CHAPTER 19

# アクセス ルールの設定

## Access Rules

Access Rules ウィンドウには、ルールで表現されたネットワーク全体のセキュリティ ポリシーが表示されます。

**Access Rules** オプションを選択するとき、このウィンドウでは、使用可能なプロトコルやポートなど、特定ホストまたはネットワークによる別のホストまたはネットワークへのアクセスを制御するアクセス コントロール リストを定義できます。アクセスリストはコンジット リストおよびアウトバウンド リストに取って代わります。

デフォルトではセキュリティ アプライアンスで、より高いセキュリティ レベルからのトラフィック（内部など）は低いセキュリティ レベル（外部など）にアクセスできます。内部ネットワークからのすべてのアウトバウンド IP トラフィックを許可する内部インターフェイスには、暗黙のアクセスリストがあります（セキュリティ アプライアンスは、アダプティブ セキュリティ アルゴリズムを使用して外部ネットワークから内部ネットワークに宛てたトラフィックを拒否します。アダプティブ セキュリティ アルゴリズムは、セキュリティへのステートフルなアプローチ方法です。各インバウンド パケットは、アダプティブ セキュリティ アルゴリズムおよびメモリのコネクション ステート情報に対して検査されます）。ASDM には暗黙のアクセスリストが表示されますが、編集することはできません。アウトバウンド トラフィックを制限するには、アクセスリストを追加します（この場合、暗黙のアクセスリストは削除されます）。

接続がすでに確立されていない限り、各インバウンド パケットはアダプティブ セキュリティ アルゴリズムを使用して検査されます。デフォルトでは、許可するアクセスリストを追加しない限り、セキュリティ アプライアンスでトラフィックはファイアウォールを通過できません。

通常、アダプティブ セキュリティ アルゴリズムで拒否されるトラフィックを許可するには、アクセスリストを追加します。たとえば、外部インターフェイスにアクセスリストを追加すれば、DMZ ネットワーク上の Web サーバへのパブリック アクセスを許可できます。

### 制約事項

各アクセスリストの最後には、許可されないすべてのトラフィックを拒否する、表記されない暗黙のルールがあります。トラフィックが access control entry（ACE; アクセス コントロール エントリ）で明示的に許可されていない場合、そのトラフィックは拒否されます。このトピックでは、ACE をルールと呼びます。

### 前提条件

必要であれば、Addresses タブでネットワーク グループを作成します。

### フィールド

注 : カーソルをカラムの線に重ねて二重矢印になったら、その矢印を動かしてテーブル カラムの幅を調整できます。カラムの線をクリックして希望のサイズにドラッグします。

- Add : 新しいアクセス ルールを追加します。
- Edit : アクセス ルールを編集します。
- Delete : アクセス ルールを削除します。
- Move Up : ルールを上に移動します。ルールは、このテーブルに表示される順序で評価されるため、重複するルールがあると順序によって評価が異なります。
- Move Down : ルールを下に移動します。
- Cut : ルールを切り取ります。
- Copy : ルールのパラメータをコピーします。Paste ボタンを使用すれば、新しいルールを同じパラメータで開始できます。
- Paste: コピーまたは切り取ったルールのパラメータがあらかじめ入力された Add/Edit Rule ダイアログボックスが開きます。そこでルールを変更し、テーブルに追加します。Paste ボタンをクリックすると、選択したルールの上にルールが追加されます。Paste ドロップダウン リストから Paste After 項目を選択すると、選択したルールの後にルールが追加されます。
- Find : 一致するルールだけを表示するように、表示内容をフィルタリングします。**Find** をクリックすると、Filter フィールドが開きます。もう 1 回 **Find** をクリックすると、Filter フィールドが非表示になります。
  - Filter ドロップダウン リスト : フィルタリングする基準を、Interface、Source、Destination、Source or Destination、Destination Service、または Rule Query のいずれかから選択します。ルール クエリーとは、複数の基準の集合で、保存して繰り返し使用できます。
  - Condition ドロップダウン リスト : 基準が Source、Destination、Source or Destination、Destination Service の場合、条件を is または includes から選択します。
  - Filter フィールド : Interface タイプの場合、このフィールドはドロップダウン リストになり、インターフェイス名を選択できます。Rule Query タイプの場合、ドロップダウン リストにはすべての定義済みルール クエリーが含まれています。Source および Destination タイプの場合は、IP アドレスを受け入れます。IP アドレスを 1 つ手動で入力するか、**...** ボタンをクリックし、Browse Address ダイアログボックスを開いて参照します。Destination Service タイプの場合は、TCP、UDP、TCP-UDP、ICMP、または IP プロトコル タイプを受け入れます。プロトコル タイプを 1 つ手動で入力するか、**...** ボタンをクリックし、Browse Service Groups ダイアログボックスを開いて参照します。Filter フィールドは、カンマまたはスペースで区切って、複数のエントリを受け入れます。また、ワイルドカードも受け入れます。
  - Filter : フィルタリングを実行します。
  - Clear : 一致内容および表示内容をすべてクリアします。
  - Rule Query : 名前付きルール クエリーを管理できる Rule Queries ダイアログボックスを開きます。
- Diagram : ルール テーブルの下に Rule Flow Diagram 領域を表示します。この図では、ネットワーク、トラフィックのタイプ、インターフェイス名、フローの方向、およびアクションを示しています。
- Export : カンマ区切り形式または html 形式でファイルにエクスポートします。
- Show : Real-Time Log Viewer に選択したアクセス ルールが生成した syslog を表示します。

