アクセス コントロール リスト

アクセス コントロール リスト（ACL）は、さまざまな機能で使用されます。ACL をアクセス ルールとしてインターフェイスに適用するか、グローバルに適用すると、アプライアンスを通過するトラフィックが許可または拒否されます。ACL では、他の機能のために、機能を適用するトラフィックを選択し、制御サービスではなく照合サービスを実行します。

ここでは、ACL の基本と ACL を設定およびモニタする方法について説明します。アクセス ルールとは、グローバルに、またはインターフェイスに適用される ACL のことです。これについては、「アクセス ルール」で詳しく説明します。

ACL について

アクセス コントロール リスト（ACL）では、ACL のタイプに応じてトラフィック フローを 1 つまたは複数の特性（送信元および宛先 IP アドレス、IP プロトコル、ポート、EtherType、その他のパラメータを含む）で識別します。ACL は、さまざまな機能で使用されます。ACL は 1 つまたは複数のアクセス コントロール エントリ（ACE）で構成されます。

ACL タイプ

ASA では、次のタイプの ACL が使用されます。

- 拡張 ACL：主に使用されるタイプです。この ACL は、サービス ポリシー、AAA ルール、WCCP、ボットネット トラフィック フィルタ、VPN グループおよび DAP ポリシーを含むさまざまな機能で、トラフィックがデバイスを通過するのを許可および拒否するアクセス ルールとトラフィックの照合に使用されます。ASDM では、これらの機能の多くに独自のルール ページがあります。これらのページでは、ACL Manager で定義した拡張 ACL は使

用できません。ただし、ACL Manager には、これらのページで作成した ACL が表示されます。拡張 ACL の設定 （8 ページ） を参照してください。

- EtherType ACL：EtherType ACL はブリッジ グループ メンバーのインターフェイスの非 IP レイヤ 2 トラフィックにのみ適用されます。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 ACL では、デバイスでの非 IP トラフィック フローを制御できます。EtherType ルールの設定を参照してください。
- Webtype ACL：クライアントレス SSL VPN トラフィックのフィルタリングに使用されます。この ACL では、URL または宛先アドレスに基づいてアクセスを拒否できます。Webtype ACL の設定 （14 ページ）を参照してください。
- 標準 ACL：宛先アドレスだけでトラフィックを識別します。このタイプの ACL は、少数の機能（ルート マップと VPN フィルタ）でしか使用されません。VPN フィルタでは拡張アクセス リストも使用できるので、標準 ACL の使用はルート マップだけにしてください。標準 ACL の設定 （13 ページ）を参照してください。

次の表に、ACL の一般的な使用目的と使用するタイプを示します。

表 *1: ACL* のタイプと一般的な使用目的

ACL の使用目的	ACL タイプ	説明
IP トラフィックのネットワーク アクセスの制御（ルーテッド モードおよびトランスペアレント モード）	拡張	ASA では、拡張 ACL により明示的に許可されている場合を除き、低位のセキュリティ インターフェイスから高位のセキュリティインターフェイスへのトラフィックは認められません。ルーテッドモードでは、ACLを使用して、ブリッジグループメンバーのインターフェイスと同じブリッジ グループの外部のインターフェイスとの間のトラフィックを許可する必要があります。 （注） 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 ACL 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。
AAA ルールでのトラフィック識別	拡張	AAA ルールでは、ACL を使用してトラフィックを識別します。
特定のユーザの IP トラフィックに対するネットワーク アクセス コントロールの強化	拡張、ユーザごとに AAA サーバからダウンロード	ユーザに適用するダイナミック ACL をダウンロードするように RADIUS サーバを設定できます。または、ASA 上に設定済みの ACL の名前を送信するようにサーバを設定できます。

