Configurazione di ASA 5506W-X con IP non predefinito o con più VLAN

Sommario

Introduzione

In questo documento viene descritto come eseguire l'installazione iniziale e la configurazione di un dispositivo Cisco Adaptive Security Appliance (ASA) 5506W-X quando è necessario modificare lo schema di indirizzamento IP predefinito in modo che si adatti a una rete esistente o se sono necessarie più VLAN wireless. Sono necessarie diverse modifiche alla configurazione quando si

modificano gli indirizzi IP predefiniti per accedere al punto di accesso wireless (WAP) e per assicurarsi che altri servizi (ad esempio DHCP) continuino a funzionare come previsto. Inoltre, questo documento fornisce alcuni esempi di configurazione CLI per il punto di accesso wireless (WAP) integrato per semplificare il completamento della configurazione iniziale del punto di accesso wireless. Questo documento è stato redatto per integrare la guida introduttiva di Cisco ASA 5506-X disponibile sul sito Web Cisco.

Prerequisiti

Questo documento è valido solo per la configurazione iniziale di un dispositivo Cisco ASA5506W-X che contiene un punto di accesso wireless ed è progettato solo per apportare le varie modifiche necessarie quando si modifica lo schema di indirizzamento IP esistente o si aggiungono altre VLAN wireless. Per le installazioni della configurazione predefinita, è necessario fare riferimento alla Guida introduttiva di ASA 5506-X esistente.

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco ASA 5506W-X Device
- Computer client con un programma di emulazione terminale come Putty, SecureCRT, ecc.
- Cavo console e adattatore terminale PC seriale (da DB-9 a RJ-45)

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

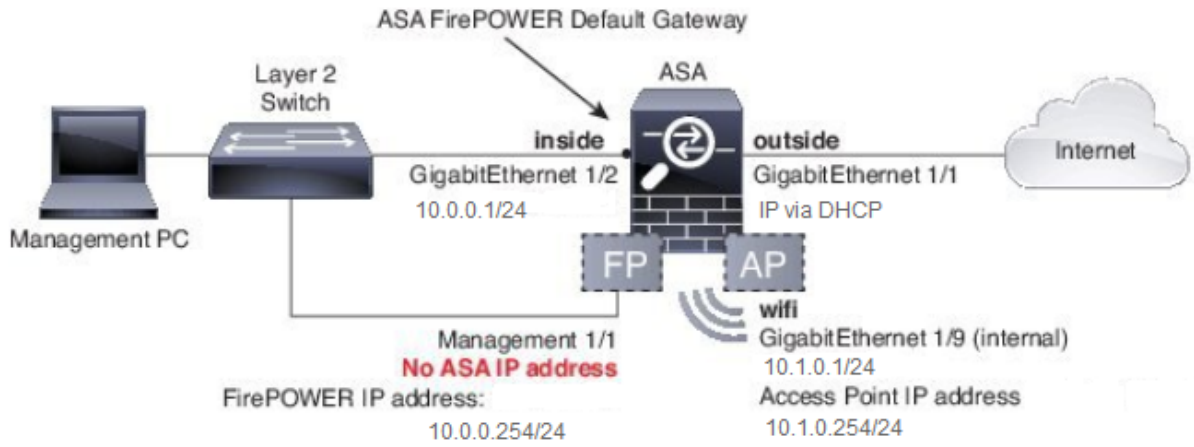
- Cisco ASA 5506W-X Device
- Computer client con un programma di emulazione terminale come Putty, SecureCRT, ecc.
- Cavo console e adattatore terminale PC seriale (da DB-9 a RJ-45)
- ASA FirePOWER Module
- Access point wireless Cisco Aironet 702i integrato (WAP integrato)

