map] または [Add Websense Parameter Map]/[Edit Websense Parameter Map] ダイアログボックス

要素	説明
名前	ポリシー オブジェクトの名前。最大 40 文字を使用できます。
説明	ポリシー オブジェクトの説明。最大 200 文字を使用できます。
URL Filtering Server Table	URL フィルタリング サーバのリストとそれらの属性。 • サーバを追加するには、[Add] ボタンをクリックし、[Add External Filter] ダイアログボックスに入力します（[Add External Filter]/[Edit External Filter] ダイアログボックス （55 ページ）を参照）。 • サーバを編集するには、サーバを選択し、[Edit] ボタンをクリックします。 • サーバを削除するには、サーバを選択し、[Delete] ボタンをクリックします。
Enable Alert	ステートフル パケット インスペクションのアラート メッセージをコンソールで生成するかどうか。
Enable Allow Mode	URL フィルタリング プロセスが URL フィルタリング データベースに接続していない場合に、URL 要求を許可するかまたはブロックするか。許可モードがオンの場合、一致しないすべての URL 要求が許可され、オフの場合は、一致しないすべての URL 要求がブロックされます。

要素	説明
Block Page	ブロックしているページにユーザがアクセスしようとした場合に、ユーザに表示する Web ページ。次の中から選択できます。 • [None]：ユーザには何の情報も示されません。 • [Message]：編集ボックスに入力したテキスト メッセージがユーザに表示されます。 • [リダイレクトURL（Redirect URL）]：編集ボックスに入力した URL にユーザーがリダイレクトされます。
送信元インターフェイス（Source Interface）	TCP 接続がシステムと URL フィルタリング サーバ間で確立された場合に、送信元 IP アドレスとして使用される IP アドレスのインターフェイス。
Maximum Cache Entries	分類キャッシュに格納されるエントリの最大数。デフォルトは 5000 です。
Cache Life Time	エントリがキャッシュ テーブルに残る時間の長さ（時間数）。デフォルトは 24 です。
Maximum Requests	保留中の要求の最大数。範囲は、1 ～ 2147483647 です。デフォルトは 1000 です。
Maximum Responses	バッファできる HTTP 要求の最大数。範囲は、0 ～ 20000 です。デフォルトは 200 です。
Truncate Hostname Truncate Script Parameters	URL を切り捨てるかどうかを次のように指定します。： • オプションを選択しない場合、URL は切り捨てられません。 • ホスト名を選択した場合、URL はドメイン名の末尾で切り捨てられます。 • スクリプト パラメータを選択した場合、URL は、URL 内の左端の疑問符で切り捨てられます。 **ヒント** 両方のオプションを選択できますが、そのような指定方法は論理的ではありません。
Enable Server Log	HTTP 要求に関する情報を URL フィルタリングサーバーのログサーバーに送信するかどうか。この情報には、URL、ホスト名、送信元 IP アドレス、および宛先 IP アドレスが含まれます。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用F を参照してください。

要素	説明
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可および個々のデバイスのポリシー オブジェクト オーバーライドについてを参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトをオーバーライドするデバイスの数が表示されます。

[Add External Filter]/[Edit External Filter] ダイアログボックス

[Add External Filter]/[Edit External Filter] ダイアログボックスを使用して、URL フィルタリング サーバを N2H2、Websense、または URL フィルタ パラメータ マップ ポリシー オブジェクトに追加します。

ナビゲーション パス

次のいずれかのダイアログボックスで、サーバーテーブルの下の [追加（Add）] ボタンをクリックするか、サーバーを選択して [編集（Edit）] ボタンをクリックします。

- [Add N2H2 Parameter Map]/[Edit N2H2 Parameter Map] または [Add Websense Parameter Map]/[Edit Websense Parameter Map] ダイアログボックス N2H2 または WebSense パラメータ マップの設定 （52 ページ）を参照してください。
- [Add URL Filter Parameter Map]/[Edit URL Filter Parameter Map] ダイアログボックス URL フィルタ パラメータ マップの設定 （57 ページ）を参照してください。

フィールド リファレンス

表 15 : [Add External Filter]/[Edit External Filter] ダイアログボックス

要素	説明
サーバ	URL フィルタリング サーバの完全修飾ドメイン名または IP アドレス。
[ポート（Port）]	要求をリスニングするポート。
Retransmission Count	サーバからの応答がないときに、ルータがルックアップ要求を再送信する回数。値の範囲は 1 ～ 10 です。
タイムアウト（Timeout）	サーバからの応答をルータが待機する秒数。範囲は、1 ～ 300 です。
外部	サーバがネットワークの外部にあるかどうか。

Trend パラメータ マップの設定

[Add Trend Parameter Map]/[Edit Trend Parameter Map] ダイアログボックスを使用して、ルータのゾーンベースのファイアウォール ポリシーの Trend Micro Web フィルタリング用のパラメータ マップを定義します。ゾーン ベースのファイアウォール ポリシールールのアクションを [Content Filter] に設定する場合は、（[Parameter] タブでパラメータ タイプに [Trend] を選択するときに）Trend Web フィルタ パラメータ マップを組み込む Web フィルタ ポリシー マップを選択できます。Web フィルタ ポリシー マップの詳細については、Web フィルタ マップの設定（64 ページ）を参照してください。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、次にコンテンツテーブルから **[マップ（Maps）] > [パラメータマップ（Parameter Maps）] > [Webフィルタ（Web Filter）] > [傾向（Trend）]** を選択します。作業領域内を右クリックして [新規オブジェクト（New Object）] を選択するか、行を右クリックして [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- マップ オブジェクトについて
- ゾーンベースのファイアウォール ポリシーのコンテンツ フィルタリング マップの設定（48 ページ）
- ゾーンベースのファイアウォール ルールについて （3 ページ）

フィールド リファレンス

表 16 : [Add Trend Parameter Map]/[Edit Trend Parameter Map] ダイアログボックス

要素	説明
名前	ポリシー オブジェクトの名前。最大 40 文字を使用できます。
説明	ポリシー オブジェクトの説明。最大 200 文字を使用できます。
Enable Allow Mode	URL フィルタリング プロセスが URL フィルタリング データベースに接続していない場合に、URL 要求を許可するかまたはブロックするか。許可モードがオンの場合、一致しないすべての URL 要求が許可され、オフの場合は、一致しないすべての URL 要求がブロックされます。

要素	説明
Block Page	ブロックしているページにユーザがアクセスしようとした場合に、ユーザに表示する Web ページ。次の中から選択できます。 • [None]：ユーザには何の情報も示されません。 • [Message]：編集ボックスに入力したテキスト メッセージがユーザに表示されます。 • [リダイレクトURL（Redirect URL）]：編集ボックスに入力した URL にユーザーがリダイレクトされます。
Maximum Requests	保留中の要求の最大数。範囲は、1 ～ 2147483647 です。デフォルトは 1000 です。
Maximum Responses	バッファできる HTTP 要求の最大数。範囲は、0 ～ 20000 です。デフォルトは 200 です。
Truncate Hostname	ドメイン名の末尾で URL を切り捨てるかどうか。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用を参照してください。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可および個々のデバイスのポリシー オブジェクト オーバーライドについてを参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

URL フィルタ パラメータ マップの設定

[Add URL Filter Parameter Map]/[Edit URL Filter Parameter Map] ダイアログボックスを使用して、ルータのゾーンベースのファイアウォール ポリシーで使用するインスペクション マップのパラメータ、および一致基準と値を定義します。

ゾーンベースのファイアウォール ポリシールールのアクションを [Content Filter] に設定する場合は、URL フィルタ パラメータ マップを選択して、Web フィルタリング パラメータと一致基準を定義できます。ただし、ルータが Cisco IOS Software Release 12.4(20)T 以降を実行している場合、適切なサーバータイプ（ローカル、N2H2、Trend、または Websense）のパラメータおよびクラスマップとともに Web フィルタポリシーマップを設定することを推奨します。詳細については、Web フィルタ マップの設定 （64 ページ）を参照してください。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、次に目次から [マップ（Maps）] > [パラメータマップ（Parameter Maps）] > [Web フィルタ（Web Filter）] > [URL フィルタ（URL Filter）] を選択します。作業領域内を右クリックして [新規オブジェクト（New Object）] を選択するか、行を右クリックして [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- マップ オブジェクトについて
- ゾーンベースのファイアウォール ポリシーのコンテンツ フィルタリング マップの設定（48 ページ）
- ゾーンベースのファイアウォール ルールについて （3 ページ）

フィールド リファレンス

表 *17 : [Add URL Filter Parameter Map]/[Edit URL Filter Parameter Map]* ダイアログボックス

要素	説明
名前	ポリシー オブジェクトの名前。最大 40 文字を使用できます。
説明	ポリシー オブジェクトの説明。最大 200 文字を使用できます。
[Local Filtering] タブ このタブのフィールドでは、ローカル URL フィルタリングのプロパティを定義します。	

要素	説明
[許可リスト登録ドメイン（Permitlisted Domains）] テーブルと [ブロックリスト登録ドメイン（Blocklisted Domains）] テーブル	これらのテーブルでは、ソフトウェアが外部 URL フィルタリング サーバにアクセスしないドメイン名を定義します。許可リストにあるドメイン名は常に許可されます。ブロックリストにあるドメイン名は常にブロックされます。これらのリストを使用して、制限なしで許可する（自社の Web サイトなど）または完全にブロックする（ポルノサイトなど）ドメイン全体を識別します。 ドメイン名は完全な形式（www.cisco.com など、ホスト名を含む）にしたり、部分的な形式（cisco.com など）にしたりできます。部分的な名前の場合、そのドメイン上のすべての Web サイト ホストが、許可されるか、または拒否されます。また、ホストの IP アドレスを入力することもできます。 • ドメイン名を追加するには、[Add] ボタンをクリックし、[Add Server] ダイアログボックスに入力します（URL フィルタ パラメータの [Add URL Domain Name]/[Edit URL Domain Name] ダイアログボックス （61 ページ）を参照）。 • ドメイン名を編集するには、ドメインを選択し、[Edit] ボタンをクリックします。 • ドメイン名を削除するには、ドメインを選択し、[Delete] ボタンをクリックします。
Enable Alert	ステートフル パケット インスペクションのアラート メッセージをコンソールで生成するかどうか。
Enable Audit Trail	URL 情報を syslog サーバまたはルータのログに記録するかどうか。
Enable Allow Mode	URL フィルタリング プロセスが URL フィルタリング データベースに接続していない場合に、URL 要求を許可するかまたはブロックするか。許可モードがオンの場合、一致しないすべての URL 要求が許可され、オフの場合は、一致しないすべての URL 要求がブロックされます。
[External Filtering] タブ このタブのフィールドでは、外部 URL フィルタリング サーバのプロパティを定義します。	

