# Configurar o ASA 5506W-X com uma configuração não-padrão IP ou de vlan múltiplo

## Índice


Introdução
Pré-requisitos
Requisitos
Componentes Utilizados
Diagramas da rede
Configurar
Etapa 1. Altere a configuração IP da relação no ASA
Etapa 2. Altere ajustes do conjunto de DHCP em ambos internos e em relações do wifi
Etapa 3. Especifique o servidor DNS para passar aos clientes DHCP internos e de WiFi
Etapa 4. Altere a configuração do acesso HTTP no ASA para o acesso adaptável do Security Device Manager (ASDM):
Etapa 5. Altere o IP da relação para o Gerenciamento do Access point no console WLAN (relação BVI1):
Etapa 6. Altere o gateway padrão no WAP
Etapa 7. Altere o endereço IP de gerenciamento do módulo de FirePOWER (opcional)
Se a relação ASA Management1/1 é conectada a um interno comute:
Se o ASA não é conectado a um interno comute:
Etapa 8. Conecte a AP GUI para permitir rádios e ajustar a outra configuração WAP
A configuração de CLI WAP para um único VLAN sem fio que usa o IP alterado varia
Configurações
Configuração ASA
Configuração de Aironet WAP (sem a configuração do exemplo SSID)
Configuração de módulo de FirePOWER (com interruptor interno)
Configuração de módulo de FirePOWER (sem interruptor interno)
Verificar
Configurar o DHCP com VLAN sem fio múltiplos
Etapa 1. Remova configuração de DHCP existente em Gig1/9
Etapa 2. Crie subinterfaces para cada VLAN em Gig1/9
Etapa 3. Designe um conjunto de DHCP para cada VLAN
Etapa 4. Configurar o Access point SSID, salvar a configuração, e restaure o módulo
Troubleshooting


## Introdução

Este documento descreve como executar a instalação inicial e a configuração de um dispositivo 5506W-X adaptável da ferramenta de segurança de Cisco (ASA) quando o método de endereçamento do IP padrão precisa de ser alterado para caber em uma rede existente ou se os VLAN sem fio múltiplos estão exigidos.  Há diversas alterações de configuração que são exigidas ao alterar os endereços IP padrão a fim alcançar o ponto de acesso Wireless (WAP) assim como

se assegurar de que os outros serviços (tais como o DHCP) continuem a funcionar como esperado.  Além, este documento fornece alguns exemplos da configuração de CLI para o ponto de acesso Wireless integrado (WAP) para facilitá-lo terminar a configuração inicial do WAP.  Este documento é pretendido suplementar o guia de início rápido existente de Cisco ASA 5506-X disponível na site da Cisco na Web.

# Pré-requisitos

Este documento aplica-se somente à configuração inicial de um dispositivo de Cisco ASA5506W-X que contenha um ponto de acesso Wireless e esteja pretendido somente endereçar as várias mudanças necessárias quando você altera o esquema de endereçamento de IP existente ou adiciona-se VLAN sem fio adicionais.  Para as instalações da configuração padrão, o guia de início rápido existente ASA 5506-X deve ser provido.

## Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Dispositivo de Cisco ASA 5506W-X
- Máquina cliente com um programa de simulação terminal tal como a massa de vidraceiro, o SecureCRT, etc.
- Cabo do console e adaptador do terminal de PC da série (DB-9 ao RJ-45)

## Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

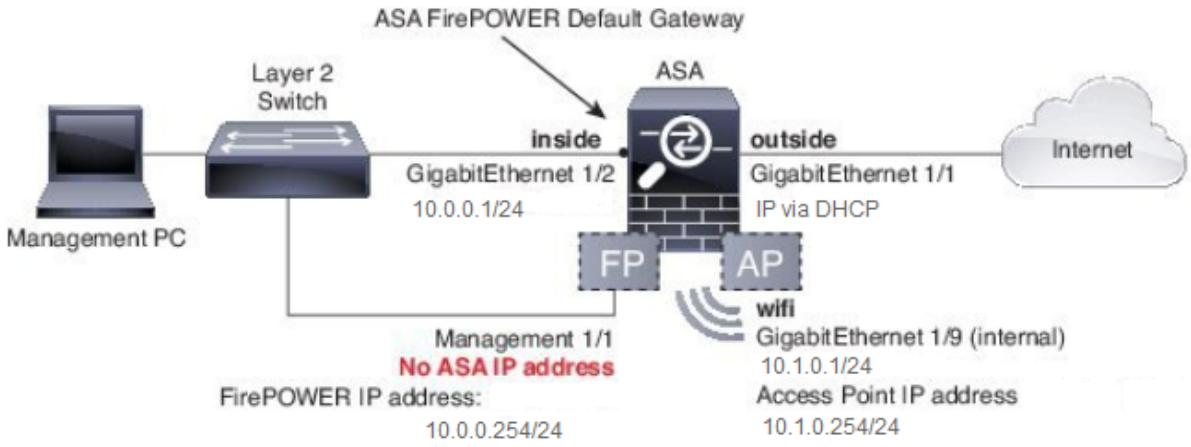
- Dispositivo de Cisco ASA 5506W-X
- Máquina cliente com um programa de simulação terminal tal como a massa de vidraceiro, o SecureCRT, etc.
- Cabo do console e adaptador do terminal de PC da série (DB-9 ao RJ-45)
- Módulo ASA FirePOWER
- Ponto de acesso Wireless integrado do Cisco Aironet 702i (acessório WAP)

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

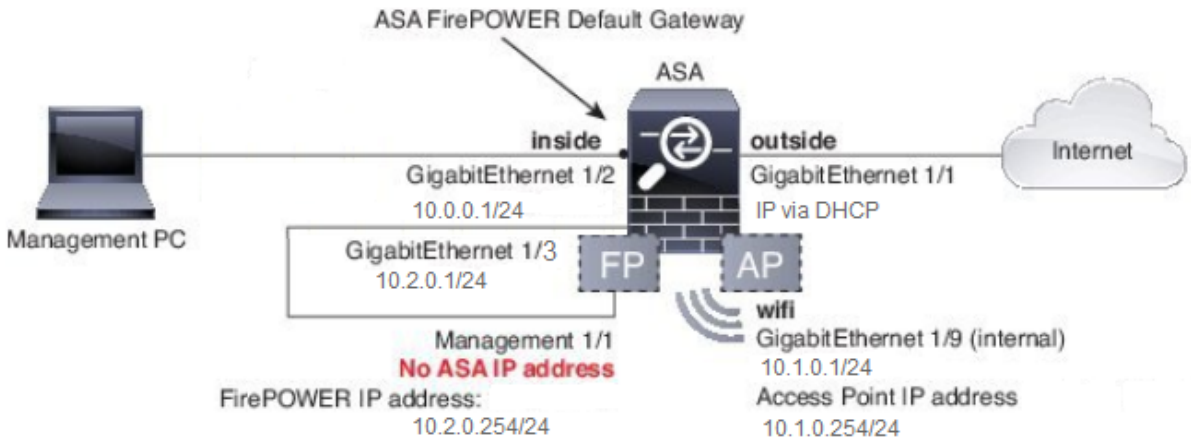
# Diagramas da rede

Segundo as indicações desta imagem, exemplos do endereçamento de IP que será aplicado em duas topologias diferentes:

**ASA + FirePOWER com um interruptor interno:**




**ASA + FirePOWER sem um interruptor interno:**




# Configurar

Estas etapas devem ser executadas em ordem depois que você põe sobre e carreg o ASA com o cabo do console conectado ao cliente.

