http://www.cisco.com/c/en/us/support/docs/security/anyconnect-secure-mobility-client/118084-configure-anyconnect-00.html

**Introdução**

Este documento descreve como configurar o Cisco 5500-X Series Adaptive Security Appliance (ASA) para fazer o servidor DHCP forneça o endereço IP do cliente para todos os clientes AnyConnect com o uso do Gerenciador de Adaptive Security dispositivo (ASDM) ou CLI.

**Pré-requisitos**

**requisitos**

Este documento assume que o ASA está totalmente operacional e configurado para permitir que o ASDM Cisco ou CLI para fazer alterações na configuração.

**Nota** :  Consulte o  [Livro 1: Series Guia de Configuração Cisco ASA Operações Gerais CLI, 9.2](http://www.cisco.com/c/en/us/td/docs/security/asa/asa92/configuration/general/asa-general-cli/admin-management.html#pgfId-1877733)  para permitir que o dispositivo a ser configurado remotamente pelo ASDM ou Secure Shell (SSH).

**componentes usados**

As informações contidas neste documento é baseado nessas versões de software e hardware:

* Cisco ASA 5500-X Next Generation Firewall Versão 9.2 (1)
* Manager Versão Adaptive Dispositivo de segurança 7.1 (6)
* Cisco AnyConnect Cliente Mobilidade Segura 3.1.05152

As informações contidas neste documento foi criado a partir dos dispositivos em um ambiente de laboratório específico. Todos os aparelhos utilizados neste documento começou com uma configuração afastada (padrão). Se a sua rede é ao vivo, certifique-se de que você entenda o impacto potencial de qualquer comando.

**produtos relacionados**

Esta configuração também pode ser usado com o Cisco ASA 5500 Series Security Appliance versão 7.x e mais tarde.

**Informação de fundo**

VPNs de acesso remoto responder à exigência de força de trabalho móvel para conectar com segurança à rede da organização. Os usuários móveis são capazes de configurar uma conexão segura usando o software cliente Mobilidade Segura Cisco AnyConnect. O cliente Mobilidade Segura Cisco AnyConnect inicia uma conexão com um dispositivo site central configurado para aceitar esses pedidos. Neste exemplo, o dispositivo local central é um ASA 5500-X Series Adaptive Security Appliance que utiliza mapas de cifra dinâmicos.

Em gerenciamento de endereços de dispositivos de segurança, você tem que configurar endereços IP que se conectam um cliente com um recurso na rede privada, através do túnel, e deixe a função de cliente como se estivesse diretamente conectado à rede privada.

Além disso, você está lidando apenas com os endereços IP privados que são atribuídos a clientes. Os endereços IP atribuídos a outros recursos na rede privada fazem parte de suas responsabilidades de administração de rede, não faz parte da gestão VPN.Portanto, quando endereços IP são discutidas aqui, Cisco significam os endereços IP disponíveis na sua rede privada esquema de endereçamento que permite a função de cliente como um ponto final do túnel.

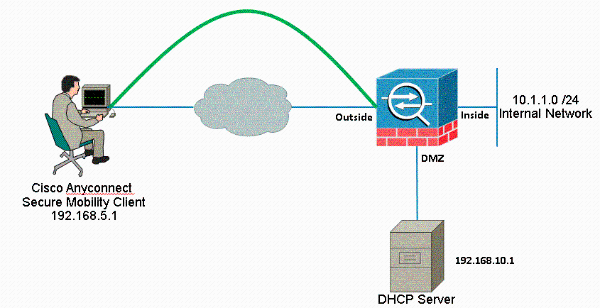
**configurar**

Nesta seção, você é apresentado com as informações para configurar as funções descritas neste documento.

**Nota** : Use as  [Command Lookup Tool](http://tools.cisco.com/Support/CLILookup/cltSearchAction.do)  ( [registrados](http://tools.cisco.com/RPF/register/register.do)  apenas os clientes) para obter mais informações sobre os comandos utilizados nesta seção.

**Diagrama de rede**

Este documento usa essa configuração de rede:



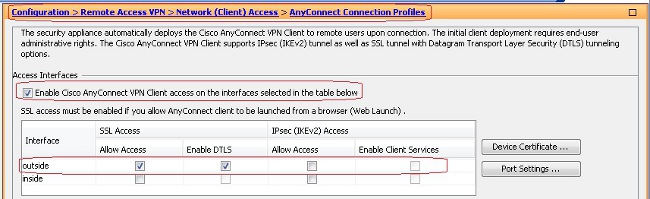
**Nota** :  O esquemas de endereçamento IP usado nesta configuração não são legalmente roteáveis ​​na Internet. Eles são RFC 1918 endereços que foram usados ​​em um ambiente de laboratório.