要素	説明
サーバー タイプ Server Table	設定している外部URL フィルタリング サーバのタイプ（[SmartFilter (N2H2)] または [Websense]）。 • サーバを追加するには、[Add] ボタンをクリックし、[Add External Filter] ダイアログボックスに入力します（[Add External Filter]/[Edit External Filter] ダイアログボックス （55 ページ）を参照）。 • サーバを編集するには、サーバを選択し、[Edit] ボタンをクリックします。 • サーバを削除するには、サーバを選択し、[Delete] ボタンをクリックします。
送信元インターフェイス（Source Interface）	TCP 接続がシステムと URL フィルタリング サーバ間で確立された場合に、送信元 IP アドレスとして使用される IP アドレスのインターフェイス。
Maximum Cache Entries	分類キャッシュに格納されるエントリの最大数。デフォルトは5000です。
Maximum Requests	保留中の要求の最大数。範囲は、1 ～ 2147483647 です。デフォルトは 1000 です。
Maximum Responses	バッファできる HTTP 要求の最大数。範囲は、0 ～ 20000 です。デフォルトは 200 です。
Truncate Hostname Truncate Script Parameters	URL を切り捨てるかどうかを次のように指定します。: • オプションを選択しない場合、URL は切り捨てられません。 • ホスト名を選択した場合、URL はドメイン名の末尾で切り捨てられます。 • スクリプト パラメータを選択した場合、URL は、URL 内の左端の疑問符で切り捨てられます。 12.4(15)T よりも前のソフトウェア リリースを実行しているデバイスには切り捨てオプションを選択しないでください。選択すると検証エラーが発生します。 **ヒント** 両方のオプションを選択できますが、そのような指定方法は論理的ではありません。
Enable Server Log	HTTP要求に関する情報をURL フィルタリングサーバーのログサーバーに送信するかどうか。この情報には、URL、ホスト名、送信元 IP アドレス、および宛先 IP アドレスが含まれます。

要素	説明
その他のフィールド	
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用を参照してください。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシーオブジェクトの上書きの許可および個々のデバイスのポリシー オブジェクト オーバーライドについてを参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

URL フィルタ パラメータの [Add URL Domain Name]/[Edit URL Domain Name] ダイアログボックス

[URLドメイン名の追加（Add URL Domain Name）] ダイアログボックスを使用して、許可リスト（許可）またはブロックリスト（拒否）に Web サイトのドメイン名を追加します。

ドメイン名は完全な形式（www.cisco.com など、ホスト名を含む）にしたり、部分的な形式（cisco.com など）にしたりできます。部分的な名前の場合、そのドメイン上のすべての Web サイト ホストが、許可されるか、または拒否されます。また、ホストの IP アドレスを入力することもできます。

ナビゲーション パス

[URLフィルタパラメータマップの追加（Add URL Filter Parameter Map）]/[URLフィルタパラメータマップの編集（Edit URL Filter Parameter Map）] ダイアログボックスで、許可リストまたはブロックリストテーブルの下にある [追加（Add）] ボタンをクリックするか、名前を選択して [編集（Edit）] ボタンをクリックします。URL フィルタ パラメータ マップの設定 （57 ページ） を参照してください。

URLF Glob パラメータ マップの設定

[Add URLF Glob Parameter Map]/[Edit URLF Glob Parameter Map] ダイアログボックスを使用して、ローカル Web フィルタ クラス マップの URL のインスペクション用のパラメータ マップを定義します。

1 つの URLF Glob に、ブロックまたは許可する URL のセグメントだけが含まれている必要があります。許可またはブロックリスト URL のクラスマップを作成することが目的です。続い

て、ローカル Web フィルタ ポリシー マップを定義して、識別された URL を許可またはブロックできます。

1 つの URLF Glob は、次のタイプの URL セグメントの 1 つに制限する必要もあります。

- URL のサーバ名に出現する文字列。これには、サーバ名とネットワークのドメイン名が含まれます。たとえば、www.cisco.com などです。
- URL キーワードに出現する文字列。これは、URL 内の / 文字の間に出現する文字列、またはファイル名です。たとえば、URL セグメント www.cisco.com/en/US/ では、en と US の両方がキーワードです。index.html など、URL 内のファイル名もキーワードと見なされます。

URLF Glob では、/、{、}、? の文字を使用できません。

サーバ名または URL キーワードが一致するためには、ワイルドカード メタ文字を使用して可変文字列パターンを指定しないかぎり、URL 内の文字列が URLF Glob に含まれる文字列と完全に一致する必要があります。サーバ名または URL キーワードのパターン マッチングには、次のメタ文字を使用できます。

- *（アスタリスク）。0 個以上の任意の文字のシーケンスと一致します。たとえば、*.edu は教育機関ドメインにあるすべてのサーバと一致し、hack* を使用すると www.example.com/hacksite/123.html をブロックできます。
- [abc]（文字クラス）。カッコ内の任意の文字と一致します。文字のマッチングでは大文字と小文字が区別されます。たとえば、[abc] は a、b、または c と一致しますが、A、B、または C とは一致しません。このため、www.[ey]xample.com を使用して、www.example.com と www.yxample.com をブロックできます。
- [a-c]（文字範囲クラス）。範囲内の任意の文字と一致します。文字のマッチングでは大文字と小文字が区別されます。[a-z] は、任意の小文字と一致します。文字と範囲を混合できます。たとえば、[abcq-z] は、a、b、c、q、r、s、t、u、v、w、x、y、z と一致し、[a-cq-z] も同じです。ダッシュ（-）文字は、角カッコ内の最後または最初の文字である場合にだけリテラルになります（[abc-] または [-abc]）。
- [0-9]（数字範囲クラス）。カッコ内のすべての数字とマッチします。たとえば、[0-9] は 0、1、2、3、4、5、6、7、8、または 9 と一致します。このため、www.example[0-9][0-9].com を使用して、www.example01.com、www.example33.com、および www.example99.com などをブロックできます。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、次にコンテンツテーブルから [マップ（Maps）] > [パラメータマップ（Parameter Maps）] > [Webフィルタ（Web Filter）] > [URLFグロブパラメータ（URLF Glob Parameters）] を選択します。作業領域内を右クリックして [新規オブジェクト（New Object）] を選択するか、行を右クリックして [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- マップ オブジェクトについて
- ローカル Web フィルタ クラスの [Add Match Criterion]/[Edit Match Criterion] ダイアログボックス （38 ページ）
- ゾーンベースのファイアウォール ポリシーのコンテンツ フィルタリング マップの設定（48 ページ）
- ゾーンベースのファイアウォール ルールについて （3 ページ）

フィールド リファレンス

表 *18 : [Add URLF Glob Parameter Map]/[Edit URLF Glob Parameter Map]* ダイアログボックス

要素	説明
名前	ポリシー オブジェクトの名前。最大 40 文字を使用できます。
説明	ポリシー オブジェクトの説明。最大 200 文字を使用できます。

値	ターゲットとしている URL のサーバ ドメインまたはキーワード。1 種類の Glob だけを入力できます（すべてのサーバ ドメイン、またはすべての URL キーワードは指定できますが、両方の混合はできません）。
	複数のエントリを含める場合は、エントリを改行で区切ります。たとえば、次のエントリは、すべての政府または教育機関の Web サーバを識別します。
	`*.gov`
	`*.edu`

カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用を参照してください。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可および個々のデバイスのポリシー オブジェクト オーバーライドについてを参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

Web フィルタ マップの設定

[Add Web Filter Map]/[Edit Web Filter Map] ダイアログボックスを使用して、ルータのゾーンベースのファイアウォール ポリシーで使用するインスペクション マップのパラメータ、および一致基準と値を定義します。

ゾーンベースのファイアウォール ポリシールールのアクションを [Content Filter] に設定する場合は、Web フィルタ ポリシー マップを選択して、Web フィルタリング パラメータと一致基準を定義できます。Web フィルタポリシーマップは、Cisco IOS ソフトウェアリリース 12.4(20)T 以降を実行しているルータでだけ選択できます。Cisco IOS Software Release 12.4(6)T から 12.4(20)T までを実行しているルータにゾーンベースのファイアウォールを設定する場合は、Web フィルタ ポリシー マップの代わりに URL フィルタ パラメータ マップを設定する必要があります。詳細については、URL フィルタ パラメータ マップの設定 （57 ページ）を参照してください。

ローカル Web フィルタリングとサーバベースの Web フィルタリングの組み合わせを設定できます。これを設定するには、使用しているサーバのタイプおよび一致基準に適したパラメータ マップと、ローカルおよびサーバ クラス マップの適切な組み合わせを選択する必要があります。異なるタイプのサーバのクラスマップとパラメータ マップは組み合わせないでください。

