Configuration de l'ASA 5506W-X avec une configuration IP non par défaut ou VLAN multiple

Table des matières

Introduction

Ce document décrit comment effectuer l'installation et la configuration initiales d'un périphérique Cisco Adaptive Security Appliance (ASA) 5506W-X lorsque le schéma d'adressage IP par défaut doit être modifié pour s'adapter à un réseau existant ou si plusieurs VLAN sans fil sont nécessaires. Plusieurs modifications de configuration sont nécessaires lors de la modification des

adresses IP par défaut afin d'accéder au point d'accès sans fil (WAP) et de garantir que les autres services (tels que DHCP) continuent à fonctionner comme prévu. En outre, ce document fournit des exemples de configuration CLI pour le point d'accès sans fil intégré (WAP) afin de faciliter la configuration initiale du WAP. Ce document est destiné à compléter le guide de démarrage rapide Cisco ASA 5506-X existant disponible sur le site Web Cisco.

Conditions préalables

Ce document ne s'applique qu'à la configuration initiale d'un périphérique Cisco ASA5506W-X qui contient un point d'accès sans fil et n'est destiné qu'à répondre aux diverses modifications nécessaires lorsque vous modifiez le schéma d'adressage IP existant ou ajoutez des VLAN sans fil supplémentaires. Pour les installations de configuration par défaut, le Guide de démarrage rapide de l'ASA 5506-X doit être référencé.

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Périphérique Cisco ASA 5506W-X
- Machine client avec un programme d'émulation de terminal tel que Putty, SecureCRT, etc.
- Câble de console et adaptateur de terminal PC série (DB-9 à RJ-45)

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

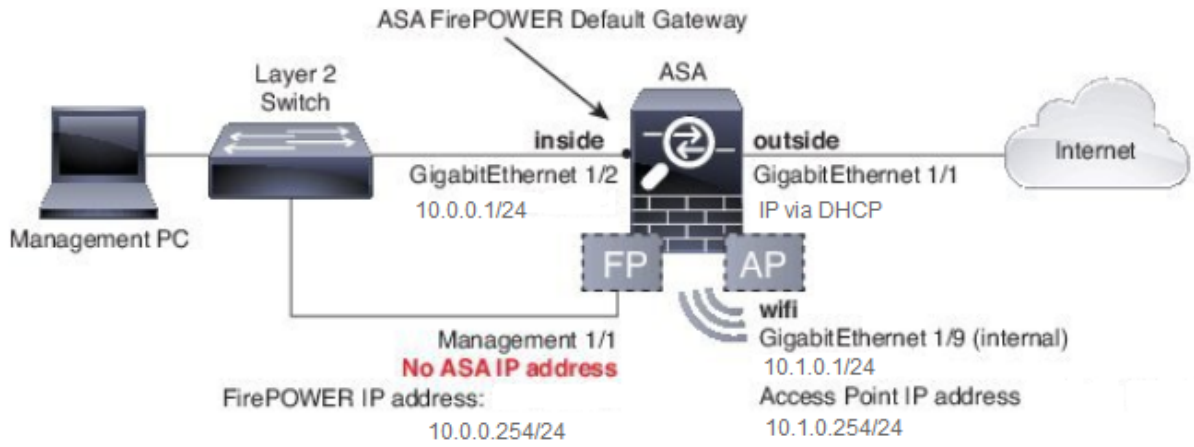
- Périphérique Cisco ASA 5506W-X
- Machine client avec un programme d'émulation de terminal tel que Putty, SecureCRT, etc.
- Câble de console et adaptateur de terminal PC série (DB-9 à RJ-45)
- Module ASA FirePOWER
- Point d'accès sans fil Cisco Aironet 702i intégré (WAP intégré)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

