Configure o ASA 5506W-X com uma configuração de IP não padrão ou de várias VLANs

Contents

Introduction

Este documento descreve como executar a instalação inicial e a configuração de um dispositivo Cisco Adaptive Security Appliance (ASA) 5506W-X quando o esquema de endereçamento IP padrão precisa ser modificado para se ajustar a uma rede existente ou se várias VLANs sem fio

são necessárias. Há várias alterações de configuração que são necessárias ao modificar os endereços IP padrão para acessar o ponto de acesso sem fio (WAP) e garantir que outros serviços (como o DHCP) continuem funcionando conforme esperado. Além disso, este documento fornece alguns exemplos de configuração de CLI para o WAP (Wireless Access Point, ponto de acesso sem fio) integrado para facilitar a configuração inicial do WAP. Este documento destina-se a complementar o guia de início rápido do Cisco ASA 5506-X existente disponível no site da Cisco.

Prerequisites

Este documento aplica-se somente à configuração inicial de um dispositivo Cisco ASA5506W-X que contém um ponto de acesso sem fio e destina-se somente a endereçar as várias alterações necessárias quando você modifica o esquema de endereçamento IP existente ou adiciona VLANs sem fio adicionais. Para instalações de configuração padrão, o Guia de início rápido do ASA 5506-X existente deve ser referenciado.

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Dispositivo Cisco ASA 5506W-X
- Máquina cliente com um programa de emulação de terminal como Putty, SecureCRT etc.
- Cabo do console e adaptador do terminal do PC serial (DB-9 para RJ-45)

Componentes Utilizados

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

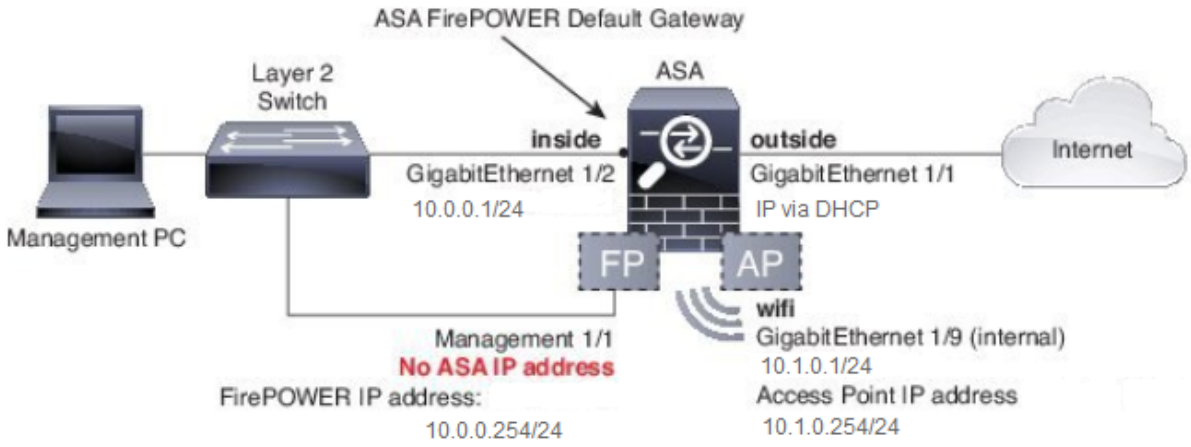
- Dispositivo Cisco ASA 5506W-X
- Máquina cliente com um programa de emulação de terminal como Putty, SecureCRT etc.
- Cabo do console e adaptador do terminal do PC serial (DB-9 para RJ-45)
- Módulo ASA FirePOWER
- Access point sem fio Cisco Aironet 702i integrado (WAP integrado)

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.

