

アクセス ルール

この章では、アクセスルールを使用して ASA へのネットワーク アクセスや ASA を通過する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。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。



(注)

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。必要なのは、一般的な操作の設定ガイドに従って管理 アクセスを設定することだけです。

- ネットワーク アクセスの制御 (1ページ)
- アクセス制御に関するガイドライン (7ページ)
- アクセス制御の設定 (9ページ)
- アクセス ルールのモニタリング (18 ページ)
- アクセス ルールの履歴 (19ページ)

ネットワーク アクセスの制御

アクセス ルールは、ASA の通過を許可するトラフィックを定義したものです。複数の異なる レイヤのルールを組み合わせてアクセス コントロール ポリシーを実装できます。

- インターフェイスに割り当てられる拡張アクセスルール (レイヤ3以上のトラフィック): 着信方向と発信方向のそれぞれで異なるルールセット (ACL) を適用できます。拡張アクセスルールでは、送信元と宛先のトラフィックの基準に基づいてトラフィックが許可または拒否されます。
- グローバルに割り当てられる拡張アクセス ルール: デフォルトのアクセス コントロール として使用する単一のグローバル ルール セットを作成できます。グローバル ルールはインターフェイス ルールの後に適用されます。

- 管理アクセスルール(レイヤ3以上のトラフィック): インターフェイスに対するトラフィック(通常は管理トラフィック)を制御する単一のルールセットを適用できます。これらのルールは、CLIの「コントロールプレーン」アクセスグループに相当します。デバイスに対するICMPトラフィックについては、代わりにICMPルールを設定できます。
- インターフェイスに割り当てられる EtherTypeルール(レイヤ2のトラフィック)(ブリッジ グループ メンバーのインターフェイスのみ):着信方向と発信方向のそれぞれで異なるルール セットを適用できます。EtherType ルールは、IP 以外のトラフィックのネットワーク アクセスを制御するルールです。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。また、ブリッジ グループ メンバーのインターフェイスに拡張アクセス ルールを適用して、レイヤ3以上のトラフィックを制御できます。

ルールに関する一般情報

次のトピックでは、アクセスルールおよび EtherType ルールに関する一般的な情報を提供します。

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

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、特定の着信インターフェイス アクセス ルールが常に汎用のグローバル アクセス ルールよりも先に処理されます。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。

インバウンド ルールとアウトバウンド ルール

トラフィックの方向に基づいてアクセスルールを設定できます。

- インバウンド:インバウンドアクセスルールは、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および管理アクセスルールは常にインバウンドルールになります。
- アウトバウンド:アウトバウンドルールは、インターフェイスから送信されるトラフィックに適用されます。

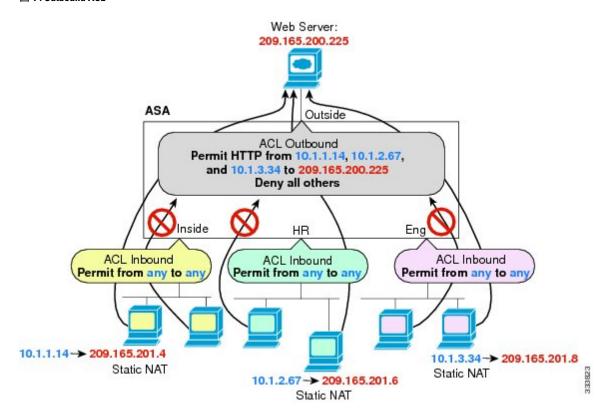


(注)

「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(次の図を参照してくだ さい)。他のすべてのホストは、アウトバウンド ACL により外部ネットワークから遮断されます。

図 1: Outbound ACL



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、適用されるACLにおける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。

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 および IPv6 のユニキャストトラフィック。

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 および IPv6 のユニキャスト トラフィック。
- 双方向の ARP。ARP トラフィックの制御には ARP インスペクションを使用します。アクセス ルールでは制御できません。
- 双方向の BPDU。

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

暗黙的な拒否

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。

管理(コントロール プレーン)の ACL は to-the-box トラフィックを管理していますが、インターフェイスの一連の管理ルールの末尾には暗黙の deny がありません。その代わりに、管理アクセスルールに一致しない接続は通常のアクセス制御ルールで評価されます。

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ルールですべてのトラフィックを明示的に拒否した場合は、IPと ARPのトラフィックが拒否され、物理的なプロトコルのトラフィック(自動ネゴシエーションなど)だけが許可されます。

