Client Anyconnect per ASA con uso di DHCP per l'assegnazione degli indirizzi

Sommario

Introduzione

In questo documento viene descritto come configurare Cisco serie 5500-X Adaptive Security Appliance (ASA) in modo che il server DHCP fornisca l'indirizzo IP del client a tutti i client Anyconnect con l'uso di Adaptive Security Device Manager (ASDM) o della CLI.

Prerequisiti

Requisiti

In questo documento si presume che l'ASA sia completamente operativa e configurata per consentire a Cisco ASDM o CLI di apportare modifiche alla configurazione.

> **Nota**: fare riferimento al libro 1: Cisco ASA Series General Operations CLI Configuration Guide, 9.2 per consentire la configurazione remota del dispositivo da parte di ASDM o Secure Shell (SSH).

Componenti usati

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

- Cisco ASA 5500-X Next-Generation Firewall versione 9.2(1)
- Adaptive Security Device Manager versione 7.1(6)
- Cisco Anyconnect Secure Mobility Client 3.1.05152

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.

Prodotti correlati

Questa configurazione può essere utilizzata anche con Cisco ASA Security Appliance serie 5500 versione 7.x e successive.

Premesse

Le VPN ad accesso remoto soddisfano i requisiti della forza lavoro mobile per connettersi in modo sicuro alla rete dell'organizzazione. Gli utenti mobili possono configurare una connessione protetta utilizzando il software Cisco Anyconnect Secure Mobility Client. Cisco Anyconnect Secure Mobility Client avvia una connessione a un dispositivo del sito centrale configurato per accettare queste richieste. Nell'esempio, il dispositivo del sito centrale è un'appliance ASA 5500-X Adaptive Security che usa mappe crittografiche dinamiche.

Nella gestione degli indirizzi di un accessorio di protezione è necessario configurare gli indirizzi IP che connettono un client a una risorsa della rete privata, tramite il tunnel, e consentono al client di funzionare come se fosse connesso direttamente alla rete privata.

Inoltre, si tratta solo degli indirizzi IP privati assegnati ai client. Gli indirizzi IP assegnati ad altre risorse sulla rete privata fanno parte delle responsabilità di amministrazione della rete e non della gestione VPN. Pertanto, quando si parla di indirizzi IP, Cisco indica gli indirizzi IP disponibili nello schema di indirizzamento della rete privata che consentono al client di funzionare come endpoint del tunnel.

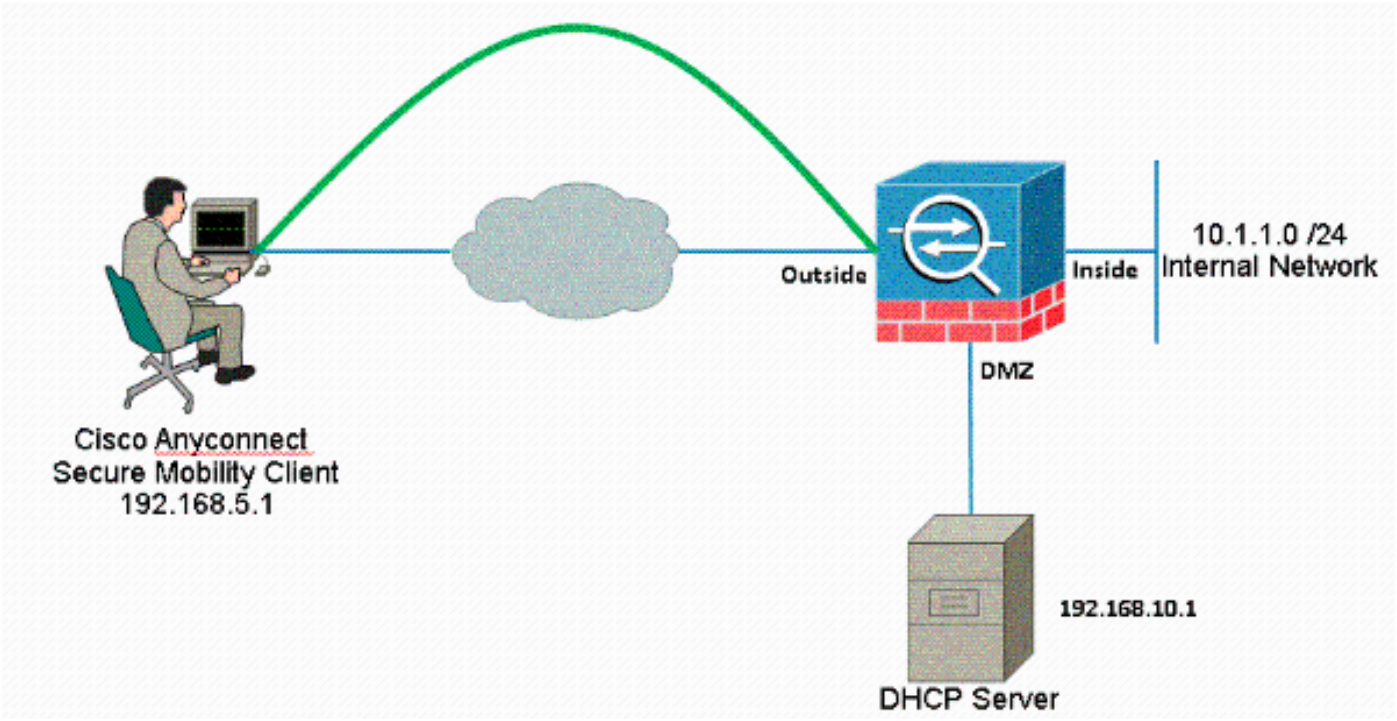
Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