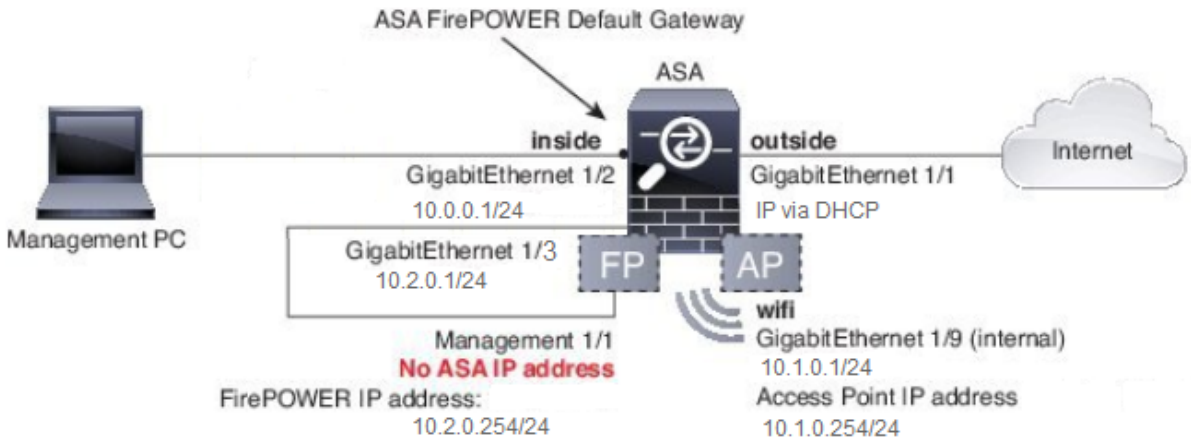
Diagramas de rede

Como mostrado nesta imagem, exemplos do endereçamento IP que serão aplicados em duas topologias diferentes:

ASA + FirePOWER com um switch interno:



ASA + FirePOWER sem um switch interno:



Configurar

Essas etapas devem ser executadas em ordem depois que você ligar e inicializar o ASA com o cabo de console conectado ao cliente.

Etapa 1. Modificar a configuração IP da interface no ASA

Configure as interfaces internas (GigabitEthernet 1/2) e wifi (GigabitEthernet 1/9) para ter endereços IP conforme necessário no ambiente existente. Neste exemplo, os clientes internos estão na rede 10.0.0.1/24 e os clientes 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 receberá esse aviso quando alterar os endereços IP da interface acima. Isso é esperado.

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

Etapa 2. Modificar as configurações do pool DHCP em interfaces internas e wifi

Essa etapa é necessária se o ASA for usado como o servidor DHCP no ambiente. Se outro servidor DHCP for usado para atribuir endereços IP a clientes, o DHCP deverá ser desabilitado no ASA. Como agora você alterou nosso esquema de endereçamento IP, é necessário alterar os intervalos de endereços IP existentes que o ASA está fornecendo aos clientes. Esses comandos criarão novos pools para corresponder ao novo intervalo de endereços IP:

```
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
```

Além disso, a modificação dos pools de DHCP desativará o servidor DHCP anterior no ASA e você precisará reativá-lo.

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

Se você não alterar os endereços IP da interface antes de fazer as alterações de DHCP, 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. Especificar o servidor DNS para passar para os clientes DHCP internos e WiFI

Quando eles atribuem endereços IP via DHCP, a maioria dos clientes também precisa receber um servidor DNS pelo servidor DHCP. Esses comandos configurarão o ASA para incluir o servidor DNS localizado em 10.0.0.250 para todos os clientes. Você precisa substituir o 10.0.0.250 por um servidor DNS interno ou um servidor DNS fornecido pelo ISP.

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

Etapa 4. Modificar a configuração de acesso HTTP no ASA para acesso do Adaptive Security Device Manager (ASDM):

Como o endereçamento IP foi alterado, o acesso HTTP ao ASA também precisa ser modificado para que os clientes dentro e as redes WiFi possam acessar o ASDM para gerenciar 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: Essa configuração permite que qualquer cliente dentro ou interfaces wifi acessem o

ASA via ASDM. Como prática recomendada de segurança, você deve limitar o escopo dos endereços somente a clientes confiáveis.

