CHAPTER 9

ファイアウォールの作成

ファイアウォールは、LAN のリソースを保護するために使用されるルールのセットです。これらのルールによって、ルータに到達するパケットにフィルタをかけます。ルールで指定された条件を満たさないパケットは廃棄されます。条件を満たすパケットは、ルールが適用されているインターフェイスを通過できます。このウィザードを使用すると、一連の画面に表示される指示に従って LAN のファイアウォールを作成できます。

このウィンドウでは、作成するファイアウォールのタイプを選択します。

（注）

- Cisco Configuration Professional（Cisco CP）を使用してルータにファイアウォールを設定するには、ファイアウォール フィーチャ セットをサポートする Cisco IOS イメージがルータで使用されている必要があります。
- また、ファイアウォールを設定する前に、LAN と WAN の設定を完了する必要があります。

基本ファイアウォール

Cisco CP でデフォルト ルールを使用してファイアウォールを作成する場合にクリックします。ユース ケース シナリオとして、このタイプのファイアウォールが使用されている一般的なネットワーク設定が表示されます。

拡張ファイアウォール

Cisco CP の指示に従ってファイアウォールを設定する場合にクリックします。DMZ ネットワークを作成したり、インスペクション ルールを指定したりできます。このオプションを選択すると、ユース ケース シナリオとして、インターネット用の一般的なファイアウォール設定が表示されます。

実行する操作

目的	手順
Cisco CP で自動的にファイアウォールを作成する。	［基本ファイアウォール］をクリックする。次に、［選択したタスクを実行する］をクリックする。
DMZ ネットワークを設定しない場合、または外部インターフェイスが 1 つしか存在しない場合は、このオプションを選択できる。	Cisco CP によってルータのインターフェイスを指定するように指示される。インターフェイスを指定すると、Cisco CP のデフォルトのアクセス ルールとインスペクション ルールを使用してファイアウォールが作成される。
Cisco CP の指示に従って拡張ファイアウォールを作成する。	［拡張ファイアウォール］を選択する。次に、［選択したタスクを実行する］をクリックする。
ルータに複数の内部インターフェイスと外部インターフェイスがある場合、DMZ ネットワークを設定するときは、このオプションを選択する必要がある。	デフォルトのインスペクション ルールが表示され、そのルールをファイアウォールに使用できる。または、独自のインスペクション ルールを作成できる。Cisco CP では、ファイアウォールにデフォルトのアクセス ルールが使用される。

目的	手順
このウィザードで実行できない操作に関する情報を入手する。	次のリストからトピックを選択する。 • ファイアウォール上のアクティビティを表示する方法 • サポートされていないインターフェイス上でファイアウォールを設定する方法 • VPN を設定した後にファイアウォールを設定する方法 • 特定のトラフィックに DMZ インターフェイスの通過を許可する方法 • 新しいネットワークまたはホストからのトラフィックを許可するように既存のファイアウォールを変更する方法 • サポートされていないインターフェイスで NAT を設定する方法 • ファイアウォールに対して NAT パススルーを設定する方法 • Easy VPN コンセントレータへのトラフィックを、ファイアウォールを通過するように許可する方法 • ルールをインターフェイスに関連付ける方法 • アクセス　ルールとインターフェイスの関連付けを解除する方法 • インターフェイスに関連付けられているルールを削除する方法 • Java リストのアクセス リストを作成する方法 • ルータに送信中の IOS コマンドを表示する方法 • DMZ　ネットワークがない場合のトラフィックを許可する方法

基本ファイアウォール設定ウィザード

このオプションを選択すると、LAN はデフォルト ファイアウォールで保護されます。そのためには、次のウィンドウで内部インターフェイスと外部インターフェイスを指定する必要があります。設定を開始するには、［次へ］をクリックします。

基本ファイアウォールのインターフェイス設定

ファイアウォールが正しいインターフェイスに適用されるように、ルータのインターフェイスを指定します。

外部インターフェイス

インターネットまたは組織の WAN に接続されるルータ インターフェイスを選択します。

（注） Cisco CP へのアクセスに使用したインターフェイスを外部インターフェイスとして選択しないでください。選択すると、Cisco CP との接続が切断されます。そのインターフェイスはファイアウォールで保護されるため、ファイアウォール ウィザードの終了後は、外部インターフェイスから Cisco CP を起動できなくなります。

アウトバウンド インターフェイスからのセキュアな Cisco CP アクセスを許可チェック ボックス

ファイアウォール外部のユーザが Cisco CP を使用してルータにアクセスできるようにする場合は、このチェック ボックスを選択します。このウィザードによって、ホストの IP アドレスまたはネットワーク アドレスを指定できる画面が表示されます。ファイアウォールは、指定したアドレスへのアクセスを許可するように変更されます。ネットワーク アドレスを指定した場合、そのネットワークにあるホストすべてが、ファイアウォール経由で許可されます。

内部インターフェイス

LAN に接続する物理インターフェイスと論理インターフェイスを選択します。複数のインターフェイスを選択できます。

リモート アクセス用ファイアウォールの設定

ファイアウォールを作成すると、リモート管理者が必要とするルータへのアクセスまでブロックされてしまうことがあります。リモート管理アクセスに使用するルータ インターフェイス、およびルータ管理のために管理者が Cisco CP にログオンする起点となるホストを指定できます。ファイアウォールは、指定したホストまたはネットワークからのセキュアなリモート アクセスを許可するように変更されます。

