使用非預設IP或多個VLAN配置配置ASA 5506W-X

目錄

簡介

本文檔介紹在需要修改預設IP編址方案以適合現有網路或需要多個無線VLAN時，如何執行思科自適應安全裝置(ASA)5506W-X裝置的初始安裝和配置。 在修改預設IP地址以訪問無線接入點(WAP)並確保其他服務（如DHCP）繼續按預期運行時，需要進行多項配置更改。 此外，本文檔還提供了整合無線接入點(WAP)的一些CLI配置示例，以便更輕鬆地完成WAP的初始配置。本文檔旨在補充思科網站上提供的現有Cisco ASA 5506-X快速入門手冊。

必要條件

本文檔僅適用於包含無線接入點的Cisco ASA5506W-X裝置的初始配置，僅用於解決修改現有IP編址方案或新增其他無線VLAN時所需的各種更改。 對於預設配置安裝，必須參考現有的ASA 5506-X快速啟動指南。

需求

思科建議您瞭解以下主題：

- Cisco ASA 5506W-X裝置
- 具有終端模擬程式（如Putty、SecureCRT等）的客戶端。
- 控制檯電纜和串列PC終端介面卡（DB-9到RJ-45）

採用元件

本文中的資訊係根據以下軟體和硬體版本：

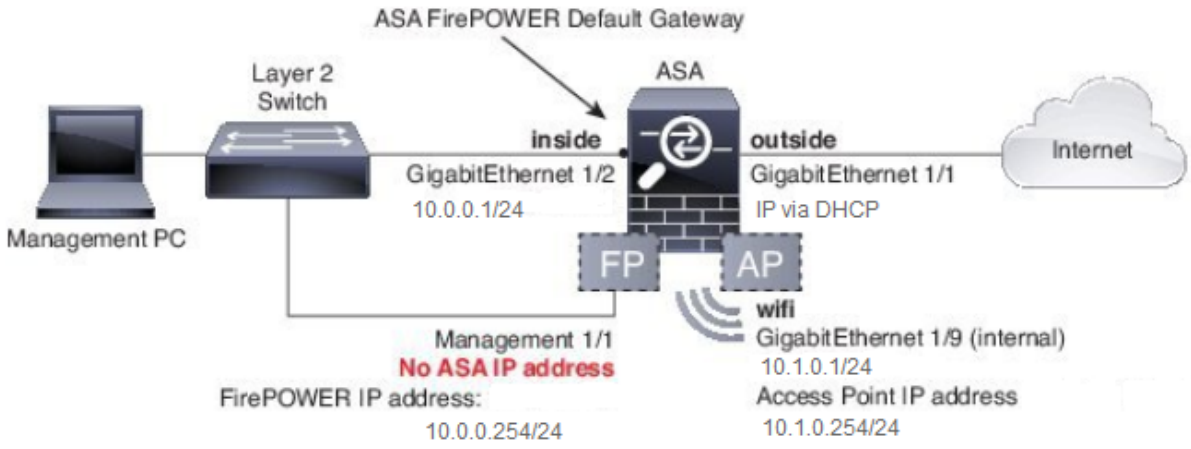
- Cisco ASA 5506W-X裝置
- 具有終端模擬程式（如Putty、SecureCRT等）的客戶端。
- 控制檯電纜和串列PC終端介面卡（DB-9到RJ-45）
- ASA FirePOWER模組
- 整合Cisco Aironet 702i無線接入點（內建WAP）

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

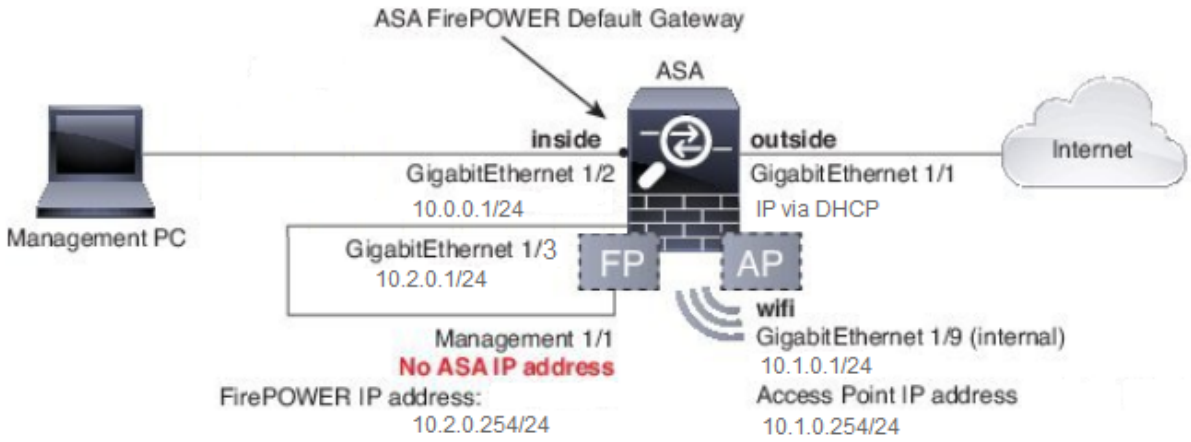
網路圖

如圖所示，適用於兩種不同拓撲的IP編址範例：

帶內部交換機的ASA + FirePOWER:



沒有內部交換機的ASA + FirePOWER:



設定

在開啟電源並啟動ASA且控制檯電纜連線到客戶端後，必須按順序執行這些步驟。

步驟1.修改ASA上的介面IP配置

配置內部(GigabitEthernet 1/2)和wifi(GigabitEthernet 1/9)介面，使其具有現有環境中所需的IP地址。 在本示例中，內部客戶端位於10.0.0.1/24網路上，WIFI客戶端位於10.1.0.1/24網路上。

```
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
```

附註：當您更改上述介面IP地址時，將會收到此警告。 這是意料之中的。

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

步驟2.修改內部和wifi介面上的DHCP地址池設定

如果要將ASA用作環境中的DHCP伺服器，則需要執行此步驟。 如果使用另一個DHCP伺服器將IP地址分配給客戶端，則應在ASA上完全禁用DHCP。 由於您現在更改了我們的IP編址方案，因此需要更改ASA提供給客戶端的現有IP地址範圍。 這些命令將建立新的池以匹配新的IP地址範圍：

```
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
```

此外，DHCP池的修改將禁用ASA上以前的DHCP伺服器，您需要重新啟用它。

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

如果在更改DHCP之前未更改介面IP地址，您將收到以下錯誤：

```
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
```

步驟3.指定要傳遞給內部和WiFI DHCP客戶端的DNS伺服器

當通過DHCP分配IP地址時，大多數客戶端還需要由DHCP伺服器分配DNS伺服器。 這些命令將配置ASA，使其包括所有客戶端的DNS伺服器（位於10.0.0.250）。 您需要將10.0.0.250替換為內部DNS伺服器或ISP提供的DNS伺服器。

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

步驟4.在ASA上修改自適應安全裝置管理器(ASDM)訪問的HTTP訪問配置：

由於IP地址已更改，因此還需要修改對ASA的HTTP訪問，以便內部和WiFI網路上的客戶端可以訪問ASDM來管理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
```

> **附註**：此配置允許內部或wifi介面上的任何客戶端通過ASDM訪問ASA。 作為安全最佳實踐，您必須將地址範圍限製為僅受信任的客戶端。

步驟5.修改WLAN控制檯中接入點管理的介面IP（介面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
```

步驟6.修改WAP上的預設網關

要使WAP知道要將並非源自本地子網的所有流量傳送到何處，必須執行此步驟。 要通過HTTP從ASA內部介面上的客戶端訪問WAP GUI，必須執行此操作。

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

步驟7.修改FirePOWER模組管理IP地址（可選）

如果您還計畫部署Cisco FirePOWER（也稱為SFR）模組，則還需要更改其IP地址，以便從ASA上的物理管理1/1介面訪問它。有兩種基本部署方案可確定如何配置ASA和SFR模組：

1. ASA Management1/1介面連線到內部交換機的拓撲（根據一般快速入門手冊）
2. 不存在內部交換機的拓撲。

根據您的情況，以下是相應的步驟：

如果ASA Management1/1介面連線到內部交換機：

您可以將會話加入模組並從ASA進行更改，然後再將其連線到內部交換機。 此配置允許您通過IP訪問SFR模組，方法是將其放置在IP地址為10.0.0.254的ASA內部介面所在的同一子網中。

粗體行特定於此示例，是建立IP連線所必需的。

斜體中的線條因環境而異。

```
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.
```

附註：在SFR模組上應用預設訪問控制策略可能需要幾分鐘時間。 完成後，您可以通過按CTRL + SHIFT + 6 +X(CTRL ^ X)退出SFR模組CLI並返回ASA

如果ASA未連線到內部交換機：

某些小型部署中可能不存在內部交換機。 在這種型別的拓撲中，客戶端通常通過WiFi介面連線到ASA。 在此方案中，通過將Management1/1介面交叉連線到另一個物理ASA介面，可以消除對外部交換機的需求並通過單獨的ASA介面訪問SFR模組。

在本示例中，ASA GigabitEthernet1/3介面和Management1/1介面之間必須存在物理乙太網連線。接下來，將ASA和SFR模組配置為位於單獨的子網上，然後您可以從ASA以及位於內部或wifi介面上的客戶端訪問SFR。

ASA介面配置：

```
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模組配置：

```
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.
```

附註：在SFR模組上應用預設訪問控制策略可能需要幾分鐘時間。 完成後，您可以通過按CTRL + SHIFT + 6 +X(CTRL ^ X)退出SFR模組CLI並返回ASA。

應用SFR配置後，您必須能夠從ASA ping通SFR管理IP地址：

