CHAPTER 6

アクセス ルールの設定

この章では、アクセス ルールを使用して、ASA 経由でのネットワーク アクセスを制御する方法について説明します。この章は次の項で構成されています。

（注） ルーテッド ファイアウォール モードの場合もトランスペアレント ファイアウォール モードの場合も、ネットワーク アクセスを制御するには、アクセス ルールを使用します。トランスペアレント モードでは、アクセス ルール（レイヤ 3 トラフィックの場合）と EtherType ルール（レイヤ 2 トラフィックの場合）の両方を使用できます。

また、ASA インターフェイスに管理アクセスの目的でアクセスするには、ホスト IP アドレスを許可するアクセス ルールは必要ありません。一般的な操作のコンフィギュレーション ガイドの Chapter 43, “Configuring Management Access,” に従って管理アクセスを設定することだけが必要です。

アクセス ルールに関する情報

アクセス ポリシーは、1 つ以上のアクセス ルール、インターフェイスごとのまたはすべてのインターフェイスに対するグローバルな EtherType ルール、またはその両方から構成されます。

ルーテッド ファイアウォール モードおよびトランスペアレント ファイアウォール モードの場合は、アクセス ルールを使用して IP トラフィックを制御できます。アクセス ルールでは、プロトコル、送信元および宛先の IP アドレスまたはネットワーク、および任意で送信元ポートと宛先ポートに基づいてトラフィックが許可または拒否されます。

トランスペアレント モードの場合に限り、EtherType ルールによって非 IP トラフィックのネットワーク アクセスが制御されます。EtherType ルールでは、EtherType に基づいてトラフィックが許可または拒否されます。

この項は、次の内容で構成されています。

ルールに関する一般情報

この項では、アクセス ルールと EtherType ルールの両方について説明します。次の項目を取り上げます。

暗黙的な許可

ルーテッド モードの場合、デフォルトでは次のタイプのトラフィックが許可されます。

- 高セキュリティ インターフェイスから低セキュリティ インターフェイスへの IPv4 トラフィック。
- 高セキュリティ インターフェイスから低セキュリティ インターフェイスへの IPv6 トラフィック。

トランスペアレント モードの場合、デフォルトでは次のタイプのトラフィックが許可されます。

- 高セキュリティ インターフェイスから低セキュリティ インターフェイスへの IPv4 トラフィック。
- 高セキュリティ インターフェイスから低セキュリティ インターフェイスへの IPv6 トラフィック。
- 双方向の Address Resolution Protocol（ARP; アドレス解決プロトコル）。

（注）　ARP トラフィックは ARP インスペクションによって制御できますが、アクセス ルールによって制御することはできません。

- 双方向の Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）。

他のトラフィックには、アクセス ルール（IPv4 および IPv6）、または EtherType ルール（非 IPv4/IPv6）のいずれかを使用する必要があります。

インターフェイス アクセス ルールとグローバル アクセス ルールに関する情報

アクセス ルールを特定のインターフェイスに適用するか、またはアクセス ルールを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。インターフェイス アクセス ルールと一緒にグローバル アクセス ルールを設定できます。この場合、特定のインターフェイス アクセス ルールが常に汎用のグローバル アクセス ルールよりも前に処理されます。

（注）　グローバル アクセス ルールは、着信トラフィックにだけ適用されます。「着信ルールと発信ルール」（P.6-3）を参照してください。

同じインターフェイスでのアクセス ルールと EtherType ルールの使用

アクセス ルールと EtherType ルールの両方を各方向のインターフェイスに適用できます。

ルールの順序

ルールの順序が重要です。ASA において、パケットを転送するかドロップするかの判断が行われる場合、ASA では、パケットと各ルールとの照合が、それらのルールの並び順に従って行われます。いずれかのルールに合致した場合、それ以降のルールはチェックされません。たとえば、先頭に作成したアクセス ルールが、インターフェイスに対してすべてのトラフィックを明示的に許可するものであれば、それ以降のルールはチェックされません。詳細については、「暗黙の拒否」（P.6-3）を参照してください。

ルールは、非アクティブにすることで、ディセーブルにできます。

暗黙の拒否

ACL の最後で暗黙的な拒否が設定されるため、明示的に許可しない限り、トラフィックは通過できません。たとえば、特定のアドレスを除くすべてのユーザに、ASA 経由でのネットワークにアクセスすることを許可する場合、特定のアドレスを拒否したうえで、他のすべてのユーザを許可します。