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

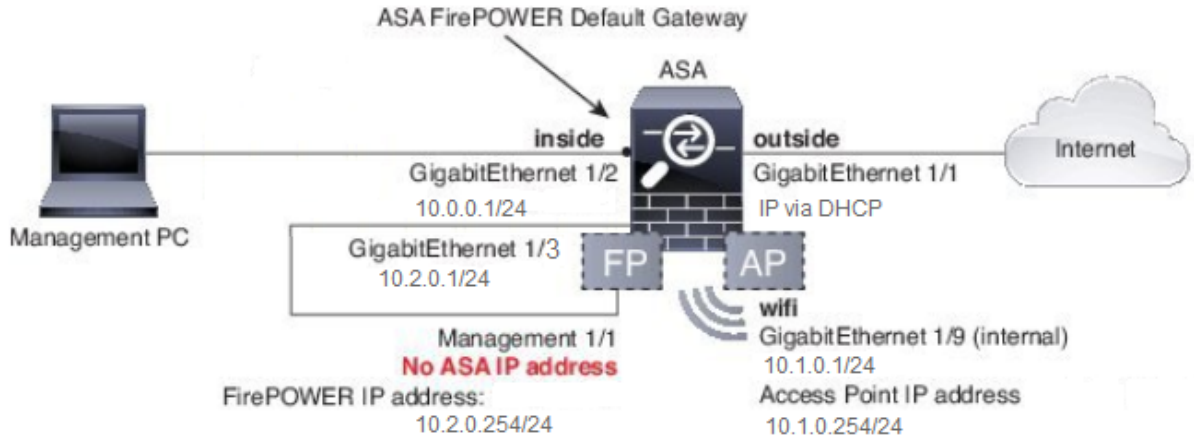
Diagrammi di rete

Come mostrato nell'immagine, alcuni esempi di indirizzi IP vengono applicati a due diverse topologie:

ASA + FirePOWER con switch interno:



ASA + FirePOWER senza switch interno:



Configurazione

Dopo aver acceso e avviato l'ASA con il cavo console collegato al client, queste operazioni devono essere eseguite in ordine.

Passaggio 1. Modifica della configurazione dell'IP interfaccia sull'ASA

Configurare le interfacce interne (Gigabit Ethernet 1/2) e wifi (Gigabit Ethernet 1/9) in modo che dispongano degli indirizzi IP necessari all'interno dell'ambiente esistente. In questo esempio, i client interni sono sulla rete 10.0.0.1/24 e i client WIFI sono sulla rete 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
```

Nota: questo messaggio di avviso viene visualizzato quando si modificano gli indirizzi IP dell'interfaccia sopra indicati. Questo è previsto.

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

Passaggio 2. Modifica le impostazioni del pool DHCP sia sull'interfaccia interna che su quella wifi

Questa procedura è obbligatoria se l'ASA deve essere usata come server DHCP nell'ambiente. Se si usa un altro server DHCP per assegnare gli indirizzi IP ai client, il protocollo DHCP deve essere disabilitato sull'appliance ASA. Poiché lo schema di indirizzi IP è stato modificato, è necessario modificare gli intervalli di indirizzi IP esistenti forniti dall'ASA ai client. Questi comandi creeranno nuovi pool per soddisfare il nuovo intervallo di indirizzi 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
```

Inoltre, la modifica dei pool DHCP disabiliterà il server DHCP precedente sull'appliance ASA e sarà necessario riabilitarlo.

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

Se non si modificano gli indirizzi IP dell'interfaccia prima di apportare le modifiche DHCP, viene visualizzato questo errore:

```
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
```

Passaggio 3. Specificare il server DNS da passare ai client DHCP interni e WiFI

Quando gli indirizzi IP vengono assegnati tramite DHCP, alla maggior parte dei client deve essere assegnato un server DNS anche dal server DHCP. Questi comandi configurano l'ASA in modo che includa il server DNS situato a 10.0.0.250 in tutti i client. È necessario sostituire la versione 10.0.0.250 con un server DNS interno o un server DNS fornito dall'ISP.

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

Passaggio 4. Modificare la configurazione dell'accesso HTTP sull'appliance ASA per l'accesso Adaptive Security Device Manager (ASDM):

Poiché l'indirizzo IP è stato modificato, è necessario modificare anche l'accesso HTTP all'appliance ASA in modo che i client sulle reti interna e WiFI possano accedere ad ASDM per gestire l'appliance.

```
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
```

Nota: questa configurazione consente a qualsiasi client sull'interfaccia interna o Wi-Fi di accedere all'appliance ASA tramite ASDM. Come buona norma per la sicurezza, è necessario limitare l'ambito degli indirizzi solo ai client attendibili.

Passaggio 5. Modificare l'indirizzo IP dell'interfaccia per la gestione dei punti di accesso nella console WLAN (interfaccia 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
```

Passaggio 6. Modifica default-gateway in WAP

Questo passaggio è obbligatorio in modo che il WAP sappia dove inviare tutto il traffico non originato nella subnet locale. Questo comando è necessario per fornire l'accesso alla GUI WAP tramite HTTP da un client sull'interfaccia interna dell'ASA.

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

Passaggio 7. Modifica dell'indirizzo IP di gestione del modulo FirePOWER (opzionale)

Se si intende installare anche il modulo Cisco FirePOWER (noto anche come SFR), è necessario modificare anche il relativo indirizzo IP per potervi accedere dall'interfaccia fisica Management1/1 sull'appliance ASA. La configurazione dell'ASA e del modulo SFR viene determinata in due scenari di distribuzione di base:

1. Topologia in cui l'interfaccia ASA Management1/1 è collegata a uno switch interno (come da normale guida introduttiva)
2. Topologia in cui non è presente uno switch interno.

A seconda dello scenario, è necessario eseguire le operazioni seguenti:

Se l'interfaccia ASA Management1/1 è collegata a uno switch interno:

È possibile effettuare la sessione nel modulo e modificarlo dall'appliance ASA prima di collegarlo a uno switch interno. Questa configurazione consente di accedere al modulo SFR tramite l'IP e di collocarlo sulla stessa subnet dell'interfaccia interna dell'ASA con un indirizzo IP di 10.0.0.254.

Le righe in grassetto sono specifiche di questo esempio e sono necessarie per stabilire la connettività IP.

Le righe in corsivo variano a seconda dell'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.
```

