Firepower 1010 スイッチポートの基本インターフェイス設定

各 Firepower 1010 インターフェイスは、通常のファイアウォール インターフェイスとしてまたはレイヤ 2 ハードウェア スイッチ ポートとして実行するように設定できます。この章では、スイッチモードの有効化と無効化、VLANインターフェイスの作成、そのインターフェイスのスイッチポートへの割り当てなど、スイッチポート設定を開始するためのタスクについて説明します。また、サポート対象のインターフェイスで Power on Ethernet（PoE）をカスタマイズする方法についても説明します。

Firepower 1010 スイッチ ポートについて

この項では、Firepower 1010 のスイッチ ポートについて説明します。

Firepower 1010 ポートおよびインターフェイスについて

ポートとインターフェイス

Firepower 1010 物理インターフェイスごとに、ファイアウォール インターフェイスまたはスイッチポートとしてその動作を設定できます。物理インターフェイスとポートタイプ、およびスイッチポートを割り当てる論理 VLAN インターフェイスについては、次の情報を参照してください。

- 物理ファイアウォールインターフェイス：ルーテッドモードでは、これらのインターフェイスは、設定済みのセキュリティポリシーを使用してファイアウォールと VPN サービスを適用することによって、レイヤ3のネットワーク間でトラフィックを転送します。 トラ

ンスペアレントモードでは、これらのインターフェイスは、設定済みのセキュリティポリシーを使用してファイアウォールサービスを適用することによって、レイヤ2の同じネットワーク上のインターフェイス間でトラフィックを転送するブリッジグループメンバーです。ルーテッドモードでは、一部のインターフェイスでブリッジグループメンバーとして、その他のインターフェイスでレイヤ3インターフェイスとして、統合ルーティングおよびブリッジングを使用することもできます。デフォルトでは、イーサネット 1/1 インターフェイスはファイアウォール インターフェイスとして設定されます。

- 物理スイッチポート：スイッチポートは、ハードウェアのスイッチ機能を使用して、レイヤ 2 でトラフィックを転送します。同じ VLAN 上のスイッチポートは、ハードウェアスイッチングを使用して相互に通信できます。トラフィックには、ASA セキュリティポリシーは適用されません。アクセスポートはタグなしトラフィックのみを受け入れ、単一の VLANに割り当てることができます。トランクポートはタグなしおよびタグ付きトラフィックを受け入れ、複数の VLAN に属することができます。デフォルトでは、イーサネット 1/2 ～ 1/8 は VLAN 1 のアクセススイッチポートとして設定されています。Management インターフェイスをスイッチポートとして設定することはできません。
- 論理 VLAN インターフェイス：これらのインターフェイスは物理ファイアウォール インターフェイスと同じように動作しますが、サブインターフェイス、またはEtherChannelインターフェイスを作成できないという例外があります。スイッチポートが別のネットワークと通信する必要がある場合、ASA デバイスは VLAN インターフェイスにセキュリティポリシーを適用し、別の論理 VLAN インターフェイスまたはファイアウォール インターフェイスにルーティングします。ブリッジグループメンバーとして VLAN インターフェイスで統合ルーティングおよびブリッジングを使用することもできます。同じ VLAN 上のスイッチポート間のトラフィックに ASA セキュリティポリシーは適用されませんが、ブリッジグループ内の VLAN 間のトラフィックにはセキュリティポリシーが適用されるため、ブリッジグループとスイッチポートを階層化して特定のセグメント間にセキュリティポリシーを適用できます。

Power Over Ethernet

イーサネット 1/7 およびイーサネット 1/8 は Power on Ethernet+（PoE+）をサポートしています。

Auto-MDI/MDIX 機能

すべての Firepower 1010 インターフェイスでは、デフォルトの自動ネゴシエーション設定に Auto-MDI/MDIX機能も含まれています。Auto-MDI/MDIXは、オートネゴシエーション フェーズでストレート ケーブルを検出すると、内部クロスオーバーを実行することでクロス ケーブルによる接続を不要にします。インターフェイスの Auto-MDI/MDIX を有効にするには、速度とデュプレックスのいずれかをオートネゴシエーションに設定する必要があります。速度とデュプレックスの両方に明示的に固定値を指定すると、両方の設定でオートネゴシエーションが無効にされ、Auto-MDI/MDIX も無効になります。速度と二重通信をそれぞれ 1000 と全二重に設定すると、インターフェイスでは常にオートネゴシエーションが実行されるため、Auto-MDI/MDIX は常に有効になり、無効にできません。