> **Nota**: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Esempio di rete

Nel documento viene usata questa impostazione di rete:



Nota: gli schemi di indirizzamento IP utilizzati in questa configurazione non sono indirizzabili legalmente su Internet. Si tratta degli indirizzi RFC 1918 utilizzati in un ambiente lab.

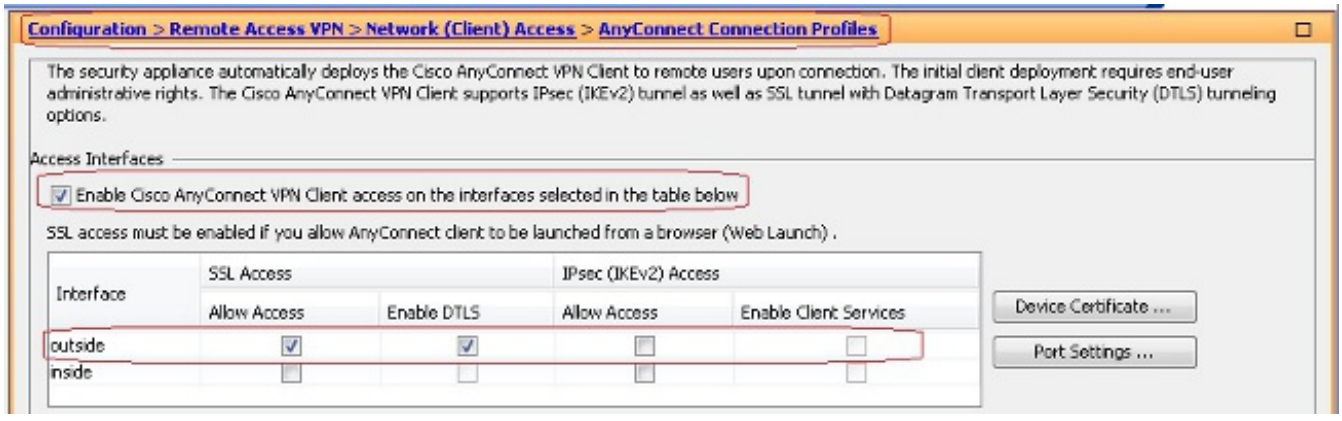
Configurazione Del Client Cisco Anyconnect Secure Mobility

Procedura ASDM

Per configurare la VPN di accesso remoto, completare i seguenti passaggi:

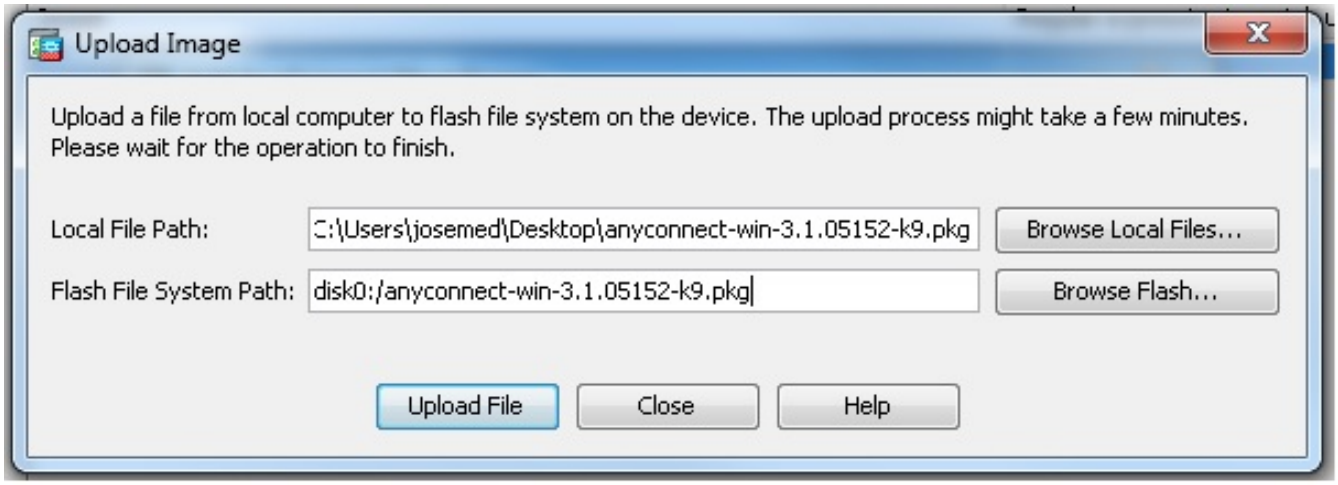
- Abilita WebVPN.

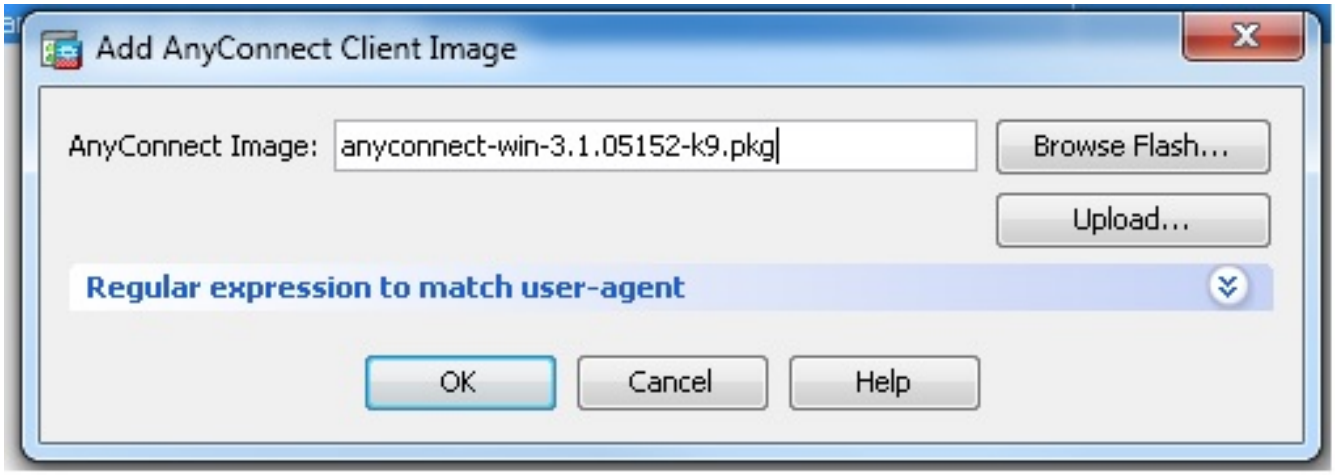
  Scegliere **Configurazione > VPN ad accesso remoto > Accesso di rete (client) > Profili di connessione VPN SSL** e in **Interfacce di accesso**, fare clic sulle caselle di controllo **Consenti accesso** e **Abilita DTLS** per l'interfaccia esterna. Inoltre, selezionare la casella di controllo **Abilita accesso client VPN Cisco AnyConnect o client VPN SSL legacy sull'interfaccia selezionata in questa tabella** per abilitare VPN SSL sull'interfaccia esterna.



