기본값이 아닌 IP 또는 다중 VLAN 컨피그레이션으로 ASA 5506W-X 구성

목차

소개

이 문서에서는 기존 네트워크에 맞게 기본 IP 주소 지정 체계를 수정해야 하거나 여러 무선 VLAN이 필요한 경우 Cisco ASA(Adaptive Security Appliance) 5506W-X 디바이스의 초기 설치 및 컨피그레이션을 수행하는 방법에 대해 설명합니다. WAP(무선 액세스 포인트)에 액세스하기 위해 기본 IP 주소를 수정할 때 필요한 몇 가지 컨피그레이션 변경 사항이 있으며, DHCP와 같은 다른 서비스가 예상대로 계속 작동합니다. 또한 이 문서에서는 WAP의 초기 구성을 보다 쉽게 완료할 수 있도록 WAP(Integrated Wireless Access Point)에 대한 몇 가지 CLI 구성 예를 제공합니다. 이 문서는

Cisco 웹 사이트에서 사용할 수 있는 기존 Cisco ASA 5506-X 빠른 시작 가이드를 보완하기 위한 것입니다.

사전 요구 사항

이 문서는 무선 액세스 포인트가 포함된 Cisco ASA5506W-X 디바이스의 초기 컨피그레이션에만 적용되며, 기존 IP 주소 지정 체계를 수정하거나 무선 VLAN을 추가할 때 필요한 다양한 변경 사항만 해결하도록 설계되었습니다. 기본 컨피그레이션 설치의 경우 기존 ASA 5506-X 빠른 시작 가이드를 참조해야 합니다.

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco ASA 5506W-X 장치
- Putty, SecureCRT 등과 같은 터미널 에뮬레이션 프로그램이 있는 클라이언트 시스템
- 콘솔 케이블 및 직렬 PC 터미널 어댑터(DB-9 - RJ-45)

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

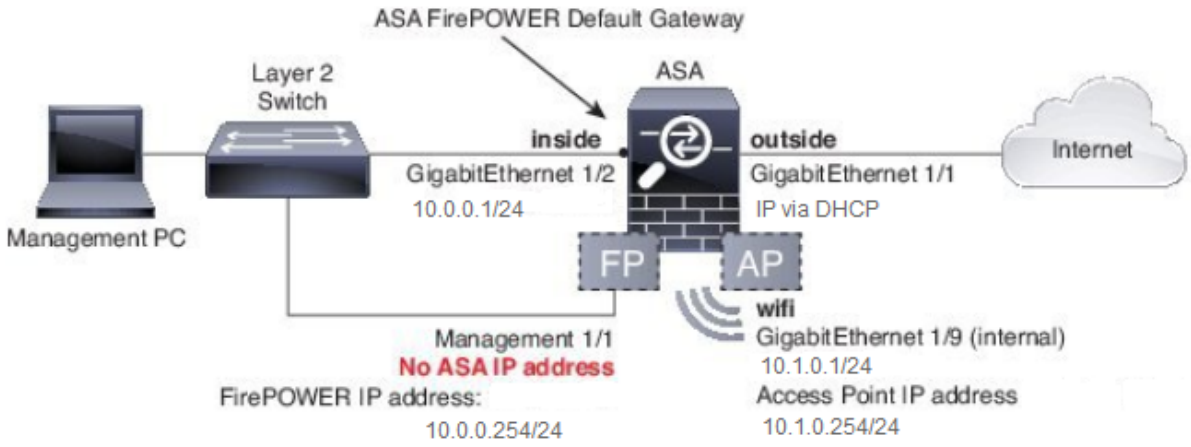
- Cisco ASA 5506W-X 장치
- Putty, SecureCRT 등과 같은 터미널 에뮬레이션 프로그램이 있는 클라이언트 시스템
- 콘솔 케이블 및 직렬 PC 터미널 어댑터(DB-9 - RJ-45)
- ASA FirePOWER 모듈
- 통합 Cisco Aironet 702i 무선 액세스 포인트(내장형 WAP)