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。

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。

拡張アクセス ルール

この項では、拡張アクセスルールについて説明します。

リターン トラフィックに対する拡張アクセス 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。たとえば、ping を制御するには、echo-reply($\mathbf{0}$)(ASA からホストへ)または echo($\mathbf{8}$)(ホストから ASA へ)を指定します。

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が含まれます。ダイナミックルーティングプロトコルまたはDHCPリレーを、このトラフィックを許可するように設定する必要があります。

トランスペアレント ファイアウォール モードで同じブリッジ グループのメンバーであるイン ターフェイスでは、アクセス ルールを使用して IP トラフィックを許可することができます。



(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、アクセスルールを着信および発信の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。

次の表に、同じブリッジ グループのメンバーであるインターフェイス間のアクセス ルールを 使用して、ユーザが許可できる一般的なトラフィック タイプを示します。

表 1:同じブリッジ グループのメンバー間のアクセス ルールの特別なトラフィック

トラフィック タ イプ	プロトコルまたはポート	注
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	_

トラフィック タ イプ	プロトコルまたはポート	注
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(インターフェイスへの HTTP、Telnet、SSH などによる接続)に対するアクセス制御ルールは、される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。

通常のアクセスルールとは異なり、インターフェイスの一連の管理ルールの末尾には暗黙のdenyがありません。その代わりに、管理アクセスルールに一致しない接続は通常のアクセス制御ルールで評価されます。

また、デバイスへの ICMP トラフィックは、ICMP ルールを使用して制御できます。デバイス を通過する ICMP トラフィックの制御には、通常の拡張アクセス ルールを使用します。

EtherType ルール

この項では、EtherType ルールについて説明します。

サポートされている EtherType およびその他のトラフィック

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 含まれるため、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。
- Intermediate System to Intermediate System (IS-IS) 。
- IEEE 802.2 論理リンク制御パケット。宛先サービス アクセス ポイントのアドレスに基づいてアクセスを制御できます。

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 EtherType 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、Label Distribution Protocol および Tag Distribution Protocol 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。

mpls ldp router-id interface force

または

tag-switching tdp router-id interface force

アクセス制御に関するガイドライン

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。

Per-User ACL の注意事項

- ユーザごとの ACL では、timeout uauth コマンドの値が使用されますが、この値は AAA のユーザごとのセッション タイムアウト値でオーバーライドできます。
- ユーザごとの ACL のためにトラフィックが拒否された場合、syslog メッセージ 109025 が ログに記録されます。トラフィックが許可された場合、syslog メッセージは生成されません。ユーザごとの ACL の \log オプションの効果はありません。

その他のガイドラインと制限事項

• オブジェクトグループ検索をイネーブルにすると、ルックアップのパフォーマンスは低下し、CPU 使用率は増加しますが、アクセス ルールの検索に必要なメモリを抑えることができます。オブジェクト グループ検索を有効にした場合、ネットワーク オブジェクトまたはサービスオブジェクトは拡張されませんが、それらのグループの定義に基づいて一致するアクセス ルールが検索されます。このオプションを設定するには、アクセス ルールテーブルの下ある [Advanced] ボタンをクリックします。

接続ごとに、送信元と宛先の両方の IP アドレスがネットワーク オブジェクトと照合されます。発信元アドレスに一致するオブジェクトの数が、宛先アドレスと一致する数の1万倍を超えると接続が切断されます。このチェックは、パフォーマンスの低下を防止します。一致件数が膨大になることを防ぐためにルールを設定します。



(注)

オブジェクトグループの検索は、ネットワークオブジェクトとサービスオブジェクトのみで動作します。セキュリティグループまたはユーザオブジェクトでは動作しません。ACL にセキュリティグループが含まれている場合は、この機能を有効にしないでください。ACLが非アクティブになったり、その他の予期しない動作となる可能性があります。

