

サービス ポリシー

サービスポリシーにより、一貫性のある柔軟な方法でASAの機能を設定できます。たとえば、サービス ポリシーを使用すると、すべての TCP アプリケーションに適用されるタイムアウト 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。サービスポリシーは、1つのインターフェイスに適用されるか、またはグローバルに適用される複数のアクションまたはルールで構成されます。

- サービス ポリシーについて （1 ページ）
- サービス ポリシーのガイドライン （8 ページ）
- サービス ポリシーのデフォルト （9 ページ）
- サービス ポリシーの設定 （11 ページ）
- サービス ポリシーの履歴 （19 ページ）

サービス ポリシーについて

次の各トピックでは、サービス ポリシーの仕組みについて説明します。

サービス ポリシーのコンポーネント

サービスポリシーのポイントは、許可しているトラフィックに高度なサービスを適用することです。アクセスルールによって許可されるトラフィックにサービスポリシーを適用し、サービス モジュールへのリダイレクトやアプリケーション インスペクションの適用などの特別な処理を実行できます。

次のタイプのサービス ポリシーを使用できます。

- すべてのインターフェイスに適用される 1 つのグローバル ポリシー。
- インターフェイスごとに適用される1つのサービスポリシー。このポリシーは、デバイスを通過するトラフィックを対象とするクラスと、ASAインターフェイスに向けられた（インターフェイスを通過するのではない）管理トラフィックを対象とするクラスの組み合わせである場合があります。

各サービス ポリシーは、次の要素で構成されます。

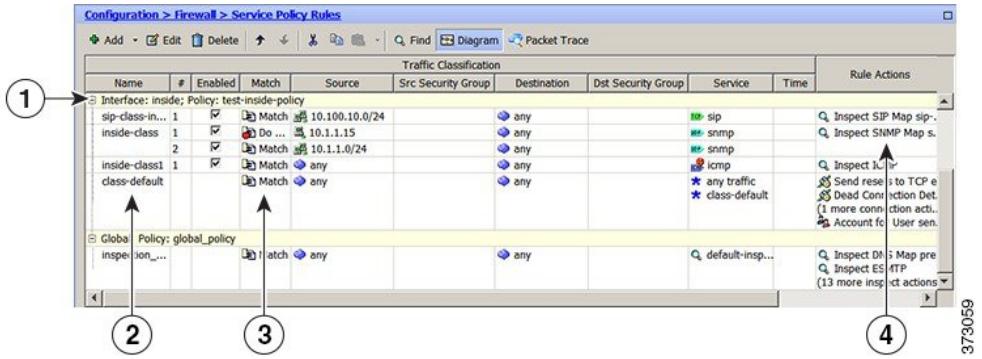
1. サービス ポリシー マップ。これはルールの順序セットであり、**service-policy** コマンドで命名されます。ASDM では、ポリシー マップは [Service Policy Rules] ページにフォルダとして表示されます。

2. ルール。各ルールは、サービス ポリシー内の、**class** コマンドと **class** に関連するコマンド群で構成されます。ASDM では、各ルールは個別の行に表示され、ルールの名前はクラス名です。

   class コマンドは、ルールのトラフィック照合基準を定義します。

   inspect や set connection timeout などの class 関連のコマンドは、一致するトラフィックに適用するサービスと制約を定義します。inspect コマンドは、検査対象トラフィックに適用するアクションを定義するインスペクション ポリシー マップを指す場合があります。インスペクション ポリシー マップとサービス ポリシー マップは同じではないことに注意してください。

次の例では、サービス ポリシーが CLI と ASDM でどのように表示されるかを比較します。図の吹き出しと CLI の行は 1 対 1 で対応しないことに注意してください。



次の CLI は、上の図に示すルールによって生成されます。

```
: Access lists used in class maps.
: In ASDM, these map to call-out 3, from the Match to the Time fields.
access-list inside_mpc line 1 extended permit tcp 10.100.10.0 255.255.255.0 any eq sip
access-list inside_mpc_1 line 1 extended deny udp host 10.1.1.15 any eq snmp
access-list inside_mpc_1 line 2 extended permit udp 10.1.1.0 255.255.255.0 any eq snmp
access-list inside_mpc_2 line 1 extended permit icmp any any
: SNMP map for SNMP inspection. Denies all but v3.
: In ASDM, this maps to call-out 4, rule actions, for the class-inside policy.
snmp-map snmp-v3only
  deny version 1
  deny version 2
  deny version 2c
: Inspection policy map to define SIP behavior.
: The sip-high inspection policy map must be referred to by an inspect sip command
: in the service policy map.
: In ASDM, this maps to call-out 4, rule actions, for the sip-class-inside policy.
policy-map type inspect sip sip-high
  parameters
    rtp-conformance enforce-payloadtype
    no traffic-non-sip
    software-version action mask log
    uri-non-sip action mask log
```

```
    state-checking action drop-connection log
    max-forwards-validation action drop log
    strict-header-validation action drop log
: Class map to define traffic matching for the inside-class rule.
: In ASDM, this maps to call-out 3, from the Match to the Time fields.
class-map inside-class
  match access-list inside_mpc_1
: Class map to define traffic matching for the sip-class-inside rule.
: In ASDM, this maps to call-out 3, from the Match to the Time fields.
class-map sip-class-inside
  match access-list inside_mpc
: Class map to define traffic matching for the inside-class1 rule.
: In ASDM, this maps to call-out 3, from the Match to the Time fields.
class-map inside-class1
  match access-list inside_mpc_2
: Policy map that actually defines the service policy rule set named test-inside-policy.
: In ASDM, this corresponds to the folder at call-out 1.
policy-map test-inside-policy
: First rule in test-inside-policy, named sip-class-inside. Inspects SIP traffic.
: The sip-class-inside rule applies the sip-high inspection policy map to SIP inspection.
: In ASDM, each rule corresponds to call-out 2.
  class sip-class-inside
    inspect sip sip-high
: Second rule, inside-class. Applies SNMP inspection using an SNMP map.
  class inside-class
    inspect snmp snmp-v3only
: Third rule, inside-class1. Applies ICMP inspection.
  class inside-class1
    inspect icmp
: Fourth rule, class-default. Applies connection settings and enables user statistics.
  class class-default
    set connection timeout embryonic 0:00:30 half-closed 0:10:00 idle 1:00:00
reset dcd 0:15:00 5
    user-statistics accounting
: The service-policy command applies the policy map rule set to the inside interface.
: This command activates the policies.
service-policy test-inside-policy interface inside
```

