CHAPTER 5

ファイアウォール ロード バランシングの設定

この章では、CSS の Firewall Load Balancing （FWLB; ファイアウォール ロード バランシング）機能の設定方法について説明します。この章の記載情報は、特に指示がない限り、CSS の全モデルに共通です。

この章の主な内容は次のとおりです。

- FWLB の概要
- FWLB の設定
- VIP および仮想インターフェイスの冗長設定と FWLB の設定
- ファイアウォール フローの要約の表示
- ファイアウォール IP ルートの表示
- ファイアウォール IP 情報の表示

FWLB の概要

ファイアウォール ロード バランシング（FWLB）機能を使用すると、1 台の CSS に対して最高 15 個までのファイアウォールを設定することができます。複数のファイアウォールを設定することにより、ファイアウォールの性能が向上し、すべてのトラフィックが単一のファイアウォールだけを通過する場合に発生するシングル ポイント障害を防止できます。FWLB 機能により、CSS は、同じ送信元 IP アドレスと宛先 IP アドレスを持つパケットをすべて必ず同じファイアウォール経由で転送します。この処理は、CSS が送信元 IP アドレスと宛先 IP アドレスに XOR を実行することにより実現されます。

CSS は、ファイアウォールのどちら側にも設置できるため、トラフィックを複数のファイアウォール経由で同時にバランシング処理することができます。各ファイアウォールは、ファイアウォールのロード バランシング アルゴリズムで使用可能です。CSS は、このアルゴリズムで送信元 IP アドレスと宛先 IP アドレスを使用し、各フローに対してどのファイアウォールを使用するかを計算します。

CSS は、ファイアウォールの反対側にあるリモート CSS にカスタムの ICMP キープアライブ要求を毎秒送信して、ファイアウォールの状態を監視します。リモート CSS からキープアライブ要求が 3 ～ 16 秒間（タイムアウト時間は設定可能）届かない場合、CSS はファイアウォール パスが使用不能であると宣言します。各 CSS は、送信側の CSS に応答せず、他の CSS とは全く関係なく独自のキープアライブ要求を毎秒送信します。キープアライブ タイムアウト設定の詳細については、「ファイアウォールのキープアライブ タイムアウトの設定」を参照してください。

FWLB はレイヤ 3 デバイスとして動作します。ファイアウォールへの各接続は、独立した IP サブネットです。1 組の IP アドレス間にあるすべてのフローは、双方向とも同じファイアウォールを通過します。FWLB はルーティング機能を実行します。FWLB の決定にはコンテンツ ルールは適用されません。

（注） ファイアウォールでは、Network Address Translation（NAT; ネットワーク アドレス変換）を実行することはできません。NAT の設定が必要な場合は、CSS で、この機能を使用するためのコンテンツ ルールまたはソース グループを設定してください。

FWLB を設定するには、ローカルおよびリモートの CSS 上で、ファイアウォールを通過する各パスに対して次のパラメータを定義する必要があります。

- ファイアウォール インデックス（物理的なファイアウォールを特定）、ローカル ファイアウォールの IP アドレス、リモート ファイア ウォールの IP アドレス、および CSS VLAN の IP アドレス
- CSS が各ファイアウォールに対して使用するスタティック ルート

FWLB の設定に関しては、以降の項を参照してください。

ファイアウォールの同期

Check Point™ FireWall-1® などの、ステートフル インスペクション機能が搭載されたファイアウォール ソリューションでは、デバイスを経由するすべての接続（UDP や RPC などのステートレスなプロトコルを含む）に対して仮想状態が作成、維持されます。NAT についての詳細などのステート情報は、転送されたデータに応じて更新されます。これにより、異なるコンピュータ上で実行されている複数のファイアウォール モジュール（1 つの FWLB 環境内にある複数のモジュールなど）間で、接続に関するステート情報が相互に更新されて、情報の共有が可能になります。

ファイアウォールの同期（図 5-1 参照）には大きな利点があり、この機能によってファイアウォールの各デバイスは、ファイアウォール ロード バランシング環境にあるすべての接続を認識し、一部のファイアウォールに障害が発生した場合でも、ユーザに透過的にただちに障害から回復します。

