Configure el ASA 5506W-X con una configuración IP o del VLAN múltiple del no valor por defecto

Contenido

Introducción

Este documento describe cómo realizar la instalación inicial y la configuración de un dispositivo

adaptante 5506W-X del dispositivo de seguridad de Cisco (ASA) cuando el esquema de direccionamiento del IP predeterminado necesita ser modificado para caber en una red existente o si se requieren los VLAN inalámbricos múltiples. Hay varios cambios de configuración se requieren que al modificar los default IP Address para acceder el unto de acceso de red inalámbrica (WAP) así como asegurarse de que los otros servicios (tales como DHCP) continúan funcionando como se esperaba. Además, este documento proporciona algunos ejemplos de la configuración CLI para el unto de acceso de red inalámbrica integrado (WAP) para hacerlo más fácil completar la configuración inicial del WAP. Este documento se piensa para complementar la guía de inicio rápido existente de Cisco ASA 5506-X disponible en el sitio Web de Cisco.

Prerequisites

Este documento se aplica solamente a la configuración inicial de un dispositivo de Cisco ASA5506W-X que contenga un unto de acceso de red inalámbrica y se piense solamente dirigir los diversos cambios necesarios cuando usted modifica el esquema de IP Addressing existente o agrega los VLAN inalámbricos adicionales. Para las instalaciones de la configuración predeterminada, la guía de inicio rápido existente ASA 5506-X debe ser referida.

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Dispositivo de Cisco ASA 5506W-X
- Máquina del cliente con un programa de emulación de terminal tal como putty, SecureCRT, etc.
- Cable de la consola y adaptador del serial terminal de PC (DB-9 al RJ-45)

Componentes Utilizados

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

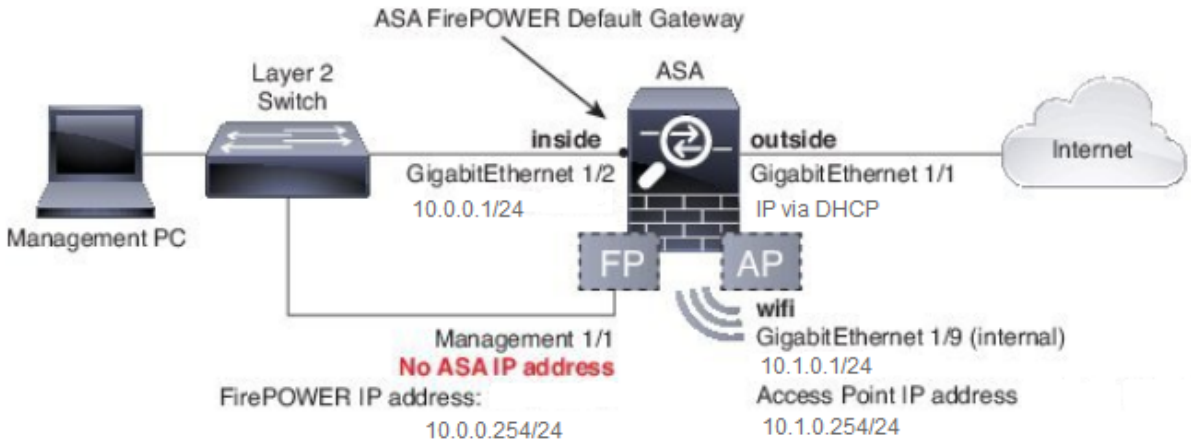
- Dispositivo de Cisco ASA 5506W-X
- Máquina del cliente con un programa de emulación de terminal tal como putty, SecureCRT, etc.
- Cable de la consola y adaptador del serial terminal de PC (DB-9 al RJ-45)
- Módulo ASA FirePOWER
- Unto de acceso de red inalámbrica integrado del Cisco Aironet 702i (accesorio WAP)