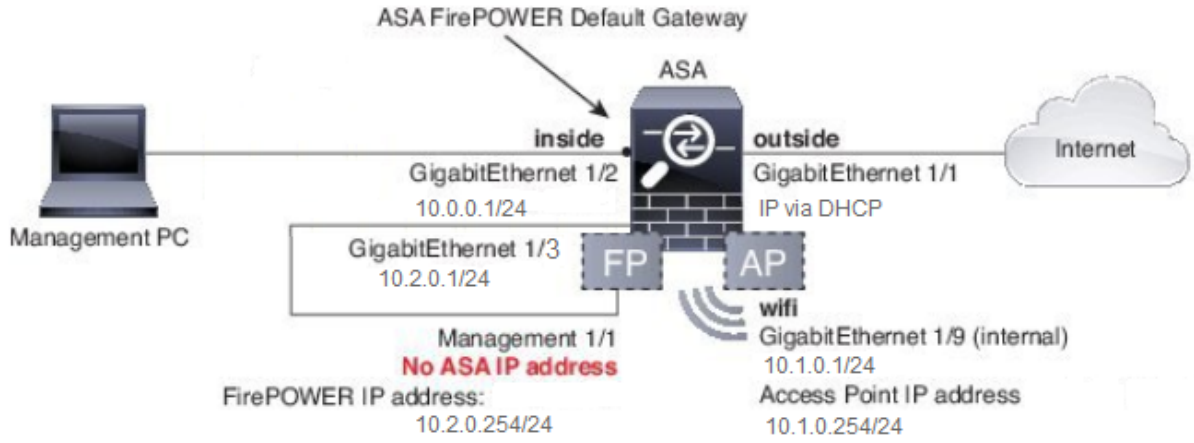
Diagrammes du réseau

Comme le montre cette image, des exemples d’adressage IP qui seront appliqués dans deux topologies différentes :

ASA + FirePOWER avec commutateur interne :



ASA + FirePOWER sans commutateur interne :



Configurer

Ces étapes doivent être effectuées dans l'ordre après la mise sous tension et le démarrage de l'ASA avec le câble de console connecté au client.

Étape 1. Modifier la configuration IP de l'interface sur ASA

Configurez les interfaces internes (GigabitEthernet 1/2) et wifi (GigabitEthernet 1/9) pour qu'elles disposent des adresses IP nécessaires dans l'environnement existant. Dans cet exemple, les clients internes se trouvent sur le réseau 10.0.0.1/24 et les clients WIFI sur le réseau 10.1.0.1/24.

```
asa(config)# interface gigabitEthernet 1/2
asa(config-if)# ip address 10.0.0.1 255.255.255.0

asa(config)# interface gigabitEthernet 1/9
asa(config-if)# ip address 10.1.0.1 255.255.255.0
```

Remarque : cet avertissement s'affiche lorsque vous modifiez les adresses IP d'interface ci-dessus. C'est prévu.

```
Interface address is not on same subnet as DHCP pool
WARNING: DHCPD bindings cleared on interface 'inside', address pool removed
```

Étape 2. Modifier les paramètres du pool DHCP sur les interfaces internes et Wi-Fi

Cette étape est nécessaire si l'ASA doit être utilisé comme serveur DHCP dans l'environnement. Si un autre serveur DHCP est utilisé pour attribuer des adresses IP aux clients, le protocole DHCP doit être entièrement désactivé sur l'ASA. Puisque vous avez modifié notre schéma d'adressage IP, vous devez modifier les plages d'adresses IP existantes que l'ASA fournit aux clients. Ces commandes créent de nouveaux pools correspondant à la nouvelle plage d'adresses IP :

```
asa(config)# dhcpd address 10.0.0.2-10.0.0.100 inside
asa(config)# dhcpd address 10.1.0.2-10.1.0.100 wifi
```

En outre, la modification des pools DHCP désactivera le serveur DHCP précédent sur l'ASA et vous devrez le réactiver.

```
asa(config)# dhcpd enable inside
asa(config)# dhcpd enable wifi
```

