Konfigurieren der ASA 5506W-X mit einer nicht standardmäßigen IP- oder mehreren VLAN-Konfigurationen

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie eine Erstinstallation und -konfiguration einer Cisco

Adaptive Security Appliance (ASA) 5506W-X durchführen, wenn das standardmäßige IP-Adressierungsschema so geändert werden muss, dass es in ein bestehendes Netzwerk passt oder wenn mehrere Wireless-VLANs erforderlich sind. Es gibt verschiedene Konfigurationsänderungen, die erforderlich sind, wenn die Standard-IP-Adressen geändert werden, um auf den Wireless Access Point (WAP) zuzugreifen und sicherzustellen, dass andere Dienste (wie DHCP) wie erwartet funktionieren. Darüber hinaus enthält dieses Dokument einige CLI-Konfigurationsbeispiele für den integrierten Wireless Access Point (WAP), um die Erstkonfiguration des WAP zu vereinfachen. Dieses Dokument soll die bestehende Cisco ASA 5506-X Schnellstartanleitung ergänzen, die auf der Cisco Website verfügbar ist.

Voraussetzungen

Dieses Dokument gilt nur für die Erstkonfiguration eines Cisco ASA5506W-X-Geräts mit einem Wireless Access Point und ist nur für die verschiedenen Änderungen vorgesehen, die erforderlich sind, wenn Sie das vorhandene IP-Adressierungsschema ändern oder zusätzliche Wireless-VLANs hinzufügen. Bei Installationen der Standardkonfiguration muss auf die bestehende ASA 5506-X Schnellstartanleitung verwiesen werden.

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Cisco ASA 5506W-X-Gerät
- Client-Rechner mit Terminal-Emulationsprogramm wie Putty, SecureCRT usw.
- Konsolenkabel und serieller PC-Terminal-Adapter (DB-9 zu RJ-45)

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

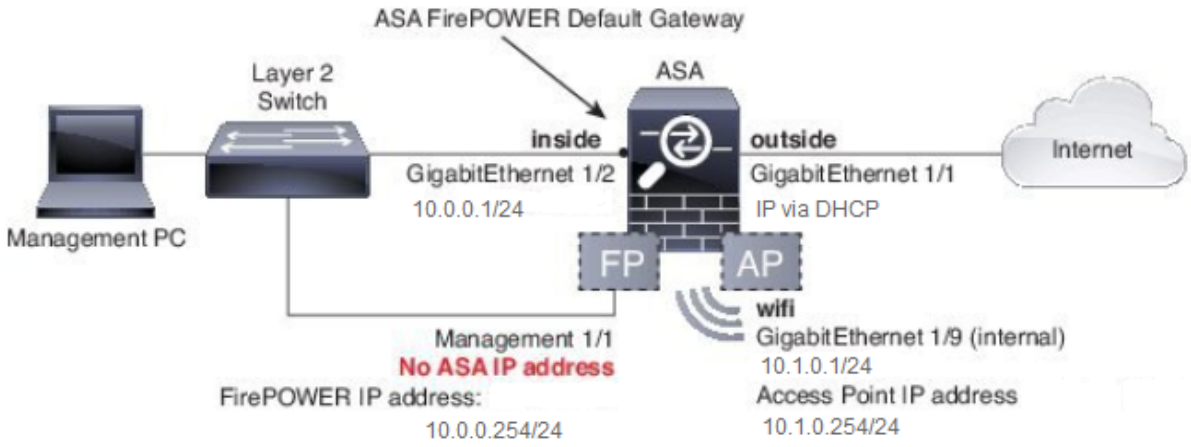
- Cisco ASA 5506W-X-Gerät
- Client-Rechner mit Terminal-Emulationsprogramm wie Putty, SecureCRT usw.
- Konsolenkabel und serieller PC-Terminal-Adapter (DB-9 zu RJ-45)
- ASA FirePOWER-Modul
- Integrierter Cisco Aironet 702i Wireless Access Point (integriertes WAP)

