Cliente de Anyconnect ao ASA com uso do DHCP para a atribuição de endereço

Índice

Introdução

Este documento descreve como configurar a ferramenta de segurança adaptável do Cisco 5500-X Series (ASA) para fazer o servidor DHCP fornecer o endereço IP cliente a todos os clientes de Anyconnect o uso do Security Device Manager adaptável (ASDM) ou do CLI.

Pré-requisitos

Requisitos

Este documento supõe que o ASA é plenamente operacional e configurado para permitir que Cisco ASDM ou CLI faça alterações de configuração.

> Nota: Consulte para registrar 1: Guia de configuração de CLI das operações gerais da série de Cisco ASA, 9.2 para permitir que o dispositivo seja configurado remotamente pelo ASDM ou pelo Shell Seguro (ssh).

Componentes Utilizados

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

- Versão de firewall da próxima geração de Cisco ASA 5500-X 9.2(1)

- Versão 7.1(6) adaptável do Security Device Manager
- Cliente de mobilidade Cisco AnyConnect Secure 3.1.05152

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.

Produtos Relacionados

Esta configuração pode igualmente ser usada com versão 7.x e mais recente do 5500 Series da ferramenta de segurança de Cisco ASA.

Informações de Apoio

Os acessos remoto VPN endereçam a exigência da força de trabalho móvel conectar firmemente à rede da organização. Os usuários móveis podem estabelecer uma conexão segura usando o software do Cliente de mobilidade Cisco AnyConnect Secure. O Cliente de mobilidade Cisco AnyConnect Secure inicia uma conexão a um dispositivo da instalação central configurado para aceitar estes pedidos. Neste exemplo, o dispositivo da instalação central é uma ferramenta de segurança adaptável do 5500-X Series ASA que use mapas cripto dinâmico.

Na gerência de endereços da ferramenta de segurança, você tem que configurar os endereços IP de Um ou Mais Servidores Cisco ICM NT que conectam um cliente com um recurso na rede privada, através do túnel, e deixam o cliente funcionar como se foi conectado diretamente à rede privada.

Além disso, você está tratando somente os endereços IP privados que são atribuídos aos clientes. Os endereços IP de Um ou Mais Servidores Cisco ICM NT atribuídos a outros recursos em sua rede privada são parte de suas responsabilidades da administração de rede, não parte de Gerenciamento de VPN. Consequentemente, quando os endereços IP de Um ou Mais Servidores Cisco ICM NT são discutidos aqui, Cisco significa aqueles endereços IP de Um ou Mais Servidores Cisco ICM NT disponíveis em seu método de endereçamento da rede privada que deixa o cliente funcionar como um ponto final de túnel.