EtherType ACL の場合、ACL の末尾にある暗黙的な拒否は、IP トラフィックや ARP には影響しません。たとえば、EtherType 8037 を許可する場合、ACL の末尾にある暗黙的な拒否によって、拡張 ACL で以前許可（または高位のセキュリティ インターフェイスから低位のセキュリティ インターフェイスへ暗黙的に許可）した IP トラフィックがブロックされることはありません。ただし、EtherType ACE とのすべてのトラフィックを明示的に拒否する場合、IP と ARP のトラフィックが拒否されます。

グローバル アクセス ルールを設定すると、暗黙的な拒否はグローバル ルールが処理された *後*になります。次の動作の順序を参照してください。

1. インターフェイス アクセス ルール。
2. グローバル アクセス ルール。
3. 暗黙的な拒否。

コメントの使用

[ASDM access rule] ウィンドウでは、ルールの隣に表示されるコメントは、そのルールの前に設定されたものです。つまり、CLI から設定したコメントを [ASDM access rule] ウィンドウで表示する場合、CLI でコメントの後に設定されたルールの隣にそのコメントが表示されます。ただし、ASDM のパケット トレーサは、CLI の照合ルール後に設定されたコメントに一致します。

NAT とアクセス ルール

アクセス ルールは、NAT を設定している場合でも、アクセス ルールの一致を決定する際に常に実際の IP アドレスを使用します。たとえば、内部サーバ 10.1.1.5 用の NAT を設定して、パブリックにルーティング可能な外部の IP アドレス 209.165.201.5 をこのサーバに付与する場合は、この内部サーバへのアクセスを外部トラフィックに許可するアクセス ルールの中で、サーバのマッピング アドレス（209.165.201.5）ではなく実際のアドレス（10.1.1.5）を参照する必要があります。

着信ルールと発信ルール

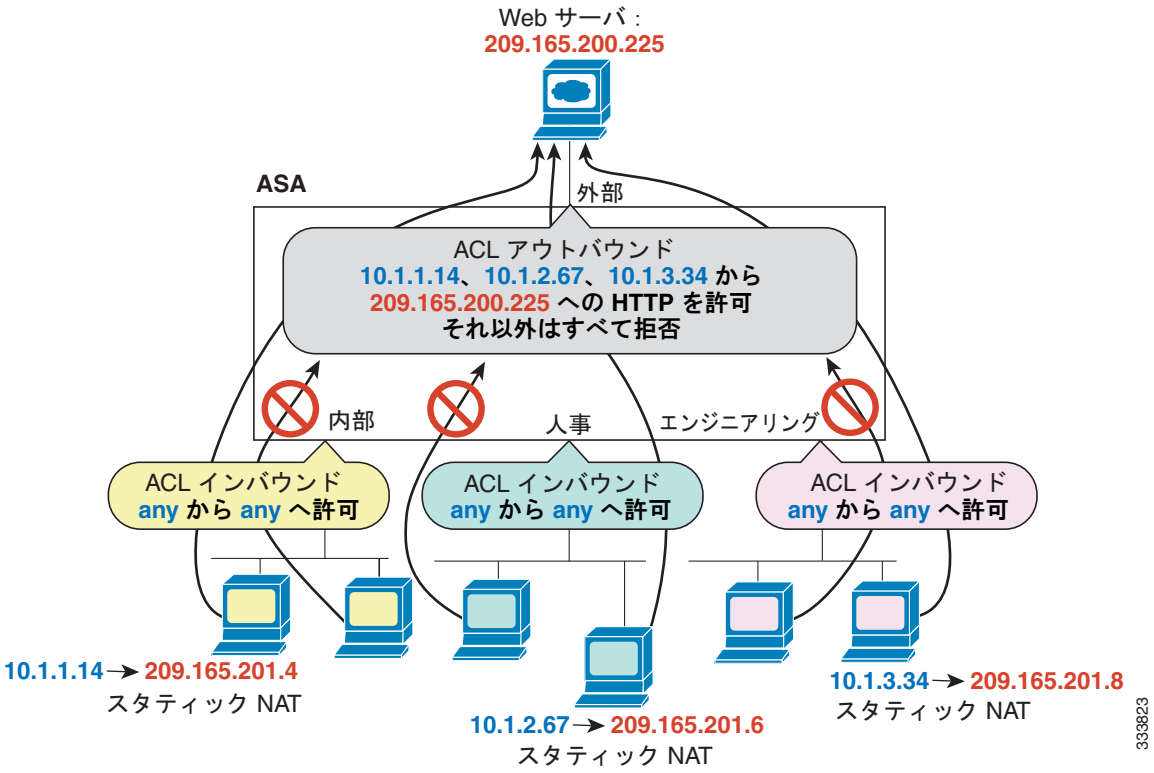
ASA では、次の 2 つの ACL タイプがサポートされています。

- 着信：着信アクセス ルールは、インターフェイスに入ってくるトラフィックに適用されます。グローバル アクセス ルールは常に着信です。
- アウトバウンド：アウトバウンド ACL は、インターフェイスから送信されるトラフィックに対して適用されます。

