Contents

Introduction

This document describes how to perform initial installation and configuration of a Cisco Adaptive Security Appliance (ASA) 5506W-X device when the default IP addressing scheme needs to be modified to fit into an existing network or if multiple wireless VLANs are required. There are several configuration changes that are required when modifying the default IP addresses in order to access the wireless access point (WAP) as well as ensure that other services (such as DHCP) continue to function as expected. In addition, this document provides some CLI configuration examples for the integrated Wireless Access Point (WAP) to make it easier to complete initial configuration of the WAP. This document is intended to supplement the existing Cisco ASA 5506-X Quick Start guide available on the Cisco website.

Prerequisites

This document only applies to the initial configuration of a Cisco ASA5506W-X device that contains a wireless access point and is only intended to address the various changes needed when you modify the existing IP addressing scheme or add additional wireless VLANs. For default configuration installations, the existing ASA 5506-X Quick Start Guide must be referenced.

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco ASA 5506W-X device
- Client machine with a terminal emulation program such as Putty, SecureCRT, etc.
- Console Cable and Serial PC Terminal Adapter (DB-9 to RJ-45)

Components Used

The information in this document is based on these software and hardware versions:

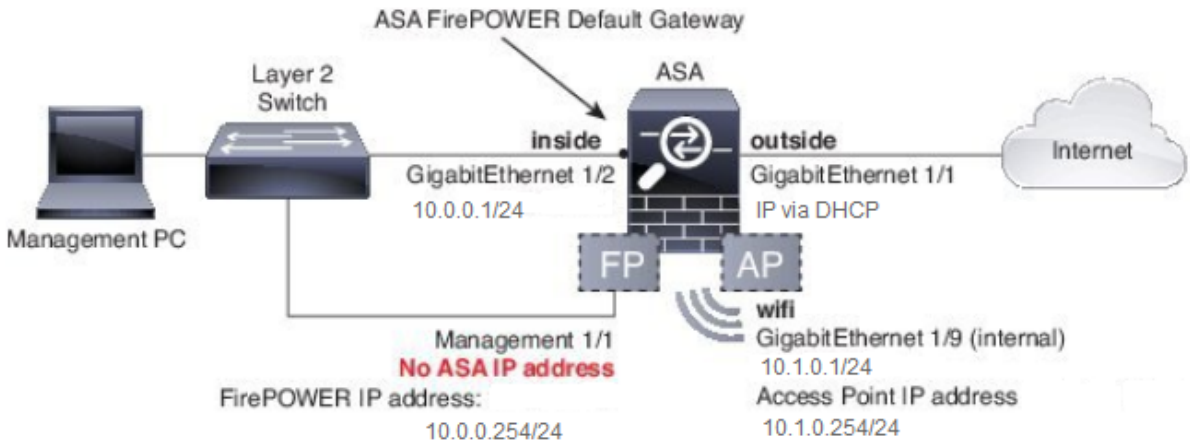
- Cisco ASA 5506W-X device
- Client machine with a terminal emulation program such as Putty, SecureCRT, etc.
- Console Cable and Serial PC Terminal Adapter (DB-9 to RJ-45)
- ASA FirePOWER Module
- Integrated Cisco Aironet 702i wireless access point (Built-in WAP)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

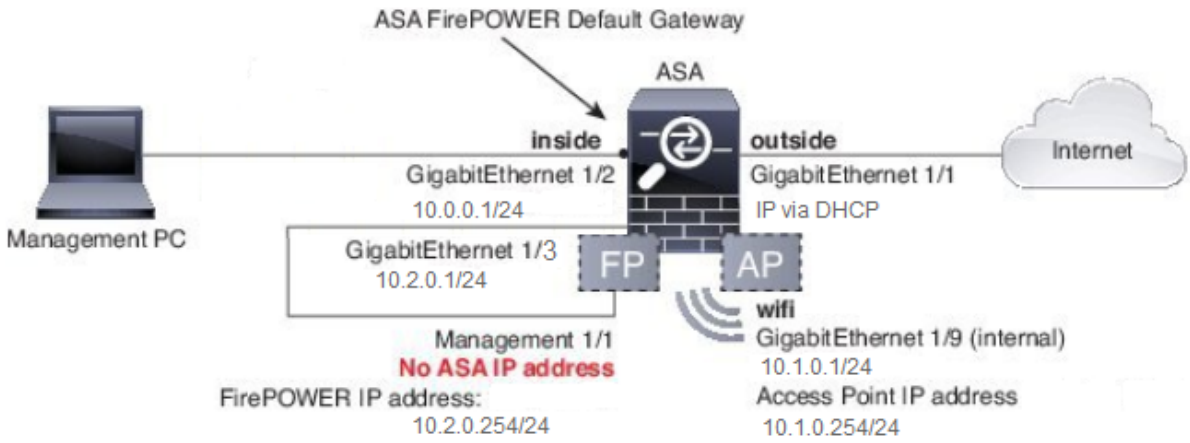
Network Diagrams

As shown in this image, examples of the IP addressing that will be applied in two different topologies:

ASA + FirePOWER with an inside switch:



ASA + FirePOWER without an inside switch:



Configure

These steps must be performed in order after you power on and boot the ASA with the console cable connected to the client.

