ASA/PIX: Endereçamento do cliente do IPSec VPN usando o servidor DHCP com exemplo da configuração ASDM

Índice

Introdução

Este documento descreve como configurar o Cisco 5500 Series Adaptive Security Appliance (ASA) para fazer com que o servidor DHCP forneça o endereço IP do cliente para todos clientes VPN utilizando o Adaptive Security Device Manager (ASDM) ou a CLI. O ASDM oferece gerenciamento de segurança de nível mundial e monitoramento através de uma interface de gerenciamento baseada na Web intuitiva e fácil de usar. Quando a configuração de roteador Cisco estiver concluída, ela pode ser verificada usando o Cisco VPN Client.

Refira PIX/ASA 7.x e Cisco VPN Client 4.x com exemplo da configuração de autenticação do RAIO de Windows 2003 IAS (contra o diretório ativo) a fim estabelecer a conexão VPN de acesso remoto entre um Cisco VPN Client (4.x para Windows) e a ferramenta de segurança 7.x da série PIX 500. O usuário de cliente VPN remoto autentica contra o diretório ativo usando um servidor Radius do Internet Authentication Service de Microsoft Windows 2003 (IAS).

Refira PIX/ASA 7.x e Cisco VPN Client 4.x para o exemplo da configuração de autenticação do

Cisco Secure ACS a fim estabelecer uma conexão VPN de acesso remoto entre um Cisco VPN Client (4.x para Windows) e a ferramenta de segurança 7.x da série PIX 500 usando um Serviço de controle de acesso Cisco Secure (versão de ACS 3.2) para a autenticação extendida (XAUTH).

Pré-requisitos

Requisitos

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

Nota: Refira permitir o acesso HTTPS para ASDM ou PIX/ASA 7.x: SSH no exemplo de configuração da interface interna e externa 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 software adaptável 7.x da ferramenta de segurança de Cisco e mais tarde
- Versão 5.x e mais recente adaptável do Security Device Manager
- Versão Cliente VPN Cisco 4.x e mais tarde

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 da ferramenta de segurança de Cisco PIX.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

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 VPN instalado em seus PC. O cliente VPN 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 Series ASA que use mapas cripto dinâmico.

Na gerência de endereços da ferramenta de segurança nós temos 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, nós estamos tratando somente os endereços IP privados que obtêm 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, nós significamos 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.