（注） ファイアウォールの同期を設定する場合、詳細はそのファイアウォール製品のマニュアルを参照してください。FireWall-1 デバイスの設定の詳細については、『*Check Point Software FireWall-1 Architecture and Administration* guide』の「Active Network Management」の章を参照してください。

FWLB の設定

CSS は、ファイアウォールの両側に設置して、各フローに対して使用するファイアウォールの管理を行う必要があります。ファイアウォールの設定では、ローカルおよびリモートの各 CSS に同じファイアウォール インデックス番号を設定する必要があります。

パケット漏れを防止するため、CSS では、1 組の IP アドレスの間に存在するパケットをすべて同じファイアウォールに送出します。これは、どちらの方向で送信されるパケットに対しても適用されます。あるパス上で障害が発生した場合、すべてのトラフィックは、残りのパスが 1 つの場合はそのパスを使用し、残りのパスが複数の場合は、それらのパスに分散されます。

（注） ファイアウォールのインデックスは、ファイアウォール ルートを指定する前に定義する必要があります。インデックスを定義しない場合、エラー メッセージが返されます。ルートの設定方法は、**ip route... firewall** コマンドの記述を参照してください。

ファイアウォールのパラメータは、ローカルおよびリモートの CSS で、ファイアウォールを通過するパスそれぞれに対して定義する必要があります。ファイアウォールのパラメータを定義するには、**ip firewall** コマンドを使用します。

このグローバル設定モードのコマンドのシンタックスは次のとおりです。

ip firewall *index local_firewall_IP_address remote_firewall_IP_address remote_switch_IP_address*

変数の内容は次のとおりです。

（注） すべての IP アドレスはドット付き 10 進表記（たとえば、192.168.11.1）で入力します。

- *index*：ファイアウォールを識別するためのインデックス番号。1 ～ 254 の数値を入力します。

- *local_firewall_IP_address* ：CSS に接続されたサブネット上にあるファイアウォールの IP アドレス
- *remote_firewall_IP_address* ：リモートの CSS に接続されたリモート サブネット上にあるファイアウォールの IP アドレス
- *remote_switch_IP_address* ：リモートの CSS の IP アドレス

たとえば、次のように入力します。

```
(config)# ip firewall 1 192.168.27.1 192.168.28.1 192.168.28.3
```

ファイアウォールのインデックスを削除するには、次のコマンドを入力します。

```
(config)# no ip firewall 1
```

注意　ファイアウォールのインデックスを削除すると、そのインデックスに関連するルートもすべて削除されます。

ファイアウォールのキープアライブ タイムアウトの設定

CSS は、ファイアウォールの反対側にあるリモート CSS にカスタムの ICMP キープアライブ要求を毎秒送信します。ファイアウォール構成のエンドポイントにある 2 台の CSS スイッチでは、ファイアウォール キープアライブのタイムアウト値に同じ値を使用する必要があります。同じ値を設定しないと、一方の CSS 上のルートがもう一方の CSS 上のルートと同時にフェールオーバーせず、そのファイアウォールをはさんで非対称のルーティングが起こる可能性があります。

CSS がリモート CSS からのキープアライブ メッセージを待機した結果、ファイアウォールが到達不可能であると宣言するまでの時間を、秒数で指定するには、**ip firewall timeout** *number* コマンドを使用します。タイムアウトの範囲は 3 ～ 16 秒です。デフォルトは 3 秒です。

（注）　ファイアウォール パスが利用できるようになるまでに必要な時間は、このコマンドの影響を受けず 3 秒のままです。

たとえば、タイムアウトを 16 に設定するには、次のように入力します。

```
(config)# ip firewall timeout 16
```

タイムアウトをデフォルトの 3 秒にリセットするには、次のように入力します。

```
(config)# no ip firewall timeout
```

ファイアウォール用 IP スタティック ルートの設定

ファイアウォールに使用するスタティック ルートを設定するには、**ip route... firewall** コマンドを使用します。また、オプションで、この IP ルートに対して管理上の距離を設定することもできます。

（注） ファイアウォールのインデックスは、ファイアウォールのスタティック ルートを指定する前に定義する必要があります。インデックスを定義しない場合、エラー メッセージが返されます。ファイアウォールのインデックスの設定方法は、**ip firewall** コマンドの記述を参照してください。