次の説明では、Access Rules テーブルのカラムをまとめています。テーブル行をダブルクリックすれば、カラムの内容を編集できます。ルールは、実行順に表示されます。ルールを右クリックすると、Insert および Insert After 項目と共に、ボタンで表されているオプションがすべて上に表示されます。これらの項目では、選択したルールの前に新しいルールが挿入されるか（Insert）、選択したルールの後ろに新しいルールが挿入されます（Insert After）。

- No : ルールの評価順序を示します。
- Enabled: ルールがイネーブルになっているか、またはディセーブルになっているかを示します。

- Source：Destination Type フィールドで指定された宛先へのトラフィックが許可または拒否される IP アドレス、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 any を指定します。アドレス カラムには、単語 any が付いたインターフェイス名が含まれることがあります（inside: any など）。これは、内部インターフェイスのすべてのホストが、このルールの影響を受けるという意味です。
- Destination：Source Type 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 IP アドレス、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 any を指定します。アドレス カラムには、単語 any が付いたインターフェイス名が含まれることがあります（outside: any など）。これは、外部インターフェイスのすべてのホストが、このルールの影響を受けるという意味です。また、詳細モードでは、アドレス カラムに角カッコで囲まれた IP アドレスが含まれることもあります（[209.165.201.1-209.165.201.30] など）。これらのアドレスは、変換済みアドレスです。内部ホストが外部ホストへの接続を作成すると、ファイアウォールは内部ホストのアドレスをプールのアドレスにマッピングします。ホストがアウトバウンド接続を作成した後、ファイアウォールはこのアドレス マッピングを維持します。アドレス マッピング構造は xlate と呼ばれ、一定の時間、メモリに保持されます。アクセスリストで許可されていれば、この時間内に、外部ホストはプールの変換済みアドレスを使用して、内部ホストへの接続を開始できます。通常、内部ホストは常に同じ IP アドレスを使用するため、外部から内部への接続にはスタティック トランスレーションが必要です。
- Service：ルールで指定されるサービスまたはプロトコルを表示します。
- Action：ルールに適用されるアクションです（Permit または Deny）。
- Hits：ルールにヒットした数を表示します。このカラムは Preferences ダイアログボックスで設定した頻度に応じて動的に更新されます。ヒット数は、明示的なルールにだけ適用されます。暗黙のルールのヒット数は Access Rules テーブルに表示されません。
- Logging：アクセスリストのロギングをイネーブルにしている場合、このカラムには、ロギング レベル、およびログ メッセージ間の間隔が秒数で表示されます。
- Time：ルールが適用される時間範囲が表示されます。
- Description：ルールを追加したときに入力した説明が表示されます。暗黙のルールには、「Implicit outbound rule」という説明が含まれます。
- Addresses：このタブでは、サービス グループまたはネットワーク オブジェクト グループを追加、編集、削除、または検索できます。IP アドレス オブジェクトは、その後のルール作成で簡単に選択できるように、ルール作成の間、送信元エントリおよび宛先エントリに基づいて自動的に作成されます。手動では追加、編集、または削除できません。
- Services：このタブでは、サービスを追加、編集、削除、または検索できます。
- Time Ranges：時間範囲を追加、編集、または削除できるタブです。