ACL の使用目的	ACL タイプ	説明
VPN アクセスおよびフィルタリング	拡張 規格	リモート アクセスおよびサイト間 VPN のグループ ポリシーでは、標準または拡張ACLがフィルタリングに使用されます。リモート アクセス VPN では、クライアント ファイアウォール設定とダイナミック アクセス ポリシーにも拡張 ACL が使用されます。
トラフィック クラス マップでのモジュラ ポリシー フレームワークのトラフィックの識別	拡張	ACL を使用すると、クラスマップ内のトラフィックを識別できます。このマップは、モジュラ ポリシー フレームワークをサポートする機能に使用されます。モジュラ ポリシー フレームワークをサポートする機能には、TCP および一般的な接続設定やインスペクションなどがあります。
ブリッジ グループ メンバーのインターフェイスに対する非 IP トラフィックのネットワーク アクセスの制御	EtherType	ブリッジ グループのメンバーであるすべてのインターフェイスの EtherType に基づいて、トラフィックを制御をする ACL を設定できます。
ルート フィルタリングおよび再配布の特定	規格 拡張	各種のルーティング プロトコルでは、IP アドレスのルート フィルタリングと（ルートマップを介した）再配布に ACL が使用されます（IPv4 アドレスの場合は標準 ACL が、IPv6 アドレスの場合は拡張 ACL がそれぞれ使用されます）。
クライアントレス SSL VPN のフィルタリング	Webtype	Webtype ACL は、URL と宛先をフィルタリングするように設定できます。

ACL Manager

ACL Manager は、次の 2 つの方法で表示できます。

- メイン ウィンドウで、たとえば **[Configuration] > [Firewall] > [Advanced] > [ACL Manager]** の順に選択する。この場合、ACL Manager には拡張 ACL のみが表示されます。これらの ACL には、[Access Rules]、[Service Policy Rules]、および [AAA Rules] の各ページで作成したルールによって生成された ACL が含まれます。ACL Manager で編集を行う場合は、これらのルールに悪影響を与えないように注意してください。ここで加えた変更は、これらの他のページに反映されます。
- ACL が必要なポリシーから、フィールドの横にある [Manage] ボタンをクリックする。この場合、ポリシーで標準 ACL と拡張 ACL が許可されていれば、両方の ACL のタブが個別に表示されます。許可されていない場合は、標準、拡張、または Webtype の ACL のみを表示するようにビューがフィルタリングされます。EtherType ACL は表示されません。

メイン ウィンドウで標準 ACL と Webtype ACL を設定できるように、これらの ACL 用の個別のページが用意されています。これらのページは、名前のない ACL Manager と機能的に同じです。

- 標準 ACL：**[Configuration]** > **[Firewall]** > **[Advanced]** > **[Standard ACL]**。
- Webtype ACL：**[Configuration]** > **[Remote Access VPN]** > **[Clientless SSL VPN Access]** > **[Advanced]** > **[Web ACLs]**。

ACL 名

各 ACL には、outside_in、OUTSIDE_IN、101 などの名前または数値 ID があります。名前は 241 文字以下にする必要があります。実行コンフィギュレーションを表示するときに名前を簡単に見つけられるように、すべて大文字にすることを検討してください。

ACL の目的を識別するのに役立つ命名規則を作成します。ASDM では、「*interface-name_purpose_direction*」などの命名規則が使用されます。たとえば、「外部」インターフェイスにインバウンド方向で適用される ACL の場合には、「outside_access_in」のようになります。

従来、 ACL ID は数値でした。標準 ACL は、1 ～ 99 または 1300 ～ 1999 の範囲にありました。拡張 ACL は、100 ～ 199 または 2000 ～ 2699 の範囲にありました。ASA では、これらの範囲は強制されませんが、数値を使用する場合は、IOS ソフトウェアを実行するルータとの一貫性を保つために、これらの命名規則を引き続き使用することをお勧めします。

アクセス コントロール エントリの順序

1 つの ACL は、1 つまたは複数の ACE で構成されます。特定の行に明示的に ACE を挿入しない限り、ある ACL 名について入力した各 ACE はその ACL の末尾に追加されます。

ACE の順序は重要です。ASA は、パケットを転送するかドロップするかを決定するとき、エントリがリストされている順序で各 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。

したがって、一般的なルールの後に具体的なルールを配置した場合、具体的なルールは決してヒットしない可能性があります。たとえば、ネットワーク 10.1.1.0/24 を許可し、そのサブネット上のホスト 10.1.1.15 からのトラフィックをドロップする場合、10.1.1.15 を拒否する ACE は 10.1.1.0/24 を許可する ACE の前に置く必要があります。10.1.1.0/24 を許可する ACE を先にすると、10.1.1.15 は許可され、拒否 ACE は決して一致しません。