ナビゲーション パス

[管理（Manage）]>[ポリシーオブジェクト（Policy Objects）] を選択し、次にオブジェクトタイプセレクタから **[マップ（Maps）]>[ポリシーマップ（Policy Maps）]>[Webフィルタ（Web Filter）]>[Webフィルタ（Web Filter）]** を選択します。テーブル内を右クリックして [新規オブジェクト（New Object）] を選択するか、行を右クリックして [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- マップ オブジェクトについて
- ゾーンベースのファイアウォール ポリシーのコンテンツ フィルタリング マップの設定（48 ページ）
- ゾーンベースのファイアウォール ルールについて （3 ページ）

フィールド リファレンス

表 19 : [Add FTP Map]/[Edit FTP Map] ダイアログボックス

要素	説明
名前	ポリシー オブジェクトの名前。最大 40 文字を使用できます。
説明	ポリシー オブジェクトの説明。最大 200 文字を使用できます。

要素	説明
[パラメータ（Parameters）] タブ	
パラメータ タイプ パラメータマップ	Web フィルタ ポリシー マップに含めるパラメータ マップのタイプ。パラメータ マップを選択しない場合は [None] を選択します。 特定のパラメータタイプを選択する場合は、[パラメータ マップ（Parameter Map）] フィールドにパラメータマップの名前を入力します。[選択（Select）] をクリックしてリストからマップを選択するか、新しいパラメータマップオブジェクトを作成します。
[Match Condition and Action] タブ [Match All] テーブルには、ポリシーマップに含まれているクラスマップ、およびこのクラスに一致するトラフィックに適用するアクションが表示されます。トラフィックがこのクラスと照合される場合、選択したクラスマップで定義されているすべての基準を満たす必要があります。 • 基準を追加するには、[Add] ボタンをクリックし、[Match Condition and Action] ダイアログボックスに入力します（ゾーンベースのファイアウォール ポリシーおよび Web フィルタ ポリシーの [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス （46 ページ）を参照）。 • 基準を編集するには、基準を選択し、[Edit] ボタンをクリックします。 • 基準を削除するには、基準を選択し、[Delete] ボタンをクリックします。	
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用を参照してください。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可および個々のデバイスのポリシー オブジェクト オーバーライドについてを参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）]ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

デフォルトのドロップ動作の変更

デフォルトでは、ゾーン間のすべてのトラフィックは明示的に許可されていないかぎりドロップされます。ただし、この項の説明に従って、このデフォルト動作を変更できます。

Security Managerは、ゾーンベースのファイアウォール ルールに対して指定されているパラメータ（クラス、パラメータ、およびポリシー マップを含みます）を、ルータが認識する一連のIOS コマンドに変換します。これらはいわゆる「CLI」（コマンドライン インターフェイス）コンフィギュレーション コマンドであり、[ツール（Tools）] > [設定のプレビュー（Preview Configuration）] を選択することで別のウィンドウでプレビューできます。詳細については、設定のプレビューを参照してください。また、ゾーンベースのルールと設定のトラブルシューティング （73 ページ）では、ゾーンベースのファイアウォールの CLI コマンドの例について説明しています。

この説明の目的では、これらのコマンドのうち最も重要なコマンドは **policy-map** です。このコマンドは、ゾーンの各ペアにゾーンポリシーを適用するために使用します。つまり、任意のゾーンペアに対して、トラフィック（クラス）とアクションを定義するすべてのルールが 1 つの policy-map で適用されます。さらに、Security Manager は、現在の **class-default** クラスを policy-map のクラスリストの末尾に追加して、ゾーンルールで処理されないすべてのパケットをキャプチャします。

デフォルトの class-default はドロップです。このクラスを各 policy-map に追加すると、ゾーン間のトラフィックの暗黙的なドロップが実現されます。ただし、前に述べたように、このデフォルト動作は任意のゾーンペアに対して変更できます。たとえば、すべての不一致トラフィックを渡すことを選択したり、デフォルトを [Drop and Log] に変更して、既存のルールで一致しないトラフィックを判断したりできます。

（注） デフォルト動作のオプションは、[Drop]、[Drop and Log]、[Pass]、および [Pass and Log] だけです。

デフォルト ポリシーでパケットを引き続きドロップする場合は、Security Manager で何も行う必要がありません。このルールは自動的に生成されます。ゾーンペアのデフォルト動作を変更しない場合は、**Permit any any IP** ルール（つまり、ゾーンベースのファイアウォール ルールの追加と編集 （82 ページ）の [一致（Match）] : 許可（Permit）、[送信元（Sources）] : any、[宛先（Destinations）] : any、[サービス（Services）] : IP）を指定し、[アクション（Action）] として [ドロップして記録（Drop and Log）]、[通過（Pass）]、または [通過させて記録（Pass and Log）] を選択する必要があります。このルールがゾーン ペアのルールのリストの最後にあることも確認する必要があります。Security Manager は、これを目的の class-default ルールとして解釈します。

ゾーンベースのルール テーブルに大量のルールが含まれる場合は、このルールがゾーン ペアの他のすべてのルールよりもあとにあることを確認するのが難しい場合があります。この確認作業を軽減するのに使用できる手法をいくつか示します。

- セクションを使用して、ゾーンペアごとに1つのセクションでテーブルを編成します。これにより、ゾーンペアのルールを並べること、また class-default ルールが最後にくるようにすることができます。セクションでの作業の詳細については、セクションを使用したルール テーブルの編成を参照してください。
- [デフォルト（Default）] スコープに class-default ルールを含む共有ゾーンベースルールポリシーを作成し、デバイスのローカル ゾーンベース ルール ポリシーでこのルールを継承します。共有ポリシーの継承と作成の詳細については、ルールの継承または継承の解除および新しい共有ポリシーの作成を参照してください。

ゾーンベースのファイアウォール ルールの設定

[ゾーンベースのファイアウォール（Zone Based Firewall）]設定ページを使用して、参照されないゾーンの識別、VPN インターフェイス用のゾーンの指定、WAAS サポートの有効化または無効化、Trend Micro のサーバーと証明書情報のメンテナンス、およびグローバルログ設定の指定をします。

（注） バージョン 4.21 以降、Cisco Security Manager では、すべてのアグリゲーション サービス ルータ、統合サービスルータ、埋め込み型サービスルータ、および Cisco IOS ソフトウェアで動作するすべてのデバイスについて、バグ修正または拡張機能のサポートを含むサポート全体が終了します。

関連項目

- [Zone Based Firewall] ページ （68 ページ）
- ゾーンベースのファイアウォール ルールについて （3 ページ）

ステップ 1 [Zone Based Firewall] ページ （68 ページ）へのアクセス方法を次に示します。

- （デバイスビュー）IOS デバイスを選択し、ポリシーセレクタから **[ファイアウォール（Firewall）] > [設定（Settings）] > [ゾーンベースのファイアウォール（Zone Based Firewall）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[ファイアウォール（Firewall）] > [設定（Settings）] > [ゾーンベースのファイアウォール（Zone Based Firewall）]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

ステップ 2 （任意）[Zones] タブで、参照されないゾーンを追加、編集、および削除します。

[Zones] タブには、デバイスに定義されているすべての参照されないゾーン、つまり関連付けられているインターフェイス、ルール、またはポリシーのないゾーンがリストされます。参照されないゾーンは、通常、デバイス検出時に検索および表示されますが、名前を付けた「空の」ゾーンをこの手順で作成することもできます。

ステップ 3 （任意）[VPN] タブで、VPN トラフィックに対して設定されたゾーンの名前を指定します。

このゾーンは、このルータのゾーンベースのファイアウォール ルールで動的 VPN トラフィックを処理できるようにします。詳細については、ゾーンベースのファイアウォールポリシーでの VPN の使用 （7 ページ）を参照してください。

ステップ 4 （任意）[WAAS] タブで、[WAASの有効化（Enable WAAS）] を選択して Wide Area Application Services 相互運用性を有効にします。

このオプションがイネーブルになっていない場合、WAASデバイスによって最適化されたパケットは、TCP ハンドシェイク時に WAAS によって TCP パケット シーケンス番号が増加したため、ドロップされる可能性があります。この動作は、IOS デバイスによって潜在的攻撃と見なされる可能性があります。

ステップ 5 （任意）[コンテンツフィルタの設定（Content Filter Settings）] タブで、Trend Micro ベースのコンテンツ フィルタリング用のサーバー 0 設定を指定します。

Trend Micro ベースのコンテンツ フィルタリングを使用するには、[Zone Based Firewall] ページのこのタブで、Trend Micro サーバの接続情報を設定する必要があります。このタブでは、Trend Micro の登録および証明書のダウンロードへのリンクも提供されます。この形式のコンテンツ フィルタリングを利用するには、Trend Micro とのアクティブなサブスクリプションを取得し、有効なサブスクリプション証明書をダウンロードして IOS デバイスにインストールする必要があります。

詳細については、[Zone Based Firewall] ページ - [Content Filter] タブ （71 ページ）を参照してください。

ステップ 6 （任意）[Global Parameters (ASR)] タブで、ASR デバイスに固有のグローバルなログ関連設定を設定できます。

- [Log Dropped Packets]：このオプションを選択して、デバイスによってドロップされたすべてのパケットを記録し、syslog ロギングをイネーブルにして情報を表示する必要があります。
- [Log Flow export timeout rate]：フローが期限切れになるか、またはタイムアウトしたあとに NetFlow ログが作成されます。フローが期限切れになるまでアクティブでいられる期間に関して時間制限を設定することが重要です。この値は、フローが期限切れになるまでアクティブなままでいることのできる最大分数です。この値は、1 ～ 3600 の任意の整数で、デフォルトは 30 です。
- [Log Flow export destination IP]：フロー データの送信先となる、NetFlow Collector の IP アドレスまたはホスト名。
- [Log Flow export destination port]：NetFlow Collector によってモニタされる、フロー データの UDP ポート。