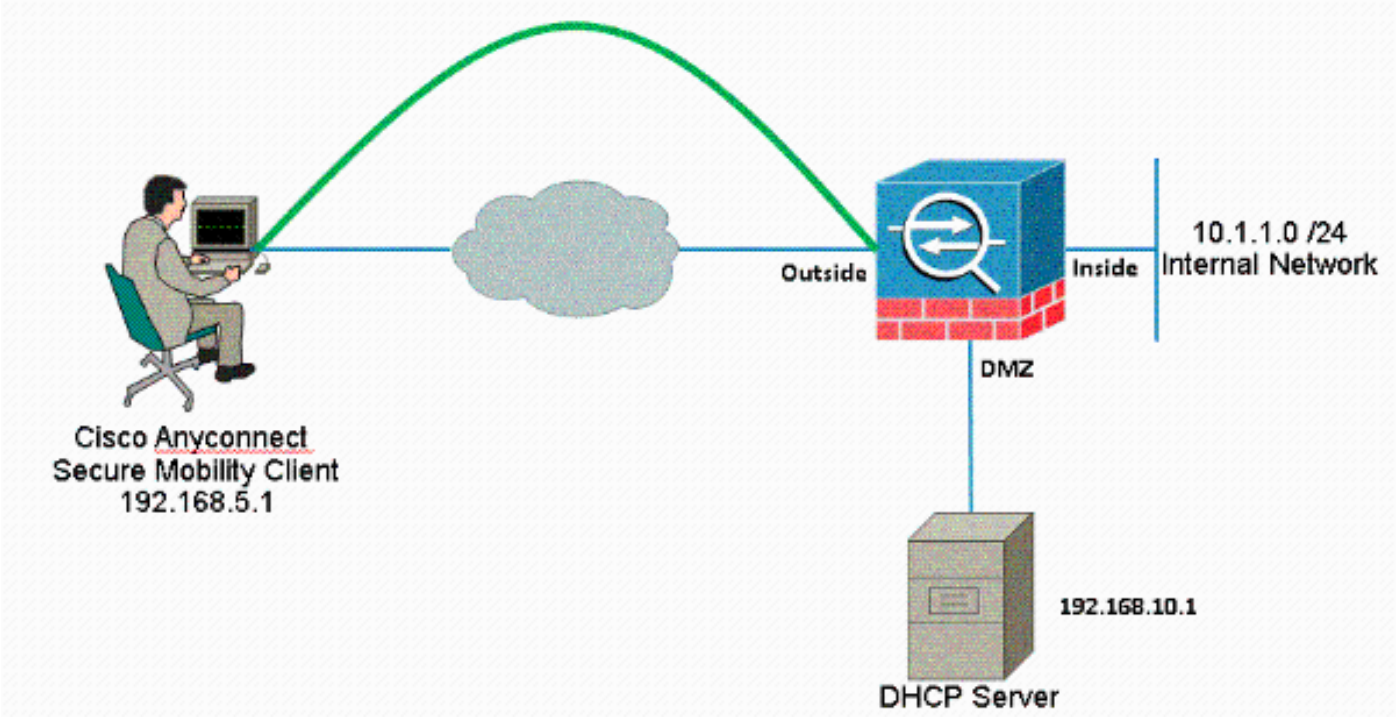
Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

> Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Nota: Os esquemas de endereçamento IP usados nesta configuração não são legalmente roteáveis na Internet. São os endereços do RFC 1918 que foram usados em um ambiente de laboratório.

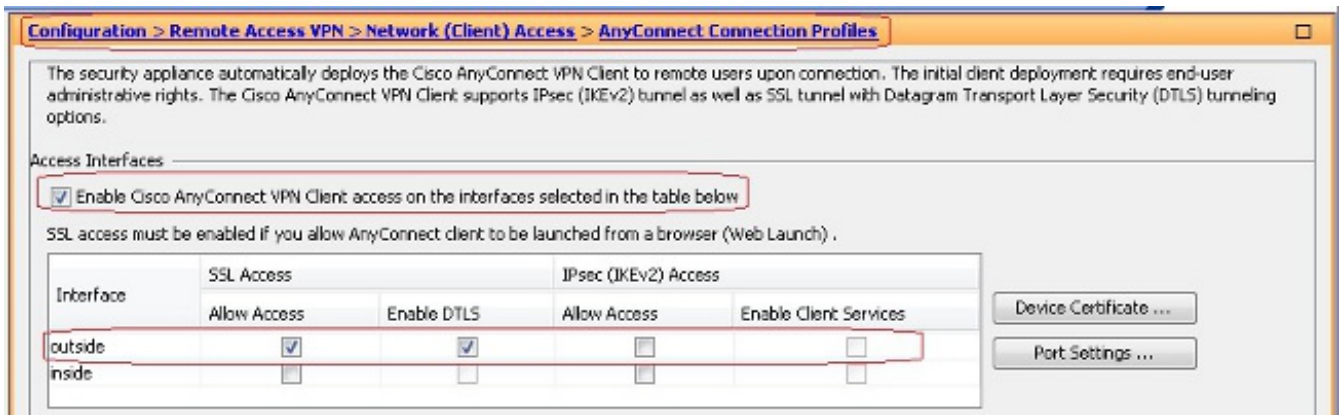
Configurar o Cliente de mobilidade Cisco AnyConnect Secure

Procedimento ASDM

Termine estas etapas a fim configurar o acesso remoto VPN:

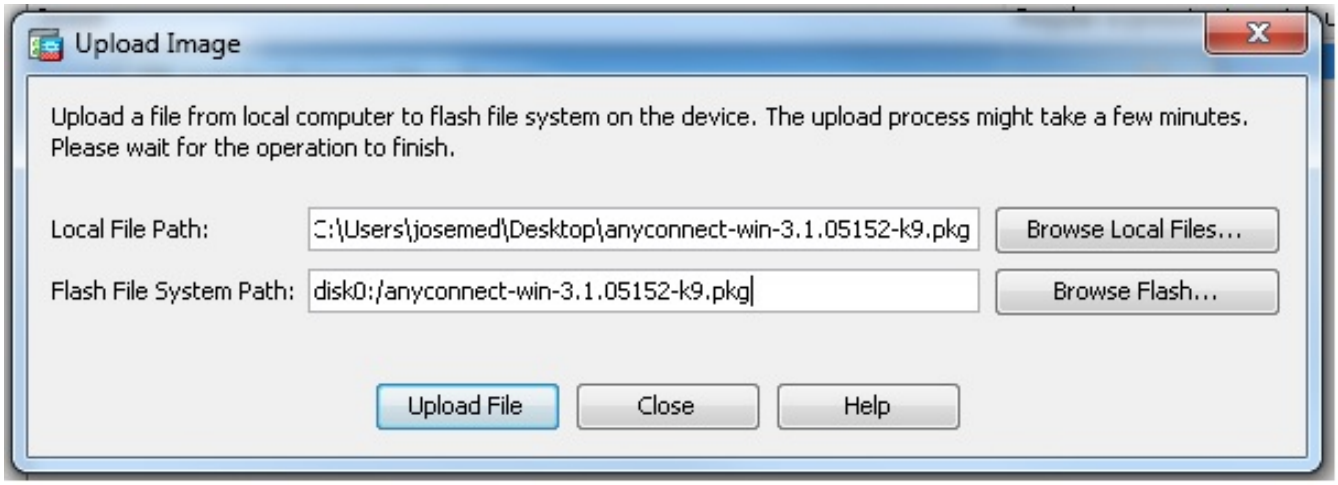
- Ative o WebVPN.

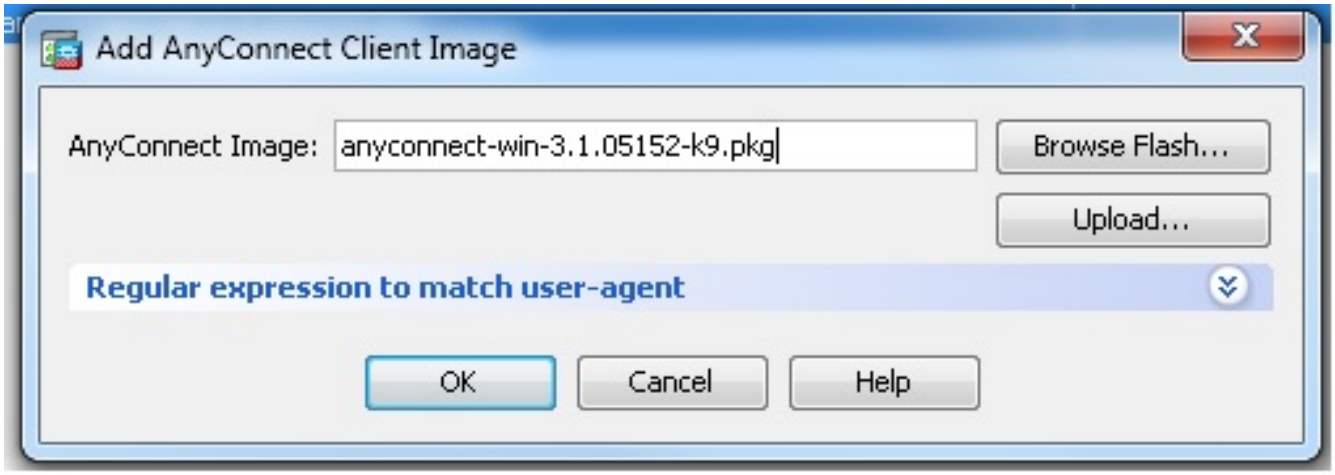
  Selecione **Configuration > Remote Access VPN > Network (Client) Access > SSL VPN Connection Profiles** e, sob **Access Interfaces**, clique nas caixas de seleção **Allow Access** e **Enable DTLS** para a interface externa. Também, verifique o **acesso do Cisco AnyConnect VPN Client da possibilidade ou de cliente VPN do legado SSL na relação selecionada nesta** caixa de verificação da **tabela** a fim permitir SSL VPN na interface externa.