必要に応じて、[Up] ボタンと [Down] ボタンを使用してルールを再配置します。

許可/拒否と一致/不一致

アクセス コントロール エントリでは、ルールに一致するトラフィックを「許可」または「拒否」します。グローバルアクセスルールやインターフェイスアクセスルールなど、トラフィッ

クが ASA の通過を許可されるか、ドロップされるかを決定する機能に ACL を適用する場合、「許可」と「拒否」は文字どおりの意味を持ちます。

サービス ポリシー ルールなどのその他の機能の場合、「許可」と「拒否」は実際には「一致」または「不一致」を意味します。この場合、ACL では、アプリケーション インスペクションやサービス モジュールへのリダイレクトなど、その機能のサービスを受けるトラフィックを選択しています。「拒否される」トラフィックは、単に ACL に一致せず、したがってサービスを受けないトラフィックのことです（ASDM では、たとえば、サービス ポリシー ルールでは実際には一致/不一致が使用され、AAA ルールでは認証/未認証が使用されますが、CLI では常に許可/拒否が使用されます）。

アクセス コントロールによる暗黙的な拒否

through-the-box アクセス ルールに使用する ACL には末尾に暗黙の deny ステートメントがあります。したがって、インターフェイスに適用される ACL などのトラフィック制御 ACL では、あるタイプのトラフィックを明示的に許可しない場合、そのトラフィックはドロップされます。たとえば、1 つまたは複数の特定のアドレス以外のすべてのユーザが ASA 経由でネットワークにアクセスできるようにするには、特定のアドレスを拒否してから、その他のすべてのアドレスを許可する必要があります。

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。

サービス対象のトラフィックの選択に使用される ACL の場合は、明示的にトラフィックを「許可」する必要があります。「許可」されていないトラフィックはサービスの対象になりません。「拒否された」トラフィックはサービスをバイパスします。

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 で明示的にすべてのトラフィックを拒否すると、IP および ARP トラフィックが拒否されます。許可されるのは、自動ネゴシエーションなどの物理プロトコル トラフィックだけです。

NAT 使用時に拡張 ACL で使用する IP アドレス

NAT または PAT を使用すると、アドレスまたはポートが変換され、通常は内部アドレスと外部アドレスがマッピングされます。変換されたポートまたはアドレスに適用される拡張 ACL を作成する必要がある場合は、実際の（変換されていない）アドレスまたはポートを使用するか、マッピングされたアドレスまたはポートを使用するかを決定する必要があります。要件は機能によって異なります。

実際のアドレスとポートが使用されるので、NAT コンフィギュレーションが変更されても ACL を変更する必要はなくなります。

実際の IP アドレスを使用する機能

次のコマンドおよび機能では、インターフェイスに表示されるアドレスがマッピング アドレスである場合でも、実際の IP アドレスを使用します。

- アクセス ルール（access-group コマンドで参照される拡張 ACL）
- サービス ポリシー ルール（モジュラ ポリシー フレームワークの match access-list コマンド）
- ボットネット トラフィック フィルタのトラフィック分類（dynamic-filter enable classify-list コマンド）
- AAA ルール（aaa ... match コマンド）
- WCCP（wccp redirect-list group-list コマンド）

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。

マッピング IP アドレスを使用する機能

次の機能は、ACL を使用しますが、これらの ACL は、インターフェイス上で認識されるマッピングされた値を使用します。

- IPsec ACL
- capture コマンドの ACL
- ユーザ単位 ACL
- ルーティング プロトコルの ACL
- 他のすべての機能の ACL

時間ベース ACE

ルールが一定期間だけアクティブになるように、拡張 ACE と Webtype ACE に時間範囲オブジェクトを適用することができます。このタイプのルールを使用すると、特定の時間帯には許容できるものの、それ以外の時間帯には許容できないアクティビティを区別できます。たとえば、勤務時間中に追加の制限を設け、勤務時間後または昼食時にその制限を緩めることができます。逆に、勤務時間外は原則的にネットワークをシャットダウンすることもできます。

時間範囲オブジェクトが含まれていないルールでは、プロトコル、送信元、宛先、およびサービス基準が正確に同じ時間ベースのルールを作成することはできません。時間ベースではないルールは、重複した時間ベースのルールを常にオーバーライドします（冗長であるため）。