[Zone Based Firewall] ページ

[Zone Based Firewall] ページを使用して、参照されないゾーンの設定と識別、VPN ゾーンの指定、WAAS サポートのイネーブル化またはディセーブル化、Trend Micro のサーバと証明書情報のメンテナンス、およびサポートされる ASR デバイスでのグローバル ログ設定の指定を行います。

次のタブについては、このページの表で説明されています。

- **ゾーン**
- **VPN**
- **WAAS**
- **Global Parameters (ASR)**

[コンテンツフィルタリング（Content Filtering）] タブの詳細については、[Zone Based Firewall] ページ - [Content Filter] タブ （71 ページ）を参照してください。

ナビゲーション パス

[Zone Based Firewall] ページにアクセスするには、次のいずれかを実行します。

- （デバイスビュー）デバイスを選択し、ポリシーセレクタから **[ファイアウォール（Firewall）] > [設定（Settings）] > [ゾーンベースのファイアウォール（Zone Based Firewall）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[ファイアウォール（Firewall）] > [設定（Settings）] > [ゾーンベースのファイアウォール（Zone Based Firewall）]** を選択します。新しいポリシーを作成するか、または既存のポリシーを選択します。
- （マップビュー）デバイスを右クリックし、**[ファイアウォール設定の編集（Edit Firewall Settings）] > [ゾーンベースのファイアウォール（Zone Based Firewall）]** を選択します。

関連項目

- ゾーンベースのファイアウォール ルールの設定 （67 ページ）
- ゾーンベースのファイアウォール ルールについて （3 ページ）
- ゾーンベースのファイアウォールルールの追加 （16 ページ）

フィールド リファレンス

表 *20 : [Zone Based Firewall]* ページ

要素	説明
[Zones] タブ	このタブには、参照されないゾーン、つまり関連付けられているインターフェイス、ルール、またはポリシーのないゾーンをリストする [Zones] テーブルが表示されます。参照されないゾーンは、通常、デバイス検出時に検索および表示されますが、名前を付けた「空の」ゾーンをこの手順で作成することもできます。 [Zones] テーブルには、参照されないゾーンごとに次の情報がリストされます。 • [Zone]：ゾーン/インターフェイス ロールの名前。 • [Content]：ゾーンに割り当てられているインターフェイス。 • [Description]：ゾーンに関してユーザが指定するコメント。 このテーブルにゾーンを追加するには、[Add Row] ボタンをクリックし、[Zone] ダイアログボックスでゾーン名を指定します。
[VPN] タブ	このタブには、[VPN Zone] フィールドが表示されます。このフィールドのゾーン エントリによって、動的 VPN トラフィックをこのルータ上のゾーンベースのファイアウォール ルールで処理できます。このゾーンの詳細については、ゾーンベースのファイアウォールポリシーでの VPN の使用 （7 ページ）を参照してください。 VPN トラフィックが通過するゾーンを入力または選択します。
[WAAS] タブ	このタブには、[Enable WAAS] チェックボックスが表示されます。このオプションをオンにすると、Wide Area Application Services 相互運用性がイネーブルになります。 このオプションがイネーブルになっていない場合、WAAS デバイスによって最適化されたパケットは、TCP ハンドシェイク時に WAAS によって TCP パケット シーケンス番号が増加したため、ドロップされる可能性があります。この動作は、IOS デバイスによって潜在的攻撃と見なされる可能性があります。
[Content Filtering] タブ	このタブには、Trend Micro ベースのコンテンツ フィルタリングのサーバ設定と証明書リンクが表示されます。詳細については、[Zone Based Firewall] ページ - [Content Filter] タブ （71 ページ）を参照してください。

要素	説明
[Global Parameters (ASR)] タブ	このタブには、ASR デバイスに固有のグローバルなロギング関連設定が表示されます。これらの設定は、次のように設定します。 • [Log Dropped Packets]：このオプションを選択して、デバイスによってドロップされたすべてのパケットを記録し、syslog ロギングをイネーブルにして情報を表示する必要があります。 • [Log Flow export timeout rate]：フローが期限切れになるか、またはタイムアウトしたあとに NetFlow ログが作成されます。フローが期限切れになるまでアクティブでいられる期間に関して時間制限を設定することが重要です。この値は、フローが期限切れになるまでアクティブなままでいることのできる最大分数です。この値は、1 ～ 3600 の任意の整数で、デフォルトは 30 です。 • [Log Flow export destination IP]：フロー データの送信先となる、NetFlow Collector の IP アドレスまたはホスト名。 • [Log Flow export destination port]：NetFlow Collector によってモニタされる、フロー データの UDP ポート。

[Zone Based Firewall] ページ - [Content Filter] タブ

Trend Micro ベースのコンテンツ フィルタリングを使用するには、[Zone Based Firewall] ページのこのタブで、Trend Micro サーバの接続情報を設定する必要があります。このタブでは、Trend Micro の登録および証明書のダウンロードへのリンクも提供されます。この形式のコンテンツ フィルタリングを利用するには、Trend Micro とのアクティブなサブスクリプションを取得し、有効なサブスクリプション証明書をダウンロードして IOS デバイスにインストールする必要があります。

ナビゲーション パス

[Zone Based Firewall] ページにアクセスするには、次のいずれかを実行します。

- （デバイスビュー）デバイスを選択し、デバイスセレクタから **[ファイアウォール（Firewall）] > [設定（Settings）] > [ゾーンベースのファイアウォール（Zone Based Firewall）]** を選択します。
- （ポリシービュー）ポリシーセレクタから **[ファイアウォール（Firewall）] > [設定（Settings）] > [ゾーンベースのファイアウォール（Zone Based Firewall）]** を選択します。
- （マップビュー）デバイスを右クリックし、**[ファイアウォール設定の編集（Edit Firewall Settings）] > [ゾーンベースのファイアウォール（Zone Based Firewall）]** を選択します。

関連項目

- [Zone-based Firewall Rules] ページ （78 ページ）

- ゾーンベースのファイアウォール ポリシーのコンテンツ フィルタリング マップの設定（48 ページ）
- ゾーンベースのファイアウォール ルールについて （3 ページ）
- ゾーンベースのファイアウォールルールの追加 （16 ページ）

フィールド リファレンス

表 21 : [Zone Based Firewall] ページ - [Content Filter] タブ

要素	説明
Trend Micro Server Settings	
Cache-entry-lifetime (hrs)	Trend Micro サーバーへのルックアップ要求がルータのローカル URL キャッシュ テーブルに残る時間数。許可される範囲は 0 ～ 120 です。デフォルト値は 24 です。
Cache-size (KBytes)	ルータのローカル URL キャッシュで使用する最大メモリ量。許可される範囲は 0 ～ 120,000 KB です。デフォルト値は 250 です。
サーバー（Server）	Trend Micro URL フィルタリング サーバの完全修飾ドメイン名または IP アドレス。
HTTP ポート（HTTP Port）	Trend Micro サーバが HTTP 要求をリスニングするポート。デフォルトは 80 です。
HTTPS ポート（HTTPS Port）	Trend Micro サーバが HTTPS 要求をリスニングするポート。デフォルトは 443 です。
Retransmission Count	サーバからの応答がないときに、ルータがルックアップ要求を再送信する回数。指定できる範囲は 1 ～ 10 です。
Retransmission Timeout	サーバからの応答をルータが待機する秒数。範囲は 1 ～ 300 です。
アラート（Alert）	ステートフル パケット インスペクション メッセージが syslog にコピーされるかどうか。
Trend Micro Server Certificate Download Links	
Link to download certificates	Cisco IOS ルータに Trend URL フィルタリング サポートの信頼できる CA の証明書をインストールするページを開きます。
Link for product registration	製品ライセンス登録のページを開きます。製品認証キーを入力し、ルータを登録する必要があります。

[Add Zone]/[Edit Zone] ダイアログボックス

[Add Zone]/[Edit Zone] ダイアログボックスを使用して、参照されないゾーン（関連付けられているインターフェイス、ルール、またはポリシーのないゾーン）を追加および編集します。

ナビゲーション パス

[Add Zone]/[Edit Zone] ダイアログボックスにアクセスするには、次のいずれかを行います。

- （デバイスビュー）デバイスを選択し、デバイスセレクタから **[ファイアウォール（Firewall）] > [設定（Settings）] > [ゾーンベースのファイアウォール（Zone Based Firewall）]** を選択します。[ゾーン（Zones）] テーブル内を右クリックして [行の追加（Add Row）] を選択するか、行項目を右クリックして [行の編集（Edit Row）] を選択します。
- （ポリシービュー）ポリシーセレクタから **[ファイアウォール（Firewall）] > [設定（Settings）] > [ゾーンベースのファイアウォール（Zone Based Firewall）]** を選択します。テーブル内を右クリックして [行の追加（Add Row）] を選択するか、行項目を右クリックして [行の編集（Edit Row）] を選択します。
- （マップビュー）デバイスを右クリックし、**[ファイアウォールポリシーの編集（Edit Firewall Policies）] > [ゾーンベースのファイアウォールルール（Zone Based Firewall Rules）]** を選択します。

[ゾーン（Zone）] フィールドにゾーン名を入力するか、[選択（Select）] をクリックして [インターフェイスセレクタ（Interfaces Selector）] ダイアログボックスからゾーンを選択します。

関連項目

- [Zone Based Firewall] ページ （68 ページ）
- ゾーンベースのファイアウォール ルールについて （3 ページ）
- ゾーンベースのファイアウォール ルールの設定 （67 ページ）

ゾーンベースのルールと設定のトラブルシューティング

ゾーンベースのファイアウォール ルールは強力ですが、複雑でもあります。ゾーン ルールを使用して、アクセル ルール、インスペクション ルール、および Web フィルタ ルールを 1 種類のファイアウォール ルールで置換できます。ゾーンベースのファイアウォール ルールでは非常に多くのアクションを実行できるため、アクセス コントロール リスト（ACL）、クラスマップ、およびポリシーマップの構造といった、これらのアクションから生成された設定では、多くの異なるタイプのコンフィギュレーション コマンドが使用されます。（たとえばアクセス ルールとは異なり）ゾーンベースのファイアウォール ルールと設定の行との間には、1 対 1 対応はありません。

