CHAPTER 35

ゾーンベースのポリシー ファイアウォール

ゾーンベースのポリシー ファイアウォール（「ゾーン ポリシー ファイアウォール」または「ZPF」）は、古いインターフェイスベースのモデルから、より柔軟性のある、より理解しやすいゾーンベースの設定モデルに、ファイアウォールを変更します。インターフェイスはゾーンに割り当てられ、インスペクション ポリシーはゾーン間を移動するトラフィックに適用されます。ゾーン間ポリシーでは、柔軟性と精度が高いため、同一のルータ インターフェイスに接続されている複数のホスト グループに複数のインスペクション ポリシーを適用できます。

ファイアウォール ポリシーは、Cisco Common Classification Policy Language（C3PL）を使用して設定されます。C3PL では、階層構造を使用して、ネットワーク プロトコルとインスペクションの適用先のホスト グループにインスペクションが定義されます。

ゾーンベースのポリシー ファイアウォールの実装の詳細については、『Zone-Based Policy Firewall Design Guide』を参照してください。このガイドは、cisco.com で提供されています。[Support] > [Select a Product] > [Cisco IOS Software] > [Cisco IOS] > [Cisco IOS Software Release 12.4 Family] > [Cisco IOS Software Releases 12.4 Mainline] > [Configure] > [Feature Guides] の順に進み、[Zone-Based Policy Firewall Design Guide] をクリックしてください。このドキュメントには、次のリンクからもアクセスできます。

http://www.cisco.com/en/US/products/ps6350/products_feature_guide09186a008072c6e3.html

設定作業の順序

ゾーンベースのポリシー ファイアウォールの設定作業は、次の順序で行います。

1. ゾーンを定義します。
2. ゾーンペアを定義します。
3. ゾーンペアを通過するときにポリシーを適用しておく必要のあるトラフィックを示すクラス マップを定義します。
4. クラス マップのトラフィックにアクションを適用するためのポリシー マップを定義します。
5. ポリシー マップをゾーンペアに適用します。
6. インターフェイスをゾーンに割り当てます。

作業の順序は重要というわけではありませんが、順番どおりに作業を終えておかないと、次の作業に進めない場合もあります。たとえば、クラス マップをポリシー マップに割り当てるには、クラス マップを設定しておく必要があります。同様に、ポリシー マップをゾーンペアに割り当てるには、ポリシーを設定しておく必要があります。別の部分の設定に依存する作業を行おうとしたときに、その部分がまだ設定されていないと、Cisco CP でその作業を行うことができなくなります。

ゾーン ウィンドウ

ゾーン、つまりセキュリティ ゾーンは、セキュリティ ポリシーを適用できるインターフェイスのグループです。1 つのゾーン内のインターフェイスはすべて、共通の機能を持つ必要があります。たとえば、ローカル LAN に接続されている 2 つのインターフェイスを 1 つのセキュリティ ゾーンに配置し、インターネットに接続されているインターフェイスを別のセキュリティ ゾーンに配置するとします。

ゾーンベースのポリシーの全般ルールによって、インターフェイスの動作とゾーンメンバのインターフェイス間トラフィックのフローを管理するルールが示されます。

このウィンドウには、各セキュリティ ゾーンの名前、それらのゾーンに含まれるインターフェイス、およびゾーンがメンバとなっている関連ゾーンペアが表示されます。1 つのゾーンが、複数のゾーンペアのメンバになっている場合があります。

新しいゾーンを作成するには［追加］をクリックします。

既存のゾーンに別のインターフェイスを選択するには、［編集］をクリックします。

ゾーンを削除するには、［削除］をクリックします。ゾーンペアのメンバとなっているゾーンを削除することはできません。

ゾーンの追加 / 編集

新しいゾーン（セキュリティ ゾーン）を追加するには、ゾーンの**名前**を入力し、ゾーンに含めるインターフェイスを選択します。［インターフェイス］リストに、選択可能なインターフェイスの名前が表示されます。物理インターフェイスは 1 つのゾーンにしか配置できないため、物理インターフェイスがすでにいずれかのゾーンに配置されている場合は、リストにはそれらの物理インターフェイスは表示されません。ダイヤラ インターフェイスや仮想テンプレート インターフェイスなどの仮想インターフェイスは複数のゾーンに配置でき、常にリストに表示されます。