（注） ACL を非アクティブにするための指定の終了時刻の後、約 80 ～ 100 秒の遅延が発生する場合があります。たとえば、指定の終了時刻が 3:50 の場合、この 3:50 は終了時刻に含まれているため、コマンドは、3:51:00 ～ 3:51:59 の間に呼び出されます。コマンドが呼び出された後、ASA は現在実行されているすべてのタスクを終了し、コマンドに ACL を無効にさせます。

アクセス制御リストのライセンス

アクセス制御リストは特別なライセンスを必要としません。

ただし、エントリ内でプロトコルとして **sctp** を使用する場合は、キャリア ライセンスが必要です。

ACL のガイドライン

ファイアウォール モード

- 標準 ACL と拡張 ACL は、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ます。
- Webtype ACL は、ルーテッド モードのみでサポートされます。
- EtherType ACL は、ルーテッドおよびトランスペアレント モードで、ブリッジ グループ メンバーのインターフェイスに対してのみサポートされます。

フェールオーバーとクラスタリング

コンフィギュレーション セッションは、フェイルオーバーまたはクラスタ ユニット間で同期されません。あるセッションで変更をコミットすると、通常どおりすべてのフェイルオーバーおよびクラスタ ユニットでその変更が反映されます。

IPv6

- 拡張 ACL と Webtype ACL では、IPv4 アドレスと IPv6 アドレスを組み合わせて使用できます。
- 標準 ACL では、IPv6 アドレスは使用できません。
- EtherType ACL では、IP アドレスは使用しません。

その他のガイドライン

- ネットワーク マスクを指定するときは、指定方法が Cisco IOS ソフトウェアの **access-list** コマンドとは異なることに注意してください。ASA では、ネットワーク マスク（たとえ

ば、Class C マスクの 255.255.255.0）が使用されます。Cisco IOS マスクでは、ワイルドカード ビット（たとえば、0.0.0.255）が使用されます。

- 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。
- 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。
- （拡張 ACL のみ）次の機能では、ACL を使用しますが、アイデンティティ ファイアウォール（個人またはグループ名を指定）、FQDN（完全修飾ドメイン名）、または Cisco TrustSec 値を含む ACL は使用できません。
  - VPN の crypto map コマンド
  - VPN の group-policy コマンド、ただし、vpn-filter を除く
  - WCCP
  - DAP

ACL の設定

次の各セクションでは、さまざまなタイプの汎用 ACL の設定方法について説明します。ただし、アクセス ルール（EtherType を含む）、サービス ポリシー ルール、および AAA ルールとして使用される ACL と、ASDM がこれらのルールベースのポリシー用に特定目的のページを提供しているその他の用途に使用される ACL は除きます。

拡張 ACL の設定

拡張 ACL は ACE の名前付きコンテナとして表されます。新しい ACL を作成するには、まずコンテナを作成する必要があります。その後、ACL Manager でテーブルを使用して ACE を追加したり、既存の ACE を編集したり、ACE を並べ替えたりできます。

拡張 ACL 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。

手順

ステップ 1 [Configuration] > [Firewall] > [Advanced] > [ACL Manager] を選択します。

ステップ 2 新しい ACL を作成する場合は、**[Add]** > **[Add ACL]** を選択し、名前を入力して [OK] をクリックします。

ACL コンテナがテーブルに追加されます。後でこのコンテナを選択して [Edit] をクリックすることにより、コンテナの名前を変更できます。

ステップ 3 次のいずれかを実行します。

- ACL の末尾に ACE を追加するには、ACL 名または ACL 内の任意の ACE を選択し、[Add] > [Add ACE] を選択します。
- ACE を特定の場所に挿入するには、既存の ACE を選択し、[Add] > [Insert] を選択してそのルールの上に ACE を追加するか、[Add] > [Insert After] を選択します。
- ルールを編集するには、ルールを選択して [Edit] をクリックします。

ステップ 4 ACE のプロパティを入力します。選択する主なオプションは次のとおりです。

- [Action: Permit/Deny]：指定したトラフィックを許可（選択）するか、拒否（選択解除、不一致）するかを選択します。
- [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。Cisco 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については、拡張 ACE のプロパティ （9 ページ）を参照してください。

ACE の定義が完了したら、[OK] をクリックしてテーブルにルールを追加します。

ステップ 5 [Apply] をクリックします。

拡張 ACE のプロパティ

拡張ACLのACEを追加または編集するときに、次のプロパティを設定できます。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、フィールドで使用できるオブジェクトを選択、作成、または編集できます。