（注）「インバウンド」および「アウトバウンド」は、インターフェイスにおける ACL の適用対象を表したもので、前者は、インターフェイスにおいて ASA により受信されるトラフィックに ACL が適用されることを表し、後者はインターフェイスにおいて ASA から送信されるトラフィックに ACL が適用されることを表しています。これらの用語は、一般に着信と呼ばれる、セキュリティの低いインターフェイスから高いインターフェイスへのトラフィックの移動や、一般に発信と呼ばれる、セキュリティの高いインターフェイスから低いインターフェイスへのトラフィックの移動を意味しません。

たとえば、内部ネットワーク上の特定のホストに限って、外部ネットワーク上の Web サーバにアクセスできるようにする場合などには、アウトバウンド ACL が有用です。複数のインバウンド ACL を作成してアクセスを制限することもできますが、指定したホストだけアクセスを許可するアウトバウンド ACL を 1 つだけ作成する方が効率的です（図 6-1 を参照）。このアウトバウンド ACL を使用すれば、その他のホストが外部ネットワークへアクセスすることもできなくなります。

図 6-1　アウトバウンド ACL



アクセス ルールに関する情報

この項では、アクセス ルールについて説明します。次の項目を取り上げます。

- 「リターン トラフィックに対するアクセス ルール」（P.6-5）

- 「アクセス ルールを使用したトランスペアレント ファイアウォールを介したブロードキャストとマルチキャスト トラフィックの許可」（P.6-5）
- 「管理アクセス ルール」（P.6-6）

リターン トラフィックに対するアクセス ルール

ルーテッド モードとトランスペアレント モードの両方に対する TCP 接続および UDP 接続については、リターン トラフィックを許可するためのアクセス ルールは必要ありません。ASA は、確立された双方向接続のリターン トラフィックをすべて許可します。

ただし、ICMP などのコネクションレス型プロトコルについては、ASA は単方向セッションを確立します。したがって、（ACL を送信元インターフェイスと宛先インターフェイスに適用することで）アクセス ルールで双方向の ICMP を許可するか、ICMP インスペクション エンジンをイネーブルにする必要があります。ICMP インスペクション エンジンは、ICMP セッションを双方向接続として扱います。

アクセス ルールを使用したトランスペアレント ファイアウォールを介したブロードキャストとマルチキャスト トラフィックの許可

ルーテッド ファイアウォール モードでは、ブロードキャストとマルチキャスト トラフィックは、アクセス ルールで許可されている場合でもブロックされます。これには、サポートされていないダイナミック ルーティング プロトコルおよび DHCP（DHCP リレーを設定している場合を除く）が含まれます。トランスペアレント ファイアウォール モードでは、すべての IP トラフィックの通過を許可できます。この機能は、たとえば、ダイナミック ルーティングが許可されていないマルチ コンテキスト モードで特に有用です。

（注） これらの特殊なタイプのトラフィックはコネクションレス型であるため、アクセス ルールを両方のインターフェイスに適用して、リターン トラフィックの通過を許可する必要があります。

表 6-1 に、トランスペアレント ファイアウォールの通過を許可できる一般的なトラフィック タイプを示します。

表 6-1　トランスペアレント ファイアウォールの特殊トラフィック

トラフィックのタイプ	プロトコルまたはポート	注釈
DHCP	UDP ポート 67 および 68	DHCP サーバがイネーブルの場合、ASA は DHCP パケットの通過を拒否します。
EIGRP	プロトコル 88	—
OSPF	プロトコル 89	—
マルチキャスト ストリーム	UDP ポートは、アプリケーションによって異なります。	マルチキャスト ストリームは、常に Class D アドレス（224.0.0.0 to 239.x.x.x）に送信されます。
RIP（v1 または v2）	UDP ポート 520	—

管理アクセス ルール

ASA 宛ての管理トラフィックを制御するアクセス ルールを設定できます。to-the-box 管理トラフィックに関するアクセス コントロール ルール（HTTP、Telnet、および SSH など）は、管理アクセス ルールよりも優先されます。したがって、このような許可された管理トラフィックは、to-the-box ACL で明示的に拒否されている場合でも着信が許可されます。

