
# 簡易ファイアウォール

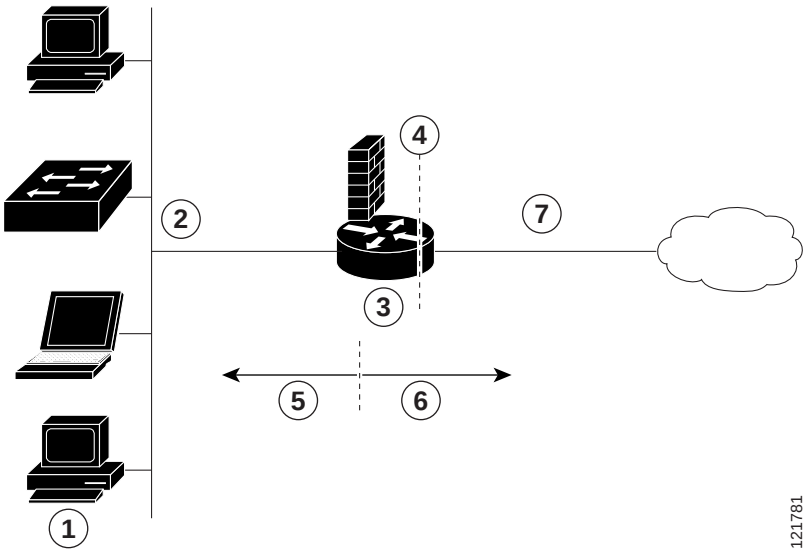
Cisco 1800 サービス統合型ルータは、アクセス リストによるネットワーク トラフィックのフィルタリングをサポートしています。また、Context-Based Access Control（CBAC; コンテキストベースのアクセス制御）によるパケット インスペクションおよび一時的なダイナミック アクセス リストについてもサポートしています。

基本的なトラフィック フィルタリングは、設定されたアクセス リストの実装に制限されます。つまり、パケットは、ネットワーク層、または最大でもトランスポート層で検証されて、ファイアウォールの通過が許可または拒否されます。ただし、CBAC でインスペクション ルールを使用することによって、一時的なダイナミック アクセス リストの作成および使用が可能になります。このダイナミック リストは、設定されたアクセス リストの一時的な開口部をファイアウォール インターフェイスで許可します。これらの開口部は、指定したユーザ セッションのトラフィックがファイアウォールを介して内部ネットワークから出るときに作成されます。開口部によって、指定したセッション（通常、ブロックされるセッション）に対するトラフィックをファイアウォールを介して戻すことが可能になります。

トラフィック フィルタリングおよびファイアウォールの詳細については『*Cisco IOS Security Configuration Guide, Release 12.3*』を参照してください。

図 8-1 は、NAT による PPPoE または PPPoA およびファイアウォールを使用したネットワーク導入を示します。

**図 8-1　　ファイアウォールが設定されたルータ**



| | |
|---|---|
| 1 | 複数のネットワーク デバイス：デスクトップ、ラップトップ PC、スイッチ |
| 2 | ファスト イーサネット LAN インターフェイス（NAT 用の内部インターフェイス） |
| 3 | PPPoE または PPPoA クライアントおよびファイアウォール実装：それぞれ Cisco 1811/1812J または Cisco 1801/1802/1803 シリーズサービス統合型ルータ |
| 4 | NAT が実行されるポイント |
| 5 | 保護されたネットワーク |
| 6 | 保護されていないネットワーク |
| 7 | ファスト イーサネットまたは ATM WAN インターフェイス（NAT 用の外部インターフェイス） |

この後の設定例では、Cisco 1811 または Cisco 1812J 上の外部 WAN インターフェイス（FE0）にファイアウォールを適用し、ファスト イーサネット WAN インターフェイス FE1 でルータに入るすべてのトラフィックにフィルタリングとインスペクションを行って、FE2 のファスト イーサネット LAN を保護します。この例では、企業ネットワークから発信されるネットワーク トラフィック（ネットワーク アドレスは 10.1.1.0）は、安全なトラフィックと見なされ、フィルタリングされません。

### 設定作業

次の作業を実行して、このネットワーク シナリオを設定します。

- 「アクセス リストの設定」
- 「インスペクション ルールの設定」
- 「インターフェイスへのアクセス リストおよびインスペクション ルールの適用」

各設定作業の結果を示す例は、「設定例」に示されています。

（注）　この章の手順では、基本的なルータ機能と、NAT を使用した PPPoE または PPPoA がすでに設定されていることを前提とします。これらの設定作業を行っていない場合は、ご使用のルータに応じて第 1 章「ルータの基本設定」、第 3 章「PPP over Ethernet と NAT の設定」、および第 4 章「PPP over ATM と NAT の設定」を参照してください。DHCP、VLAN、およびセキュアなトンネルが設定されていることもあります。