## Etapa 1. Altere a configuração IP da relação no ASA

Configurar o interior (gigabitethernet 1/2) e relações do wifi (gigabitethernet 1/9) para ter endereços IP de Um ou Mais Servidores Cisco ICM NT como necessários dentro do ambiente existente.  Neste exemplo, os clientes internos estão nas 10.0.0.1/24 redes e os clientes de WIFI estão na rede 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
```

**Note**: Você obterá este aviso quando você muda os endereços IP de Um ou Mais

Servidores Cisco ICM NT acima da relação.  Isto é esperado.

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

## Etapa 2. Altere ajustes do conjunto de DHCP em ambos internos e em relações do wifi

Esta etapa é exigida se o ASA deve ser usada como o servidor DHCP no ambiente.  Se um outro servidor DHCP é usado para atribuir endereços IP de Um ou Mais Servidores Cisco ICM NT aos clientes então o DHCP deve ser desabilitado no ASA completamente.  Desde que você tem mudado agora nosso esquema de endereçamento de IP, você precisa de alterar os intervalos de endereço IP existentes que o ASA está fornecendo aos clientes.  Estes comandos criarão associações novas para combinar o intervalo de endereço IP novo:

```
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
```

Igualmente a alteração dos conjuntos de DHCP desabilitará o servidor DHCP precedente no ASA, e você precisará re-de permiti-lo.

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

Se você não muda os endereços IP de Um ou Mais Servidores Cisco ICM NT da relação antes de fazer as mudanças DHCP então você receberá este erro:

```
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
```

## Etapa 3. Especifique o servidor DNS para passar aos clientes DHCP internos e de WiFi

Quando atribuem endereços IP de Um ou Mais Servidores Cisco ICM NT através do DHCP, a maioria de clientes igualmente precisam de ser atribuídos um servidor DNS pelo servidor DHCP. Estes comandos configurarão o ASA para incluir o servidor DNS situado em 10.0.0.250 a todos os clientes.  Você precisa de substituir 10.0.0.250 para um servidor interno de DNS ou um servidor DNS fornecido por seu ISP.

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

## Etapa 4. Altere a configuração do acesso HTTP no ASA para o acesso adaptável do Security Device Manager (ASDM):

Desde que o endereçamento de IP foi mudado, acesso HTTP ASA às necessidades igualmente de ser alterado de modo que os clientes nas redes internas e de WiFi possam alcançar o ASDM para controlar o 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**: Esta configuração permite que todo o cliente nas relações internas ou do wifi alcance o ASA através do ASDM. Como um melhor prática da Segurança, você deve limitar o espaço dos endereços aos clientes confiados somente.

## Etapa 5. Altere o IP da relação para o Gerenciamento do Access point no console WLAN (relação 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
```

## Etapa 6. Altere o gateway padrão no WAP

Esta etapa é exigida de modo que o WAP saiba onde enviar todo o tráfego que não é originado na sub-rede local. Isto é exigido para fornecer para alcançar o WAP GUI através do HTTP de um cliente na interface interna ASA.

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

## Etapa 7. Altere o endereço IP de gerenciamento do módulo de FirePOWER (opcional)

Se você igualmente planeia distribuir o módulo de Cisco FirePOWER (igualmente conhecido como SFR) então você igualmente precisa de mudar seu endereço IP de Um ou Mais Servidores Cisco ICM NT a fim alcançá-lo da relação Management1/1 física no ASA. Há dois cenários de distribuição básicos que determinam como configurar o ASA e o módulo SFR:

1. Uma topologia em que a relação ASA Management1/1 é conectada a um interruptor interno (conforme o guia de início rápido normal)
2. Uma topologia onde um interruptor interno não está atual.

Segundo sua encenação, estas são as etapas apropriadas:

### Se a relação ASA Management1/1 é conectada a um interno comute:

Você pode sessão no módulo e para mudá-lo do ASA antes de conectá-lo a um interruptor interno. Esta configuração permite que você alcance o módulo SFR através do IP colocando o na mesma sub-rede como a interface interna ASA com um endereço IP de Um ou Mais Servidores Cisco ICM NT de 10.0.0.254.

As linhas em corajoso são específicas a este exemplo e são exigidas estabelecendo a conectividade IP.