EtherType ルールに関する情報

この項では、EtherType ルールについて説明します。次の項目を取り上げます。

- 「サポートされている EtherType およびその他のトラフィック」（P.6-6）
- 「リターン トラフィックに対するアクセス ルール」（P.6-6）
- 「MPLS の許可」（P.6-6）

サポートされている EtherType およびその他のトラフィック

EtherType ルールは次を制御します。

- 一般的なタイプの IPX および MPLS ユニキャストまたはマルチキャストを含む、16 ビットの 16 進数値で示された EtherType。
- イーサネット V2 フレーム。
- デフォルトで許可される BPDU。BPDU は、SNAP でカプセル化されており、ASA は特別に BPDU を処理するように設計されています。
- トランク ポート（シスコ専用）BPDU。トランク BPDU のペイロードには VLAN 情報が含まれるので、BPDU を許可すると、ASA により、発信 VLAN を使用してペイロードが修正されます。
- IS-IS。

次のタイプのトラフィックはサポートされていません。

- 802.3 形式フレーム：type フィールドではなく length フィールドが使用されるため、ルールでは処理されません。

リターン トラフィックに対するアクセス ルール

EtherType はコネクションレス型であるため、トラフィックを両方向に通過させる必要がある場合は、両方のインターフェイスにルールを適用する必要があります。

MPLS の許可

MPLS を許可する場合は、ラベル配布プロトコル（LDP）およびタグ配布プロトコル（TDP）の TCP 接続が ASA を経由して確立されるようにしてください。これには、ASA インターフェイス上の IP アドレスを LDP セッションまたは TDP セッションの router-id として使用するように、ASA に接続されている両方の MPLS ルータを設定します（LDP および TDP を使用することにより、MPLS ルータは、転送するパケットに使用するラベル（アドレス）をネゴシエートできるようになります）。

Cisco IOS ルータで、使用プロトコル（LDP または TDP）に適したコマンドを入力します。*interface* は、ASA に接続されているインターフェイスです。

```
hostname(config)# mpls ldp router-id interface force
```

または

```
hostname(config)# tag-switching tdp router-id interface force
```

アクセス ルールのライセンス要件

モデル	ライセンス要件
すべてのモデル	基本ライセンス

ガイドラインと制限事項

この項では、この機能のガイドラインと制限事項について説明します。

コンテキスト モードのガイドライン

シングル コンテキスト モードとマルチ コンテキスト モードでサポートされています。

ファイアウォール モードのガイドライン

ルーテッド ファイアウォール モードとトランスペアレント ファイアウォール モードでサポートされています。

IPv6 のガイドライン

IPv6 をサポートします。（9.0 以降）送信元アドレスと宛先アドレスには IPv4 アドレスと IPv6 アドレスの組み合わせを含めることができます。9.0 よりも前のバージョンでは、別の IPv6 アクセス ルールを作成する必要があります。

デフォルト設定

「暗黙的な許可」（P.6-2）を参照してください。

アクセス ルールの設定

この項では、次のトピックについて取り上げます。

アクセス ルールの追加

アクセス ルールを適用するには、次の手順を実行します。

手順の詳細

ステップ 1　[Configuration] > [Firewall] > [Access Rules] の順に選択します。

ステップ 2　[Add] をクリックし、次のいずれかのオプションを選択します。

[Add Access Rule] ダイアログボックスが表示されます。

ステップ 3　[Interface] ドロップダウン リストから、ルールを適用するインターフェイスを選択します。グローバル ルールを適用する場合は、[Any] を選択します。

ステップ 4　[Action] フィールドで、目的のアクションに対応するオプション ボタンをクリックします。オプション ボタンは次のいずれかです。

- [Permit]：条件に合致した場合にアクセスが許可されます。
- [Deny]：条件に合致した場合にアクセスが拒否されます。

ステップ 5　指定した宛先に対してトラフィックを許可または拒否する送信元のネットワーク、インターフェイス IP、またはアドレスに対応する IP アドレスを、[Source] フィールドに入力します。IPv4 または IPv6 アドレスのいずれかを使用できます。

インターフェイスで IPv6 をイネーブルにする方法の詳細については、一般的な操作のコンフィギュレーション ガイドの “Configuring IPv6 Addressing” section on page 10-18 を参照してください。

ステップ 6　[User] フィールドに、ACL に対するユーザ名またはグループを入力します。ユーザ名は、*domain_NetBIOS_name\user_name* という形式で入力します。グループ名は、*domain_NetBIOS_name\group_name* という形式で入力します。