Firepower 1010 スイッチ ポートの注意事項と制約事項

コンテキスト モード

Firepower 1010 はマルチ コンテキスト モードをサポートしません。

フェールオーバー とクラスタリング

- クラスタのサポートなし。
- アクティブ/スタンバイのフェールオーバーのサポートのみ。
- フェールオーバー を使用する場合は、スイッチポート機能を使用しないでください。スイッチポートはハードウェアで動作するため、アクティブユニットとスタンバイユニットの両方でトラフィックを通過させ続けます。フェールオーバーは、トラフィックがスタンバイユニットを通過するのを防ぐように設計されていますが、この機能はスイッチポートには拡張されていません。通常の フェールオーバー のネットワーク設定では、両方のユニットのアクティブなスイッチ ポートがネットワーク ループにつながります。スイッチング機能には外部スイッチを使用することをお勧めします。VLAN インターフェイスはフェールオーバーによってモニターできますが、スイッチポートはモニターできません。理論的には、1 つのスイッチ ポートを VLAN に配置して、フェールオーバー を正常に使用することができますが、代わりに物理ファイアウォールインターフェイスを使用する設定の方が簡単です。
- ファイアウォールインターフェイスはフェールオーバー リンクとしてのみ使用できます。

論理 VLAN インターフェイス

- 最大 60 の VLAN インターフェイスを作成できます。
- また、ファイアウォール インターフェイスで VLAN サブインターフェイスを使用する場合、論理 VLAN インターフェイスと同じ VLAN ID は使用できません。
- MAC アドレス：
  - ルーテッド ファイアウォール モード：すべての VLAN インターフェイスが 1 つの MAC アドレスを共有します。接続スイッチがどれもこのシナリオをサポートできるようにします。接続スイッチに固有の MAC アドレスが必要な場合、手動で MAC アドレスを割り当てることができます。MACアドレスの手動設定を参照してください。
  - トランスペアレント ファイアウォール モード：各 VLAN インターフェイスに固有の MAC アドレスがあります。必要に応じて、手動で MAC アドレスを割り当てて、生成された MAC アドレスを上書きできます。MAC アドレスの手動設定を参照してください。

ブリッジ グループ

同じブリッジ グループ内に論理 VLAN インターフェイスと物理ファイアウォール インターフェイスを混在させることはできません。

VLAN インターフェイスおよびスイッチ ポートでサポートされていない機能

VLAN インターフェイスおよびスイッチポートは、次の機能をサポートしていません。

- ダイナミック ルーティング
- マルチキャスト ルーティング
- ポリシーベース ルーティング
- 等コストマルチパス（ECMP）ルーティング
- VXLAN
- EtherChannel
- フェールオーバーおよびステートリンク
- トラフィック ゾーン
- セキュリティグループタグ（SGT）

その他のガイドラインと制約事項

- Firepower 1010 には、最大 60 の名前付きインターフェイスを設定できます。
- Management インターフェイスをスイッチポートとして設定することはできません。

デフォルト設定

- イーサネット 1/1 はファイアウォール インターフェイスです。
- イーサネット 1/2 ～ 1/8 は、VLAN 1 に割り当てられたスイッチ ポートです。
- デフォルトの速度とデュプレックス：デフォルトでは、速度とデュプレックスは自動ネゴシエーションに設定されます。

スイッチ ポートと Power Over Ethernet の設定

スイッチ ポートおよび PoE を設定するには、次のタスクを実行します。

スイッチ ポート モードの有効化または無効化

各インターフェイスは、ファイアウォール インターフェイスまたはスイッチ ポートのいずれかになるように個別に設定できます。デフォルトでは、イーサネット 1/1 はファイアウォール

インターフェイスで、残りのイーサネット インターフェイスはスイッチ ポートとして設定されます。

手順

ステップ 1 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。

interface ethernet1/*port*

- *port*：ポート （1 ～ 8）を設定します。

管理 1/1 インターフェイスをスイッチポートモードに設定することはできません。

例：

```
ciscoasa(config)# interface ethernet1/4
ciscoasa(config-if)#
```

ステップ 2 スイッチポートモードを有効にします。

switchport

このインターフェイスがすでにスイッチポートモードの場合、モードを変更する代わりにスイッチポートパラメータを入力するように求められます。

```
ciscoasa(config-if)# switchport
ciscoasa(config-if)# switchport ?
interface mode commands/options:
  access         Set access mode characteristics of the interface
  mode           Set trunking mode of the interface
  monitor        Monitor another interface
  protected      Configure an interface to be a protected port
  trunk          Set trunking characteristics of the interface
<cr>
ciscoasa(config-if)#
```