Clique em Apply.

Escolha o **> Add da configuração > do acesso do acesso remoto VPN > da rede (cliente) > do software do cliente de Anyconnect** a fim adicionar a imagem do Cisco AnyConnect VPN Client da memória Flash do ASA como mostrada.



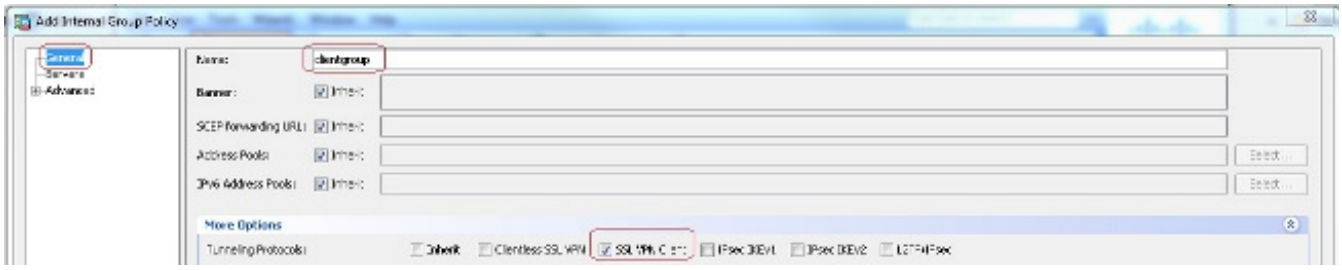


Configuração via CLI Equivalente:

```
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
```

- Configure a Política de Grupo.

Selecione **Configuration > Remote Access VPN > Network (Client) Access > Group Policies** para criar uma política de grupo interna **clientgroup**. Sob o **tab geral**, selecione a caixa de verificação do **cliente VPN SSL** a fim permitir o SSL como o protocolo de tunelamento.



Configurar o escopo de rede de DHCP na aba dos **server**, escolha **mais opções** a fim configurar o escopo de DHCP para que os usuários sejam atribuídos automaticamente.