Si vous ne modifiez pas les adresses IP de l'interface avant d'effectuer les modifications DHCP, vous recevrez cette erreur :

```
asa(config)# dhcpd address 10.0.0.2-10.0.0.100 inside
Address range subnet 10.0.0.2 or 10.0.0.100 is not the same as inside interface subnet 192.168.1.1
```

Étape 3. Spécifier le serveur DNS à transmettre aux clients DHCP internes et WiFI

Lorsqu’ils attribuent des adresses IP via DHCP, la plupart des clients doivent également se voir attribuer un serveur DNS par le serveur DHCP. Ces commandes configurent l'ASA pour inclure le serveur DNS situé à l'adresse 10.0.0.250 à tous les clients. Vous devez remplacer 10.0.0.250 par un serveur DNS interne ou un serveur DNS fourni par votre FAI.

```
asa(config)# dhcpd dns 10.0.0.250 interface inside
asa(config)# dhcpd dns 10.0.0.250 interface wifi
```

Étape 4. Modifiez la configuration d'accès HTTP sur l'ASA pour l'accès à Adaptive Security Device Manager (ASDM) :

Comme l'adressage IP a été modifié, l'accès HTTP à l'ASA doit également être modifié afin que les clients internes et les réseaux WiFI puissent accéder à l'ASDM pour gérer l'ASA.

```
asa(config)# no http 192.168.1.0 255.255.255.0 inside
asa(config)# no http 192.168.10.0 255.255.255.0 wifi

asa(config)# http 0.0.0.0 0.0.0.0 inside
asa(config)# http 0.0.0.0 0.0.0.0 wifi
```

> Remarque : cette configuration permet à tout client à l'intérieur ou aux interfaces wifi d'accéder à l'ASA via l'ASDM. Par mesure de sécurité, vous devez limiter l'étendue des adresses aux clients approuvés uniquement.

Étape 5. Modifier l'adresse IP d'interface pour la gestion des points d'accès dans la console WLAN (interface BVI1) :

```
asa# session wlan console
ap>enable
Password: Cisco
ap#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ap(config)#interface BVI1
ap(config-if)#ip address 10.1.0.254 255.255.255.0
```

Étape 6. Modifier la passerelle par défaut sur WAP

Cette étape est nécessaire pour que le WAP sache où envoyer tout le trafic qui n'est pas originaire du sous-réseau local. Ceci est nécessaire pour fournir un accès à l'interface utilisateur graphique WAP via HTTP à partir d'un client sur l'interface interne ASA.

```
ap(config)#ip default-gateway 10.1.0.1
```

Étape 7. Modification de l'adresse IP de gestion du module FirePOWER (facultatif)

Si vous prévoyez également de déployer le module Cisco FirePOWER (également appelé SFR), vous devez également modifier son adresse IP afin d'y accéder à partir de l'interface physique Management1/1 sur l'ASA. Deux scénarios de déploiement de base déterminent la configuration de l'ASA et du module SFR :

1. Topologie dans laquelle l'interface ASA Management1/1 est connectée à un commutateur interne (conformément au guide de démarrage rapide normal)
2. Topologie dans laquelle aucun commutateur interne n'est présent.

En fonction de votre scénario, voici les étapes appropriées :

Si l'interface ASA Management1/1 est connectée à un commutateur interne :

Vous pouvez ouvrir une session dans le module et le modifier à partir de l'ASA avant de le connecter à un commutateur interne. Cette configuration vous permet d'accéder au module SFR via IP en le plaçant sur le même sous-réseau que l'interface interne ASA avec l'adresse IP 10.0.0.254.

Les lignes en gras sont spécifiques à cet exemple et sont nécessaires pour établir la connectivité IP.