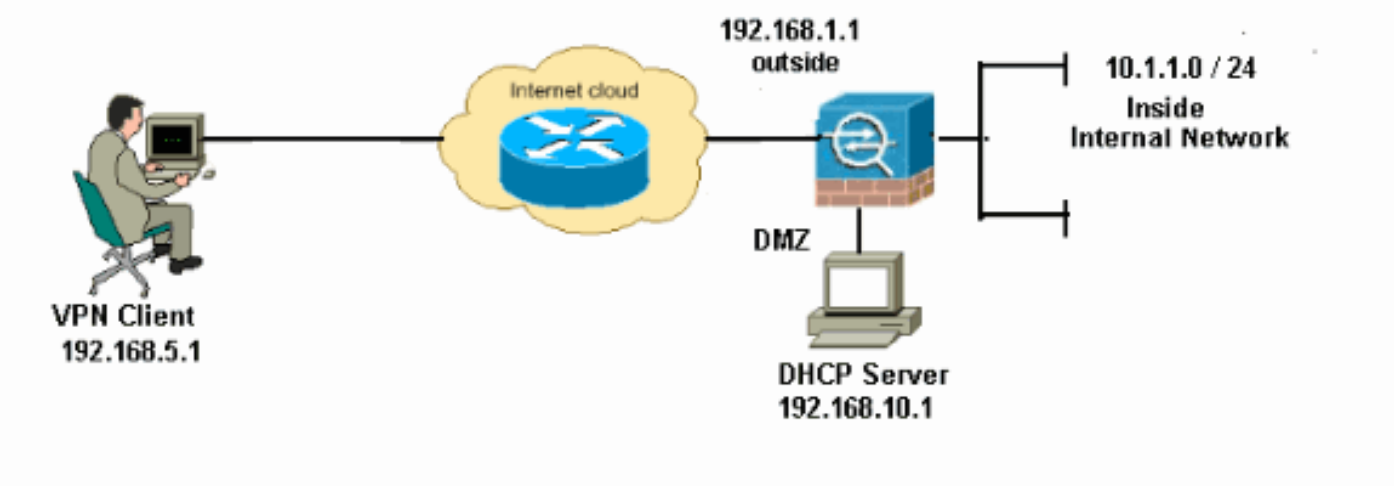
Configurar

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:



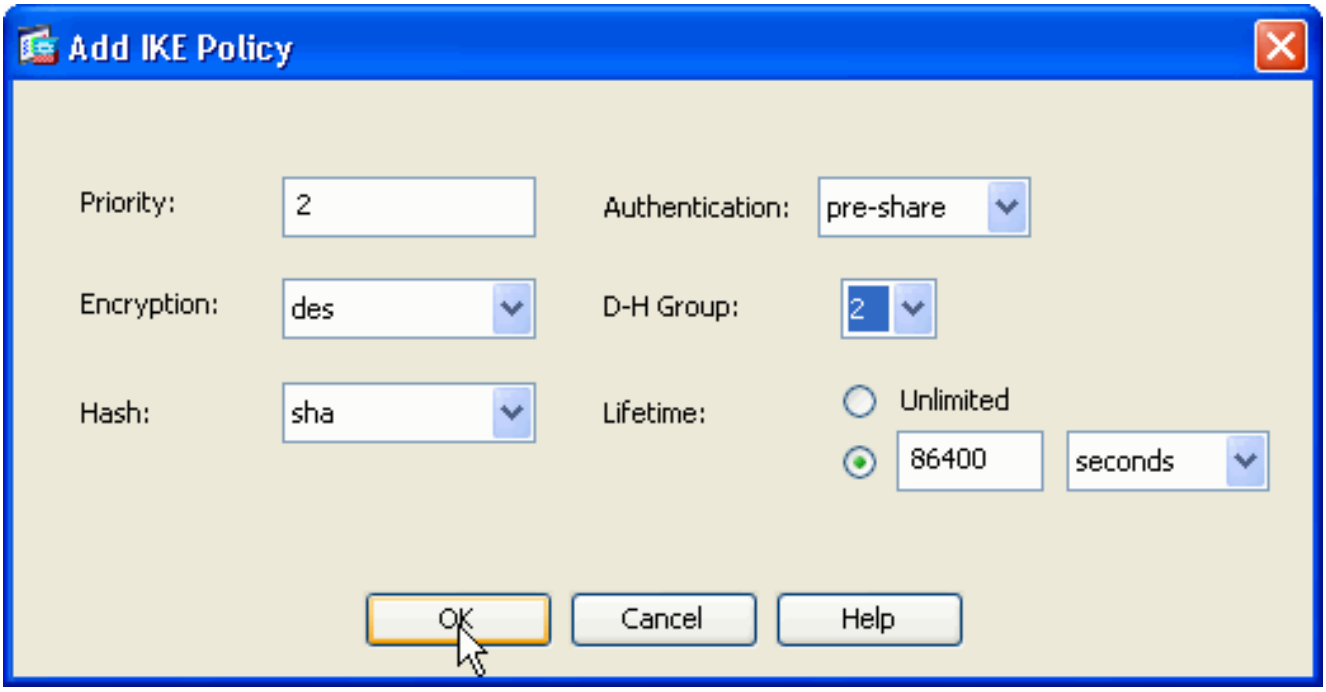
Nota: Os esquemas de endereçamento IP usados nesta configuração não são legalmente roteáveis na Internet. São os endereços do RFC 1918 que foram usados em um ambiente de laboratório.