サービス ポリシーで設定される機能

次の表に、サービス ポリシーを使用して設定する機能を示します。

表 *1*:サービス ポリシーで設定される機能

機能	通過トラフィック用か	管理トラフィック用か	次を参照してください。
アプリケーション インスペクション（複数タイプ）	RADIUS アカウンティングを除くすべて	**RADIUS アカウンティング**のみ	• アプリケーション レイヤ プロトコル インスペクションの準備。 • 基本インターネット プロトコルのインスペクション。 • 音声とビデオのプロトコルのインスペクション。 • モバイル ネットワークのインスペクション。

機能	通過トラフィック用か	管理トラフィック用か	次を参照してください。
ASA FirePOWER（ASA SFR）	対応	非対応	ASA FirePOWER モジュール。
NetFlow セキュア イベント ロギングのフィルタリング	対応	対応	NetFlow 実装ガイドを参照してください。
QoS 入出力ポリシング	対応	非対応	QoS。
QoS 標準プライオリティ キュー	対応	非対応	QoS。
TCP と UDP の接続制限値とタイムアウト、および TCP シーケンス番号のランダム化	対応	対応	接続設定。
TCP の正規化	対応	非対応	接続設定。
TCP ステート バイパス	対応	非対応	接続設定。
アイデンティティ ファイアウォールのユーザー統計情報	対応	対応	コマンド リファレンスの user-statistics コマンドを参照してください。

機能の方向性

アクションは、機能に応じて双方向または単方向にトラフィックに適用されます。双方向に適用される機能の場合、トラフィックが両方向のクラスマップと一致した場合に、ポリシーマップを適用するインターフェイスを出入りするすべてのトラフィックが影響を受けます。

（注） グローバル ポリシーを使用する場合は、すべての機能が単方向です。単一インターフェイスに適用する場合に通常双方向の機能は、グローバルに適用される場合、各インターフェイスの入力にのみ適用されます。ポリシーはすべてのインターフェイスに適用されるため、ポリシーは両方向に適用され、この場合の双方向は冗長になります。

QoS プライオリティ キューなど単方向に適用される機能の場合は、ポリシー マップを適用するインターフェイスに出入りする（機能によって異なります）トラフィックだけが影響を受けます。各機能の方向については、次の表を参照してください。

表 *2:* 機能の方向性

機能	単一インターフェイスでの方向	グローバルでの方向
アプリケーション インスペクション（複数タイプ）	双方向	入力

機能	単一インターフェイスでの方向	グローバルでの方向
ASA FirePOWER（ASA SFR）	双方向	入力
NetFlow セキュア イベント ロギングのフィルタリング	該当なし	入力
QoS 入力ポリシング	入力	入力
QoS 出力ポリシング	出力	出力
QoS 標準プライオリティ キュー	出力	出力
TCP と UDP の接続制限値とタイムアウト、および TCP シーケンス番号のランダム化	双方向	入力
TCP の正規化	双方向	入力
TCP ステート バイパス	双方向	入力
アイデンティティ ファイアウォールのユーザー統計情報	双方向	入力

サービス ポリシー内の機能照合

パケットは、次のルールに従って特定のインターフェイスのポリシーのルールに一致します。

1. パケットは、各機能タイプのインターフェイスのにだけ一致します。
2. パケットが機能タイプの ルールに一致した場合、ASA は、その機能タイプの後続の ルールとは照合しません。
3. ただし、パケットが別の機能タイプの後続のルールと一致した場合、ASAは、後続のルールのアクションも適用します（サポートされている場合）。サポートされていない組み合わせの詳細については、特定の機能アクションの非互換性 （7 ページ）を参照してください。

（注） アプリケーション インスペクションには、複数のインスペクション タイプが含まれ、ほとんどのタイプは相互に排他的です。組み合わせ可能なインスペクションの場合、各インスペクションは個々の機能と見なされます。

パケット照合の例

次に例を示します。

- パケットが接続制限値のルールと一致し、アプリケーションインスペクションのルールとも一致した場合、両方のクラス マップ アクションが適用されます。
- パケットが HTTP インスペクションで 1 つの ルールと一致し、HTTP インスペクションを含む別のルールとも一致した場合、2 番目のルールのアクションは適用されません。
- パケットが FTP インスペクションで 1 つのルールと一致し、HTTP インスペクションを含む別のルールとも一致した場合、HTTP および FTP インスペクションは組み合わせることができないため、2 番目の ルールのアクションは適用されません。
- パケットが HTTP インスペクションで 1 つのルールと一致し、さらに IPv6 インスペクションを含む別のルールとも一致した場合、IPv6 インスペクションは他のタイプのインスペクションと組み合わせることができるため、両方のアクションが適用されます。