[Action]：**[Permit]/[Deny]**

指定したトラフィックを許可（選択）するか、拒否（選択解除、不一致）するかを選択します。

[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 ～ 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、UDP または SCTP を宛先サービスとして指定した場合は、TCP、UDP、TCP-UDP、または SCTP 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 ～ 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。

サービス

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、UDP、または SCTP 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、UDP、および SCTP 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）、sctp/diameter のようにポートを指定できます。サービスの指定の詳細については、拡張 ACE のサービスの仕様 （12 ページ）を参照してください。

説明

ACE 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。各行は CLI の注釈として追加され、注釈は ACE 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。これらのオプションは、アクセス ルールとして使用される ACL、つまり、インターフェイスに接続されている ACL またはグローバルに適用されている ACL のみに適用されます。このオプションは他の機能に使用されている ACL では無視されます。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] > [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。

拡張 ACE のサービスの仕様

拡張 ACE の宛先サービスには、次の条件を指定できます。送信元サービスの場合は、オプションは似ていますが、より限定されており、TCP、UDP、TCP-UDP、または SCTP 条件しか指定できません。

オブジェクト名

任意のタイプのサービス オブジェクトまたはサービス オブジェクト グループの名前。これらのオブジェクトには、以下で説明するさまざまな仕様を含めることができます。このため、ACL 間でサービス定義を再利用することが簡単にできます。定義済みオブジェクトが多数用意されているため、手動で仕様を入力したり、独自のオブジェクトを作成したりすることなく、必要なオブジェクトが見つかる場合があります。

プロトコル

1 ～ 255 の範囲の数値または**ip**、**tcp**、**udp**、**gre** などの既知の名前。

TCP、UDP、TCP-UDP、SCTP ポート

tcp、**udp**、**tcp-udp**、および **sctp** キーワードにポートを指定することができます。tcp-udp キーワードを使用すると、tcp と udp を個別に指定せずに両方のプロトコルのポートを定義できます。ポートは次の方法で指定できます。

- 単一ポート：tcp/80、udp/80、tcp-udp/80、sctp/3868、または tcp/www、udp/snmp、または sctp/diameter などの既知のサービス名。
- ポート範囲：tcp/1-100、udp/1-100、tcp-udp/1-100、sctp/1-100 は、ポート 1 ～ 100（1 と 100 を含む）に一致します。

- ポートに等しくない：仕様の先頭に != を追加します。たとえば、TCP ポート 80（HTTP）以外の任意の TCP トラフィックに一致させるには、!=tcp/80 と指定します。
- ポート番号より小さい：< を追加します。たとえば、150 未満の任意のポートの TCP トラフィックに一致させるには、<tcp/150 と指定します。
- ポート番号より大きい：> を追加します。たとえば、150 超の任意のポートの TCP トラフィックに一致させるには、>tcp/150 と指定します。

（注） DNS、Discard、Echo、Ident、NTP、RPC、SUNRPC、および Talk は、それぞれに TCP の定義と UDP の定義の両方が必要です。TACACS+ では、ポート 49 に対して 1 つの TCP 定義が必要です。

ICMP、ICMP6 メッセージ

特定のメッセージ（ping エコー要求や応答メッセージなど）やメッセージ コードをターゲットにできます。ICMP（IPv4 向け）および ICMP6（IPv6 向け）をカバーする定義済みオブジェクトが多数用意されているため、手動での条件定義が不要になる場合があります。形式は次のようになります。

icmp/*icmp_message_type*[/*icmp_message_code*]

icmp6/*icmp6_message_type*[/*icmp6_message_code*]

メッセージ タイプは 1 ～ 255 の範囲の数値または既知の名前で、コードは 0 ～ 255 の範囲の数値です。選択した数値が実際のタイプ/コードに一致することを確認します。そうしないと、ACE が一致しません。

標準 ACL の設定

標準 ACL は ACE の名前付きコンテナとして表されます。新しい ACL を作成するには、まずコンテナを作成する必要があります。その後、標準 ACL テーブルを使用して ACE を追加したり、既存の ACE を編集したり、ACE を並べ替えたりできます。このテーブルは、ACL を設定するときと ACL を使用するポリシーを設定するときに ACL Manager でタブとして表示されます。どちらの場合も、ウィンドウへの行き方を除いて手順は同じです。