ステップ 3 スイッチポートモードを無効にします。

no switchport

```
ciscoasa(config-if)# no switchport
ciscoasa(config-if)# switchport ?

interface mode commands/options:
<cr>
```

例

次に、イーサネット 1/3 および 1/4 をファイアウォールモードに設定する例を示します。

```
ciscoasa(config)# interface ethernet1/3
ciscoasa(config-if)# no switchport
ciscoasa(config-if)# interface ethernet1/3
ciscoasa(config-if)# no switchport
ciscoasa(config-if)#
```

VLAN インターフェイスの設定

ここでは、関連付けられたスイッチ ポートで使用するための VLAN インターフェイスの設定方法について説明します。

手順

ステップ 1 VLAN インターフェイスを追加します。

interface vlan *id*

- *id*：このインターフェイスの VLAN ID を 1 ～ 4070 の範囲で設定します。ただし、内部使用のために予約されている 3968 ～ 4047 の範囲の ID は除きます。

例：

```
ciscoasa(config)# interface vlan 100
ciscoasa(config-if)#
```

ステップ 2 （任意） 別の VLAN への転送を無効にします。

no forward interface *vlan_id*

- *vlan_id*：この VLAN インターフェイスでトラフィックの開始を禁止する先の VLAN ID を指定します。

たとえば、1 つの VLAN をインターネット アクセスの外部に、もう 1 つを内部ビジネス ネットワーク内に、そして 3 つ目をホーム ネットワークにそれぞれ割り当てます。ホームネットワークはビジネスネットワークにアクセスする必要がないので、ホーム VLAN で **no forward interface** コマンドを使用できます。ビジネスネットワークはホームネットワークにアクセスできますが、その反対はできません。

例：

```
ciscoasa(config-if)# no forward interface 200
ciscoasa(config-if)#
```

スイッチ ポートのアクセス ポートとしての設定

1 つの VLAN にスイッチ ポートを割り当てるには、アクセス ポートとして設定します。アクセス ポートは、タグなしのトラフィックのみを受け入れます。デフォルトでは、Ethernet1/2 ～ 1/8 のスイッチ ポートが有効になっていて、VLAN 1 に割り当てられています。

（注） Firepower 1010 では、ネットワーク内のループ検出のためのスパニングツリー プロトコルはサポートされません。したがって、ASA との接続はいずれもネットワークループ内で終わらないようにする必要があります。

手順

ステップ 1 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。

interface ethernet1/*port*

- *port*：ポート （1 ～ 8）を設定します。

例：

```
ciscoasa(config)# interface ethernet1/4
ciscoasa(config-if)#
```

ステップ 2 このスイッチポートを VLAN に割り当てます。

switchport access vlan *number*

- *number*：VLAN ID を 1 ～ 4070 の間で設定します。デフォルトは VLAN 1 です。

例：

```
ciscoasa(config-if)# switchport access vlan 100
ciscoasa(config-if)#
```

ステップ 3 （任意）このスイッチポートを保護対象として設定します。これにより、スイッチポートが同じ VLAN 上の他の保護されたスイッチポートと通信するのを防ぐことができます。

switchport protected

スイッチ ポート上のデバイスが主に他の VLAN からアクセスされる場合、VLAN 内アクセスを許可する必要がない場合、および感染やその他のセキュリティ侵害に備えてデバイスを相互に分離する場合に、スイッチ ポートが相互に通信しないようにします。たとえば、3 つの Web サーバーをホストする DMZ がある場合、各スイッチポートに **switchport protected** コマンドを適用すると、Web サーバーを相互に分離できます。内部ネットワークと外部ネットワークはいずれも 3 つの Web サーバーすべてと通信でき、その逆も可能ですが、Web サーバーは相互に通信できません。

