ファイアウォール デバイスでのサービス ポリシールールの設定

ここでは、サービス ポリシールールを設定する方法について説明します。サービス ポリシーを使用すると、一貫した柔軟な方法で、プライオリティ キューイング、アプリケーション インスペクション、Quality of Service（QoS）など、特定のセキュリティ アプライアンス機能を設定できます。たとえば、サービス ポリシーを使用すると、すべての TCP アプリケーションに適用されるタイムアウト コンフィギュレーションではなく、特定の TCP アプリケーションに固有のタイムアウト コンフィギュレーションを作成できます。

サービス ポリシールールについて

サービス ポリシールールには、次の機能が含まれています。

- TCP 接続設定および一般接続設定（TCP ステート バイパスを含む。 TCP ステート バイパスについて （3 ページ）を参照）
- Content Security Control（CSC）
- アプリケーション インスペクション
- 侵入防御サービス
- QoS キューイングおよびポリシング
- ASA CX リダイレクション（ ASA CX について （23 ページ）を参照）
- ASA FirePOWER リダイレクション

- アイデンティティベースのファイアウォール ポリシーのユーザ統計情報

これらの機能の設定オプションは、Cisco Security Manager の 2 つのページ（[プライオリティ キュー（Priority Queues）] および [ルール（Rules）]）にあります。これらのページには、[プラットフォーム（Platform）] > [サービスポリシー（Service Policy）] に移動してアクセスできます。

プライオリティ キューイング

プライオリティキューイングでは、低遅延キューイング（LLQ）プライオリティキューおよび「ベストエフォート」キューの2つのキューがインターフェイスに設定されます。この機能により、音声およびビデオなど、遅延の影響を受けやすいトラフィックを優先して、他のトラフィックより先に送信できます。プライオリティキュー内のパケットは、常にベストエフォート キュー内のパケットより先に送信されます。

キューは無限大ではないため、いっぱいになってオーバーフローすることがあります。キューが一杯になると、それ以上はパケットをキューに格納することができなくなり、パケットはドロップされます。これは「テールドロップ」と呼ばれます。テールドロップを最小限に抑えるには、キューのバッファサイズを大きくします。送信キューに入れることのできるパケットの最大数も微調整できます。これらのオプションにより、プライオリティキューイングの遅延およびロバストネスを制御できます。

プライオリティ キューイングは Quality of Service（QoS）の機能です。Security Manager では、プライオリティ キュー サイズおよび送信キュー サイズを [Priority Queues] ページ （4 ページ）で管理します。一方、トラフィック クラスのプライオリティ キューイングは、Service Policy (MPC) Rule ウィザードの [QoS] タブにあるオプションで設定します。このウィザードには、[サービスポリシールール（Service Policy Rules）] ページ （6 ページ）からアクセスします。

アプリケーション インスペクションおよび QoS

アプリケーションの中には、セキュリティ アプライアンスによる特別な処理を必要とするものがあります。このため、固有のアプリケーション インスペクション エンジンが用意されています。特に、ユーザ データ パケットに IP アドレス情報を埋め込むアプリケーション、または動的に割り当てられるポートでセカンダリ チャネルを開くアプリケーションなどでは特別な検査が必要です。

アプリケーションインスペクションは、デフォルトで多くのプロトコルに対してイネーブルになっていますが、ディセーブルになっているプロトコルもあります。多くの場合、アプリケーション インスペクション エンジンがトラフィックをモニタするポートは変更可能です。

アプリケーション インスペクション エンジンはネットワーク アドレス変換（NAT）と連動し、埋め込まれたアドレス情報の位置を特定できます。このことにより、これらの埋め込みアドレスを NAT で変換し、変換によって影響を受けるチェックサムまたはその他のフィールドを更新できるようになります。

サービス ポリシー ルールでは、セキュリティ アプライアンスで処理されるさまざまなタイプのトラフィックに、特定タイプのアプリケーションインスペクションを適用する方法を定義し

ます。ルールは、特定のインターフェイスに適用するか、またはすべてのインターフェイスにグローバルに適用できます。

これらのルールにより、Cisco IOS ソフトウェアの Quality of Service（QoS）CLI と同じ仕組みで、セキュリティ アプライアンスの機能を設定できます。たとえば、サービス ポリシールールを使用して、トラフィックを識別する基準の 1 つとして IP precedence を追加し、レートを制限できます。すべての TCP アプリケーションに適用されるタイムアウト設定を作成する一方で、特定の TCP アプリケーションに固有のタイムアウト設定を作成することもできます。

アプリケーション インスペクションを適用するトラフィックのタイプを定義するには、トラフィック一致基準を使用します。たとえば、ポート 23 の TCP トラフィックは Telnet トラフィック クラスに分類できます。すると、トラフィック クラスを使用して接続制限を適用できます。

トラフィック一致基準は、単一のインターフェイスに複数割り当てることができます。ただし、パケットが一致するのは、特定のサービス ポリシールール内の最初の基準だけです。

TCP ステート バイパスについて

デフォルトでは、ASA または FWSM を通過するすべてのトラフィックは、アダプティブ セキュリティ アルゴリズムを使用して検査され、セキュリティポリシーに基づいて、通過を許可されるか、またはドロップされます。デバイスは、各パケットの状態をチェックして（新規の接続か確立済み接続であるかを判定し）、そのパケットをセッション管理パス（新規接続の SYN パケットの場合）、高速パス（確立済みの接続の場合）、またはコントロールプレーンパス（高度なインスペクションの場合）に割り当てることによって、ファイアウォールのパフォーマンスを最大限に高めます。

（注） TCP ステート バイパスは、FWSM 3.2+ デバイスおよび ASA 8.2+ デバイスだけで使用可能です。

高速パスの既存の接続に一致する TCP パケットは、セキュリティ ポリシーをすべて再チェックしなくてもアプライアンスを通過できます。この機能によってパフォーマンスは最大になります。ただし、SYN パケットを使用して高速パスでセッションを確立する方式、および高速パス内で発生するチェック（TCP シーケンス番号など）は、接続のアウトバウンドおよびインバウンド フローが同じデバイスを通過する必要があり、非対称ルーティング環境に該当しません。

たとえば、新規接続がセキュリティ デバイス 1 に割り当てられるとします。SYN パケットはセッション管理パスを通過し、接続のエントリが高速パステーブルに追加されます。この接続の後続パケットがデバイス 1 を通過した場合、高速パス内のエントリに一致するのでこのパケットは送信されます。ただし、後続パケットがデバイス 2 に向かった場合、SYN パケットはこのデバイスのセッション管理パスを通過していないので、高速パス内に接続のエントリは存在せず、パケットはドロップされます。

したがって、アップストリームルータに非対称ルーティングが設定されていて、トラフィックが 2 つのセキュリティデバイスを通過することがある場合は、これらの特定のトラフィックフローの TCP ステートバイパスをイネーブルにします。TCP ステート バイパスは、高速パスで

のセッションの確立方法を変更し、高速パスのインスペクションをディセーブルにします。この場合、TCP トラフィックは UDP 接続を処理するときと同じように処理されます。つまり、指定されたネットワークに一致する SYN パケット以外のパケットがセキュリティ デバイスに送信され、高速パス エントリが存在しない場合、そのパケットは高速パス内で接続を確立するためにセッション管理パスを通過します。いったん高速パスに入ると、トラフィックは高速パスのインスペクションをバイパスします。

サポートされない機能

TCP ステート バイパスをイネーブルにする場合、次の機能はサポートされません。

- アプリケーション インスペクション：アプリケーション インスペクションでは、インバウンドおよびアウトバウンドのトラフィックが同じセキュリティデバイスを通過する必要があります。したがって、TCP ステート バイパスではアプリケーション インスペクションがサポートされていません。
- AAA 認証セッション：あるセキュリティ デバイスでユーザを認証した場合、トラフィックが他のセキュリティデバイスを経由すると、そのデバイスではユーザが認証されていないため、トラフィックは拒否されます。
- TCP 代行受信、最大初期接続の制限、TCP シーケンス番号のランダム化：TCP ステート バイパスをイネーブルにした場合、デバイスは接続の状態を追跡しません。したがって、これらの機能は適用できません。
- Cisco Content Security and Control Security Services Module（CSC SSM）：TCP ステート バイパスで SSM および SSC 機能は使用できません。

NAT との互換性

変換セッションはセキュリティ デバイスごとに独立して確立されるため、スタティック NAT は必ず TCP ステート バイパス トラフィックの両方のデバイスに設定します。ダイナミック NAT を使用する場合、デバイス 1 のセッションに選択されるアドレスと、デバイス 2 のセッションに選択されるアドレスは異なります。

関連項目

- サービス ポリシールールについて （1 ページ）

[Priority Queues] ページ

プライオリティ キューにより、ネットワークのトラフィックにプライオリティを付ける方法を定義できます。パケットの特性に基づいてプライオリティの異なるキューにトラフィックを格納する、一連のフィルタを定義できます。プライオリティの最も高いキューが最初に処理され、そのキューが空になると、プライオリティが次に高いキューから低いキューへと順番に処理が進みます。