As linhas nos itálicos variarão pelo ambiente.

```
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**: Pode tomar minutos de um par para que a política do controle de acesso do padrão aplique-se no módulo SFR.  Uma vez que está completa, você pode escapar fora do módulo CLI SFR e de novo no ASA pressionando CTRL + SHIFT + 6 +X (^ CTRL X)

### Se o ASA não é conectado a um interno comute:

Um interruptor interno não pode existir em algumas disposições pequenas.  Neste tipo de topologia, os clientes conectariam geralmente ao ASA através da relação de WiFi.  Nesta encenação, é possível elimina a necessidade para um switch externo e alcança o módulo SFR através de uma relação separada ASA cruz-conectando a relação Management1/1 a uma outra relação física ASA.

Neste exemplo, uma conexão Ethernet física deve existir entre a relação ASA GigabitEthernet1/3 e a relação Management1/1. Em seguida, você configura o módulo ASA e SFR para estar em uma sub-rede separada e então você pode alcançar o SFR do ASA assim como dos clientes situados nas relações internas ou do wifi.

### Configuração da interface ASA:

```
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
```

### Configuração de módulo SFR:

```
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**: Pode tomar minutos de um par para que a política do controle de acesso do padrão aplique-se no módulo SFR. Uma vez que está completa, você pode escapar fora do módulo CLI SFR e de novo no ASA pressionando CTRL + SHIFT + 6 +X (^ CTRL X).

Uma vez que a configuração SFR se aplica, você deve poder sibilar o endereço IP de gerenciamento SFR do 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#
```

Se você não pode sibilar a relação com sucesso, verifique a configuração e o estado de conexões Ethernet físicas.

## Etapa 8. Conecte a AP GUI para permitir rádios e ajustar a outra configuração WAP

Neste momento você deve ter a Conectividade para controlar o WAP através do HTTP GUI como discutido no guia de início rápido.  Você uma ou outra necessidade de consultar ao endereço IP de Um ou Mais Servidores Cisco ICM NT da interface de BVI do WAP de um navegador da Web de um cliente que seja conectado à rede interna no 5506W ou você pode aplicar o exemplo de configuração e conectá-lo ao SSID do WAP.  Se você não usa o CLI abaixo, você precisa de obstruir dentro o cabo do Ethernet de seu cliente à relação Gigabit1/2 no ASA.

Se você prefere usar o CLI para configurar o WAP, você pode sessão nela do ASA e para usar este exemplo de configuração. Isto cria um SSID aberto com o nome de 5506W e de 5506W_5Ghz de modo que você possa usar um cliente Wireless para conectar a e para controlar mais o WAP.

> **Note**: Após ter aplicado esta configuração você quererá alcançar o GUI e aplicar a Segurança aos SSID de modo que o tráfego Wireless seja cifrado.

### A configuração de CLI WAP para um único VLAN sem fio que usa o IP alterado varia

```
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
```

A partir daqui, você pode executar as etapas normais para terminar a configuração do WAP e você deve poder alcançá-lo do navegador da Web de um cliente conectado ao SSID acima criado.  O nome de usuário padrão do Access point é Cisco com uma senha de Cisco com um C principal.

### Guia de início rápido do 5506-X Series de Cisco ASA

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

Você precisa de usar o endereço IP de Um ou Mais Servidores Cisco ICM NT de 10.1.0.254 em vez de 192.168.10.2 como exposto no guia de início rápido.

## Configurações

A configuração resultante deve combinar a saída (o supor usou as escalas, se não o substituto IP do exemplo em conformidade:

### Configuração ASA

Relações:

> **Note**: As linhas nos itálicos aplicam-se somente se você não tem um interruptor interno:

```
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#
```

## Configuração de Aironet WAP (sem a configuração do exemplo SSID)

```
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
```

## Configuração de módulo de FirePOWER (com interruptor interno)

```
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

>
```

## Configuração de módulo de FirePOWER (sem interruptor interno)