この複雑さを示すために、ここではゾーンベースのファイアウォール ルールと、そのルールから生成された設定の関係を説明します。ゾーンベースのファイアウォール ルールを作成および展開するために、このトピックの情報を理解する必要はありません。ただし、CLI（コマンド

ラインインターフェイス）に精通している場合、またはルールによって望ましくない結果が生成される場合は、ゾーンベースのファイアウォールルールを理解およびトラブルシューティングするのにこの情報が役立つ場合があります。

次の図に示すルールのセットについて考えます。これらのルールは単一のゾーン ペアのポリシーを構成し、内部ゾーンから外部ゾーンに移動するトラフィックに影響します。これは、インターネットに向かう内部ネットワークからのトラフィックです。ルールでは、次のアクションを定義します。

- 10.100.10.0/24 および 10.100.11.0/24 ネットワークからのすべてのトラフィックをドロップする。
- 10.100.12.0/24 ネットワークからのすべての FTP および FTPS トラフィックをドロップする。
- 任意のネットワークからのすべてのピアツーピア トラフィックをドロップする。
- すべての FTP/FTPS トラフィック（すでにドロップされている 10.100.12.0/24 からのトラフィックを除く）を検査（および許可）する。
- 追加の詳細インスペクション ポリシー マップを使用して、すべての HTTP トラフィックを検査する。
- 最後に、残りのすべての TCP/UDP トラフィックの汎用インスペクションを実行する。

図 *3:* ゾーン ペアのゾーンベース ルールの例

No.	Permit	Source	Destination	Service	From Zone	To Zone	Inspected Protocol	Action
Local - Mandatory (7 Rules)								
1	✓	10.100.10.0/24	any	IP	Inside	Outside		Drop
2	✓	10.100.11.0/24	any	IP	Inside	Outside		Drop
3	✓	10.100.12.0/24	any	IP	Inside	Outside	Ftp Ftps	Drop
4	✓	any	any	IP	Inside	Outside	Bittorrent Edonkey Fasttrack Icq Kazaa2	Drop
5	✓	any	any	IP	Inside	Outside	Ftp Ftps	Inspect
6	✓	any	any	IP	Inside	Outside	Http(HTTPpmap)	Inspect
7	✓	any	any	IP	Inside	Outside	Tcp Udp	Inspect

194853

これらのルールを展開すると、Security Manager は次の設定を生成します。太字は、設定に続く説明の参照用に追加されています。

A.

```
class-map type inspect http match-any HTTPcmap
 match req-resp protocol-violation
 match request port-misuse any
!
```

B.

```
policy-map type inspect http HTTPpmap
 class type inspect http HTTPcmap
  reset
  log
!
```

C.

```
class-map type inspect CSM_ZBF_CLASS_MAP_1
 match access-group name CSM_ZBF_CMAP_ACL_1
!
```

D.

```
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_1
 match protocol ftp
 match protocol ftps
!
```

E.

```
class-map type inspect CSM_ZBF_CLASS_MAP_2
 match access-group name CSM_ZBF_CMAP_ACL_2
 match class-map CSM_ZBF_CMAP_PLMAP_1
!
```

F.

```
class-map type inspect match-any CSM_ZBF_CLASS_MAP_3
 match protocol bittorrent
 match protocol edonkey
 match protocol fasttrack
 match protocol icq
 match protocol kazaa2
!
```

G.

```
class-map type inspect CSM_ZBF_CLASS_MAP_4
 match protocol http
!
```

H.

```
class-map type inspect match-any CSM_ZBF_CLASS_MAP_5
 match protocol tcp
 match protocol udp
!
```

I.

```
policy-map type inspect CSM_ZBF_POLICY_MAP_1
 class type inspect CSM_ZBF_CLASS_MAP_1
  drop
 class type inspect CSM_ZBF_CLASS_MAP_2
  drop
 class type inspect CSM_ZBF_CLASS_MAP_3
  drop
class type inspect CSM_ZBF_CMAP_PLMAP_1
  inspect
 class type inspect CSM_ZBF_CLASS_MAP_4
  inspect
  service-policy http HTTPpmap
 class type inspect CSM_ZBF_CLASS_MAP_5
  inspect
 class class-default
  drop
!
```

J.

```
zone security Inside
zone security Outside
zone-pair security CSM_Inside-Outside_1 source Inside destination Outside
 service-policy type inspect CSM_ZBF_POLICY_MAP_1
!
interface GigabitEthernet0/1
 ip address dhcp
 zone-member security Inside
!
interface GigabitEthernet0/2
 ip address dhcp
 zone-member security Outside
!
```

K.

```
ip access-list extended CSM_ZBF_CMAP_ACL_1
 permit ip 10.100.10.0 0.0.0.255 any
 permit ip 10.100.11.0 0.0.0.255 any
!
```

L.

```
ip access-list extended CSM_ZBF_CMAP_ACL_2
 permit ip 10.100.12.0 0.0.0.255 any
!
```

次のリストでは、Security Manager のルールが device-configuration コマンドにどのように変換されるかを説明し、このルールとコマンドの関係を理解できるようにします。リストの番号は、Security Manager のルール テーブルのルール番号に対応します（前の図を参照）。

1. このルールでは、10.100.10.0/24 ネットワークからのすべてのトラフィックがドロップされます。[Permit]、[Source]、[Destination]、[Service] の各フィールドは、（K）で定義されている CSM_ZBF_CMAP_ACL_1 という名前の ACL の最初のアクセス コントロール エントリ（ACE）の作成に使用されます。この ACL は、（I）で定義されているポリシー マップ

CSM_ZBF_POLICY_MAP_1 の最初の廃棄ルールを定義する、（C）で定義されているクラス マップ CSM_ZBF_CLASS_MAP_1 から参照されます。

ポリシー マップ（I）は、（J）のゾーン サービス ポリシーの定義に使用されます。このポリシー マップはすべてのルールがゾーン ペアに割り当てられる方法であるため、（J）は再び言及されていません。

1. このルールでは、10.100.11.0/24 ネットワークからのすべてのトラフィックがドロップされます。このルールは、（K）で定義されている ACL に ACE を追加することで、ルール 1 に結合されています。残りの設定は、ルール 1 と同じです。このため、ルール 1 と 2 は、基本的にデバイス設定の単一のルールになります。

2. このルールでは、10.100.10.12/24 ネットワークからのすべての FTP/FTPS トラフィックがドロップされます。[Permit]、[Source]、[Destination]、[Service] の各フィールドは、（L）で定義されている CSM_ZBF_CMAP_ACL_2 という名前の ACL の作成に使用されます。[Protocol] テーブルでは、FTP および FTPS プロトコルを指定する、（D）で定義されているクラス マップ CSM_ZBF_CMAP_PLMAP_1 が生成されます。ACL および FTP/FTPS クラス マップは、（E）で定義されている新しいクラス マップ CSM_ZBF_CLASS_MAP_2 で使用されます。これにより、送信元とプロトコルの組み合わせに基づいてトラフィックの特徴付けが完了します。最後に、（E）は、ポリシー マップ（I）で第 2 のルールとして参照されています。

3. このルールは、Bittorrent、eDonkey、FastTrack、ICQ、または Kazaa2 のいずれかのプロトコルを使用する送信元からのピアツーピア トラフィックをドロップします。このルールにより、内部サーバがこれらのサービスのファイル共有ソースとして使用されることを防ぎます。ルールはデフォルト IP サービスのすべての送信元と宛先に適用されるため、ACL は不要です。代わりに、設定は（F）で定義されているクラス マップ CSM_ZBF_CLASS_MAP_3 から開始します。このクラス マップは、ポリシー マップ（I）の第 3 の廃棄ルールで参照されています。

4. このルールは、任意の送信元から任意の宛先への FTP/FTPS トラフィックを検査します。これは、これらのサービスが許可されることを意味します。ルール 3 は、ルール 5 よりも上にあるため 10.100.12.0/24 ネットワークからの FTP/FTPS トラフィックをすでにドロップしています。このため、これらのルールの組み合わせは、FTP/FTPS トラフィックが 10.100.12.0/24 以外のすべての送信元に対して検査されることを意味します。[Protocol] テーブルでは、ルール 3 に対するのと同じプロトコルを指定するため、新しいクラス マップは不要です。代わりに、ポリシー マップ（I）は、クラス マップ（D）を単純に第 4 のクラス タイプとして参照しますが、今回は Inspect アクションを伴います。

5. このルールは、HTTP トラフィックを検査し、HTTPpmap という名前の詳細インスペクション ポリシー マップを適用します。HTTPpmap ポリシー マップ（B）は、トラフィックがクラス マップ HTTPcmap（A）で定義されている基準と一致する場合に実行するアクションを定義します。これらのマップでは、HTTP プロトコルに違反する HTTP 接続、またはポートを誤用する HTTP 接続をリセット（ドロップ）し、syslog エントリを生成する必要があることを指定します（プロトコル違反とポートの誤用は、サービス妨害（DoS）攻撃の特徴を示している可能性があります）。（A）と（B）の組み合わせにより、このポリシーの詳細検査ルールが定義されます。

追加のクラス マップ CSM_ZBF_CLASS_MAP_4 は、HTTP プロトコル（G）を指定するために必要です。次に、ポリシー マップ（I）の第 5 のクラス タイプ ルールは、インスペクションのクラス マップ（G）を参照し、service-policy コマンドは詳細インスペクションのポリシー マップ（B）を参照します。