Security Manager では、このページでプライオリティ キュー サイズおよび送信キュー サイズを管理します。一方、トラフィック クラスのプライオリティ キューイングは、Service Policy (MPC) Rule ウィザードの [QoS] タブにあるオプションで設定します。このウィザードには、[サービスポリシールール（Service Policy Rules）] ページ （6 ページ）からアクセスします。

これらのキューを追加および編集するには、[Priority Queue Configuration] ダイアログボックスを使用します。このページの [Priority Queues] テーブルに表示されるフィールドの詳細については、 [Priority Queue Configuration] ダイアログボックス （5 ページ）を参照してください。

（注） プライオリティキューイングは Catalyst 6500 サービスモジュール（ファイアウォール サービス モジュールおよび適応型セキュリティ アプライアンス サービス モジュール）では使用できません。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから [プラットフォーム（Platform）]>[サービスポリシールール（Service Policy Rules）] > [プライオリティキュー（Priority Queues）] 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 [PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [サービスポリシールール（Service Policy Rules）] > [プライオリティキュー（Priority Queues）] を選択します。共有ポリシーセレクタから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。

関連項目

- Insert/Edit Service Policy (MPC) Rule ウィザード （8 ページ）
- サービス ポリシールールについて （1 ページ）
- キューイング パラメータについて

[Priority Queue Configuration] ダイアログボックス

[Priority Queues] ページでプライオリティ キューを定義および編集するには、[Priority Queue Configuration] ダイアログボックスを使用します。

（注） プライオリティキューイングは Catalyst 6500 サービスモジュール（ファイアウォール サービス モジュールおよび適応型セキュリティ アプライアンス サービス モジュール）では使用できません。

ナビゲーション パス

[Priority Queue Configuration] ダイアログボックスを開くには、[Priority Queues] ページ （4 ページ）で [Add Row] ボタンまたは [Edit Row] ボタンをクリックします。

関連項目

- Insert/Edit Service Policy (MPC) Rule ウィザード （8 ページ）
- サービス ポリシールールについて （1 ページ）
- キューイング パラメータについて

フィールド リファレンス

表 1 : [Priority Queue Configuration] ダイアログボックス

要素	説明
Interface Name	このルールが適用されるインターフェイスを指定します。インターフェイス名を入力するか、または[Select]をクリックして使用可能なインターフェイスを選択できます。
キュー制限（Queue Limit）	プライオリティ キューに格納できるパケットの最大数を入力します。この最大数を超えると、データがドロップされます。この制限には、0 ～ 2048 パケットの範囲を指定する必要があります。
Transmission Ring Limit	送信キューに格納できるパケットの最大数を入力します。これで送信キューを微調整すると遅延を短縮でき、送信ドライバを介してパフォーマンスを向上できます。 PIX デバイスの場合、この値の範囲は 3 ～ 128 パケットです。バージョン 7.2 よりも前の ASA の場合は、この制限を 3 ～ 256 パケットの範囲で指定します。また、バージョン 7.2 以降を実行している ASA の場合は、3 ～ 512 パケットの範囲で指定します。

[サービスポリシールール（Service Policy Rules）] ページ

新しいサービスポリシールールを定義し、既存のサービスポリシールールを編集または削除するには、[サービスポリシールール（Service Policy Rules）] ページを使用します。

サービスポリシールールの設定は、次の 3 つのタスクで構成されています。

1. **サービスポリシーの設定**。サービス ポリシーを作成し、そのサービス ポリシーが適用されるインターフェイスを決定します。詳細については、手順 1：サービス ポリシーの設定（8 ページ）を参照してください。

2. **トラフィッククラスの設定**。サービス ポリシーが適用されるトラフィックを識別する基準を指定します。詳細については、手順 2：トラフィック クラスの設定 （9 ページ）を参照してください。

3. **アクションの設定**。情報またはリソースを保護するために実行するアクション、またはこのサービス ポリシーで指定されたトラフィックの QoS 機能を実行するアクションを指定します。詳細については、手順 3：MPC アクションの設定 （10 ページ）を参照してください。

この 3 つのタスクの実行には、Insert/Edit Service Policy (MPC) Rule ウィザード （8 ページ）を使用します。このページの [サービスポリシールール（Service Policy Rules）] テーブルに表示されるフィールドの詳細については、個々のタスクのトピックを参照してください。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから [プラットフォーム（Platform）]>[サービスポリシールール（Service Policy Rules）] > [プライオリティキュー（Priority Queues）] 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 [PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [サービスポリシー（Service Policy）] > [ルール（Rules）] を選択します。共有ポリシーセレクタから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。

ASA CX 認証プロキシの設定

[サービスポリシールール（Service Policy Rules）] テーブルの下にある [CXSC認証プロキシ（CXSC Auth Proxy）] ボタンをクリックすると、ASA CX 認証プロキシの設定 （24 ページ）で説明されている [CXSC認証プロキシ設定の追加/編集（Add/Edit CXSC Auth Proxy Configuration）] ダイアログボックスが開きます。

[CXSC認証プロキシ（CXSC Auth Proxy）] ボタンには、デバイスビューの [サービスポリシールール（Service Policy Rules）] テーブルの下でのみアクセスできます。ポリシービューには表示されません。

（注） Security Manager は、ASA CX セキュリティ サービス プロセッサ（SSP）を参照する場所の一部で「CXSC」を使用します。

関連項目

- サービス ポリシールールについて （1 ページ）
- 標準のルール テーブルに関する内容：
  - ルール テーブルの使用
  - テーブルのフィルタリング

- テーブル カラムおよびカラム見出しの機能

Insert/Edit Service Policy (MPC) Rule ウィザード

[サービスポリシールール（Service Policy Rules）]ページでサービスポリシールールを追加および編集するには、Insert/Edit Service Policy (MPC) Rule ウィザードを使用します。Insert/Edit Service Policy (MPC) Rule ウィザードにより、次の手順が示されます。

- 手順 1：サービス ポリシーの設定 （8 ページ）
- 手順 2：トラフィック クラスの設定 （9 ページ）
- 手順 3：MPC アクションの設定 （10 ページ）

（注） 「MPC」は現在モジュラー ポリシー フレームワークを指します。詳細については、「モジュラ ポリシー フレームワークの使用」を参照してください。

ナビゲーション パス

[サービスポリシールール（Service Policy Rules）] ページ （6 ページ）で [Add Row or Edit Row] ボタンをクリックして、Insert/Edit Service Policy (MPC) Rule ウィザードを開きます。

手順 1：サービス ポリシーの設定

サービスポリシー（MPC）ルールの挿入/編集（Insert/Edit Service Policy (MPC) Rule）ウィザードを使用してサービスポリシールールを設定する最初の手順は、ルールのイネーブル化とルールを適用するインターフェイスの指定です。

ナビゲーション パス

[サービスポリシールール（Service Policy Rules）] ページ （6 ページ）で [Add Row or Edit Row] ボタンをクリックして、Insert/Edit Service Policy (MPC) Rule ウィザードを開きます。

関連項目

- 手順 2：トラフィック クラスの設定 （9 ページ）
- 手順 3：MPC アクションの設定 （10 ページ）

表 *2 : Insert/Edit Service Policy (MPC) Rule* ウィザード - 手順 *1*：サービス ポリシーの設定

要素	説明
Enable The Current MPC Rule	このサービス ポリシールールをイネーブルにするには、このチェックボックスをオンにします。現時点でルールを定義しておき、あとからデバイスに展開する場合は、このオプションの選択を解除します。
カテゴリ	ルールをカテゴリに割り当てるには、このリストからカテゴリを選択します。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。詳細については、カテゴリ オブジェクトの使用を参照してください。
説明	（任意）サービス ポリシールールの説明を入力します。
Global - Applies to All Interfaces	すべてのインターフェイスにグローバルにルールを適用するには、このオプションを選択します。このオプションは、アクセス リストを使用して、送信元または宛先 IP アドレスに基づいてトラフィックを照合する機能とは互換性がありません。
インターフェイス	特定のインターフェイスまたはインターフェイスのグループ（あるいはインターフェイス ロール）にルールを適用するには、このオプションを選択したあと、インターフェイスまたはインターフェイス オブジェクトの名前を入力または選択します。 この選択は、アクセス リストを使用して、送信元または宛先 IP アドレスに基づいてトラフィックを照合する場合は必須です。 （注） インターフェイス固有のルールは、指定した機能のグローバル サービス ポリシーに優先します。たとえば、FTP インスペクションを行うグローバル ポリシーと、TCP 接続制限を行うインターフェイス ポリシーが設定されている場合、インターフェイスには FTP インスペクションおよび TCP 接続制限がどちらも適用されます。これに対し、FTP インスペクションのグローバル ポリシーと、FTP インスペクションのインターフェイス ポリシーがある場合は、インターフェイス ポリシーの FTP インスペクションだけがインターフェイスに適用されます。