```
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#
```

如果無法成功ping通介面，請檢驗物理乙太網連線的配置和狀態。

步驟8.連線到AP GUI以啟用無線電並設定其他WAP配置

此時，您應該具有通過HTTP GUI管理WAP的連線，如快速入門手冊中所述。 您將需要從客戶端的Web瀏覽器瀏覽WAP的BVI介面的IP地址，該客戶端已連線到5506W的內部網路，或者可以應用示例配置並連線到WAP的SSID。如果您不使用下面的CLI，則需要將乙太網電纜從您的客戶端連線到ASA上的Gigabit1/2介面。

如果您更喜歡使用CLI配置WAP，則可以從ASA進行會話進入該WAP，然後使用此示例配置。這將建立一個名為5506W和5506W_5Ghz的開放式SSID，以便您可以使用無線客戶端連線並進一步管理WAP。

附註：應用此配置後，您需要訪問GUI並將安全應用到SSID，以便加密無線流量。

使用修改的IP範圍為單個無線VLAN配置WAP CLI

```
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
```

從此以後，您可以執行正常步驟完成WAP的配置，並且您必須能夠從連線到上述建立SSID的客戶端的Web瀏覽器訪問它。接入點的預設使用者名稱是Cisco，密碼為Cisco，大寫C。

Cisco ASA 5506-X系列快速入門手冊

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

您需要使用IP地址10.1.0.254，而不是快速入門手冊中所述的192.168.10.2。

組態

產生的配置必須與輸出匹配(假定您使用示例IP範圍，否則請相應地替換：

ASA配置

介面：

附註：只有當您沒有內部交換器時，斜體中的行才適用：

```
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配置（沒有示例SSID配置）

```
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模組配置（帶內部交換機）

```
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模組配置（不含內部交換機）

```
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

>
```

驗證

要驗證您與WAP是否具有正確的連線以完成安裝過程，請執行以下操作：

1. 將您的測試客戶端連線到ASA內部介面，並確保它通過DHCP從ASA接收位於所需IP範圍之內的IP地址。
2. 在客戶端上使用Web瀏覽器導航至https://10.1.0.254，並驗證現在是否可以訪問AP GUI。
3. 從內部客戶端和ASA對SFR管理介面執行ping操作以驗證連線是否正確。

為多個無線VLAN配置DHCP

此組態假設使用單一無線VLAN。無線AP上的網橋虛擬介面(BVI)可為多個VLAN提供網橋。由於ASA上的DHCP語法，如果要將5506W配置為多個VLAN的DHCP伺服器，則需要在Gigabit1/9介面上建立子介面並為每個子介面指定一個名稱。本節指導您完成如何刪除預設配置以及應用將ASA設定為多個VLAN的DHCP伺服器所需的配置。

步驟1.刪除Gig1/9上的現有DHCP配置

首先，刪除Gig1/9(wifi)介面上的現有DHCP配置：

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

步驟2.為Gig1/9上的每個VLAN建立子介面

對於已在接入點上配置的每個VLAN，您需要配置Gig1/9的子介面。在此示例配置中，您新增兩個子介面：

-Gig1/9.5，將具有nameif vlan5，並將對應於VLAN 5和子網10.5.0.0/24。

-Gig1/9.30，將具有nameif vlan30，並將對應於VLAN 30和子網10.3.0.0/24。

實際上，此處配置的VLAN和子網必須與接入點上指定的VLAN和子網相匹配。nameif和子介面編號

可以是您選擇的任何數字。 有關連結，請參閱前面提到的快速入門手冊，以便使用Web GUI配置接入點。

```
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
```

步驟3.為每個VLAN指定DHCP池

為配置的每個VLAN建立一個單獨的DHCP池。此命令的語法要求您列出nameif，ASA將從該名稱中為該池提供服務。如本範例所示，此範例使用VLAN 5和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
```

步驟4.配置接入點SSID、儲存配置並重置模組

最後，需要配置接入點以符合ASA的配置。接入點的GUI介面允許您通過連線到ASA內部(Gigabit1/2)介面的客戶端在AP上配置VLAN。但是，如果您希望使用CLI通過ASA控制檯會話配置AP，然後無線連線以管理AP，則可以將此配置用作在VLAN 5和30上建立兩個SSID的模板。必須在全域性配置模式下的AP控制檯中輸入此配置：

```
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
```

此時，ASA和AP的管理配置必須完成，並且ASA充當VLAN 5和30的DHCP伺服器。在AP上使用 ***write memory****命令儲存配置後，如果仍有連線問題，則必須使用****reload****命令從CLI重新載入AP。但是，如果在新建立的SSID上收到IP地址，則無需執行進一步的操作。*

```
ap#write memory
Building configuration...
[OK]
ap#reload
```

```
Proceed with reload? [confirm]
Writing out the event log to flash:/event.log ...
```

附註：您無需重新載入整個ASA裝置。您必須只重新載入內建存取點。

AP完成重新載入後，您必須從WiFi或內部網路上的客戶端電腦連線到AP GUI。 通常AP完全重新啟動大約需要兩分鐘。 從此以後，您可以應用常規步驟完成WAP配置。

Cisco ASA 5506-X系列快速入門手冊

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

疑難排解

排除ASA連線故障不在本檔案的範圍之內，因為這適用於初始配置。 請參閱驗證和配置部分，確保所有步驟都已正確完成。