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

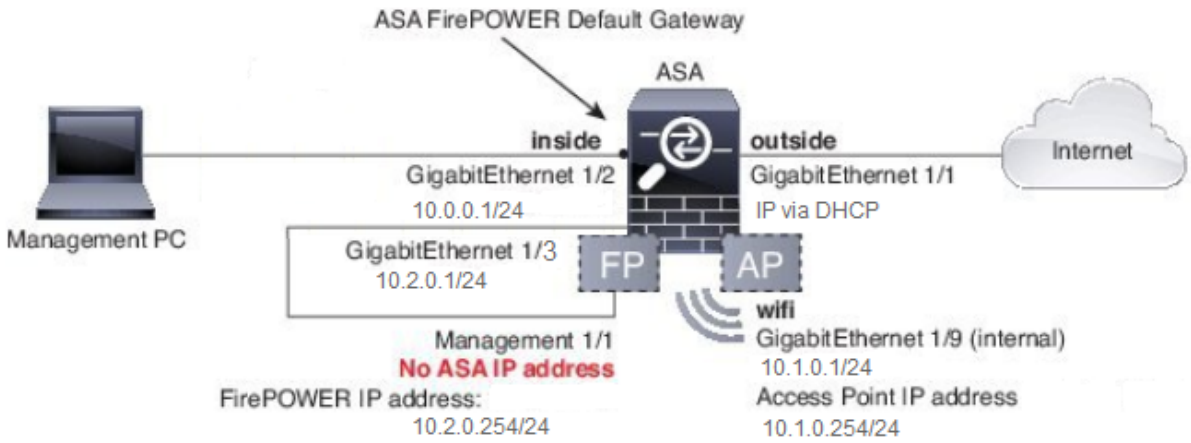
Diagramas de la Red

Tal y como se muestra en de esta imagen, ejemplos del IP Addressing que será aplicado en dos diversas topologías:

ASA + FirePOWER con un Switch del interior:



ASA + FirePOWER sin un Switch del interior:



Configurar

Estos pasos se deben realizar en la orden después de que usted accione encendido y inicie el ASA con el cable de la consola conectado con el cliente.

Paso 1. Modifique la configuración IP de la interfaz en el ASA

Configure el interior (gigabitethernet el 1/2) y las interfaces del wifi (gigabitethernet 1/9) para tener IP Addresses según las necesidades dentro del entorno existente. En este ejemplo, los clientes interiores están en las 10.0.0.1/24 redes y los clientes de 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
```

> **Note**: Usted conseguirá esta advertencia cuando usted cambia los IP Addresses antedichos de la interfaz. Se espera esto.

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

Paso 2. Modifique las configuraciones del agrupamiento DHCP en ambos interiores y las interfaces del wifi

Se requiere este paso si se va el ASA a ser utilizado como el servidor DHCP en el entorno. Si utilizan a otro servidor DHCP para asignar los IP Addresses a los clientes entonces el DHCP se debe inhabilitar en el ASA en conjunto. Puesto que usted ahora ha cambiado nuestro esquema de IP Addressing, usted necesita alterar los alcances del IP Address existentes a que el ASA está proporcionando a los clientes. Estos comandos crearán a los nuevos pools para hacer juego el nuevo alcance del IP Address:

```
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
```

También la modificación de los agrupamientos DHCP inhabilitará al servidor DHCP anterior en el ASA, y usted necesitará volverlo a permitir.

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

Si usted no cambia los IP Addresses de la interfaz antes de realizar los cambios del DHCP entonces usted 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 al servidor DNS para pasar a los clientes DHCP interiores y de WiFi

Cuando asignan los IP Addresses vía el DHCP, la mayoría de los clientes también necesitan ser asignados un servidor DNS por el servidor DHCP. Estos comandos configurarán el ASA para incluir al servidor DNS situado en 10.0.0.250 a todos los clientes. Usted necesita substituir 10.0.0.250 para un servidor DNS interno o un servidor DNS proporcionado por su 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 del acceso HTTP en el ASA para el acceso adaptante del Administrador de dispositivos de seguridad (ASDM):

Puesto que se ha cambiado el IP Addressing, acceso HTTP ASA a las necesidades también de ser modificado de modo que los clientes en las redes interiores y de WiFi puedan acceder el ASDM para manejar 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
```

> **Note**: Esta configuración permite que cualquier cliente en las interfaces interiores o del wifi acceda el ASA vía el ASDM. Como mejor práctica de la Seguridad, usted debe limitar el alcance de los direccionamientos a los clientes de confianza solamente.

Paso 5. Modifique el IP de la interfaz para la Administración del Punto de acceso en la consola de la red inalámbrica (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. Modifique el gateway predeterminado en el WAP

Se requiere este paso de modo que el WAP sepa dónde enviar todo el tráfico que no se origine en la subred local. Esto se requiere para proporcionar para acceder el WAP GUI vía el HTTP de un cliente en la interfaz interior ASA.