### モード

次の表に、この機能を使用できるモードを示します。

| ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|
| | | | マルチ | |
| ルーテッド | 透過 | シングル | コンテキスト | システム |
| • | • | • | • | — |

## Rule Queries

Rule Queries ダイアログボックスでは、ルールを検索するときに Filter フィールドで使用できる名前付きルール クエリーを管理できます。

### フィールド

- Add：ルール クエリーを追加します。
- Edit：ルール クエリーを編集します。
- Delete：ルール クエリーを削除します。
- Name：ルール クエリーの名前を一覧表示します。
- Description：ルール クエリーの説明を一覧表示します。

### モード

次の表に、この機能を使用できるモードを示します。

| ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|
| | | | マルチ | |
| ルーテッド | 透過 | シングル | コンテキスト | システム |
| • | • | • | • | — |

## New/Edit Rule Query

New/Edit Rule Query ダイアログボックスでは、ルールを検索するときに Filter フィールドで使用できる名前付きルール クエリーを追加または編集できます。

### フィールド

- Name：ルール クエリーの名前を入力します。
- Description：ルール クエリーの説明を入力します。
- Match Criteria：この領域には、フィルタリングのための基準が一覧表示されます。
  - any of the following criteria：一覧表示された任意の基準に一致するようにルール クエリーを設定します。
  - all of the following criteria：一覧表示されたすべての基準に一致するようにルール クエリーを設定します。
  - Field：基準のタイプを一覧表示します。インターフェイスまたは送信元などです。
  - Value：「inside」など、基準の値を一覧表示します。
  - Remove：選択した基準を削除します。
- Define New Criteria：この領域では、新しい基準を定義して、照合基準に追加します。
  - Field：ルール クエリーにネストされる Interface、Source、Destination、Service、Action、または他の Rule Query などの基準のタイプを選択します。
  - Value：検索する値を入力します。Interface タイプの場合、このフィールドはドロップダウン リストになり、インターフェイス名を選択できます。Action タイプの場合、ドロップダウン リストには Permit と Deny が表示されます。Rule Query タイプの場合、ドロップダウン リストにはすべての定義済みルール クエリーが含まれています。Source および Destination タイプの場合は、IP アドレスを受け入れます。IP アドレスを 1 つ手動で入力するか、または ... ボタンをクリックし、Browse Address ダイアログボックスを開いて参照します。Service タイプの場合は、TCP、UDP、TCP-UDP、ICMP、または IP プロトコル タイプを受け入れます。プロトコル タイプを 1 つ手動で入力するか、... ボタンをクリックし、Browse Service Groups ダイアログボックスを開いて参照します。

— Add：Match Criteria テーブルに基準を追加します。

### モード

次の表に、この機能を使用できるモードを示します。

| ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|
| | | | マルチ | |
| ルーテッド | 透過 | シングル | コンテキスト | システム |
| • | • | • | • | — |

## Add/Edit Access Rule

Add/Edit Rule ダイアログボックスでは、新しいルールの作成、または既存のルールの変更を実行できます。

### フィールド

- Interface：ルールを適用するインターフェイスを指定します。
- Action：新しいルールのアクション タイプを決定します。Permit または Deny のいずれかを選択します。
  - Permit：すべての一致トラフィックを許可します。
  - Deny：すべての一致トラフィックを拒否します。
- Source：Destination フィールドで指定された宛先へのトラフィックが許可または拒否される IP アドレス、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 any を指定します。

  ...：既存の IP アドレス オブジェクト、IP 名、ネットワーク オブジェクト グループ、またはすべてを選択、追加、編集、削除、または検索できます。
- Destination：Source Type 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 IP アドレス、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 any を指定します。

  ...：既存の IP アドレス オブジェクト、IP 名、ネットワーク オブジェクト グループ、またはすべてを選択、追加、編集、削除、または検索できます。
- Service：サービスのリストからポート番号、ポートの範囲、またはウェルノウン サービス名やグループを指定するには、このオプションを選択します。

  ...：事前に設定したリストから既存のサービスを選択、追加、編集、削除、または検索できます。
- Description：（オプション）アクセス ルールの説明を入力します。
- Enable Logging：アクセスリストのロギングをイネーブルにします。
  - Logging Level：default、emergencies、alerts、critical、errors、warnings、notifications、informational、または debugging を指定します。
- More Options：ルールの追加設定オプションを表示します。
  - Enable Rule：ルールをイネーブルまたはディセーブルにします。
  - Traffic Direction：どちらの方向のトラフィックにルールを適用するかを決定します。オプションには Incoming と Outgoing があります。
  - Source Service：送信元のプロトコルとサービスを指定します（TCP または UDP サービスのみ）。