- アクセス グループにトランザクション コミット モデルを使用することで、システムのパフォーマンスと信頼性を高めることができます。詳細については、一般的な操作設定ガイドの基本設定の章を参照してください。このオプションは、[Configurations] > [Device Management] > [Advanced] > [Rule Engine] の下にあります。
- ASDM では、ACL のルールの前にあるアクセス リストのコメントに基づいてルールの説明が設定されます。ASDMで新しいルールを作成した場合も、関連するルールの前にあるコメントが説明として設定されます。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。
- 送信元または宛先アドレス、あるいは送信元または宛先サービスに複数の項目を入力する と、ASDM でそれらの項目に対してプレフィックス DM_INLINE のオブジェクト グルー プが自動的に作成されます。これらのオブジェクトは、ルール テーブル ビューのそれら のコンポーネントパートに自動的に拡張されますが、[Tools] > [Preferences] で [Auto-expand network and service objects with specified prefix] ルール テーブル設定を選択解除すると、オブジェクト名を表示できます。
- 通常、ACL またはオブジェクト グループに存在しないオブジェクトを参照したり、現在 参照しているオブジェクトを削除したりすることはできません。また、access-group コマンドで指定していない ACL を参照(アクセスルールを適用)することもできません。ただし、このデフォルトの動作を変更し、オブジェクトまたは ACL を作成する前にそれらを「前方参照」できるようにすることができます。オブジェクトまたは ACL を作成するまでは、それらを参照するルールやアクセスグループは無視されます。前方参照をイネーブルにするには、[Configuration] > [Access Rules] を選択し、[Advanced] ボタンをクリックして、アクセスルールの詳細設定のオプションを選択します。

アクセス制御の設定

ここでは、アクセスコントロールを設定する方法について説明します。

アクセス ルールの設定

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

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

ルールはインターフェイスおよび方向別に構成され、グローバル ルールはそれらとは別のグループにまとめられています。管理アクセスルールを設定する場合は、このページで繰り返されます。これらのグループが、作成されてアクセスグループとしてインターフェイスまたはグローバルに割り当てられた拡張 ACL に相当します。それらの ACL も [ACL Manager] ページに表示されます。

ステップ2次のいずれかを実行します。

- 新しいルールを追加するには、[Add] > [Add Access Rule] の順に選択します。
- コンテナ内の特定の場所にルールを挿入するには、追加する場所の下にある既存のルール を選択して [Add] > [Insert] の順に選択するか、[Add] > [Insert After] の順に選択します。
- ルールを編集するには、ルールを選択し、[Edit] をクリックします。

ステップ3 ルールのプロパティを入力します。選択する主なオプションを次に示します。

- [Interface]:ルールを適用するインターフェイスを指定します。 グローバル ルールを作成 する場合は [Any] を選択します。
- [Action]: [Permit] または [Deny]: 対象のトラフィックを許可するか拒否(破棄) するかを 指定します。
- [Source/Destination criteria]: 送信元(発信アドレス)と宛先(トラフィックフローのターゲットアドレス)を定義します。通常は、ホストまたはサブネットの IPv4 アドレスまたは IPv6 アドレスを設定します。これはネットワークまたはネットワーク オブジェクト グループで表すことができます。送信元のユーザ名またはユーザ グループ名も指定できます。また、[Service] フィールドでトラフィックの種類を指定すると、すべての IP トラフィックではなく、特定のトラフィックを対象とするルールを作成できます。 Trustsec を実装している場合は、セキュリティ グループを使用して送信元と宛先を定義できます。

使用可能なすべてのオプションの詳細については、アクセス ルールのプロパティ (10 ページ) を参照してください。

ルールの定義が完了したら、[OK] をクリックしてルール テーブルに追加します。

ステップ4 [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 ルールのプロパティ

アクセス ルールを追加または編集するときに設定できるプロパティを次に示します。多くのフィールドでは、編集ボックスの右にある[...]ボタンをクリックして、そのフィールドに対応するオブジェクトを選択、作成、編集できます。

Interface

ルールが適用されるインターフェイス。グローバルルールを作成する場合は[Any]を選択します。

[Action] : [Permit]/[Deny]

対象のトラフィックを許可するか拒否(破棄)するかを指定します。

[Source Criteria]

照合しようとしているトラフィックの発信者の特性。[Source] は設定する必要がありますが、その他のプロパティはオプションです。

[Source]

送信元の IPv4 または IPv6 アドレス。デフォルト値は **any** です。これはすべての IPv4 または IPv6 アドレスに一致します。IPv4 のみをターゲットにする場合は **any4** を、IPv6 のみをターゲットにする場合は **any6** をそれぞれ使用できます。単一のホストアドレス(10.100.10.5 または 2001:DB8::0DB8:800:200C:417A など)、サブネット(10.100.10.0/24 または 10.100.10.0/255.255.255.0 形式、または IPv6 の場合は2001:DB8:0:CD30::/60)、ネットワーク オブジェクトまたはネットワーク オブジェクト グループの名前、またはインターフェイスの名前を指定できます。