Configurar o acesso remoto VPN (o IPsec)

Procedimento ASDM

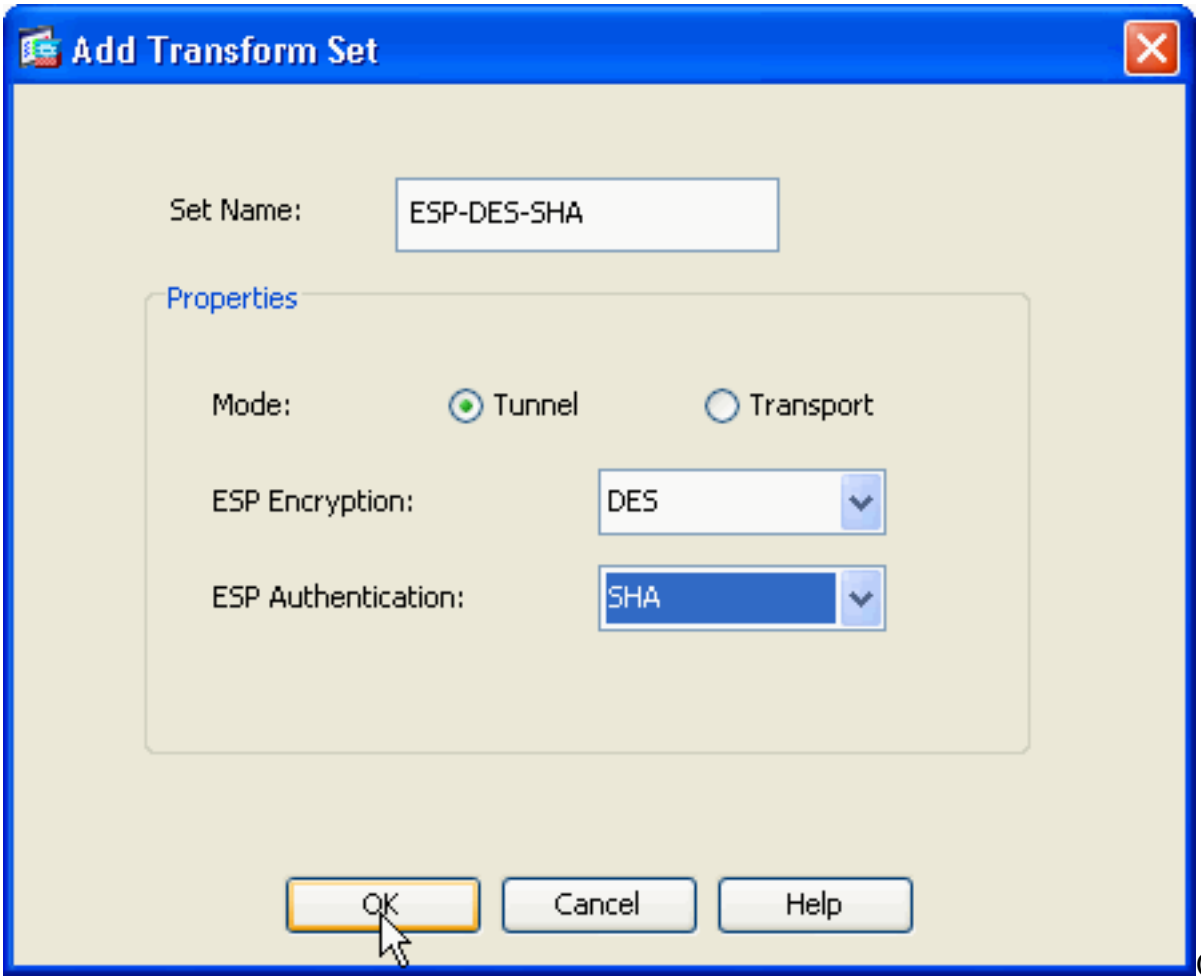
Termine estas etapas a fim configurar o acesso remoto VPN:

1. Escolha a **configuração > o acesso do acesso remoto VPN > da rede (cliente) > avançou > > Add do IPsec > das políticas de IKE** a fim criar uma política de ISAKMP 2, como mostrado.