# アクセス リストの設定

ファイアウォールで使用するアクセス リストを作成するには、グローバル コンフィギュレーション モードから始め、次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **access-list** *access-list-number* {**deny** \| **permit**} *protocol source source-wildcard* [**operator** [*port*]] *destination*<br><br>**例：**<br>`Router(config)# access-list 103 permit host 200.1.1.1 eq isakmp any`<br>`Router(config)#` | インターネットから発信されたトラフィックがルータのローカル（内部）ネットワークに到達しないように、送信元および宛先ポートを比較するアクセス リストを作成します。<br><br>このコマンドの詳細については、『*Cisco IOS IP Command Reference, Volume 1 of 4: Addressing and Services*』を参照してください。 |
| ステップ 2 | **access-list** *access-list-number* {**deny** \| **permit**} *protocol source source-wildcard destination destination-wildcard*<br><br>**例：**<br>`Router(config)# access-list 105 permit ip 10.1.1.0 0.0.0.255 192.168.0.0 0.0.255.255`<br>`Router(config)#` | 設定された VPN トンネルを介してネットワーク トラフィックが企業ネットワークとローカル ネットワーク間を自由に行き来できるようにアクセス リストを作成します。 |

# インスペクション ルールの設定

TCP および UDP のすべてのトラフィックにファイアウォール インスペクション ルールを設定し、セキュリティ ポリシーによって定義されている特定のアプリケーション プロトコルを設定するには、グローバル コンフィギュレーション モードから始め、次の手順を実行します。

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **ip inspect name** *inspection-name protocol*<br><br>**例：**<br>`Router(config)# ip inspect name firewall tcp`<br>`Router(config)#` | 特定のプロトコルのインスペクション ルールを定義します。 |
| ステップ 2 | **ip inspect name** *inspection-name protocol*<br><br>**例：**<br>`Router(config)# ip inspect name firewall rtsp`<br>`Router(config)# ip inspect name firewall h323`<br>`Router(config)# ip inspect name firewall netshow`<br>`Router(config)# ip inspect name firewall ftp`<br>`Router(config)# ip inspect name firewall sqlnet`<br>`Router(config)#` | 使用する各インスペクション ルールに対して、このコマンドを繰り返します。 |

# インターフェイスへのアクセス リストおよびインスペクション ルールの適用

ネットワーク インターフェイスに ACL およびインスペクション ルールを適用するには、グローバル コンフィギュレーション モードから始め、次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **interface** *type number*<br><br>**例：**<br>`Router(config)# interface vlan 1`<br>`Router(config-if)#` | ルータの内部ネットワーク インターフェイスのインターフェイス コンフィギュレーション モードを開始します。 |
| ステップ 2 | **ip inspect** *inspection-name* {***in*** \| ***out***}<br><br>**例：**<br>`Router(config-if)# ip inspect firewall in`<br>`Router(config-if)#` | ルータの内部インターフェイスにファイアウォール インスペクション ルールのセットを割り当てます。 |

| | コマンド | 目的 |
|---|---|---|
| ステップ 3 | **exit**<br><br>**例：**<br>`Router(config-if)# exit`<br>`Router(config)#` | グローバル コンフィギュレーション モードに戻ります。 |
| ステップ 4 | **interface** *type number*<br><br>**例：**<br>`Router(config)# interface fastethernet 0`<br>`Router(config-if)#` | ルータの外部ネットワーク インターフェイスのインターフェイス コンフィギュレーション モードを開始します。 |
| ステップ 5 | **ip access-group** {*access-list-number* \| *access-list-name*} {**in** \| **out**}<br><br>**例：**<br>`Router(config-if)# ip access-group 103 in`<br>`Router(config-if)#` | 定義した ACL をルータの外部インターフェイスに割り当てます。 |
| ステップ 6 | **exit**<br><br>**例：**<br>`Router(config-if)# exit`<br>`Router(config)#` | グローバル コンフィギュレーション モードに戻ります。 |

# 設定例

在宅勤務者は、IPSec トンネリングを使用して、企業ネットワークに安全にアクセスできます。ネットワークへのセキュリティは、ファイアウォール インスペクションによって実現されます。許可されているプロトコルは、TCP、UDP、RTSP、H.323、NetShow、FTP および SQLNet のすべてです。ホーム ネットワークにはサーバがないため、外部から発信されるトラフィックは許可されません。IPSec トンネリングは、ホーム LAN から企業ネットワークへの接続を保護します。

Java ブロッキングが必要ないため、インターネット ファイアウォール ポリシーと同様に、HTTP を指定する必要がありません。Telnet や HTTP などのシングルチャネル プロトコルに、TCP インスペクションを指定できます。UDP は、DNS に対して指定されます。

次の設定例は、これまでの項で説明してきた簡易ファイアウォール シナリオのコンフィギュレーション ファイルの一部を示します。

```
! Firewall inspection is setup for all tcp and udp traffic as well as specific application
protocols as defined by the security policy.
ip inspect name firewall tcp
ip inspect name firewall udp
ip inspect name firewall rtsp
ip inspect name firewall h323
ip inspect name firewall netshow
ip inspect name firewall ftp
ip inspect name firewall sqlnet
!
interface vlan 1! This is the internal home network
ip inspect firewall in ! inspection examines outbound traffic
```

```
    no cdp enable
!
interface fastethernet 0! FE0 is the outside or internet exposed interface.
ip access-group 103 in ! acl 103 permits ipsec traffic from the corp. router as well as
denies internet initiated traffic inbound.
    ip nat outside
    no cdp enable
!
! acl 103 defines traffic allowed from the peer for the ipsec tunnel.
access-list 103 permit udp host 200.1.1.1 any eq isakmp
access-list 103 permit udp host 200.1.1.1 eq isakmp any
access-list 103 permit esp host 200.1.1.1 any
access-list 103 permit icmp any any ! allow icmp for debugging but should be disabled due
to security implications.
access-list 103 deny ip any any ! prevents internet initiated traffic inbound.
no cdp run
!
```