例：

```
ciscoasa(config-if)# switchport protected
ciscoasa(config-if)#
```

ステップ 4 （任意） 速度を設定します。

speed {**auto** | **10** | **100** | **1000**}

デフォルトは **auto** です。

例：

```
ciscoasa(config-if)# speed 100
ciscoasa(config-if)#
```

ステップ 5 （任意） 二重通信を設定します。

duplex {**auto** | **full** | **half**}

デフォルトは **auto** です。

例：

```
ciscoasa(config-if)# duplex half
ciscoasa(config-if)#
```

ステップ 6 スイッチポートをイネーブルにします。

no shutdown

スイッチポートをディセーブルにするには、**shutdown** コマンドを入力します。

例：

```
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)#
```

例

次の例では、イーサネット 1/3、イーサネット 1/4、およびイーサネット 1/5 を VLAN 101 に割り当て、イーサネット 1/3 とイーサネット 1/4 を保護対象として設定します。

```
ciscoasa(config)# interface ethernet1/3
ciscoasa(config-if)# switchport access vlan 101
ciscoasa(config-if)# switchport protected
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet1/4
ciscoasa(config-if)# switchport access vlan 101
ciscoasa(config-if)# switchport protected
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet1/5
```

```
ciscoasa(config-if)# switchport access vlan 101
ciscoasa(config-if)# no shutdown
```

スイッチ ポートのトランク ポートとしての設定

この手順では、802.1Q タグ付けを使用して複数の VLAN を伝送するトランク ポートの作成方法について説明します。トランクポートは、タグなしおよびタグ付きトラフィックを受け入れます。許可された VLAN のトラフィックは、トランクポートを変更せずに通過します。

トランクは、タグなしトラフィックを受信すると、そのトラフィックをネイティブ VLAN ID にタグ付けして、ASA が正しいスイッチポートにトラフィックを転送したり、別のファイアウォールインターフェイスにルーティングしたりできるようにします。ASA は、トランクポートからネイティブ VLAN ID トラフィックを送信する際に VLAN タグを削除します。タグなしトラフィックが同じ VLAN にタグ付けされるように、他のスイッチのトランク ポートに同じネイティブ VLAN を設定してください。

手順

ステップ 1 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。

interface ethernet1/*port*

- *port*：ポート （1 ～ 8）を設定します。

例：

```
ciscoasa(config)# interface ethernet1/4
ciscoasa(config-if)#
```

ステップ 2 このスイッチポートをトランクポートにします。

switchport mode trunk

このポートをアクセスモードに復元するには、**switchport mode access** コマンドを入力します。

例：

```
ciscoasa(config-if)# switchport mode trunk
ciscoasa(config-if)#
```

ステップ 3 このトランクに VLAN を割り当てます。

switchport trunk allowed vlan *vlan_range*

- *vlan_range*：VLAN ID を 1 ～ 4070 の間で設定します。次のいずれかの方法で最大 20 個の ID を指定できます。
  - 単一の番号（n）
  - 範囲（n-x）

- 番号および範囲は、カンマで区切ります。たとえば、次のように指定します。

  5,7-10,13,45-100

カンマの代わりにスペースを入力できますが、コマンドはカンマ付きでコンフィギュレーションに保存されます。

このコマンドにネイティブVLANを含めても無視されます。トランクポートは、ネイティブ VLAN トラフィックをポートから送信するときに、常に VLAN タグを削除します。また、まだネイティブ VLAN タグが付いているトラフィックを受信しません。

例：

```
ciscoasa(config-if)# switchport trunk allowed vlan 100,200,300
ciscoasa(config-if)#
```

ステップ 4 ネイティブ VLAN を選択します。

switchport trunk native vlan *vlan_id*

- *vlan_range*：VLAN ID を 1 ～ 4070 の間で設定します。デフォルト値は VLAN 1 です。

各ポートのネイティブ VLAN は 1 つのみですが、すべてのポートに同じネイティブ VLAN または異なるネイティブ VLAN を使用できます。

例：

```
ciscoasa(config-if)# switchport trunk native vlan 2
ciscoasa(config-if)#
```

ステップ 5 （任意） このスイッチポートを保護対象として設定します。これにより、スイッチポートが同じ VLAN 上の他の保護されたスイッチポートと通信するのを防ぐことができます。

switchport protected

スイッチ ポート上のデバイスが主に他の VLAN からアクセスされる場合、VLAN 内アクセスを許可する必要がない場合、および感染やその他のセキュリティ侵害に備えてデバイスを相互に分離する場合に、スイッチ ポートが相互に通信しないようにします。たとえば、3 つの Web サーバーをホストする DMZ がある場合、各スイッチポートに **switchport protected** コマンドを適用すると、Web サーバーを相互に分離できます。内部ネットワークと外部ネットワークはいずれも 3 つの Web サーバーすべてと通信でき、その逆も可能ですが、Web サーバーは相互に通信できません。