    ...：事前に設定したリストから送信元サービスを選択、追加、編集、削除、または検索できます。
  - Logging Interval：ロギングが設定されている場合、ロギング間隔を秒単位で指定します。

— Time Range：このルールに定義されている時間範囲をドロップダウン リストから指定します。

...：事前に設定したリストから時間範囲を選択、追加、編集、削除、または検索できます。

**モード**

次の表に、この機能を使用できるモードを示します。

| ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|
| | | | マルチ | |
| ルーテッド | 透過 | シングル | コンテキスト | システム |
| • | • | • | • | — |

## Manage Service Groups

Manage Service Groups ダイアログボックスでは、名前付きグループにある複数の TCP、UDP、または TCP-UDP サービス（ポート）を関連付けます。以後、アクセスや、IPSec ルール、コンジットなどの ASDM および CLI 内の機能でサービス グループを使用できます。

用語の *サービス*は、既知のポート番号と「リテラル」名（ftp、telnet、smtp など）を持つ、アプリケーション レベル サービスと関連付けられた上位レイヤ プロトコルを指します。

セキュリティ アプライアンスは、次の TCP リテラル名を許可します。

bgp、chargen、cmd、daytime、discard、domain、echo、exec、finger、ftp、ftp-data、gopher、h323、hostname、http、ident、irc、klogin、kshell、lpd、nntp、pop2、pop3、pptp、smtp、sqlnet、sunrpc、tacacs、talk、telnet、time、uucp、whois、www。

サービス グループの名前は、オブジェクト グループの 4 つすべてのタイプで、一意である必要があります。たとえば、サービス グループとネットワーク グループで、同じ名前を共有することはできません。

複数のサービス グループを「グループのグループ」にネストして、単一グループとして使用できます。サービス オブジェクト グループを削除すると、使用されているすべてのサービス オブジェクト グループから削除されます。

サービス グループがアクセス ルールで使用されている場合は、削除しないでください。アクセス ルールで使用されているサービス グループを空にすることはできません。

**フィールド**

- TCP：TCP サービスまたはポート番号をオブジェクト グループに追加するには、このオプションを選択します。
- UDP：UDP サービスまたはポート番号をオブジェクト グループに追加するには、このオプションを選択します。
- TCP-UDP：TCP および UDP に共通のサービスまたはポート番号をオブジェクト グループに追加するには、このオプションを選択します。
- Service Group table：このテーブルには、各サービス オブジェクト グループの記述名を含みます。このリストのグループを変更または削除するには、グループを選択して Edit または Delete をクリックします。新しいグループをこのリストに追加するには、Add をクリックします。

### モード

次の表に、この機能を使用できるモードを示します。

| ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|
| | | | マルチ | |
| ルーテッド | 透過 | シングル | コンテキスト | システム |
| • | • | • | • | — |

## Add/Edit Service Group

Add/Edit Service Group ダイアログボックスでは、TCP および UDP サービスまたはポートのグループを管理できます。

### フィールド

- Service Group Name：サービス グループの名前を指定します。名前は、すべてのオブジェクト グループで一意である必要があります。サービス グループ名はネットワーク グループと名前を共有できません。
- Description：サービス グループの説明を指定します。
- Service：事前定義済みドロップダウン リストからサービス グループのサービスを選択できます。
- Range/Port #：サービス グループのポートの範囲を指定できます。

### モード

次の表に、この機能を使用できるモードを示します。

| ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|
| | | | マルチ | |
| ルーテッド | 透過 | シングル | コンテキスト | システム |
| • | • | • | • | — |

## Advanced Access Rule Configuration

Advanced Access Rule Configuration ダイアログボックスでは、グローバル アクセスリストのロギング 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 ACE と一致した場合、セキュリティ アプライアンスはフロー エントリを作成して、指定された時間内で受信したパケットの数を追跡します（ログ オプションを参照）。セキュリティ アプライアンスは、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、その間隔におけるヒットの合計数を示します。各間隔の終わりに、セキュリティ アプライアンスはヒット数を 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、セキュリティ アプライアンスはそのフロー エントリを削除します。

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、セキュリティ アプライアンス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のみ設定されます（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、セキュリティ アプライアンス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を作成しません。