標準 ACL では、 IPv4 アドレスのみを使用して、宛先アドレスのみを定義します。

手順

ステップ 1 [Configuration] > [Firewall] > [Advanced] > [Standard ACL] を選択します。

ステップ 2 新しい ACL を作成する場合は、**[Add]** > **[Add ACL]** を選択し、名前を入力して [OK] をクリックします。

ACL コンテナがテーブルに追加されます。標準 ACL の名前は変更できません。

ステップ 3 次のいずれかを実行します。

- ACL の末尾に ACE を追加するには、ACL 名または ACL 内の任意の ACE を選択し、[Add] > [Add ACE] を選択します。
- ACE を特定の場所に挿入するには、既存の ACE を選択し、[Add] > [Insert] を選択してそのルールの上に ACE を追加するか、[Add] > [Insert After] を選択します。
- ルールを編集するには、ルールを選択して [Edit] をクリックします。

ステップ 4 ACE のプロパティを入力します。次のオプションがあります。

- [Action: Permit/Deny]：指定したトラフィックを許可（選択）するか、拒否（選択解除、不一致）するかを選択します。
- [Address]：トラフィック フローの宛先またはターゲット アドレスを定義します。10.100.1.1 などのホスト アドレスか、ネットワーク（10.100.1.0/24 または 10.100.1.0/255.255.255.0 形式）を指定できます。または、ネットワーク オブジェクトを選択することもできます（単にオブジェクトの内容が [Address] フィールドにロードされます）。
- [Description]：ACE の目的に関する説明を 1 行あたり 100 文字以下で入力します。複数行を入力できます。各行は CLI の注釈として追加され、注釈は ACE 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。

ACE の定義が完了したら、[OK] をクリックしてテーブルにルールを追加します。

ステップ 5 [Apply] をクリックします。

Webtype ACL の設定

Webtype ACL は、クライアントレス SSL VPN トラフィックのフィルタリング、特定のネットワーク、サブネット、ホスト、およびWebサーバへのユーザアクセスの制限に使用されます。フィルタを定義しない場合は、すべての接続が許可されます。Webtype ACL は ACE の名前付きコンテナとして表されます。新しい ACL を作成するには、まずコンテナを作成する必要があります。その後、Web ACL テーブルを使用して ACE を追加したり、既存の ACE を編集したり、ACE を並べ替えたりできます。このテーブルは、ACL を設定するときと ACL を使用するポリシーを設定するときにACL Managerでタブとして表示されます。どちらの場合も、ウィンドウへの行き方を除いて手順は同じです。

Webtype ACL には、URL 仕様に加えて 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。

手順

ステップ 1 [Configuration] > **[Remote Access VPN]** > **[Clientless SSL VPN Access]** > **[Advanced]** > **[Web]** > **[ACLs]** の順に選択します。

ステップ 2 新しい ACL を作成する場合は、**[Add]** > **[Add ACL]** を選択し、名前を入力して [OK] をクリックします。

ACL コンテナがテーブルに追加されます。後でこのコンテナを選択して [Edit] をクリックすることにより、コンテナの名前を変更できます。

ステップ 3 次のいずれかを実行します。

- ACL の末尾に ACE を追加するには、ACL 名または ACL 内の任意の ACE を選択し、[Add] > [Add ACE] を選択します。
- ACE を特定の場所に挿入するには、既存の ACE を選択し、[Add] > [Insert] を選択してそのルールの上に ACE を追加するか、[Add] > [Insert After] を選択します。
- ルールを編集するには、ルールを選択して [Edit] をクリックします。

ステップ 4 ACE のプロパティを入力します。選択する主なオプションは次のとおりです。

- [Action: Permit/Deny]：指定したトラフィックを許可（選択）するか、拒否（選択解除、不一致）するかを選択します。
- [Filter]：宛先に基づくトラフィック一致条件。プロトコルを選択してサーバ名（オプションでパスとファイル名）を入力することによって URL を指定するか、IPv4 または IPv6 アドレスと TCP サービスを指定することができます。

使用可能なすべてのオプションについては、Webtype ACE のプロパティ （15 ページ）を参照してください。

ACE の定義が完了したら、[OK] をクリックしてテーブルにルールを追加します。

ステップ 5 [Apply] をクリックします。

Webtype ACE のプロパティ

Webtype ACL の ACE を追加または編集するときに、次のプロパティを設定できます。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、フィールドで使用できるオブジェクトを選択、作成、または編集できます。