例：

```
ciscoasa(config-if)# switchport protected
ciscoasa(config-if)#
```

ステップ 6 （任意） 速度を設定します。

speed {**auto** | **10** | **100** | **1000**}

デフォルトは **auto** です。

例：

```
ciscoasa(config-if)# speed 100
ciscoasa(config-if)#
```

ステップ 7 （任意） 二重通信を設定します。

duplex {**auto** | **full** | **half**}

デフォルトは **auto** です。

例：

```
ciscoasa(config-if)# duplex half
ciscoasa(config-if)#
```

ステップ 8 スイッチポートをイネーブルにします。

no shutdown

スイッチポートをディセーブルにするには、**shutdown** コマンドを入力します。

例：

```
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)#
```

例

次に、イーサネット 1/6 を VlAN 20 ～ 30 のトランクポートとして設定し、ネイティブ VLAN を 4 に設定する例を示します。

```
ciscoasa(config)# interface ethernet1/6
ciscoasa(config-if)# switchport mode trunk
ciscoasa(config-if)# switchport trunk allowed vlan 20-30
ciscoasa(config-if)# switchport trunk native vlan 4
ciscoasa(config-if)# no shutdown
```

Power over Ethernet の設定

Ethernet 1/7 および Ethernet 1/8 は、IP 電話や無線アクセスポイントなどのデバイス用に Power over Ethernet（PoE）をサポートしています。Firepower 1010 は、IEEE 802.3af（PoE）と 802.3at（PoE+）の両方をサポートしています。PoE+ は、Link Layer Discovery Protocol（LLDP）を使用して電力レベルをネゴシエートします。PoE+ は、受電デバイスに最大 30 ワットの電力を提供できます。電力は必要なときのみ供給されます。

インターフェイスをシャットダウンすると、デバイスへの給電が無効になります。

PoE は、デフォルトで Ethernet 1/7 および Ethernet 1/8 で有効になっています。この手順では、PoE を無効および有効にする方法と、オプションパラメータを設定する方法について説明します。

手順

ステップ 1 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。

interface ethernet1/{**7** | **8**}

例：

```
ciscoasa(config)# interface ethernet1/7
ciscoasa(config-if)#
```

ステップ 2 PoE+ を有効または無効にします。

power inline {**auto** | **never** | **consumption wattage** *milliwatts*}

- **auto**：給電先デバイスのクラスに適したワット数を使用して、給電先デバイスに自動的に電力を供給します。Firepower 1010 は LLDP を使用して、適切なワット数をさらにネゴシエートします。
- **never**：PoE を無効にします。
- **consumption wattage** *milliwatts*：ワット数をミリワット単位で手動で指定します（4000 ～ 30000）。ワット数を手動で設定し、LLDP ネゴシエーションを無効にする場合は、このコマンドを使用します。

show power inline コマンドを使用して、現在の PoE+ ステータスを表示します。

例：

```
ciscoasa(config-if)# power inline auto
ciscoasa(config-if)# show power inline
Interface     Power   Class   Current (mA)   Voltage (V)
   ---------     -----   -----   ------------   -----------
   Ethernet1/1   n/a     n/a     n/a            n/a
   Ethernet1/2   n/a     n/a     n/a            n/a
   Ethernet1/3   n/a     n/a     n/a            n/a
   Ethernet1/4   n/a     n/a     n/a            n/a
   Ethernet1/5   n/a     n/a     n/a            n/a
   Ethernet1/6   n/a     n/a     n/a            n/a
   Ethernet1/7   On      4       121.00         53.00
   Ethernet1/8   On      4       88.00          53.00
```

例

次に、イーサネット 1/7 のワット数を手動で設定し、イーサネット 1/8 の電力を auto に設定する例を示します。

```
ciscoasa(config)# interface ethernet1/7
ciscoasa(config-if)# power inline consumption wattage 10000
ciscoasa(config-if)# interface ethernet1/8
ciscoasa(config-if)# power inline auto
ciscoasa(config-if)#
```