Les lignes en italique varient selon l'environnement.

```
asa# session sfr console
Opening console session with module sfr.
Connected to module sfr. Escape character sequence is 'CTRL-^X'.

Cisco ASA5506W v5.4.1 (build 211)
Sourcefire3D login: admin
Password: Sourcefire

<<Output Truncated - you will see a large EULA>>

Please enter 'YES' or press <ENTER> to AGREE to the EULA: YES

System initialization in progress.  Please stand by.
You must change the password for 'admin' to continue.
Enter new password:
Confirm new password:
You must configure the network to continue.
You must configure at least one of IPv4 or IPv6.
Do you want to configure IPv4? (y/n) [y]: y
Do you want to configure IPv6? (y/n) [n]: n
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
```

```
Enter an IPv4 address for the management interface [192.168.45.45]: 10.0.0.254



Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.255.0
Enter the IPv4 default gateway for the management interface []:



10.0.0.1



Enter a fully qualified hostname for this system [Sourcefire3D]: Cisco_SFR
Enter a comma-separated list of DNS servers or 'none' []: 10.0.0.250
Enter a comma-separated list of search domains or 'none' [example.net]: example.net
If your networking information has changed, you will need to reconnect.

For HTTP Proxy configuration, run 'configure network http-proxy'

Applying 'Default Allow All Traffic' access control policy.
```

> Remarque : l'application de la stratégie de contrôle d'accès par défaut sur le module SFR peut prendre quelques minutes. Une fois terminé, vous pouvez sortir de l'interface de ligne de commande du module SFR et revenir à l'ASA en appuyant sur CTRL + MAJ + 6 +X (CTRL ^ X)

Si l'ASA N'EST PAS connecté à un commutateur interne :

Un commutateur interne peut ne pas exister dans certains petits déploiements. Dans ce type de topologie, les clients se connectent généralement à l'ASA via l'interface WiFi. Dans ce scénario, il est possible d'éliminer le besoin d'un commutateur externe et d'accéder au module SFR via une interface ASA distincte en interconnectant l'interface Management1/1 à une autre interface ASA physique.

Dans cet exemple, une connexion Ethernet physique doit exister entre l'interface ASA GigabitEthernet1/3 et l'interface Management1/1. Ensuite, vous configurez les modules ASA et SFR pour qu'ils se trouvent sur un sous-réseau distinct, puis vous pouvez accéder au SFR à partir de l'ASA ainsi que des clients situés sur les interfaces internes ou wifi.

Configuration de l'interface ASA :

```
asa(config)# interface gigabitEthernet 1/3
asa(config-if)# ip address 10.2.0.1 255.255.255.0
asa(config-if)# nameif sfr
INFO: Security level for "sfr" set to 0 by default.
```

```
asa(config-if)# security-level 100
asa(config-if)# no shut
```

Configuration du module SFR :

```
asa# session sfr console
Opening console session with module sfr.
Connected to module sfr. Escape character sequence is 'CTRL-^X'.

Cisco ASA5506W v5.4.1 (build 211)
Sourcefire3D login: admin
Password: Sourcefire

<<Output Truncated - you will see a large EULA>>

Please enter 'YES' or press <ENTER> to AGREE to the EULA: YES

System initialization in progress.  Please stand by.
You must change the password for 'admin' to continue.
Enter new password:
Confirm new password:
You must configure the network to continue.
You must configure at least one of IPv4 or IPv6.
Do you want to configure IPv4? (y/n) [y]: y
Do you want to configure IPv6? (y/n) [n]: n
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:



Enter an IPv4 address for the management interface [192.168.45.45]: 10.2.0.254
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.255.0
Enter the IPv4 default gateway for the management interface []: 10.2.0.1



Enter a fully qualified hostname for this system [Sourcefire3D]: Cisco_SFR
Enter a comma-separated list of DNS servers or 'none' []: 10.0.0.250
Enter a comma-separated list of search domains or 'none' [example.net]: example.net
If your networking information has changed, you will need to reconnect.

For HTTP Proxy configuration, run 'configure network http-proxy'

Applying 'Default Allow All Traffic' access control policy.
```

> Remarque : l'application de la stratégie de contrôle d'accès par défaut sur le module SFR peut prendre quelques minutes. Une fois terminé, vous pouvez vous échapper de l'interface de ligne de commande du module SFR et revenir à l'ASA en appuyant sur CTRL + MAJ + 6 +X (CTRL ^ X).