複数の機能アクションが適用される順序

サービス ポリシーの各種のアクションが実行される順序は、テーブル中に出現する順序とは無関係です。

アクションは次の順序で実行されます。

1. QoS 入力ポリシング
2. TCP の正規化、TCP と UDP の接続制限値とタイムアウト、TCP シーケンス番号のランダム化、および TCP ステート バイパス

（注） ASA がプロキシサービス（AAA など）を実行したり、TCP ペイロード（FTP インスペクションなど）を変更したりするときは、TCP ノーマライザはデュアルモードで動作します。その場合、サービスを変更するプロキシやペイロードの前後で適用されます。

3. 他のインスペクションと組み合わせることができるアプリケーションインスペクション：
   1. IPv6
   2. IP オプション
   3. WAAS
4. 他のインスペクションと組み合わせることができないアプリケーション インスペクション：詳細については、「特定の機能アクションの非互換性 （7 ページ）」を参照してください。
5. ASA FirePOWER（ASA SFR）
6. QoS 出力ポリシング
7. QoS 標準プライオリティ キュー

（注） NetFlow セキュア イベント ロギングのフィルタリングとアイデンティティ ファイアウォールのユーザー統計情報は順番に依存しません。

特定の機能アクションの非互換性

一部の機能は同じトラフィックに対して相互に互換性がありません。次のリストには、すべての非互換性が含まれていない場合があります。各機能の互換性については、機能に関する章または項を参照してください。

- QoS プライオリティ キューイングと QoS ポリシングは同じトラフィックの集合に対して設定できません。
- ほとんどのインスペクションは別のインスペクションと組み合わせられないため、同じトラフィックに複数のインスペクションを設定しても、ASA は 1 つのインスペクションだけを適用します。例外は、複数の機能アクションが適用される順序 （6 ページ）に記載されています。
- トラフィックを複数のモジュールに送信されるように設定することはできません。
- HTTP インスペクションは、ASA FirePOWER と互換性がありません。

（注） デフォルト グローバル ポリシーで使用される Default Inspection Traffic トラフィック クラスは、デフォルト ポートをすべてのインスペクションと照合する特別な CLI ショートカットです。ポリシー マップで使用すると、このクラス マップでは、トラフィックの宛先ポートに基づいて、各パケットに正しいインスペクションが適用されます。たとえば、宛先がポート 69 の UDP トラフィックが ASA に到達すると、ASA は TFTP インスペクションを適用し、宛先がポート 21 の TCP トラフィックが到着すると、ASA は FTP インスペクションを適用します。そのため、この場合に限って同じクラス マップに複数のインスペクションを設定できます。通常、ASA は、ポート番号を使用して適用するインスペクションを決定しないため、標準以外のポートなどにも柔軟にインスペクションを適用できます。

複数のサービス ポリシーの機能照合

TCP および UDP トラフィック（およびステートフル ICMP インスペクションがイネーブルの場合は ICMP）の場合、サービス ポリシーはトラフィック フローに対して作用し、個々のパケットに限定されません。トラフィックが、1 つのインターフェイスのポリシーで定義されている機能に一致する既存の接続の一部である場合、そのトラフィック フローを別のインターフェイスのポリシーにある同じ機能と照合することはできません。最初のポリシーのみが使用されます。

たとえば、HTTP トラフィックが、HTTP トラフィックを検査する内部インターフェイスのポリシーと一致するときに、HTTP インスペクション用の外部インターフェイスに別のポリシーがある場合、そのトラフィックが外部インターフェイスの出力側でも検査されることはありません。同様に、その接続のリターン トラフィックが外部インターフェイスの入力ポリシーによって検査されたり、内部インターフェイスの出力ポリシーによって検査されたりすることもありません。

ステートフル ICMP インスペクションをイネーブルにしない場合の ICMP のように、フローとして扱われないトラフィックの場合は、リターン トラフィックを戻り側のインターフェイスの別のポリシー マップと照合できます。

サービス ポリシーのガイドライン

インスペクションのガイドライン

アプリケーション インスペクションのサービス ポリシーに関する詳細なガイドラインを提供する単独のトピックがあります。アプリケーションインスペクションのガイドラインを参照してください。

IPv6 のガイドライン

IPv6 は次の機能でサポートされています。

- 複数の、しかしすべてではないプロトコルに対するアプリケーション インスペクション。詳細については、アプリケーション インスペクションのガイドラインを参照してください。
- ASA FirePOWER
- NetFlow セキュア イベント ロギングのフィルタリング
- SCTP ステート バイパス
- TCP と UDP の接続制限値とタイムアウト、および TCP シーケンス番号のランダム化
- TCP の正規化
- TCP ステート バイパス
- アイデンティティ ファイアウォールのユーザー統計情報

クラスマップ（トラフィック クラス）のガイドライン

すべてのタイプのクラスマップ（トラフィック クラス）の最大数は、シングルモードでは255個、マルチ モードではコンテキストごとに 255 個です。クラス マップには、次のタイプがあります。