送信元 IP アドレスではなくユーザ名とユーザ グループ名に基づいてアクセス ルールを設定できます。ASA は、IP アドレスと Windows Active Directory のログイン情報の関連付けに基づいてセキュリティ ポリシーを適用し、ネットワーク IP アドレスではなくマッピングされたユーザ名を使用してイベントを報告します。

詳細については、一般的な操作のコンフィギュレーション ガイドの “Configuring Identity-Based Security Policy” section on page 36-24 を参照してください。

ステップ 7　ユーザ名とユーザ グループを参照するには、省略符号（[...]）ボタンをクリックします。[Browse User] ダイアログボックスが表示されます。

ステップ 8　[Source] フィールドで指定した送信元からのトラフィックを許可または拒否する宛先のネットワーク、インターフェイス IP、またはアドレスに対応する IP アドレスを、[Destination] フィールドに入力します。IPv4 または IPv6 アドレスのいずれかを使用できます。

ステップ 9　サービス タイプを選択します。

ステップ 10　（任意）トラフィックをどのような場合に許可しどのような場合に拒否するかを指定するアクセス ルールに時間範囲を追加する場合は、[More Options] をクリックしてリストを展開します。

a.　[Time Range] ドロップダウン リストの右側にある参照ボタンをクリックします。

[Browse Time Range] ダイアログボックスが表示されます。

b.　[Add] をクリックします。

[Add Time Range] ダイアログボックスが表示されます。

c.　[Time Range Name] フィールドに、時間範囲の名前を入力します。ただし、スペースは使用できません。

d. [Start Time] および [End Time] で、開始時間および終了時間を選択します。

e. 毎日または隔週でその時間範囲がアクティブになるようにするなど、時間範囲に関する追加制限を指定する場合は、[Add] をクリックし、指定する内容を選択します。

f. [OK] をクリックすると、時間範囲について任意で指定した内容が適用されます。

ステップ 11　（任意）[Description] フィールドに、アクセス ルールの内容説明を入力します。

この説明は、複数行に渡って入力できますが、各行に入力できるのは最大で 100 文字までです。

ステップ 12　（任意）デフォルトでは、ロギングがイネーブルになっています。ロギングをディセーブルにするには、チェックボックスをオフにします。また、ドロップダウン リストからロギング レベルを変更することもできます。デフォルトのロギング レベルは [Informational] です。

ステップ 13　[OK] をクリックします。新規に設定したアクセス ルールとともにアクセス ルールが表示されます。

ステップ 14　[Apply] をクリックし、アクセス ルールを設定に保存します。

アクセス ルールを選択して [Edit] または [Delete] をクリックすると、特定のアクセス ルールを編集または削除できます。

EtherType ルールの追加（トランスペアレント モードのみ）

[EtherType Rules] ウィンドウに、パケット EtherType に基づくアクセス ルールが表示されます。EtherType ルールは、トランスペアレント モードで動作する ASA において、非 IP 関連トラフィック ポリシーを設定する場合に使用されます。トランスペアレント モードでは、拡張アクセス ルールと EtherType アクセス ルールの両方をインターフェイスに適用できます。EtherType ルールは、拡張アクセス ルールに優先されます。

EtherType ルールの詳細については、「アクセス ルールに関する情報」（P.6-1）を参照してください。

EtherType ルールを追加するには、次の手順を実行します。

ステップ 1　[Configuration] > [Device Management] > [Management Access] > [EtherType Rules] を選択します。

ステップ 2　[Add] をクリックします。

[Add EtherType rules] ウィンドウが表示されます。

ステップ 3　（任意）特定の位置に新しい EtherType ルールを追加する場合は、まず既存のルールをいずれか 1 つ選択します。そのうえで [Insert...] をクリックすると、選択したルールの前に目的の EtherType ルールが追加されます。選択したルールの後に EtherType ルールを追加する場合は、[Insert After...] をクリックします。

ステップ 4　[Interface] ドロップダウン リストから、ルールを適用するインターフェイスを選択します。グローバル ルールを適用する場合は、[Any] を選択します。

ステップ 5　[Action] フィールドで、目的のアクションに対応するオプション ボタンをクリックします。オプション ボタンは次のいずれかです。

- [Permit]：条件に合致した場合にアクセスが許可されます。
- [Deny]：条件に合致した場合にアクセスが拒否されます。

ステップ 6　[EtherType] フィールドで、ドロップダウン リストから、EtherType 値を選択します。

ステップ 7　（任意）[Description] フィールドに、ルールの内容説明を入力します。

この説明は、複数行に渡って入力できますが、各行に入力できるのは最大で 100 文字までです。

ステップ 8　（任意）このルールを適用するトラフィックの方向を指定する場合は、[More Options] をクリックしてリストを展開し、次のいずれかのオプション ボタンをクリックして、方向を指定します。