User

アイデンティティファイアウォールを有効にしている場合は、ユーザまたはユーザグループをトラフィックの送信元として指定できます。ユーザが現在使用しているIPアドレスはルールに一致します。ユーザ名(DOMAIN\user)、ユーザグループ(DOMAIN\group(2つの\はグループ名を示します))、またはユーザオブジェクトグループを指定できます。このフィールドでは、[...]をクリックして AAA サーバグループから名前を選択するほうが名前を入力するよりもはるかに簡単です。

Security Group

Cisco Trustsec を有効にしている場合は、セキュリティグループの名前やタグ($1 \sim 65533$)、またはセキュリティグループオブジェクトを指定できます。

[More Options] > [Source Service]

TCP またはUDP を宛先サービスとして指定した場合は、TCP、UDP、またはTCP-UDP を表す定義済みのサービスオブジェクトか、独自のオブジェクトをオプションで指定できます。通常は、宛先サービスのみを定義し、送信元サービスは定義しません。送信元サービスを定義する場合、宛先サービスのプロトコルは送信元サービスに一致する必要があります(たとえば、両方ともポート定義のある/ないTCP など)。

[Destination Criteria]

照合しようとしているトラフィックのターゲットの特性。[Destination] は設定する必要がありますが、その他のプロパティはオプションです。

Destination

宛先の IPv4 または IPv6 アドレス。デフォルト値は any です。これはすべての IPv4 または IPv6 アドレスに一致します。IPv4 のみをターゲットにする場合は any4 を、IPv6 のみをターゲットにする場合は any6 をそれぞれ使用できます。単一のホストアドレス(10.100.10.5 または 2001:DB8::0DB8:800:200C:417A など)、サブネット(10.100.10.0/24 または 10.100.10.0/255.255.255.0 形式、または IPv6 の場合は 2001:DB8:0:CD30::/60)、ネットワーク オブジェクトまたはネットワーク オブジェクト グループの名前、またはインターフェイスの名前を指定できます。

Security Group

Cisco Trustsec を有効にしている場合は、セキュリティグループの名前やタグ $(1 \sim 65533)$ 、またはセキュリティグループオブジェクトを指定できます。

Service

IP、TCP、UDP などのトラフィックのプロトコル。オプションで TCP および UDP のポートを指定できます。デフォルトは IP ですが、より具体的なプロトコルを指定して、ターゲットにするトラフィックをより細かく設定することができます。通常は、何らかのタイプのサービス オブジェクトを選択します。TCP および UDP の場合は、tcp/80、tcp/http、tcp/10-20(ポート範囲)、tcp-udp/80(ポート 80 の任意の TCP または UDP トラフィックに一致)のようにポートを指定できます。

Description

ルールの目的の説明を入力します。1行の最大文字数は100文字までです。複数行を入力できます。CLIでは、各行がコメントとして追加され、ルールの前に配置されます。



(注)

1つのプラットフォーム(Windows など)上で英語以外の文字でコメントを追加し、それらの文字を別のプラットフォーム(Linux など)から削除しようとした場合、元の文字が正しく認識されないため編集や削除を実行できない可能性があります。この制限は、各種言語の文字をさまざまな方法でエンコードするプラットフォームの依存性によるものです。

[Enable Logging] : [Logging Level] : [More Options] > [Logging Interval]

ロギング オプションでは、ルールについて syslog メッセージをどのように生成するかを 定義します。次のロギング オプションを実装できます。

[Deselect Enable Logging]

ルールのロギングが無効になります。このルールに一致する接続については、どのタイプの syslog メッセージも発行されません。

[Select Enable Logging with Logging Level = Default]

ルールにデフォルトのロギングが提供されます。拒否された接続ごとに syslog メッセージ 106023 が発行されます。アプライアンスが攻撃を受けている場合、このメッセージの発行頻度はサービスに影響を及ぼす可能性があります。

[Select Enable Logging with Non-Default Logging Level]

106023 の代わりに、集約された syslog メッセージ 106100 が提供されます。メッセージ 106100 は、まず最初にヒットしたときに発行されます。その後、[More Options] > [Logging Interval] で設定した間隔ごとに再発行され、その間隔内のヒット数を示します。推奨されるロギング レベルは [Informational] です。

拒否メッセージを集約すると、攻撃の影響を軽減できるとともに、場合によってはメッセージの分析が容易になります。DoS攻撃を受けている場合、メッセージ106101が表示されることがあります。これは、メッセージ106100のヒットカウントの生成に使用されるキャッシュされた拒否フローの数が、1つの間隔における最大数を超えたことを示します。この時点で、アプライアンスは攻撃を軽減するために、次の間隔まで統計情報の収集を停止します。

