De ASA 5506W-X configureren met een niet-standaard IP of meerdere VLAN-configuratie

Inhoud

Inleiding

Dit document beschrijft hoe u de eerste installatie en configuratie van een Cisco adaptieve security applicatie (ASA) 5506W-X apparaat kunt uitvoeren wanneer de standaard IP-adresseringsregeling moet worden aangepast om in een bestaand netwerk te passen of wanneer er meerdere draadloze VLAN's vereist zijn. Er zijn verschillende configuratieveranderingen nodig die bij het wijzigen van de standaard IP-adressen nodig zijn om toegang te krijgen tot het

draadloze access point (WAP) en om te verzekeren dat andere services (zoals DHCP) blijven functioneren zoals verwacht. Daarnaast biedt dit document een aantal CLI-configuratievoorbeelden voor het geïntegreerde draadloze access point (WAP) om het makkelijker te maken om de initiële configuratie van de WAP te voltooien. Dit document is bedoeld om de bestaande Cisco ASA 5506-X Quick Start gids beschikbaar op de Cisco website aan te vullen.

Voorwaarden

Dit document is alleen van toepassing op de initiële configuratie van een Cisco ASA 5506W-X apparaat dat een draadloos access point bevat en alleen bedoeld is om de verschillende benodigde veranderingen aan te pakken wanneer u het bestaande IP-adresseringsschema wijzigt of extra draadloze VLAN's toevoegt. Voor standaardinstellingen dient de bestaande ASA 5506-X Quick Start Guide te worden geraadpleegd.

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco ASA 5506W-X apparaat
- Clientmachine met een terminalemulatieprogramma zoals Poetin, SecureCRT, enz.
- Console Cable and Serial PC Terminal Adapter (DB-9 tot RJ-45)

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

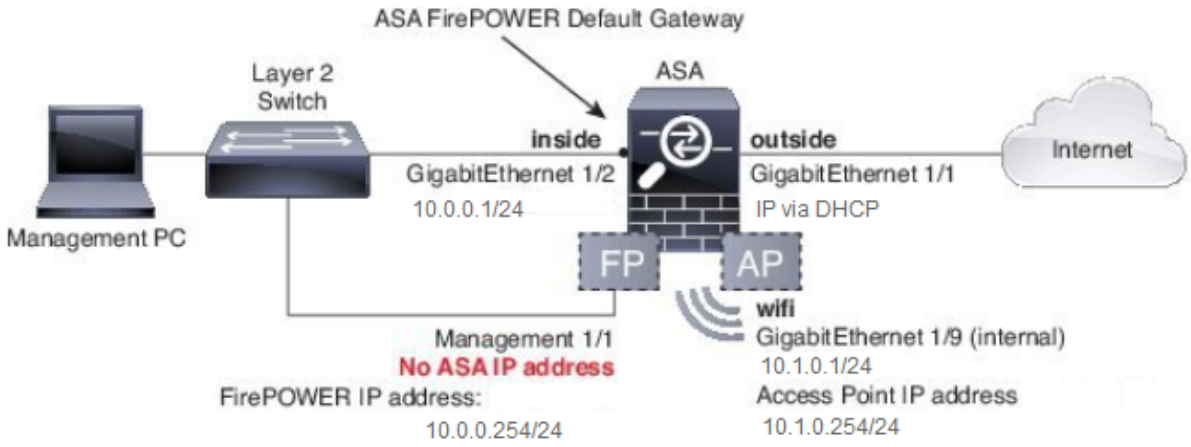
- Cisco ASA 5506W-X apparaat
- Clientmachine met een terminalemulatieprogramma zoals Poetin, SecureCRT, enz.
- Console Cable and Serial PC Terminal Adapter (DB-9 tot RJ-45)
- ASA FirePOWER-module
- Geïntegreerd Cisco Aironet 702i draadloos access point (ingebouwde WAP)