特定の ACE について、URL またはアドレスでフィルタリングすることができます。ただし、両方でフィルタすることはできません。

- [Action: Permit/Deny]：指定したトラフィックを許可（選択）するか、拒否（選択解除、不一致）するかを選択します。

- [Filter on URL] ：宛先 URL に基づくトラフィック一致条件。プロトコルを選択してサーバ名（オプションでパスとファイル名）を入力します。たとえば、http://www.example.com と指定します。または、すべてのサーバを対象にするには、http://*.example.com と指定します。以下では、URL の指定に関するヒントと制限事項をいくつか示します。
  - すべての URL を照合する場合は、**any** を選択します。
  - 「Permit url any」と指定すると、「プロトコル://サーバ IP/パス」の形式の URL はすべて許可され、このパターンに一致しないトラフィック（ポート転送など）はブロックされます。暗黙的な拒否が発生しないよう、必要なポート（Citrix の場合はポート 1494）への接続を許可する ACE を使用してください。
  - スマート トンネルと ica プラグインは、smart-tunnel:// と ica:// のタイプにのみ一致するため、「permit url any」を使用した ACL によって影響を受けることはありません。
  - 使用できるプロトコルは、cifs://、citrix://、citrixs://、ftp://、http://、https://、imap4://、nfs://、pop3://、smart-tunnel://、および smtp:// です。プロトコルでワイルドカードを使用することもできます。たとえば、htt* は http および https に一致し、アスタリスク * はすべてのプロトコルに一致します。たとえば、*://*.example.com は、example.com ネットワークへのすべてのタイプの URL ベース トラフィックに一致します。
  - smart-tunnel:// URL を指定すると、サーバ名だけを含めることができます。URL にパスを含めることはできません。たとえば、smart-tunnel://www.example.com は受け入れ可能ですが、smart-tunnel://www.example.com/index.html は受け入れ不可です。
  - アスタリスク（*）：空の文字列を含む任意の文字列に一致します。すべての http URL に一致させるには、http://*/* と入力します。
  - 疑問符 ? は任意の 1 文字に一致します。
  - 角カッコ（[]）：文字の範囲を指定する際に使用する演算子です。角カッコ内に指定された範囲に属する任意の 1 文字に一致します。たとえば、http://www.cisco.com:80/ と http://www.cisco.com:81/ の両方に一致させるには、「**http://www.cisco.com:8[01]/**」と入力します。

- [Filter on Address and Service] ：宛先アドレスとサービスに基づいてトラフィックを照合します。
  - [Address]：宛先の IPv4 または IPv6 アドレスです。すべてのアドレスに一致させるには、すべての IPv4 または IPv6 アドレスに一致する **any** を使用します。IPv4 のみに一致させるには **any4** を、IPv6 のみに一致させるには **any6** を使用します。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）を指定できます。または、ネットワーク オブジェクトを選択して、オブジェクトの内容をフィールドにロードすることもできます。

- [Service]：単一の TCP サービス仕様。デフォルトはポートなしの **tcp** ですが、単一のポート（tcp/80 や tcp/www など）またはポート範囲（tcp/1-100 など）を指定できます。演算子を含めることができます。たとえば、!=tcp/80 は 80 以外のポート、<tcp/80 は 80 未満のすべてのポート、>tcp/80 は 80 超のすべてのポートです。

- [Enable Logging]、[Logging Level]、[More Options] > [Logging Interval]：ロギング オプションでは、実際にトラフィックを拒否するルールについて 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] ：ルールのロギングを無効にします。このルールで拒否されるトラフィックについては、どのタイプの syslog も発行されません。
  - [Select Enable Logging with Logging Level = Default]： ルールのデフォルト ロギングを提供します。拒否されたパケットごとに syslog メッセージ 106103 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]： 106103 の代わりに、集約された syslog メッセージ 106102 を提供します。メッセージ 106102 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。

