Configuration de base de l'interface pour les ports de commutation du Firepower 1010

Vous pouvez configurer chaque interface Firepower 1010 pour qu'elle fonctionne comme une interface pare-feu normale ou comme un port de commutateur matériel de couche 2. Ce chapitre comprend les tâches de démarrage de la configuration de votre port de commutation, notamment l'activation ou la désactivation du mode de commutation, la création d'interfaces VLAN et l'affectation des ports de commutation aux réseaux VLAN. Ce chapitre décrit également comment personnaliser l'alimentation par Ethernet (PoE) sur les interfaces prises en charge.

À propos des ports de commutation

Cette section décrit les ports de commutation du Firepower 1010 et du .

Comprendre les ports et les interfaces de commutation

Ports et interfaces

Pour chaque interface physique 1010, vous pouvez définir son fonctionnement comme interface de pare-feu ou comme port de commutation. Consultez les renseignements suivants sur les interfaces physiques et les types de port, ainsi que sur les interfaces VLAN logiques auxquelles vous affectez des ports de commutation :

- Interface de pare-feu physique : En mode routé, ces interfaces transmettent le trafic entre les réseaux de la couche 3 en utilisant la politique de sécurité configurée pour appliquer les services de pare-feu et VPN. En mode transparent, ces interfaces sont des membres de groupes de ponts qui acheminent le trafic entre les interfaces du même réseau au niveau de la couche 2, en utilisant la politique de sécurité configurée pour appliquer les services de pare-feu. En mode routé, vous pouvez également utiliser le routage et le pont intégrés avec certaines interfaces comme membres du groupe de ponts et d'autres comme interfaces de couche 3. Par défaut, l'interface Ethernet 1/1 est configurée comme interface de pare-feu.

- Port de commutation physique : les ports de commutation transfèrent le trafic à la couche 2 en utilisant la fonction de commutation dans le matériel. Les ports de commutation sur le même VLAN peuvent communiquer entre eux grâce à la commutation matérielle, et le trafic n'est pas soumis à la politique de sécurité ASA. Les ports d'accès acceptent uniquement le trafic non balisé et vous pouvez les affecter à un seul VLAN. Les ports de ligne principale acceptent le trafic non balisé et peuvent appartenir à plus d'un VLAN. Par défaut, Ethernet 1/2 à 1/8 sont configurés comme ports de commutation d'accès sur VLAN 1. Vous ne pouvez pas configurer l'interface Management (gestion) comme port de commutation.
- Logical VLAN interface (interface VLAN logique) : Ces interfaces fonctionnent de la même façon que les interfaces de pare-feu physiques, à la différence que vous ne pouvez pas créer des sous-interfaces, des , des ou des interfaces EtherChannel. Lorsqu'un port de commutation doit communiquer avec un autre réseau, le périphérique ASA applique la politique de sécurité à l'interface VLAN et achemine le routage vers une autre interface VLAN logique ou une interface de pare-feu. Vous pouvez même utiliser le routage et le pont intégrés avec des interfaces VLAN comme membres du groupe de ponts. Le trafic entre les ports de commutation sur le même VLAN n'est pas soumis à la politique de sécurité, mais le trafic entre les VLAN d'un groupe de ponts est soumis à la politique de sécurité ASA. Vous pouvez donc choisir de superposer les groupes de ponts et les ports de commutation pour appliquer la politique de sécurité entre certains segments.

Alimentation par Ethernet

La PoE est disponible sur Ethernet 1/7 et Ethernet 1/8 en utilisant les protocoles IEEE 802.3af (PoE) et 802.3at (PoE+), jusqu'à 30 W par port.

PoE+ utilise le protocole LLDP (Link Layer Discovery Protocol) pour négocier le niveau de puissance. L'alimentation n'est fournie qu'en cas de besoin.

Si vous désactivez l'interface, vous désactivez l'alimentation du périphérique.

Fonctionnalité Auto-MDI/MDIX

Pour tous les ports de commutation, le paramètre de négociation automatique par défaut inclut également la fonction Auto-MDI/MDIX. La fonction Auto-MDI/MDIX élimine le besoin de câblage croisé en effectuant un croisé interne lorsqu'un câble droit est détecté pendant la phase de négociation automatique. La vitesse ou le duplex doivent être réglés pour qu'ils soient négociés automatiquement afin d'activer Auto-MDI/MDIX pour l'interface. Si vous définissez explicitement la vitesse et le duplex à une valeur fixe, désactivant ainsi la négociation automatique pour les deux paramètres, Auto-MDI/MDIX est également désactivé. Lorsque la vitesse et le mode duplex sont définis à 1000 et que la vitesse maximale est atteinte, l'interface négocie toujours automatiquement; par conséquent, Auto-MDI/MDIX est toujours activé et vous ne pouvez pas le désactiver.