1. このルールは、TCP/UDP トラフィックに対する汎用インスペクションを提供し、内部ネットワークからインターネットおよびその戻り方向の他の TCP/UDP トラフィックを許可および検査します。（H）で定義されているクラス マップ CSM_ZBF_CLASS_MAP_5 は、[Protocols] テーブルから生成されています。このクラス マップは、ポリシー マップ（I）の最後から 2 つめのルールになります。
2. 最後に、ポリシー マップ（I）の最後の class-default ルールとして出現する自動ルールがあります。このルールは、ポリシー マップ（I）で参照されているクラス マップの 1 つと一致しないトラフィックをドロップします。たとえば、内部ネットワークからインターネットへの ICMP トラフィックは許可されません。さまざまな class-default ルールの設定方法については、デフォルトのドロップ動作の変更 （66 ページ）を参照してください。

[Zone-based Firewall Rules] ページ

ゾーンベースのファイアウォールルールは、「ゾーン」と呼ばれるインターフェイスのグループ間でファイアウォールポリシーを一方向に適用します。つまり、インターフェイスはゾーンに割り当てられ、特定のインスペクションポリシーがゾーン間を一方向に移動するトラフィックに適用されます。

ゾーンは、トラフィックがネットワークの別の領域に移動するときに特定の制限の対象となる境界を定義します。ゾーン間のデフォルトのゾーンベース ファイアウォール ポリシーは、[すべて拒否（deny all）] です。このため、ポリシーが明示的に設定されていない場合は、ゾーン間のすべてのトラフィックがブロックされます。

（注） バージョン 4.21 以降、Cisco Security Manager では、すべてのアグリゲーション サービス ルータ、統合サービスルータ、埋め込み型サービスルータ、および Cisco IOS ソフトウェアで動作するすべてのデバイスについて、バグ修正または拡張機能のサポートを含むサポート全体が終了します。

[Zone Based Firewall Rules] ページには、現在設定されているゾーンベースのファイアウォール ルールのリストが表示され、ルールを追加、編集、および削除できます。

ヒント ディセーブルなルールには、テーブルの行にハッシュ マークが重なって表示されます。設定を展開すると、ディセーブルなルールはデバイスから削除されます。詳細については、ルールのイネーブル化とディセーブル化を参照してください。

ナビゲーション パス

[Zone Based Firewall Rules] ページにアクセスするには、次のいずれかを実行します。

- （デバイスビュー）デバイスを選択し、ポリシーセレクタから [ファイアウォール（Firewall）] > [設定（Settings）] > [ゾーンベースのファイアウォールルール（Zone Based Firewall Rules）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [ファイアウォール（Firewall）] > [ゾーンベースのファイアウォールルール（Zone Based Firewall Rules）] を選択します。新しいポリシーを作成するか、または既存のポリシーを選択します。
- （マップビュー）デバイスを右クリックし、[ファイアウォールポリシーの編集（Edit Firewall Policies）] > [ゾーンベースのファイアウォールルール（Zone Based Firewall Rules）] を選択します。

関連項目

- ゾーンベースのファイアウォール ルールについて （3 ページ）
- ゾーンベースのファイアウォールルールの追加 （16 ページ）
- テーブルのフィルタリング

フィールド リファレンス

表 22 : [Zone Based Firewall Rules] ページ

要素	説明
番号	この番号は、リスト内の順序におけるルールの位置を示します。[Up Row] ボタンおよび [Down Row] ボタンを使用して、選択したルールの位置を変更できます。
許可（Permit）	ルールでトラフィックが許可されるか拒否されるかを示します。 • [Permit]：緑色のチェック マークとして表示されます。 • [Deny]：スラッシュの入った赤色の丸として表示されます。

要素	説明
ソース	ルールのトラフィックの送信元。ネットワークまたはセキュリティグループにすることができます。複数のエントリは、テーブルセル内の個別の行に表示されます。 • [ネットワーク（Network）]：このルールの送信元として定義されているネットワーク、ホスト、または IP アドレスオブジェクトおよび定義。「All-Address」オブジェクトは、ルールを特定のホストまたはネットワークに制限しません。 これらの定義の詳細については、 ネットワーク/ホストオブジェクトについておよびポリシー定義中の IP アドレスの指定を参照してください。 （注） バージョン 4.21 以降、Cisco Security Manager は、すべてのアグリゲーション サービス ルータ、統合サービスルータ、組み込みサービスルータ、および Cisco IOS ソフトウェアで動作するすべてのデバイスについて、バグ修正または拡張機能のサポートを含むサポート全体を終了します。 各仕様を他の仕様と組み合わせて、トラフィックの一致をすべての定義を含むフローのみに制限します。たとえば、指定された送信元アドレス範囲内から発信された指定されたユーザートラフィックなどに制限します。
宛先	ルールのトラフィックの宛先。ネットワークまたはセキュリティグループにすることができます。複数のエントリは、テーブルセル内に個別の行に表示されます。 • [ネットワーク（Network）]：このルールの宛先として定義されているネットワーク、ホスト、またはIPアドレスオブジェクトおよび定義。「All-Address」オブジェクトは、ルールを特定のホストまたはネットワークに制限しません。 これらの定義の詳細については、 ネットワーク/ホストオブジェクトについておよびポリシー定義中の IP アドレスの指定を参照してください。 （注） バージョン 4.21 以降、Cisco Security Manager は、すべてのアグリゲーション サービス ルータ、統合サービスルータ、組み込みサービスルータ、および Cisco IOS ソフトウェアで動作するすべてのデバイスについて、バグ修正または拡張機能のサポートを含むサポート全体を終了します。 各仕様を他の仕様と組み合わせて、トラフィックの一致をすべての定義を含むフローのみに制限します。たとえば、指定された送信元アドレス範囲内から発信された指定されたユーザートラフィックなどに制限します。

要素	説明
サービス	このルールで照合されるトラフィックのタイプを定義するサービス。サービスは、プロトコルおよびポート情報を指定するオブジェクトで定義されます。詳細については、サービスとサービス オブジェクトおよびポート リスト オブジェクトの理解と指定を参照してください。
From Zone	このルールは、このゾーンから発信されるトラフィックにだけ適用されます。
To Zone	このルールは、このゾーンを宛先とするトラフィックにだけ適用されます。
Inspected Protocol	ルールが選択されたアクションを実行するプロトコル。
操作	一致したプロトコルの処理方法を識別します。 • [Drop]：一致したトラフィックはサイレントにドロップされます。すべてのトラフィックに適用されるデフォルト アクション。 • [Drop and Log]：一致したトラフィックは、記録され、ドロップされます。 • [Pass]：ルータは、一致したトラフィックを送信元ゾーンから宛先ゾーンに転送します。 • [Pass and Log]：トラフィックが記録され、転送されます。 • [Inspect]：状態ベースのトラフィック コントロール。[Inspect] は、Port to Application Mapping（PAM）に基づいて、特定のプロトコルのアプリケーション インスペクションとコントロールを提供できます。 • [Content Filter]：WebFilter パラメータ マップまたは WebFilter ポリシー マップに基づく HTTP コンテンツ インスペクション。 （注） ログ オプションによって、システム ログ メッセージが生成されます。これらのメッセージをキャプチャするように syslog ロギングが設定されていることを確認する必要があります。
オプション	このルールに割り当てられているインスペクション パラメータ マップ。[Inspect] アクションと [Content Filter] アクションでだけ使用できます。
カテゴリ	ルールに割り当てられるカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用を参照してください。
説明	このルールの説明（提供されている場合）。最大 1024 文字を使用できます。

要素	説明
[最後のチケット（Last Ticket(s)）]	ルールの最終変更に関連付けられたチケットを表示します。[最後のチケット（Last Ticket(s)）] 列のチケット ID をクリックして、チケットの詳細を表示し、そのチケットに移動できます。外部チケット管理システムへのリンクが設定されている場合は、チケットの詳細からそのシステムに移動することもできます（[チケット管理（Ticket Management）]ページを参照）。
[クエリ（Query）] ボタン	ポリシークエリを実行します。実行すると、ルールを評価して、効果が得られない削除可能なルールを特定できます。ポリシー クエリー レポートの生成を参照してください。
[Find and Replace] ボタン（双眼鏡アイコン）	テーブル内でのルールの検索と変更を容易にするために、IP アドレスやポリシー オブジェクト名などのルール テーブルの値を検索します。ルール テーブルの項目の検索と置換を参照してください。
[Up] ボタン	選択したルールをテーブル内で 1 行上に移動します。
[Down] ボタン	選択したルールをテーブル内で 1 行下に移動します。
[追加（Add）] ボタン	新しいルールを作成できる [Add Zone-based Firewall Rule] ダイアログボックスを開きます。
[編集（Edit）] ボタン	テーブル内の選択したルールの編集に使用します。[Edit Zone-based Firewall Rule] ダイアログボックスを開きます。
[削除（Delete）] ボタン	選択したルールをテーブルから削除します。

ゾーンベースのファイアウォール ルールの追加と編集

[Add Zone based Firewall Rule]/[Edit Zone based Firewall Rule] ダイアログボックスを使用して、Cisco IOS および ASR デバイスに対するゾーンベースのファイアウォール ルールを追加および編集します。

ナビゲーション パス

[Zone-based Firewall Rules] ページ （78 ページ）から、[列の追加（Add Row）] ボタンをクリックするか、または行を選択して [行の編集（Edit Row）] ボタンをクリックします。

関連項目

- ゾーンベースのファイアウォール ルールについて （3 ページ）
- ゾーンベースのファイアウォール ルールの設定 （67 ページ）
- ゾーンベースのファイアウォールルールの追加 （16 ページ）

フィールド リファレンス

表 *23 : [Add Zone based Firewall Rule]* および *[Edit Zone based Firewall Rule]* ダイアログボックス

