配置与一非默认IP或多个VLAN配置的ASA 5506W-X

目录

简介

本文描述如何执行思科可适应安全工具(ASA) 5506W-X设备的初始安装和配置，当需要修改默认IP编址方案适合到现有的网络时或，如果多无线VLAN要求。 有要求，当正在修改默认IP地址为了访问无线接入点的几个配置更改(WAP)以及保证其他服务(例如DHCP)继续作用正如所料。 另外，本文为集成无线接入点(WAP)提供一些CLI配置示例使更加容易完成WAP的初始配置。 本文打算补充在Cisco网站的现有思科ASA 5506-X快速入门指南联机。

先决条件

本文只适用于包含无线接入点和只打算寻址需要的多种更改思科ASA5506W-X设备的初始配置，当您修改现有IP编址方案时或添加另外的无线VLAN。 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
- 有一个终端仿真程序的客户端机器例如PuTTY、SecureCRT等等。
- 控制台电缆和序列个人计算机终端适配器(对RJ-45的DB-9)

使用的组件

本文档中的信息基于以下软件和硬件版本：

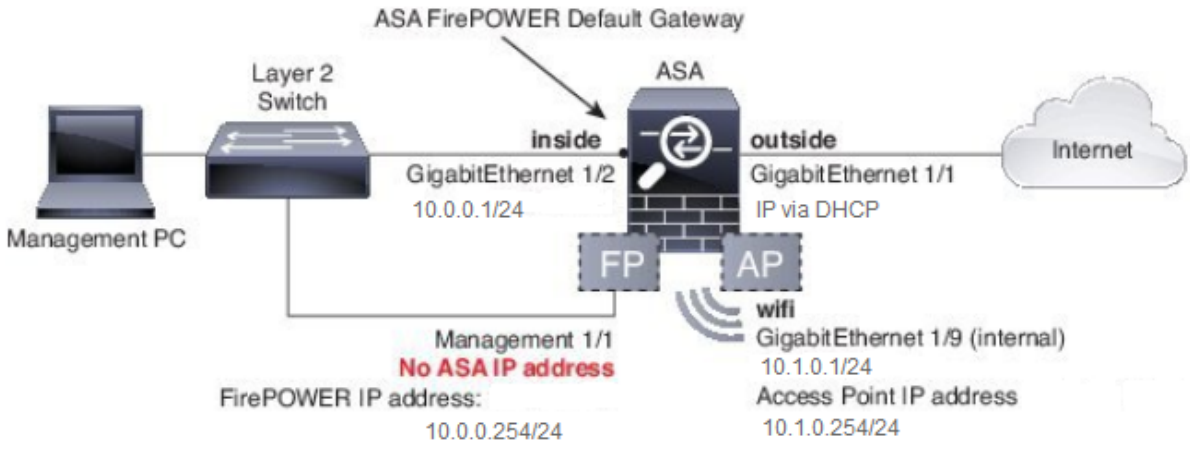
- 思科ASA 5506W-X设备
- 有一个终端仿真程序的客户端机器例如PuTTY、SecureCRT等等。
- 控制台电缆和序列个人计算机终端适配器(对RJ-45的DB-9)
- ASA Firepower模块
- 集成Cisco Aironet 702i无线接入点(内置的WAP)