Lignes directrices et limites pour les ports de commutation

Mode contextuel

- Firepower 1010 ne prend pas en charge le mode contexte multiple.
- Le Secure Firewall 1210/1220 ne prend pas en charge le mode de contexte multiple.

Failover (basculement) et mise en grappe

- Aucune prise en charge de grappe.
- Prise en charge du basculement actif/veille uniquement.
- Vous ne devez pas utiliser la fonctionnalité de port de commutateur lors de l'utilisation de Failover (basculement). Étant donné que les ports de commutation fonctionnent dans le matériel, ils continuent de faire circuler le trafic sur les unités actives *et* en veille. Failover (basculement) est conçu pour empêcher le trafic de passer par l'unité en veille, mais cette fonctionnalité ne s'étend pas aux ports de commutation. Dans une configuration réseau Failover (basculement) normale, les ports de commutateur actifs sur les deux unités mèneront à des boucles réseau. Nous vous suggérons d'utiliser des commutateurs externes pour toute capacité de commutation. Notez que les interfaces VLAN peuvent être surveillées par basculement, contrairement aux ports de commutation. Théoriquement, vous pouvez mettre un port de commutation unique sur un réseau VLAN et utiliser Failover (basculement) avec succès, mais une configuration plus simple consiste à utiliser des interfaces physiques de pare-feu à la place.
- Vous ne pouvez utiliser qu'une interface de pare-feu comme liaison de basculement.

Interfaces logiques VLAN (SVI)

- Vous pouvez créer jusqu'à 60 interfaces VLAN.
- Si vous utilisez également des sous-interfaces VLAN sur une interface de pare-feu, vous ne pouvez pas utiliser le même ID VLAN que pour une interface VLAN logique.
- Adresses MAC
  - Mode de pare-feu routé : toutes les interfaces VLAN partagent une adresse MAC. Assurez-vous que tous les commutateurs connectés peuvent prendre en charge ce scénario. Si les commutateurs connectés nécessitent des adresses MAC uniques, vous pouvez attribuer manuellement des adresses MAC. Consultez Configurer manuellement l'adresse MAC
  - Mode pare-feu transparent : chaque interface VLAN a une adresse MAC unique. Vous pouvez remplacer les adresses MAC générées si vous le souhaitez en attribuant manuellement des adresses MAC. Consultez Configurer manuellement l'adresse MAC.

Groupes de ponts

Vous ne pouvez pas mélanger des interfaces VLAN logiques et des interfaces de pare-feu physiques dans le même groupe de ponts.

Fonctionnalités non prises en charge de l'interface VLAN et du port de commutation

Les interfaces VLAN et les ports de commutation ne prennent pas en charge :

- Routage dynamique
- Routage multidiffusion
- Routage basé sur les politiques
- Routage multiples chemins à coûts égaux (ECMP)
- VXLAN

- EtherChannels : les ports de commutation ne peuvent pas faire partie d'un EtherChannel. Le PoE n'est pas non plus pris en charge sur un port d'un EtherChannel.
- Basculement et lien d'état
- Zones de circulation
- Balise du groupe de sécurité (SGT)

Autres directives et limites

- Vous pouvez configurer un maximum de 60 interfaces nommées sur le Firepower 1010.
- Vous ne pouvez pas configurer l'interface Management (gestion) comme port de commutation.

Paramètres d'usine

- Ethernet 1/1 est une interface de pare-feu.
- Ethernet 1/2 à Ethernet 1/8 sont des ports de commutation affectés au VLAN 1.
- Vitesse et duplex par défaut: par défaut, la vitesse et le duplex sont configurés pour la négociation automatique.

Configurer les ports de commutation et l'alimentation par Ethernet (PoE)

Pour configurer les ports de commutation et la PoE, procédez comme suit :

Activer ou désactiver le mode Port de commutation

Vous pouvez définir chaque interface indépendamment comme interface de pare-feu ou comme port de commutation. Par défaut, Ethernet 1/1 est une interface de pare-feu et les autres interfaces Ethernet sont configurées comme des ports de commutation.

Procédure

Étape 1 Entrez en mode de configuration d'interface.

interface ethernet1/*port*

- *port* : définit le port, de 1 à 8.

Vous ne pouvez pas définir l'interface de gestion Management 1/1 sur le mode du port de commutation.