Configuração via 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
```

- Escolha a **configuração > o acesso remoto VPN > dos usuários > dos usuários locais AAA/Local > Add** a fim criar uma conta de novo usuário **ssluser1**. Clique em **OK** e, em seguida, em **Apply**.

Configuração via CLI Equivalente:`ciscoasa(config)#username ssluser1 password asdmASA`

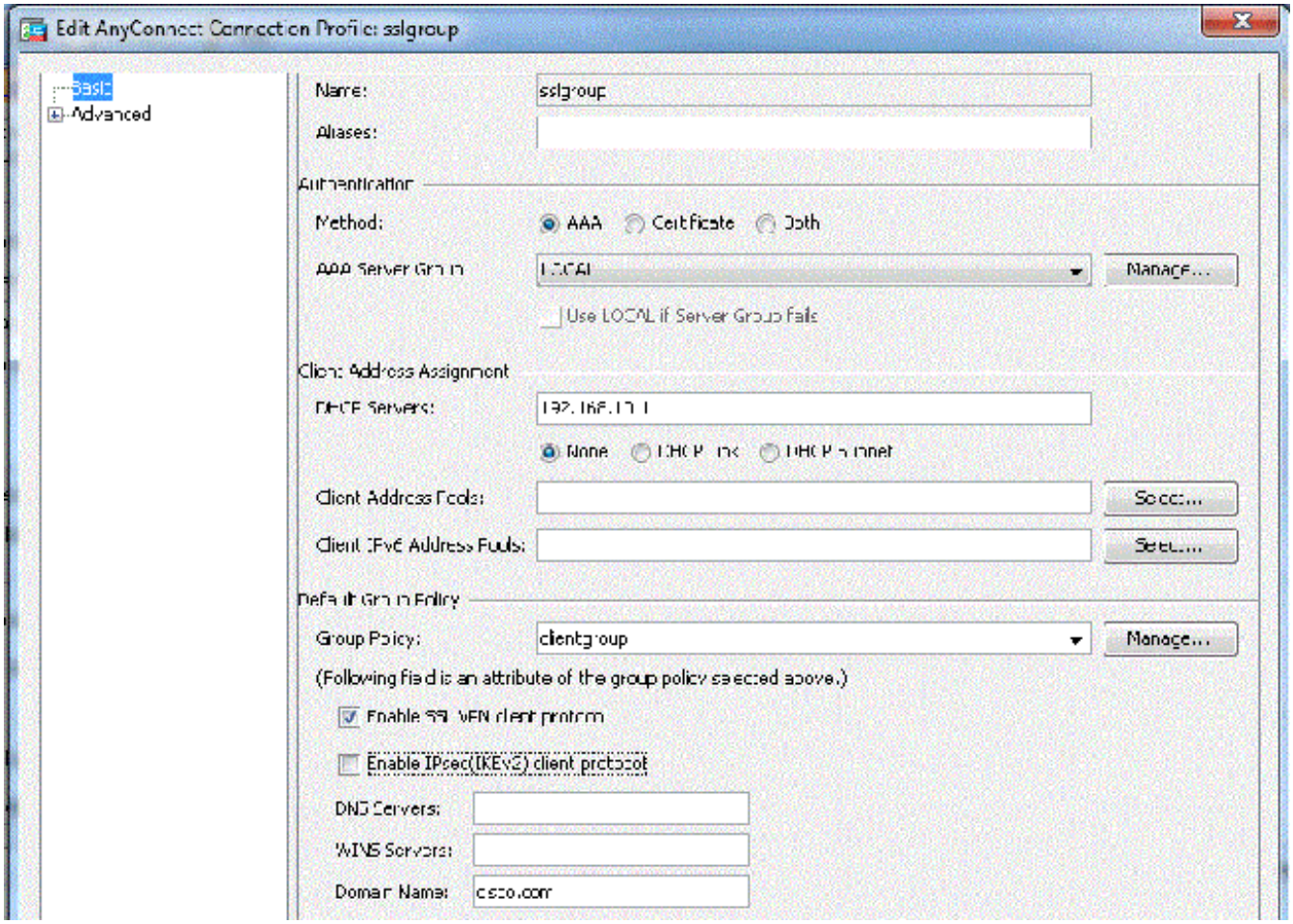
- Configure o Grupo de Túneis.

Escolha a **configuração > o acesso do acesso remoto VPN > da rede (cliente) > o > Add dos perfis de conexão de Anyconnect** a fim criar um **sslgroup** novo do grupo de túneis.

Na guia **Basic**, você pode executar a lista de configurações como mostrado:

Nomeie o grupo de túneis como **sslgroup**.Forneça o endereço IP de servidor DHCP no espaço fornecido para **servidores DHCP**.Sob a política do grupo padrão, escolha o **clientgroup da** política do grupo da lista de drop-down da política do grupo.Configurar o link

DHCP ou a sub-rede DHCP.



Sob o **avançado > o grupo** aba **aliás/grupo URL**, especifica o nome de pseudônimo do grupo como **sslgroup_users** e clica a **APROVAÇÃO**.

Configuração via 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
```