**Configurar Cisco AnyConnect Cliente mobilidade segura**

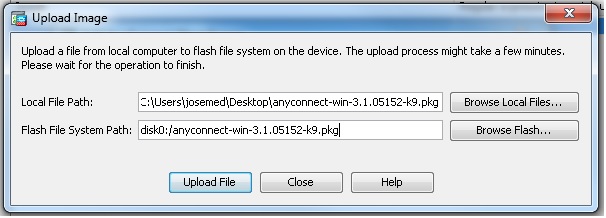
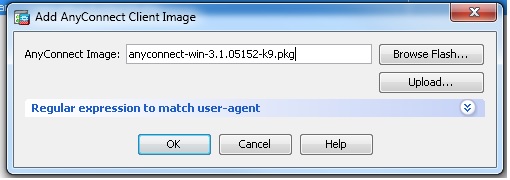
**ASDM Procedimento**

Concluir essas etapas, a fim de configurar o acesso remoto VPN:

* Ativar WebVPN.
  1. Escolha  **configuração> VPN Acesso Remoto> Rede (cliente) de acesso> Perfis SSL VPN conexão**  e sob  **Acesso Interfaces** , clique nas caixas de verificação  **Permitir acesso**  e  **Ativar DTLS**  para a interface externa. Além disso, verifique o  **Ativar Cisco AnyConnect VPN Client ou legado SSL VPN de acesso de cliente na interface selecionada nesta tabela**  caixa de seleção, a fim de ativar o SSL VPN na interface externa.



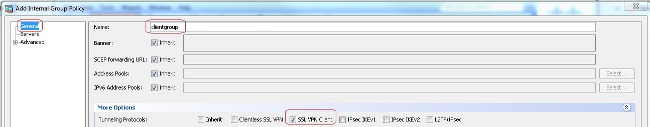
* 1. Clique  **em Aplicar** .
  2. Escolha  **Configurações> VPN Acesso Remoto> Network (Client) Acesso> Anyconnect Client Software> Adicionar** para adicionar a imagem cliente Cisco AnyConnect VPN a partir da memória flash da ASA como mostrado.

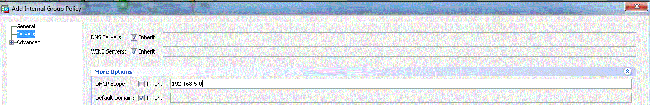
  
  


**Configuração Equivalente:**

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**

Configurar a Política de Grupo.

* Escolha  **Configurações> VPN Acesso Remoto> Network (Client) Acesso> Políticas de Grupo**  , a fim de criar uma política de grupo interno  **clientgroup** . Sob o  **Geral**  guia, selecione o  **cliente VPN SSL**  caixa de seleção, a fim de permitir que o SSL como protocolo de encapsulamento.  
    
  
* Configurar o DHCP Rede-Scope na  **Servers**  guia, escolha  **Mais opções**  , a fim de configurar o escopo DHCP para os usuários a ser atribuído automaticamente.



**Equivalent CLI Configuration:**

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)#

Escolha  **configuração> VPN de acesso remoto> AAA / utilizadores locais> Usuários Locais> Adicionar**  a fim de criar uma nova conta de usuário  **ssluser1** . Clique  **em OK**  e, em seguida  **Aplicar** .

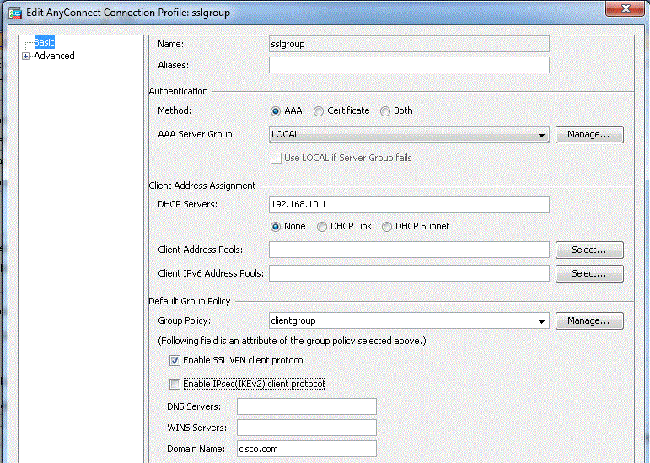


**Equivalent CLI Configuration:**

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

Configurar Grupo Tunnel.