Exemple :

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

Étape 2 Activez le mode Port de commutation.

switchport

Si cette interface est déjà en mode Port de commutation, vous êtes invité à configurer les paramètres du port de commutation au lieu de modifier le mode.

```
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)#
```

Étape 3 Désactivez le mode Port de commutation.

no switchport

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

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

Exemple

L'exemple suivant définit Ethernet 1/3 et 1/4 en mode de pare-feu :

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

Configurer une interface VLAN

Cette section décrit comment configurer les interfaces VLAN (SVI) à utiliser avec les ports de commutation associés. Vous pouvez créer jusqu'à 60 interfaces VLAN associées aux ports de commutation.

Procédure

Étape 1 Ajoutez une interface VLAN.

interface vlan *ID*

- *id* : définit l'ID de VLAN pour cette interface, entre 1 et 4070, en excluant les ID de 3968 à 4047, qui sont réservés à un usage interne.

Exemple :

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

Étape 2 (Facultatif) Désactivez le transfert vers un autre VLAN.

no forward interface *vlan_id*

- *vlan_id* : spécifie l'ID de VLAN vers lequel cette interface VLAN ne peut pas initier le trafic.

Par exemple, vous avez un VLAN affecté à l'extérieur pour l'accès Internet, un VLAN affecté à un réseau interne d'entreprise et un troisième VLAN affecté à votre réseau domestique. Le réseau domestique n'a pas besoin d'accéder au réseau de l'entreprise, vous pouvez donc utiliser la commande **no forward interface** sur le VLAN domestique; le réseau professionnel peut accéder au réseau domestique, mais le réseau domestique ne peut pas accéder au réseau d'entreprise.

Exemple :

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

Configurer les ports de commutation comme ports d'accès

Pour affecter un port de commutation à un seul VLAN, configurez-le comme port d'accès. Les ports d'accès acceptent uniquement le trafic non balisé. Par défaut, Ethernet 1/2 à Ethernet 1/8 sont des ports de commutation affectés au VLAN 1.

Remarque L'appareil ne prend pas en charge le protocole Spanning Tree pour la détection de boucle dans le réseau. Par conséquent, vous devez vous assurer qu'une connexion avec l'ASA ne finit pas dans une boucle de réseau.

Procédure

Étape 1 Entrez en mode de configuration d'interface.

interface ethernet1/*port*

- *port* : définit le port, de 1 à 8.

Exemple :

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

Étape 2 Attribuez ce port de commutation à un VLAN.

switchport access vlan *number*

- *number* : définit l'ID de VLAN entre 1 et 4070. La valeur par défaut est VLAN 1.

Exemple :

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

Étape 3 (Facultatif) Définissez ce port de commutation comme protégé afin de pouvoir l'empêcher de communiquer avec d'autres ports de commutation protégés sur le même VLAN.

switchport protected

Vous pourriez souhaiter empêcher les ports de commutation de communiquer entre eux dans les cas suivants : les périphériques sur ces ports de commutation sont principalement accessibles à partir d'autres VLAN; vous n'avez pas besoin d'autoriser l'accès intra-VLAN; et vous souhaitez isoler les périphériques les uns des autres en cas d'infection ou de toute autre faille de sécurité. Par exemple, si vous avez une DMZ qui héberge trois serveurs Web, vous pouvez isoler les serveurs Web les uns des autres si vous appliquez la commande **switchport protected** à chaque port de commutation. Les réseaux interne et externe peuvent tous deux communiquer avec les trois serveurs Web, et inversement, mais les serveurs Web ne peuvent pas communiquer entre eux.

Exemple :

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

Étape 4 (Facultatif) Définissez la vitesse.

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

La valeur par défaut est **auto**.

Exemple :

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

Étape 5 (Facultatif) Définissez le duplex.

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

La valeur par défaut est **auto**.

Exemple :

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

Étape 6 Activez le port de commutation.

no shutdown

Pour désactiver le port de commutation, saisissez la commande **shutdown**.

Exemple :

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

Exemple

L'exemple suivant affecte Ethernet 1/3, Ethernet 1/4 et Ethernet 1/5 au VLAN 101 et définit Ethernet 1/3 et Ethernet 1/4 comme protégés :

```
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
```

Configurer les ports de commutation comme ports de ligne principale

Cette procédure décrit comment créer un port de liaison qui peut acheminer plusieurs VLAN à l'aide du balisage 802.1Q. Les ports de ligne principale acceptent le trafic non balisé et balisé. Le trafic sur les VLAN autorisés passe par le port de liaison sans changement.