Sub-rede-seleção ou Link-seleção

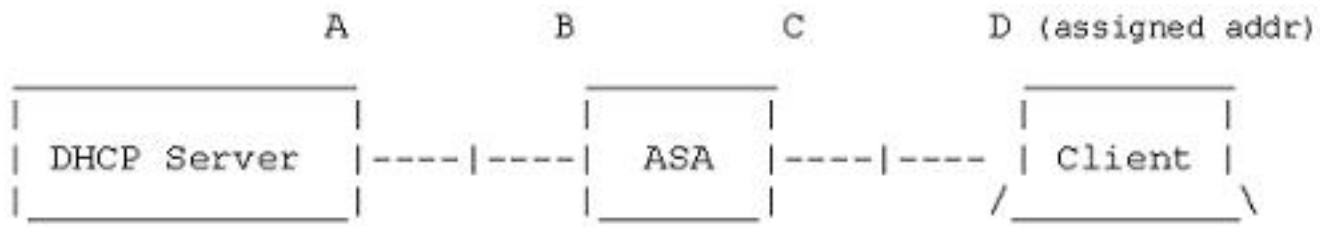
O suporte de proxy DHCP para o RFC 3011 e o RFC 3527 é uma característica introduzida nos 8.0.5 e nos 8.2.2 e foi apoiada em liberações para a frente.

- O RFC 3011 define uma opção de DHCP nova, a opção da seleção da sub-rede, que permite que o DHCP Client especifique a sub-rede em que para atribuir um endereço. Esta opção toma a precedência sobre o método que o servidor DHCP se usa para determinar a sub-rede em que para selecionar um endereço.
- O RFC 3527 define uma subopção nova DHCP, a subopção da seleção do link, que permite que o DHCP Client especifique o endereço a que o servidor DHCP deve responder.

Em termos do ASA, estes RFC permitirão que um usuário especifique um DHCP-rede-espaço

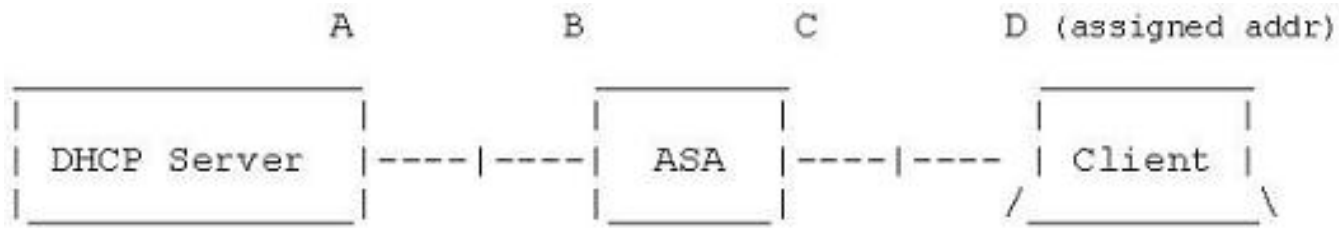
para a atribuição de endereço de DHCP que não é local ao ASA, e o servidor DHCP ainda poderá responder diretamente à relação do ASA. Os diagramas abaixo devem ajudar a ilustrar o comportamento novo. Isto permitirá ao uso espaços NON-locais sem ter que criar uma rota estática para esse espaço em sua rede.

Quando o RFC 3011 ou o RFC 3527 não são permitidos, a troca do proxy DHCP olha similar a esta:




```
Message Exchange:
     Discover: B -> A

     Offer:    A -> dhcp-network-scope

     Request:  B -> A

     Ack:      A -> dhcp-network-scope

     Release:  B -> A
```

Com o qualquer um destes RFC permitidos, a troca olha similar a esta pelo contrário, e o cliente VPN é atribuído ainda um endereço na sub-rede correta:




```
Message Exchange:
     Discover: B -> A

     Offer:    A -> B

     Request:  B -> A

     Ack:      A -> B

     Release:  B -> A
```

Configurar o ASA com uso do CLI

Termine estas etapas a fim configurar o servidor DHCP para fornecer o endereço IP de Um ou Mais Servidores Cisco ICM NT aos clientes VPN da linha de comando. Refira referências adaptáveis do Dispositivo-comando da Segurança do 5500 Series de Cisco ASA para obter mais informações sobre de cada comando que é usado.

```
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#
```