このコマンドのシンタックスは次のとおりです。

ip route *ip_address subnet_mask* **firewall** *index distance*

変数の内容は次のとおりです。

- *ip_address* ：宛先のネットワーク アドレス。IP アドレスは、ドット付き 10 進表記（192.168.11.1 など）で入力します。
- *subnet_mask* ：IP サブネット マスク。マスクは次のいずれかの形式で入力します。
  - CIDR ビット数表記（たとえば、/24）。IP アドレスとプレフィクス長との間にはスペースを入力しないでください。
  - ドット付き 10 進表記（たとえば、255.255.255.0）
- *index* ：ファイアウォール ルートの既存のインデックス番号。ファイアウォール インデックスの設定方法については、**ip firewall** コマンドの項を参照してください。

- *distance* ：（オプション）管理上の距離。1 ～ 254 の整数を入力します。できるだけ小さい数値を指定します。デフォルト値は 1 です。

（注） CLI では、宛先アドレスと管理コストが同じ IP スタティック ルートで、ファイアウォール ルートであるものとそれ以外のものを同時に設定できません。ファイアウォール ルートとファイアウォール以外のルートの、コストかアドレスのいずれかを変更する必要があります。

たとえば、次のように入力します。

```
(config)# ip route 192.168.2.0/24 firewall 1 2
```

ファイヤウォールのルートを削除するには、次のように入力します。

```
(config)# no ip route 192.168.2.0/24 firewall 1
```

ファイアウォール ルートをアドバタイズするための OSPF の設定

他のプロトコルからのファイアウォール ルートを OSPF でアドバタイズするには、**ospf redistribute firewall** コマンドを使用します。これらのルートは、再配布すると OSPF 外部ルートになります。

任意で、次の処理を行えます。

- **metric** オプションを使用して、ルートのネットワーク コストを定義します。1 ～ 16,777,215 の範囲内の数値を指定します。デフォルトは 1 です。
- **tag** オプションを使用して、各外部ルートをアドバタイズするための 32 ビット タグ値を定義します。この値は、autonomous system boundary router（ASBR; 自律システム境界ルータ）間で情報を交換するために使用できます。
- **type1** オプションを指定して、ルートを ASE タイプ 1 としてアドバタイズします。デフォルトは、ASE タイプ 2 です。タイプ 1 とタイプ 2 ではコストの計算方法が異なります。タイプ 2 の ASE では、同一の宛先への複数のパスを比較する際に外部コスト（メトリック）だけが考慮されます。タイプ 1 の ASE では、外部コストと ASBR へ到達するためのコストが組み合わされます。

たとえば、次のように入力します。

```
(config)# ospf redistribute firewall metric 3 type1
```

ファイアウォール ルートのアドバタイジングを中止するには、次のコマンドを入力します。

```
(config)# no ospf redistribute firewall
```

ファイアウォール ルートをアドバタイズするための RIP の設定

他のプロトコルからのファイアウォール ルートを RIP でアドバタイズするには、**rip redistribute firewall** コマンドを使用します。また、このルートをアドバタイズする際に CSS が使用するオプションのメトリックを追加することもできます。1 ～ 15 の値を入力します。デフォルトは 1 です。

たとえば、RIP を使用してファイアウォール ルートをアドバタイズするには、次のように入力します。

```
(config)# rip redistribute firewall 3
```

（注） RIP は、デフォルトで RIP ルートと、RIP を実行するインターフェイスのローカル ルートをアドバタイズします。このコマンドは他のルートもアドバタイズします。

ファイアウォール ルートのアドバタイジングを中止するには、次のコマンドを入力します。

```
(config)# no rip redistribute firewall
```

FWLB スタテック ルート設定の例

ここでは、2 台の CSS 間に 2 つのファイアウォールを設置する構成で FWLB を設定する方法について説明します。FWLB のスタティック ルートを設定するには、ローカル（クライアント側）およびリモート（サーバ側）の両方の CSS 上で、ファイアウォールを経由する各パスに対して次のパラメータを定義する必要があります。

