



Firepower 1010 スイッチポートの基本インターフェイス構成

Firepower 1010220/ の各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構成できます。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。

- [スイッチポートについて \(1 ページ\)](#)
- [スイッチポートの前提条件 \(3 ページ\)](#)
- [スイッチポートのガイドライン \(3 ページ\)](#)
- [スイッチポートと Power Over Ethernet の設定 \(5 ページ\)](#)
- [スイッチポートのモニタリング \(13 ページ\)](#)
- [スイッチポートの例 \(15 ページ\)](#)
- [スイッチポートの履歴 \(19 ページ\)](#)

スイッチポートについて

この項では、レイヤ2スイッチを搭載したモデルのスイッチポートについて説明します。

スイッチ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

物理インターフェイスごとに、その動作を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 以上は VLAN 1 のアクセススイッチポートとして構成されています。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

PoE は、IEEE 802.3af (PoE) および 802.3at (PoE+) を使用して、イーサネット 1/7 およびイーサネット 1/8 でポートあたり最大 30 ワットまで供給できます。

PoE+ では、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。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。

Auto-MDI/MDIX 機能

すべてのスイッチポートで、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。

スイッチポートの前提条件

モデルのサポート

- Firepower 1010

スイッチポートのガイドライン

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。
- Cisco Secure Firewall 1210/1220 はマルチコンテキストモードをサポートしません。

フェイルオーバーおよびクラスタリング

- クラスタはサポートされません。
- アクティブ/スタンバイのフェールオーバーのみサポートされます。
- フェイ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。フェイルオーバーは、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。通常のフェイ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、フェイ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 (SVI)

- 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：スイッチのポートを EtherChannel の一部にはできません。PoE も、EtherChannel のポートではサポートされません。
- 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)

その他の注意事項と制約事項

- 最大 60 の名前付きインターフェイスを構成できます。
- 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 が、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 (SVI) の構成方法について説明します。スイッチポートを関連付けられた最大 60 個の VLAN インターフェイスを作成できます。

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構成

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、イーサネット 1/2 ～ イーサネット 1/8 スイッチポートが有効になっており、VLAN 1 に割り当てられています。



- (注) デバイスは、ネットワーク内のループ検出に使用されるスパニングツリープロトコルをサポートしていません。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、タグなしトラフィックと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

Power over Ethernet (PoE) ポートは、IP 電話や無線アクセスポイントなどのデバイスに電力を供給します。PoE はデフォルトでイネーブルです。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。ファイアウォールは LLDP を使用して、さらに適切なワット数をネゴシエートします。特定クラスのデバイスを接続すると、より多くの電力を使用する必要がある場合に備えて、そのクラスの最大値までプロビジョニングが行われます。たとえば、12.95W を要求するクラス 4 デバイスを追加した場合、そのデバイスが現在その電力すべてを使用していなくても、30W が割り当てられます。一部のデバイスは、電力要件を再ネゴシエートできます。デバイスに必要な電力が割り当てられている電力よりも少ないことがわかっている場合は、代わりに **consumption wattage** を手動で設定して、他のデバイス用に電力を解放できます。
- **never** : PoE を無効にします。
- **consumption wattage milliwatts** : 4,000 ～ 30,000 のワット数をミリワット単位で手動で指定します。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。手動割り当ての場合、出力にクラスが **n/a** と表示されます。これは、クラスが消費電力の決定に使用されないためです。

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

この例では、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

この例では、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。

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。