使用非默认IP或多VLAN配置ASA 5506W-X

目录

简介

本文档介绍在需要修改默认IP编址方案以适合现有网络或需要多个无线VLAN时如何执行思科自适应安全设备(ASA)5506W-X设备的初始安装和配置。 修改默认IP地址以访问无线接入点(WAP)并确保其他服务（如DHCP）继续按预期运行时，需要进行多项配置更改。 此外，本文档还提供一些集成无线接入点(WAP)的CLI配置示例，以便更轻松地完成WAP的初始配置。本文档旨在补充Cisco网站上提供的现有Cisco ASA 5506-X快速入门指南。

先决条件

本文档仅适用于包含无线接入点的Cisco ASA5506W-X设备的初始配置，并仅用于解决修改现有IP编址方案或添加其他无线VLAN时所需的各种更改。 对于默认配置安装，必须参考现有ASA 5506-X快速入门指南。

要求

Cisco 建议您了解以下主题：

- 思科ASA 5506W-X设备
- 带有终端仿真程序（如Putty、SecureCRT等）的客户端机器
- 控制台电缆和串行PC终端适配器（DB-9到RJ-45）

使用的组件

本文档中的信息基于以下软件和硬件版本：

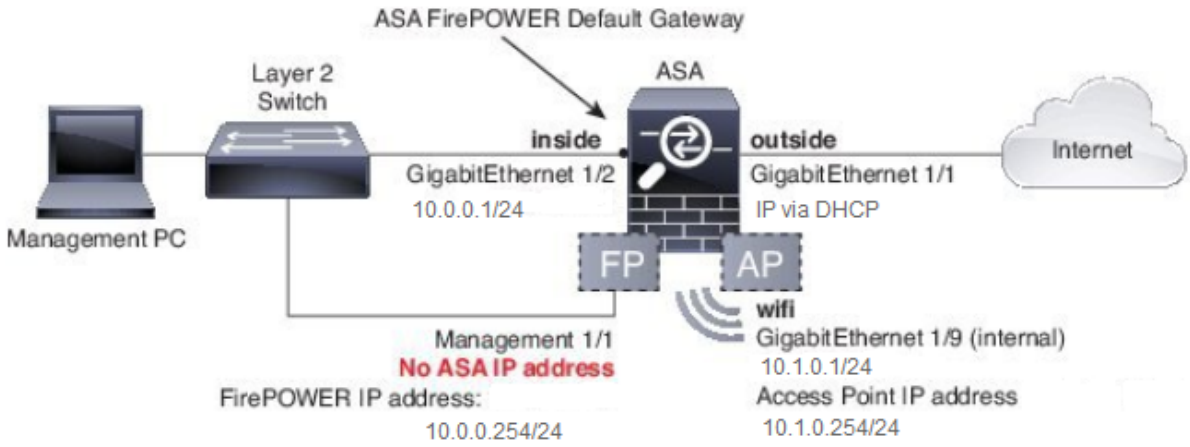
- 思科ASA 5506W-X设备
- 带有终端仿真程序（如Putty、SecureCRT等）的客户端机器
- 控制台电缆和串行PC终端适配器（DB-9到RJ-45）
- ASA FirePOWER模块
- 集成Cisco Aironet 702i无线接入点（内置WAP）

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

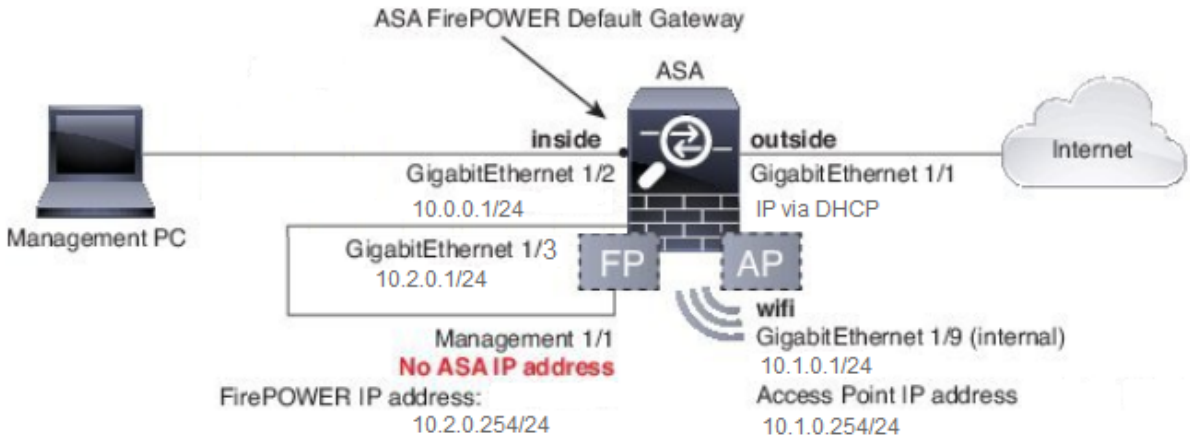
网络图

如下图所示，将应用于两种不同拓扑的IP编址示例：

带内部交换机的ASA + FirePOWER:



ASA + FirePOWER，不带内部交换机：



配置

在您通电并使用连接到客户端的控制台电缆启动ASA后，必须按顺序执行这些步骤。

步骤1.修改ASA上的接口IP配置

配置内部(GigabitEthernet 1/2)和WiFi(GigabitEthernet 1/9)接口，使其在现有环境中根据需要具有IP地址。 在本例中，内部客户端在10.0.0.1/24网络上，而WIFI客户端在10.1.0.1/24网络上。

```
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
```

注意：更改上述接口IP地址时，您将收到此警告。 这是预期。

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

步骤2.在内部和WiFi接口上修改DHCP池设置

如果ASA要用作环境中的DHCP服务器，则需要执行此步骤。 如果使用另一台DHCP服务器为客户端分配IP地址，则应在ASA上完全禁用DHCP。 由于您现在更改了我们的IP编址方案，因此您需要更改ASA为客户端提供的现有IP地址范围。 以下命令将创建新池以匹配新的IP地址范围：

```
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，修改DHCP池将禁用ASA上以前的DHCP服务器，您需要重新启用它。

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

如果在更改DHCP之前不更改接口IP地址，您将收到以下错误：

```
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
```

步骤3.指定DNS服务器以传递到内部和WiFI DHCP客户端

当它们通过DHCP分配IP地址时，大多数客户端也需要由DHCP服务器分配DNS服务器。 这些命令将配置ASA，将位于10.0.0.250的DNS服务器包括到所有客户端。 您需要将10.0.0.250替换为内部DNS服务器或ISP提供的DNS服务器。

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

步骤4.修改ASA上的HTTP访问配置，以实现自适应安全设备管理器(ASDM)访问：

由于IP编址已更改，因此还需要修改对ASA的HTTP访问，以便内部和WiFI网络上的客户端可以访问ASDM来管理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
```

> **注意**：此配置允许内部或wifi接口上的任何客户端通过ASDM访问ASA。 作为安全最佳实践，您必须将地址范围限制为仅限受信任客户端。

步骤5.在WLAN控制台（接口BVI1）中修改接入点管理的接口IP:

```
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
```

步骤6.修改WAP上的默认网关

需要执行此步骤，以便WAP知道将未在本地子网上发起的所有流量发送到何处。 要通过HTTP从ASA内部接口上的客户端访问WAP GUI，需要提供此功能。

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

步骤7.修改FirePOWER模块管理IP地址（可选）

如果您还计划部署Cisco FirePOWER（也称为SFR）模块，则您还需要更改其IP地址，以便从ASA上的物理Management1/1接口访问该模块。有两种基本部署方案可确定如何配置ASA和SFR模块：

1. ASA管理1/1接口连接到内部交换机的拓扑（根据常规快速入门指南）
2. 内部交换机不存在的拓扑。

根据您的场景，以下是适当的步骤：

如果ASA Management1/1接口连接到内部交换机：

您可以在将模块连接到内部交换机之前，先与模块进行会话并从ASA进行更改。 此配置允许您通过IP访问SFR模块，方法是将其与IP地址为10.0.0.254的ASA内部接口置于同一子网。

粗体行是本示例所特有的，是建立IP连接所必需的。

斜体行因环境而异。

```
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.
```

注意：默认访问控制策略可能需要几分钟时间才能应用于SFR模块。 完成后，您可以通过按CTRL + SHIFT + 6 + X(CTRL ^ X)从SFR模块CLI中转出并返回ASA

如果ASA未连接到内部交换机：

某些小型部署中可能不存在内部交换机。 在此类拓扑中，客户端通常通过WiFi接口连接到ASA。在此场景中，通过交叉连接管理1/1接口到另一物理ASA接口，可以消除对外部交换机的需求，并通过单独的ASA接口访问SFR模块。

在本例中，ASA GigabitEthernet1/3接口和Management1/1接口之间必须存在物理以太网连接。 接下来，您将ASA和SFR模块配置为位于单独的子网中，然后您可以从ASA以及位于内部或wifi接口上的客户端访问SFR。

ASA接口配置：

```
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模块配置：

```
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.
```

注意：默认访问控制策略可能需要几分钟时间才能应用于SFR模块。 完成后，您可以通过按CTRL + SHIFT + 6 + X(CTRL ^ X)从SFR模块CLI转出并返回ASA。

应用SFR配置后，您必须能够从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#
```