Clique a **APROVAÇÃO** e **aplique-a**.

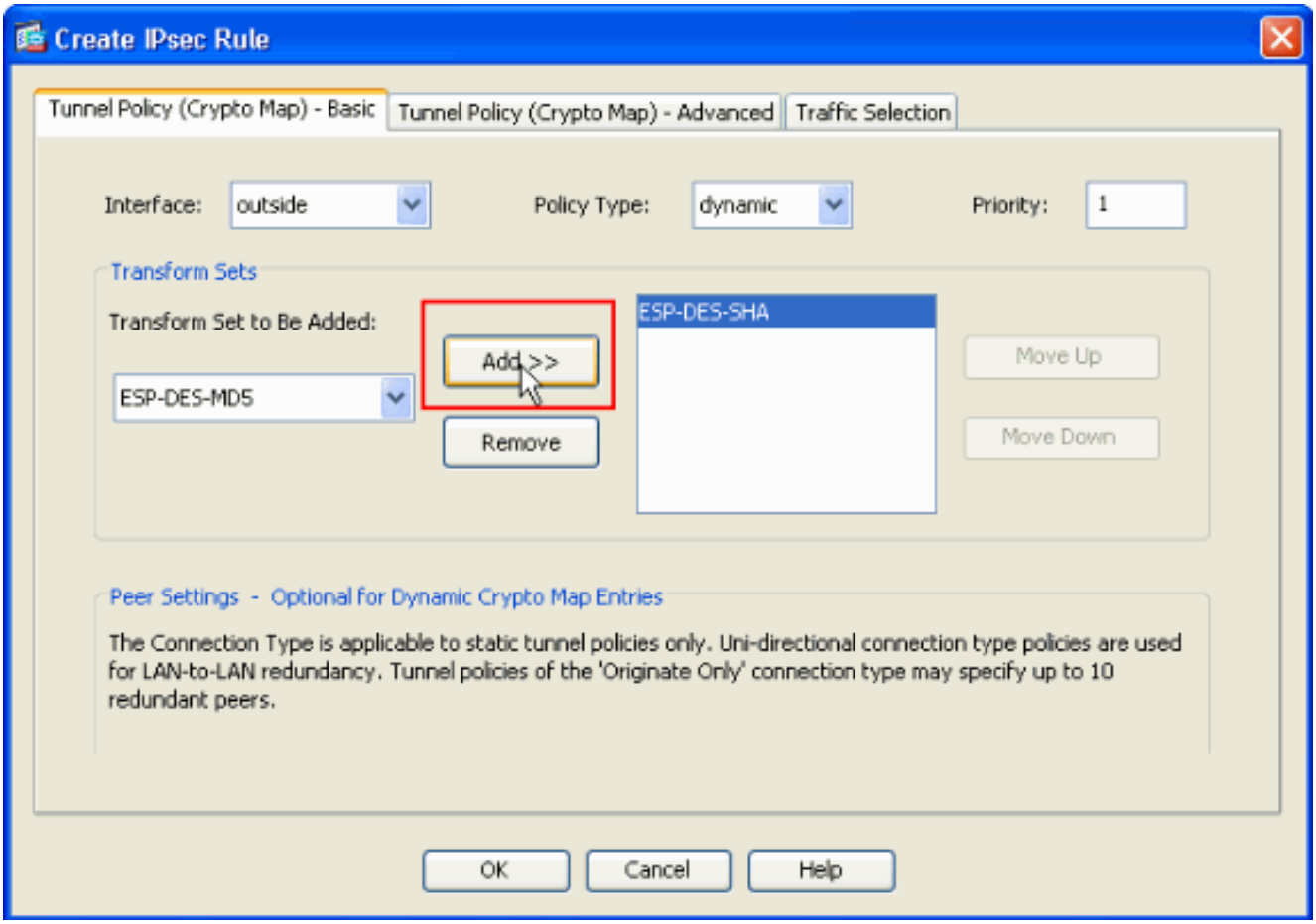
2. Escolha a **configuração > o acesso do acesso remoto VPN > da rede (cliente) > avançou > IPsec > IPsec transformam o > Add dos grupos** a fim criar o **ESP-DES-SHA** transformam o grupo, como
mostrado.