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

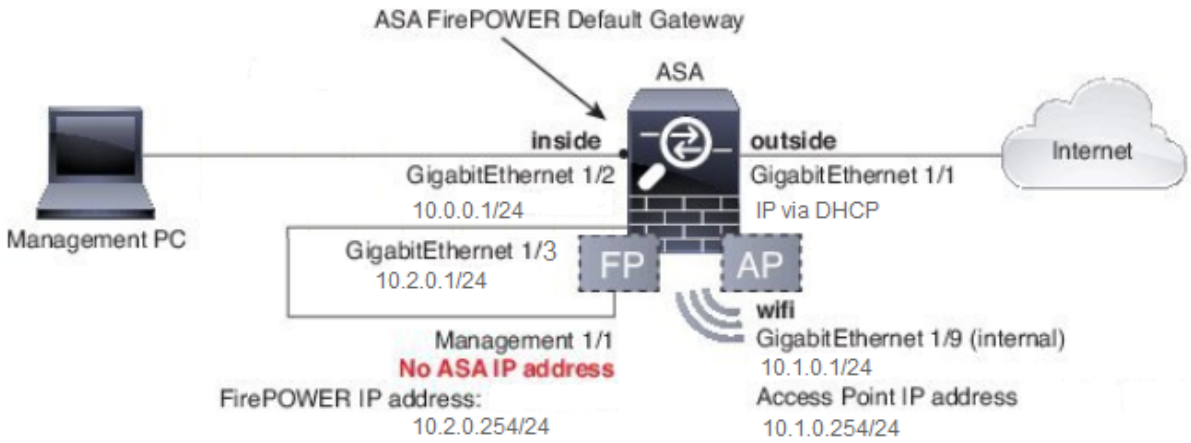
Netzwerkdiagramme

Wie in diesem Bild gezeigt, werden Beispiele für die IP-Adressierung in zwei verschiedenen Topologien angewendet:

ASA + FirePOWER mit einem internen Switch:



ASA + FirePOWER ohne internen Switch:



Konfigurieren

Diese Schritte müssen in der richtigen Reihenfolge ausgeführt werden, nachdem Sie die ASA-Geräte mit dem am Client angeschlossenen Konsolenkabel hochfahren und starten.

Schritt 1: Ändern der IP-Schnittstellenkonfiguration auf der ASA

Konfigurieren Sie die internen (GigabitEthernet 1/2) und Wi-Fi (GigabitEthernet 1/9)-Schnittstellen so, dass sie in der vorhandenen Umgebung nach Bedarf über IP-Adressen verfügen. In diesem Beispiel befinden sich interne Clients im Netzwerk 10.0.0.1/24, und WIFI-Clients befinden sich im Netzwerk 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
```

Hinweis: Sie erhalten diese Warnung, wenn Sie die oben angegebenen IP-Adressen für die

Benutzeroberfläche ändern. Dies ist zu erwarten.

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

Schritt 2: Ändern Sie die DHCP-Pool-Einstellungen für interne und WiFi-Schnittstellen.

Dieser Schritt ist erforderlich, wenn die ASA als DHCP-Server in der Umgebung verwendet werden soll. Wenn ein anderer DHCP-Server verwendet wird, um Clients IP-Adressen zuzuweisen, sollte DHCP auf der ASA komplett deaktiviert werden. Da Sie jetzt unser IP-Adressierungsschema geändert haben, müssen Sie die vorhandenen IP-Adressbereiche ändern, die die ASA Clients bereitstellt. Diese Befehle erstellen neue Pools, die dem neuen IP-Adressbereich entsprechen:

```
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
```

Durch die Änderung der DHCP-Pools wird auch der vorherige DHCP-Server auf der ASA deaktiviert, und Sie müssen ihn erneut aktivieren.

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

Wenn Sie die IP-Schnittstellenadressen vor den DHCP-Änderungen nicht ändern, wird folgender Fehler angezeigt:

```
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
```

Schritt 3: Angeben des DNS-Servers für die Weiterleitung an interne und WiFi-DHCP-Clients

Wenn sie IP-Adressen über DHCP zuweisen, müssen die meisten Clients vom DHCP-Server auch einen DNS-Server zugewiesen werden. Mit diesen Befehlen wird die ASA so konfiguriert, dass sie den unter 10.0.0.250 angegebenen DNS-Server für alle Clients enthält. Sie müssen 10.0.0.250 durch einen internen DNS-Server oder einen DNS-Server ersetzen, der von Ihrem ISP bereitgestellt wird.

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

Schritt 4: Ändern Sie die HTTP-Zugriffskonfiguration auf dem ASA für den ASDM-Zugriff (Adaptive Security Device Manager):

Da die IP-Adressierung geändert wurde, muss auch der HTTP-Zugriff auf die ASA so geändert werden, dass Clients in internen und WiFi-Netzwerken auf ASDM zugreifen können, um die ASA zu verwalten.