外部インターフェイスの選択

拡張ファイアウォール ウィザードを使用する場合、ユーザが Cisco CP を起動する際に経由するインターフェイスを選択します。このフィールドは、基本ファイアウォール ウィザードには表示されません。

送信元ホスト / ネットワーク

単一ホストからのファイアウォール経由アクセスを許可する場合は、［ホスト アドレス］を選択して、ホストの IP アドレスを入力します。ネットワーク上のホストによるファイアウォール経由のアクセスを許可するには、［ネットワーク アドレス］を選択して、そのネットワークとサブネット マスクのアドレスを入力します。ホストやネットワークは、指定したインターフェイスからアクセス可能でなければなりません。［任意］を選択して、指定したインターフェイスに接続されている任意のホストからネットワークへのセキュア アクセスを許可します。

拡張ファイアウォール設定ウィザード

Cisco CP では、ルータのインターフェイスに関する情報、DMZ ネットワークを設定するかどうか、およびファイアウォールで使用するルールを指定して、インターネット ファイアウォールを作成できます。

設定を開始するには、［次へ］をクリックします。

拡張ファイアウォールのインターフェイス設定

ルータの内部 / 外部インターフェイスと DMZ ネットワークに接続するインターフェイスを指定します。

［外部］または［内部］を選択して、各インターフェイスを外部インターフェイスまたは内部インターフェイスとして指定します。外部インターフェイスは、組織の WAN またはインターネットに接続します。内部インターフェイスはローカル LAN に接続します。

アウトバウンド インターフェイスからのセキュアな Cisco CP アクセスを許可チェック ボックス

ファイアウォール外部のユーザが Cisco CP を使用してルータにアクセスできるようにする場合は、このチェック ボックスを選択します。ホストの IP アドレスまたはネットワーク アドレスを指定できる、ウィザードの画面が表示されます。ファイアウォールは、指定したアドレスへのアクセスを許可するように変更されます。ネットワーク アドレスを指定した場合、そのネットワークにあるホストすべてが、ファイアウォール経由で許可されます。

DMZ インターフェイス

DMZ ネットワークが存在する場合は、そのネットワークに接続するルータ インターフェイスを選択します。DMZ ネットワークは、外部ネットワークから送信されたトラフィックを隔離するために使用される緩衝地帯です。DMZ ネットワークがある場合は、そのネットワークに接続するインターフェイスを選択します。

拡張ファイアウォールの DMZ サービス設定

このウィンドウでは、DMZ の内部で使用可能なサービスをルータの外部インターフェイスからも使用可能にする場合に、そのサービスを指定するルール エントリを表示できます。指定されたサービス タイプのトラフィックは、外部インターフェイス経由で DMZ ネットワークに入ることを許可されます。

DMZ サービス設定

このエリアには、ルータに設定されている DMZ サービス エントリが表示されます。

開始 IP アドレス

DMZ ネットワーク内のホストを指定する範囲内の最初の IP アドレスです。

終了 IP アドレス

DMZ ネットワーク内のホストを指定する範囲内の最後の IP アドレスです。このカラムに値が表示されない場合は、［開始 IP アドレス］カラムの IP アドレスが DMZ ネットワーク内で唯一のホストに割り当てられていると考えられます。最大 254 台のホストを範囲で指定できます。

サービス タイプ

サービスのタイプです。値は、［転送制御プロトコル（TCP）］または［ユーザ データグラム プロトコル（UDP）］のどちらかになります。

サービス

Telnet、FTP などのサービス名、またはプロトコル番号です。

DMZ サービス エントリを設定するには

［追加］をクリックし、［DMZ サービス設定］ウィンドウでエントリを作成します。

DMZ サービス エントリを編集するには

サービス エントリを選択して［編集］をクリックします。次に、［DMZ サービス設定］ウィンドウでエントリを編集します。

DMZ サービス設定

このウィンドウでは、DMZ サービス エントリを作成または編集します。

ホスト IP アドレス

アドレス範囲を入力して、このエントリを適用する DMZ 内のホストを指定します。指定した TCP または UDP サービスのトラフィックは、ファイアウォールによってこれらのホストへの到達を許可されます。

開始 IP アドレス

範囲内の最初の IP アドレスを入力します。たとえば、172.20.1.1 と入力します。ネットワーク アドレス変換（NAT）が有効になっている場合は、NAT で変換されたアドレス（*内部グローバル アドレス*と呼ばれる）を入力する必要があります。

終了 IP アドレス

範囲内の最後の IP アドレスを入力します。たとえば、172.20.1.254 と入力します。NAT が有効になっている場合は、NAT で変換されたアドレスを入力する必要があります。

サービス

TCP

TCP サービスのトラフィックを許可する場合にクリックします。

UDP

UDP サービスのトラフィックを許可する場合にクリックします。

サービス

サービス名または番号を入力します。名前または番号がわからない場合は、ボタンをクリックして、表示されるリストからサービスを選択します。

アプリケーション セキュリティ設定

Cisco CP には、アプリケーション セキュリティ ポリシーがあらかじめ設定されており、ネットワークの保護に利用できます。スライダ バーを使用して目的のセキュリティ レベルを選択し、そのレベルで実現するセキュリティの説明を表示します。ウィザードの要約画面には、ポリシー名（SDM_HIGH、SDM_MEDIUM、SDM_LOW のいずれか）およびポリシーの設定ステートメントが表示されます。また、［アプリケーション セキュリティ］タブをクリックしてポリシーの名前を選択すると、ポリシーの詳細を表示することもできます。