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

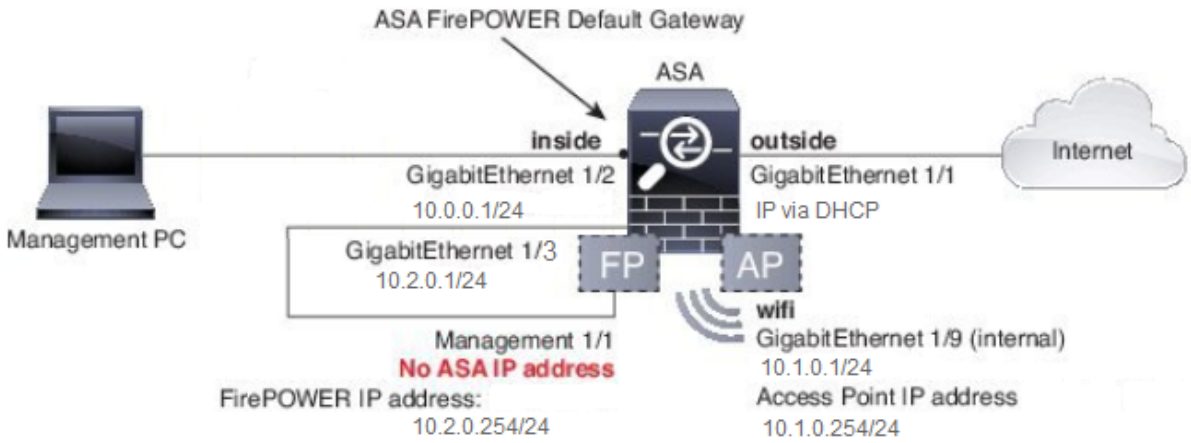
Netwerkdiagrammen

Zoals in dit beeld wordt getoond, zullen voorbeelden van IP-adressering die in twee verschillende topologieën zullen worden toegepast:

ASA + FirePOWER met een binnenschakelaar:



ASA + FirePOWER zonder binnenschakelaar:



Configureren

Deze stappen moeten worden uitgevoerd nadat u de ASA hebt ingeschakeld en de ASA hebt gestart met de console-kabel die is aangesloten op de client.

Stap 1. Wijzig de IP-configuratie van interface op ASA

Configureer de interne (Gigabit Ethernet 1/2) en Wi-Fi (Gigabit Ethernet 1/9) interfaces om IP-adressen te hebben zoals nodig in de bestaande omgeving. In dit voorbeeld, zijn de binnencliënten op het 10.0.0.1/24 netwerk en de cliënten van WIFI zijn op het 10.1.0.1/24 netwerk.

```
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
```

> Opmerking: U krijgt deze waarschuwing wanneer u de bovenstaande interface-IP-adressen wijzigt. Dit wordt verwacht.

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

Stap 2. Wijzig de instellingen van de DHCP-pool op zowel binnen- als Wi-Fi-interfaces

Deze stap is vereist als de ASA als DHCP-server in de omgeving moet worden gebruikt. Als een andere DHCP-server wordt gebruikt om IP-adressen aan clients toe te wijzen, moet DHCP in zijn geheel worden uitgeschakeld aan de ASA. Aangezien u nu ons IP-adresseringsschema hebt gewijzigd, moet u de bestaande IP-adresbereik wijzigen die de ASA aan klanten biedt. Deze opdrachten maken nieuwe pools die overeenkomen met het nieuwe IP-adresbereik:

```
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
```

Ook zal de wijziging van de DHCP-pools de vorige DHCP-server op de ASA uitschakelen en u moet deze opnieuw inschakelen.

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

Als u de interface-IP-adressen niet wijzigt voordat DHCP wordt gewijzigd, ontvangt u deze fout:

```
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
```

Stap 3. Specificeer DNS-server om naar interne en WiFI DHCP-clients over te gaan

Wanneer zij IP-adressen via DHCP toewijzen, moeten de meeste clients ook een DNS-server via de DHCP-server krijgen. Deze opdrachten vormen de ASA om de DNS-server op 10.0.250 aan alle klanten te kunnen toevoegen. U moet de 10.0.250 vervangen voor een interne DNS-server of een DNS-server die door uw ISP is geleverd.