- [In]：着信トラフィック
- [Out]：発信トラフィック

ステップ 9　[OK] をクリックします。

管理アクセス ルールの設定

特定のピア（または複数のピア）からセキュリティ アプライアンスへの to-the-box 管理トラフィックに関するアクセス コントロールをサポートするインターフェイス ACL を設定できます。このタイプの ACL は、IKE DoS（サービス拒絶）攻撃をブロックする場合などに有用です

to-the-box トラフィックのパケットを許可または拒否する拡張 ACL を設定するには、次の手順を実行します。

ステップ 1　[Configuration] > [Device Management] > [Management Access] > [Management Access Rules] を選択します。

ステップ 2　[Add] をクリックし、次のいずれかの処理内容を選択します。

[Add Management Access Rule] ダイアログボックスが表示されます。

ステップ 3　[Interface] ドロップダウン リストから、ルールを適用するインターフェイスを選択します。グローバル ルールを適用する場合は、[Any] を選択します。

ステップ 4　[Action] フィールドで、次のいずれかのオプション ボタンをクリックし、アクションを選択します。

- [Permit]：条件に合致した場合にアクセスが許可されます。
- [Deny]：条件に合致した場合にアクセスが拒否されます。

ステップ 5　トラフィックを許可または拒否する送信元のネットワーク オブジェクト グループ、インターフェイス IP、またはアドレスに対応する IP アドレスを、[Source] フィールドに入力します。IPv4 または IPv6 アドレスのいずれかを使用できます。

（注）　IPv6 アドレスを使用して拡張 ACL を設定する場合は、少なくとも 1 つのインターフェイスで IPv6 を事前にイネーブルにしておく必要があります。インターフェイスで IPv6 をイネーブルにする方法の詳細については、一般的な操作のコンフィギュレーション ガイドの “Configuring IPv6 Addressing” section on page 10-18 を参照してください。

ステップ 6　[Service] フィールドで、ルールに指定するトラフィックのサービス名を入力するか、省略符号（[...]）ボタンをクリックしてサービスを参照します。

ステップ 7　（任意）[Description] フィールドに、追加する管理アクセス ルールについての内容説明を入力します。

この説明は、複数行に渡って入力できますが、各行に入力できるのは最大で 100 文字までです。

ステップ 8　（任意）デフォルトでは、ロギングがイネーブルになっています。ロギングをディセーブルにするには、チェックボックスをオフにします。また、ドロップダウン リストからロギング レベルを変更することもできます。デフォルトのロギング レベルは [Informational] です。

ステップ 9　（任意）トラフィックをどのような場合に許可しどのような場合に拒否するかを指定するアクセス ルールに、送信元サービス（TCP、UDP、および TCP-UDP に限る）および時間範囲を追加する場合は、[More Options] をクリックしてリストを展開します。この管理アクセス ルールをオフにする場合は、[Enable Rule] をオフにします。

- [Source Service] フィールドに送信元サービスを入力するか、省略符号（[...]）ボタンをクリックしてサービスを参照します。

  宛先サービスと送信元サービスは同じである必要があります。[Destination Service] フィールドをコピーし、[Source Service] フィールドに貼り付けます。

- ロギング間隔を設定する場合（ただし、ロギングをイネーブルにし、デフォルト以外の設定を選択した場合）は、[Logging Interval] フィールドに値を入力します。
- 追加するルールに対して事前定義済みの時間範囲を選択する場合は、[Time Range] ドロップダウン リストから時間範囲を選択するか、省略符号（[...]）ボタンをクリックして時間範囲を参照します。曜日を指定したり、時間範囲が繰り返してアクティブになる間隔を週単位で指定したりなど、追加の時間範囲の制限を指定することもできます。

ステップ 10　[OK] をクリックします。ダイアログボックスが閉じ、管理アクセス ルールが追加されます。

ステップ 11　[Apply] をクリックします。ルールが実行コンフィギュレーションに保存されます。

高度なアクセス ルール設定

[Advanced Access Rule Configuration] ダイアログボックスでは、グローバル アクセス ルールのロギング オプションを設定できます。