[More Options] > [Traffic Direction]

ルールの方向([In] または [Out]) を指定します。デフォルトは [In] で、グローバル アクセス ルールと管理アクセス ルールではこのオプションしか選択できません。

[More Options] > [Enable Rule]

ルールがデバイスでアクティブになっているかどうか。無効になっているルールは、ルールテーブルに取り消し線付きのテキストで表示されます。ルールを無効にすると、ルールを削除することなく、ルールのトラフィックへの適用を停止できます。このため、そのルールが必要だと判断した場合は、後で再度有効にすることができます。

[More Options] > [Time Range]

ルールがアクティブになっている必要がある時間帯と曜日を定義する時間範囲オブジェクトの名前。時間範囲を指定しない場合、ルールは常にアクティブです。

アクセス ルールの詳細オプションの設定

アクセスルールの詳細オプションを使用して、ルールの動作の一部をカスタマイズすることができます。ただし、これらのオプションは、ほとんどの場合に適切に動作するようにデフォルトで設定されています。

手順

- ステップ**1** [設定(Configuration)]>[ファイアウォール(Firewall)]>[アクセス ルール(Access Rules)] を選択します。
- ステップ2 ルール テーブルの下にある [Advanced] ボタンをクリックします。
- ステップ3 次のオプションを必要に応じて設定します。

- [Advanced Logging Settings]: デフォルト以外のロギングを設定すると、メッセージ106100 の統計情報を得るために拒否フローがキャッシュされます(アクセスルールの syslog メッセージの評価(18ページ)を参照)。メモリおよび CPU リソースが無制限に消費されないようにするために、ASA は同時拒否フロー数に制限を設定します。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。この制限に達すると、メッセージ 106101 が発行されます。106101 について以下を設定できます。
 - [Maximum Deny-flows]: ASA によりフローのキャッシュが停止される前に許可される 拒否フローの最大数を、 $1 \sim 4096$ の範囲で指定します。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 106101 が発行される時間間隔(1 \sim 3600 秒)を指定します。デフォルトは 300 秒で す。
- [Per User Override] のテーブル: ユーザの認証用に RADIUS サーバからダウンロードした ダイナミック ユーザ ACL をインターフェイスに割り当てられた ACL よりも優先するかど うかを指定します。たとえば、インターフェイス ACLが 10.0.0.0からのトラフィックをすべて拒否し、ダイナミック ACLが 10.0.0.0からのトラフィックをすべて許可する場合、そのユーザに関しては、ダイナミック ACL によってインターフェイス ACL が上書きされます。ユーザの上書きを許可する各インターフェイスについて、[Per User Override] チェック ボックスをオンにします(着信方向のみ)。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。

デフォルトでは、VPN リモートアクセストラフィックはインターフェイス ACL と照合されません。ただし、[Enable inbound VPN sessions to bypass interface access lists] 設定

([Configuration] > [Remote Access VPN] > [Network (Client) Access] > [AnyConnect Connection Profiles] ペイン) の選択を解除した場合は、グループ ポリシーで VPN フィルタが適用されているかどうか ([Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] > [Add/Edit] > [General] > [More Options] > [Filter] フィールド)、および [Per User Override] オプションを設定しているかどうかによって動作が異なります。

- [No Per User Override, no VPN filter]: トラフィックはインターフェイス ACL と照合されます。
- [No Per User Override, VPN filter]: 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 filter]: 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] : [Enable Object Group Search Algorithm] を選択すると、ルックアップのパフォーマンスは低下しますが、オブジェクトグループを使用するアクセスルールの検索に必要なメモリを抑えることができます。オブジェクトグループ検索をイネーブルにした場合、ネットワークオブジェクトは拡張されませんが、それらのグループの定義に基づいて一致するアクセスルールが検索されます。

- (注) オブジェクトグループの検索は、ネットワークオブジェクトとサービスオブジェクトのみで動作します。セキュリティグループオブジェクトでは動作しません。 ACL にセキュリティグループが含まれている場合は、この機能を有効にしないでください。ACLが非アクティブになったり、その他の予期しない動作となる可能性があります。
- [Forward Reference Setting]: 通常、ACL またはオブジェクトグループにないオブジェクトやオブジェクトグループを参照したり、現在参照されているオブジェクトやオブジェクトグループを削除することはできません。また、access-groupコマンドで指定していないACLを参照(アクセスルールを適用)することもできません。ただし、このデフォルトの動作を変更し、オブジェクトまたはACLを作成する前にそれらを「前方参照」できるようにすることができます。オブジェクトまたはACLを作成するまでは、それらを参照するルールやアクセスグループは無視されます。事前参照をイネーブルにするには、[Enable the forward reference of objects and object-groups] を選択します。事前参照をイネーブルにすると、既存のオブジェクトの参照の入力ミスか事前参照かを ASDM で判別できなくなることに注意してください。