Une fois la configuration SFR appliquée, vous devez pouvoir envoyer une requête ping à l'adresse

IP de gestion SFR à partir de l'ASA :

```
asa# ping 10.2.0.254



Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.0.254, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
asa#
```

Si vous ne parvenez pas à envoyer une requête ping à l'interface, vérifiez la configuration et l'état des connexions Ethernet physiques.

Étape 8. Connectez-vous à l'interface graphique AP pour activer les radios et définir une autre configuration WAP

À ce stade, vous devez disposer d'une connectivité pour gérer le WAP via l'interface utilisateur graphique HTTP, comme indiqué dans le guide de démarrage rapide. Vous devrez soit rechercher l'adresse IP de l'interface BVI du WAP à partir d'un navigateur Web d'un client connecté au réseau interne sur le 5506W, soit appliquer l'exemple de configuration et vous connecter au SSID du WAP. Si vous n'utilisez pas l'interface de ligne de commande ci-dessous, vous devez brancher le câble Ethernet de votre client à l'interface Gigabit1/2 sur l'ASA.

Si vous préférez utiliser l'interface de ligne de commande pour configurer le WAP, vous pouvez vous y connecter à partir de l'ASA et utiliser cet exemple de configuration. Ceci crée un SSID ouvert avec le nom 5506W et 5506W_5Ghz afin que vous puissiez utiliser un client sans fil pour vous connecter au WAP et le gérer davantage.

> Remarque : après avoir appliqué cette configuration, vous souhaiterez accéder à l'interface utilisateur graphique et appliquer la sécurité aux SSID afin que le trafic sans fil soit chiffré.

Configuration WAP CLI pour un VLAN sans fil unique utilisant des plages IP modifiées

```
dot11 ssid 5506W
   authentication open
   guest-mode
dot11 ssid 5506W_5Ghz
   authentication open
   guest-mode
!
interface Dot11Radio0
 !
 ssid 5506W
 !
```

```
interface Dot11Radio1
 !
 ssid 5506W_5Ghz
 !
interface BVI1
 ip address 10.1.0.254 255.255.255.0
ip default-gateway 10.1.0.1
!
interface Dot11Radio0
 no shut
!
interface Dot11Radio1
 no shut
```

À partir de ce moment, vous pouvez effectuer les étapes normales pour terminer la configuration du WAP et vous devez être en mesure d'y accéder à partir du navigateur Web d'un client connecté au SSID créé ci-dessus. Le nom d'utilisateur par défaut du point d'accès est Cisco avec un mot de passe Cisco avec un C majuscule.

Guide de démarrage rapide de la gamme Cisco ASA 5506-X

http://www.cisco.com/c/en/us/td/docs/security/asa/quick_start/5506X/5506x-quick-start.html#pgfId-138410

Vous devez utiliser l'adresse IP 10.1.0.254 au lieu de 192.168.10.2, comme indiqué dans le Guide de démarrage rapide.

Configurations

La configuration résultante doit correspondre au résultat (en supposant que vous ayez utilisé les plages IP de l'exemple, sinon remplacez en conséquence :

Configuration ASA

Interfaces:

> Remarque : les lignes en italique s'appliquent uniquement si vous n'avez PAS de commutateur interne :

```
asa# sh run interface gigabitEthernet 1/2
```

```
!
interface GigabitEthernet1/2
 nameif inside
 security-level 100
 ip address 10.0.0.1 255.255.255.0
```

```
asa# sh run interface gigabitEthernet 1/3
```

```
!
interface GigabitEthernet1/3
 nameif sfr
 security-level 100
 ip address 10.2.0.1 255.255.255.0
```

```
asa# sh run interface gigabitEthernet 1/9
```

```
!
interface GigabitEthernet1/9
 nameif wifi
 security-level 100
 ip address 10.1.0.1 255.255.255.0
asa#
```