- ファイアウォール インデックス（物理的なファイアウォールを特定）、ローカル ファイアウォールの IP アドレス、リモート ファイアウォールの IP アドレス、および CSS VLAN の IP アドレス。スタティック ルートを設定する前に、**ip firewall** コマンドを設定する必要があります。設定しない場合、エラー メッセージが返されます。
- CSS が各ファイアウォールに対して使用するスタティック ルート

図 5-1 の CSS-A （ネットワークのクライアント側に設置）を設定するには、次の手順を実行します。

1. **ip firewall** コマンドを使用して、ファイアウォール 1 を定義します。たとえば、次のように入力します。

   ```
   (config)# ip firewall 1 192.168.28.1 192.168.27.1 192.168.27.3
   ```

2. **ip route** コマンドを使用して、ファイアウォール 1 のスタティック ルートを定義します。たとえば、次のように入力します。

   ```
   (config)# ip route 192.168.2.0/24 firewall 1
   ```

3. **ip firewall** コマンドを使用して、ファイアウォール 2 を定義します。たとえば、次のように入力します。

   ```
   (config)# ip firewall 2 192.168.28.2 192.168.27.2 192.168.27.3
   ```

4. **ip route** コマンドを使用して、ファイアウォール 2 のスタティック ルートを定義します。たとえば、次のように入力します。

   ```
   (config)# ip route 192.168.2.0/24 firewall 2
   ```

図 5-1 の CSS-B（ネットワークのサーバ側に設置）を設定するには、次の手順を実行します。

1. **ip firewall** コマンドを使用して、ファイアウォール 1 を定義します。たとえば、次のように入力します。

   ```
   (config)# ip firewall 1 192.168.27.1 192.168.28.1 192.168.28.3
   ```

2. **ip route** コマンドを使用して、ファイアウォール 1 のスタティック ルートを定義します。たとえば、次のように入力します。

   ```
   (config)# ip route 0.0.0.0/0 firewall 1
   ```

3. **ip firewall** コマンドを使用して、ファイアウォール 2 を定義します。たとえば、次のように入力します。

   ```
   (config)# ip firewall 2 192.168.27.2 192.168.28.2 192.168.28.3
   ```

4. **ip route** コマンドを使用して、ファイアウォール 2 のスタティック ルートを定義します。たとえば、次のように入力します。

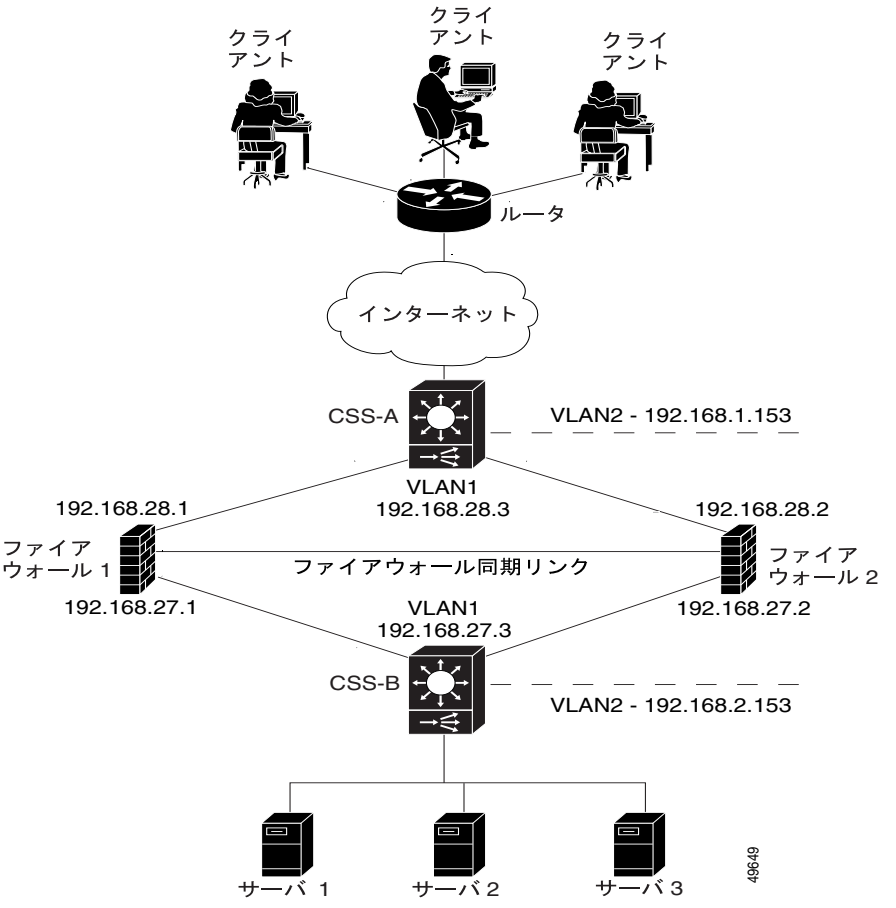
   ```
   (config)# ip route 0.0.0.0/0 firewall 2
   ```