Etapa 5. Modificar o IP da Interface para o Gerenciamento do Ponto de Acesso no console da WLAN (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
```

Etapa 6. Modificar gateway padrão em WAP

Essa etapa é necessária para que o WAP saiba para onde enviar todo o tráfego que não está originado na sub-rede local. Isso é necessário para fornecer acesso à GUI do WAP via HTTP de um cliente na interface interna do ASA.

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

Passo 7. Modifique o endereço IP de gerenciamento do módulo FirePOWER (opcional)

Se você também planeja implantar o módulo Cisco FirePOWER (também conhecido como SFR), também precisará alterar seu endereço IP para acessá-lo da interface física Management1/1 no ASA. Há dois cenários básicos de implantação que determinam como configurar o ASA e o módulo SFR:

1. Uma topologia na qual a interface ASA Management1/1 está conectada a um switch interno (de acordo com o guia de início rápido normal)
2. Uma topologia em que um switch interno não está presente.

Dependendo do seu cenário, estas são as etapas apropriadas:

Se a interface ASA Management1/1 estiver conectada a um switch interno:

Você pode fazer uma sessão no módulo e alterá-lo do ASA antes de conectá-lo a um switch interno. Essa configuração permite acessar o módulo SFR via IP colocando-o na mesma sub-rede da interface interna do ASA com um endereço IP de 10.0.0.254.

As linhas em negrito são específicas a este exemplo e são necessárias para estabelecer a conectividade IP.

As linhas em itálico variam de acordo com o 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 levar alguns minutos para que a política de controle de acesso padrão seja aplicada no módulo SFR. Quando estiver concluído, você poderá sair da CLI do módulo SFR e voltar para o ASA pressionando CTRL + SHIFT + 6 +X (CTRL ^ X)

Se o ASA NÃO estiver conectado a um switch interno:

Um switch interno pode não existir em algumas pequenas implantações. Nesse tipo de topologia, os clientes geralmente se conectariam ao ASA por meio da interface WiFi. Nesse cenário, é possível eliminar a necessidade de um switch externo e acessar o módulo SFR por meio de uma interface ASA separada, conectando a interface Management1/1 a outra interface ASA física.

Neste exemplo, uma conexão Ethernet física deve existir entre a interface ASA GigabitEthernet1/3 e a interface Management1/1. Em seguida, você configura o ASA e o módulo SFR em uma sub-rede separada e, em seguida, pode acessar o SFR do ASA, bem como dos clientes localizados nas interfaces internas ou 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 do 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 levar alguns minutos para que a política de controle de acesso padrão seja aplicada no módulo SFR. Depois de concluído, você pode sair da CLI do módulo SFR e voltar para o ASA pressionando CTRL + SHIFT + 6 +X (CTRL ^ X).

Depois que a configuração do SFR se aplicar, você deve conseguir fazer ping no endereço IP de gerenciamento do 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 conseguir fazer ping na interface com êxito, verifique a configuração e o estado das conexões Ethernet físicas.

Etapa 8. Conectar-se à GUI do AP para ativar rádios e definir outras configurações do WAP

Nesse ponto, você deve ter conectividade para gerenciar o WAP através da GUI HTTP, conforme discutido no guia de início rápido. Você precisará navegar até o endereço IP da interface BVI do WAP a partir de um navegador da Web de um cliente conectado à rede interna no 5506W ou pode aplicar o exemplo de configuração e se conectar ao SSID do WAP. Se não usar a CLI abaixo, você precisará conectar o cabo Ethernet do cliente à interface Gigabit1/2 no ASA.

Se preferir usar a CLI para configurar o WAP, você pode fazer sessão nele a partir do ASA e usar este exemplo de configuração. Isso cria um SSID aberto com o nome 5506W e 5506W_5Ghz para que você possa usar um cliente sem fio para se conectar e gerenciar o WAP.

> **Note**: Depois de aplicar essa configuração, você vai querer acessar a GUI e aplicar segurança aos SSIDs para que o tráfego sem fio seja criptografado.

Configuração da CLI do WAP para uma única VLAN sem fio usando intervalos de IP modificados

```
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 desse ponto, você pode executar as etapas normais para concluir a configuração do WAP e deve ser capaz de acessá-lo a partir do navegador da Web de um cliente conectado ao SSID criado acima. O nome de usuário padrão do access point é Cisco com uma senha da Cisco com um C maiúsculo.

Guia de início rápido do Cisco ASA 5506-X Series

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

Você precisa usar o endereço IP 10.1.0.254 em vez do endereço 192.168.10.2 como indicado no Guia de início rápido.