DHCP :

```
asa# sh run dhcpd
```

```
dhcpd auto_config outside
**auto-config from interface 'outside'
**auto_config dns x.x.x.x x.x.x.x  <-- these lines will depend on your ISP
**auto_config domain isp.domain.com   <-- these lines will depend on your ISP
!
dhcpd address 10.0.0.2-10.0.0.100 inside
dhcpd dns 10.0.0.250 interface inside
dhcpd enable inside
!
dhcpd address 10.1.0.2-10.1.0.100 wifi
dhcpd dns 10.0.0.250 interface wifi
dhcpd enable wifi
!
asa#
```

HTTP :

```
asa# show run http



http server enable
http 0.0.0.0 0.0.0.0 outside
http 0.0.0.0 0.0.0.0 inside
asa#
```

Configuration WAP Aironet (sans l'exemple de configuration SSID)

```
asa# session wlan console
ap>enable
Password: Cisco
ap#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.



ap#show configuration | include default-gateway



ip default-gateway 10.1.0.1



ap#show configuration | include ip route



ip route 0.0.0.0 0.0.0.0 10.1.0.1



ap#show configuration | i interface BVI|ip address 10



interface BVI1 ip address
 10.1.0.254 255.255.255.0
```

Configuration du module FirePOWER (avec commutateur interne)

```
asa# session sfr console
Opening console session with module sfr.
Connected to module sfr. Escape character sequence is 'CTRL-^X'.
> show network
===============[ System Information ]===============
Hostname                  : Cisco_SFR
Domains                   : example.net
DNS Servers               : 10.0.0.250
Management port           : 8305



IPv4 Default route
  Gateway                 : 10.0.0.1




======================[ eth0 ]======================
State                     : Enabled
Channels                  : Management & Events
Mode                      :
MDI/MDIX                  : Auto/MDIX
MTU                       : 1500
MAC Address               : B0:AA:77:7C:84:10



----------------------[ IPv4 ]----------------------



Configuration             : Manual
Address                   : 10.0.0.254
Netmask                   : 255.255.255.0
Broadcast                 : 10.0.0.255



----------------------[ IPv6 ]----------------------
Configuration             : Disabled

===============[ Proxy Information ]================
State                     : Disabled
Authentication            : Disabled

>
```

Configuration du module FirePOWER (sans commutateur interne)

```
asa# session sfr console
Opening console session with module sfr.
Connected to module sfr. Escape character sequence is 'CTRL-^X'.
> show network
===============[ System Information ]===============
Hostname                  : Cisco_SFR
Domains                   : example.net
DNS Servers               : 10.0.0.250
Management port           : 8305



IPv4 Default route
  Gateway                 : 10.2.0.1




======================[ eth0 ]======================
State                     : Enabled
Channels                  : Management & Events
Mode                      :
MDI/MDIX                  : Auto/MDIX
MTU                       : 1500
MAC Address               : B0:AA:77:7C:84:10



----------------------[ IPv4 ]----------------------
Configuration             : Manual
Address                   : 10.2.0.254
Netmask                   : 255.255.255.0
Broadcast                 : 10.2.0.255



----------------------[ IPv6 ]----------------------
Configuration             : Disabled

===============[ Proxy Information ]================
State                     : Disabled
Authentication            : Disabled

>
```

Vérifier

Afin de vérifier que vous avez la connectivité appropriée au WAP pour terminer le processus

d'installation :

1. Connectez votre client test à l'interface interne ASA et assurez-vous qu'il reçoit une adresse IP de l'ASA via DHCP qui se trouve dans la plage IP souhaitée.
2. Utilisez un navigateur Web sur votre client afin de naviguer vers https://10.1.0.254 et vérifiez que l'interface graphique de l'AP est maintenant accessible.
3. Envoyez une requête ping à l'interface de gestion SFR depuis le client interne et l'ASA pour vérifier la connectivité appropriée.