ファイアウォールの設定は、実行設定の IP 部分に表示されます。たとえば、次のように入力します。

```
(config)# show running-config
```

図 5-1 に、上記のファイアウォール コマンドで定義した構成を示します。

図 5-1　FWLB の例



VIP および仮想インターフェイスの冗長設定と FWLB の設定

FWLB の設定時に、VIP および仮想インターフェイスの冗長設定を行うと、次のような利点があります。

- フェールオーバーの高速化（通常 1 ～ 3 秒）
- シングル ポイント障害の回避
- すべての CSS がトラフィックを転送（アクティブ / バックアップ設定）

（注）　VIP および仮想インターフェイスの冗長設定の詳細については、『*Cisco Content Services Switch Redundancy Configuration Guide*』を参照してください。

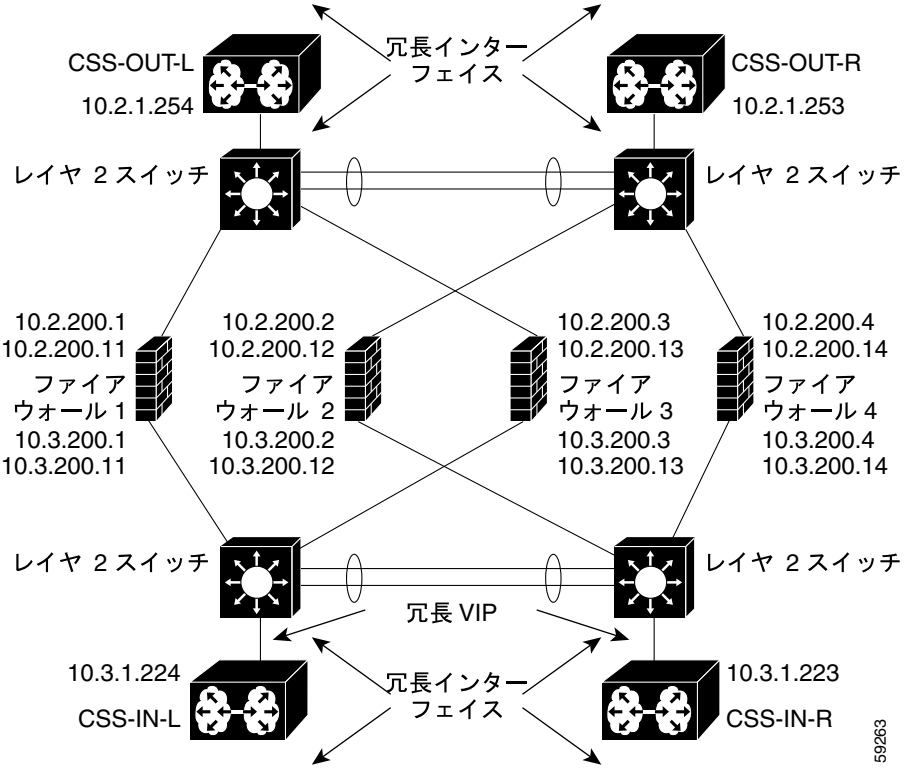
この設定では、ファイアウォールのそれぞれの側に 2 台の冗長 CSS と 2 台の L2 デバイスを使用します。1 台の CSS に障害が発生すると、ファイアウォールの同じ側の冗長 CSS が残りの負荷を引き受けます。