Configurações

A configuração resultante deve corresponder à saída (supondo que você tenha usado os intervalos IP de exemplo, caso contrário substitua de acordo:

Configuração do ASA

Interfaces:

> **Note**: As linhas em itálico se aplicam somente se você NÃO tiver um switch 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 do Aironet WAP (sem o exemplo de configuração do 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 do módulo FirePOWER (com switch 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 do módulo FirePOWER (sem switch 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

Para verificar se você tem a conectividade adequada ao WAP para concluir o processo de instalação:

1. Conecte seu cliente de teste à interface interna do ASA e assegure-se de receber um endereço IP do ASA via DHCP que esteja dentro do intervalo de IP desejado.
2. Use um navegador da Web no seu cliente para navegar até https://10.1.0.254 e verificar se a GUI do AP está agora acessível.
3. Faça ping na interface de gerenciamento do SFR do cliente interno e do ASA para verificar a conectividade apropriada.

Configurar o DHCP com várias VLANs sem fio

A configuração pressupõe que você use uma única VLAN sem fio. A BVI (Bridge Virtual Interface) no AP sem fio pode fornecer uma bridge para várias VLANs. Devido à sintaxe do DHCP no ASA, se você quiser configurar o 5506W como um servidor DHCP para várias VLANs, precisará criar subinterfaces na interface Gigabit1/9 e dar um nome a cada uma. Esta seção o orienta no processo de como remover a configuração padrão e aplicar a configuração necessária para configurar o ASA como um servidor DHCP para várias VLANs.

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

Primeiro, remova a configuração DHCP existente na interface Gig1/9 (wifi):

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

Etapa 2. Criar subinterfaces para cada VLAN em Gig1/9

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

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

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

Na prática, é essencial que a VLAN e a sub-rede configuradas aqui correspondam à VLAN e à sub-rede especificadas no ponto de acesso. O nome e o número da subinterface podem ser qualquer coisa que você escolher. Consulte o guia de início rápido mencionado anteriormente para obter links para configurar o ponto de acesso usando a GUI da Web.

```
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. Designar um pool DHCP para cada VLAN

Crie um pool DHCP separado para cada VLAN que está sendo configurada. A sintaxe desse comando exige que você liste o nome se o ASA atenderá ao pool em questão. Como visto neste exemplo, que usa as VLANs 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. Configure os SSIDs do ponto de acesso, salve a configuração e redefina o módulo

Finalmente, o access point precisa ser configurado para corresponder à configuração do ASA. A interface GUI do access point permite configurar VLANs no AP através do cliente conectado à interface interna do ASA (Gigabit1/2). No entanto, se preferir usar a CLI para configurar o AP através da sessão de console ASA e, em seguida, conectar-se sem fio para gerenciar o AP, você poderá usar essa configuração como um modelo para criar dois SSIDs nas VLANs 5 e 30. Isso deve ser inserido no 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 ponto, a configuração de gerenciamento do ASA e do AP deve estar completa, e o ASA

atua como um servidor DHCP para as VLANs 5 e 30. Depois de salvar a configuração usando o comando ***write memory*** *no AP, se ainda tiver problemas de conectividade, você deverá recarregar o AP usando o comando* ***reload*** *do CLI. No entanto, se você receber um endereço IP nos SSIDs recém-criados, nenhuma ação adicional será necessária.*

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

> **Note**: NÃO é necessário recarregar todo o dispositivo ASA. Você deve apenas recarregar o ponto de acesso integrado.

Quando o AP terminar de recarregar, você deverá ter conectividade com a GUI do AP de uma máquina cliente no wifi ou em redes internas. Geralmente leva cerca de dois minutos para o AP reinicializar completamente. A partir desse ponto, você pode aplicar as etapas normais para concluir a configuração do WAP.

Guia de início rápido do Cisco ASA 5506-X Series

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

Troubleshoot

A solução de problemas de conectividade do ASA está fora do escopo deste documento, pois ele se destina à configuração inicial. Consulte as seções de verificação e configuração para verificar se todas as etapas foram concluídas corretamente.