Configuration de DHCP avec plusieurs VLAN sans fil

La configuration suppose que vous utilisez un seul VLAN sans fil. L'interface BVI (Bridge Virtual Interface) sur le point d'accès sans fil peut fournir un pont pour plusieurs VLAN. En raison de la syntaxe pour DHCP sur l'ASA, si vous souhaitez configurer le 5506W comme serveur DHCP pour plusieurs VLAN, vous devez créer des sous-interfaces sur l'interface Gigabit1/9 et donner un nom à chacune d'elles. Cette section vous guide tout au long du processus de suppression de la configuration par défaut et d'application de la configuration nécessaire pour configurer l'ASA en tant que serveur DHCP pour plusieurs VLAN.

Étape 1. Supprimer la configuration DHCP existante sur Gig1/9

Commencez par supprimer la configuration DHCP existante sur l'interface Gig1/9 (wifi) :

```
ciscoasa# no dhcpd address 10.1.0.2-10.1.0.100 wifi
ciscoasa# no dhcpd enable wifi
```

Étape 2. Créer des sous-interfaces pour chaque VLAN sur Gig1/9

Pour chaque VLAN que vous avez configuré sur le point d'accès, vous devez configurer une sous-interface de Gig1/9. Dans cet exemple de configuration, vous ajoutez deux sous-interfaces :

-Gig1/9.5, qui portera le nom vlan5 et correspondra au VLAN 5 et au sous-réseau 10.5.0.0/24.

-Gig1/9.30, qui portera le nom vlan30 et correspondra au VLAN 30 et au sous-réseau 10.3.0.0/24.

En pratique, il est essentiel que le VLAN et le sous-réseau configurés ici correspondent au VLAN et au sous-réseau spécifiés sur le point d'accès. Le nom et le numéro de sous-interface peuvent être tout ce que vous choisissez. Reportez-vous au guide de démarrage rapide mentionné précédemment pour obtenir des liens permettant de configurer le point d'accès à l'aide de l'interface utilisateur graphique Web.

```
ciscoasa(config)# interface g1/9.5
ciscoasa(config-if)# vlan 5
ciscoasa(config-if)# nameif vlan5
ciscoasa(config-if)# security-level 100
```

```
ciscoasa(config-if)# ip address 10.5.0.1 255.255.255.0

ciscoasa(config-if)# interface g1/9.30
ciscoasa(config-if)# vlan 30
ciscoasa(config-if)# nameif vlan30
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.30.0.1 255.255.255.0
```

Étape 3. Désigner un pool DHCP pour chaque VLAN

Créez un pool DHCP distinct pour chaque VLAN configuré. La syntaxe de cette commande nécessite que vous listiez le nom si l'ASA servira le pool en question. Comme indiqué dans cet exemple, qui utilise les VLAN 5 et 30 :

```
ciscoasa(config)# dhcpd address 10.5.0.2-10.5.0.254 vlan5
ciscoasa(config)# dhcpd address 10.30.0.2-10.30.0.254 vlan30
ciscoasa(config)# dhcpd enable vlan5
ciscoasa(config)# dhcpd enable vlan30
```

Étape 4. Configurez les SSID du point d'accès, enregistrez la configuration et réinitialisez le module