コマンドのプレビュー ボタン

このポリシーを設定する IOS コマンドを表示する場合にクリックします。

カスタム アプリケーション セキュリティ ポリシー ボタン

このボタンと［ポリシー名］フィールドは、拡張ファイアウォール ウィザードを終了する場合に表示されます。このオプションは、独自のアプリケーション セキュリティ ポリシーを作成する場合に選択します。ポリシーがすでに存在する場合は、このフィールドに名前を入力するか、右側のボタンをクリックして［既存のポリシーを選択］を選択し、ポリシーを選択します。ポリシーを作成するには、このボタンをクリックして［新しいポリシーを作成］を選択し、表示されたダイアログでポリシーを作成します。

ドメイン ネーム サーバの設定

アプリケーション セキュリティが機能するためには、少なくとも 1 つの DNS サーバの IP アドレスをルータに設定する必要があります。［DNS ベースのホスト名からアドレスへの変換を有効にする］をクリックして、プライマリ DNS サーバを指定します。セカンダリ DNS サーバが使用可能な場合は、［セカンダリ DNS サーバ］フィールドにその IP アドレスを入力します。

ここで入力した IP アドレスは、［DNS プロパティ］ウィンドウの［追加タスク］に表示されます。

URL フィルタ サーバ設定

URL フィルタ サーバでは、ルータのコンフィギュレーション ファイルに比べて、はるかに多くの URL フィルタリング情報を格納し、管理できます。ネットワークに URL フィルタ サーバが配置されている場合は、それらのサーバを使用するようにルータを設定できます。追加の URL フィルタ サーバ パラメータを設定するには、［設定］>［セキュリティ（詳細設定）］>［URL フィルタリング］>［URL フィルタ サーバ］の順に選択します。詳細については、「URL フィルタリング」を参照してください。

URL フィルタ サーバからの HTTP リクエストをフィルタ

URL フィルタ サーバによる URL フィルタリングを有効にするには、［URL フィルタ サーバからの HTTP リクエストをフィルタ］チェック ボックスを選択します。

URL フィルタ サーバ タイプ

Cisco CP は、Secure Computing URL フィルタ サーバおよび Websense URL フィルタ サーバをサポートしています。［Secure Computing］または［Websense］のいずれかを選択して、ネットワーク上の URL フィルタ サーバのタイプを指定します。

IP アドレス / ホスト名

URL フィルタ サーバの IP アドレスまたはホスト名を入力します。

インターフェイス ゾーンの選択

このウィンドウは、設定中のルータ インターフェイス以外のルータ インターフェイスが、ゾーンベースのポリシー ファイアウォールのセキュリティ ゾーンのメンバである場合に表示されます。このトピックの詳細については、「ゾーンベースのポリシー ファイアウォール」を参照してください。

ゾーンの選択

インターフェイスをメンバにするセキュリティ ゾーンを選択します。インターフェイスをゾーンに割り当てないと、トラフィックがそのインターフェイスを通過しない可能性が高くなります。

ZPF インサイドゾーン

ジェネリック ルーティング カプセル化（GRE）トンネルに使用されるインターフェイスが含まれるゾーンは、GRE トラフィックがファイアウォールを通過するように、内部（信頼できる）ゾーンとして指定する必要があります。

このウィンドウには、設定されているゾーンとそのメンバのインターフェイスが一覧表示されます。ゾーンを内部ゾーンとして指定するには、そのゾーンの行内の［内部］カラムを選択します。

音声設定

ルータのファイアウォール ポリシーに音声トラフィックを含めるには、この画面で必要な情報を指定します。

フィールド リファレンス

表 9-1 で、この画面のフィールドについて説明します。

表 9-1　音声設定のフィールド

項目	説明
音声設定を有効にする	［音声設定を有効にする］を選択して、この画面の他のフィールドを有効にします。
インターフェイス	ルータ インターフェイスの名前（GigabitEthernet0/1 など）です。
外部	インターフェイスを使用して WAN に接続する場合は、そのインターフェイスの横にある［外部］チェック ボックスを選択します。
内部	インターフェイスを使用して LAN または他の内部ネットワークに接続する場合は、そのインターフェイスの横にある［内部］チェック ボックスを選択します。

表 9-1　音声設定のフィールド（続き）

項目	説明
回線側プロトコルを選択	回線側プロトコルは、ネットワーク上の電話機との間でトラフィックを送受信する場合に使用されるプロトコルです。次のいずれかのオプションを選択します。 • SIP — Session Initiation Protocol。 • SCCP — スキニー クライアント制御プロトコル。
トランク側プロトコルを選択	トランク側プロトコルは、インターネット上でトラフィックを送信する場合に使用されるプロトコルです。次のいずれかのオプションを選択します。 • SIP — Session Initiation Protocol。 • H.323
音声トラフィックのロギングを有効にする	音声トラフィックに関連するロギング メッセージを監視画面に表示するには、［音声トラフィックのロギングを有効にする］チェック ボックスを選択します。これらのメッセージを表示するには、Cisco CP ツールバーで［監視］をクリックし、［ファイアウォール］をクリックします。