- レイヤ 3/4 クラスマップ（通過トラフィックと管理トラフィック向け）。
- インスペクション クラス マップ

- 正規表現クラス マップ
- **match** インスペクション ポリシー マップ下で直接使用されるコマンド

この制限には、すべてのタイプのデフォルト クラス マップも含まれ、ユーザー設定のクラス マップを約 235 に制限します。

サービス ポリシーのガイドライン

- 入力インターフェイスのインターフェイス サービス ポリシーは、特定の機能に対するグローバル サービス ポリシーより優先されます。たとえば、FTP インスペクションのグローバル ポリシーと、TCP 正規化のインターフェイス ポリシーがある場合、FTP インスペクションと TCP 正規化の両方がインターフェイスに適用されます。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入力インターフェイス ポリシーがある場合は、入力インターフェイス ポリシーの FTP インスペクションだけがそのインターフェイスに適用されます。入力またはグローバル ポリシーが機能を実装していない場合は、機能を指定する出力インターフェイスのインターフェイス サービス ポリシーが適用されます。
- 適用できるグローバル ポリシーは 1 つだけです。たとえば、機能セット 1 が含まれたグローバル ポリシーと、機能セット 2 が含まれた別のグローバル ポリシーを作成できません。すべての機能は 1 つのポリシーに含める必要があります。
- コンフィギュレーションに対してサービス ポリシーの変更を加えた場合は、すべての新しい接続で新しいサービス ポリシーが使用されます。既存の接続では、その接続が確立された時点で設定されていたポリシーの使用が続行されます。show コマンドの出力には、古い接続に関するデータは含まれません。

  たとえば、インターフェイスから QoS サービス ポリシーを削除し、変更したバージョンを追加した場合、**show service-policy** コマンドには、新しいサービス ポリシーに一致する新しい接続に関連付けられた QoS カウンタだけが表示されます。古いポリシーの既存の接続はコマンド出力には表示されなくなります。

  すべての接続が新しいポリシーを確実に使用するように、現在の接続を解除し、新しいポリシーを使用して再度接続できるようにします。**clear conn** または **clear local-host** コマンドを使用します。

サービス ポリシーのデフォルト

次の各トピックでは、サービス ポリシーとモジュラ ポリシー フレームワークのデフォルト設定について説明します。

デフォルトのサービス ポリシー設定

デフォルトでは、すべてのデフォルト アプリケーション インスペクション トラフィックに一致するポリシーがコンフィギュレーションに含まれ、特定のインスペクションがすべてのイン

ターフェイスのトラフィックに適用されます（グローバル ポリシー）。すべてのインスペクションがデフォルトでイネーブルになっているわけではありません。適用できるグローバル ポリシーは1つだけなので、グローバル ポリシーを変更する場合は、デフォルトのポリシーを編集するか、デフォルトのポリシーをディセーブルにして新しいポリシーを適用します。（特定の機能では、グローバル ポリシーはインターフェイス ポリシーより優先されます）。

デフォルト ポリシーには、次のアプリケーション インスペクションが含まれます。

- DNS
- FTP
- H323（H225）
- H323（RAS）
- RSH
- RTSP
- ESMTP
- SQLnet
- Skinny（SCCP）
- SunRPC
- SIP
- NetBios
- TFTP
- IP オプション

デフォルトのクラス マップ（トラフィック クラス）

設定には、ASA が default-inspection-trafficDefault Inspection Traffic というデフォルト グローバル ポリシーで使用するデフォルトのレイヤ 3/4 クラス マップ（トラフィック クラス）が含まれます。このクラス マップは、デフォルトのインスペクション トラフィックを照合します。デフォルト グローバル ポリシーで使用されるこのクラスは、デフォルト ポートをすべてのインスペクションと照合する特別なショートカットです。

ポリシーで使用すると、このクラスでは、トラフィックの宛先ポートに基づいて、各パケットに正しいインスペクションが適用されます。たとえば、宛先がポート 69 の UDP トラフィックが ASA に到達すると、ASA は TFTP インスペクションを適用し、宛先がポート 21 の TCP トラフィックが到着すると、ASA は FTP インスペクションを適用します。そのため、この場合に限って同じクラス マップに複数のインスペクションを設定できます。通常、ASA は、ポート番号を使用して適用するインスペクションを決定しないため、標準以外のポートなどにも柔軟にインスペクションを適用できます。

デフォルト コンフィギュレーションにある別のクラス マップは、class-default と呼ばれ、すべてのトラフィックと一致します。このクラス マップは、すべてのレイヤ 3/4 ポリシー マップ

の最後に示され、原則的に、他のすべてのトラフィックでどのようなアクションも実行しないようにASAに通知します。class-defaultクラス（ASDMの任意の通信クラス）を使用する場合は、TCPシーケンスのランダム化、TTLデクリメント、またはその他のオプション属性の変更を有効にするなど、より広範な目的で使用してください。インスペクションには使用しないでください。使用すると、通信の中断が発生する可能性があります。一部の機能はclass-defaultでしか使用できません。

サービス ポリシーの設定

サービス ポリシーの設定では、インターフェイスあたりのサービス ポリシー ルール、またはグローバル ポリシーのサービス ポリシー ルールを1つ以上追加します。ASDMでは、ウィザードを使用してサービスポリシーを作成できます。それぞれのルールごとに、次の要素を指定します。

1. ルールを適用するインターフェイスまたはグローバル ポリシー。
2. アクションを適用するトラフィック。レイヤ3および4のトラフィックを指定できます。
3. トラフィック クラスに適用するアクション。トラフィック クラスごとに複数の競合しないアクションを適用できます。

ポリシーを作成した後にルールを追加したり、ルールやポリシーを移動、変更、または削除したりできます。次の各トピックでは、サービス ポリシーの設定方法について説明します。