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

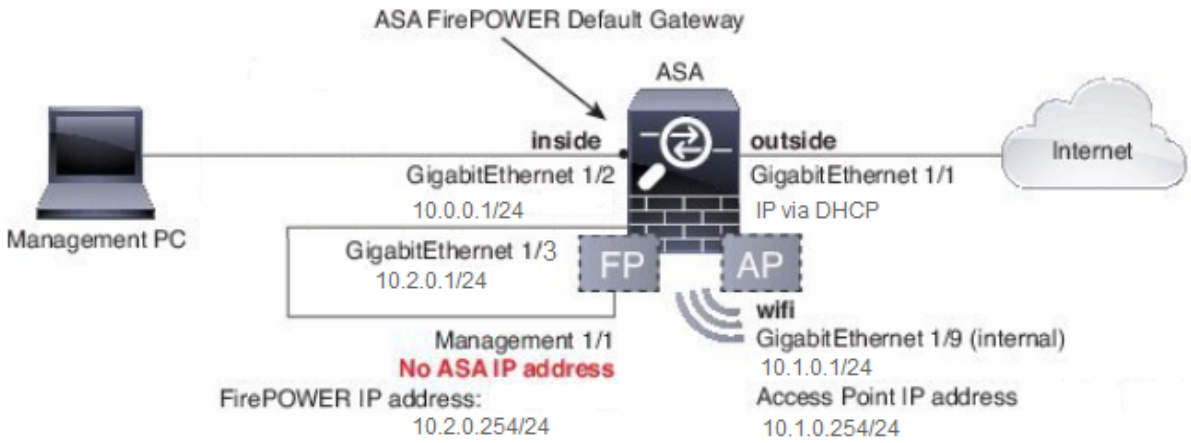
네트워크 다이어그램

이 이미지에 표시된 것처럼, 두 가지 다른 토폴로지에 적용될 IP 주소 지정의 예는 다음과 같습니다.

내부 스위치가 있는 ASA + FirePOWER:



내부 스위치가 없는 ASA + FirePOWER:



구성

이러한 단계는 전원을 켜고 클라이언트에 연결된 콘솔 케이블을 사용하여 ASA를 부팅한 후에 수행해야 합니다.

1단계. ASA에서 인터페이스 IP 컨피그레이션 수정

내부(GigabitEthernet 1/2) 및 wifi(GigabitEthernet 1/9) 인터페이스를 구성하여 기존 환경에서 필요에 따라 IP 주소를 사용할 수 있습니다. 이 예에서 내부 클라이언트는 10.0.0.1/24 네트워크에 있으며 WIFI 클라이언트는 10.1.0.1/24 네트워크에 있습니다.

```
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
```

참고:위의 인터페이스 IP 주소를 변경하면 이 경고가 표시됩니다. 예상된 일입니다.

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

2단계. 내부 및 wifi 인터페이스 모두에서 DHCP 풀 설정을 수정합니다.

ASA를 환경에서 DHCP 서버로 사용하려면 이 단계가 필요합니다. 다른 DHCP 서버를 사용하여 클라이언트에 IP 주소를 할당하는 경우 ASA에서 DHCP를 완전히 비활성화해야 합니다. 이제 IP 주소 지정 체계를 변경했으므로 ASA가 클라이언트에 제공하는 기존 IP 주소 범위를 변경해야 합니다. 다음 명령은 새 IP 주소 범위와 일치하는 새 풀을 생성합니다.

```
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
```

또한 DHCP 풀을 수정하면 ASA의 이전 DHCP 서버가 비활성화되며 다시 활성화해야 합니다.

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

DHCP를 변경하기 전에 인터페이스 IP 주소를 변경하지 않으면 다음 오류가 발생합니다.

```
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
```

3단계. 내부 및 WiFI DHCP 클라이언트에 전달할 DNS 서버를 지정합니다.

DHCP를 통해 IP 주소를 할당할 때 대부분의 클라이언트에는 DHCP 서버에서 DNS 서버를 할당해야 합니다. 이러한 명령은 10.0.0.250에 있는 DNS 서버를 모든 클라이언트에 포함하도록 ASA를 구성합니다. 10.0.0.250은 ISP에서 제공하는 내부 DNS 서버 또는 DNS 서버로 대체해야 합니다.