要約

この画面には、ファイアウォール情報の要約が表示されます。この画面で情報を確認したり、［戻る］ボタンでウィザードの任意の画面に戻って設定を変更したりできます。

要約画面では、平易な言葉で設定内容が説明されています。

内部インターフェイス

このウィザード セッションで内部インターフェイスとして指定したルータの論理インターフェイスと物理インターフェイスが IP アドレスとともに表示されます。またその下に、内部インターフェイスに適用される設定ステートメントごとに、平易な言葉による説明が表示されます。その例を次に示します。

```
Inside(trusted) Interfaces:
FastEthernet0/0 (10.28.54.205)
Apply access rule to the inbound direction to deny spoofing traffic.
Apply access rule to the inbound direction to deny traffic sourced
from broadcast, local loopback address.
Apply access rule to the inbound direction to permit all other
traffic.
Apply application security policy SDM_HIGH to the inbound direction.
```

この例で示すのは、このインターフェイス上のインバウンド トラフィックに適用される Cisco CP アプリケーション セキュリティ ポリシー SDM_HIGH です。

外部インターフェイス

このウィザード セッションで外部インターフェイスとして指定したルータの論理インターフェイスと物理インターフェイスが IP アドレスとともに表示されます。またその下に、外部インターフェイスに適用される設定ステートメントごとに、平易な言葉による説明が表示されます。その例を次に示します。

```
FastEthernet0/1 (142.120.12.1)
Turn on unicast reverse path forwarding check for non-tunnel
interfaces.
Apply access rule to the inbound direction to permit IPSec tunnel
traffic if necessary.
Apply access rule to the inbound direction to permit GRE tunnel
traffic for interfaces if necessary.
Apply access rule to the inbound direction to permit ICMP traffic.
Apply access rule to the inbound direction to permit NTP traffic if
necessary.
Apply access rule to the inbound direction to deny spoofing traffic.
Apply access rule to the inbound direction to deny traffic sourced
from broadcast, local loopback and private address.
Apply access rule to the inbound direction to permit service traffic
going to DMZ interface.
Service ftp at 10.10.10.1 to 10.10.10.20
Apply access rule to the inbound direction to permit secure SDM access
from 140.44.3.0 255.255.255.0 host/network
Apply access rule to the inbound direction to deny all other traffic.
```

この設定では、逆方向パス転送機能が有効になり、検証可能な送信元 IP アドレスのないパケットをルータが破棄でき、10.10.10.1 ～ 10.10.10.20 の DMZ アドレスへの ftp トラフィックが許可されます。

DMZ インターフェイス

拡張ファイアウォールを設定している場合は、指定した DMZ インターフェイスがその IP アドレスとともに表示されます。また、このインターフェイスに関連付けられているアクセス ルールとインスペクション ルールが下に表示されます。その例を次に示します。

```
FastEthernet (10.10.10.1)
Apply CBAC inspection rule to the outbound direction
Apply access rule to the inbound direction to deny all other traffic.
```

この設定をルータの実行コンフィギュレーションに保存してウィザードを終了するには

［完了］をクリックします。設定の変更がルータの実行コンフィギュレーションに保存されます。変更はすぐに有効になりますが、ルータの電源を切ると失われます。

［ユーザ プリファレンス］ウィンドウで［コマンドをルータに配信する前にプレビューする］チェック ボックスを選択した場合は、［設定をルータに配信する］ウィンドウが表示されます。このウィンドウで、ルータに配信する CLI コマンドを確認できます。

Cisco CP 警告：Cisco CP アクセス

このウィンドウは、Cisco CP が外部インターフェイスからルータにアクセスできるように設定されている場合に表示されます。この警告では、SSH と HTTPS が設定されていること、および外部インターフェイスとして指定されている 1 つ以上のインターフェイスが静的 IP アドレスで設定されていることを確認するよう通知されます。これらの設定を確認するには、外部インターフェイスが静的 IP アドレスで設定されていることを確認してから、そのインターフェイスに管理ポリシーを関連付ける必要があります。

外部インターフェイスが静的 IP アドレスで設定されていることの確認

外部インターフェイスが静的 IP アドレスで設定されているかどうかを確認する手順は、次のとおりです。

ステップ 1　［設定］>［ルータ］>［インターフェイスと接続］>［インターフェイス / 接続の編集］の順にクリックします。

ステップ 2　［インターフェイス リスト］表の［IP］カラムで、外部インターフェイスに静的 IP アドレスが設定されているかどうかを確認します。

ステップ 3　静的 IP アドレスが設定された外部インターフェイスがない場合は、［編集］をクリックし、インターフェイスの IP アドレス情報を再設定できるダイアログを表示します。

静的 IP アドレスが設定された外部インターフェイスがある場合は、そのインターフェイスの名前をメモして、次の手順を実行します。

SSH と HTTPS の設定

ルータに SSH および HTTPS の管理ポリシーを設定する手順は、次のとおりです。

ステップ 1　［設定］>［ルータ］>［ルータ アクセス］>［管理アクセス］の順にクリックします。

ステップ 2　管理ポリシーがない場合は、［追加］をクリックします。既存の管理ポリシーを編集する場合は、そのポリシーを選択して、［編集］をクリックします。

（注）　管理ポリシーを編集する場合は、そのポリシーを、静的 IP アドレスが設定されたインターフェイスに関連付ける必要があります。

ステップ 3　表示されるダイアログの［送信元ホスト / ネットワーク］ボックスに、アドレス情報を入力します。入力する IP アドレス情報には、ルータの管理に使用する PC の IP アドレスを含める必要があります。