ステップ4 [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 ASA への to-the-box 管理トラフィックを制御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

通常のアクセスルールとは異なり、インターフェイスの一連の管理ルールの末尾には暗黙のdenyがありません。その代わりに、管理アクセスルールに一致しない接続は通常のアクセス制御ルールで評価されます。

手順

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

ルールはインターフェイス別に構成されています。各グループが、作成されてコントロールプレーン ACL としてインターフェイスに割り当てられた拡張 ACL に相当します。それらの ACL も [Access Rules] ページおよび [ACL Manager] ページに表示されます。

ステップ2 次のいずれかを実行します。

- 新しいルールを追加するには、[Add] > [Add Management Access Rule] の順に選択します。
- コンテナ内の特定の場所にルールを挿入するには、追加する場所の下にある既存のルール を選択して [Add] > [Insert] の順に選択するか、[Add] > [Insert After] の順に選択します。

•ルールを編集するには、ルールを選択し、[Edit] をクリックします。

ステップ3 ルールのプロパティを入力します。選択する主なオプションを次に示します。

- [Interface]:ルールを適用するインターフェイスを指定します。
- [Action]: [Permit] または [Deny]: 対象のトラフィックを許可するか拒否(破棄) するかを 指定します。
- [Source/Destination criteria]: 送信元(発信アドレス)と宛先(トラフィックフローのターゲットアドレス)を定義します。通常は、ホストまたはサブネットの IPv4 アドレスまたは IPv6 アドレスを設定します。これはネットワークまたはネットワーク オブジェクトグループで表すことができます。送信元のユーザ名またはユーザグループ名も指定できます。また、[Service] フィールドでトラフィックの種類を指定すると、すべての IPトラフィックではなく、特定のトラフィックを対象とするルールを作成できます。 Trustsec を実装している場合は、セキュリティグループを使用して送信元と宛先を定義できます。

使用可能なすべてのオプションの詳細については、アクセスルールのプロパティ (10ページ)を参照してください。

ルールの定義が完了したら、[OK] をクリックしてルール テーブルに追加します。

ステップ4 [Apply] をクリックし、ルールを設定に保存します。

EtherType ルールの設定

EtherType ルールはブリッジグループメンバーのインターフェイス(トランスペアレントファイアウォールモード)の非 IP レイヤ 2 トラフィックに適用されます。これらのルールを使用して、レイヤ2パケット内の EtherType 値に基づいてトラフィックを許可または破棄できます。 EtherType ルールでは、ASA を経由する非 IP トラフィックのフローを制御できます。

ブリッジ グループ メンバーのインターフェイスに拡張および EtherType アクセス ルールの両 方を適用できます。EtherType ルールは、拡張アクセス ルールに優先されます。

手順

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

ルールはインターフェイスおよび方向別に構成されています。各グループが、作成されてインターフェイスに割り当てられた EtherType ACL に相当します。

ステップ2次のいずれかを実行します。

• 新しいルールを追加するには、**[追加(Add)]**>**[EtherTypeの追加(Add EtherType Rule)]** を選択します。

- コンテナ内の特定の場所にルールを挿入するには、追加する場所の下にある既存のルールを選択して[追加(Add)]>[挿入(Insert)]を選択するか、[追加(Add)]>[後に追加(Insert After)]を選択します。
- •ルールを編集するには、ルールを選択し、[Edit] をクリックします。