手順 2：トラフィック クラスの設定

Insert/Edit Service Policy (MPC) Rule ウィザードを使用してサービスポリシールールを設定する 2 番めの手順は、ルールを適用するトラフィック クラスの指定です。

このルールのトラフィックを照合するクラスを指定します。

- [class-defaultをトラフィック クラスとして使用（Use class-default As The Traffic Class）]：このサービスポリシーでトラフィック クラス class-default を使用するには、このオプションを選択します。class-default トラフィック クラスは、すべてのトラフィックを照合します。

- [トラフィッククラス（Traffic Class）]：特定のトラフィッククラスにこのルールを適用するには、このオプションを選択します。定義済みのトラフィッククラスの名前を入力するか、または [選択（Select）] をクリックしてトラフィックフローセレクタからトラフィッククラスを選択します。

また、トラフィックフローセレクタで [作成（Create）] または [編集（Edit）] ボタンをクリックし、「オンザフライ」でトラフィックフローを定義または編集できます（トラフィックフローは Policy Object Manager の [トラフィックフロー（Traffic Flows）] ページでも作成および編集できます）。詳細については、トラフィック フロー オブジェクトの設定　（25 ページ）を参照してください。

関連項目

- 手順 1：サービス ポリシーの設定　（8 ページ）
- 手順 3：MPC アクションの設定　（10 ページ）

手順 3：MPC アクションの設定

Insert/Edit Service Policy (MPC) Rule ウィザードの 3 番めの手順は、ルールに関する IPS、CXSC、FirePOWER、接続設定、QoS、CSC、ユーザー統計情報、ScanSafe Web セキュリティ、および NetFlow のパラメータの指定です。各パラメータセットは、別々のタブ付きパネルに表示されます。

関連項目

- 手順 1：サービス ポリシーの設定　（8 ページ）
- 手順 2：トラフィック クラスの設定　（9 ページ）

フィールド リファレンス

***表 3 : Insert/Edit Service Policy (MPC) Rule* ウィザード - 手順 *3*：アクションの設定。**

要素	説明
[Intrusion Prevention] タブ	
Enable IPS for this Traffic	このトラフィック フローの侵入防御をイネーブルまたはディセーブルにします。このチェックボックスをオンにすると、このパネル上の他のパラメータが使用可能になります。 （注）　これらのパラメータは、IPS モジュールが取り付けられている ASA 7.0 以降のデバイスにのみ適用できます。詳細については、ASA デバイスでの IPS モジュールについて　（21 ページ）を参照してください。

要素	説明
IPS Mode	侵入防御の動作モードを選択します。 • [インライン（Inline）]：このモードでは、IPS モジュールをトラフィックフローに直接配置します。IPS 検査対象と認識されたトラフィックは、最初に IPS モジュールに渡されて検査を受けないと、ASA を通過できません。インスペクションの対象と識別されたすべてのパケットが分析されてから通過を許可されるため、このモードが最も安全です。また、IPS モジュールはパケット単位でブロッキング ポリシーを実装できます。ただし、このモードはスループットに影響する可能性があります。 • [無差別（Promiscuous）]：このモードでは、トラフィックの重複ストリームが IPS モジュールに送信されます。このモードの安全性はインライン モードより低くなりますが、トラフィックのスループットにはほとんど影響しません。[Inline] モードとは異なり、[Promiscuous] モードでは IPS モジュールは元のパケットをドロップできません。トラフィックをブロックできるのは、ASA にトラフィックの排除を指示するか、またはアプライアンス上の接続をリセットした場合だけです。 また、IPS モジュールがトラフィックを分析している間、IPS モジュールがそのトラフィックを排除する前に少量のトラフィックが ASA を通過することがあります。
On IPS Card Failure	IPS モジュールが動作不能になった場合に実行するアクションを指定します。次のいずれかを選択します。 • [開く（Open）]：モジュールまたはカードで障害が発生した場合にトラフィックを許可します。 • [閉じる（Close）]：モジュールまたはカードで障害が発生した場合にトラフィックをブロックします。
仮想センサー	追加または編集しているサービスポリシー内の仮想センサーを表示、編集、または削除できるテキストボックス
[CXSC] タブ （注） Cisco Security Manager は、ASA CX セキュリティ サービス プロセッサ（SSP）を参照する場所で「CXSC」を使用します。	

要素	説明
このトラフィックのCXSCの有効化（Enable CXSC For This Traffic）	ASA にインストールされている ASA CX へのトラフィックフローのリダイレクトを有効にするには、このボックスをオンにします。このチェックボックスをオンにすると、このパネル上の他のパラメータが使用可能になります。 （注） これらのパラメータは、ASA CX SSP がインストールされている、バージョン 8.4(4) 以降を実行している ASA 5585-X デバイスおよびバージョン 9.1(1) 以降を実行している ASA 55xx-X デバイスにのみ適用されます。
コンテキストセキュリティカードの障害時（On Context Security Card Failure）	ASA CX が動作不能になった場合に実行するアクションを指定します。次のいずれかを選択します。 • [開く（Open）]：何らかの理由で ASA CX に障害が発生した場合、ASA は、本来なら ASA CX にリダイレクトされるトラフィックを引き続き通過させます。 • [閉じる（Close）]：ASA CX に障害が発生した場合、ASA は、本来なら ASA CX にリダイレクトされるトラフィックをドロップします。
認証プロキシの有効化（Enable Auth Proxy）	認証プロキシを有効にするには、このボックスをオンにします。認証プロキシは、アクティブ認証を ASA CX での ID ポリシーに使用する場合に必要です。オンになっていない場合、認証は実行されません。 （注） 認証プロキシに使用されるポートを変更できます。詳細については、ASA CX 認証プロキシの設定 （24 ページ）を参照してください。
[FirePOWER] タブ	
このトラフィックに対するFirePOWERカードの有効化（Enable FirePOWER Card For This Traffic）	ASA にインストールされている ASA FirePOWER モジュールへのトラフィックフローのリダイレクトを有効にするには、このボックスをオンにします。このチェックボックスをオンにすると、このパネル上の他のパラメータが使用可能になります。 （注） これらのパラメータは、バージョン 9.2(1) 以降を実行している ASA 55xx-X デバイスにのみ適用されます。

要素	説明
FirePOWERカード障害時（On FirePOWER Card Failure）	ASA FirePOWER モジュールが動作不能になった場合に実行するアクションを指定します。次のいずれかを選択します。 • [開く（Open）]：何らかの理由で ASA FirePOWER モジュールに障害が発生した場合、ASA は、本来なら ASA FirePOWER にリダイレクトされるトラフィックを引き続き通過させます。 • [閉じる（Close）]：ASA FirePOWER モジュールに障害が発生した場合、ASA は、本来なら ASA FirePOWER モジュールにリダイレクトされるトラフィックをドロップします。
モニター専用の有効化（Enable Monitor Only）	モジュールをモニタ専用モードに設定します。モニタ専用モードでは、モジュールはデモンストレーションを目的としてトラフィックを処理できますが、その後トラフィックをドロップします。トラフィック転送インターフェイスまたはデバイスを実稼働用に使用することはできません。
[接続設定（Connection Settings）] タブ	
Enable Connection Settings For This Traffic	このトラフィック フローの接続設定をイネーブルまたはディセーブルにします。このチェックボックスをオンにすると、このパネル上の他のパラメータがアクティブになります。[Connection Settings] タブでは、最大接続、初期接続、タイムアウト、およびTCPのパラメータを設定できます。

要素	説明
最大接続数	TCP 接続と UDP 接続の最大数、およびこのトラフィック フローの初期接続の最大数を指定できます。 • [TCP接続とUDP接続の最大数（Maximum TCP & UDP Connections）]：サブネット全体の TCP および UDP の最大同時接続数を指定します。上限は、8.4(5) より前の ASA バージョンの場合は 65,535、ASA 8.4(5) 以降のバージョンの場合は 2,000,000 です。どちらのプロトコルもデフォルトは 0 で、この場合に許可される接続は無制限です。 • [クライアントごとのTCP接続とUDP接続の最大数（Maximum TCP & UDP Connections Per Client）]：ASA/PIX 7.1 以降の場合のみ、クライアント単位で TCP および UDP の最大同時接続数を指定します。ASA 8.4(5) 以降の場合、最大数は 2,000,000 です。 • [最大初期接続数（Maximum Embryonic Connections）]：ASA/PIX 7.0 以降の場合のみ、ホストごとの最大初期接続数を指定します。上限は、8.4(5) より前の ASA バージョンの場合は 65,535、ASA 8.4(5) 以降のバージョンの場合は 2,000,000 です。初期接続とは、送信元と宛先の間で必要になるハンドシェイクを完了していない接続要求のことです。この制限により、TCP 代行受信機能がイネーブルになります。デフォルトは 0 で、この場合の初期接続数は無制限です。TCP 代行受信は、TCP SYN パケットを使用してインターフェイスをフラッディングすることによる DoS 攻撃から内部システムを保護します。初期接続制限を超えると、クライアントからセキュリティ レベルのより高いサーバに送信される TCP SYN パケットが、TCP 代行受信機能によって代行受信されます。検証プロセス中には SYN クッキーが使用され、有効なトラフィックのドロップ量を最小限に抑えることができます。したがって、到達不能なホストからの接続試行がサーバに到達することはありません。この機能は、TCP ステート バイパスがイネーブルになっている場合には適用されません。 • [クライアントごとの最大初期接続数（Maximum Embryonic Connections Per Client）]：ASA/PIX 7.1 以降の場合のみ、クライアント単位で最大初期接続数を指定します。ASA 8.4(5) 以降の場合、最大数は 2,000,000 です。この機能は、TCP ステート バイパスがイネーブルになっている場合には適用されません。