ロギングがイネーブルで、パケットがアクセス ルールに合致した場合、ASA では、フロー エントリが作成され、指定された時間内に受信したパケット数の追跡が行われます。ASA は、最初のヒットがあったとき、および各間隔の終わりにシステム ログ メッセージを生成して、その間隔におけるヒットの合計数を示し、最後のヒットの時間を報告します。

（注）　[ASA] ペインの [last rule hit] 行にヒット数の情報が表示されます。ルールのヒット数とタイムスタンプを表示するには、[Configuration] > [Firewall] > [Advanced] > [ACL Manager] の順に選択し、マウスのポインタを [ACL Manager] テーブルのセルに重ねます。

各間隔の終わりに、ASA はヒット数を 0 にリセットします。追跡期間中、アクセス ルールに合致するパケットがなかった場合は、ASA によりそのフロー エントリは削除されます。

どの時点でも大量のフローが同時に存在する可能性があります。メモリおよび CPU のリソースが無制限に消費されないようにするため、ASA では同時拒否フロー数に制限が設定されます。この制限は、拒否フローに対してだけ設定されます（許可フローには設定されません）。これは、拒否フローが攻撃を示している可能性があるためです。制限に達した場合、ASA では既存の拒否フローが期限切れになるまで新しい拒否フローは作成されません。DoS 攻撃（サービス拒絶攻撃）が開始された場合、ASA ではごく短時間のうちに大量の拒否フローが作成される可能性があります。拒否フロー数を制限することで、メモリおよび CPU のリソースが無制限に消費されるのを防ぐことができます。

前提条件

これらの設定は、アクセス ルールの新しいロギング メカニズムをイネーブルにしている場合にのみ適用されます。

フィールド

- [Maximum Deny-flows]：ASA によりロギングが停止される前に許可される拒否フローの最大数を、1 からとデフォルト値までの間で指定します。デフォルトは 4096 です。
- [Alert Interval]：拒否フローが最大数に達したことを示すシステム ログ メッセージ（番号 106101）が生成される時間間隔（1 ～ 3600 秒）を指定します。デフォルトは 300 秒です。
- [Per User Override table]：ユーザごとの上書き機能の状態を指定します。インバウンド アクセス ルールに対してユーザごとの上書き機能をイネーブルになると、RADIUS サーバによって提供されるアクセス ルールは、そのインターフェイス上で設定されたアクセス ルールに置き換えられます。ユーザごとの上書き機能がディセーブルになると、RADIUS サーバによって提供されるアクセス ルールは、そのインターフェイス上で設定されたアクセス ルールと結合されます。インターフェイスにインバウンド アクセス ルールが設定されていない場合、ユーザごとの上書きは設定できません。

  VPN リモート アクセス トラフィックの場合、グループ ポリシーで適用される VPN フィルタがあるかどうか（[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] > [Add/Edit] > [General] > [More Options] > [Filter] フィールドを参照）、および [Per User Override] オプションを設定しているどうかによって動作が異なります。

  - [Per User Override] なし、VPN フィルタなし：トラフィックは、インターフェイス ACL と照合されます（[Configurartion] > [Remote Access VPN] > [Network (Client) Access] > [AnyConnect Connection Profiles] ペインで、デフォルトの [Enable inbound VPN sessions to bypass interface access lists] を設定（ディスエーブル）することによる）。
  - [Per User Override] なし、VPN フィルタ：トラフィックはまずインターフェイス ACL と照合され、次に VPN フィルタと照合されます。
  - [Per User Override]、VPN フィルタ：トラフィックは VPN フィルタのみと照合されます。
- [Object Group Search Setting]：サービス ルールの保存に使用されるメモリの量が削減されますが、一致するアクセス ルールの検索にかかる時間が増大します。

アクセス ルールの拡張機能

セキュリティ アプライアンスを使用すると、特定のオブジェクト グループを含むアクセス ルールの拡張機能をオフにできます。拡張機能がオフになっている場合、検索にはオブジェクト グループ検索が使用されます。これにより、拡張されたルールの保存に必要なメモリ量は削減されますが、検索のパフォーマンスが低下します。メモリ使用率に対するパフォーマンスのトレードオフによって、検索をオンおよびオフにできます。

特定のオブジェクト グループを含むアクセス ルールの拡張機能をオフにするオプションを設定するには、次の手順を実行します。

ステップ 1　[Configuration] > [Firewall] > [Access Rules] の順に選択します。

ステップ 2　[Advanced] ボタンをクリックします。

ステップ 3　[Enable Object Group Search Algorithm] チェックボックスをオンにします。

HTTP Redirect の設定

HTTP Redirect テーブルには、ASA の各インターフェイス、そのインターフェイスが HTTP 接続を HTTPS にリダイレクトするように設定されているかどうか、および接続のリダイレクトに使用するポート番号が表示されます。