ステップ3 ルールのプロパティを入力します。選択する主なオプションを次に示します。

- [Interface]:ルールを適用するインターフェイスを指定します。
- [Action]: [Permit] または [Deny]: 対象のトラフィックを許可するか拒否(破棄) するかを 指定します。
- [EtherType]: 次のオプションを使用してトラフィックを照合できます。
 - any: すべてのトラフィック。
 - bpdu: デフォルトで許可されるブリッジ プロトコル データ ユニット。
 - dsap: IEEE 802.2 論理リンク制御パケットの宛先サービス アクセス ポイントのアドレス。 さらに、[DSAP Value] に $0x01 \sim 0xff$ の範囲の 16 進数で許可または拒否するアドレスを含める必要があります。次に、一部の共通アドレスの値を示します。
 - 0x42: ブリッジプロトコルデータ ユニット (BPDU)。
 - 0xe0 : Internet Packet Exchange (IPX) 802.2 LLC_o
 - **0xfe**: Intermediate System to Intermediate System (IS-IS) _o
 - **0xff**: Raw IPX 802.3 形式。
 - ipx : Internetwork Packet Exchange (IPX) 。
 - isis: Intermediate System to Intermediate System (IS-IS) 。
 - mpls-multicast: MPLS マルチキャスト。
 - mpls-unicast: MPLS ユニキャスト。
 - [hex_number]: 16 ビットの 16 進数 0x600 ~ 0xffff で指定できる任意の EtherType。 EtherType のリストについては、http://www.ietf.org/rfc/rfc1700.txt にアクセスして、RFC 1700「Assigned Numbers」を参照してください。
- [Description]:ルールの目的の説明を入力します。1行の最大文字数は100文字までで、複数行を入力できます。CLIでは、各行がコメントとして追加され、ルールの前に配置されます。
- [その他のオプション(More Options)] > [方向(Direction)]: ルールの方向が[イン(In)] か [アウト(Out)] かを指定します。デフォルトは [In] です。

ルールの定義が完了したら、[OK]をクリックしてルールテーブルに追加します。

ステップ4 [Apply] をクリックし、ルールを設定に保存します。

ICMP アクセス ルールの設定

デフォルトでは、IPv4 または IPv6 を使用して任意のインターフェイスに ICMP パケットを送信できます。ただし、次の例外があります。

- ASA は、ブロードキャストアドレス宛ての ICMP エコー要求に応答しません。
- ASAは、トラフィックが着信するインターフェイス宛ての ICMP トラフィックにのみ応答します。ICMP トラフィックは、インターフェイス経由で離れたインターフェイスに送信できません。

デバイスを攻撃から保護するために、ICMP ルールを使用して、インターフェイスへの ICMP アクセスを特定のホスト、ネットワーク、または ICMP タイプに限定できます。ICMP ルール にはアクセスルールと同様に順序があり、パケットに最初に一致したルールのアクションが適用されます。

インターフェイスに対して any ICMP ルールを設定すると、ICMP ルールのリストの最後に暗黙の deny ICMP ルールが追加され、デフォルトの動作が変更されます。そのため、一部のメッセージ タイプだけを拒否する場合は、残りのメッセージ タイプを許可するように ICMP ルールのリストの最後に permit any ルールを含める必要があります。

ICMP到達不能メッセージタイプ(タイプ3)の権限を常に付与することを推奨します。ICMP到達不能メッセージを拒否すると、ICMPパスMTUディスカバリがディセーブルになり、IPsecおよびPPTPトラフィックが停止することがあります。また、IPv6のICMPパケットは、IPv6のネイバー探索プロセスに使用されます。

手順

ステップ1 [Configuration] > [Device Management] > [Management Access] > [ICMP] の順に選択します。 ステップ2 ICMP ルールを設定します。

- a) ルールを追加する([Add] > [Rule]、[Add] > [IPv6 Rule]、または [Add] > [Insert])か、ルールを選択して編集します。
- b) 制御するICMPタイプを選択します。すべてのタイプに適用する場合はanyを選択します。
- c) ルールを適用するインターフェイスを選択します。各インターフェイスに対して個別に ルールを作成する必要があります。
- d) 一致したトラフィックに対してアクセスを許可するか拒否するかを選択します。
- e) すべてのトラフィックにルールを適用する場合は、[Any Address]を選択します。特定のホストまたはネットワークを制御する場合は、アドレスとマスク (IPv4の場合) またはアドレスとプレフィックス長 (IPv6 の場合) を入力します。
- f) [OK] をクリックします。

- ステップ3 (オプション) ICMP の到達不能メッセージに対する制限は、次の各オプションを使用して設定します。ASA をホップの1つとして表示するトレースルートに対して ASA の通過を許可するためには、サービスポリシーで [Decrement time to live for a connection] オプション ([Configuration] > [Firewall] > [Service Policy Rules] > [Rule Actions] > [Connection Settings] ダイアログボックス) をイネーブルにするほか、レート制限を大きくする必要があります。
 - Rate Limit: 到達不能メッセージのレート制限を、1 秒あたり $1 \sim 100$ の範囲で設定します。デフォルトは、1 秒あたり 1 メッセージです。
 - Burst Size: バースト レートを $1 \sim 10$ の範囲で設定します。現在、この値はシステムによって使用されていません。