Nota: l'applicazione della policy di controllo di accesso predefinita al modulo SFR potrebbe richiedere alcuni minuti. Al termine, è possibile uscire dalla CLI del modulo SFR e tornare all'appliance ASA premendo CTRL + MAIUSC + 6 +X (CTRL ^ X)

Se l'ASA NON è collegata a uno switch interno:

In alcune piccole distribuzioni potrebbe non esistere uno switch interno. In questo tipo di topologia, i client in genere si connettono all'ASA tramite l'interfaccia WiFi. In questo scenario, è possibile eliminare la necessità di uno switch esterno e accedere al modulo SFR tramite un'interfaccia ASA separata tramite la connessione incrociata dell'interfaccia Management1/1 con un'altra interfaccia ASA fisica.

Nell'esempio, deve essere presente una connessione Ethernet fisica tra l'interfaccia ASA Gigabit Ethernet1/3 e l'interfaccia Management1/1. Quindi, configurare il modulo ASA e SFR in modo che si trovino su una subnet separata e poter accedere all'SFR sia dall'ASA che dai client situati sull'interfaccia interna o Wi-Fi.

Configurazione interfaccia 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
```

Configurazione modulo 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.
```

Nota: l'applicazione della policy di controllo di accesso predefinita al modulo SFR potrebbe richiedere alcuni minuti. Al termine, è possibile uscire dalla CLI del modulo SFR e tornare all'appliance ASA premendo CTRL + MAIUSC + 6 +X (CTRL ^ X).

Una volta applicata la configurazione SFR, è necessario poter eseguire il ping dell'indirizzo IP di gestione SFR dall'appliance 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 non è possibile eseguire il ping dell'interfaccia correttamente, verificare la configurazione e lo stato delle connessioni Ethernet fisiche.

Passaggio 8. Connettersi alla GUI AP per abilitare le radio e impostare un'altra configurazione WAP

A questo punto è necessario disporre della connettività per gestire il WAP tramite l'interfaccia GUI HTTP, come descritto nella guida introduttiva. È necessario selezionare l'indirizzo IP dell'interfaccia BVI del WAP dal browser di un client connesso alla rete interna sullo switch 5506W oppure è possibile applicare la configurazione di esempio e connettersi all'SSID del WAP. Se non si utilizza la CLI seguente, è necessario collegare il cavo Ethernet del client all'interfaccia Gigabit1/2 sull'appliance ASA.

Se si preferisce usare la CLI per configurare il WAP, è possibile eseguire una sessione in esso dall'ASA e usare questa configurazione di esempio. In questo modo viene creato un SSID aperto con il nome di 5506W e 5506W_5Ghz che consente di utilizzare un client wireless per connettersi al WAP e gestirlo ulteriormente.

> Nota: dopo aver applicato questa configurazione, si desidera accedere alla GUI e applicare la sicurezza agli SSID in modo che il traffico wireless sia crittografato.

Configurazione WAP CLI per una singola VLAN wireless che usa intervalli IP modificati

```
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
```

Da questo momento in poi, è possibile eseguire i normali passaggi per completare la configurazione del WAP e occorre essere in grado di accedervi dal browser Web di un client connesso al SSID creato in precedenza. Il nome utente predefinito del punto di accesso è Cisco con una password di Cisco con una C maiuscola.

Cisco ASA serie 5506-X Quick Start Guide

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

È necessario utilizzare l'indirizzo IP 10.1.0.254 invece di 192.168.10.2 come indicato nella Guida introduttiva.