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。

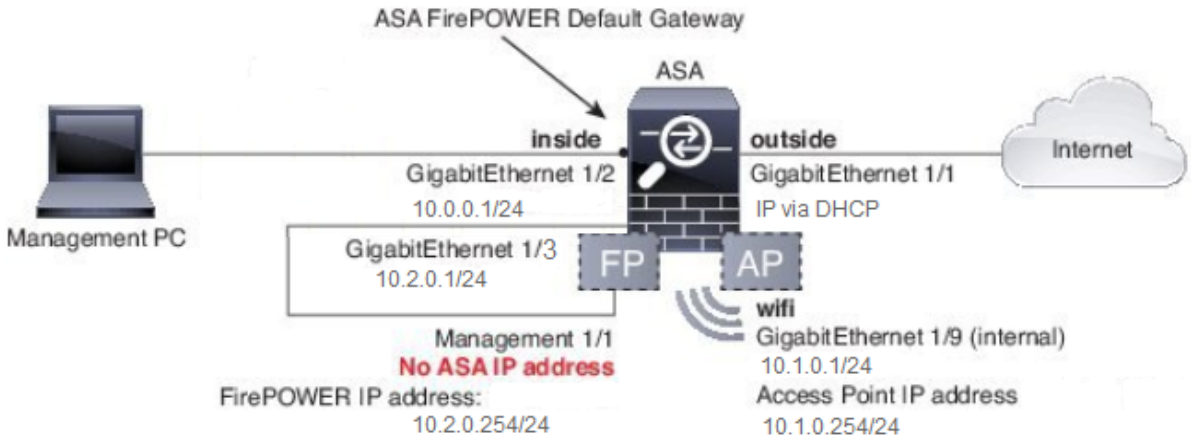
网络图

如此镜像所显示，在两不同的拓扑方面将应用IP寻址的示例：

ASA + Firepower用里面交换机：



没有里面交换机的ASA + Firepower ：



配置

在您启动并且启动ASA用控制台电缆连接对客户端后，按顺序必须执行这些步骤。

步骤1.修改在ASA的接口IP配置

配置里面(千兆以太网1/2)和wifi (千兆以太网1/9)接口有IP地址当必要时在现有的环境内。 在本例中，内部的客户端是在10.0.0.1/24网络，并且WIFI客户端是在10.1.0.1/24网络。

```
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
```

Note:当您更改上述接口IP地址，您将获得此警告。 这预计。

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

步骤2.修改在内部的两个和wifi接口的DHCP池设置

如果ASA将使用作为DHCP服务器在环境，此步骤要求。 如果另一个DHCP服务器是使用的分配IP地址给客户端那么在ASA应该一共禁用DHCP。 因为您当前更改我们的IP编址方案，您需要修改ASA提供给客户端的现有IP地址范围。 这些命令将创建新建的池匹配新的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
```

并且DHCP池的修改将禁用在ASA的上一个DHCP服务器，并且您将需要重新启用它。

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

如果不更改接口IP地址，在进行DHCP更改前您然后将收到此错误：

```
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服务器通过对内部和WiFi DHCP客户端

当他们通过DHCP时分配IP地址，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包括DNS服务器查找在10.0.0.250对所有客户端。 您需要用您的ISP或DNS服务器替代10.0.0.250提供的内部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HTTP在ASA的访问配置可适应安全设备管理器(ASDM)访问的：

因为IP寻址更改，对也ASA需要的HTTP访问被修改，以便内部和WiFi网络的客户端能访问ASDM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
```

> **Note**:此配置允许内部或wifi接口的所有客户端通过ASDM访问ASA。 作为最佳安全做法，您必须限制范围对委托客户端的仅地址。

步骤5.修改接入点管理的接口IP在WLAN控制台(接口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
```

步骤6.在WAP的修改默认网关

此步骤要求，以便WAP在哪里知道发送在本地子网没有产生的所有流量。 这要求提供通过从一个客户端的HTTP访问WAP GUI ASA内部接口的。

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

步骤7.修改Firepower模块管理IP地址(可选)

如果也计划部署思科Firepower (亦称SFR)模块那么您也需要更改其IP地址为了从在ASA的物理Management1/1接口访问它。有确定如何配置ASA和SFR模块的两个基本部署方案：

1. 方面ASA Management1/1接口连接到里面交换机的拓扑在(根据正常快速入门指南)
2. 里面交换机不存在的拓扑。

根据您的方案，这些是适当的步骤：

如果ASA Management1/1接口连接到里面交换机：

您能会话到模块和从ASA更改它在连接它前到里面交换机。 此配置允许您通过IP访问SFR模块通过放置它在相同子网作为与10.0.0.254的IP地址的ASA内部接口。

在粗体的线路是特定对此示例和为设立IP连通性要求。

线路以斜体字将由环境变化。

```
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.
```

Note:它在SFR模块可能花费默认访问控制策略的夫妇分钟能应用。 一旦它完成，您能退出在SFR模块CLI外面和回到ASA通过按CTRL+SHIFT+6 +X (CTRL ^ X)

如果ASA没有连接到里面交换机：

里面交换机在一些小部署可能不存在。 在此种拓扑方面，客户端通常会连接对ASA通过WiFi接口。 在此方案中，是可能的排除需要对于外部交换机并且通过一个分开的ASA接口访问SFR模块通过交叉连接Management1/1接口在另一个物理ASA接口。

在本例中，一个物理以太网连接必须存在ASA GigabitEthernet1/3接口和Management1/1接口之间。 其次，您配置ASA和SFR模块是在独立子网然后您能访问从在内部或wifi接口以及客户端的SFR查找的ASA。

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.
```

Note:它在SFR模块可能花费默认访问控制策略的夫妇分钟能应用。 一旦它完成，您能退出在SFR模块CLI外面和回到ASA通过按CTRL+SHIFT+6 +X (CTRL ^ X)。

一旦SFR配置适用，您一定能ping从ASA的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#
```