スイッチポートのモニタリング

- **show interface**

  インターフェイス統計情報を表示します。

- **show interface ip brief**

  インターフェイスの IP アドレスとステータスを表示します。

- **show switch vlan**

  VLAN とスイッチポートの関連付けを表示します。

```
ciscoasa# show switch vlan
VLAN Name                 Status    Ports
---- -------------------- --------- --------------------
1    -                     down      Ethernet1/3,
                                     Ethernet1/4,
                                     Ethernet1/5,
                                     Ethernet1/6
                                     Ethernet1/7,
                                     Ethernet1/8
10   inside                up        Ethernet1/1
20   outside               up        Ethernet1/2
```

- **show switch mac-address-table**

  スタティックおよびダイナミック MAC アドレス エントリを表示します。

```
ciscoasa# show switch mac-address-table
Legend: Age - entry expiration time in seconds
  Mac Address  | VLAN |       Type       | Age | Port
-----------------------------------------------------
0c75.bd11.c504 | 0010 |     dynamic      | 330 | In0/0
885a.92f6.c6e3 | 0010 |     dynamic      | 330 | Et1/1
0c75.bd11.c504 | 0020 |     dynamic      | 330 | In0/0
885a.92f6.c45b | 0020 |     dynamic      | 330 | Et1/2
```

- **show arp**

ダイナミック、スタティック、およびプロキシ ARP エントリを表示します。ダイナミック ARP エントリには、ARP エントリの秒単位のエージングが含まれています。エージングの代わりに、スタティック ARP エントリにはダッシュ（-）が、プロキシ ARP エントリには「alias」という状態が含まれています。次に、**show arp** コマンドの出力例を示します。1 つめのエントリは、2 秒間エージングされているダイナミック エントリです。2 つめのエントリはスタティック エントリ、3 つめのエントリはプロキシ ARP のエントリです。

```
ciscoasa# show arp
outside 10.86.194.61 0011.2094.1d2b 2
outside 10.86.194.1 001a.300c.8000 -
outside 10.86.195.2 00d0.02a8.440a alias
```

- **show power inline**

  PoE+ ステータスを表示します。

```
ciscoasa# show power inline
   Interface     Power   Class   Current (mA)   Voltage (V)
   ---------     -----   -----   ------------   -----------
   Ethernet1/1   n/a     n/a     n/a            n/a
   Ethernet1/2   n/a     n/a     n/a            n/a
   Ethernet1/3   n/a     n/a     n/a            n/a
   Ethernet1/4   n/a     n/a     n/a            n/a
   Ethernet1/5   n/a     n/a     n/a            n/a
   Ethernet1/6   n/a     n/a     n/a            n/a
   Ethernet1/7   On      4       121.00         53.00
   Ethernet1/8   On      4       88.00          53.00
```

スイッチポートの例

次のトピックでは、ルーテッドモードおよびトランスペアレントモードでスイッチポートを設定する例を示します。

ルーテッドモードの例

次の例では、2 つの VLAN インターフェイスを作成し、2 つのスイッチポートを内部インターフェイスに、もう 1 つを外部インターフェイスに割り当てます。

```
interface Vlan11
nameif inside
security-level 100
ip address 10.11.11.1 255.255.255.0
no shutdown
!
interface Vlan20
nameif outside
security-level 0
ip address 10.20.20.1 255.255.255.0
no shutdown
```

```
!
interface Ethernet1/1
switchport
switchport access vlan 11
no shutdown
!
interface Ethernet1/2
switchport
switchport access vlan 20
no shutdown
!
interface Ethernet1/3
switchport
switchport access vlan 11
no shutdown
```

トランスペアレントモードの例

次の例では、ブリッジグループ 1 に 2 つの VLAN インターフェイスを作成し、2 つのスイッチポートを内部インターフェイスに、もう 1 つを外部インターフェイスに割り当てます。

```
firewall transparent
!
interface BVI1
ip address 10.20.20.1 255.255.255.0
!
interface Vlan11
bridge-group 1
nameif inside
security-level 100
no shutdown
!
interface Vlan20
bridge-group 1
nameif outside
security-level 0
no shutdown
!
interface Ethernet1/1
switchport
switchport access vlan 11
no shutdown
!
interface Ethernet1/2
switchport
switchport access vlan 20
no shutdown
!
interface Ethernet1/3
switchport
switchport access vlan 11
no shutdown
```