如果无法成功ping接口，请检验物理以太网连接的配置和状态。

步骤8.连接到AP GUI以启用无线电和设置其他WAP配置

此时，您应能通过HTTP GUI进行WAP管理，如快速入门指南中所述。 您需要从连接到5506W内部网络的客户端的Web浏览器浏览到WAP BVI接口的IP地址，或者可以应用示例配置并连接到WAP的SSID。如果不使用下面的CLI，则需要插入从客户端到Gigabit1/2接口的以太网电缆在ASA上。

如果您希望使用CLI配置WAP，可以从ASA与WAP建立会话并使用此示例配置。这将创建名称为5506W和5506W_5Ghz的开放SSID，以便您可以使用无线客户端连接并进一步管理WAP。

注意：应用此配置后，您将希望访问GUI并对SSID应用安全性，以便对无线流量进行加密。

使用修改的IP范围为单个无线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
```

从此开始，您可以执行正常步骤完成WAP的配置，并且必须能够从连接到上述创建的SSID的客户端的Web浏览器访问WAP。接入点的默认用户名是Cisco，密码是Cisco，密码是大写C。

Cisco ASA 5506-X系列快速入门指南

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，而不是快速入门指南中所述的192.168.10.2。

配置

产生的配置必须与输出匹配(假设您使用了示例IP范围，否则请相应地替换：

ASA 配置

接口:

注意：斜体行仅在没有内部交换机时适用：

```
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（不带示例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模块配置（带内部交换机）

```
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模块配置（不带内部交换机）

```
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

>
```

验证

要验证您是否与WAP有正确的连接以完成安装过程，请执行以下操作：

1. 将测试客户端连接到ASA内部接口，并确保其通过DHCP从ASA接收IP地址，该地址在所需IP范围内。
2. 在客户端上使用Web浏览器导航至https://10.1.0.254，并验证AP GUI现在是否可访问。
3. 从内部客户端和ASA对SFR管理接口执行ping操作，以验证连接是否正确。

使用多个无线VLAN配置DHCP

配置假设您使用单个无线VLAN。无线AP上的网桥虚拟接口(BVI)可以为多个VLAN提供网桥。由于ASA上DHCP的语法，如果要将5506W配置为多个VLAN的DHCP服务器，您需要在Gigabit1/9接口上创建子接口并为每个接口指定名称。本节将指导您完成如何删除默认配置并应用将ASA设置为多个VLAN的DHCP服务器所需的配置的过程。

步骤1.删除Gig1/9上的现有DHCP配置

首先，删除Gig1/9(wifi)接口上的现有DHCP配置：

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

步骤2.在Gig1/9上为每个VLAN创建子接口

对于您在接入点上配置的每个VLAN，您需要配置Gig1/9的子接口。在本示例配置中，您添加了两个子接口：

-Gig1/9.5，它将包含nameif vlan5，并且与VLAN 5和子网10.5.0.0/24对应。

-Gig1/9.30，它将包含nameif vlan30，并与VLAN 30和子网10.3.0.0/24对应。

实际上，此处配置的VLAN和子网必须与接入点上指定的VLAN和子网匹配。nameif和子接口编号可以是您选择的任意值。 请参阅前面提到的快速入门指南，了解链接，以便使用Web GUI配置接入点

。

```
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
```

步骤3.为每个VLAN指定DHCP池

为所配置的每个VLAN创建单独的DHCP池。此命令的语法要求您列出ASA将从中为相关池提供服务的nameif。本示例中使用VLAN 5和VLAN 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
```

步骤4.配置接入点SSID，保存配置并重置模块

最后，需要配置接入点以与ASA的配置对应。接入点的GUI界面允许您通过连接到ASA内部(Gigabit1/2)接口的客户端在AP上配置VLAN。但是，如果您希望使用CLI通过ASA控制台会话配置AP，然后无线连接以管理AP，则可以使用此配置作为模板在VLAN 5和30上创建两个SSID。必须在AP控制台中以全局配置模式输入此配置：

```
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
```

*此时，ASA和AP的管理配置必须完成，并且ASA充当VLAN 5和VLAN 30的DHCP服务器。在AP上使用**write memory**命令保存配置后，如果仍然存在连接问题，则必须使用CLI中的**reload**命令重新加载AP。但是，接收新创建的SSID的IP地址，无需进一步操作。*

```
ap#write memory
Building configuration...
[OK]
ap#reload
Proceed with reload? [confirm]
```

Writing out the event log to flash:/event.log ...

注意：您无需重新加载整个ASA设备。您只能重新加载内置接入点。

AP完成重新加载后，您必须从WiFi或内部网络上的客户端计算机连接到AP GUI。 AP完全重新启动通常需要大约两分钟。 从此开始，您可以应用常规步骤完成WAP配置。

Cisco ASA 5506-X系列快速入门指南

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

故障排除

排除ASA连接故障不在本文档的范围内，因为这是用于初始配置。 请参阅验证和配置部分，确保所有步骤均已正确完成。