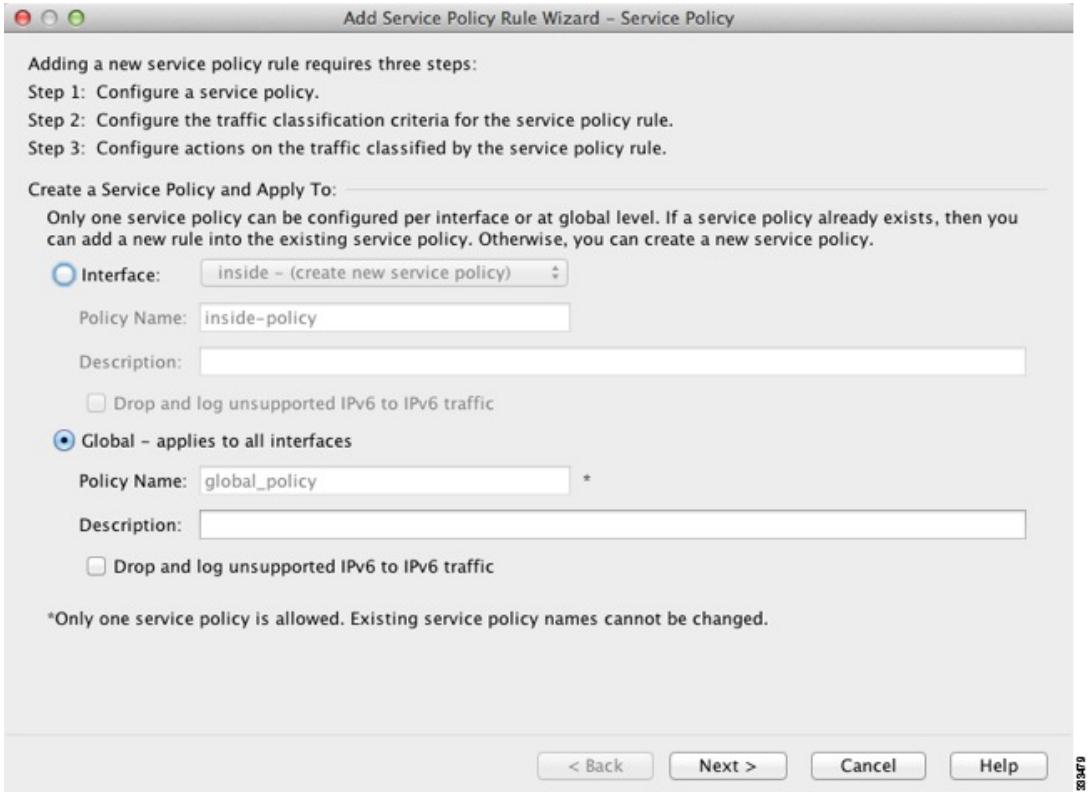
通過トラフィックのサービス ポリシー ルールの追加

通過トラフィックのサービス ポリシー ルールを追加するには、[Add Service Policy Rule Wizard]を使用します。ポリシーの適用範囲として特定のインターフェイスまたはグローバルのいずれかを選択するように求められます。

- インターフェイス サービス ポリシーは、特定の機能に対するグローバル サービス ポリシーより優先されます。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。
- グローバル サービス ポリシーは、すべてのインターフェイスにデフォルト サービスを提供します。インターフェイス固有のポリシーで上書きされない限り、グローバル ポリシーが適用されます。デフォルト アプリケーション インスペクションのサービス ポリシー ルールを含むグローバル ポリシーは、デフォルトで存在します。ウィザードを使用してルールをグローバル ポリシーに追加できます。

手順

ステップ 1 **[Configuration]** > **[Firewall]** > **[Service Policy Rules]** を選択し、[Add] または **[Add]** > **[Add Service Policy Rule]** をクリックします。



ステップ 2 [Create a Service Policy and Apply To] 領域で次の操作を行います。

a) ポリシーを特定の**インターフェイス**に適用するか、すべてのインターフェイスに**グローバル**に適用するかを選択します。

b) [Interface] を選択した場合は、インターフェイスの名前を選択します。インターフェイスにすでにポリシーが設定されている場合は、既存のポリシーにルールを追加していることになります。

c) インターフェイスにまだサービス ポリシーが設定されていない場合は、新しいポリシーの名前を入力します。

d) （任意）ポリシーの説明を入力します。

e) （任意）[Drop and log unsupported IPv6 to IPv6 traffic] オプションをオンにして、IPv6 トラフィックをサポートしないアプリケーション インスペクションによってドロップされる IPv6 トラフィックの syslog（767001）を生成します。デフォルトでは、syslog が生成されません。

f) [Next] をクリックします。

ステップ 3 [Traffic Classification Criteria] ページで、次のいずれかのオプションを選択してポリシー アクションを適用するトラフィックを指定し、[Next] をクリックします。

- [Create a new traffic class]。トラフィック クラスの名前を入力し、任意で説明を入力します。

  基準のいずれかを使用してトラフィックを特定します。

  - [Default Inspection Traffic]：このクラスは、ASA が検査可能なすべてのアプリケーションによって使用される、デフォルトの TCP および UDP ポートを照合します。[Next] をクリックすると、このクラスで定義されているサービスとポートが表示されます。

    デフォルト グローバル ポリシーで使用されるこのオプションは、ルール内で使用されると、トラフィックの宛先ポートに基づいて、パケットごとに正しい検査が適用されるようにします。詳細については、デフォルトのクラス マップ（トラフィック クラス）（10 ページ）を参照してください。

    デフォルト ポートのリストについては、デフォルト インスペクションと NAT に関する制限事項を参照してください。ASA には、デフォルトのインスペクション トラフィックに一致して、すべてのインターフェイス上のトラフィックに共通検査を適用するデフォルト グローバル ポリシーが含まれます。Default Inspection Traffic クラスにポートが含まれているすべてのアプリケーションが、ポリシーマップにおいてデフォルトでイネーブルになっているわけではありません。