（注）　FWLB を、VIP および仮想インターフェイスの冗長化を行うように設定した場合、共有 VIP は設定しないでください。共有 VIP は FWLB トポロジではサポートしていません。共有 VIP の詳細については、『*Cisco Content Services Switch Redundancy Configuration Guide*』を参照してください。

VIP は、サービスが直接接続されているか、レイヤ 2 デバイスを介して接続されている CSS 上で設定する必要があります。サービスが、ファイアウォールの向こう側に置かれ、FWLB のメンバーである別の CSS に接続されている場合、CSS に VIP を使用したコンテンツ ルールを設定することはできません。このような設定は、非対称パスとなり、ステートフル インスペクションを行うファイアウォールによって接続が中断される可能性があります。

図 5-2 では、CSS-OUT-L と CSS-IN-L にサービスするレイヤ 2 スイッチに奇数番号のファイアウォールが接続されています。CSS-OUT-R と CSS-IN-R にサービスするレイヤ 2 スイッチには、偶数番号のファイアウォールが接続されています。

図 5-2　VIP/ インターフェイスが冗長化された FWLB



各ファイアウォールにはその両側に 2 つずつアドレスを設定する必要があります。最初のアドレスは、低コストのスタティック（プライマリ）パス上のネクストホップに使用します。2 番目のアドレスは、高コストのフローティングスタティック（セカンダリ）パス上のネクストホップに使用します。

フローティングスタティック パスには、スタティック パスとして指定したパス（通常はコスト 1）より高いコスト（通常はコスト 10）を設定します。1 台の CSS（たとえば、CSS-OUT-L）が故障すると、CSS-OUT-R が CSS-IN-L に高いコストのパスを使用してトラフィックを送るようになります。

ファイアウォールがマルチネッティングをサポートする場合、そのファイアウォールに複数のアドレスを設定することでマルチネッティングを使用できます。ファイアウォールが物理インターフェイスごとに複数のアドレスをサポートしない場合、ap-kal-fwlb-multinet スクリプトを使用してファイアウォールの複数のアドレスをシミュレートします。このスクリプトは、引数 realAddress secondaryAddress をとります。このスクリプトにより、各ファイアウォール インターフェイスにつき、スタティック ARP エントリが 1 つ作成されます。

（注） 手動でスタティック ARP エントリを入力することもできますが、スクリプトを使用するほうが、ファイアウォールを交換したことによって MAC アドレスが変わった場合に、ARP エントリも変更されるので便利です。

フェールオーバー時間は、次の理由で 1 ～ 3 秒と非常に高速です。

- フローティングスタテック パスがすでに起動している
- ファイアウォール パス情報が交換されている
- 回線が動作している

レイヤ 2 スイッチの 1 台に障害が発生すると、1 つおきのファイアウォールについてハッシュ値が再度計算されトラフィックのパスが決められます。ファイアウォールが偶数個ある場合、トラフィックの 50 パーセントが同じファイアウォールに再ハッシュされます。

（注） CSS の両側に冗長インターフェイスを設定する場合は、クリティカル サービスを使用して、一方のインターフェイスに障害が発生してバックアップに切り替わった場合にもう一方のインターフェイスでも同じことが行われるようにします。複数のインターフェイスを実装する場合は、ファイアウォール インターフェイスを外側の CSS 上のクリティカル サービスとして使用し、サービス タイプを redundancy-up として設定したファイアウォール インターフェイスとバックエンド サーバを内側の CSS 上のクリティカル サービスとして使用します。クリティカル サービスの設定および冗長アップリンク サービスの設定の詳細については、『*Cisco Content Services Switch Redundancy Configuration Guide*』を参照してください。