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

4단계. ASDM(Adaptive Security Device Manager) 액세스를 위해 ASA에서 HTTP 액세스 컨피그레이션을 수정합니다.

IP 주소 지정이 변경되었으므로 내부 및 WiFI 네트워크의 클라이언트가 ASA를 관리하기 위해 ASDM에 액세스할 수 있도록 ASA에 대한 HTTP 액세스도 수정해야 합니다.

```
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
```

> **참고:**이 컨피그레이션을 사용하면 내부 또는 wifi 인터페이스의 모든 클라이언트가 ASDM을 통해 ASA에 액세스할 수 있습니다. 보안 모범 사례로서, 주소의 범위를 신뢰할 수 있는 클라이언트로만 제한해야 합니다.

5단계. WLAN 콘솔(인터페이스 BVI1)에서 액세스 포인트 관리를 위한 인터페이스 IP 수정:

```
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
```

6단계. WAP에서 기본 게이트웨이 수정

WAP가 로컬 서브넷에서 시작되지 않은 모든 트래픽을 전송할 위치를 파악하려면 이 단계가 필요합니다. 이는 ASA 내부 인터페이스의 클라이언트에서 HTTP를 통해 WAP GUI에 액세스하는 데 필요합니다.

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

7단계. FirePOWER 모듈 관리 IP 주소 수정(선택 사항)

또한 Cisco FirePOWER(SFR이라고도 함) 모듈을 구축하려는 경우 ASA의 물리적 Management1/1 인터페이스에서 액세스하기 위해 해당 IP 주소도 변경해야 합니다.ASA 및 SFR 모듈을 구성하는 방법을 결정하는 두 가지 기본 구축 시나리오가 있습니다.

1. ASA Management1/1 인터페이스가 내부 스위치에 연결된 토폴로지(일반 빠른 시작 설명서에 따라)
2. 내부 스위치가 없는 토폴로지.

시나리오에 따라 다음 단계가 적절합니다.

ASA Management1/1 인터페이스가 내부 스위치에 연결된 경우:

내부 스위치에 연결하기 전에 모듈에 세션을 시작하고 ASA에서 변경할 수 있습니다. 이 컨피그레이션을 사용하면 IP 주소가 10.0.0.254인 ASA 내부 인터페이스와 동일한 서브넷에 배치하여 IP를 통해 SFR 모듈에 액세스할 수 있습니다.

굵게 표시된 줄은 이 예와 관련이 있으며 IP 연결을 설정하는 데 필요합니다.

기울임꼴로 된 선은 환경에 따라 달라집니다.

```
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.
```

> **참고:**기본 액세스 제어 정책이 SFR 모듈에 적용되는 데 몇 분 정도 걸릴 수 있습니다. 완료되면 Ctrl + Shift + 6 +X(Ctrl^ X)를 눌러 SFR 모듈 CLI에서 벗어나 ASA로 다시 이동할 수 있습니다.

ASA가 내부 스위치에 연결되지 않은 경우:

일부 소규모 구축에는 내부 스위치가 없을 수 있습니다. 이 토폴로지 유형에서 클라이언트는 일반적으로 WiFi 인터페이스를 통해 ASA에 연결됩니다. 이 시나리오에서는 Management1/1 인터페이스를 다른 물리적 ASA 인터페이스에 교차 연결하여 외부 스위치가 필요하지 않고 별도의 ASA 인터페이스를 통해 SFR 모듈에 액세스할 수 있습니다.

이 예에서는 ASA GigabitEthernet1/3 인터페이스와 Management1/1 인터페이스 사이에 물리적 이더넷 연결이 있어야 합니다. 다음으로, ASA 및 SFR 모듈이 별도의 서브넷에 있도록 구성한 다음 ASA와 내부 또는 wifi 인터페이스에 있는 클라이언트 모두에서 SFR에 액세스할 수 있습니다.