ステップ 4　［管理インターフェイス］ボックスで、静的 IP アドレスが設定された外部インターフェイスを選択します。このインターフェイスには、［送信元ホスト / ネットワーク］ボックスに指定した IP アドレスへのルートが設定されている必要があります。

ステップ 5　［管理プロトコル］ボックスで、［SDM を許可する］チェック ボックスを選択します。

ステップ 6　［HTTPS］および［SSH］チェック ボックスを選択して、これらのプロトコルを許可します。

ステップ 7　［OK］をクリックして、ダイアログを閉じます。

ステップ 8　管理アクセス　ポリシーが表示されているウィンドウの［変更の適用］をクリックします。

その他の手順

ここでは、ウィザードで設定できないタスクの手順を示します。

ファイアウォール上のアクティビティを表示する方法

ファイアウォール上のアクティビティは、ログ エントリの作成を通じて監視されます。ルータでロギングが有効になっている場合は、ログ エントリを生成するように設定されているアクセス ルールが呼び出されるたびに（たとえば、拒否された IP アドレスからの接続試行のたびに）ログ エントリが生成され、そのエントリを監視モードで表示できます。

ロギングを有効にする

ファイアウォールのアクティビティを表示するには、まずルータでロギングを有効にします。ロギングを有効にするには、次の手順に従ってください。

ステップ 1　機能バーで、［設定］>［ルータ］>［ロギング］の順に選択します。

ステップ 2　［編集］をクリックします。

ステップ 3　［シスログ（Syslog）］画面で［バッファへのロギング］を選択します。

ステップ 4　［バッファ サイズ］フィールドに、ロギング バッファに使用するルータのメモリ容量を入力します。デフォルト値は 4,096 バイトです。バッファ サイズが大きいほど格納されるログ エントリは多くなります。ただし、ロギング バッファを大きくする必要性とルータ パフォーマンスが低下する可能性を考慮して、両方のバランスをとる必要があります。

ステップ 5　［OK］をクリックします。

ログ エントリを生成するアクセス ルールを指定する

ロギングを有効にしたら、ログ エントリを生成するアクセス ルールを指定する必要があります。ログ エントリを生成するアクセス ルールを設定するには、次の手順に従ってください。

ステップ 1　機能バーで、［設定］>［セキュリティ］>［ACL エディタ］の順に選択します。

ステップ 2　［アクセス ルール］をクリックします。

画面の右上の表に各アクセス ルールが表示されます。右下の表には、ルールによって許可または拒否される特定の送信元 IP アドレス、宛先 IP アドレス、およびサービスが表示されます。

ステップ 3　右上の表で変更するルールを選択します。

ステップ 4　［編集］をクリックします。

［ルールの編集］ダイアログ ボックスが表示されます。

ステップ 5　［ルール エントリ］フィールドに、ルールによって許可または拒否される送信元 IP、宛先 IP、およびサービスの各組み合わせが表示されます。ログ エントリを生成するように設定するルール エントリをクリックします。

ステップ 6　［編集］をクリックします。

ステップ 7　［ルール エントリ］ダイアログ ボックスで、［このエントリに一致した場合にログ］チェック ボックスを選択します。

ステップ 8　［OK］をクリックして、表示されているダイアログ ボックスを閉じます。

これで、変更したルール エントリで定義されている IP アドレス範囲とサービスからの接続試行のたびに、ログ エントリが生成されるようになります。

ステップ 9　ログ エントリを生成するように設定する各ルール エントリに対して手順 4 ～ 8 を繰り返します。

ロギングの設定が完了したら、次の手順に従ってファイウォールのアクティビティを表示します。

ステップ 1　機能バーで、［監視］>［セキュリティ］の順に選択します。

ステップ 2　［ファイアウォール ステータス］を選択します。

［ファイアウォール統計情報］で、ファイアウォールが設定されていることを確認したり、拒否した接続試行の回数を表示したりできます。

表に、ファイアウォールによって生成された各ルータ ログ エントリが表示され、ログ エントリが生成された時間と理由が示されます。

サポートされていないインターフェイス上でファイアウォールを設定する方法

Cisco CP では、サポートされていないタイプのインターフェイスにファイアウォールを設定できます。ファイアウォールを設定する前に、まずルータ CLI を使用して、インターフェイスを設定する必要があります。インターフェイスには、少なくとも IP アドレスを設定する必要があり、また、機能していなければなりません。CLI を使用してインターフェイスを設定する方法については、ルータのソフトウェア設定ガイドを参照してください。

接続が機能していることを確認するには、［インターフェイスと接続］ウィンドウでインターフェイスのステータスが［稼働］になっていることを確認します。

次の例は、Cisco 3620 ルータにおける ISDN インターフェイスの設定の一部です。

```
!
isdn switch-type basic-5ess
!
interface BRI0/0
!  This is the data BRI WIC
 ip unnumbered Ethernet0/0
 no ip directed-broadcast
 encapsulation ppp
 no ip mroute-cache
 dialer map ip 100.100.100.100 name junky 883531601
 dialer hold-queue 10
 isdn switch-type basic-5ess
 isdn tei-negotiation first-call
 isdn twait-disable
 isdn spid1 80568541630101 6854163
 isdn incoming-voice modem
```