要素	説明
接続タイムアウト数	このトラフィック フローの次の接続タイムアウト設定を指定できます。 • [初期接続タイムアウト（Embryonic Connection Timeout）]：初期接続スロットが解放されるまでのアイドル時間を指定します。接続のタイムアウトを無効にするには、0:00:00 と入力します。デフォルトは FWSM で 20 秒、ASA/PIX デバイスで 30 秒です。 • [ハーフクローズ接続タイムアウト（Half Closed Connection Timeout）]：ハーフクローズ接続スロットが解放されるまでのアイドル時間を指定します。接続のタイムアウトを無効にするには、0:00:00 と入力します。 FWSM の場合、デフォルト値は 20 秒、最大値は 255 秒（4 分 15 秒）です。 ASA 9.1.2 以降のデバイスの場合、最小値は 30 秒です。他のすべての ASA/PIX デバイスの場合、最小値は 5 分です。すべての ASA/PIX デバイスのデフォルト値は 10 分です。 • [アイドル接続タイムアウト（Idle Connection Timeout）]：接続スロットが解放されるまでのアイドル時間を指定します。接続のタイムアウトを無効にするには、0:00:00 と入力します。この期間は 5 分以上にする必要があります。デフォルトは 1 時間です。
Reset Connection Upon Timeout	選択した場合、タイムアウト発生後に接続がリセットされます。ASA/PIX 7.0(4)+ だけで選択可能です。
Detect Dead Connections	デッド接続検出機能をイネーブルにします。ASA/PIX 7.2+ デバイスだけで選択可能です。このオプションを選択すると、次の 2 つのフィールドがイネーブルになります。 • [デッド接続検出タイムアウト（Dead Connection Detection Timeout）]：デッド接続が検出された場合の再試行間隔を指定します。デフォルトは 15 秒です。 • [デッド接続検出再試行数（Dead Connection Detection Retries）]：デッド接続の検出後に実行される再試行の回数を指定します。デフォルトは 5 です。
トラフィックフローアイドルタイムアウト（Traffic Flow Idle Timeout）	トラフィックフローがアイドルになってからフローが切断されるまでの期間を指定します。FWSM 3.2+ だけに適用できます。デフォルトは 1 時間です。

要素	説明
Enable TCP Normalization	TCP 正規化をイネーブルにし、TCP マップ選択オプションをアクティブにします。ASA/PIX 7.0+ だけに適用されます。ただし、TCP ステート バイパスがイネーブルになっている場合には適用されません。
TCP map	TCP 正規化に使用する TCP マップを指定します。TCP マップの名前を入力または選択します。詳細については、TCP マップの設定 （31 ページ）を参照してください。
Randomize TCP Sequence Number	シーケンス番号のランダム化機能をイネーブルにします。別のインライン セキュリティ アプライアンスもシーケンス番号をランダム化していて、結果としてデータが混乱している場合にだけ、この機能をディセーブルにします。それぞれの TCP 接続には 2 つの初期シーケンス番号が割り当てられており、そのうちの 1 つはクライアントで生成され、もう 1 つはサーバで生成されます。セキュリティ アプライアンスは、ホスト/サーバから生成された ISN をセキュリティ レベルの高いインターフェイス上でランダム化します。攻撃者が次の ISN を予測してセッション ハイジャックを実行できないように、少なくとも 1 つの ISN をランダムに生成する必要があります。TCP ステートバイパスがイネーブルになっている場合には適用されません。
Enable TCP State Bypass	このトラフィック フローの TCP ステートバイパスをイネーブルにします。このオプションにより、接続のアウトバウンドおよびインバウンド フローが同じデバイスを通過しない場合に、非対称ルーティング環境で特定のトラフィック フローが許可されます。FWSM 3.2+ および ASA 8.2+ だけに適用できます。詳細については、TCP ステート バイパスについて （3 ページ）を参照してください。
SCTPステートバイパスの有効化（Enable SCTP State Bypass）（ASA 9.5.2 以降のみ）	Stream Control Transmission Protocol（SCTP）プロトコル検証が不要な場合、SCTP ステートフル インスペクションをバイパスできます。
Enable Decrement TTL	このオプションを選択すると、セキュリティ アプライアンスから渡されるパケットの存続可能時間（TTL）値の減分が有効になります。PIX/ASA 7.2.2+ だけに適用できます。

要素	説明
フローオフロードの設定（Configure Flow Offload）（Firepower 9000/4000 シリーズ ASA 9.6(1) 以降）	（注） Cisco Security Manager の Service Policy ウィザードでフローオフロードを設定する前に、ASA でフローオフロードを手動で有効にしてデバイスを再起動する必要があります。フローオフロードとフローオフロードの統計情報は、シングルコンテキストモードとシステムコンテキストモードの ASA でのみサポートされます。管理コンテキストまたはユーザーコンテキストではサポートされていません。ASA ではバージョン 9.5.2(1) 以降からフローオフロードがサポートされていますが、Cisco Security Manager では ASA 9.6(1) からフローオフロードがサポートされてます。 特定のトラフィックを超高速パスにオフロードするには、このオプションを選択します。トラフィックは、ASA ではなく NIC でスイッチングおよび処理されます。オフロードによって、大容量ファイルの転送など、データ集約型アプリケーションのパフォーマンスを向上させることができます。 ヒント デバイスで TCP ステートバイパスと SCTP ステートバイパスが有効になっていない場合にのみ、フローオフロードを設定できます。
[QoS] タブ	
Enable QoS For This Traffic	このトラフィック フローの Quality of Service（QoS）オプションをイネーブルにします。選択すると、[Enable Priority For This Flow] オプションおよび [Traffic Policing] オプションがアクティブになります。 （注） このタブ上のオプションは、PIX/ASA 7.0 以降のデバイスにのみ適用できます。
Enable Priority For This Flow	このフローの厳密なスケジューリング プライオリティをイネーブルにします。[Priority Queues] ページ （4 ページ）でプライオリティ キューを定義する必要があります。
トラフィックポリシング	出力および入力のトラフィック ポリシングをイネーブルにします。トラフィック ポリシングにより、インターフェイス上で送受信されるトラフィックの最大レートを制御できます。

要素	説明
Output (Traffic Policing)	デバイスから出力されるトラフィックのポリシングをイネーブルにします。ポリシングをイネーブルにする場合は、次の値を指定できます。 • [認定レート（Committed Rate）]：このトラフィックフローのレート制限。8,000 ～ 2,000,000,000 の範囲の値で、許容最大速度（1秒あたりのビット数）を指定します。 • [バーストレート（Burst Rate）]：1,000 ～ 512,000,000 の範囲の値で、適合レート値まで抑制するまでに、持続的バーストにおいて許可される最大瞬間バイト数を指定します。 • [適合アクション（Conform Action）]：レートが適合バースト値未満の場合に実行するアクション。選択肢は [Transmit] または [Drop] です。 • [超過アクション（Exceed Action）]：レートが適合レート値と適合バースト値の間である場合に、このアクションを実行します。選択肢は [Transmit] または [Drop] です。
Input (Traffic Policing)	デバイスに入力されるトラフィックのポリシングをイネーブルにします。これらのオプションは、ASA/PIX 7.2+ デバイスだけに適用されます。ポリシングをイネーブルにする場合は、次の値を指定できます。 • [認定レート（Committed Rate）]：このトラフィックフローのレート制限。8,000 ～ 2,000,000,000 の範囲の値で、許容最大速度（1秒あたりのビット数）を指定します。 • [バーストレート（Burst Rate）]：1,000 ～ 512,000,000 の範囲の値で、適合レート値まで抑制するまでに、持続的バーストにおいて許可される最大瞬間バイト数を指定します。 • [適合アクション（Conform Action）]：レートが適合バースト値未満の場合に実行するアクション。選択肢は [Transmit] または [Drop] です。 • [超過アクション（Exceed Action）]：レートが適合レート値と適合バースト値の間である場合に、このアクションを実行します。選択肢は [Transmit] または [Drop] です。
[CSC] タブ	