    Source and Destination IP Address (ACL を使用) クラスを Default Inspection Traffic クラスと一緒に指定して、照合されるトラフィックを絞り込むことができます。Default Inspection Traffic クラスは一致するポートとプロトコルを指定するので、アクセス リストのポートとプロトコルはすべて無視されます。

  - [Source and Destination IP Address (uses ACL)] ：このクラスは拡張アクセス リストで指定されているトラフィックを照合します。 [**Next**] をクリックすると、アクセス コントロール エントリの属性を入力するように求められ、ウィザードが ACL を作成します。必要に応じて、既存の ACL を選択できます。

    ACE を定義するときに [Match] オプションを選択すると、アドレスに一致するトラフィックにアクションを適用するルールが作成されます。[Do Not Match] オプションでは、トラフィックを指定したアクションの適用から免除します。たとえば、10.1.1.25 を除いて、10.1.1.0/24 のトラフィックすべてを照合し、そのトラフィックに接続制限を適用するとします。この場合は、2 つのルール（[Match] オプションを使用した 10.1.1.0/24 に対するルールおよび [Do Not Match] オプションを使用した 10.1.1.25 に対するルール）を作成します。必ず、Do Not Match ルールが Match ルールの上になるように配置してください。順序を逆にすると、10.1.1.25 が最初に Match ルールを照合することになります。

（注） このタイプの新しいトラフィック クラスを作成する場合は、最初にアクセス コントロール エントリ（ACE）を 1 つだけ指定できます。ルールを追加した後は、同じインターフェイスまたはグローバル ポリシーに新しいルールを追加し、それから [Add rule to existing traffic class] を指定することによって、ACE を追加できます（以下を参照）。

- [Tunnel Group] ：このクラスは、QoS を適用するトンネル グループ（接続プロファイル）のトラフィックを照合します。その他にもう 1 つのトラフィック照合オプションを指定してトラフィック照合対象をさらに絞込み、[Any Traffic]、[Source and Destination IP Address (uses ACL)]、または [Default Inspection Traffic] を排除できます。

  [Next] をクリックすると、トンネル グループを選択するように求められます（必要に応じて新しい接続グループを作成できます）。各フローをポリシングするには、[Match flow destination IP address] をオンにします。固有の IP 宛先アドレスに向かうトラフィックは、すべてフローと見なされます。

- **[TCP or UDP or SCTP Destination Port]**：クラスは 1 つのポートまたは連続する一定範囲のポートを照合します。[Next] をクリックすると、プロトコルを選択してポート番号を入力するように求められます。ASDM ですでに定義されているポートを選択するには、[...] をクリックします。

ヒント 複数の非連続ポートを使用するアプリケーションの場合は、[Source and Destination IP Address (uses ACL)] を使用して各ポートを照合します。

- [RTP Range]：クラス マップは、RTP トラフィックを照合します。[Next] をクリックすると、2000 ～ 65534 の間の RTP ポート範囲を入力するように求められます。範囲内の最大ポート数は、16383 です。

- [IP DiffServ CodePoints (DSCP)]：このクラスは、IP ヘッダーの最大 8 つの DSCP 値を照合します。[Next] をクリックすると、目的の値を選択または入力する（それらの値を [Match] または [DSCP] リストに移動する）ように求められます。

- [IP Precedence]：このクラス マップは、IP ヘッダーの TOS バイトによって表される、最大 4 つの Precedence 値を照合します。[Next] をクリックすると、値を入力するように求められます。

- [Any Traffic]：すべてのトラフィックを照合します。

- [Add rule to existing traffic class]。 すでに同じインターフェイスにサービス ポリシー ルールを指定している場合、またはグローバル サービス ポリシーを追加する場合は、このオプションによって既存のアクセス リストに ACE を追加できます。このインターフェイスの

サービス ポリシー ルールで [Source and Destination IP Address (uses ACL)] オプションを選択した場合は、事前に作成したすべてのアクセス リストに ACE を追加できます。このトラフィック クラスでは、複数の ACE を追加する場合であっても、1 セットのルール アクションしか指定できません。この手順全体を繰り返すことによって、複数の ACE を同じトラフィック クラスに追加できます。[Next] をクリックすると、アクセス コントロール エントリの属性を入力するように求められます。

- **[Use an existing traffic class]。**別のインターフェイスのルールで使用されるトラフィック クラスを作成した場合は、そのトラフィック クラス定義をこのルールで再使用できます。1 つのルールのトラフィック クラスを変更すると、その変更は同じトラフィック クラスを使用するすべてのルールに継承されます。コンフィギュレーションに CLI で入力した **class-map** コマンドが含まれている場合は、それらのトラフィック クラス名も使用できます（ただし、そのトラフィック クラスの定義を表示するには、そのルールを作成する必要があります）。
- [Use class default as the traffic class]。このオプションでは、すべてのトラフィックを照合する class-default クラスを使用します。class-default クラスは、ASA によって自動的に作成され、ポリシーの最後に配置されます。このクラスは、アクションを何も適用しない場合でも ASA によって作成されますが、内部での使用に限られます。必要に応じて、このクラスにアクションを適用できます。これは、すべてのトラフィックを照合する新しいトラフィック クラスを作成するよりも便利な場合があります。class-default クラスを使用して、このサービス ポリシーにルールを 1 つだけ作成できます。これは、各トラフィック クラスを関連付けることができるのは、サービス ポリシーごとに 1 つのルールだけであるためです。