その他の設定については、ルータのソフトウェア設定ガイドを参照してください。

CLI を使用してサポートされていないインターフェイスを設定した後で、Cisco CP を使用してファイアウォールを設定できます。サポートされていないインターフェイスは、ルータ インターフェイスを表示するフィールドに［その他］として表示されます。

VPN を設定した後にファイアウォールを設定する方法

VPN で使用されているインターフェイスにファイアウォールを設定する場合は、ファイアウォールでローカル VPN ピアとリモート VPN ピア間のトラフィックを許可する必要があります。基本または拡張ファイアウォール ウィザードを使用すると、VPN ピア間のトラフィック フローが Cisco CP によって自動的に許可されます。

［追加タスク］から利用できる ACL エディタでアクセス ルールを作成する場合は、ユーザ自身が許可と拒否のステートメントをルールに含めるため、VPN ピア間のトラフィックを許可する必要があります。次のステートメントは、VPN トラフィックを許可するために設定に含める必要があるステートメント タイプの例です。

```
access-list 105 permit ahp host 123.3.4.5 host 192.168.0.1
access-list 105 permit esp host 123.3.4.5 host 192.168.0.1
access-list 105 permit udp host 123.3.4.5 host 192.168.0.1 eq isakmp
access-list 105 permit udp host 123.3.4.5 host 192.168.0.1 eq
non500-isakmp
```

特定のトラフィックに DMZ インターフェイスの通過を許可する方法

DMZ ネットワーク上の Web サーバへのファイアウォール経由のアクセスを設定するには、次の手順に従ってください。

ステップ 1　機能バーで、［設定］>［セキュリティ］>［ファイアウォールと ACL］の順に選択します。

ステップ 2　［拡張ファイアウォール］を選択します。

ステップ 3　［選択したタスクを実行する］をクリックします。

ステップ 4　［次へ］をクリックします。

［拡張ファイアウォールのインターフェイス設定］画面が表示されます。

ステップ 5　［インターフェイス］の表で、ファイアウォールの内部のネットワークに接続するインターフェイスとファイアウォールの外部のネットワークに接続するインターフェイスを選択します。

ステップ 6　［DMZ インターフェイス］フィールドで、DMZ ネットワークに接続するインターフェイスを選択します。

ステップ 7　［次へ >］をクリックします。

ステップ 8　［IP アドレス］フィールドに、Web サーバの IP アドレスまたは IP アドレス範囲を入力します。

ステップ 9　［サービス］フィールドから［TCP］を選択します。

ステップ 10　［ポート］フィールドに、**80** または **www** と入力します。

ステップ 11　［次へ >］をクリックします。

ステップ 12　［完了］をクリックします。

新しいネットワークまたはホストからのトラフィックを許可するように既存のファイアウォールを変更する方法

新しいネットワークまたはホストからのトラフィックを許可するようにファイアウォール設定を変更するには、［ファイアウォール ポリシーの編集］タブを使用します。

ステップ 1　機能バーで、［設定］>［セキュリティ］>［ファイアウォールと ACL］の順に選択します。

ステップ 2　［ファイアウォール ポリシーの編集］タブをクリックします。

ステップ 3　トラフィック選択パネルで送信元インターフェイスと宛先インターフェイスを選択し、ファイアウォールが適用されているトラフィック フローを指定して［実行］をクリックします。指定したトラフィック フローにファイアウォールが適用されている場合は、ルータの図にファイアウォール アイコンが表示されます。変更する必要があるアクセス ルールが指定したトラフィック フローに表示されない場合は、別の送信元インターフェイスまたは宛先インターフェイスを選択します。

ステップ 4　［サービス］エリアでアクセス ルールを確認します。［追加］ボタンをクリックして新しいアクセス ルール エントリ用のダイアログを表示します。

ステップ 5　ネットワークへのアクセスを許可するネットワークまたはホストに対して許可のステートメントを入力します。［ルール エントリ］ダイアログで［OK］をクリックします。

ステップ 6　［サービス］エリアに新しいエントリが表示されます。

ステップ 7　必要な場合は、［切り取り］および［貼り付け］ボタンを使用してリスト内のエントリを並べ替えます。

サポートされていないインターフェイスで NAT を設定する方法

Cisco CP では、サポートされていないタイプのインターフェイスにネットワークアドレス変換（NAT）を設定できます。ファイアウォールを設定する前に、まずルータ CLI を使用して、インターフェイスを設定する必要があります。インターフェイスには、少なくとも IP アドレスを設定する必要があり、また、機能していなければなりません。接続が機能していることを確認するには、インターフェイスのステータスが［稼働］になっていることを確認します。

CLI を使用してサポートされていないインターフェイスを設定した後で、NAT を設定できます。サポートされていないインターフェイスは、ルータ インターフェイスのリストに［その他］として表示されます。

ファイアウォールに対して NAT パススルーを設定する方法

NAT の設定後にファイアウォールを設定する場合は、パブリック IP アドレスからのトラフィックを許可するようにファイアウォールを設定する必要があります。そのためには、ACL を設定する必要があります。パブリック IP アドレスからのトラフィックを許可する ACL を設定するには、次の手順に従ってください。