ASA 인터페이스 구성:

```
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
```

SFR 모듈 구성:

```
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.

> **참고:**기본 액세스 제어 정책이 SFR 모듈에 적용되는 데 몇 분 정도 걸릴 수 있습니다. 완료되면 Ctrl + Shift + 6 +X(Ctrl^ X)를 눌러 SFR 모듈 CLI에서 벗어나 ASA로 다시 이동할 수 있습니다.

SFR 컨피그레이션이 적용되면 ASA에서 SFR 관리 IP 주소를 ping할 수 있어야 합니다.

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#
```

인터페이스를 성공적으로 ping할 수 없는 경우 물리적 이더넷 연결의 컨피그레이션 및 상태를 확인합니다.

8단계. AP GUI에 연결하여 무선 장치를 활성화하고 다른 WAP 컨피그레이션을 설정합니다.

이 시점에서 빠른 시작 가이드에서 설명한 대로 HTTP GUI를 통해 WAP를 관리할 수 있는 연결이 있어야 합니다. 5506W에서 내부 네트워크에 연결된 클라이언트의 웹 브라우저에서 WAP BVI 인터페이스의 IP 주소를 찾아보거나, 예제 컨피그레이션을 적용하고 WAP의 SSID에 연결할 수 있습니다. 아래 CLI를 사용하지 않는 경우 클라이언트에서 ASA의 Gigabit1/2 인터페이스에 이더넷 케이블을 연결해야 합니다.

CLI를 사용하여 WAP를 구성하려는 경우 ASA에서 CLI로 세션을 시작하고 이 예제 컨피그레이션을 사용할 수 있습니다.이렇게 하면 5506W 및 5506W_5Ghz라는 이름의 개방형 SSID가 생성되므로 무선 클라이언트를 사용하여 WAP에 연결하고 더 자세히 관리할 수 있습니다.

> **참고:**이 컨피그레이션을 적용한 후 무선 트래픽이 암호화되도록 GUI에 액세스하고 SSID에 보안을 적용할 수 있습니다.

수정된 IP 범위를 사용하는 단일 무선 VLAN에 대한 WAP CLI 구성

```
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
```

이 시점부터 일반적인 단계를 수행하여 WAP 컨피그레이션을 완료할 수 있으며 위에서 생성한 SSID에 연결된 클라이언트의 웹 브라우저에서 WAP에 액세스할 수 있어야 합니다. 액세스 포인트의 기본 사용자 이름은 Cisco이고 Cisco의 비밀번호가 대문자 C입니다.

Cisco ASA 5506-X Series 빠른 시작 가이드

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

빠른 시작 설명서에 명시된 192.168.10.2 대신 10.1.0.254의 IP 주소를 사용해야 합니다.

구성

결과 컨피그레이션은 출력과 일치해야 합니다(예: IP 범위를 사용했다고 가정하고, 그렇지 않으면 그에 따라 대체합니다.

ASA 컨피그레이션

인터페이스:

참고:기울임꼴로 표시된 줄은 내부 스위치가 없는 경우에만 적용됩니다.

```
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#
```

Aironet WAP 컨피그레이션(예 SSID 컨피그레이션 없음)

```
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
```

FirePOWER 모듈 구성(내부 스위치 포함)

```
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

>
```

FirePOWER 모듈 구성(내부 스위치 제외)

```
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

>
```

다음을 확인합니다.

설치 프로세스를 완료하기 위해 WAP에 올바르게 연결되었는지 확인하려면 다음을 수행합니다.

1. 테스트 클라이언트를 ASA 내부 인터페이스에 연결하고 원하는 IP 범위 내에 있는 DHCP를 통해 ASA에서 IP 주소를 수신하는지 확인합니다.
2. 클라이언트에서 웹 브라우저를 사용하여 https://10.1.0.254으로 이동하고 AP GUI에 액세스할 수 있는지 확인합니다.
3. 내부 클라이언트와 ASA에서 SFR 관리 인터페이스를 ping하여 올바른 연결을 확인합니다.

여러 무선 VLAN으로 DHCP 구성

컨피그레이션에서는 단일 무선 VLAN을 사용하는 것으로 가정합니다.무선 AP의 BVI(Bridge Virtual Interface)는 여러 VLAN에 대한 브리지를 제공할 수 있습니다.ASA에서 DHCP의 구문 때문에, 5506W를 여러 VLAN에 대한 DHCP 서버로 구성하려면 Gigabit1/9 인터페이스에 하위 인터페이스를 생성하고 각 인터페이스에 이름을 지정해야 합니다.이 섹션에서는 기본 컨피그레이션을 제거하고 ASA를 여러 VLAN에 대한 DHCP 서버로 설정하는 데 필요한 컨피그레이션을 적용하는 프로세스를 안내합니다.