```
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
```

> **Hinweis**: Diese Konfiguration ermöglicht es jedem Client auf der internen oder Wi-Fi-Schnittstelle, über ASDM auf die ASA zuzugreifen. Als Best Practice im Bereich Sicherheit müssen Sie den Adressbereich auf vertrauenswürdige Clients beschränken.

Schritt 5: Ändern Sie die Schnittstellen-IP für die Access Point-Verwaltung in der WLAN-Konsole (Schnittstelle 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
```

Schritt 6: Ändern Sie das Standard-Gateway auf WAP.

Dieser Schritt ist erforderlich, damit der WAP weiß, wohin der gesamte Datenverkehr gesendet werden soll, der nicht vom lokalen Subnetz stammt. Dies ist erforderlich, um über HTTP von einem Client auf der ASA-internen Schnittstelle auf die WAP-GUI zuzugreifen.

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

Schritt 7: Ändern Sie die IP-Adresse des FirePOWER-Modulmanagements (optional).

Wenn Sie auch die Bereitstellung des Cisco FirePOWER-Moduls (auch bekannt als SFR) planen, müssen Sie auch dessen IP-Adresse ändern, um von der physischen Management1/1-Schnittstelle auf der ASA darauf zuzugreifen. Es gibt zwei grundlegende Bereitstellungsszenarien, die die Konfiguration von ASA und SFR-Modul bestimmen:

1. Eine Topologie, in der die ASA Management1/1-Schnittstelle mit einem internen Switch verbunden ist (wie in der normalen Schnellstartanleitung beschrieben)
2. Eine Topologie, bei der kein interner Switch vorhanden ist.

Je nach Szenario sind folgende Schritte erforderlich:

Wenn die ASA Management1/1-Schnittstelle mit einem internen Switch verbunden ist:

Sie können eine Sitzung mit dem Modul herstellen und es von der ASA ändern, bevor Sie es mit einem internen Switch verbinden. Mit dieser Konfiguration können Sie auf das SFR-Modul über IP zugreifen, indem Sie es im gleichen Subnetz wie die interne ASA-Schnittstelle mit der IP-Adresse 10.0.0.254 platzieren.

Fettgedruckte Zeilen sind für dieses Beispiel spezifisch und werden für die Einrichtung einer IP-Verbindung benötigt.

Die Kursivschrift kann je nach Umgebung variieren.

```
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.
```

> **Hinweis**: Es kann ein paar Minuten dauern, bis die standardmäßige Zugriffskontrollrichtlinie auf das SFR-Modul angewendet wird. Wenn der Vorgang abgeschlossen ist, können Sie die CLI des SFR-Moduls verlassen und wieder in die ASA zurückkehren, indem Sie STRG + UMSCHALTTASTE + 6 +X (STRG ^ X) drücken.

Wenn die ASA NICHT mit einem internen Switch verbunden ist:

In einigen kleinen Bereitstellungen ist möglicherweise kein interner Switch vorhanden. Bei dieser Topologie würden Clients in der Regel über die WiFi-Schnittstelle eine Verbindung zur ASA herstellen. In diesem Szenario ist ein externer Switch nicht erforderlich, und der Zugriff auf das SFR-Modul über eine separate ASA-Schnittstelle ist möglich, indem die Management1/1-

Schnittstelle mit einer anderen physischen ASA-Schnittstelle verbunden wird.

In diesem Beispiel muss eine physische Ethernet-Verbindung zwischen der ASA GigabitEthernet1/3-Schnittstelle und der Management1/1-Schnittstelle bestehen. Als Nächstes konfigurieren Sie das ASA- und das SFR-Modul in einem separaten Subnetz, und Sie können dann sowohl von der ASA als auch von den Clients in der internen Schnittstelle oder von der WiFi-Schnittstelle auf die SFR zugreifen.