DoS 攻撃（サービス拒絶攻撃）が開始された場合、セキュリティ アプライアンスは非常に大量の拒否フローをごく短時間のうちに作成する可能性があります。拒否フロー数を制限することにより、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します。

### 前提条件

アクセスリストのアクセス コントロール エントリ（別名ルール）に対して、さらに新しいロギング メカニズムをイネーブルにする場合にのみ、この設定が適用されます。詳細については、「Log Options」を参照してください。

### フィールド

- Maximum Deny-flows：セキュリティ アプライアンスがロギングを停止する前に許可される拒否フローの最大数で、1 とデフォルト値の間です。デフォルトは 4096 です。
- Alert Interval：拒否フローの最大数に達したことを識別するシステム ログ メッセージ（番号 106101）の間の時間（1 ～ 3600 秒）です。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 アクセスリストでユーザごとの上書き機能がイネーブルになっている場合、RADIUS サーバによって提供されるアクセスリストは、そのインターフェイス上で設定されたアクセスリスト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っている場合、RADIUS サーバによって提供されるアクセスリストは、そのインターフェイス上で設定されたアクセスリストに結合されます。インターフェイスにインバウンド アクセスリスト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。

### モード

次の表に、この機能を使用できるモードを示します。

| ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|
| | | | マルチ | |
| ルーテッド | 透過 | シングル | コンテキスト | システム |
| • | • | • | • | — |

## Log Options

Log Options ダイアログボックスでは、アクセス コントロール リストの各アクセス コントロール エントリ（別名ルール）のロギング オプションを設定できます。コンジット リストおよびアウトバウンド リストはロギングをサポートしません。グローバル ロギング オプションの設定については、「高度なアクセス ルール設定」を参照してください。

このダイアログボックスでは、旧式のロギング メカニズム（拒否されたトラフィックだけが記録される）を使用したり、新しいロギング メカニズム（許可および拒否されたトラフィックがパケットのヒット数などの追加情報と共に記録される）を使用したり、ロギングをディセーブルにしたりできます。

Log オプションをイネーブルにすると、一定量のメモリを消費します。潜在的な DoS 攻撃のリスクを制御するには、Access Rules ウィンドウの Advanced を選択して、Maximum Deny-flow 設定を実行すると役立ちます。

### フィールド

- Use default logging behavior：旧式のアクセスリスト ロギング メカニズムを使用します。セキュリティ アプライアンスは、パケットが拒否されるとシステム ログ メッセージ番号 106023 を記録します。デフォルト設定に戻すには、このオプションを選択します。

- Enable logging for the rule：新しいアクセスリスト ロギング メカニズムをイネーブルにします。セキュリティ アプライアンスは、パケットが ACE（許可または拒否のいずれか）に一致したとき、システム ログ メッセージ番号 106100 を記録します。

  パケットが ACE と一致した場合、セキュリティ アプライアンスはフロー エントリを作成して、指定された間隔で受信したパケットの数を追跡します（Logging Interval フィールドを参照）。セキュリティ アプライアンスは、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、その間隔におけるヒットの合計数を示します。各間隔の終わりに、セキュリティ アプライアンスはヒット数を 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、セキュリティ アプライアンスはそのフロー エントリを削除します。

  - Logging Level：syslog サーバに送信されるロギング メッセージのレベルをドロップダウン リストから選択します。レベルは次のように定義されています。

    Emergencies（レベル 0）：セキュリティ アプライアンスでは、このレベルは使用しません。

    Alert（レベル 1、即時対処が必要）

    Critical（レベル 2、クリティカル条件）

    Error（レベル 3、エラー条件）

    Warning（レベル 4、警告条件）

    Notification（レベル 5、正常だが顕著な条件）

    Informational（レベル 6、情報メッセージのみ）

    Debugging（レベル 7、デバッグ中のみ表示）

  - Logging Interval：セキュリティ アプライアンスがフロー統計情報を syslog に送信する前に待機する時間を秒数（1 ～ 600 秒）で設定します。この設定は、ACE と一致するパケットがない場合にフローを削除するタイムアウト値としても機能します。デフォルトは、300 秒です。

- Disable logging for the rule：ACE のすべてのロギングをディセーブルにします。

### モード

次の表に、この機能を使用できるモードを示します。

| ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|
| | | | マルチ | |
| ルーテッド | 透過 | シングル | コンテキスト | システム |
| • | • | • | • | — |