ファイアウォールとルート設定の例

次の **ip firewall** と **ip route** の設定例は、4 つのアクティブなファイアウォールからなる図 5-2 で有効です。

CSS-OUT-L の設定

```
ip firewall 1 10.2.200.1 10.3.200.1 10.3.1.224
ip firewall 2 10.2.200.2 10.3.200.2 10.3.1.224
ip firewall 3 10.2.200.3 10.3.200.3 10.3.1.224
ip firewall 4 10.2.200.4 10.3.200.4 10.3.1.224
ip firewall 11 10.2.200.11 10.3.200.11 10.3.1.223
ip firewall 12 10.2.200.12 10.3.200.12 10.3.1.223
ip firewall 13 10.2.200.13 10.3.200.13 10.3.1.223
ip firewall 14 10.2.200.14 10.3.200.14 10.3.1.223
ip route 10.3.0.0 255.255.0.0 firewall 1 1
ip route 10.3.0.0 255.255.0.0 firewall 2 1
ip route 10.3.0.0 255.255.0.0 firewall 3 1
ip route 10.3.0.0 255.255.0.0 firewall 4 1
ip route 10.3.0.0 255.255.0.0 firewall 11 10
ip route 10.3.0.0 255.255.0.0 firewall 12 10
ip route 10.3.0.0 255.255.0.0 firewall 13 10
ip route 10.3.0.0 255.255.0.0 firewall 14 10
```

CSS-OUT-R の設定

```
ip firewall 11 10.2.200.11 10.3.200.11 10.3.1.223
ip firewall 12 10.2.200.12 10.3.200.12 10.3.1.223
ip firewall 13 10.2.200.13 10.3.200.13 10.3.1.223
ip firewall 14 10.2.200.14 10.3.200.14 10.3.1.223
ip firewall 1 10.2.200.1 10.3.200.1 10.3.1.224
ip firewall 2 10.2.200.2 10.3.200.2 10.3.1.224
ip firewall 3 10.2.200.3 10.3.200.3 10.3.1.224
ip firewall 4 10.2.200.4 10.3.200.4 10.3.1.224
ip route 10.3.0.0 255.255.0.0 firewall 11 1
ip route 10.3.0.0 255.255.0.0 firewall 12 1
ip route 10.3.0.0 255.255.0.0 firewall 13 1
ip route 10.3.0.0 255.255.0.0 firewall 14 1
ip route 10.3.0.0 255.255.0.0 firewall 1 10
ip route 10.3.0.0 255.255.0.0 firewall 2 10
ip route 10.3.0.0 255.255.0.0 firewall 3 10
ip route 10.3.0.0 255.255.0.0 firewall 4 10
```

CSS-IN-L の設定

```
ip firewall 1 10.3.200.1 10.2.200.1 10.2.1.254
ip firewall 2 10.3.200.2 10.2.200.2 10.2.1.254
ip firewall 3 10.3.200.3 10.2.200.3 10.2.1.254
ip firewall 4 10.3.200.4 10.2.200.4 10.2.1.254
ip firewall 11 10.3.200.11 10.2.200.11 10.2.1.253
ip firewall 12 10.3.200.12 10.2.200.12 10.2.1.253
ip firewall 13 10.3.200.13 10.2.200.13 10.2.1.253
ip firewall 14 10.3.200.14 10.2.200.14 10.2.1.253
ip route 0.0.0.0 0.0.0.0 firewall 1 1
ip route 0.0.0.0 0.0.0.0 firewall 2 1
ip route 0.0.0.0 0.0.0.0 firewall 3 1
ip route 0.0.0.0 0.0.0.0 firewall 4 1
ip route 0.0.0.0 0.0.0.0 firewall 11 10
ip route 0.0.0.0 0.0.0.0 firewall 12 10
ip route 0.0.0.0 0.0.0.0 firewall 13 10
ip route 0.0.0.0 0.0.0.0 firewall 14 10
```

CSS-IN-R の設定

```
ip firewall 11 10.3.200.11 10.2.200.11 10.2.1.253
ip firewall 12 10.3.200.12 10.2.200.12 10.2.1.253
ip firewall 13 10.3.200.13 10.2.200.13 10.2.1.253
ip firewall 14 10.3.200.14 10.2.200.14 10.2.1.253
ip firewall 1 10.3.200.1 10.2.200.1 10.2.1.254
ip firewall 2 10.3.200.2 10.2.200.2 10.2.1.254
ip firewall 3 10.3.200.3 10.2.200.3 10.2.1.254
ip firewall 4 10.3.200.4 10.2.200.4 10.2.1.254
ip route 0.0.0.0 0.0.0.0 firewall 11 1
ip route 0.0.0.0 0.0.0.0 firewall 12 1
ip route 0.0.0.0 0.0.0.0 firewall 13 1
ip route 0.0.0.0 0.0.0.0 firewall 14 1
ip route 0.0.0.0 0.0.0.0 firewall 1 10
ip route 0.0.0.0 0.0.0.0 firewall 2 10
ip route 0.0.0.0 0.0.0.0 firewall 3 10
ip route 0.0.0.0 0.0.0.0 firewall 4 10
```