Fare clic su Apply (Applica).

Scegliere **Configurazione > VPN ad accesso remoto > Accesso di rete (client) > Software client Anyconnect > Aggiungi** per aggiungere l'immagine del client VPN Cisco AnyConnect dalla memoria flash dell'ASA, come mostrato.



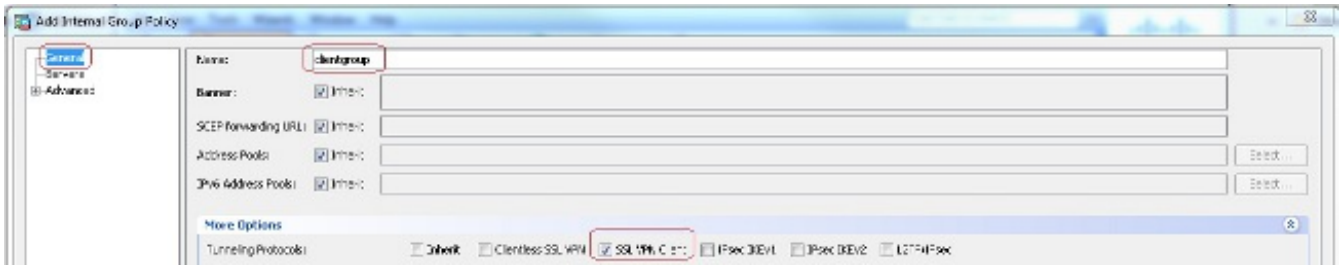


Configurazione CLI equivalente:

```
ciscoasa(config)#webvpn
ciscoasa(config-webvpn)#enable outside
ciscoasa(config-webvpn)#anyconnect image disk0:/anyconnect-win-3.1.05152-k9.pkg 1
ciscoasa(config-webvpn)#tunnel-group-list enable
ciscoasa(config-webvpn)#anyconnect enable
```

- Configurare Criteri di gruppo.

Per creare un gruppo di **client di** Criteri di gruppo interno, scegliere **Configurazione > VPN ad accesso remoto > Accesso di rete (client)** > Criteri di gruppo. Nella scheda **Generale**, selezionare la casella di controllo **SSL VPN Client** per abilitare SSL come protocollo di tunneling.



Configurare l'ambito di rete DHCP nella scheda **Server**, selezionare **Altre opzioni** per configurare l'ambito DHCP in modo che gli utenti vengano assegnati automaticamente.

Configurazione CLI equivalente:

```
ciscoasa(config)#group-policy clientgroup internal
ciscoasa(config)#group-policy clientgroup attributes
ciscoasa(config-group-policy)#vpn-tunnel-protocol ssl-client
ciscoasa(config-group-policy)#
```

- Per creare un nuovo account utente **ssluser1,** scegliere **Configurazione > VPN ad accesso remoto > Utenti AAA/locali > Utenti locali > Aggiungi**. Fare clic su **OK** e quindi su **Applica**.

Configurazione CLI equivalente:

```
ciscoasa(config)#username ssluser1 password asdmASA
```