Lorsque la ligne principale reçoit un trafic non balisé, elle le balise à l'ID de VLAN natif afin que l'ASA puisse transférer le trafic vers les ports de commutation appropriés ou l'acheminer vers une autre interface de pare-feu. Lorsque l'ASA envoie le trafic d'ID de VLAN natif hors du port de liaison, il supprime la balise VLAN. Assurez-vous de définir le même VLAN natif sur le port de liaison de l'autre commutateur afin que le trafic non balisé soit balisé vers le même VLAN.

Procédure

Étape 1 Entrez en mode de configuration d'interface.

interface ethernet1/*port*

- *port* : définit le port, de 1 à 8.

Exemple :

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

Étape 2 Configurez ce port de commutateur en tant que port de liaison.

switchport mode trunk

Pour rétablir ce port en mode d'accès, saisissez la commande **switchport mode access**.

Exemple :

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

Étape 3 Attribuez des VLAN à cette liaison.

switchport trunk allowed vlan *vlan_range*

- *vlan_range* : définit les ID de VLAN entre 1 et 4070. Vous pouvez identifier jusqu'à 20 identifiants de l'une des manières suivantes :
  - Nombre unique (n)
  - Plage A (n à x)
  - Chiffres et plages séparés par des virgules, par exemple :

    5,7-10,13,45-100

  Vous pouvez saisir des espaces au lieu de virgules, mais la commande est enregistrée dans la configuration avec des virgules.

  Si vous incluez le VLAN natif dans cette commande, il est ignoré; le port de liaison supprime toujours le balisage VLAN lors de l'envoi de trafic VLAN natif hors du port. De plus, il ne recevra pas le trafic qui a toujours un balisage VLAN natif.

Exemple :

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

Étape 4 Définissez le VLAN natif.

switchport trunk native vlan *vlan_id*

- *vlan_range* : définit l'ID de VLAN entre 1 et 4070. La valeur par défaut est VLAN 1.

Chaque port ne peut avoir qu'un seul VLAN natif, mais chaque port peut avoir le même VLAN natif ou un différent.

Exemple :

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

Étape 5 (Facultatif) Définissez ce port de commutation comme protégé afin de pouvoir l'empêcher de communiquer avec d'autres ports de commutation protégés sur le même VLAN.

switchport protected

Vous pourriez souhaiter empêcher les ports de commutation de communiquer entre eux dans les cas suivants : les périphériques sur ces ports de commutation sont principalement accessibles à partir d'autres VLAN; vous

n'avez pas besoin d'autoriser l'accès intra-VLAN; et vous souhaitez isoler les périphériques les uns des autres en cas d'infection ou de toute autre faille de sécurité. Par exemple, si vous avez une DMZ qui héberge trois serveurs Web, vous pouvez isoler les serveurs Web les uns des autres si vous appliquez la commande **switchport protected** à chaque port de commutation. Les réseaux interne et externe peuvent tous deux communiquer avec les trois serveurs Web, et inversement, mais les serveurs Web ne peuvent pas communiquer entre eux.

Exemple :

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

Étape 6 (Facultatif) Définissez la vitesse.

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

La valeur par défaut est **auto**.

Exemple :

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

Étape 7 (Facultatif) Définissez le duplex.

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

La valeur par défaut est **auto**.

Exemple :

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

Étape 8 Activez le port de commutation.

no shutdown

Pour désactiver le port de commutation, saisissez la commande **shutdown**.

Exemple :

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

Exemple

L'exemple suivant définit Ethernet 1/6 comme port de liaison avec les VLAN 20 à 30 et définit le VLAN natif comme 4 :

```
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
```

Configurer Power Over Ethernet (alimentation électrique par câble Ethernet)

Les ports Power over Ethernet (PoE) alimentent les périphériques tels que les téléphones IP ou les points d'accès sans fil. Le mode PoE est activé par défaut. Cette procédure décrit comment activer et désactiver la PoE et comment définir les paramètres facultatifs.

Procédure

Étape 1 Entrez en mode de configuration d'interface.

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

Exemple :

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

Étape 2 Activez ou désactivez PoE.