ステップ 1　機能バーで、［設定］>［セキュリティ］>［ACL エディタ］の順に選択します。

ステップ 2　［アクセス ルール］を選択します。

ステップ 3　［追加］をクリックします。

［ルールの追加］ダイアログ ボックスが表示されます。

ステップ 4　［名前/番号］フィールドに、新しいルールの一意の名前または番号を入力します。

ステップ 5　［タイプ］フィールドから［標準ルール］を選択します。

ステップ 6　［説明］フィールドに、「NAT パススルーを許可する」などの新しいルールについての簡単な説明を入力します。

ステップ 7　［追加］をクリックします。

［標準ルール エントリの追加］ダイアログ ボックスが表示されます。

ステップ 8　［アクション］フィールドで、［許可］を選択します。

ステップ 9　［タイプ］フィールドで、［ホスト］を選択します。

ステップ 10　［IP アドレス］フィールドにパブリック IP アドレスを入力します。

ステップ 11　［説明］フィールドに、「パブリック IP アドレス」などの簡単な説明を入力します。

ステップ 12　［OK］をクリックします。

ステップ 13　［OK］をクリックします。

新しいルールが［アクセス ルール］テーブルに表示されます。

Easy VPN コンセントレータへのトラフィックを、ファイアウォールを通過するように許可する方法

VPN コンセントレータへのファイアウォール経由のトラフィックを許可するには、VPN トラフィックを許可するアクセス ルールを作成または変更する必要があります。これらのルールを作成するには、次の手順に従ってください。

ステップ 1　機能バーで、［設定］>［セキュリティ］>［ACL エディタ］の順に選択します。

ステップ 2　［アクセス ルール］を選択します。

ステップ 3　［追加］をクリックします。

［ルールの追加］ダイアログ ボックスが表示されます。

ステップ 4　［名前 / 番号］フィールドに、このルールの一意の名前または番号を入力します。

ステップ 5　［説明］フィールドに、VPN コンセントレータのトラフィック などのルールについての説明を入力します。

ステップ 6　［追加］をクリックします。

［拡張ルール エントリの追加］ダイアログ ボックスが表示されます。

ステップ 7　［送信元ホスト / ネットワーク］グループの［タイプ］フィールドで、［ネットワーク］を選択します。

ステップ 8　［IP アドレス］および［ワイルドカード マスク］フィールドに、VPN の送信元ピアの IP アドレスとネットワーク マスクを入力します。

ステップ 9　［宛先ホスト / ネットワーク］グループの［タイプ］フィールドで、［ネットワーク］を選択します。

ステップ 10　［IP アドレス］および［ワイルドカード マスク］フィールドに、VPN の宛先ピアの IP アドレスとネットワーク マスクを入力します。

ステップ 11［プロトコルとサービス］グループで［TCP］を選択します。

ステップ 12［送信元ポート］フィールドで［=］を選択し、ポート番号 **1023** を入力します。

ステップ 13［宛先ポート］フィールドで［=］を選択し、ポート番号 **1723** を入力します。

ステップ 14［OK］をクリックします。

［ルール エントリ］リストに新しいルールが表示されます。

ステップ 15 手順 7 ～ 15 を繰り返して、次のプロトコルのルール エントリを作成し、必要な場合はポート番号も入力します。

- プロトコル **IP**、IP プロトコル **GRE**
- プロトコル **UDP**、送信元ポート **500**、宛先ポート **500**
- プロトコル **IP**、IP プロトコル **ESP**
- プロトコル **UDP**、送信元ポート **10000**、宛先ポート **10000**

ステップ 16［OK］をクリックします。

ルールをインターフェイスに関連付ける方法

Cisco CP ファイアウォール ウィザードを使用する場合は、作成したアクセス ルールとインスペクション ルールは、ファイアウォールを作成したインターフェイスに自動的に関連付けられます。［追加タスク］から［ACL エディタ］を選択してルールを作成する場合は、［ルールの追加 / 編集］ウィンドウでそのルールをインターフェイスに関連付けることができます。その後でも関連付けることができます。

ステップ 1 機能バーで、［ルータ］>［インターフェイスと接続］>［インターフェイス / 接続の編集］の順にクリックします。

ステップ 2　ルールを関連付けるインターフェイスを選択して［編集］をクリックします。

ステップ 3　［関連付け］タブで、［アクセス ルール］または［インスペクション ルール］ボックス内の［インバウンド］または［アウトバウンド］フィールドにルール名または番号を入力します。インターフェイスに到達する前にルールに従ってトラフィックをフィルタするには、［インバウンド］フィールドを使用します。すでにルータに到達し、選択したインターフェイス経由でルータから出るトラフィックをフィルタするには、［アウトバウンド］フィールドを使用します。

ステップ 4　［関連付け］タブで［OK］をクリックします。

ステップ 5　［アクセス ルール］または［インスペクション ルール］ウィンドウで、［使用元］カラムを調べて、ルールがインターフェイスに関連付けられていることを確認します。