（注）

- このインターフェイスを通過して流れるトラフィックは、ゾーンに関連付けられているポリシー マップによって管理されます。
- ゾーンに関連付けるインターフェイスは、サイト間の VPN、DMVPN、Easy VPN、SSL VPN、またはトラフィックがファイアウォールにブロックされる可能性のあるその他のタイプの接続に使用できます。このダイアログ ボックスでインターフェイスをゾーンに関連付ける際に、Cisco CP によってこのようなトラフィックを許可するパススルー ACL が作成されることはありません。ポリシー マップに必要なパススルーは、次の 2 つの方法で設定できます。
  - ［設定］>［セキュリティ］>［ファイアウォールと ACL］>［ファイアウォール ポリシーの編集］>［追加］>［新しいトラフィックのルール］の順に進みます。表示されるダイアログ ボックスに、送信元と宛先の IP アドレス情報を入力し、ファイアウォールの通過を許可する必要のあるトラフィックを入力します。［アクション］フィールドで、［ACL の許可］を選択します。
  - ［設定］>［セキュリティ］>［セキュリティ（詳細設定）］>［C3PL］>［ポリシー マップ］>［プロトコル インスペクション］の順に進みます。必要なトラフィックがファイアウォールを通過するのを許可するプロトコル インスペクション ポリシー マップを指定します。

ゾーンの作成後、そのゾーンに関連付けられているインターフェイスを変更できますが、ゾーンの名前を変更することはできません。

ゾーンベースのポリシーの全般ルール

ゾーン内のルータ ネットワーク インターフェイスのメンバシップは、ゾーン メンバのインターフェイス間を移動するトラフィックと同様に、インターフェイスの動作を管理するいくつかのルールに従います。

- ゾーンにインターフェイスを割り当てるには、そのゾーンを設定しておく必要があります。
- 1 つのインターフェイスを 1 つのセキュリティ ゾーンだけに割り当てることができます。

- 指定されたインターフェイスを通過するトラフィックは、そのインターフェイスがゾーンに割り当てられると、同一ゾーン内の他のインターフェイスを通過するトラフィックとルータ上のインターフェイスを通過するトラフィックを除き、すべて暗黙的にブロックされます。
- デフォルトでは、同一ゾーンのメンバとなっているインターフェイス間のトラフィックのフローが、暗黙的に許可されます。
- ゾーン メンバのインターフェイスを通過するトラフィックを許可するには、そのゾーンとそれ以外のゾーン間でトラフィックを許可または検査するポリシーを設定する必要があります。
- 自ゾーンは、すべてのトラフィックを拒否するデフォルトのポリシーの唯一の例外です。ルータ インターフェイスへのトラフィックはすべて、そのトラフィックが明示的に拒否されるまで許可されます。
- ゾーン メンバのインターフェイスとゾーン メンバではないインターフェイスとの間をトラフィックが流れることはできません。
- 通過、検査、および廃棄のアクションは、2 つのゾーン間だけに適用できます。
- ゾーンに割り当てられていないインターフェイスは、従来のルータ　ポートとして機能します。また、このようなインターフェイスでは、従来のステートフル インスペクションまたは CBAC 設定が引き続き使用される場合があります。
- ボックスのインターフェイスがゾーニング　ポリシーまたはファイアウォール ポリシーに属さないようにする必要がある場合でも、このインターフェイスをゾーンに配置し、配置先のゾーンとトラフィックが流れるようにしたいその他のゾーンとの間にすべてのトラフィックの通過を許可するポリシー（ダミー ポリシーのようなもの）を設定する必要があることがあります。
- 上記のことから、トラフィックがルータ内のすべてのインターフェイス間を流れる場合は、すべてのインターフェイスがそのゾーニング モデルに属さなければならないことになります（各インターフェイスがいずれかのゾーンのメンバである必要があります）。
- 上記のデフォルトのトラフィック拒否における唯一の例外は、ルータを通過するトラフィックであり、それらのトラフィックはデフォルトで許可されます。また、明示的にポリシーを設定すれば、そうしたトラフィックを制限することもできます。

このルール セットは、次のリンク先で参照可能な『The Zone-Based Policy Firewall Design Guide』から採用しました。

http://www.cisco.com/en/US/products/ps6350/products_feature_guide09186a008072c6e3.html

