Configuración del ASA 5506W-X con una configuración de IP no predeterminada o de VLAN múltiple

Contenido

Introducción

Este documento describe cómo realizar la instalación y configuración inicial de un dispositivo Cisco Adaptive Security Appliance (ASA) 5506W-X cuando el esquema de direccionamiento IP predeterminado debe modificarse para que encaje en una red existente o si se necesitan varias

VLAN inalámbricas. Se requieren varios cambios de configuración al modificar las direcciones IP predeterminadas para acceder al punto de acceso inalámbrico (WAP), así como para garantizar que otros servicios (como DHCP) sigan funcionando según lo esperado. Además, este documento proporciona algunos ejemplos de configuración de CLI para el punto de acceso inalámbrico integrado (WAP) para facilitar la configuración inicial del WAP. Este documento se ha diseñado para complementar la guía de inicio rápido Cisco ASA 5506-X existente disponible en el sitio web de Cisco.

Prerequisites

Este documento sólo se aplica a la configuración inicial de un dispositivo Cisco ASA5506W-X que contiene un punto de acceso inalámbrico y solo tiene como objetivo abordar los diversos cambios necesarios cuando se modifica el esquema de direccionamiento IP existente o se agregan VLAN inalámbricas adicionales. Para las instalaciones de configuración predeterminadas, se debe hacer referencia a la Guía de inicio rápido ASA 5506-X existente.

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Dispositivo Cisco ASA 5506W-X
- Máquina cliente con un programa de emulación de terminal como Putty, SecureCRT, etc.
- Cable de consola y adaptador de terminal de PC serie (DB-9 a RJ-45)

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

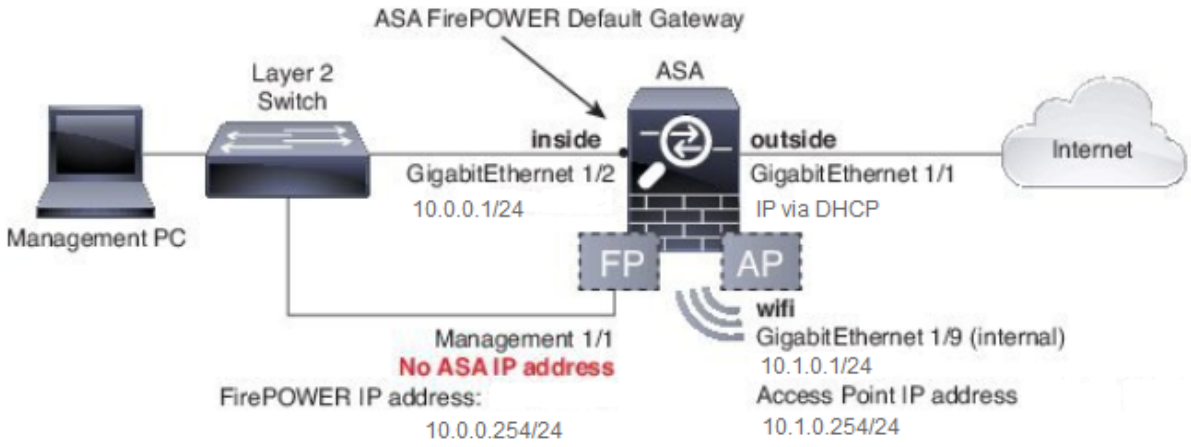
- Dispositivo Cisco ASA 5506W-X
- Máquina cliente con un programa de emulación de terminal como Putty, SecureCRT, etc.
- Cable de consola y adaptador de terminal de PC serie (DB-9 a RJ-45)
- Módulo FirePOWER ASA
- Punto de acceso inalámbrico Cisco Aironet 702i integrado (WAP integrado)

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.