アクセス ルールとインターフェイスの関連付けを解除する方法

アクセス ルールとインターフェイスの関連付けの解除が必要になることがあります。関連付けを解除しても、アクセス ルールは削除されません。必要な場合は、ルールを別のインターフェイスに関連付けることができます。アクセス ルールとインターフェイスの関連付けを解除するには、次の手順に従ってください。

ステップ 1　機能バーで、［ルータ］>［インターフェイスと接続］>［インターフェイス / 接続の編集］の順にクリックします。

ステップ 2　アクセス ルールの関連付けを解除するインターフェイスを選択します。

ステップ 3　［編集］をクリックします。

ステップ 4　［関連付け］タブで、［アクセス ルール］ボックス内の［インバウンド］または［アウトバウンド］フィールドからアクセス ルールを探します。アクセス ルールは名前または番号で表示されます。

ステップ 5　［インバウンド］または［アウトバウンド］フィールドをクリックし、右のボタンをクリックします。

ステップ 6　［なし（ルールの関連付けを解除)］をクリックします。

ステップ 7　［OK］をクリックします。

インターフェイスに関連付けられているルールを削除する方法

Cisco CP では、インターフェイスに関連付けられているルールを削除できません。削除するには、まずルールとインターフェイスの関連付けを解除する必要があります。

ステップ 1　機能バーで、［ルータ］>［インターフェイスと接続］>［インターフェイス / 接続の編集］の順にクリックします。

ステップ 2　ルールの関連付けを解除するインターフェイスを選択します。

ステップ 3　［編集］をクリックします。

ステップ 4　［関連付け］タブで、［アクセス ルール］ボックスまたは［インスペクション ルール］ボックスからルールを探します。ルールは名前または番号で表示されます。

ステップ 5　［関連付け］タブでルールを選択します。アクセス ルールの場合は、［なし（ルールの関連付けを解除）］をクリックします。インスペクション ルールの場合は、［なし］をクリックします。

ステップ 6　［OK］をクリックします。

ステップ 7　左側のフレームで［ルール］をクリックします。［ルール］ツリーを使用して［アクセス ルール］または［インスペクション ルール］ウィンドウに移動します。

ステップ 8　削除するルールを選択して［削除］をクリックします。

Java リストのアクセス リストを作成する方法

インスペクション ルールでは、Java リストを指定できます。Java リストは、信頼できる送信元からの Java アプレット トラフィックを許可するために使用されます。これらの送信元は、Java リストが参照するアクセス ルールで定義します。この種類のアクセス ルールを作成してそれを Java リストで使用するには、次の手順に従ってください。

ステップ 1　［インスペクション ルール］ウィンドウを開いて［Java リスト］をクリックした場合は、［番号］フィールドの右側にあるボタンをクリックして［新しいルール（ACL）を作成して選択する］をクリックします。［ルールの追加］ウィンドウが表示されます。

［アクセス ルール］ウィンドウを開いている場合は、［追加］をクリックして［ルールの追加］ウィンドウを開きます。

ステップ 2　［ルールの追加］ウィンドウで、信頼できるアドレスからのトラフィックを許可する標準アクセス ルールを作成します。たとえば、ホスト 10.22.55.3 と 172.55.66.1 からの Java アプレットを許可する場合は、［ルールの追加］ウィンドウで次のアクセス ルール エントリを作成できます。

```
permit host 10.22.55.3
permit host 172.55.66.1
```

エントリの説明とルールの説明を入力できます。

インスペクション ルールを適用するインターフェイスにアクセス ルールを関連付ける必要はありません。

ステップ 3　［ルールの追加］ウィンドウで［OK］をクリックします。

ステップ 4　この手順を［インスペクション ルール］ウィンドウから開始した場合は、［Java リスト］ウィンドウで［OK］をクリックします。手順 5 と 6 を実行する必要はありません。

ステップ 5　この手順を［アクセス　ルール］ウィンドウから開始した場合は、［インスペクション ルール］ウィンドウに移動し、Java リストを作成するインスペクション ルールを選択して［編集］をクリックします。

ステップ 6　［プロトコル］カラムで［http］を選択し、［Java リスト］をクリックします。

ステップ 7　［Java リスト番号］フィールドに、作成したアクセス リストの番号を入力します。［OK］をクリックします。

DMZ ネットワークがない場合のトラフィックを許可する方法

ファイアウォール ウィザードでは、DMZ に入ることを許可するトラフィックを指定できます。DMZ ネットワークがない場合は、ファイアウォール ポリシー機能を使用して、指定したタイプの外部トラフィックがネットワークに入ることを許可できます。

ステップ 1　［設定］>［セキュリティ］>［ファイアウォールと ACL］の順に選択して、ファイアウォールを設定します。

ステップ 2　［ファイアウォール ポリシー /ACL の編集］をクリックします。

ステップ 3　変更する必要があるアクセス　ルールを表示するには、送信元インターフェイスとして外部インターフェイスを選択し、宛先インターフェイスとして内部インターフェイスを選択します。外部インターフェイス上のインバウンド トラフィックに適用されるアクセス ルールが表示されます。

ステップ 4　まだ許可されていない特定のタイプのトラフィックがネットワークに入ることを許可するには、［サービス］エリアで［追加］をクリックします。

ステップ 5　［ルール エントリ］ダイアログで必要なエントリを作成します。エントリを作成するたびに［追加］をクリックする必要があります。

ステップ 6　［サービス］エリアのエントリ リストに、作成したエントリが表示されます。