要素	説明
ルールの有効化（Enable Rule）	選択されている場合は、設定が生成および展開されたあとでルールがデバイスでイネーブルになります。ルールを削除せずにディセーブルにするには、このオプションの選択を解除します。
トラフィック	このルールが適用されるトラフィック フローを定義します。
一致（Match）	一致したトラフィックを許可するか拒否するかどうかを選択します。このオプションの詳細については、ゾーンベースのファイアウォールルールの Permit/Deny とアクションとの関係について （9 ページ）を参照してください。
ソース	このルールのトラフィック ソースを提供します。ネットワークまたはセキュリティ グループになります。次の 1 つ以上のタイプのソースに対して、値またはオブジェクト名を入力するか、オブジェクトを選択できます。 （注） これらのフィールドのいずれかに、 項目をカンマで区切って、1 つ以上の値を入れます。 • ネットワーク – さまざまなネットワーク、ホスト、および IP アドレスの定義を、個別に、またはオブジェクトとして指定できます。「All-Address」オブジェクトは、ルールを特定のホストまたはネットワークに制限しません。 これらの定義の詳細については、ネットワーク/ホストオブジェクトについておよびポリシー定義中の IP アドレスの指定を参照してください。 （注） バージョン 4.21 以降、Cisco Security Manager は、すべてのアグリゲーション サービス ルータ、統合サービスルータ、組み込みサービスルータ、および Cisco IOS ソフトウェアで動作するすべてのデバイスについて、バグ修正または拡張機能のサポートを含むサポート全体を終了します。 各仕様を他の仕様と組み合わせて、トラフィックの一致をすべての定義を含むフローのみに制限します。たとえば、指定された送信元アドレス範囲内から発信された指定されたユーザトラフィックです。

要素	説明
宛先	このルールのトラフィックの宛先を指定します。ネットワークまたはセキュリティグループにすることができます。次の1つ以上のタイプのソースに対して、値またはオブジェクト名を入力するか、オブジェクトを選択できます。 （注） これらのフィールドのいずれかに、 項目をカンマで区切って、1 つ以上の値を入れます。 • ネットワーク – さまざまなネットワーク、ホスト、および IP アドレスの定義を、個別に、またはオブジェクトとして指定できます。「All-Address」オブジェクトは、ルールを特定のホストまたはネットワークに制限しません。 これらの定義の詳細については、ネットワーク/ホストオブジェクトについておよびポリシー定義中の IP アドレスの指定を参照してください。 （注） バージョン 4.21 以降、Cisco Security Manager は、すべてのアグリゲーション サービス ルータ、統合サービスルータ、組み込みサービスルータ、および Cisco IOS ソフトウェアで動作するすべてのデバイスについて、バグ修正または拡張機能のサポートを含むサポート全体を終了します。 各仕様を他の仕様と組み合わせて、トラフィックの一致をすべての定義を含むフローのみに制限します。たとえば、指定された送信元アドレス範囲内から発信された指定されたユーザトラフィックです。
サービス	このルールで照合されるトラフィックのタイプを定義するサービスを指定します。サービス オブジェクトおよびサービス タイプの任意の組み合わせ（通常はプロトコルとポートの組み合わせ）をカンマで区切って入力できます。このオプションの詳細については、ゾーンベースのファイアウォール ルールの Services と Protocols の関係について （13 ページ）を参照してください。 サービスを入力する場合は、有効な値の入力を求められます。[Select] をクリックして、リストからサービスを選択することもできます。サービスを指定する方法の詳細については、サービスとサービス オブジェクトおよびポート リスト オブジェクトの理解と指定を参照してください。
From Zone To Zone	基本的なゾーンベースのファイアウォール ルールは単方向です。つまり、2 つのゾーン間で一方向にだけ移動するトラフィック フローを定義します。 このルールのトラフィックフローが発信されるゾーンを入力または選択し、トラフィックが流れる先のゾーンを入力または選択します。
[Advanced] ボタン	時間範囲オプションを選択できる [Advanced Options] ダイアログボックスを開きます。 ゾーンベースのファイアウォール ルール：[Advanced Options] ダイアログボックス （87 ページ）を参照してください。
アクション	このルールと一致するトラフィックに適用されるアクション。目的のアクションを選択します。

要素	説明
[Action]：[Drop]、[Drop and Log]、[Pass]、[Pass and Log]	• [ドロップ（Drop）]：指定したサービスに対するすべてのパケットをサイレントにドロップします。すべてのトラフィックに適用されるデフォルト アクション。 • [ドロップアンドログ（Drop and Log）]：一致したトラフィックは、記録され、ドロップされます。 • [パス（Pass）]：ルータは、一致したパケットを[送信元ゾーン（From Zone）]から[宛先ゾーン（To Zone）]に転送します。リターン トラフィックは認識されないため、リターン トラフィック用に追加のルールを指定する必要があります。このオプションは、IPsec で符号化されたトラフィックなどのプロトコルにだけ役立ちます。 • [パスアンドログ]：トラフィックが記録され、転送されます。 これらのアクションについては、[プロトコル（Protocol）] テーブルの横の [選択（Select）] ボタンをクリックして [Protocol Selector] ダイアログボックス （89 ページ）を開くことにより、照合する 1 つ以上のプロトコルを選択できます。ただし、これは必須ではありません。[Protocol] テーブルを空のままにして、[Sources]、[Destinations]、および [Services] パラメータに基づいてトラフィックを渡すかドロップできます。実際には、これらは標準アクセス ルールです。 [Protocol Selector] ダイアログボックスでは、選択したプロトコルの Port Application Mapping（PAM; ポートアプリケーションマッピング）パラメータを編集できる [Configure Protocol] ダイアログボックス （90 ページ）にもアクセスできます。 （注） ログオプションによって、システム ログ メッセージが生成されます。これらのメッセージをキャプチャするように syslog ロギングが設定されていることを確認する必要があります。

要素	説明
[Action]：[Inspect]	[検査（Inspect）]は状態に基づくトラフィック制御を提供します。デバイスは、TCP および UDP トラフィックに関する接続またはセッション情報を維持するため、接続要求に対するリターントラフィックが許可されます。 選択したレイヤ 4（TCP、UDP）プロトコルおよびレイヤ 7（HTTP、IMAP、インスタントメッセージング、およびピアツーピア）プロトコルに基づいたパケット インスペクションを適用する場合、このオプションを選択します。選択したプロトコルの PAM も編集でき、ディープ パケット インスペクション（DPI）を設定して、レイヤ 7 プロトコルの追加のプロトコル関連情報を提供できます。詳細については、ゾーンベースのファイアウォール ポリシーのインスペクション マップの設定 （19 ページ）を参照してください。 **1.** [プロコトル（Protocol）]テーブルの横の[選択（Select）]ボタンをクリックして [Protocol Selector] ダイアログボックス （89 ページ）を開くことにより、インスペクションに対して 1 つ以上のプロトコルを選択できます。 **2.** [Protocol Selector] ダイアログボックスでは、カスタム プロトコルを作成し、選択したプロトコルの PAM および DPI パラメータを編集できる [Configure Protocol] ダイアログボックス （90 ページ）にもアクセスできます。 **3.** [検査パラメータ（Inspect Parameters）]：このフィールドにインスペクション パラメータ マップの名前を入力するか、または [選択（Select）] を選択してリストから選択することで、カスタマイズされた一連の接続、タイムアウト、およびその他の設定を適用できます。選択リスト ダイアログボックスから新しいインスペクション パラメータ マップを作成することもできます。詳細については、インスペクション パラメータ マップの設定 （40 ページ）を参照してください。 インスペクション パラメータ マップを指定しない場合、デフォルト設定が使用されます。

要素	説明
[Action]：[Content Filter]	[コンテンツフィルタ（Content Filter）] では、指定されたパラメータまたはポリシーマップに基づく URL フィルタリングが提供されます。ルータが HTTP 要求を代行受信し、プロトコル関連の検査を実行します。また、任意で、要求を許可するかブロックするかを決定するためにサードパーティ製サーバに接続します。WebFilter パラメータ マップを提供できます。このマップにより、ローカル URL リスト、および外部 SmartFilter（以前の N2H2）や Websense サーバからの情報に基づくフィルタリングを定義します。または、ローカル、N2H2、Websense、または Trend Micro フィルタリング データにアクセスする WebFilter ポリシー マップを提供できます。 1. アクションとして [コンテンツフィルタ（Content Filter）] が選択されている場合は、HTTP がプロトコルとして指定されます。[Configure] をクリックして、HTTP PAM 設定を編集し、HTTP DPI マップを適用できる [Configure Protocol] ダイアログボックス （90 ページ）を開くことができます。 2. [ウェブフィルタパラメータマップ（WebFilter Parameter Map）] または [ウェブフィルタポリシーマップ（WebFilter Policy Map）] を選択し、適切なマップの名前を指定します。適切な [Select] ボタンをクリックしてリストからマップを選択できます。選択リスト ダイアログボックスから新しいマップを作成することもできます。これらのマップの設定の詳細については、ゾーンベースのファイアウォール ポリシーのコンテンツ フィルタリング マップの設定 （48 ページ）を参照してください。 3. [検査パラメータ（Inspect Parameters）]：このフィールドにインスペクション パラメータ マップの名前を入力するか、または [選択（Select）] を選択してリストから選択することで、カスタマイズされた一連の接続、タイムアウト、およびその他の設定を適用できます。選択リスト ダイアログボックスから新しいインスペクション パラメータ マップを作成することもできます。詳細については、インスペクション パラメータ マップの設定 （40 ページ）を参照してください。 インスペクション パラメータ マップを指定しない場合、デフォルト設定が使用されます。
説明	（任意）ルール テーブルを表示するときにルールを識別するのに役立つ最大 1024 文字の説明を入力できます。
カテゴリ	（任意）ルールにカテゴリを割り当てて、ルールとオブジェクトの整理および識別に役立てることができます。カテゴリ オブジェクトの使用 を参照してください。

ゾーンベースのファイアウォール ルール：[Advanced Options] ダイアログボックス

ゾーンベースのファイアウォール ルールの [Advanced Options] ダイアログボックスを使用して、特定の時間範囲情報をゾーンベースのファイアウォール ルールに適用します。