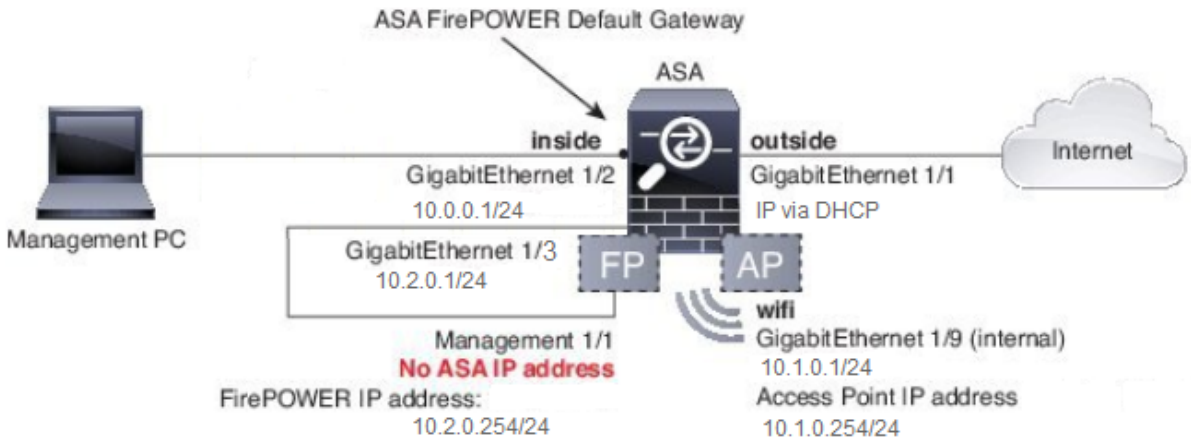
Diagramas de la Red

Como se muestra en esta imagen, ejemplos del direccionamiento IP que se aplicará en dos topologías diferentes:

ASA + FirePOWER con un switch interno:



ASA + FirePOWER sin switch interno:



Configurar

Estos pasos deben realizarse en orden después de encender y arrancar el ASA con el cable de consola conectado al cliente.

Paso 1. Modificar la configuración de IP de interfaz en ASA

Configure las interfaces interna (GigabitEthernet 1/2) y wifi (GigabitEthernet 1/9) para que tengan direcciones IP según sea necesario dentro del entorno existente. En este ejemplo, los clientes internos están en la red 10.0.0.1/24 y los clientes WIFI están en la red 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
```

Nota: Recibirá esta advertencia cuando cambie las direcciones IP de interfaz anteriores. Esto se espera.

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

Paso 2. Modificar la configuración del conjunto DHCP en interfaces internas y WiFi

Este paso es necesario si el ASA se va a utilizar como servidor DHCP en el entorno. Si se utiliza otro servidor DHCP para asignar direcciones IP a los clientes, DHCP se debe inhabilitar por completo en el ASA. Dado que ahora ha cambiado nuestro esquema de direccionamiento IP, debe modificar los rangos de direcciones IP existentes que el ASA proporciona a los clientes. Estos comandos crearán nuevos grupos para que coincidan con el nuevo rango de direcciones 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
```

Además, la modificación de los conjuntos DHCP desactivará el servidor DHCP anterior en el ASA y deberá volver a habilitarlo.

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

Si no cambia las direcciones IP de la interfaz antes de realizar los cambios DHCP, recibirá este error:

```
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
```

Paso 3. Especifique el servidor DNS que se pasará a los clientes DHCP internos y WiFI

Cuando asignan direcciones IP a través de DHCP, el servidor DHCP también debe asignar un servidor DNS a la mayoría de los clientes. Estos comandos configurarán el ASA para incluir el servidor DNS ubicado en 10.0.0.250 para todos los clientes. Debe sustituir 10.0.0.250 por un servidor DNS interno o un servidor DNS proporcionado por el ISP.

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

Paso 4. Modifique la configuración de acceso HTTP en el ASA para el acceso de Adaptive Security Device Manager (ASDM):

Dado que se ha cambiado el direccionamiento IP, el acceso HTTP al ASA también debe modificarse para que los clientes en las redes internas y WiFI puedan acceder a ASDM para administrar el 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
```

Nota: Esta configuración permite que cualquier cliente en las interfaces internas o wifi acceda al ASA a través de ASDM. Como práctica recomendada de seguridad, debe limitar el alcance de las direcciones únicamente a clientes de confianza.

Paso 5. Modificar IP de interfaz para la administración de punto de acceso en la consola WLAN (interfaz 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
```

Paso 6. Modificar gateway predeterminado en WAP

Este paso es necesario para que el WAP sepa dónde enviar todo el tráfico que no se origina en la subred local. Esto es necesario para proporcionar acceso a la GUI de WAP a través de HTTP desde un cliente en la interfaz interna de ASA.

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

Paso 7. Modificar la dirección IP de administración del módulo FirePOWER (opcional)

Si también planea implementar el módulo Cisco FirePOWER (también conocido como SFR), también debe cambiar su dirección IP para acceder desde la interfaz física Management1/1 en el ASA. Hay dos escenarios de implementación básicos que determinan cómo configurar el ASA y el módulo SFR:

1. Topología en la que la interfaz ASA Management1/1 está conectada a un switch interno (según la guía de inicio rápido normal)
2. Topología donde no hay un switch interno.