ゾーンペア

ゾーンペアでは、2 つのセキュリティ ゾーン間に単方向のファイアウォール ポリシーを指定できます。送信元と宛先のセキュリティ ゾーンを指定することによって、トラフィックの方向を指定します。同一のゾーンを送信元と宛先の両方として定義することはできません。

2 つのゾーン間をトラフィックが双方向に流れるようにするには、方向ごとにゾーンペアを作成する必要があります。すべてのインターフェイス間をトラフィックが自由に流れるようにするには、ゾーン内の各インターフェイスを設定する必要があります。

次の表は、4 つのゾーンペアの例を示しています。

ゾーンペア	送信元	宛先	ポリシー
LAN-out	zone-VLAN1	zone-FE1	inspection-policymap-a
LAN-in	zone-FE1	zone-VLAN1	inspection-policymap-b
Bkup-out	自	zone-BRI0	inspection-policymap-c
Bkup-in	zone-BRI0	自	inspection-policymap-c

LAN-out および LAN-in は、LAN インターフェイスの VLAN1 と FastEthernet 1 インターフェイスとの間を流れるトラフィックに設定されたゾーンペアです。各ゾーンペアは、個別のポリシーによって制御されます。Bkup-out および Bkup-in は、ルータによって生成されるトラフィックに設定されています。自ゾーンとして表されるルータから送信されるトラフィックと同じポリシーによって、zone-BRI0 から送信されるトラフィックが制御されます。

ゾーンペアを作成するには［追加］をクリックします。

ゾーンペアに関連付けられているポリシーを変更するには、［編集］をクリックします。

ゾーンペアを削除するには、［削除］をクリックします。

ゾーンペアの追加 / 編集

新しいゾーンペアを設定するには、ゾーンペアの名前、トラフィックの**送信元ゾーン**、トラフィックの**宛先ゾーン**、およびこれらのゾーン間で送信が可能なトラフィックを定義する**ポリシー**を指定します。**送信元ゾーン**と**宛先ゾーン**のリストには、ルータで設定されているゾーンと**自**ゾーンが示されます。自ゾーンは、SNMP トラフィックに設定されるゾーンペアのように、ルータ自体が送信元または宛先となっているトラフィックにゾーンペアを設定するときに使用します。［ポリシー］リストには、ルータに設定されている各ポリシー マップの名前が示されます。

ゾーンペアを編集する場合は、ポリシー マップを変更することはできますが、ゾーンペアの名前、送信元ゾーン、または宛先ゾーンは変更できません。

ゾーンの追加

［インターフェイス / 接続の編集］ダイアログ ボックスの［関連付け］タブで、インターフェイスをセキュリティ ゾーンのメンバとして設定できます。追加するゾーンには、ゾーン メンバとして編集するインターフェイスが含まれます。

（注）

- このインターフェイスを通過して流れるトラフィックは、ゾーンに関連付けられているポリシー マップによって管理されます。
- ゾーンに関連付けるインターフェイスは、サイト間の VPN、DMVPN、Easy VPN、SSL VPN、またはトラフィックがファイアウォールにブロックされる可能性のあるその他のタイプの接続に使用できます。このダイアログ ボックスでインターフェイスをゾーンに関連付ける際に、Cisco CP によってこのようなトラフィックを許可するパススルー ACL が作成されることはありません。ポリシー マップに必要なパススルーは、次の 2 つの方法で設定できます。
  - ［設定］>［セキュリティ］>［ファイアウォールと ACL］>［ファイアウォール ポリシーの編集］>［追加］>［新しいトラフィックのルール］の順に進みます。表示されるダイアログ ボックスに、送信元と宛先の IP アドレス情報を入力し、ファイアウォールの通過を許可する必要のあるトラフィックを入力します。［アクション］フィールドで、［ACL の許可］を選択します。

- ［設定］>［セキュリティ］>［セキュリティ（詳細設定）］>［C3PL］>［ポリシー マップ］>［プロトコル インスペクション］の順に進みます。必要なトラフィックがファイアウォールを通過するのを許可するプロトコル インスペクション ポリシー マップを指定します。

ゾーン名

追加するゾーンの名前を入力します。

ゾーンの選択

ルータ上にセキュリティ ゾーンが設定されている場合は、そのゾーンのメンバとして設定するインターフェイスを追加できます。

インターフェイスのゾーンの選択

インターフェイスを追加するゾーンを選択して、［OK］をクリックします。