ASA-Schnittstellenkonfiguration:

```
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
```

Konfiguration des SFR-Moduls:

```
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.

> **Hinweis**: Es kann ein paar Minuten dauern, bis die standardmäßige Zugriffskontrollrichtlinie auf das SFR-Modul angewendet wird. Wenn der Vorgang abgeschlossen ist, können Sie die CLI des SFR-Moduls verlassen und wieder in die ASA zurückkehren, indem Sie STRG + UMSCHALT + 6 +X (STRG ^ X) drücken.

Wenn die SFR-Konfiguration angewendet wurde, müssen Sie in der Lage sein, von der ASA die IP-Adresse für das SFR-Management zu pingen:

```
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#
```

Wenn Sie die Schnittstelle nicht erfolgreich pingen können, überprüfen Sie die Konfiguration und den Zustand der physischen Ethernet-Verbindungen.

Schritt 8: Herstellen einer Verbindung zur AP-GUI, um Funkmodule zu aktivieren und andere WAP-Konfigurationen festzulegen

An diesem Punkt sollten Sie über Konnektivität verfügen, um den WAP über die HTTP-GUI zu verwalten, wie in der Schnellstartanleitung beschrieben. Sie müssen entweder von einem Webbrowser eines Clients, der mit dem internen Netzwerk des 5506W verbunden ist, zur IP-Adresse der BVI-Schnittstelle des WAP navigieren oder die Beispielkonfiguration anwenden und eine Verbindung mit der SSID des WAP herstellen. Wenn Sie die folgende CLI nicht verwenden, müssen Sie das Ethernet-Kabel vom Client an die Gigabit1/2-Schnittstelle der ASA anschließen.

Wenn Sie die Konfiguration des WAP mithilfe der CLI vorziehen, können Sie über die ASA eine Sitzung mit dieser Konfiguration durchführen. Dadurch wird eine offene SSID mit dem Namen 5506W und 5506W_5GHz erstellt, sodass Sie einen Wireless-Client für die Verbindung mit dem WAP und für die weitere Verwaltung verwenden können.

> **Hinweis**: Nach Anwenden dieser Konfiguration sollten Sie auf die GUI zugreifen und die SSIDs mit Sicherheitsfunktionen versehen, sodass der Wireless-Datenverkehr verschlüsselt wird.

WAP-CLI-Konfiguration für ein einzelnes WLAN mit geänderten IP-Bereichen

```
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
```

Ab diesem Punkt können Sie die normalen Schritte durchführen, um die Konfiguration des WAP abzuschließen, und Sie müssen über den Webbrowser eines mit der oben erstellten SSID verbundenen Clients darauf zugreifen können. Der Standardbenutzername des Access Points ist Cisco mit einem Kennwort von Cisco mit einem Großbuchstaben C.

Schnellstartanleitung für die Cisco Serie ASA 5506-X

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

Sie müssen die IP-Adresse 10.1.0.254 anstelle von 192.168.10.2 verwenden, wie in der Schnellstartanleitung angegeben.

Konfigurationen

Die resultierende Konfiguration muss mit der Ausgabe übereinstimmen (unter der Annahme, dass Sie die Beispiel-IP-Bereiche verwendet haben, andernfalls dementsprechend ersetzen:

ASA-Konfiguration

Schnittstellen:

> **Hinweis**: Die kursiv dargestellten Zeilen sind nur gültig, wenn Sie KEINEN internen Schalter haben:

```
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-Konfiguration (ohne SSID-Beispielkonfiguration)

```
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
```

Konfiguration des FirePOWER-Moduls (mit internem 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

>
```

Konfiguration des FirePOWER-Moduls (ohne internen 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

>
```

Überprüfen

So stellen Sie sicher, dass Sie über die richtige Verbindung zum WAP verfügen, um den Installationsprozess abzuschließen:

1. Verbinden Sie den Testclient mit der internen ASA-Schnittstelle, und stellen Sie sicher, dass er über DHCP eine IP-Adresse von der ASA erhält, die innerhalb des gewünschten IP-Bereichs liegt.
2. Verwenden Sie einen Webbrowser auf Ihrem Client, um zu https://10.1.0.254 zu navigieren und zu überprüfen, ob der Zugriff auf die Access Point-GUI jetzt möglich ist.
3. Pingen Sie die SFR-Management-Schnittstelle vom internen Client und der ASA, um die ordnungsgemäße Konnektivität zu überprüfen.

Konfigurieren von DHCP mit mehreren Wireless-VLANs

Bei der Konfiguration wird davon ausgegangen, dass Sie ein einzelnes WLAN verwenden. Die Bridge Virtual Interface (BVI) am Wireless AP kann eine Bridge für mehrere VLANs bereitstellen. Wenn Sie den 5506W als DHCP-Server für mehrere VLANs konfigurieren möchten, müssen Sie aufgrund der DHCP-Syntax auf der ASA-Schnittstelle Unterschnittstellen auf der Gigabit1/9-Schnittstelle erstellen und jedem einen Namen geben. Dieser Abschnitt führt Sie durch den Prozess zum Entfernen der Standardkonfiguration und zum Anwenden der erforderlichen Konfiguration, um die ASA als DHCP-Server für mehrere VLANs einzurichten.