ステップ 4 追加設定が必要なトラフィック一致基準を選択した場合は、目的のパラメータを入力して [Next] をクリックします。

ステップ 5 [Rule Actions] ページで、1 つまたは複数のルール アクションを設定します。適用できる機能およびアクション（詳細情報へのリンクを含む）については、サービス ポリシーで設定される機能 （3 ページ）を参照してください。

ステップ 6 [終了（Finish）] をクリックします。

管理トラフィックのサービス ポリシー ルールの設定

管理目的で ASA に向けられるトラフィックのサービス ポリシー ルールを追加するには、[Add Service Policy Rule] ウィザードを使用します。ポリシーの適用範囲として特定のインターフェイスまたはグローバルのいずれかを選択するように求められます。

- インターフェイス サービス ポリシーは、特定の機能に対するグローバル サービス ポリシーより優先されます。たとえば、RADIUS アカウンティング インスペクションを使用するグローバル ポリシーと接続制限を使用するインターフェイス ポリシーがある場合、RADIUS アカウンティングと接続制限の両方がそのインターフェイスに適用されます。ただし、RADIUS アカウンティングを使用するグローバル ポリシーと RADIUS アカウンティ

ングを使用するインターフェイス ポリシーがある場合、インターフェイス ポリシーRADIUS アカウンティングだけがそのインターフェイスに適用されます。

- グローバル サービス ポリシーは、すべてのインターフェイスにデフォルト サービスを提供します。インターフェイス固有のポリシーで上書きされない限り、グローバル ポリシーが適用されます。デフォルト アプリケーション インスペクションのサービス ポリシー ルールを含むグローバル ポリシーは、デフォルトで存在します。ウィザードを使用してルールをグローバル ポリシーに追加できます。

手順

ステップ 1 **[Configuration]** > **[Firewall]** > **[Service Policy Rules]** を選択し、[Add] または **[Add]** > **[Add Management Service Policy Rule]** をクリックします。

ステップ 2 [Create a Service Policy and Apply To] 領域で次の操作を行います。

a) ポリシーを特定の**インターフェイス**に適用するか、すべてのインターフェイスに**グローバル**に適用するかを選択します。

b) [Interface] を選択した場合は、インターフェイスの名前を選択します。インターフェイスにすでにポリシーが設定されている場合は、既存のポリシーにルールを追加していることになります。

c) インターフェイスにまだサービス ポリシーが設定されていない場合は、新しいポリシーの名前を入力します。

d) （任意）ポリシーの説明を入力します。

e) [Next] をクリックします。

ステップ 3 [Traffic Classification Criteria] ページで、次のいずれかのオプションを選択してポリシー アクションを適用するトラフィックを指定し、[Next] をクリックします。

- [Create a new traffic class]。トラフィック クラスの名前を入力し、任意で説明を入力します。

  基準のいずれかを使用してトラフィックを特定します。

  - [Source and Destination IP Address (uses ACL)] ：このクラスは拡張アクセス リストで指定されているトラフィックを照合します。 [**Next**] をクリックすると、アクセス コントロール エントリの属性を入力するように求められ、ウィザードが ACL を作成します。必要に応じて、既存の ACL を選択できます。

    ACE を定義するときに [Match] オプションを選択すると、アドレスに一致するトラフィックにアクションを適用するルールが作成されます。[Do Not Match] オプションでは、トラフィックを指定したアクションの適用から免除します。たとえば、10.1.1.25 を除いて、10.1.1.0/24 のトラフィックすべてを照合し、そのトラフィックに接続制限を適用するとします。この場合は、2 つのルール（[Match] オプションを使用した 10.1.1.0/24 に対するルールおよび [Do Not Match] オプションを使用した 10.1.1.25 に対するルール）を作成します。必ず、Do Not Match ルールが Match ルールの上になるように配置してください。順序を逆にすると、10.1.1.25 が最初に Match ルールを照合することになります。

- **[TCP or UDP or SCTP Destination Port]**：クラスは 1 つのポートまたは連続する一定範囲のポートを照合します。[Next] をクリックすると、プロトコルを選択してポート番号を入力するように求められます。ASDM ですでに定義されているポートを選択するには、[...] をクリックします。



ヒント　複数の非連続ポートを使用するアプリケーションの場合は、[Source and Destination IP Address (uses ACL)] を使用して各ポートを照合します。

- [Add rule to existing traffic class]。 すでに同じインターフェイスにサービス ポリシー ルールを指定している場合、またはグローバル サービス ポリシーを追加する場合は、このオプションによって既存のアクセス リストに ACE を追加できます。このインターフェイスのサービス ポリシー ルールで [Source and Destination IP Address (uses ACL)] オプションを選択した場合は、事前に作成したすべてのアクセス リストに ACE を追加できます。このトラフィック クラスでは、複数の ACE を追加する場合であっても、1 セットのルール アクションしか指定できません。この手順全体を繰り返すことによって、複数の ACE を同じトラフィック クラスに追加できます。[Next] をクリックすると、アクセス コントロール エントリの属性を入力するように求められます。
- **[Use an existing traffic class]。**別のインターフェイスのルールで使用されるトラフィック クラスを作成した場合は、そのトラフィック クラス定義をこのルールで再使用できます。1 つのルールのトラフィック クラスを変更すると、その変更は同じトラフィック クラスを使用するすべてのルールに継承されます。コンフィギュレーションに CLI で入力した **class-map** コマンドが含まれている場合は、それらのトラフィック クラス名も使用できます（ただし、そのトラフィック クラスの定義を表示するには、そのルールを作成する必要があります）。