En función de su situación, estos son los pasos adecuados:

Si la interfaz ASA Management1/1 está conectada a un switch interno:

Puede iniciar sesión en el módulo y cambiarlo del ASA antes de conectarlo a un switch interno. Esta configuración le permite acceder al módulo SFR a través de IP colocándolo en la misma subred que la interfaz interna de ASA con una dirección IP de 10.0.0.254.

Las líneas en negrita son específicas de este ejemplo y se requieren para establecer la conectividad IP.

Las líneas en cursiva variarán según el entorno.

```
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.
```

> **Nota:** Puede tardar un par de minutos en aplicar la política de control de acceso predeterminada en el módulo SFR. Una vez que se haya completado, puede salir de la CLI del módulo SFR y volver al ASA presionando CTRL + MAYÚS + 6 +X (CTRL ^ X)

Si el ASA NO está conectado a un switch interno:

Es posible que en algunas implementaciones pequeñas no exista un switch interno. En este tipo de topología, los clientes generalmente se conectarían al ASA a través de la interfaz WiFi. En esta situación, es posible eliminar la necesidad de un switch externo y acceder al módulo SFR a través de una interfaz ASA independiente mediante la conexión cruzada de la interfaz Management1/1 a otra interfaz ASA física.

En este ejemplo, debe existir una conexión Ethernet física entre la interfaz ASA GigabitEthernet1/3 y la interfaz Management1/1. A continuación, configure el módulo ASA y SFR para que se encuentre en una subred independiente y, a continuación, pueda acceder al SFR tanto desde el ASA como desde los clientes ubicados en las interfaces internas o wifi.

Configuración de la interfaz 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
```

Configuración del Módulo 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.

> **Nota:** Puede tardar un par de minutos en aplicar la política de control de acceso predeterminada en el módulo SFR. Una vez que se haya completado, puede salir de la CLI del módulo SFR y volver al ASA presionando CTRL + MAYÚS + 6 +X (CTRL ^ X).

Una vez que se aplica la configuración SFR, debe poder hacer ping a la dirección IP de administración SFR desde el 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 no puede hacer ping a la interfaz correctamente, verifique la configuración y el estado de las conexiones ethernet físicas.

Paso 8. Conexión a la GUI de AP para habilitar radios y establecer otra configuración de WAP

En este momento, debe tener conectividad para administrar el WAP a través de la GUI HTTP, como se describe en la guía de inicio rápido. Deberá buscar la dirección IP de la interfaz BVI de WAP desde un navegador web de un cliente que está conectado a la red interna en el 5506W o puede aplicar la configuración de ejemplo y conectarse al SSID del WAP. Si no utiliza la CLI siguiente, debe conectar el cable Ethernet de su cliente a la interfaz Gigabit1/2 en el ASA.

Si prefiere utilizar la CLI para configurar el WAP, puede iniciar sesión en él desde el ASA y utilizar este ejemplo de configuración. Esto crea un SSID abierto con el nombre 5506W y 5506W_5Ghz para que pueda utilizar un cliente inalámbrico para conectarse y administrar aún más el WAP.

> **Nota:** Después de aplicar esta configuración, querrá acceder a la GUI y aplicar seguridad a los SSID para que el tráfico inalámbrico esté cifrado.

Configuración de WAP CLI para una sola VLAN inalámbrica con rangos IP modificados

```
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
```

A partir de este punto, puede realizar los pasos normales para completar la configuración del WAP y debe poder acceder desde el navegador web de un cliente conectado al SSID creado anteriormente. El nombre de usuario predeterminado del punto de acceso es Cisco con una contraseña de Cisco con una C mayúscula.

Guía de inicio rápido de Cisco ASA serie 5506-X

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

Debe utilizar la dirección IP 10.1.0.254 en lugar de la 192.168.10.2, como se indica en la Guía de inicio rápido.

Configuraciones

La configuración resultante debe coincidir con el resultado (suponiendo que haya utilizado los rangos IP de ejemplo, de lo contrario sustituya en consecuencia:

Configuración ASA

Interfaces:

Nota: Las líneas en cursiva sólo se aplican si NO tiene un switch interno:

```
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#
```

Configuración WAP Aironet (sin la configuración SSID de ejemplo)

```
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
```

Configuración del módulo FirePOWER (con switch interno)