要素	説明
Enable Content Security Control For This Traffic	このトラフィック フローで Cisco Content Security and Control Security Services Module（CSC SSM）の使用をイネーブルまたはディセーブルにします。このチェックボックスをオンにすると、[On CSC SSM Failure] オプションが使用可能になります。これらのオプションは、ASA 7.1+ デバイスだけに適用できます。ただし、TCP ステート バイパスがイネーブルになっている場合には適用されません。 CSC SSM では、FTP、HTTP、POP3、および SMTP のパケットをスキャンして、ウイルス、スパイウェア、スパム、およびその他の好ましくないトラフィックから保護します。
On CSC SSM Failure	CSC SSM が動作不能になった場合に実行する次のアクションを指定します。 • [開く（Open）]：CSC SSM で障害が発生した場合にトラフィックを許可します。 • [閉じる（Close）]：CSC SSM で障害が発生した場合にトラフィックをブロックします。
[User Statistics] タブ	
Enable user statistics accounting（ASA 8.4(2)+ のみ）	アイデンティティベースのファイアウォール ポリシーで、ユーザ統計情報アカウンティング情報を収集するかどうか。これらの統計情報は、ユーザー名またはユーザー グループ メンバーシップに基づいてファイアウォールポリシーが適用されるユーザーに対して保持されます。収集する情報のタイプを選択します。 • **Account for sent drop count** • **Account for sent packet, sent drop and received packet count**
[プロトコルインスペクション（Protocol Inspection）] タブ	
このトラフィックに対するScansafe Webセキュリティの有効化（Enable Scansafe Web Security for this traffic）（ASA 9.0 以降 のみ）	トラフィックフローに対する ScanSafe Web セキュリティの使用を有効または無効にします。このボックスをオンにすると、2 つのオプションが使用可能になり、それらのオプションは、ASA 9.0 以降のデバイスにのみ適用されます。 • [ScanSafeポリシーマップ（ScanSafe Policy Map）]：ポリシーマップの選択を有効にします。 • [ScanSafe Towerの通信障害時（On ScanSafe Tower Communication Failure）]：ScanSafe Tower の通信に障害が発生した場合にシステムが実行するアクションを指定します。

要素	説明
このトラフィックに対するSCTPの有効化（Enable SCTP for this traffic）（ASA 9.5.2 以降のみ）	トラフィックフローに対する SCTP の使用を有効または無効にします。 • [SCTPポリシーマップ（SCTP Policy Map）]：ポリシーマップの選択を有効にします。
このトラフィックに対するDiameterインスペクションの有効化（Enable Diameter Inspection for this traffic）（ASA 9.5.2 以降のみ）	トラフィックフローに対する Diameter インスペクションの使用を有効または無効にします。 • [Diameterポリシーマップ（Diameter Policy Map）]：ポリシーマップの選択を可能にします。 Diameter インスペクションが有効になっている場合は、[暗号化トラフィックインスペクションの有効化（Enable encrypted traffic inspection）]チェックボックスをオンにすると、暗号化トラフィックの検査を追加で有効にできます。この検査に使用する TLS プロキシを選択する必要があります。
このトラフィックに対するLISPの有効化（Enable LISP for this traffic）（ASA 9.5.2 以降のみ）	トラフィックフローに対する LISP インスペクションの使用を有効または無効にします。 • [LISPポリシーマップ（LISP Policy Map）]：ポリシーマップの選択を有効にします。
デバイスのフローLISPモビリティの有効化（Enable Flow LISP mobility for devices）（ASA 9.5.2 以降のみ）	クラスタリングのフローモビリティを有効にします。
デバイスのSTUNインスペクションサポートの有効化（Enable STUN Inspection support for devices）（ASA 9.6.2 以降のみ）	トラフィックフローに対する STUN インスペクションの使用を有効または無効にします。シングルコンテキストモードおよびマルチコンテキストモードの ASA 9.6.2 以降でサポートされています。 （注） デフォルトのインスペクション クラスで STUN インスペクションをイネーブルにすると、STUN トラフィックに関して TCP/UDP ポート 3478 が監視されます。このインスペクションは、IPv4 アドレスと TCP/UDP のみをサポートします。ピンホールの複製時、STUN インスペクションはフェールオーバーモードとクラスタモードでサポートされます。ただし、トランザクション ID はユニット間で複製されません。あるユニットが STUN 要求を受信後に故障し、別のユニットがその STUN 応答を受信した場合、その STUN 応答はドロップされます。

要素	説明
このトラフィックのM3UAの有効化（Enable M3UA for this traffic）（ASA 9.6.2 以降のみ）	トラフィックフローに対する M3UA の使用を有効または無効にします。 • [M3UAポリシーマップ（M3UA Policy Map）]：ポリシーマップの選択を可能にします。
[NetFlow] タブ	
このトラフィックに対するNetFlowの有効化（Enable NetFlow for this traffic）	トラフィックフローに対する NetFlow の使用を有効または無効にします。このボックスをオンにすると、NetFlow オプションが使用可能になります。
[Collectors]	特定のイベントタイプの NetFlow イベントを送信するときに使用する必要があるコレクタを指定します。 （注） [NetFlow] ページ（[プラットフォーム（Platform）] > [ロギング（Logging）] > [NetFlow]）で設定されているコレクタのみを使用してください。 • フロー作成イベント • フロー拒否イベント • フローティアイベント • すべてのイベントタイプ （注） Cisco Security Manager では、ASA 9.6(4) から 9.7.0、および 9.8(2) 以降のデバイスに対する重複するネットフローコレクタは許可されません。重複するコレクタは必ず削除してください。

ASA デバイスでの IPS モジュールについて

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

一部の ASA デバイス モデルには、Advanced Inspection and Prevention Security Services Module（AIP-SSM）などのさまざまな IPS モジュールを取り付けることができます。サポートされている IPS モジュールは ASA モデルごとに異なります。IPS モジュールは、フル機能の予防的な侵入防御サービスを提供する高度な IPS ソフトウェアを実行して、ワームやネットワーク ウイルスなどの悪意のあるトラフィックがネットワークに影響を与える前にこれらを阻止します。

ASA IPS モジュールは適応型セキュリティ アプライアンスから独立して動作するため、個別のデバイスとしてデバイス インベントリに追加する必要があります。ただし、AIP SSM/SSC は ASA のトラフィック フローに統合されます。

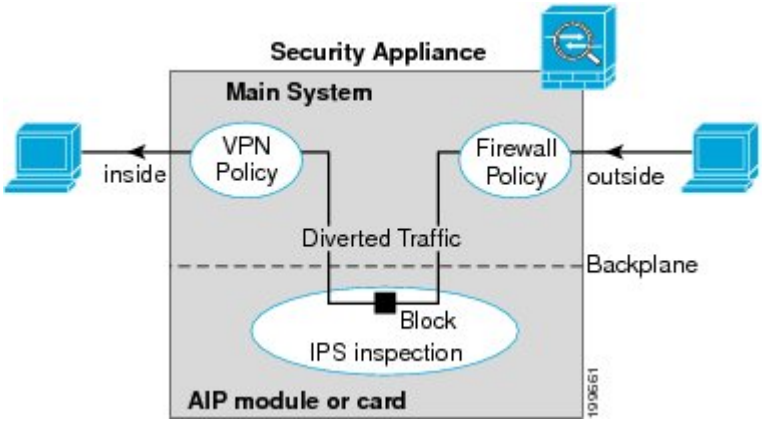
ASA IPS モジュールを設定する場合は、ホスト ASA 上にサービス ポリシールールを設定し、IPS モジュール上に IPS ポリシーを設定する必要があります。このサービス ポリシールールは、IPS モジュールで検査されるトラフィックを決定します。IPS ポリシー設定の概要については、IPS 設定の概要を参照してください。

IPS 検査のトラフィックを識別する場合、トラフィックは次のように ASA および IPS モジュールを通過します。

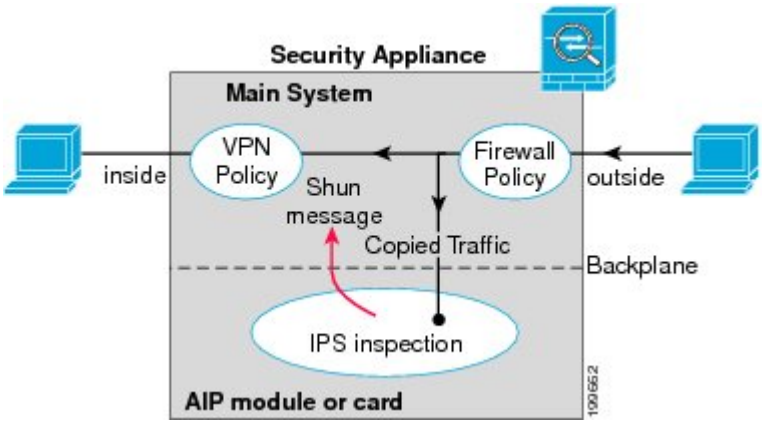
1. トラフィックが ASA に入ります。
2. インターフェイス アクセス ルールなどのファイアウォール ポリシーが適用されます。
3. インラインモードで操作する場合は、バックプレーンを介して IPS モジュールにトラフィックが送信されます。無差別モードを使用するようにシステムを設定する場合は、トラフィックのコピーが IPS モジュールに送信されます。