Schritt 1: Entfernen der vorhandenen DHCP-Konfiguration auf Gig1/9

Entfernen Sie zunächst die vorhandene DHCP-Konfiguration auf der Gig1/9 (WiFi)-Schnittstelle:

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

Schritt 2: Erstellen von Subschnittstellen für jedes VLAN auf Gig1/9

Für jedes VLAN, das Sie auf dem Access Point konfiguriert haben, müssen Sie eine Subschnittstelle von Gig1/9 konfigurieren. In dieser Beispielkonfiguration fügen Sie zwei Subschnittstellen hinzu:

-Gig1/9.5, das den Namen "vlan5" trägt und VLAN 5 und Subnetz 10.5.0.0/24 entspricht.

-Gig1/9.30, die den Namen "vlan30" tragen und VLAN 30 und Subnetz 10.3.0.0/24 entsprechen.

In der Praxis ist es wichtig, dass das hier konfigurierte VLAN und Subnetz mit dem VLAN und dem Subnetz übereinstimmen, die auf dem Access Point angegeben sind. Name und Subschnittstellennummer können beliebig sein. Links finden Sie in der zuvor erwähnten Schnellstartanleitung, um den Access Point über die Web-GUI zu konfigurieren.

```
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
```

Schritt 3: Bestimmung eines DHCP-Pools für jedes VLAN

Erstellen Sie für jedes zu konfigurierende VLAN einen separaten DHCP-Pool. Die Syntax für diesen Befehl erfordert, dass Sie den Namen angeben, unter dem die ASA den betreffenden Pool bedienen wird. Ein Beispiel aus diesem Beispiel, das die VLANs 5 und 30 verwendet:

```
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
```

Schritt 4: Konfigurieren der Access Point-SSIDs, Speichern der Konfiguration und Zurücksetzen des Moduls

Schließlich muss der Access Point entsprechend der ASA-Konfiguration konfiguriert werden. Die GUI-Schnittstelle für den Access Point ermöglicht die Konfiguration von VLANs auf dem Access Point über den mit der ASA-Schnittstelle (Gigabit1/2) verbundenen Client. Wenn Sie jedoch die Verwendung von CLI bevorzugen, um den Access Point über die ASA-Konsolensitzung zu konfigurieren und dann eine drahtlose Verbindung zum Verwalten des Access Points herzustellen, können Sie diese Konfiguration als Vorlage zum Erstellen von zwei SSIDs auf VLANs 5 und 30 verwenden. Dies muss in der AP-Konsole im globalen Konfigurationsmodus eingegeben werden:

```
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
```

*Zu diesem Zeitpunkt muss die Verwaltungskonfiguration der ASA und des AP abgeschlossen sein, und die ASA fungiert als DHCP-Server für die VLANs 5 und 30. Wenn Sie die Konfiguration mit dem Befehl **write memory** (**Schreibspeicher**) auf dem Access Point gespeichert haben, müssen Sie den Access Point mit dem Befehl **reload** aus der CLI neu laden, wenn weiterhin Verbindungsprobleme bestehen. Wenn Sie jedoch eine IP-Adresse für die neu erstellten SSIDs erhalten, ist keine weitere Aktion erforderlich.*

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

> **Hinweis**: Sie müssen NICHT das gesamte ASA-Gerät neu laden. Sie dürfen nur den integrierten Access Point neu laden.

Wenn der Access Point das Neuladen beendet hat, müssen Sie von einem Client-Rechner im WiFi-Netzwerk oder in Netzwerken eine Verbindung zur AP-GUI haben. Der vollständige Neustart des Access Points dauert in der Regel etwa zwei Minuten. Ab diesem Punkt können Sie die normalen Schritte anwenden, um die Konfiguration des WAP abzuschließen.

Schnellstartanleitung für die Cisco Serie ASA 5506-X

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

Fehlerbehebung

Die Fehlerbehebung bei ASA-Verbindungen ist nicht Bestandteil dieses Dokuments, da dies für die Erstkonfiguration vorgesehen ist. Lesen Sie die Abschnitte zur Überprüfung und Konfiguration, um sicherzustellen, dass alle Schritte ordnungsgemäß ausgeführt wurden.