- [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。

Webtype ACL の例

以下では、Webtype ACL の URL ベースのルールの例をいくつか示します。

	フィルタ	影響
拒否	url http://*.yahoo.com/	Yahoo! すべてへのアクセスを拒否します。
拒否	url cifs://fileserver/share/directory	指定された場所にあるすべてのファイルへのアクセスを拒否します。
拒否	url https://www.example.com/directory/file.html	指定されたファイルへのアクセスを拒否します。
許可	url https://www.example.com/directory	指定された場所へのアクセスを許可します。

	フィルタ	影響
拒否	url http://*:8080/	ポート 8080 を介した任意の場所への HTTPS アクセスを拒否します。
拒否	url http://10.10.10.10	10.10.10.10 への HTTP アクセスを拒否します。
許可	url any	任意の URL へのアクセスを許可します。通常は、url アクセスを拒否する ACL のあとに使用されます。

ACL のモニタリング

ACL Manager、標準 ACL、Web ACL、および EtherType ACL テーブルには、ACL がまとめて表示されます。ただし、デバイスに設定されている内容を正確に表示するには、次のコマンドを使用します。コマンドを入力するには、[Tools] > [Command Line Interface] を選択します。

- **show access-list** [*name*]：各 ACE の行番号とヒット カウントを含むアクセス リストを表示します。ACL 名を指定してください。そうしないと、すべてのアクセス リストが表示されます。
- **show running-config access-list** [*name*]：現在実行しているアクセス リスト コンフィギュレーションを表示します。ACL名を指定してください。そうしないと、すべてのアクセス リストが表示されます。

ACL の履歴

機能名	リリース	説明
標準、拡張、Webtype ACL	7.0(1)	ACL は、ネットワーク アクセスを制御したり、さまざまな機能を適用するトラフィックを指定したりするために使用されます。拡張アクセス コントロール リストは、 through-the-box アクセス コントロールとその他のいくつかの機能に使用されます。標準 ACL は、ルート マップと VPN フィルタで使用されます。Webtype ACL は、クライアントレス SSL VPN フィルタリングで使用されます。EtherType ACL は、IP 以外のレイヤ 2 トラフィックを制御します。 ACL を設定するための ACL Manager およびその他のページが追加されました。

機能名	リリース	説明
拡張 ACL での実際の IP アドレス	8.3(1)	NAT または PAT を使用するときは、さまざまな機能で、ACL でのマッピング アドレスおよびポートの使用が不要になります。これらの機能については、変換されていない実際のアドレスとポートを使用する必要があります。実際のアドレスとポートが使用されるので、NAT コンフィギュレーションが変更されても ACL を変更する必要はなくなります。
拡張 ACL でのアイデンティティ 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 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 トラフィックを制御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]。
拡張 ACL での Cisco TrustSec のサポート	9.0(1)	Cisco 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。
拡張 ACL と Webtype ACL での IPv4 アドレスと IPv6 アドレスの統合	9.0(1)	拡張 ACL と Webtype ACL で IPv4 アドレスと 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]

機能名	リリース	説明
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。 アクセス ルールの詳細設定が変更されました。
Stream Control Transmission Protocol（SCTP）の ACL のサポート	9.5(2)	**sctp** プロトコルを使用して、ポートの仕様を含む ACL ルールを作成できるようになりました。 **[Configuration]** > **[Firewall]** > **[Advanced]** > **[ACL Manager]** ページでアクセス制御エントリの追加/編集ダイアログ ボックスが変更されました。
Ethertype ルールで、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がサポートされます。	9.6(2)	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に対する Ethertype のアクセス制御ルールを作成できるようになりました。この追加により、**bpdu** キーワードが対象トラフィックに一致しなくなります。**dsap 0x42** に対して **bpdu** ルールを書き換えます。 次の画面が変更されました。**[Configuration]** > **[Firewall]** > **[EtherType Rules]**。
ブリッジ グループ メンバーのインターフェイスで Ethertype ルールのルーテッド モード、およびブリッジ グループの仮想インターフェイス（BVI）の拡張アクセス ルールのサポート。	9.7(1)	Ethertype ACL を作成し、ルーテッド モードのブリッジ グループ メンバーのインターフェイスに適用できるようになりました。また、メンバー インターフェイスに加えて、ブリッジ仮想インターフェイス（BVI）に拡張アクセス ルールを適用することもできます。 次の画面が変更されました。**[Configuration]** > **[Firewall]** > **[Access Rules]**、**[Configuration]** > **[Firewall]** > **[Ethertype Rules]**。