如果不能顺利地ping接口，请验证物理以太网连接的配置和状态。

步骤8.连接对AP GUI启用无线电和设置其他WAP配置

这时您应该有连接管理WAP通过HTTP GUI如快速入门指南所述。 您任一需要浏览到WAP的BVI接口的IP地址从连接对在5506W的网络内部客户端的Web浏览器的或您能运用配置示例和连接到WAP的SSID。 如果不使用下面的CLI，您需要接通从您的客户端的以太网电缆到在ASA的Gigabit1/2接口。

如果喜欢使用CLI配置WAP，您能会话到它从ASA和使用此配置示例。这创建与5506W和5506W_5Ghz名称的一开放SSID，以便您能使用无线客户端连接对和进一步管理WAP。

Note:在应用此配置以后您将要访问GUI和应用安全到Ssid，以便无线数据流加密。

WAP单个无线VLAN的CLI配置使用已修改IP排列

```
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
```

从这时起，您可执行正常步骤完成WAP的配置，并且您一定能从客户端的Web浏览器访问它连接对以上创建的SSID。 接入点的默认用户名是思科用思科密码与一大写C的。

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10.1.0.254的IP地址而不是192.168.10.2如快速入门指南所述。

配置

导致的配置必须匹配输出(假设您使用了示例IP范围，否则替代品相应地：

ASA 配置

接口：

Note:如果没有里面交换机，线路以斜体字只应用：

```
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(没有示例SSID设置)

```
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(用里面交换机)

```
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(没有里面交换机)

```
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

为了验证您有适当的连接对完成的安装过程WAP ：

1. 联络您的测试客户端对ASA内部接口并且保证通过DHCP收到在希望的IP范围内从ASA的一个IP地址。
2. 请使用在您的客户端的一Web浏览器为了导航到https://10.1.0.254和验证AP GUI当前可访问。
3. ping从内部的客户端和ASA的SFR管理接口验证适当的连接。

配置与多无线VLAN的DHCP

配置假设，您使用单个无线VLAN。网桥虚拟接口(BVI)在无线AP能为多个VLAN提供网桥。由于DHCP的语法在ASA，如果希望配置5506W作为多个VLAN的一个DHCP服务器，您需要创建在Gigabit1/9接口的子接口和给予每名称。此部分指南您通过进程如何删除默认配置和运用必要的配置设置ASA作为多个VLAN的一个DHCP服务器。

步骤1.存在Gig1/9的删除DHCP配置

首先，请删除在Gig1/9 (wifi)接口的现有DHCP配置：

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

步骤2.创建每个VLAN的子接口在Gig1/9

对于您在接入点配置的每个VLAN，您需要配置Gig1/9子接口。在此配置示例中，您添加两子接口：

-Gig1/9.5，将有nameif vlan5和对应于VLAN5和子网10.5.0.0/24。

-Gig1/9.30，将有nameif vlan30和对应于VLAN 30和子网10.3.0.0/24。

实际上，重要的是配置的VLAN和子网此处匹配在接入点和子网指定的VLAN。nameif和子接口号可以是您选择的任何。 使用Web GUI，请参考为链路以前提及的快速入门指南为了配置接入点。

```
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.选定每个VLAN的DHCP池

创建配置的每个VLAN的一个分开的DHCP池。此命令的语法要求您列出外面ASA将服务有问题的池的nameif在。在本例中看到的，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
```

步骤4.配置接入点Ssid，保存设置，并且重置模块

最后，接入点需要配置对应于ASA的配置。接入点的GUI界面允许您通过客户端配置在AP的VLAN连接对ASA在(Gigabit1/2)接口里面。然而，如果喜欢使用CLI通过ASA控制台会话配置AP然后连接无线地管理AP，您能使用此配置作为模板创建在VLAN 5和30的两Ssid。 必须在全局配置模式的AP控制台内输入这：

```
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
```

*这时， ASA的管理配置和AP一定完成，并且ASA作为VLAN的5和30一个DHCP服务器。 在保存配置以后使用**write memory命令**在AP，如果仍然有连通性问题然后您使用**reload命令**从CLI，必须重新加载AP。 然而，如果收到在新建立的Ssid的一个IP地址然后进一步操作没有要求。*

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

Note:您不需要重新加载整个ASA设备。您必须只重新加载内置的接入点。

一旦AP完成重新加载，然后您必须有连接到从一个客户端机器的AP GUI在wifi或网络内部。 通常需要大约AP的两分钟能完全重新启动。 从这时起，您能运用正常步骤完成WAP的配置。

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

排除故障ASA连接是在本文的范围之外，因为这供初始配置使用。 请参考验证和配置部分保证所有步骤适当地完成。