Configurazioni

La configurazione risultante deve corrispondere all'output (presupponendo che siano stati utilizzati gli intervalli IP di esempio, altrimenti sostituire di conseguenza:

Configurazione ASA

Interfacce:

Nota: le righe in corsivo sono valide solo se NON si dispone di un interruttore 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#
```

Configurazione WAP Aironet (senza la configurazione SSID di esempio)

```
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
```

Configurazione del modulo FirePOWER (con 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

>
```

Configurazione del modulo FirePOWER (senza 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

>
```

Verifica

Per verificare di disporre della corretta connettività al server WAP per completare il processo di

installazione:

1. Collegare il client di prova all'interfaccia interna dell'ASA e verificare che riceva un indirizzo IP dall'ASA tramite DHCP che rientri nell'intervallo IP desiderato.
2. Usare un browser Web sul client per accedere a https://10.1.0.254 e verificare che l'interfaccia utente sia accessibile.
3. Eseguire il ping dell'interfaccia di gestione SFR dal client interno e dall'appliance ASA per verificare la corretta connettività.

Configurazione di DHCP con più VLAN wireless

Per la configurazione si presume che venga utilizzata una singola VLAN wireless. La BVI (Bridge Virtual Interface) sull'access point wireless può fornire un bridge per più VLAN. A causa della sintassi del protocollo DHCP sull'appliance ASA, se si desidera configurare lo switch 5506W come server DHCP per più VLAN, è necessario creare delle sottointerfacce sull'interfaccia Gigabit1/9 e assegnare un nome a ciascuna di esse. In questa sezione viene illustrato come rimuovere la configurazione predefinita e applicare la configurazione necessaria per impostare l'ASA come server DHCP per più VLAN.

Passaggio 1. Rimuovi configurazione DHCP esistente in Gig1/9

Innanzitutto, rimuovere la configurazione DHCP esistente sull'interfaccia Gig1/9 (wifi):

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

Passaggio 2. Creazione di sottointerfacce per ciascuna VLAN su Gig1/9

Per ciascuna VLAN configurata sul punto di accesso, è necessario configurare un'interfaccia secondaria Gig1/9. In questa configurazione di esempio, vengono aggiunte due sottointerfacce:

-Gig1/9.5, con nome se vlan5, e corrispondente alla VLAN 5 e alla subnet 10.5.0.0/24.

-Gig1/9.30, con nome se vlan30, che corrisponderà alla VLAN 30 e alla subnet 10.3.0.0/24.

In pratica, è essenziale che la VLAN e la subnet configurate qui corrispondano alla VLAN e alla subnet specificate sul punto di accesso. Il nome if e il numero di sottointerfaccia possono essere i valori desiderati. Per configurare il punto di accesso tramite l'interfaccia Web, consultare la guida rapida menzionata in precedenza per i collegamenti.

```
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
```

Passaggio 3. Designare un pool DHCP per ciascuna VLAN

Creare un pool DHCP separato per ciascuna VLAN configurata. La sintassi del comando richiede che venga elencato il nome se l'appliance ASA non serve il pool in questione. Come mostrato nell'esempio, che usa le 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
```

Passaggio 4. Configurare gli SSID dei punti di accesso, salvare la configurazione e reimpostare il modulo

Infine, il punto di accesso deve essere configurato in modo da corrispondere alla configurazione dell'ASA. L'interfaccia GUI del punto di accesso consente di configurare le VLAN sull'access point tramite il client collegato all'interfaccia ASA interna (Gigabit1/2). Tuttavia, se si preferisce usare la CLI per configurare l'access point tramite la sessione della console ASA e quindi connettersi in modalità wireless per gestire l'access point, è possibile usare questa configurazione come modello per creare due SSID sulle VLAN 5 e 30. Questo valore deve essere immesso nella console dell'access point in modalità di configurazione globale:

```
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
```

A questo punto, la configurazione di gestione dell'ASA e dell'access point deve essere completata e l'ASA funziona come server DHCP per le VLAN 5 e 30. Dopo aver salvato la configurazione con il comando write memory sull'access point, se si hanno ancora problemi di connettività, è necessario ricaricare l'access point con il comando reload dalla CLI. Tuttavia, se si riceve un indirizzo IP sugli SSID appena creati, non è necessario eseguire altre operazioni.

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

> Nota: NON è necessario ricaricare l'intero dispositivo ASA. È necessario ricaricare solo il punto di accesso incorporato.

Al termine del ricaricamento dell'access point, è necessario essere collegati all'interfaccia utente grafica dell'access point da un computer client sulla rete wifi o nelle reti interne. In genere sono necessari circa due minuti prima che l'access point venga riavviato completamente. Da questo punto in poi, è possibile applicare i passaggi normali per completare la configurazione del WAP.

Cisco ASA serie 5506-X Quick Start Guide

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

Risoluzione dei problemi

La risoluzione dei problemi di connettività ASA non rientra nell'ambito di questo documento, in quanto è destinata alla configurazione iniziale. Fare riferimento alle sezioni di verifica e configurazione per assicurarsi che tutte le fasi siano state completate correttamente.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).