   インラインモードと無差別モードの詳細については、Insert/Edit Service Policy（MPC）Rule ウィザード（手順 3：MPC アクションの設定 （10 ページ））の [侵入防御（Intrusion Prevention）] セクションで [IPS モード（IPS Mode）] を参照してください。
4. IPS モジュールはセキュリティ ポリシーをトラフィックに適用し、適切なアクションを実行します。
5. 許可されたトラフィックがバックプレーンを介して適応型セキュリティ アプライアンスに返送されます。[Inline] モードでは、IPS モジュールはセキュリティ ポリシーに従ってトラフィックをブロックする場合があります。この場合、ブロックされたトラフィックは返送されません。
6. VPN ポリシーが適用されます（設定されている場合）。
7. トラフィックが ASA を出ます。

次の図に、IPS モジュールを [Inline] モードで実行する場合のトラフィック フローを示します。この例では、IPS モジュールが攻撃と見なしたトラフィックは、自動的にブロックされています。他のトラフィックはすべて ASA に戻されます。



次の図に、IPS モジュールを [Promiscuous] モードで実行する場合のトラフィック フローを示します。この例では、IPSモジュールは、脅威と見なしたトラフィックについての排除メッセージを ASA に送信します。



関連項目

- デバイス インベントリへのデバイスの追加

ASA CX について

ASA CX は、Cisco ASA-5585-X シリーズ適応型セキュリティアプライアンスにインストールできるセキュリティ サービス プロセッサ（SSP）です。トラフィックを ASA CX にリダイレクトするように親 ASA を設定すると、そのセキュリティポリシーが適用され、トラフィックがドロップされるか、さらに処理されて次の宛先にルーティングされるように ASA に戻されます。

ASA CX を追加する際に ASA で調整する必要がある 2 つの基本ポリシーとして、アクセスルールとインスペクションルールがあります。

- アクセスルールは、グローバルルールであっても、特定のインターフェイスに適用されるものであっても、トラフィックが ASA CX にリダイレクトされる前に必ず適用されます。そのため、セキュリティカードはすでに許可されているトラフィックのみを認識し、ASA

への入口でドロップされたトラフィックを処理しません。ASA CX で処理するすべてのトラフィックが許可されるように、ルールを調整することを検討してください。

- インスペクション ルールによって、トラフィックが検査されるかどうかを決定します。ASA CX は ASA で検査済みのトラフィックを検査しません。したがって、ASA CX で検査する予定のトラフィックを、自分で検査してはいけません。具体的には、HTTP トラフィックを検査しないでください。HTTP インスペクションは ASA CX の中核機能の 1 つであるためです。ASA のデフォルトのインスペクション ルールに HTTP インスペクションは含まれないため、HTTP ルールを追加した場合にのみお使いのインスペクション ルールを変更する必要があります。

インターフェイスにアクセスルールを作成する必要があるか、あるいはすべてのインターフェイスに適用するグローバルアクセスルールを作成する必要があるかを判断してください。ASA アクセスルールは、トラフィックを ASA CX にリダイレクトする前にフィルタリングするために使用します。絶対に渡さないトラフィッククラスがあるとわかっている場合は、ASA への入力時にすぐにドロップすると、より効率的です。

すでにアクセスルールを設定している場合、変更する必要はありません。ただし、アクセスルールを使用してドロップしている特定のタイプのトラフィックを ASA CX で処理するため、それらのアクセスルールを緩和することが必要かどうかを評価する必要があります。

インストールされている ASA CX へのトラフィック リダイレクションの有効化については、Insert/Edit Service Policy (MPC) Rule ウィザード （8 ページ）の 手順 3：MPC アクションの設定 （10 ページ）で説明されています。

関連項目

- サービス ポリシールールについて （1 ページ）

ASA CX 認証プロキシの設定

ASA CX 認証プロキシを有効にした場合（サービスポリシー（MPC）Insert/Edit Service Policy（MPC）Rule ウィザードのステップ 3 の [CXSC] タブ。 手順 3：MPC アクションの設定 （10 ページ）を参照）：アクティブ認証にデフォルト以外のポートを使用する場合は、[CXSC認証プロキシ設定の追加/編集（Add/Edit CXSC Auth Proxy Configuration）] ダイアログボックスを使用して ASA CX 認証プロキシポート番号を変更します。

ユーザに認証クレデンシャルの入力を求める必要がある場合、プロンプト要求はこのポートを通じて行われます。

（注） Security Manager は、ASA CX セキュリティ サービス プロセッサ（SSP）を参照する場所の一部で「CXSC」を使用します。

ナビゲーション パス

[サービスポリシールール（Service Policy Rules）] ページ （6 ページ）のルールテーブルの下にある [CXSC認証プロキシ（CXSC Auth Proxy）] ボタンをクリックして、[CXSC認証プロキシ設定の追加/編集（Add/Edit CXSC Auth Proxy Configuration）] ダイアログボックスを開きます。

（注） [CXSC認証プロキシ（CXSC Auth Proxy）] ボタンには、デバイスビューの [IPS]、[QoS]、および [接続ルール（Connection Rules）] テーブルの下でのみアクセスできます。ポリシービューには表示されません。

関連項目

- [サービスポリシールール（Service Policy Rules）] ページ （6 ページ）

フィールド リファレンス

表 *4 : [CXSC*認証プロキシ設定の追加/編集（*Add/Edit CXSC Auth Proxy Configuration*）*]* ダイアログボックス

要素	説明
[CXSC認証プロキシポート（CXSC Auth Proxy Port）]	デフォルトの認証プロキシの TCP ポートは 885 です。変更する場合は、1024 ～ 65535 のポート番号を入力する必要があります。

トラフィック フロー オブジェクトの設定

トラフィックの一致定義を設定するには、[Add Traffic Flow]/[Edit Traffic Flow] ダイアログボックスを使用します。これらのトラフィックフロー定義は、PIX 7.0 以降、ASA 7.0 以降、および FWSM 3.2 以降の各オペレーティングシステムが稼働するデバイスで、IPS、QoS、および接続ルールのサービスポリシーに含まれるクラスマップ（**class map** コマンド）に対応します。これらのルールの設定の詳細については、 サービス ポリシールールについて （1 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、次にオブジェクトタイプセレクタから [トラフィックフロー（Traffic Flows）] を選択します。作業領域内で右クリックして [New Object] を選択するか、または行を右クリックして [Edit Object] を選択します。

これらのダイアログボックスは、サービスポリシールールを定義しているときに、トラフィック フロー セレクタの [Create] または [Edit] ボタンをクリックして開くこともできます。トラフィック フロー クラスの選択の詳細については、 手順 2：トラフィック クラスの設定 （9 ページ）を参照してください。

関連項目

- アクセス コントロール リスト オブジェクトの作成

フィールド リファレンス

表 5 : [Add Traffic Flow]/[Edit Traffic Flow] ダイアログボックス

要素	説明
名前	トラフィック フロー オブジェクトの名前。最大 40 文字を使用できます。クラス マップのネーム スペースは、セキュリティ コンテキストに対してローカルです。したがって、複数のセキュリティ コンテキストで同じ名前を使用できます。セキュリティ コンテキストあたりのクラス マップの最大数は 255 です。
説明	トラフィック フローの説明（任意）。最大 1024 文字を使用できます。

要素	説明
Traffic Match Type	照合するトラフィックのタイプ。選択したオプションによって、ダイアログボックス内のフィールドが変更される場合があります。選択可能なすべてのフィールドについては、この表の後半を参照してください。[Traffic Match Type] のオプションは次のとおりです。 • [Any Traffic]：すべてのトラフィックを照合します。 • [Source and Destination IP Address (access-list)]：指定したアクセス コントロール リストに基づいて、パケットの送信元アドレスおよび宛先アドレスを照合します。 ASA 8.4(2) 以降のデバイスの場合、ACL に FQDN オブジェクトとユーザ指定を含めて、ID ベースのトラフィック照合を実行できます。 • [Default Inspection Traffic]：デフォルト インスペクション トラフィックを照合します。デフォルト設定のリストについては、デフォルト インスペクション トラフィック （29 ページ）を参照してください。 • [Default Inspection Traffic with access list]：指定したアクセス コントロール リストで制限されたデフォルト インスペクション トラフィックを照合します。 • [TCPまたはUDPまたはSCTP宛先ポート（TCP or UDP or SCTP Destination Port）]：トラフィックを、指定した TCP または UDP またはSCTP宛先ポートまたはポート範囲と照合します。ここで有効なポート番号は 0 ～ 65535 です。 • [RTP Range]：指定した UDP 宛先ポートの範囲に送信されるトラフィックを照合します。ここで有効なポート番号は 2000 ～ 65535 です。 • [Tunnel Group]：指定したトンネル グループに属する VPN トンネル内のフローに基づいて、宛先アドレスを照合します。 • [IP Precedence Bits]：トラフィック パケットに割り当てられた precedence 値を照合します。最大で 4 つの値を選択できます。 • [IP DiffServe Code Points (DSCP) Values]：トラフィック パケットに関連付けられた DSCP 値を照合します。最大で 8 つの値を選択できます。
可変フィールド [Add Traffic Flow]/[Edit Traffic Flow] ダイアログボックスには、[Traffic Match Type] フィールドで選択した内容に応じて次のフィールドが表示されます。次のリストに、選択可能なフィールド セットをすべて示します。	