ナビゲーション パス

[ゾーンベースのファイアウォールルールの追加（Add Zone based Firewall Rule）]/[ゾーンベースのファイアウォールルールの編集（Edit Zone based Firewall Rule）] ダイアログボックスの [トラフィック（Traffic）] セクションで、[詳細設定（Advanced）] ボタンをクリックします。

関連項目

- ゾーンベースのファイアウォール ルールの追加と編集 （82 ページ）
- ゾーンベースのファイアウォール ルールについて （3 ページ）

フィールド リファレンス

表 *24 : [Advanced Options]* ダイアログボックス

要素	説明
時間範囲（Time Range）	この機能では、このゾーンベースのファイアウォール ルールがアクティブになる期間を定義できます。時間範囲を指定しない場合は、ルールが即時に、そして常にアクティブになります。 時間範囲オブジェクトの名前を入力するか、[選択（Select）] をクリックして [時間範囲セレクタ（Time Ranges Selector）] ダイアログボックスのリストから選択します。このダイアログボックスで、時間範囲オブジェクトを作成および編集できます。詳細については、時間範囲オブジェクトの設定を参照してください。
オプション	この機能では、このゾーンベースのファイアウォール ルールに initial-packet-fragment または established-connection 制限を適用できます。次のいずれかのオプションを選択します。 • [なし（None）]：packet-fragment または established-connection 制限は適用されません。 • [フラグメント（Fragment）]：選択されている場合は、ルールが初期以外のパケットフラグメントに適用されます。フラグメントはルールに従って許可または拒否されます。ホワイトペーパー『Access Control Lists and IP Fragments』に、ゾーンベースのファイアウォールルールにも関連する追加情報が記載されています。 • [確立済み（Established）]：TCP プロトコルの場合にだけ、確立済みの接続を要求します。TCP データグラムに ACK または RST 制御ビットが設定されている場合に一致します。一致しないケースは、接続を形成する初期 TCP データグラムです。

[Protocol Selector] ダイアログボックス

[Protocol Selector] ダイアログボックスを使用して、ゾーンベースのファイアウォール ルールのトラフィック定義の一部として、1 つ以上の通信プロトコルを指定します。

[Protocol Selector] ダイアログボックスでは、カスタム プロトコルの作成および既存のプロトコルの Port Application Mapping（PAM; ポート アプリケーション マッピング）パラメータの編集に使用できる [Configure Protocol] ダイアログボックスにもアクセスできます。[Configure Protocol] ダイアログボックスでは、特定のプロトコルの詳細インスペクション ポリシー マップ、およびプロトコル情報パラメータ マップも選択します。詳細については、[Configure Protocol] ダイアログボックス （90 ページ）を参照してください。

ナビゲーション パス

[Protocol Selector] ダイアログボックスには、[Add Zone based Firewall Rule]/[Edit Zone based Firewall Rule] ダイアログボックス（ゾーンベースのファイアウォール ルールの追加と編集（82 ページ）で説明しています）からアクセスできます。いずれかのダイアログボックスで、[Content Filter] 以外のアクションを選択し、[Protocol] テーブルの横の [Select] ボタンをクリックします。

[Zone Based Firewall Rules] テーブルの任意のエントリの [Inspected Protocol] カラムを右クリックしてから [Edit Protocols] を選択することでも、[Protocol Selector] ダイアログボックスを開くことができます。

関連項目

- ゾーンベースのファイアウォール ルールについて （3 ページ）
- ゾーンベースのファイアウォール ルールの追加と編集 （82 ページ）
- ポリシーのオブジェクトの選択
- [Configure Protocol] ダイアログボックス （90 ページ）

表 *25 : [Protocol Selector]* ダイアログボックス

要素	説明
Available Protocols	ゾーンベースのファイアウォール ルールに対して選択できるプロトコルのリスト。 **ヒント** [Selected Protocols] カラムの下の [Create] ボタンをクリックして [Configure Protocol] ダイアログボックス （90 ページ）を開くことにより、カスタム プロトコルを作成できます。

要素	説明
Selected Protocols	このゾーンベースのファイアウォール ルールに対して選択したプロトコルのリスト。 ヒント [Selected Protocols] カラムで強調表示されているプロトコルの Port Application Mapping（PAM; ポート アプリケーション マッピング）設定を編集できます。[Selected Protocols] カラムの下の [Edit] ボタンをクリックして [Configure Protocol] ダイアログボックス（90 ページ）を開きます。
[>>] ボタン	強調表示されているプロトコルを [Available Protocols] カラムから [Selected Protocols] カラムに移動します。Shift を押しながらのクリックおよび Ctrl を押しながらのクリックという標準機能を使用して、複数のプロトコルを選択できます。
[<<] ボタン	強調表示されているプロトコルを [Selected Protocols] カラムから [Available Protocols] カラムに戻します。Shift を押しながらのクリックおよび Ctrl を押しながらのクリックという標準機能を使用して、複数のプロトコルを選択できます。

[Configure Protocol] ダイアログボックス

特定のプロトコル オブジェクトの選択によって、Port Application Mapping（PAM; ポート アプリケーション マッピング）パラメータ（レイヤ 4 プロトコルとポート、およびオプションで特定のネットワークとホスト）を定義するパケット インスペクションをゾーンベースのファイアウォール ルールに設定できます。レイヤ 7（HTTP、IMAP、Instant Messaging、およびピアツーピア）プロトコルには、そのプロトコルに固有の詳細パケット インスペクション ポリシーも含めることができます。ゾーンベースのファイアウォール ルールの定義中のプロトコルの選択については、ゾーンベースのファイアウォール ルールの追加と編集 （82 ページ）を参照してください。

[Configure Protocol] ダイアログボックスは、ゾーンベースのファイアウォール ルールで使用する既存のプロトコル定義の編集、およびカスタム定義の作成に使用されます。たとえば、プロトコルで一部またはすべてのネットワークにデフォルト ポートを使用しない場合は、異なるポート マッピングを設定できます。

ナビゲーション パス

[Configure Protocol] ダイアログボックスには、[Protocol Selector] ダイアログボックス （89 ページ）から次のようにアクセスします。

- [Selected Protocols] リストの下にある [Create]（+）ボタンをクリックして、新規プロトコルを作成する。
- [Selected Protocols] リストでプロトコルを選択し、[Edit]（鉛筆）ボタンをクリックしてそのプロトコルを編集する。

関連項目

- ゾーンベースのファイアウォール ルールについて （3 ページ）
- ゾーンベースのファイアウォールルールの追加 （16 ページ）
- [Protocol Selector] ダイアログボックス （89 ページ）

表 *26 : [Configure Protocol]* ダイアログボックス

要素	説明
Protocol Name	選択したプロトコルの名前。カスタム プロトコルを作成している場合は、最大 19 文字の名前を入力できます。カスタム プロトコル名は **user-** から始まる必要があります。
Enable Signature	このオプションは、ピアツーピア（eDonkey、FastTrack、Gnutella、Kazaa2）プロトコルを編集する場合にだけ使用できます。 このオプションをイネーブルにすると、Network-Based Application Recognition（NBAR; ネットワークベース アプリケーション認識）ヒューリスティックがトラフィックに適用され、特定の P2P アプリケーション アクティビティを示す「telltale」が検出されます。これらの telltale には、ポートホッピング、およびトラフィック検出を回避するためのアプリケーション動作のその他の変更が含まれます。 （注） このレベルのトラフィック インスペクションは、CPU 使用率の増加およびネットワーク スループットの低減を伴います。
Deep Inspection	このオプションは、H.323、HTTP、IM（AOL、ICQ、MSN Messenger、Windows Messenger、および Yahoo Messenger）、IMAP、P2P（eDonkey、FastTrack、Gnutella、Kazaa2）、POP3、SIP、SMTP、Sun RPC プロトコルを編集する場合、およびゾーンベースのファイアウォールルールに対して [検査（Inspect）] アクションが選択されている場合にだけ使用可能です。 選択したプロトコルで使用するインスペクション ポリシー マップの名前を入力または選択します。これらのポリシー マップの詳細については、ゾーンベースのファイアウォール ポリシーのインスペクション マップの設定 （19 ページ）を参照してください。

要素	説明
Protocol Info	このオプションは、インスタント メッセージング（AOL、ICQ、MSN Messenger、Windows Messenger、および Yahoo Messenger）と Stun-ice プロトコルを編集する場合だけ使用可能です。 選択したプロトコルで使用するプロトコル情報パラメータ マップの名前を入力または選択します。これらのパラメータ マップでは、これらのアプリケーションと対話する DNS サーバを定義します。このパラメータ マップにより、Instant Messaging（IM; インスタント メッセージング）アプリケーション エンジンが IM トラフィックを認識し、その IM アプリケーションの設定済みポリシーを適用できます。 これらのパラメータ マップの詳細については、プロトコル情報パラメータ マップの設定 （43 ページ）を参照してください。
Port Application Mapping	これらのオプションでは、選択したプロトコルの Port Application Mapping（PAM; ポート アプリケーション マッピング）パラメータをカスタマイズできます。
プロトコル	このマッピングのトランスポート プロトコルを選択します。 • TCP/UDP • [TCP] • UDP
ポート	単一のポート番号、複数のポート番号、またはポートの範囲（60000-60005 など）を任意に組み合わせて入力します。複数のエントリを指定する場合は、カンマで区切ります。すでにマッピングされているポートと重複する範囲は指定しないでください。
ネットワーク	このプロトコル/ポート マッピングが特定のネットワークまたはホストだけに対するものである場合は、ネットワークまたはホストの名前または IP アドレス、あるいはネットワーク/ホスト オブジェクトの名前を入力します。[Select] をクリックして、ネットワーク/ホスト セレクタを開くことができます。複数のエントリを指定する場合は、カンマで区切ります。

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