Enfin, le point d'accès doit être configuré pour correspondre à la configuration de l'ASA. L'interface GUI du point d'accès vous permet de configurer des VLAN sur le point d'accès via le client connecté à l'interface interne ASA (Gigabit1/2). Cependant, si vous préférez utiliser CLI pour configurer le point d'accès via la session de console ASA, puis vous connecter sans fil pour gérer le point d'accès, vous pouvez utiliser cette configuration comme modèle pour créer deux SSID sur les VLAN 5 et 30. Ceci doit être entré dans la console du point d'accès en mode de configuration globale :

```
dot11 vlan-name VLAN30 vlan 30
dot11 vlan-name VLAN5 vlan 5
!
dot11 ssid SSID_VLAN30
   vlan 30
   authentication open
   mbssid guest-mode
!
dot11 ssid SSID_VLAN5
   vlan 5
   authentication open
   mbssid guest-mode
!
interface Dot11Radio0
 !
 ssid SSID_VLAN30
 !
 ssid SSID_VLAN5
 mbssid
```

```
!
interface Dot11Radio0.5
 encapsulation dot1Q 5
 bridge-group 5
 bridge-group 5 subscriber-loop-control
 bridge-group 5 spanning-disabled
 bridge-group 5 block-unknown-source
 no bridge-group 5 source-learning
 no bridge-group 5 unicast-flooding
!
interface Dot11Radio0.30
 encapsulation dot1Q 30
 bridge-group 30
 bridge-group 30 subscriber-loop-control
 bridge-group 30 spanning-disabled
 bridge-group 30 block-unknown-source
 no bridge-group 30 source-learning
 no bridge-group 30 unicast-flooding
!
interface Dot11Radio1
 !
 ssid SSID_VLAN30
 !
 ssid SSID_VLAN5
 mbssid
!
 interface Dot11Radio1.5
 encapsulation dot1Q 5
 bridge-group 5
 bridge-group 5 subscriber-loop-control
 bridge-group 5 spanning-disabled
 bridge-group 5 block-unknown-source
 no bridge-group 5 source-learning
 no bridge-group 5 unicast-flooding
!
interface Dot11Radio1.30
 encapsulation dot1Q 30
 bridge-group 30
 bridge-group 30 subscriber-loop-control
 bridge-group 30 spanning-disabled
 bridge-group 30 block-unknown-source
 no bridge-group 30 source-learning
 no bridge-group 30 unicast-flooding
!
interface GigabitEthernet0.5
 encapsulation dot1Q 5
 bridge-group 5
 bridge-group 5 spanning-disabled
 no bridge-group 5 source-learning
!
interface GigabitEthernet0.30
 encapsulation dot1Q 30
 bridge-group 30
 bridge-group 30 spanning-disabled
 no bridge-group 30 source-learning
!
interface BVI1
 ip address 10.1.0.254 255.255.255.0
ip default-gateway 10.1.0.1
!
interface Dot11Radio0
 no shut
```

```
!
interface Dot11Radio1
 no shut
```

À ce stade, la configuration de gestion de l'ASA et de l'AP doit être complète, et l'ASA agit comme un serveur DHCP pour les VLAN 5 et 30. Après avoir enregistré la configuration à l'aide de la commande
write memory sur l'AP, si vous avez toujours des problèmes de connectivité, vous devez recharger l'AP à l'aide de la commande reload de l'interface de ligne de commande. Cependant, si vous recevez une adresse IP sur les SSID nouvellement créés, aucune autre action n'est requise.

```
ap#write memory
Building configuration...
[OK]
ap#reload
Proceed with reload? [confirm]
Writing out the event log to flash:/event.log ...
```

> Remarque : vous n'avez PAS besoin de recharger l'intégralité du périphérique ASA. Vous ne devez recharger que le point d'accès intégré.

Une fois le rechargement du point d'accès terminé, vous devez avoir une connectivité à l'interface graphique du point d'accès à partir d'une machine cliente sur le réseau Wi-Fi ou interne. Il faut généralement environ deux minutes pour que l'AP redémarre complètement. À partir de ce moment, vous pouvez appliquer les étapes normales pour terminer la configuration du WAP.

Guide de démarrage rapide de la gamme Cisco ASA 5506-X

http://www.cisco.com/c/en/us/td/docs/security/asa/quick_start/5506X/5506x-quick-start.html#pgfId-138410

Dépannage

Le dépannage de la connectivité ASA n'est pas traité dans ce document, car il est destiné à la configuration initiale. Reportez-vous aux sections de vérification et de configuration pour vous assurer que toutes les étapes ont été correctement effectuées.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.