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

Stap 4. Wijzig HTTP-toegangsconfiguratie voor de ASA voor Adaptieve Security Apparaat Manager (ASDM):

Aangezien de IP-adressering is gewijzigd, moet HTTP-toegang tot de ASA ook worden aangepast zodat klanten binnen- en WiFI-netwerken toegang hebben tot ASDM om de ASA te beheren.

```
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
```

> Opmerking: Deze configuratie maakt elke client binnen- of WiFi-interface toegang tot de ASA mogelijk via ASDM. Als best practice voor beveiliging moet u het bereik van adressen alleen

beperken tot vertrouwde klanten.

Stap 5. Wijzig interface IP voor access point Management in WLAN-console (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
```

Stap 6. Standaard gateway op WAP wijzigen

Deze stap wordt vereist zodat WAP weet waar te om al verkeer te verzenden dat niet op lokale slechts 4000 gebaseerd is. Dit is vereist om toegang tot de WAP GUI te bieden via HTTP vanaf een client in de ASA-binneninterface.

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

Stap 7. Wijzig het FirePOWER Module Management IP-adres (optioneel)

Als u ook van plan bent om de Cisco FirePOWER (ook bekend als SFR) module in te zetten dan moet u ook zijn IP-adres wijzigen om er toegang toe te hebben van de fysieke Management 1/1 interface in de ASA. Er zijn twee basisinzetscenario's die bepalen hoe de ASA en de SFR module te configureren:

1. Een topologie waarin de ASA Management 1/1-interface wordt aangesloten op een binnenschakelaar (zoals in de normale snelle start-geleider)
2. Een topologie waar een binnenschakelaar niet aanwezig is.

Afhankelijk van uw scenario, zijn dit de juiste stappen:

Als de ASA Management 1/1 interface is aangesloten op een interne switch:

U kunt een sessie uitvoeren in de module en deze van de ASA wijzigen voordat u het aansluit op een binnenschakelaar. Deze configuratie staat u toe om tot de SFR module via IP toegang te hebben door het op zelfde voorwerp als de ASA binneninterface met een IP adres van 10.0.254 te plaatsen.

Lijnen vet zijn specifiek voor dit voorbeeld en zijn vereist voor het maken van IP-connectiviteit.

De lijnen in de cursief zullen per omgeving verschillen.

```
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.
```

> Opmerking: Het kan een paar minuten duren voor het beleid van de standaard toegangscontrole van toepassing is op de SFR module. Als deze is voltooid, kunt u uit de SFR-module CLI en terug naar de ASA ontsnappen door op CTRL + SHIFT + 6 +X (CTRL ^ X) te drukken

Als de ASA NIET is aangesloten op een binnenschakelaar:

Een binnenschakelaar kan niet in sommige kleine implementaties bestaan. In dit type topologie zouden klanten over het algemeen met de ASA verbinden via de WiFi-interface. In dit scenario is het mogelijk de noodzaak van een externe switch te elimineren en toegang te krijgen tot de SFR-module via een afzonderlijke ASA-interface door de Management 1/1-interface te verbinden met een andere fysieke ASA-interface.

In dit voorbeeld moet er een fysieke Ethernet verbinding bestaan tussen de ASA Gigabit Ethernet1/3 interface en de Management1/1 interface. Daarna, vormt u de ASA en SFR module om op een afzonderlijk subnet te zijn en dan kunt u de SFR van zowel de ASA als klanten toegang hebben op de binnen of WiFi interfaces.

ASA-interfaceconconfiguratie:

```
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
```

Configuratie SFR-module:

```
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.