ステップ 4　追加設定が必要なトラフィック一致基準を選択した場合は、目的のパラメータを入力して [Next] をクリックします。

ステップ 5　[Rule Actions] ページで、1 つまたは複数のルール アクションを設定します。

- RADIUS アカウンティング インスペクションを設定するには、[RADIUS Accounting Map] ドロップダウン リストからインスペクション マップを選択するか、または [Configure] をクリックしてマップを追加します。詳細については、「サービス ポリシーで設定される機能 （3 ページ）」を参照してください。
- 接続を設定するには、特定のトラフィック クラスの接続の設定（すべてのサービス）を参照してください。

ステップ 6　[終了（Finish）] をクリックします。

サービス ポリシー ルールの順序の管理

インターフェイス上またはグローバル ポリシー内でのサービス ポリシー ルールの順序は、トラフィックへのアクションの適用方法に影響します。パケットがサービス ポリシーのルールを照合する方法については、次のガイドラインを参照してください。

- パケットは、機能タイプごとにサービス ポリシーのルールを 1 つだけ照合できます。
- パケットが、1 つの機能タイプのアクションを含むルールを照合する場合、ASA は、その機能タイプを含む、後続のどのルールに対してもそのパケットを照合しません。
- ただし、そのパケットが異なる機能タイプの後続のルールを照合する場合、ASA は後続ルールのアクションも適用します。

たとえば、パケットが接続制限のルールを照合し、アプリケーション インスペクションのルールも照合する場合は、両方のアクションが適用されます。

パケットがアプリケーション インスペクションのルールを照合し、アプリケーション インスペクションを含む別のルールを照合する場合、2 番目のルール アクションは適用されません。

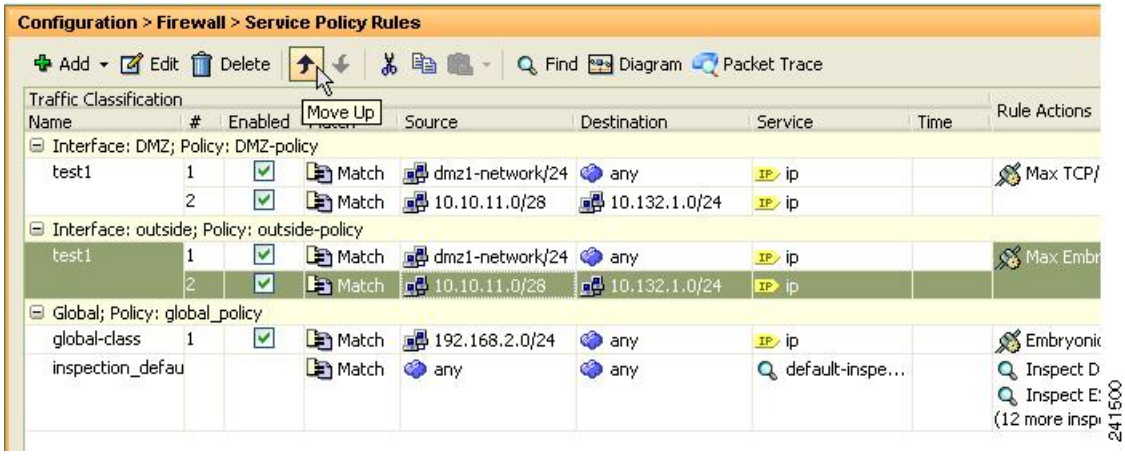
ルールに複数の ACE が組み込まれたアクセス リストが含まれる場合は、ACE の順序もパケット フローに影響します。ASA は、リストのエントリの順序に従って、各 ACE に対してパケットをテストします。一致が見つかると、ACE はそれ以上チェックされません。たとえば、すべてのトラフィックを明示的に許可する ACE を ACL の先頭に作成した場合は、残りのステートメントはチェックされません。

ルールまたはルール内での ACE の順序を変更するには、次の手順を実行します。

手順

ステップ 1 **[Configuration]** > **[Firewall]** > **[Service Policy Rules]** ペインで、上または下に動かすルールまたは ACE を選択します。

ステップ 2 [Move Up] または [Move Down] ボタンをクリックします。



（注） 複数のサービス ポリシーで使用されるアクセス リストで ACE を並べ替えると、その変更はすべてのサービス ポリシーで継承されます。

ステップ 3 ルールまたは ACE を並べ替えたら、[Apply] をクリックします。

サービス ポリシーの履歴

機能名	リリース	説明
モジュラ ポリシー フレームワーク	7.0(1)	モジュラ ポリシー フレームワークが導入されました。
RADIUS アカウンティング トラフィックで使用する管理クラス マップ	7.2(1)	RADIUS アカウンティング トラフィックで使用する管理クラス マップが導入されました。**class-map type management** コマンドおよび **inspect radius-accounting** コマンドが導入されました。
インスペクション ポリシー マップ	7.2(1)	インスペクション ポリシー マップが導入されました。**class-map type inspect** コマンドが導入されました。
正規表現およびポリシー マップ	7.2(1)	インスペクション ポリシー マップで使用される正規表現およびポリシー マップが導入されました。**class-map type regex** コマンド、**regex** コマンド、および **match regex** コマンドが導入されました。
インスペクション ポリシー マップの match any	8.0(2)	インスペクション ポリシー マップで使用される **match any** キーワードが導入されました。トラフィックを 1 つ以上の基準に照合してクラスマップに一致させることができます。以前は、**match all** だけが使用可能でした。

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。