```
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

>
```

Configuración del módulo FirePOWER (sin switch interno)

```
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

>
```

Verificación

Para verificar que tiene la conectividad adecuada con el WAP para completar el proceso de instalación:

1. Conecte el cliente de prueba a la interfaz interna de ASA y asegúrese de que recibe una dirección IP del ASA a través de DHCP que se encuentra dentro del rango de IP deseado.
2. Utilice un navegador web en su cliente para navegar a https://10.1.0.254 y verificar que la GUI de AP ahora está accesible.
3. Haga ping en la interfaz de administración SFR desde el cliente interno y el ASA para verificar la conectividad adecuada.

Configuración de DHCP con varias VLAN inalámbricas

La configuración asume que usted utiliza una sola VLAN inalámbrica. La interfaz virtual de puente (BVI) del punto de acceso inalámbrico puede proporcionar un puente para varias VLAN. Debido a la sintaxis para DHCP en el ASA, si desea configurar el 5506W como servidor DHCP para varias VLAN, necesita crear subinterfaces en la interfaz Gigabit1/9 y darle un nombre a cada una. Esta sección le guía a través del proceso de cómo quitar la configuración predeterminada y aplicar la configuración necesaria para configurar el ASA como servidor DHCP para varias VLAN.

Paso 1. Eliminar la configuración DHCP existente en Gig1/9

En primer lugar, elimine la configuración DHCP existente en la interfaz Gig1/9 (wifi):

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

Paso 2. Crear subinterfaces para cada VLAN en Gig1/9

Para cada VLAN que haya configurado en el punto de acceso, debe configurar una subinterfaz de Gig1/9. En este ejemplo de configuración, agrega dos subinterfaces:

-Gig1/9.5, que tendrá nameif vlan5, y corresponderá a VLAN 5 y subred 10.5.0.0/24.

-Gig1/9.30, que tendrá el nombre vlan30, y corresponderá a VLAN 30 y subred 10.3.0.0/24.

En la práctica, es esencial que la VLAN y la subred configuradas aquí coincidan con la VLAN y la subred especificadas en el punto de acceso. El nombre y el número de subinterfaz pueden ser cualquier cosa que elija. Consulte la guía de inicio rápido mencionada anteriormente para los links para configurar el punto de acceso usando la GUI 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
```

Paso 3. Designar un conjunto DHCP para cada VLAN

Cree un conjunto DHCP independiente para cada VLAN que se esté configurando. La sintaxis de este comando requiere que indique el nombre del que el ASA servirá al conjunto en cuestión. Un ejemplo visto en este ejemplo, que utiliza VLAN 5 y 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
```

Paso 4. Configure los SSID del punto de acceso, guarde la configuración y reinicie el módulo

Por último, el punto de acceso debe configurarse para que se corresponda con la configuración del ASA. La interfaz GUI para el punto de acceso le permite configurar las VLAN en el AP a través del cliente conectado al ASA dentro de la interfaz (Gigabit1/2). Sin embargo, si prefiere utilizar CLI para configurar el AP a través de la sesión de la consola ASA y luego conectarse de forma inalámbrica para administrar el AP, puede utilizar esta configuración como plantilla para crear dos SSID en las VLAN 5 y 30. Esto se debe ingresar dentro de la consola AP en el modo de configuración global:

```
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
```

En este punto, la configuración de administración del ASA y AP debe estar completa, y el ASA actúa como servidor DHCP para las VLAN 5 y 30. Después de guardar la configuración usando el comando ***write memory*** *en el AP, si todavía tiene problemas de conectividad, debe recargar el AP usando el comando* ***reload*** *de la CLI. Sin embargo, si recibe una dirección IP en los SSID recién creados, no se requiere ninguna otra acción.*

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

> **Nota:** NO es necesario que recargue todo el dispositivo ASA. Sólo debe recargar el punto de acceso integrado.

Una vez que el AP finaliza la recarga, debe tener conectividad con la GUI del AP desde una máquina cliente en la wifi o en las redes internas. Generalmente, el AP tarda unos dos minutos en reiniciarse completamente. A partir de este punto, puede aplicar los pasos normales para completar la configuración del WAP.

Guía de inicio rápido de Cisco ASA serie 5506-X

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

Troubleshoot

La solución de problemas de conectividad ASA está fuera del alcance de este documento, ya que está pensada para la configuración inicial. Consulte las secciones de verificación y configuración para asegurarse de que todos los pasos se han completado correctamente.