（注）　HTTP をリダイレクトするには、インターフェイスに HTTP を許可する ACL が必要です。アクセス リストがないと、インターフェイスは HTTP ポートをリッスンできません。

[Configuration] > [Device Management] > [Advanced] > [HTTP Redirect] > [Edit] ペインを使用して、インターフェイスの HTTP リダイレクト設定または HTTP 接続のリダイレクト元のポートを変更できます。テーブルでインターフェイスを選択し、[Edit] をクリックします。インターフェイスをダブルクリックすることもできます。[Edit HTTP/HTTPS Settings] ダイアログボックスが表示されます。

Edit HTTP/HTTPS Settings

[Edit HTTP/HTTPS Settings] ダイアログボックスでは、インターフェイスの HTTP リダイレクト設定またはポート番号を変更できます。

フィールド

[Edit HTTP/HTTPS Settings] ダイアログボックスには次のフィールドがあります。

- [Interface] : ASA が HTTP 要求を HTTPS にリダイレクトする（またはしない）インターフェイスを示します。
- [Redirect HTTP to HTTPS] : HTTP 要求を HTTPS にリダイレクトするにはオンにし、リダイレクトしない場合はオフにします。
- [HTTP Port] : インターフェイスが HTTP 接続のリダイレクトに使用するポートを指定します。デフォルトでは、インターフェイスはポート 80 をリッスンします。

アクセス ルールの詳細については、「アクセス ルールに関する情報」（P.6-1）を参照してください。

アクセス ルールの機能履歴

表 6-2 に、各機能変更と、それが実装されたプラットフォーム リリースを示します。ASDM は、複数のプラットフォーム リリースとの下位互換性があるため、サポートが追加された特定の ASDM リリースは一覧には含まれていません。

表 6-2　アクセス ルールの機能履歴

機能名	プラットフォーム リリース	機能情報
インターフェイス アクセス ルール	7.0(1)	ACL を使用した、ASA 経由のネットワーク アクセスの制御。 次の画面が導入されました。[Configuration] > [Firewall] > [Access Rules]。
グローバル アクセス ルール	8.3(1)	グローバル アクセス ルールが導入されました。 次の画面が変更されました。[Configuration] > [Firewall] > [Access Rules]。

表 6-2　アクセス ルールの機能履歴 （続き）

機能名	プラットフォーム リリース	機能情報
アイデンティティ ファイアウォールのサポート	8.4(2)	アイデンティティ ファイアウォールのユーザおよびグループを発信元と宛先に使用できるようになりました。アイデンティティ ファイアウォール ACL はアクセス ルールや AAA ルールとともに、および VPN 認証に使用できます。
EtherType ACL が S-IS トラフィックをサポート	8.4(5)、9.1(2)	トランスペアレント ファイアウォール モードでは、ASA は、EtherType ACL を使用して、IS-IS トラフィックを渡すことができるようになりました。 次の画面が変更されました。[Configuration] > [Device Management] > [Management Access] > [EtherType Rules]。
TrustSec のサポート	9.0(1)	TrustSec セキュリティ グループを送信元と宛先に使用できるようになりました。アイデンティティ ファイアウォール ACL をアクセス ルールとともに使用できます。
IPv4 および IPv6 の統合 ACL	9.0(1)	ACL で IPv4 および IPv6 アドレスがサポートされるようになりました。送信元および宛先に対して IPv4 および IPv6 アドレスの組み合わせも指定できます。**any** キーワードは、IPv4 および IPv6 トラフィックを表すように変更されました。IPv4 のみのトラフィックを表す **any4** キーワードと、IPv6 のみのトラフィックを表す **any6** キーワードが追加されました。IPv6 固有の ACL は非推奨です。既存の IPv6 ACL は拡張 ACL に移行されます。移行の詳細については、リリース ノートを参照してください。 次の画面が変更されました。 [Configuration] > [Firewall] > [Access Rules] [Configuration] >[Remote Access VPN] > [Network（Client） Access] > [Group Policies] > [General] > [More Options]
ICMP コードによって ICMP トラフィックをフィルタリングするための拡張 ACL とオブジェクト機能拡張	9.0(1)	ICMP コードに基づいて ICMP トラフィックの許可または拒否ができるようになりました。 次の画面が導入または変更されました。 [Configuration] > [Firewall] > [Objects] > [Service Objects/Groups] [Configuration] > [Firewall] > [Access Rule]