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

Paso 7. Modifique el IP Address de administración del módulo de FirePOWER (opcional)

Si usted también planea desplegar el módulo de Cisco FirePOWER (también conocido como SFR) entonces usted también necesita cambiar su dirección IP para accederla de la interfaz física Management1/1 en el ASA. Hay dos escenarios de instrumentación básicos que determinan cómo configurar el ASA y el módulo SFR:

1. Una topología en la cual la interfaz ASA Management1/1 está conectada con un Switch del interior (según la guía de inicio rápido normal)
2. Una topología donde no está presente un Switch del interior.

Dependiendo de su escenario, éstos son los pasos apropiados:

Si la interfaz ASA Management1/1 está conectada con un Switch del interior:

Usted puede sesión en el módulo y cambiarlo del ASA antes de conectarlo con un Switch del interior. Esta configuración permite que usted acceda el módulo SFR vía el IP colocándolo en la misma subred como la interfaz interior ASA con una dirección IP de 10.0.0.254.

Las líneas en intrépido son específicas a este ejemplo y se requieren para establecer la conectividad del IP.

Las líneas en los itálicos variarán por 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.
```

> **Note**: Puede tardar los minutos de un par para que la directiva predeterminada del control de acceso se aplique en el módulo SFR. Una vez que es completa, usted puede escapar el módulo CLI de los SFR y nuevamente dentro del ASA presionando el CTRL + el MAYÚS + 6 +X (^ del CTRL X)

Si el ASA no está conectado con un Switch del interior:

Un Switch del interior puede no existir en algunas pequeñas implementaciones. En este tipo de topología, los clientes conectarían generalmente con el ASA vía la interfaz de WiFi. En este escenario, es posible elimina la necesidad de un switch externo y accede el módulo SFR vía una interfaz separada ASA cruz-conectando la interfaz Management1/1 con otra interfaz física ASA.

En este ejemplo, una conexión de Ethernet física debe existir entre la interfaz ASA GigabitEthernet1/3 y la interfaz Management1/1. Después, usted configura el módulo ASA y SFR

para estar en una subred distinta y entonces usted puede acceder el SFR del ASA así como de los clientes situados en las interfaces interiores o del 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 de módulos 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.
```

> **Note**: Puede tardar los minutos de un par para que la directiva predeterminada del control de acceso se aplique en el módulo SFR. Una vez que es completa, usted puede escapar el módulo CLI de los SFR y nuevamente dentro del ASA presionando el CTRL + el MAYÚS + 6 +X (^ del CTRL X).

Una vez que la configuración SFR se aplica, usted debe poder hacer ping el IP Address de administración SFR del 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 usted no puede hacer ping la interfaz con éxito, verifique la configuración y el estado de las conexiones de Ethernet físicas.

Paso 8. Conecte con AP GUI para habilitar las radios y para fijar la otra configuración WAP

En este momento usted debe tener Conectividad para manejar el WAP vía el HTTP GUI como se debate en la guía de inicio rápido. Usted cualquier necesidad de hojear a la dirección IP de la interfaz BVI WAP de un buscador Web de un cliente que esté conectado con la red interna en el 5506W o usted puede aplicar el ejemplo de configuración y conectar con el SSID del WAP. Si usted no utiliza el CLI abajo, usted necesita enchufar el cable Ethernet de su cliente a la interfaz Gigabit1/2 en el ASA.

Si usted prefiere utilizar el CLI para configurar el WAP, usted puede sesión en ella del ASA y utilizar este ejemplo de configuración. Esto crea un SSID abierto con el nombre de 5506W y de 5506W_5Ghz de modo que usted pueda utilizar a un cliente de red inalámbrica para conectar con y para manejar más lejos el WAP.

> **Note**: Después de aplicar esta configuración usted querrá acceder el GUI y aplicar la Seguridad a los SSID para cifrar el tráfico de red inalámbrica.

Configuración CLI WAP para un solo VLAN inalámbrico usando los intervalos de direcciones 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
```

Desde aquí, usted puede realizar los pasos normales para completar la configuración del WAP y usted debe poder accederlo del buscador Web de un cliente conectado con el SSID arriba creado. El nombre de usuario predeterminado del Punto de acceso es Cisco con una contraseña de Cisco con un C capital.

Guía de inicio rápido de las 5506-X Series de Cisco ASA

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

Usted necesita utilizar la dirección IP de 10.1.0.254 en vez de 192.168.10.2 como se afirma en la guía de inicio rápido.

Configuraciones

La configuración resultante debe hacer juego la salida (si se asume que le utilizó los intervalos de direcciones IP, si no el substituto del ejemplo por consiguiente:

Configuración ASA

Interfaces:

Note: Las líneas en los itálicos se aplican solamente si usted no tiene un Switch del interior:

```
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 del Aironet WAP (sin los config del ejemplo 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
```

Configuración de módulos de FirePOWER (con el Switch del interior)

```
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 de módulos de FirePOWER (sin el Switch del interior)

```
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 usted tenga la conectividad apropiada al WAP para completar el proceso de instalación:

1. Conecte a su probar cliente con la interfaz interior ASA y asegúrese de que recibe una dirección IP del ASA vía el DHCP que está dentro del intervalo de direcciones IP deseado.
2. Utilice a un buscador Web en su cliente para navegar a https://10.1.0.254 y verificar que el AP GUI es accesible ahora.
3. Haga ping la interfaz de administración SFR del cliente interior y del ASA para verificar la conectividad apropiada.

Configure el DHCP con los VLAN inalámbricos múltiples

La configuración asume que usted utiliza un solo VLAN inalámbrico. El (BVI) del Interfaz Virtual de Bridge en la Tecnología inalámbrica AP puede proporcionar un Bridge para los VLAN múltiples. Debido al sintaxis para el DHCP en el ASA, si usted desea configurar el 5506W como servidor DHCP para los VLAN múltiples, usted necesita crear las subinterfaces en la interfaz Gigabit1/9 y dar cada un nombre. Esta sección le dirige con el proceso de cómo quitar la configuración predeterminada y aplicar la configuración necesaria configurar el ASA como servidor DHCP para los VLAN múltiples.

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

Primero, quite 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. Cree las subinterfaces para cada VLA N en Gig1/9

Para cada VLA N que usted ha configurado en el Punto de acceso, usted necesita configurar una subinterfaz de Gig1/9. En este ejemplo de configuración, usted agrega dos subinterfaces:

-Gig1/9.5, que tendrá nameif vlan5, y corresponderá al VLA N 5 y a la subred 10.5.0.0/24.

-Gig1/9.30, que tendrá nameif vlan30, y corresponderá al VLAN 30 y a la subred 10.3.0.0/24.

En la práctica, es esencial que el VLA N y la subred configurados aquí hacen juego el VLA N y la subred especificados en el Punto de acceso. El nameif y el número de la subinterfaz pueden ser cualquier cosa que usted elige. Refiera por favor a la guía de inicio rápido mencionada previamente para los links para configurar el Punto de acceso usando la red GUI.

```
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. Señale a un agrupamiento DHCP para cada VLA N

Cree a un agrupamiento DHCP separado para cada VLA N que es configurado. El sintaxis para este comando requiere que usted enumere el nameif fuera de las cuales el ASA servirá el pool en la pregunta. Visto en este ejemplo, que utiliza los VLA N 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 el Punto de acceso SSID, salve los config, y reajuste el módulo

Finalmente, el Punto de acceso necesita ser configurado para corresponder a la configuración ASA. La interfaz GUI para el Punto de acceso permite que usted configure los VLA N en el AP vía el cliente conectado con la interfaz del interior ASA (Gigabit1/2). Sin embargo, si usted prefiere utilizar el CLI para configurar el AP vía la sesión de consola ASA y después para conectar sin hilos para manejar el AP, usted puede utilizar esta configuración como plantilla para crear dos SSID en los VLA N 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 momento, la configuración de la administración del ASA y el AP deben ser completos, y el ASA actúa como servidor DHCP para los VLA N 5 y 30. Después de guardar la configuración usando el ***comando write memory*** *en el AP, si usted todavía tiene problemas de conectividad entonces usted debe recargar el AP usando el* ***comando reload del*** *CLI. Sin embargo, si usted recibe una dirección IP en los SSID creados recientemente entonces 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 ...
```

> **Note**: Usted no necesita recargar el dispositivo entero ASA. Usted debe recargar solamente el Punto de acceso incorporado.

Una vez que el AP acaba de recargar, después usted debe tener Conectividad al AP GUI de una máquina del cliente en el wifi o las redes internas. Tarda generalmente cerca de dos minutos para que el AP reinicie totalmente. Desde aquí, usted puede aplicar los pasos normales para completar la configuración del WAP.

Guía de inicio rápido de las 5506-X Series de Cisco ASA

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

Troubleshooting

Resolver problemas la Conectividad ASA está fuera del ámbito de este documento puesto que esto se piensa para la configuración inicial. Refiera por favor al verificar y a las secciones de configuración para asegurarse de que todos los pasos se han completado correctamente.