ステップ4 Apply をクリックします。

アクセス ルールのモニタリング

[Access Rules] ページに各ルールのヒット数が表示されます。ヒット数にカーソルを合わせると、その更新時間と間隔が表示されます。ヒット数をリセットするには、ルールを右クリックして [Clear Hit Count] を選択します。これを実行すると、同じ方向の同じインターフェイスに適用されているすべてのルールのヒット数が消去されることに注意してください。

アクセス ルールの syslog メッセージの評価

アクセスルールに関するメッセージは、syslogイベントのビューア (ASDMのビューアなど) を使用して確認できます。

デフォルトのロギングを使用している場合、明示的に拒否されたフローに対する syslog メッセージ 106023 だけが表示されます。ルールのリストの最後にある「暗黙の deny」に一致するトラフィックは記録されません。

ASA が攻撃を受けた場合、拒否されたパケットを示す syslog メッセージの数が非常に大きくなることがあります。代わりに、syslog メッセージ 106100 を使用するロギングをイネーブルにすることをお勧めします。このメッセージは各ルール(許可ルールも含む)の統計情報を示すもので、これを使用することにより、生成される syslog メッセージの数を制限できます。また、特定のルールについて、すべてのロギングをディセーブルにする方法もあります。

メッセージ 106100 のロギングがイネーブルで、パケットが ACE と一致した場合、ASA はフローエントリを作成して、指定された間隔内で受信したパケットの数を追跡します。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 syslog メッセージを生成し、その間隔におけるヒットの合計数と最後のヒットのタイムスタンプを示します。各間隔の終わりに、ASA はヒット数を 0 にリセットします。1 つの間隔内で ACE と一致するパケットがなかった場合、ASA はそのフローエントリを削除します。ルールのロギングの設定では、それぞれのルールについて、ログ メッセージの間隔のほか、重大度も制御することができます。

フローは、送信元 IP アドレス、宛先 IP アドレス、プロトコル、およびポートで定義されます。同じ2つのホスト間の新しい接続では、送信元ポートが異なる場合があるため、接続のための新しいフローが作成されると、同じフローの増加は示されない場合があります。

確立された接続に属する、許可されたパケットを ACL でチェックする必要はありません。最初のパケットだけがロギングされ、ヒット数に含められます。ICMP などのコネクションレス型プロトコルの場合は、許可されているパケットもすべてロギングされ、拒否されたパケットはすべてロギングされます。

これらのメッセージの詳細については、syslog メッセージガイドを参照してください。



ヒント

メッセージ 106100 のロギングがイネーブルで、パケットが ACE と一致した場合、ASA はフローエントリを作成して、指定された間隔内で受信したパケットの数を追跡します。ASA では、ACE 用のロギングフローを最大 32 K 保持できます。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 リソースが無制限に消費されないようにするために、ASA は同時拒否フロー数に制限を設定します。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、拒否フローは攻撃を示している可能性があるためです。制限に達すると、ASA は既存の拒否フローが期限切れになるまでロギング用の新しい拒否フローを作成せず、メッセージ 106101 を発行します。このメッセージの頻度、および拒否フローのキャッシュの最大数は、詳細設定で制御できます。アクセスルールの詳細オプションの設定(12 ページ)を参照してください。

アクセス ルールの履歴

	プラットフォー	
機能名	ムリリース	説明
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]。
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。

機能名	プラットフォー ム リリース	説明
EtherType ACL が IS-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 が 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IPv6ACL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]、
アクセス グループ ルール エンジン のトランザクション コミット モデ	9.1(5)	[Configuration] > [Firewall] > [Access Rule] イネーブルの場合、ルールの編集の完了後、ルールの更新が適用されます。ルールの照合パフォーマンスへの影響はありませ
N		ん。 次の画面が導入されました。[Configuration] > [Device Management] > [Advanced] > [Rule Engine]。
ACL およびオブジェクトを編集するためのコンフィギュレーションセッションアクセス ルール内でのオブジェクトおよび ACL の前方参照	9.3(2)	独立したコンフィギュレーション セッションで ACL およびオブジェクトを編集できるようになりました。オブジェクトおよび ACL を前方参照することも可能です。つまり、まだ存在していないオブジェクトや ACL に対するルールおよびアクセスグループを設定することができます。