要素	説明
Available ACLs	マップに選択可能なアクセス コントロール リスト（ACL）オブジェクトのリスト。ターゲット トラフィックを定義する ACL を選択するか、または [Create] ボタンをクリックして新しいオブジェクトを追加します。オブジェクトを選択して [Edit] をクリックし、定義を変更することもできます。オブジェクトのリストが大きい場合は、[Filter] フィールドを使用して表示を制限してください（セレクタ内の項目のフィルタリング）。
[TCP] または [UDP] または [SCTP] TCP/UDP/SCTP ポートまたはポート範囲（TCP/UDP/SCTP Port or Port Range）	プロトコル（TCP、UDP または SCTP）を指定するオプションボタン、および指定したプロトコル/ポートに基づいてトラフィックを照合するときに使用する、宛先ポート番号または番号の範囲を指定するテキスト フィールド。 単一のポート値またはポート番号の範囲（0-2000 など）を指定できます。有効なポート番号は 0 ～ 65535 です。
RTP Port Range	トラフィック フローに関連付けられた RTP 宛先ポートの範囲。有効な 2000 ～ 65535 の範囲内でポート範囲を入力する必要があります。 （注） ダイアログボックスを閉じると、入力したポート範囲は、終了値から開始値を引いた port-span 値に変換されます。たとえば、ダイアログボックスに範囲 2001-3000 を入力すると、[トラフィックフロー（Traffic Flows）] ポリシー オブジェクト テーブルの [照合値（Match Value）] 列に「RTP ポート2001範囲999（RTP port 2001 range 999）」が表示されます。port-span 値はデバイスから要求されます。
Tunnel group name Match Flow IP Destination Address	使用可能な VPN トンネル グループが一覧表示されます。グループを選択するか、またはグループの名前を入力します。[Match Flow IP Destination Address] を選択して、宛先アドレスを一致タイプとして認識することもできます。 ヒント FlexConfig のオブジェクトおよびポリシーを使用して、PIX 7.0+ デバイスに VPN トンネル グループを定義できます。詳細については、FlexConfig ポリシーとポリシー オブジェクトについてを参照してください。
Available IP Precedence Match on IP Precedence	IP precedence 番号。照合する値を選択し、[>>] をクリックして [一致（Match）] テーブルに追加します。複数の値を選択するには、Ctrl を押しながらクリックします。最大で 4 つの値を選択できます。 [一致（Match）] テーブルから値を削除するには、その値を選択して [<<] をクリックします。

要素	説明
Available DSCP Values Match on DSCP	IP DiffServe Code Point（DSCP）番号。照合する値を選択し、[>>] をクリックして [一致（Match）] テーブルに追加します。複数の値を選択するには、Ctrl を押しながらクリックします。最大で 8 つの値を選択できます。 [一致（Match）] テーブルから値を削除するには、その値を選択して [<<] をクリックします。
カテゴリ	トラフィック フロー 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。

デフォルト インスペクション トラフィック

トラフィック フローポリシー オブジェクトを作成すると、デフォルト インスペクション トラフィックを照合できます。詳細については、トラフィック フロー オブジェクトの設定 （25 ページ）を参照してください。次の表に、デフォルト インスペクション トラフィック カテゴリに含まれているトラフィックのタイプを示します。

表 *6:* デフォルト インスペクション トラフィック

値	[ポート（Port）]	NAT に関する制限事項	説明
CTIQBE	TCP/2748		
CuSeeMe	UDP/7648		
DNS over UDP	UDP/53	WINS 経由の名前解決では NAT は非サポート。	PTR レコードは変更されません。
FTP	TCP/21		
GTP	UDP/2123、3386		
H.323、H.225	TCP/1720、1718	同一セキュリティのインターフェイス上の NAT はサポートされません。スタティック PAT はサポートされません。	
RAS	UDP/1718、1719	同一セキュリティのインターフェイス上の NAT はサポートされません。スタティック PAT はサポートされません。	
HTTP	TCP/80		

値	[ポート（Port）]	NAT に関する制限事項	説明
ICMP	—		すべての ICMP トラフィックは、デフォルトのクラスマップで照合されます。
ILS（LDAP）	TCP/389	PAT なし。	
IP オプション	—		すべての IP オプション トラフィックは、デフォルトのクラス マップで照合されます。
MGCP	UDP/2427、2727		
NetBIOS ネームサーバ	UDP/137、138（送信元ポート）		NetBIOS は、NBNS UDP ポート 137 および NBDS UDP ポート 138 に対してパケットの NAT 処理を実行することでサポートされます。
RSH	TCP/514	PAT なし。	
RTSP	TCP/554	PAT なし。外部 NAT はサポートされません。	HTTP クローキングは処理しません。
SIP	TCP/5060、UDP/5060	外部 NAT はサポートされません。同一セキュリティのインターフェイス上の NAT はサポートされません。	
Skinny Client Control Protocol（SCCP）	TCP/2000	外部 NAT はサポートされません。同一セキュリティのインターフェイス上の NAT はサポートされません。	
SMTP および ESMTP	TCP/25		
SQL*Net	TCP/1521		バージョン 1 および 2。

値	[ポート（Port）]	NAT に関する制限事項	説明
Sun RPC over UDP	UDP/111	NAT および PAT はサポートされません。	デフォルトのルールには UDP ポート 111 が含まれています。TCP ポート 111 の Sun RPC インスペクションをイネーブルにする場合は、TCP ポート 111 を照合する新しいルールを作成し、Sun RPC インスペクションを実行する必要があります。
TFTP	UDP/69		ペイロード IP アドレスは変換されません。
XDMCP	UDP/177	NAT および PAT はサポートされません。	

TCP マップの設定

IPS、QoS、および接続ルールのサービス ポリシーで使用する TCP 正規化マップを定義するには、[Add TCP Map]/[Edit TCP Map] ダイアログボックスを使用します。TCP 正規化機能により、異常なパケットを識別する基準を指定できます。セキュリティアプライアンスは異常なパケットを検出すると、そのパケットをドロップします。このマップは、デバイスを通過する、またはデバイスに送信される TCP トラフィックに対して使用されます。

これらの TCP マップは、PIX 7.x+ デバイスおよび ASA デバイス上の TCP フローに適用できます。IPS、QoS、および接続ルールの設定の詳細については、サービス ポリシールールについて （1 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、次にオブジェクトタイプセレクタから [マップ（Maps）] > [TCPマップ（TCP Maps）] を選択します。作業領域内で右クリックして [New Object] を選択するか、または行を右クリックして [Edit Object] を選択します。

これらのダイアログボックスは、サービス ポリシールールを定義しているときに、TCP マップ セレクタの [Create] または [Edit] ボタンをクリックして開くこともできます。TCP 正規化の有効化および TCP マップの選択の詳細については、手順 3：MPC アクションの設定 （10 ページ）の「接続の設定」セクション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

フィールド リファレンス

表 *7 : [Add TCP Map]/[Edit TCP Map]* ダイアログボックス

要素	説明
名前	TCP 正規化マップの名前。最大 128 文字を使用できます。
説明	マップ オブジェクトの説明。最大 1024 文字を使用できます。
キュー制限（Queue Limit） （ASA デバイス限定）	TCP 接続で、バッファに格納して順序を並べ替えることのできる out-of-order パケットの最大数。1 ～ 250 の間の値を入力します。0 を入力すると、この設定はディセーブルになり、デフォルトのシステム キュー制限が使用されます。この制限は、トラフィックのタイプによって次のように異なります。 • アプリケーション インスペクション、IPS、および TCP check-retransmission の接続のキュー制限は 3 パケットです。セキュリティ アプライアンスがウィンドウ サイズの異なる TCP パケットを受信した場合、キュー制限はアドバタイズされた設定に一致するように動的に変更されます。 • 他の TCP 接続の場合は、異常なパケットはそのまま通過します。 ただし、[Queue Limit] を 1 以上に設定した場合、すべての TCP トラフィックで許容される out-of-order パケットの数は、指定した値に一致します。アプリケーション インスペクション、IPS、および TCP check-retransmission のトラフィックの場合、アドバタイズされた設定はすべて無視されます。その他の TCP トラフィックについては、異常なパケットはバッファに格納されて、そのまま通過するのではなく、正しい順序に設定されます。
タイムアウト（Time Out） （ASA 7.2(4)+ デバイス限定）	out-of-order パケットをバッファに格納しておくことのできる最大期間。この期間を超えると、パケットはドロップされます。1 ～ 20 秒の間の値を入力します。デフォルトは 4 秒です。 [Queue Limit] に 0 を入力した場合、この設定は無視されます。
Verify TCP Checksum	オンにすると、チェックサム検証がイネーブルになります。
Drop SYN Packets with Data	オンにすると、データを持つ TCP SYN パケットがドロップされます。
Drop Connection on Window Variation	オンにすると、ウィンドウ サイズが突然変更された接続がドロップされます。
Drop Packets that Exceed Maximum Segment Size	オンにすると、ピアに設定された Maximum Segment Size（MSS; 最大セグメント サイズ）を超えるパケットがドロップされます。