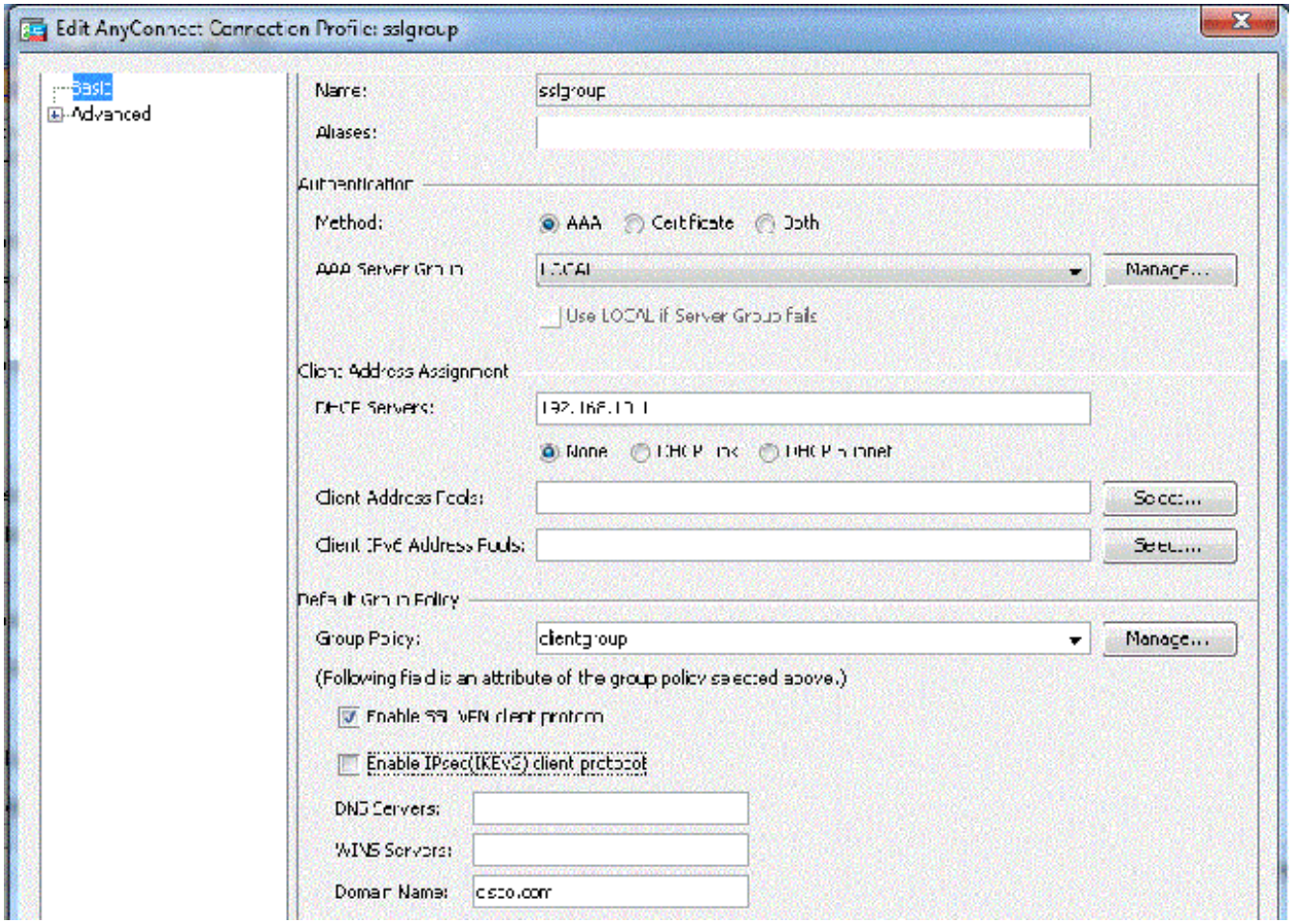
- Configurare il gruppo di tunnel.

Per creare un nuovo gruppo di tunnel, scegliere **Configurazione > VPN ad accesso remoto > Accesso di rete (client) > Profili di connessione Anyconnect > Aggiungi**.

Nella scheda **Base** è possibile eseguire l'elenco delle configurazioni come illustrato di seguito.

Assegnare al gruppo di tunnel il nome **sslgroup**.Specificare l'indirizzo IP del server DHCP nello spazio disponibile per i **server DHCP**.In Criteri di gruppo predefiniti scegliere il **gruppo**

client di Criteri di gruppo dall'elenco a discesa Criteri di gruppo.Configurare il collegamento DHCP o la subnet DHCP.



Nella scheda **Avanzate > Alias gruppo/URL gruppo**, specificare il nome alias del gruppo come **sslgroup_users** e fare clic su **OK**.