ファイアウォール インターフェイス/スイッチポートの混合の例

次の例では、内部インターフェイス用の 1 つの VLAN インターフェイスと、外部および dmz 用の 2 つのファイアウォール インターフェイスを作成します。

```
interface Vlan11
nameif inside
security-level 100
ip address 10.11.11.1 255.255.255.0
no shutdown
!
interface Ethernet1/1
switchport
switchport access vlan 11
no shutdown
!
interface Ethernet1/2
switchport
switchport access vlan 11
no shutdown
!
interface Ethernet1/3
switchport
switchport access vlan 11
no shutdown
!
interface Ethernet1/4
nameif outside
security-level 0
ip address 10.12.11.1 255.255.255.0
no shutdown
!
interface Ethernet1/5
nameif dmz
security-level 50
ip address 10.13.11.1 255.255.255.0
no shutdown
```

統合ルーティングおよびブリッジングの例

次の例では 2 つのブリッジグループを作成します。ブリッジグループ 1 に 2 つの VLAN インターフェイス（inside_1 と inside_2）、ブリッジグループ 2 に 1 つの VLAN インターフェイス（outside）を含めます。4 番目の VLAN インターフェイスはブリッジグループの一部ではなく、通常のルーテッドインターフェイスです。同じ VLAN 上のスイッチポート間のトラフィックは、ASA のセキュリティポリシーの対象にはなりません。ただし、ブリッジグループ内の VLAN 間のトラフィックにはセキュリティポリシーが適用されるため、特定のセグメント間のレイヤブリッジグループとスイッチポートを選択することができます。

```
interface BVI1
nameif inside_bvi
security-level 100
ip address 10.30.1.10 255.255.255.0
!
interface BVI2
nameif outside_bvi
```

```
security-level 0
ip address 10.40.1.10 255.255.255.0
!
interface Vlan10
bridge-group 1
nameif inside_1
security-level 100
no shutdown
!
interface Vlan20
bridge-group 2
nameif outside
security-level 0
no shutdown
!
interface Vlan30
bridge-group 1
nameif inside_2
security-level 100
no shutdown
!
interface Vlan 100
nameif dmz
security-level 0
ip address 10.1.1.1 255.255.255.0
no shutdown
!
interface Ethernet1/1
switchport
switchport access vlan 10
no shutdown
!
interface Ethernet1/2
switchport
switchport access vlan 20
no shutdown
!
interface Ethernet1/3
switchport
switchport access vlan 30
no shutdown
!
interface Ethernet1/4
switchport
switchport access vlan 20
security-level 100
no shutdown
!
interface Ethernet1/5
switchport
switchport access vlan 100
no shutdown
!
interface Ethernet1/6
switchport
switchport access vlan 10
no shutdown
!
interface Ethernet1/7
switchport
switchport access vlan 30
no shutdown
!
interface Ethernet1/8
```

```
switchport
switchport access vlan 100
no shutdown
```

フェールオーバーの例

次に、イーサネット 1/3 をフェールオーバー インターフェイスとして設定する例を示します。

```
interface Vlan11
nameif inside
security-level 100
ip address 10.11.11.1 255.255.255.0 standby 10.11.11.2
no shutdown
!
interface Vlan20
nameif outside
security-level 0
ip address 10.20.20.1 255.255.255.0 standby 10.20.20.2
no shutdown
!
interface Ethernet1/1
switchport
switchport access vlan 11
no shutdown
!
interface Ethernet1/2
switchport
switchport access vlan 20
no shutdown
!
interface Ethernet1/3
description LAN/STATE Failover Interface
no shutdown
!
failover
failover lan unit primary
failover lan interface folink Ethernet1/3
failover replication http
failover link folink Ethernet1/3
failover interface ip folink 10.90.90.1 255.255.255.0 standby 10.90.90.2
```

スイッチポートの履歴

表 *1:* スイッチポートの履歴

機能名	バージョン	機能情報
Firepower 1010 ハードウェア スイッチのサポート	9.13(1)	Firepower 1010 では、各イーサネット インターフェイスをスイッチ ポートまたはファイアウォール インターフェイスとして設定できます。 新しい/変更されたコマンド：**forward interface**、**interface vlan**、**show switch mac-address-table**、**show switch vlan**、**switchport**、**switchport access vlan**、**switchport mode**、**switchport trunk allowed vlan**
イーサネット 1/7 およびイーサネット 1/8 での Firepower 1010 PoE+ のサポート	9.13(1)	Firepower 1010 は、イーサネット 1/7 およびイーサネット 1/8 での Power over Ethernet+（PoE+） をサポートしています。 新しい/変更されたコマンド：**power inline**、**show power inline**

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。