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

- **auto** : fournit automatiquement du courant au périphérique alimenté en utilisant une puissance appropriée pour la classe du périphérique alimenté. Le pare-feu utilise LLDP pour négocier davantage la puissance en watts. Lorsque vous connectez un périphérique d'une certaine classe, il sera provisionné au maximum pour cette classe au cas où il aurait besoin d'utiliser plus de puissance. Par exemple, si vous ajoutez un périphérique de classe 4 qui demande 12,95 W, il se verra attribuer 30 W même s'il n'utilise pas actuellement toute cette puissance. Certains appareils peuvent renégocier les besoins en matière d'alimentation. Si vous savez que votre périphérique a besoin de moins d'alimentation que ce qui est alloué, vous pouvez plutôt définir la **consumption wattage** manuellement pour libérer de l'alimentation pour d'autres périphériques.
- **never** : désactive le PoE.
- **consumption wattage** *milliwatts* : spécifie manuellement la puissance en milliwatts, de 4 000 à 30 000. Utilisez cette commande si vous souhaitez définir les watts manuellement et désactiver la négociation LLDP. Pour l'attribution manuelle, la classe s'affichera comme **n/a** (s.o.) dans la sortie d'affichage, car la classe n'est pas utilisée pour déterminer la consommation d'énergie.

Affichez l'état PoE actuel à l'aide de la commande **show power inline**.

Exemple :

```
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
```

Exemple

L'exemple suivant définit manuellement la puissance en watts pour Ethernet 1/7 et règle la puissance à « auto » pour Ethernet 1/8 :

```
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)#
```

Supervision des ports de commutation

- **show interface**

  Affiche des statistiques sur l'interface.

- **show interface ip brief**

  Affiche les adresses IP et l'état de l'interface.

- **show switch vlan**

  Affiche l'association du port VLAN au commutateur.

```
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**

  Affiche les entrées d'adresse MAC statiques et dynamiques.

```
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**

  Affiche les entrées ARP dynamiques, statiques et de mandataire. Les entrées ARP dynamiques comprennent l'ancienneté de l'entrée ARP en secondes. Les entrées ARP statiques comprennent un tiret (-) au lieu de l'âge, et les entrées ARP du mandataire indiquent « alias ». Voici un exemple de sortie de la commande **show arp**. La première entrée est une entrée dynamique de 2 secondes. La deuxième entrée est une entrée statique et la troisième entrée provient d'un mandataire ARP.

```
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**

  Affichez l'état PoE+.

```
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
```

Exemples de ports de commutation

Les rubriques suivantes fournissent des exemples de configuration des ports de commutation en mode routé et transparent.

Exemple de mode routé

L'exemple suivant crée deux interfaces VLAN et affecte deux ports de commutation à l'interface interne et un à l'interface externe.

```
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
```

Exemple de mode transparent

L'exemple suivant crée deux interfaces VLAN dans le groupe de ponts 1 et affecte deux ports de commutation à l'interface interne et un à l'interface externe.

```
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
```

Exemple d'interface de pare-feu/port de commutation mixte

L'exemple suivant crée une interface VLAN pour l'interface interne et deux interfaces de pare-feu pour l'interface externe et DMZ.

```
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
```

Exemple de routage et pont intégrés

L'exemple suivant crée deux groupes de ponts, avec deux interfaces VLAN (interne_1 et interne_2) dans le groupe de ponts 1 et une (externe) dans le groupe de ponts 2. Une quatrième interface VLAN ne fait pas partie d'un groupe de ponts et constitue une interface routée standard. Le trafic entre les ports de commutation sur le même VLAN n'est pas soumis à la politique de sécurité de l'ASA. Toutefois, le trafic entre les VLAN d'un groupe de ponts est soumis à la politique de sécurité. Vous pouvez donc choisir de superposer les groupes de ponts et les ports de commutation pour appliquer la politique de sécurité entre certains segments.

```
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
```

Exemple de basculement

L'exemple suivant configure Ethernet 1/3 comme interface de basculement.

```
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
```

Historique des ports de commutation

Tableau 1 : Historique des ports de commutation

Nom de la caractéristique	Version	Renseignements sur les fonctionnalités
Prise en charge du commutateur matériel Firepower 1010	9.13(1)	L'appareil Firepower 1010 prend en charge la définition de chaque interface Ethernet comme port de commutation ou interface de pare-feu. Commandes nouvelles ou modifiées : **forward interface, interface vlan, show switch mac-address-table, show switch vlan, switchport, switchport access vlan, switchport mode, switchport trunk allowed vlan**
Prise en charge du Firepower 1010 PoE+ sur Ethernet 1/7 et Ethernet 1/8	9.13(1)	Le Firepower 1010 prend en charge Power over Ethernet+ (PoE+) sur Ethernet 1/7 et Ethernet 1/8. Commandes nouvelles ou modifiées : **power inline, show power inline**

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.