ファイアウォール フローの要約の表示

CSS の Switch Processor （SP; スイッチ プロセッサ）上で、特定の送信元 IP アドレスのフロー要約、または特定の送信元アドレスとその宛先 IP アドレスのフロー要約を表示するには、**show flows** コマンドを使用します。1 台の SP につき 4096 までのフローを表示できます。

この情報によって、次のことがわかります。

- 特定のフローに対して使用されるファイアウォールの識別
- フローの表示して FWLB の正常な動作を確認

このコマンドのシンタックスは次のとおりです。

show flows *source_address destination_address*

変数の内容は次のとおりです。

- *source_address* ：フローの送信元 IP アドレス。アドレスをドット付き 10 進表記（たとえば、192.168.11.1）で入力します。
- *destination_address* ：宛先 IP アドレス。アドレスをドット付き 10 進表記（たとえば、192.168.11.1）で入力します。

たとえば、次のように入力します。

```
(config)# show flows 192.165.22.1 192.163.2.3
```

特定の送信元 IP アドレスのフローを表示するには、次のように入力します。

```
(config)# show flows 192.165.22.1
```

特定の送信元 IP アドレスおよび宛先 IP アドレスのフローを表示するには、次のように入力します。

```
(config)# show flows 192.165.22.1 192.163.2.3
```

表 5-1 に、**show flows** コマンドで表示されるフィールドについて説明します。

表 5-1　show flow コマンドのフィールド

フィールド	説明
Src Address	フローの送信元アドレス
SPort	フローの送信元ポート
Dst Address	フローの宛先アドレス
DPort	フローの宛先ポート
NAT Dst Address	NAT 対象の宛先アドレス
Prot	フローのプロトコル（TCP または UDP）
InPort	入側フローのインターフェイス ポート
OutPort	出側フローのインターフェイス ポート

ファイアウォール IP ルートの表示

すべてのスタティック ファイアウォール ルートを表示するには、**show ip routes firewall** コマンドを使用します。たとえば、次のように設定します。

```
(config)# show ip routes firewall
```

表 5-2 に、**show ip routes firewall** コマンドで表示されるフィールドについて説明します。

表 5-2　show ip routes firewall コマンドのフィールド

フィールド	説明
Prefix/length	ルートの IP アドレスとプレフィクス長
Next hop	ネクスト ホップの IP アドレス
If	ifIndex 値。そのルートで、ネクスト ホップに到達する前に通過するローカル インターフェイスです。
Type	ルート エントリのタイプ。タイプはリモートです。
Proto	ルートのプロトコル。ファイアウォールです。
Age	ルートの最大経過時間
Metric	ルートのメトリック コスト

ファイアウォール IP 情報の表示

IP ファイアウォールのキープアライブ タイムアウトに設定された値と、CSS に設定されている各ファイアウォール パスの状態を表示するには、**show ip firewall** コマンドを使用します。たとえば、次のように入力します。

```
(config)# show ip firewall
```

表 5-3 に、**show ip firewall** コマンドのフィールドについて説明します。

表 5-3　show ip firewall コマンドのフィールド

フィールド	説明
IP Firewall KAL Timeout	CSS がリモート CSS からのキープアライブ メッセージを待機する秒数。この秒数の後、ファイアウォールが到達不可能であると宣言します。
Firewall Index	ファイアウォールを識別するためのインデックス番号
State	リモート スイッチへの接続の現在の状態（Init、Reachable、Unreachable のいずれか）
Next Hop	ネクストホップの IP アドレス
Remote Firewall	リモートの CSS に接続されたリモート サブネット上にあるファイアウォールの IP アドレス
Remote Switch	リモート CSS の IP アドレス
Time Since Last KAL Tx	最後のキープアライブ メッセージを送信してから経過した時間
Time Since Last KAL Rx	最後のキープアライブ メッセージを受信してから経過した時間