```
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

>
```

# Verificar

A fim verificar que você tem a conectividade apropriada ao WAP para terminar o processo de instalação:

1. Conecte seu cliente de teste à interface interna ASA e assegure-se de que receba um endereço IP de Um ou Mais Servidores Cisco ICM NT do ASA através do DHCP que está dentro da escala desejada IP.
2. Use um navegador da Web em seu cliente a fim navegar a https://10.1.0.254 e verificar que o AP GUI é agora acessível.
3. Sibile a interface de gerenciamento SFR do cliente interno e do ASA para verificar a conectividade apropriada.

## Configurar o DHCP com VLAN sem fio múltiplos

A configuração supõe que você usa um único VLAN sem fio. O Bridge Virtual Interface (BVI) no Sem fio AP pode fornecer uma ponte para vlan múltiplos. Devido à sintaxe para o DHCP no ASA, se você deseja configurar o 5506W como um servidor DHCP para vlan múltiplos, você precisa de criar subinterfaces na relação Gigabit1/9 e de dar cada um nome. Esta seção guia-o com o processo de como remover a configuração padrão e aplicar a configuração necessária configurar o ASA como um servidor DHCP para vlan múltiplos.

### Etapa 1. Remova configuração de DHCP existente em Gig1/9

Primeiramente, remova a configuração de DHCP existente (wifi) na relação Gig1/9:

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

### Etapa 2. Crie subinterfaces para cada VLAN em Gig1/9

Para cada VLAN que você configurou no Access point, você precisa de configurar uma subinterface de Gig1/9. Neste exemplo de configuração, você adiciona duas subinterfaces:

-Gig1/9.5, que terá o nameif vlan5, e corresponderá a VLAN 5 e sub-rede 10.5.0.0/24.

-Gig1/9.30, que terá o nameif vlan30, e corresponderá ao VLAN 30 e à sub-rede 10.3.0.0/24.

Na prática, é essencial que o VLAN e a sub-rede configurados aqui combinam o VLAN e a sub-rede especificados no Access point. O número do nameif e da subinterface pode ser qualquer coisa que você escolhe.  Refira por favor o guia de início rápido mencionado previamente para os links a fim configurar o Access point usando a 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
```

### Etapa 3. Designe um conjunto de DHCP para cada VLAN

*Crie um conjunto de DHCP separado para cada VLAN que está sendo configurado. A sintaxe para este comando exige que você alista o nameif fora de que o ASA servirá o pool na pergunta. Visto neste exemplo, que usa VLAN 5 e 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
```

### Etapa 4. Configurar o Access point SSID, salvar a configuração, e restaure o módulo

Finalmente, o Access point precisa de ser configurado para corresponder à configuração do ASA. A interface GUI para o Access point permite que você configure VLAN no AP através do cliente conectado ao ASA dentro da relação (Gigabit1/2). Contudo, se você prefere usar o CLI para configurar o AP através da sessão de console ASA e para o conectar então sem fio para controlar o AP, você pode usar esta configuração como um molde para criar dois SSID em VLAN 5 e 30.  Isto deve ser entrado dentro do console AP no modo de configuração global:

```
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
```

*Neste momento, a configuração de gerenciamento do ASA e o AP devem estar completos, e o ASA atua como um servidor DHCP para VLAN 5 e 30. Após ter salvar a configuração usar o* ***comando write memory no*** *AP, se você ainda tem problemas de conectividade então você deve recarregar o AP usando o* ***comando reload do*** *CLI. Contudo, se você recebe um endereço IP de Um ou Mais Servidores Cisco ICM NT nos SSID recém-criados então nenhuma ação mais adicional é exigida.*

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

> **Note**: Você não precisa de recarregar o dispositivo inteiro ASA. Você deve somente recarregar o Access point incorporado.

Uma vez que o AP termina recarregar, a seguir você deve ter a Conectividade ao AP GUI de uma máquina cliente no wifi ou nas redes internas. Toma geralmente aproximadamente dois minutos para que o AP recarregue completamente. A partir daqui, você pode aplicar as etapas normais para terminar a configuração do WAP.

### Guia de início rápido do 5506-X Series de Cisco ASA

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

# Troubleshooting

Pesquisar defeitos a Conectividade ASA é fora do âmbito deste documento desde que esta é pretendida para a configuração inicial. Refira por favor a verificação e as seções de configuração para assegurar-se de que todas as etapas estejam terminadas corretamente.