1단계. Gig1/9에서 기존 DHCP 컨피그레이션 제거

먼저 Gig1/9(wifi) 인터페이스에서 기존 DHCP 컨피그레이션을 제거합니다.

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

2단계. Gig1/9의 각 VLAN에 대한 하위 인터페이스 생성

액세스 포인트에 구성한 각 VLAN에 대해 Gig1/9의 하위 인터페이스를 구성해야 합니다. 이 예제 컨피그레이션에서는 두 개의 하위 인터페이스를 추가합니다.

-Gig1/9.5 - nameif vlan5가 있으며 VLAN 5 및 서브넷 10.5.0.0/24에 해당합니다.

-Gig1/9.30 - nameif vlan30이 있으며 VLAN 30 및 서브넷 10.3.0.0/24에 해당합니다.

실제로 여기에 구성된 VLAN 및 서브넷이 액세스 포인트에 지정된 VLAN 및 서브넷과 일치해야 합니다.nameif 및 하위 인터페이스 번호는 사용자가 선택하는 모든 것이 될 수 있습니다. 웹 GUI를 사용하여 액세스 포인트를 구성하려면 앞서 설명한 링크에서 빠른 시작 설명서를 참조하십시오.

```
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
```

3단계. 각 VLAN에 대해 DHCP 풀을 지정합니다.

구성할 각 VLAN에 대해 별도의 DHCP 풀을 생성합니다.이 명령의 구문은 ASA에서 문제의 풀을 서비스할 nameif를 나열해야 합니다.VLAN 5 및 30을 사용하는 이 예에서 볼 수 있는 것:

```
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
```

4단계. 액세스 포인트 SSID를 구성하고, 컨피그레이션을 저장하고, 모듈을 재설정합니다.

마지막으로, ASA의 컨피그레이션에 대응하도록 액세스 포인트를 구성해야 합니다.액세스 포인트의 GUI 인터페이스를 사용하면 ASA 내부(Gigabit1/2) 인터페이스에 연결된 클라이언트를 통해 AP에서 VLAN을 구성할 수 있습니다.그러나 CLI를 사용하여 ASA 콘솔 세션을 통해 AP를 구성한 다음 무선으로 연결하여 AP를 관리하려는 경우 이 컨피그레이션을 템플릿으로 사용하여 VLAN 5와 30에서 2개의 SSID를 생성할 수 있습니다. 이 컨피그레이션은 글로벌 컨피그레이션 모드의 AP 콘솔 내에서 입력해야 합니다.

```
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
```

이 시점에서 ASA 및 AP의 관리 컨피그레이션이 완료되어야 하며 ASA는 VLAN 5 및 30에 대한 DHCP 서버 역할을 합니다. AP에서 write memory 명령을 사용하여 컨피그레이션을 저장한 후 연결 문제가 여전히 있는 경우 CLI에서 reload 명령을 사용하여 AP를 다시 로드해야 합니다. 그러나 새로 생성된 SSID에서 IP 주소를 수신하는 경우 추가 작업이 필요하지 않습니다.

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

> **참고:**전체 ASA 디바이스를 다시 로드할 필요가 없습니다.기본 제공 액세스 포인트만 다시 로드해야 합니다.

AP의 재로드가 완료되면 wifi 또는 내부 네트워크의 클라이언트 시스템에서 AP GUI에 연결해야 합니다. 일반적으로 AP가 완전히 재부팅되는 데 약 2분이 걸립니다. 이 단계에서 일반적인 단계를 적용하여 WAP 컨피그레이션을 완료할 수 있습니다.

Cisco ASA 5506-X Series 빠른 시작 가이드

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

문제 해결

ASA 연결 트러블슈팅은 초기 컨피그레이션을 위한 것이므로 이 문서의 범위를 벗어납니다. 모든 단계가 올바르게 완료되었는지 확인하려면 verify 및 configuration 섹션을 참조하십시오.