Step 1. Modify Interface IP configuration on ASA

Configure the inside (GigabitEthernet 1/2) and wifi (GigabitEthernet 1/9) interfaces to have IP addresses as needed within the existing environment. In this example, inside clients are on the 10.0.0.1/24 network and WIFI clients are on the 10.1.0.1/24 network.

```
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**: You will get this warning when you change the above interface IP addresses. This is expected.

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

Step 2. Modify DHCP pool settings on both inside and wifi interfaces

This step is required if the ASA is to be used as the DHCP server in the environment. If another DHCP server is used to assign IP addresses to clients then DHCP should be disabled on the ASA altogether. Since you have now changed our IP addressing scheme, you need to alter the existing IP address ranges that the ASA is providing to clients. These commands will create new pools to match the new IP address range:

```
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
```

Also the modification of the DHCP pools will disable the previous DHCP server on the ASA, and

you will need to re-enable it.

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

If you do not change the interface IP addresses before making the DHCP changes then you will receive this error:

```
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
```

Step 3. Specify DNS server to pass to inside and WiFI DHCP clients

When they assign IP addresses via DHCP, most clients also need to be assigned a DNS server by the DHCP server. These commands will configure the ASA to include the DNS server located at 10.0.0.250 to all clients. You need to substitute the 10.0.0.250 for either an internal DNS server or a DNS server provided by your ISP.

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

Step 4. Modify HTTP access configuration on the ASA for Adaptive Security Device Manager (ASDM) access:

Since the IP addressing has been changed, HTTP access to the ASA also needs to be modified so that clients on the inside and WiFI networks can access ASDM to manage the 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**: This configuration allows any client on the inside or wifi interfaces to access the ASA via ASDM. As a security best practice, you must limit the scope of addresses to trusted clients only.

Step 5. Modify Interface IP for 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
```

Step 6. Modify default-gateway on WAP

This step is required so that the WAP knows where to send all traffic that is not originated on the local subnet. This is required to provide to access the WAP GUI via HTTP from a client on the ASA inside interface.

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

Step 7. Modify the FirePOWER Module Management IP Address (Optional)

If you also plan to deploy the Cisco FirePOWER (also known as SFR) module then you also need to change its IP address in order to access it from the physical Management1/1 interface on the ASA. There are two basic deployment scenarios that determine how to configure the ASA and the SFR module:

1. A topology in which the ASA Management1/1 interface is connected to an inside switch (as per the normal quick start guide)
2. A topology where an inside switch is not present.

Depending on your scenario,these are the appropriate steps:

If the ASA Management1/1 interface is connected to an inside switch:

You can session into the module and change it from the ASA before connecting it to an inside switch. This configuration allows you to access the SFR module via IP by placing it on the same subnet as the ASA inside interface with an IP address of 10.0.0.254.

Lines in bold are specific to this example and are required for establishing IP connectivity.

Lines in italics will vary by environment.

```
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]: 10.0.0.254Enter 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: It may take a couple minutes for the default access control policy to apply on the SFR

module. Once it is complete, you can escape out of the SFR module CLI and back into the ASA by pressing CTRL + SHIFT + 6 +X (CTRL ^ X)

If the ASA is NOT connected to an inside switch:

An inside switch may not exist in some small deployments. In this type of topology, clients would generally connect to the ASA via the WiFi interface. In this scenario, it is possible eliminate the need for an external switch and access the SFR module via a separate ASA interface by cross-connecting the Management1/1 interface to another physical ASA interface.

In this example, a physical ethernet connection must exist between the ASA GigabitEthernet1/3 interface and the Management1/1 interface. Next, you configure the ASA and SFR module to be on a separate subnet and then you are able to access the SFR from both the ASA as well as clients located on the inside or wifi interfaces.

ASA Interface Configuration:

```
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 Module Configuration:

```
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: It may take a couple minutes for the default access control policy to apply on the SFR module. Once it is complete, you can escape out of the SFR module CLI and back into the

ASA by pressing CTRL + SHIFT + 6 +X (CTRL ^ X).

Once the SFR configuration applies, you must be able to ping the SFR management IP address from the ASA:

```
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#
```

If you cannot ping the interface successfully, verify the configuration and state of physical ethernet connections.

Step 8. Connect to AP GUI to enable radios and set other WAP configuration

At this point you should have connectivity to manage the WAP via the HTTP GUI as discussed in the quick start guide. You will either need to browse to the IP address of the WAP's BVI interface from a web browser of a client that is connected to the inside network on the 5506W or you can apply the example configuration and connect to the SSID of the WAP. If you do not use the CLI below, you need to plug in the ethernet cable from your client to the Gigabit1/2 interface on the ASA.

If you prefer to use the CLI to configure the WAP, you can session into it from the ASA and use this example configuration. This creates an open SSID with the name of 5506W and 5506W_5Ghz so that you can use a wireless client to connect to and further manage the WAP.

> **Note**: After applying this configuration you will want to access the GUI and apply security to the SSIDs so that the wireless traffic is encrypted.

WAP CLI Configuration for a single wireless VLAN using modified IP ranges

```
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
```

From this point on, you can perform the normal steps to complete the configuration of the WAP and you must be able to access it from the web browser of a client connected to the above created SSID. The default username of the access point is Cisco with a password of Cisco with a capital C.

Cisco ASA 5506-X Series Quick Start Guide

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

You need to use the IP address of 10.1.0.254 instead of the 192.168.10.2 as stated in the Quick Start Guide.

Configurations

The resulting configuration must match the output (assuming you used the example IP ranges, otherwise substitute accordingly:

ASA Configuration

Interfaces:

> **Note**: The lines in italics only apply if you do NOT have an inside switch:

```
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 (without the example SSID config)

```
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 Configuration (with inside 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 Configuration (without inside 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

>
```

Verify

In order to verify that you have the proper connectivity to the WAP for completing the installation process:

1. Connect your test client to the ASA inside interface and ensure that it receives an IP address from the ASA via DHCP that is within the desired IP range.
2. Use a web browser on your client in order to navigate to https://10.1.0.254 and verify that the AP GUI is now accessible.
3. Ping the SFR management interface from the inside client and the ASA to verify proper connectivity.

Configure DHCP with Multiple Wireless VLANs

The configuration assumes that you use a single wireless VLAN. The Bridge Virtual Interface (BVI) on the Wireless AP can provide a bridge for Multiple VLANs. Because of the syntax for DHCP on the ASA, if you wish to configure the 5506W as a DHCP server for multiple VLANs, you need to create subinterfaces on the Gigabit1/9 interface and give each a name. This section guides you through the process of how to remove the default configuration and to apply the configuration necessary to set the ASA up as a DHCP server for multiple VLANs.

Step 1. Remove Existing DHCP configuration on Gig1/9

First, remove the existing DHCP configuration on the Gig1/9 (wifi) interface:

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

Step 2. Create Subinterfaces for Each VLAN on Gig1/9

For each VLAN that you have configured on the access point, you need to configure a subinterface of Gig1/9. In this example configuration, you add two subinterfaces:

-Gig1/9.5, which will have nameif vlan5, and will correspond to VLAN 5 and subnet 10.5.0.0/24.

-Gig1/9.30, which will have nameif vlan30, and will correspond to VLAN 30 and subnet 10.3.0.0/24.

In practice, it is essential that the VLAN and subnet configured here match the VLAN and subnet specified on the access point. The nameif and subinterface number can be anything you choose. Please refer to the quick start guide previously mentioned for links in order to configure the access point using the web GUI.

```
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
```

Step 3. Designate a DHCP pool for each VLAN

Create a separate DHCP pool for each VLAN being configured. The syntax for this command requires that you list the nameif out of which the ASA will serve the pool in question. A seen in this example, which uses VLANs 5 and 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
```

Step 4. Configure the Access Point SSIDs, save the config, and reset the module

Finally, the access point needs to be configured to correspond to the ASA's configuration. The GUI interface for the access point allows you to configure VLANs on the AP via the client connected to the ASA inside (Gigabit1/2) interface. However, if you prefer to use CLI to configure the AP via the ASA console session and then connect wirelessly to manage the AP, you can use this configuration as a template for creating two SSIDs on VLANs 5 and 30. This must be entered within the AP console in global configuration mode:

```
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
```
At this point, the management configuration of the ASA and AP must be complete, and the ASA acts as a DHCP server for VLANs 5 and 30. After saving the configuration using the ***write memory*** *command on the AP, if you still have connectivity issues then you must reload the AP using the* ***reload*** *command from the CLI. However, if you receive an IP address on the newly created SSIDs then no further action is required.*
```
ap#write memory
Building configuration...
[OK]
ap#reload
Proceed with reload? [confirm]
Writing out the event log to flash:/event.log ...
```

> **Note**: You do NOT need to reload the entire ASA device. You must only reload the built-in access point.

Once the AP finishes reloading, then you must have connectivity to the AP GUI from a client machine on the wifi or inside networks. It generally takes about two minutes for the AP to completely reboot. From this point on, you can apply the normal steps to complete the configuration of the WAP.

Cisco ASA 5506-X Series Quick Start Guide

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

Troubleshoot

Troubleshooting ASA connectivity is outside the scope of this document since this is intended for initial configuration. Please refer to the verify and configuration sections to ensure that all steps have been properly completed.