> Opmerking: Het kan een paar minuten duren voor het beleid van de standaard toegangscontrole van toepassing is op de SFR module. Als deze is voltooid, kunt u uit de SFR module CLI en terug naar de ASA ontsnappen door op CTRL + SHIFT + 6 +X (CTRL ^ X) te drukken.

Zodra de SFR-configuratie van toepassing is, moet u het SFR beheer IP-adres van de ASA kunnen pingelen:

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#
```

Als u de interface niet met succes kunt pingelen, verifieert u de configuratie en de staat van de fysieke Ethernet-verbindingen.

Stap 8. Sluit aan op AP GUI om radio's in te schakelen en andere WAP-configuratie in te stellen

Op dit punt zou u connectiviteit moeten hebben om WAP via de HTTP GUI te beheren zoals besproken in de snelle begin gids. U moet doorkijken naar het IP-adres van de WAP's BVI-interface vanuit een webbrowser van een client die is aangesloten op het interne netwerk op de 5506W of u kunt de voorbeeldconfiguratie toepassen en verbinding maken met de SSID van de WAP. Als u de CLI hieronder niet gebruikt, moet u de Ethernet-kabel van uw client naar de Gigabit1/2-interface in de ASA aansluiten.

Als u liever de CLI gebruikt om de WAP te configureren, kunt u er een sessie vanaf de ASA uitvoeren en deze voorbeeldconfiguratie gebruiken. Dit creëert een open SSID met de naam 5506W en 5506W_5Ghz zodat u een draadloze client kunt gebruiken om verbinding te maken met en verder te beheren WAP.

> Opmerking: Na het toepassen van deze configuratie zult u toegang tot de GUI willen hebben en veiligheid op SSIDs willen toepassen zodat het draadloze verkeer wordt versleuteld.

WAP CLI-configuratie voor één draadloos VLAN met behulp van gewijzigd IP-bereik

```
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
```

Vanaf dit punt op, kunt u de normale stappen uitvoeren om de configuratie van WAP te voltooien en u moet het van de web browser van een client kunnen gebruiken die is aangesloten op de hierboven gemaakte SSID. De standaardgebruikersnaam van het access point is Cisco met een wachtwoord van Cisco met een hoofdletter C.

Cisco ASA 5506-X Series Quick Start-gids

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

U moet het IP-adres van 10.1.0.254 gebruiken in plaats van de 192.168.10.2 zoals aangegeven in de Quick Start Guide.

Configuraties

De resulterende configuratie moet overeenkomen met de uitvoer (ervan uitgaande dat u de voorbeeld-IP-bereik hebt gebruikt, anders dient u dienovereenkomstig te vervangen:

ASA-configuratie

Interfaces:

> Opmerking: De lijnen in cursief zijn alleen van toepassing als u GEEN binnenschakelaar hebt:

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 Configuration (zonder de SSID-configuratie)

```
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 Module-configuratie (met interne switch)

```
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 Module-configuratie (zonder interne switch)