要素	説明
Check if Transmitted Data is the Same as Original	オンにすると、再送信データのチェックがイネーブルになります。
Clear Urgent Flag	オンにすると、セキュリティアプライアンスを介してURG（緊急）フラグがクリアされます。URGフラグは、ストリーム中の他のデータよりもプライオリティの高い情報がこのパケットに含まれていることを示すために使用します。TCPのRFCでは、URGフラグの厳密な解釈が定められていません。したがって、緊急オフセットの処理方法がエンドシステムによって異なり、エンドシステムが脆弱になる場合があります。
Enable TTL Evasion Protection	セキュリティ アプライアンスから提供される TTL 回避保護をイネーブルにします。セキュリティポリシーを回避しようとする攻撃を防ぐ場合は、このオプションをイネーブルにしないでください。 たとえば、攻撃者はTTLを非常に短くしてポリシーを通過するパケットを送信できます。TTLが0になると、セキュリティアプライアンスとエンドポイントの間のルータは、パケットをドロップします。この時点で、攻撃者は長いTTLを設定した、悪意のあるパケットを送信できます。セキュリティアプライアンスはこのパケットを再送信と見なすため、パケットは通過します。一方、エンドポイントホストにとっては、このパケットが最初に受信するパケットになります。この場合、攻撃者はセキュリティによる攻撃の防止を受けず、攻撃に成功します。
選択的受信確認	
Clear Selective Ack	オンにすると、ウィンドウ選択的確認応答メカニズムオプションが選択解除され、パケットが許可されます。オフにすると、単一の選択的確認応答オプションを含むパケットが許可されます。
[複数の選択的確認応答を許可（Selective Ack Allow Multiple）]	複数の選択的確認応答メカニズム（SACK）を備えたパケットが許可されるかどうか。
（注） 選択的確認応答オプションが設定されていない場合、デフォルトでは、単一の選択的確認応答オプションを含むパケットは許可され、複数の選択的確認応答オプションを含むパケットはドロップされます。	
[TCPタイムスタンプ（TCP Timestamp）]	

要素	説明
Clear TCP Timestamp	オンにすると、TCP タイムスタンプオプションがクリアされ、パケットが許可されます。オフにすると、単一のTCPタイムスタンプオプションを含むパケットが許可されます。 （注） [TCPタイムスタンプのクリア（Clear TCP timestamp）] オプションを有効にすると、PAWS と RTT が無効になります。
[複数のTCPタイムスタンプを許可（TCP Timestamp Allow multiple）]	複数のTCPタイムスタンプオプションを含むパケットを許可するかどうか。
（注） TCP タイムスタンプオプションが設定されていない場合、デフォルトでは、単一の TCP タイムスタンプオプションを含むパケットは許可され、複数の TCP タイムスタンプオプションを含むパケットはドロップされます。	
ウィンドウ スケール（Window Scale）	
Clear Window Scale	オンにすると、ウィンドウ スケール タイムスタンプ オプションがクリアされ、パケットが許可されます。オフにすると、単一のウィンドウスケールオプションを含むパケットが許可されます。
[複数のウィンドウスケールを許可（Window Scale Allow Multiple）]	複数のウィンドウ スケール タイムスタンプ オプションを含むパケットを許可するかどうか。
（注） ウィンドウ スケール オプションが設定されていない場合、デフォルトでは、単一のウィンドウ スケール オプションを含むパケットは許可され、複数のウィンドウ スケール オプションを含むパケットはドロップされます。	
最大セグメント サイズ（MSS）（Maximum Segment Size (MSS)）	
[MSSのクリア（Clear MSS）]	オンにすると、MSSオプションがクリアされ、パケットが許可されます。オフにすると、単一のMSSオプションを含むパケットが許可されます。
[複数のMSSを許可（MSS Allow Multiple）]	複数の MSS オプションを含むパケットを許可するかどうか。
[最大MSS（Max. MSS）]	TCP MSS制限の値をバイト単位で入力します。有効な値は、68 ～ 65535 です。
（注） MSSオプションが設定されていない場合、デフォルトでは、単一のMSSオプションを含むパケットは許可され、複数の MSS オプションを含むパケットはドロップされます。	

要素	説明
[MD5オプションを含むパケットを許可（Allow packets with MD5 option）]	MD5 オプションを含むパケットを許可するかどうか。 [許可（Allow）]、[複数を許可（Allow Multiple）]、および [クリア（Clear）] チェックボックスは、MD5 オプションを含むパケットが許可されている場合に使用できます。 [許可（Allow）]：単一の MD5 オプションを含むパケットを許可します。 [複数を許可（Allow Multiple）]：複数の MD5 オプションを含むパケットを許可します。 [クリア（Clear）]：MD5 オプションをクリアして、パケットを許可します。
（注） MD5 オプションが設定されていない場合、デフォルトでは、単一の MD5 オプションを含むパケットは許可され、複数の MD5 オプションを含むパケットはドロップされます。	
Reserved Bits	TCP ヘッダーに予約済みビットが設定された TCP パケットの処理方法を指定します。TCP ヘッダーの 6 つの予約済みビットは今後の使用が想定されるもので、通常は値が 0 に設定されています。 • [Clear and Allow]：TCP ヘッダー内の予約済みビットをクリアし、パケットを許可します。 • [許可のみ（Allow only）]：TCP ヘッダーに予約済みビットが設定されたパケットを許可します。 • [Drop]：TCP ヘッダーに予約済みビットが設定されたパケットをドロップします。

要素	説明
[TCP Range Options] テーブル	[TCP Range Options] テーブルには、TCP マップに定義された TCP オプション範囲、およびそれらのオプションに実行するアクションが一覧表示されます。一般的な数値の範囲は 6 ～ 7、9 ～ 18 および 20 ～ 255 です。下限は上限以下とする必要があります。 • 範囲を追加するには、[Add] ボタンをクリックし、[Add TCP Option Range] ダイアログボックスを開きます（[Add TCP Option Range]/[Edit TCP Option Range] ダイアログボックス（36 ページ）を参照）。 • 範囲を編集するには、範囲を選択し、[Edit] ボタンをクリックします。 • 範囲を削除するには、範囲を選択し、[Delete] ボタンをクリックします。 （注） ASA 9.6(2) より前のバージョンでは、TCP 値の範囲は 6 ～ 7 および 9 ～ 255 です。
カテゴリ	マップ 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。

[Add TCP Option Range]/[Edit TCP Option Range] ダイアログボックス

TCP 正規化マップで使用する TCP オプション範囲を定義または編集するには、[Add TCP Option Range]/[Edit TCP Option Range] ダイアログボックスを使用します。これらは、デバイスで明示的にサポートされていない TCP オプションです。この機能により、指定した TCP オプション セットを持つパケットを許可または廃棄できます。一般的な数値の範囲は 6 ～ 7、9 ～ 18、および 20 ～ 255 です。

ナビゲーション パス

[Add TCP Map]/[Edit TCP Map] ダイアログボックスで、[TCP Range Options] テーブル内を右クリックして [Add Row] を選択するか、または既存の行を右クリックして [Edit Row] を選択します。 TCP マップの設定 （31 ページ）を参照してください。

フィールド リファレンス

表 *8 : [Add TCP Option Range]/[Edit TCP Option Range]* ダイアログボックス

要素	説明
（注） ASA 9.6(2) より前では、範囲の下限と上限にそれぞれ 6 または 7、または 9 ～ 255 の整数を指定します。[下限（Lower）] の値は [上限（Upper）] の値以下とする必要があります。	
コストの	範囲の下限。6 または 7、または 9 ～ 18 の整数、または 20 ～ 255 の整数を入力します。
Upper	範囲の上限。6 または 7、または 9 ～ 18 の整数、または 20 ～ 255 の整数を入力します。
操作	指定したオプション セットを持つパケットに対して実行するアクションを選択します。 • [Allow]：指定したオプション セットを持つパケットをすべて許可します。 • [Clear]：指定したオプションが設定されたすべてのパケットからそのオプションをクリアし、パケットを許可します。 • [Drop]：指定したオプションセットを持つパケットをすべて廃棄します。

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。