* Escolha  **Configuração> Acesso Remoto VPN> Network (Client) Acesso> perfis de ligação AnyConnect> Adicionar** a fim de criar um novo grupo de túnel  **sslgroup** .
* No  **Básico**  guia, você pode executar a lista de configurações, como mostrado:
  1. Nome do grupo Tunnel como  **sslgroup** .
  2. Fornecer o endereço IP do servidor DHCP no espaço fornecido para  **servidores DHCP** .
  3. Em Default Policy Group, escolher a política de grupo  **clientgroup**  na lista drop-down de Política de Grupo.
  4. Configurar DHCP link ou DHCP de sub-rede.



* Sob a  **URL Avançado> Grupo Alias ​​/ Grupo**  guia, especifique o nome do alias grupo como  **sslgroup\_users**  e clique **OK** .
* **Equivalent CLI Configuration:**

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**

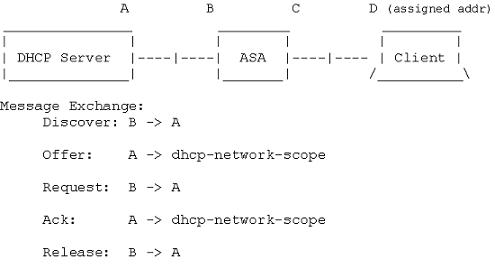
**Subnet-Seleção ou Link-Selecção**

Apoio Proxy DHCP para o  [RFC 3011](http://tools.ietf.org/html/rfc3011)  e  [RFC 3527](http://tools.ietf.org/html/rfc3527)  é uma característica introduzida no 8.0.5 e 8.2.2 e foi suportado em diante libera.

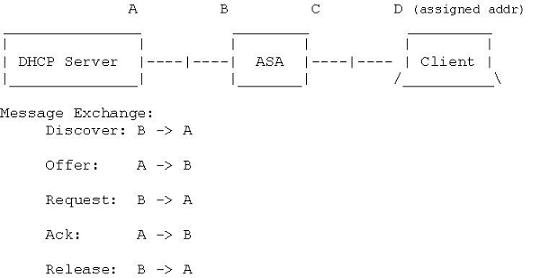
* [RFC 3011](http://tools.ietf.org/html/rfc3011)  define uma nova opção DHCP, a opção de seleção de sub-rede, o que permite que o cliente DHCP para especificar a sub-rede na qual a atribuir um endereço. Esta opção tem precedência sobre o método que o servidor DHCP utiliza para determinar a sub-rede na qual selecionar um endereço.
* [RFC 3527](http://tools.ietf.org/html/rfc3527)  define um novo sub-opção DHCP, a subopção selecção da ligação, que permite que o cliente DHCP para especificar o endereço para o qual o servidor DHCP deve responder.

Em termos do ASA, estes RFCs permitirá que um usuário para especificar um dhcp-rede de possibilidades de Atribuição de endereço DHCP que não é local para o ASA, eo servidor DHCP ainda será capaz de responder diretamente à interface do ASA. Os diagramas abaixo deve ajudar a ilustrar o novo comportamento. Isto irá permitir o uso escopos não-local sem ter que criar uma rota estática para esse escopo na sua rede.

Quando [RFC 3011](http://tools.ietf.org/html/rfc3011)  ou  [RFC 3527](http://tools.ietf.org/html/rfc3527) não está habilitado, a troca Proxy DHCP semelhante a este:

****

Com qualquer um desses RFCs ativado, a troca semelhante a este em vez disso, eo cliente VPN ainda é atribuído um endereço na sub-rede correto:

****

**Configurar o ASA com o uso do CLI**

Conclua estas etapas para configurar o servidor DHCP para fornecer o endereço IP para clientes VPN a partir da linha de comando.Consulte a  [Cisco ASA 5500 Series Adaptive Security Appliances Referências-comando](http://www.cisco.com/en/US/products/ps6120/prod_command_reference_list.html)  para mais informações sobre 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#

Configuração Anyconnect Básica:

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**

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)#

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

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**