```
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

>
```

Verifiëren

Zo controleert u of u de juiste connectiviteit met de WAP hebt voor het voltooien van het installatieproces:

1. Sluit uw testclient aan op de ASA-binneninterface en zorg ervoor dat deze een IP-adres van de ASA via DHCP ontvangt dat binnen het gewenste IP-bereik valt.
2. Gebruik een webbrowser op uw client om naar https://10.1.0.254 te navigeren en te controleren of de AP GUI nu toegankelijk is.
3. Ping van de SFR beheersinterface van de binnenclient en de ASA om juiste connectiviteit te verifiëren.

DHCP configureren met meerdere draadloze VLAN's

De configuratie veronderstelt dat u één draadloos VLAN gebruikt. De Bridge Virtual Interface (BVI) op de Draadloze AP kan een brug vormen voor meerdere VLAN's. Vanwege de syntaxis voor DHCP op de ASA, als u de 5506W wilt configureren als een DHCP-server voor meerdere VLAN's, moet u subinterfaces maken op de Gigabit1/9-interface en elke naam geven. Deze sectie leidt u door het proces van het verwijderen van de standaardconfiguratie en het toepassen van de configuratie nodig om de ASA in te stellen als een DHCP-server voor meerdere VLAN's.

Stap 1. Verwijder bestaande DHCP-configuratie op Gig1/9

Verwijder eerst de bestaande DHCP-configuratie op de Gig1/9 (Wi-Fi)-interface:

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

Stap 2. Maak subinterfaces voor elk VLAN op Gig1/9

Voor elk VLAN dat u op het toegangspunt hebt ingesteld, moet u een subinterface van Gig1/9 configureren. In deze voorbeeldconfiguratie, voegt u twee subinterfaces toe:

-Gig1/9.5, dat zal naam hebben als vlan5, en zal overeenkomen met VLAN 5 en SUBNET 10.5.0.0/24.

-Gig1/9.30, dat zal naam hebben als vlan30, en zal overeenkomen met VLAN 30 en Subnet 10.3.0.0/24.

In praktijk, is het van essentieel belang dat VLAN en SUBNET die hier worden gevormd het VLAN en SUBNET op het toegangspunt aanpassen. De naam indien en het subinterfacenummer kunnen alles zijn wat u kiest. Raadpleeg de eerder genoemde snelstartgids voor koppelingen om het toegangspunt te configureren met behulp van de webGUI.

```
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
```

Stap 3. Wijs een DHCP-pool voor elk VLAN aan

Maak een afzonderlijke DHCP-pool voor elk VLAN dat wordt geconfigureerd. De syntaxis voor deze opdracht vereist dat u de naam aangeeft waarvan de ASA de pool in kwestie zal dienen. Een voorbeeld in dit voorbeeld, dat VLANs 5 en 30 gebruikt:

```
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
```

Stap 4. Configureer de SSID's van het access point, slaat de configuratie op en stelt de module opnieuw in

Ten slotte moet het toegangspunt worden geconfigureerd om overeen te komen met de configuratie van de ASA. Met de GUI-interface voor het access point kunt u VLAN's op AP configureren via de client die is aangesloten op de ASA interne (Gigabit1/2) interface. Als u echter liever CLI gebruikt om AP via de ASA console-sessie te configureren en dan draadloos aan te sluiten om AP te beheren, kunt u deze configuratie gebruiken als een sjabloon voor het maken van twee SSID's op VLAN's 5 en 30. Dit moet binnen de AP-console in globale configuratie modus worden ingevoerd:

```
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
```

Op dit punt moet de beheerconfiguratie van de ASA en AP volledig zijn, en de ASA werkt als een server van DHCP voor VLANs 5 en 30. Na het opslaan van de configuratie met de opdracht ***schrijfgeheugen*** *op de AP, als u nog steeds connectiviteitsproblemen hebt, moet u AP opnieuw laden met de opdracht* ***herladen*** *van de CLI. Als u echter een IP adres op de nieuwe SSIDs ontvangt, dan geen verdere actie is vereist.*

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

> Opmerking: U hoeft het gehele ASA-apparaat NIET opnieuw te laden. U hoeft alleen het ingebouwde access point te herladen.

Nadat het opnieuw laden is voltooid, moet u connectiviteit met AP GUI van een clientmachine op de WiFi of binnen netwerken hebben. Over het algemeen duurt het ongeveer twee minuten voordat de AP volledig herstart. Vanaf dit punt kunt u de normale stappen toepassen om de configuratie van de WAP te voltooien.

Cisco ASA 5506-X Series Quick Start-gids

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

Problemen oplossen

ASA-connectiviteit voor probleemoplossing is buiten het bereik van dit document omdat dit voor de eerste configuratie is bedoeld. Raadpleeg de sectie voor verificatie en configuratie om er zeker van te zijn dat alle stappen correct zijn voltooid.