Configurazione CLI equivalente:

```
ciscoasa(config)#tunnel-group sslgroup type remote-access
ciscoasa(config)#tunnel-group sslgroup general-attributes
ciscoasa(config-tunnel-general)#dhcp-server 192.168.10.1
ciscoasa(config-tunnel-general)#default-group-policy clientgroup
ciscoasa(config-tunnel-general)#exit
ciscoasa(config)#tunnel-group sslgroup webvpn-attributes
ciscoasa(config-tunnel-webvpn)#group-alias sslgroup_users enable
```

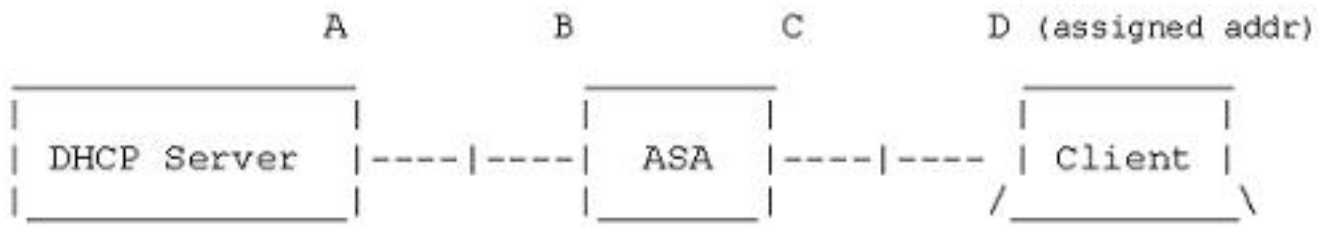
Selezione subnet o Selezione collegamento

Il supporto dei proxy DHCP per le RFC 3011 e RFC 3527 è una funzionalità introdotta nelle versioni 8.0.5 e 8.2.2 ed è supportata nelle versioni successive.

- La RFC 3011 definisce una nuova opzione DHCP, l'opzione di selezione della subnet, che consente al client DHCP di specificare la subnet su cui allocare un indirizzo. Questa opzione ha la precedenza sul metodo utilizzato dal server DHCP per determinare la subnet su cui selezionare un indirizzo.
- La RFC 3527 definisce una nuova opzione secondaria DHCP, la link selection suboption, che

consente al client DHCP di specificare l'indirizzo a cui il server DHCP deve rispondere.
Per quanto riguarda l'ASA, queste RFC permetteranno all'utente di specificare un ambito di rete dhcp per l'assegnazione dell'indirizzo DHCP non locale per l'ASA. Il server DHCP sarà comunque in grado di rispondere direttamente all'interfaccia dell'ASA. I diagrammi seguenti dovrebbero aiutare a illustrare il nuovo comportamento. In questo modo sarà possibile utilizzare gli ambiti non locali senza dover creare una route statica per l'ambito nella rete.

Quando la RFC 3011 o RFC 3527 non è abilitata, lo scambio del proxy DHCP ha un aspetto simile al seguente:



Message Exchange:

Discover: B -> A

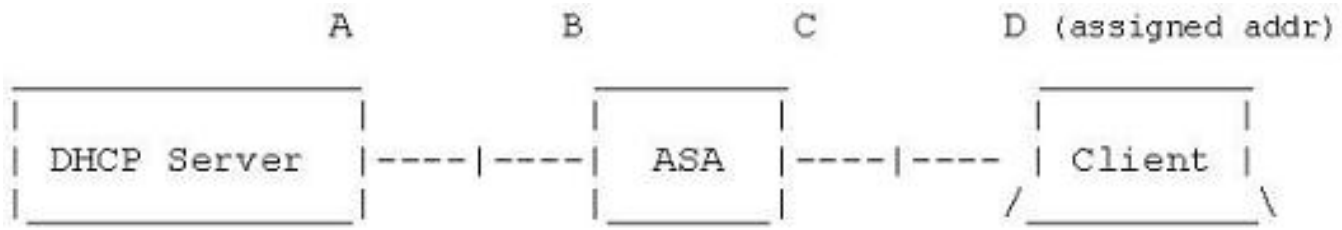
Offer: A -> dhcp-network-scope

Request: B -> A

Ack: A -> dhcp-network-scope

Release: B -> A

Se una di queste RFC è abilitata, Exchange avrà un aspetto simile a questo e al client VPN verrà ancora assegnato un indirizzo nella subnet corretta:



Message Exchange:

Discover: B -> A

Offer: A -> B

Request: B -> A

Ack: A -> B

Release: B -> A

Configurazione dell'ASA con l'uso della CLI

Completare questa procedura per configurare il server DHCP in modo che fornisca l'indirizzo IP ai client VPN dalla riga di comando. Per ulteriori informazioni su ciascun comando usato, consultare la guida di riferimento dei comandi di Cisco ASA serie 5500 Adaptive Security Appliance.

```
ASA# show run
ASA Version 9.2(1)
!

!--- Specify the hostname for the Security Appliance.

hostname ASA
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!


!--- Configure the outside and inside interfaces.

interface GigabitEthernet0/0
nameif inside
security-level 100
ip address 10.1.1.1 255.255.255.0
!
interface GigabitEthernet0/1
nameif outside
security-level 0
ip address 192.168.1.1 255.255.255.0
!
interface GigabitEthernet0/2
nameif DMZ
security-level 50
ip address 192.168.10.2 255.255.255.0


!--- Output is suppressed.


passwd 2KFQnbNIdI.2KYOU encrypted
boot system disk0:/asa802-k8.bin
ftp mode passive

object network obj-10.1.1.0
subnet 10.1.1.0 255.255.255.0
object network obj-192.168.5.0
subnet 192.168.5.0 255.255.255.0

pager lines 24
logging enable
logging asdm informational
mtu inside 1500
mtu outside 1500
mtu dmz 1500
no failover
icmp unreachable rate-limit 1 burst-size 1


!--- Specify the location of the ASDM image for ASA to fetch the image
for ASDM access.
```

```
asdm image disk0:/asdm-716.bin
no asdm history enable
arp timeout 14400

nat (inside,outside) source static obj-10.1.1.0 obj-10.1.1.0 destination static
obj-192.168.5.0 obj-192.168.5.0
!
object network obj-10.1.1.0
nat (inside,outside) dynamic interface
route outside 0.0.0.0 0.0.0.0 192.168.1.2 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
dynamic-access-policy-record DfltAccessPolicy
http server enable
http 0.0.0.0 0.0.0.0 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
parameters
message-length maximum 512
policy-map global_policy
class inspection_default
inspect dns preset_dns_map
inspect ftp
inspect h323 h225
inspect h323 ras
inspect netbios
inspect rsh
inspect rtsp
inspect skinny
inspect esmtp
inspect sqlnet
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp
!
service-policy global_policy global
!
!--- Enable webvpn and specify an Anyconnect image

webvpn
enable outside
anyconnect image disk0:/anyconnect-win-3.1.05152-k9.pkg 1
anyconnect enable
tunnel-group-list enable


group-policy clientgroup internal
```

```
group-policy clientgroup attributes


!--- define the DHCP network scope in the group policy.This configuration is Optional

dhcp-network-scope 192.168.5.0


!--- In order to identify remote access users to the Security Appliance,
!--- you can also configure usernames and passwords on the device.

username ssluser1 password ffIRPGpDSOJh9YLq encrypted


!--- Create a new tunnel group and set the connection
!--- type to remote-access.

tunnel-group sslgroup type remote-access


!--- Define the DHCP server address to the tunnel group.

tunnel-group sslgroup general-attributes
default-group-policy clientgroup
dhcp-server 192.168.10.1

!--- If the use of RFC 3011 or RFC 3527 is required then the following command will
enable support for them

tunnel-group sslgroup general-attributes
dhcp-server subnet-selection (server ip) (3011)
hcp-server link-selection (server ip) (3527)

!--- Configure a group-alias for the tunnel-group

tunnel-group sslgroup webvpn-attributes
group-alias sslgroup_users enable

prompt hostname context
Cryptochecksum:e0725ca9ccc28af488ded9ee36b7822d
: end
ASA#
```