Clique a **APROVAÇÃO** e **aplique-a**.

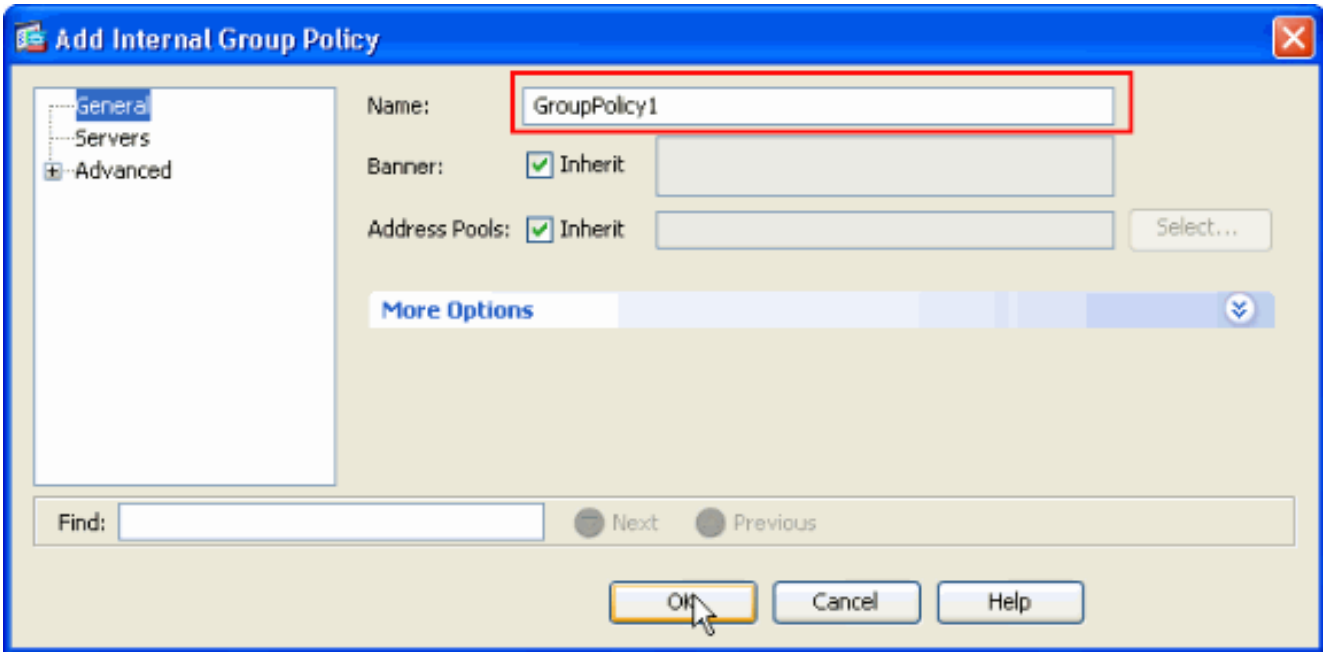
3. Escolha a **configuração > o acesso do acesso remoto VPN > da rede (cliente) > avançou > > Add do IPsec > dos crypto map** a fim criar um crypto map com a política dinâmica da prioridade 1, como

mostrado.



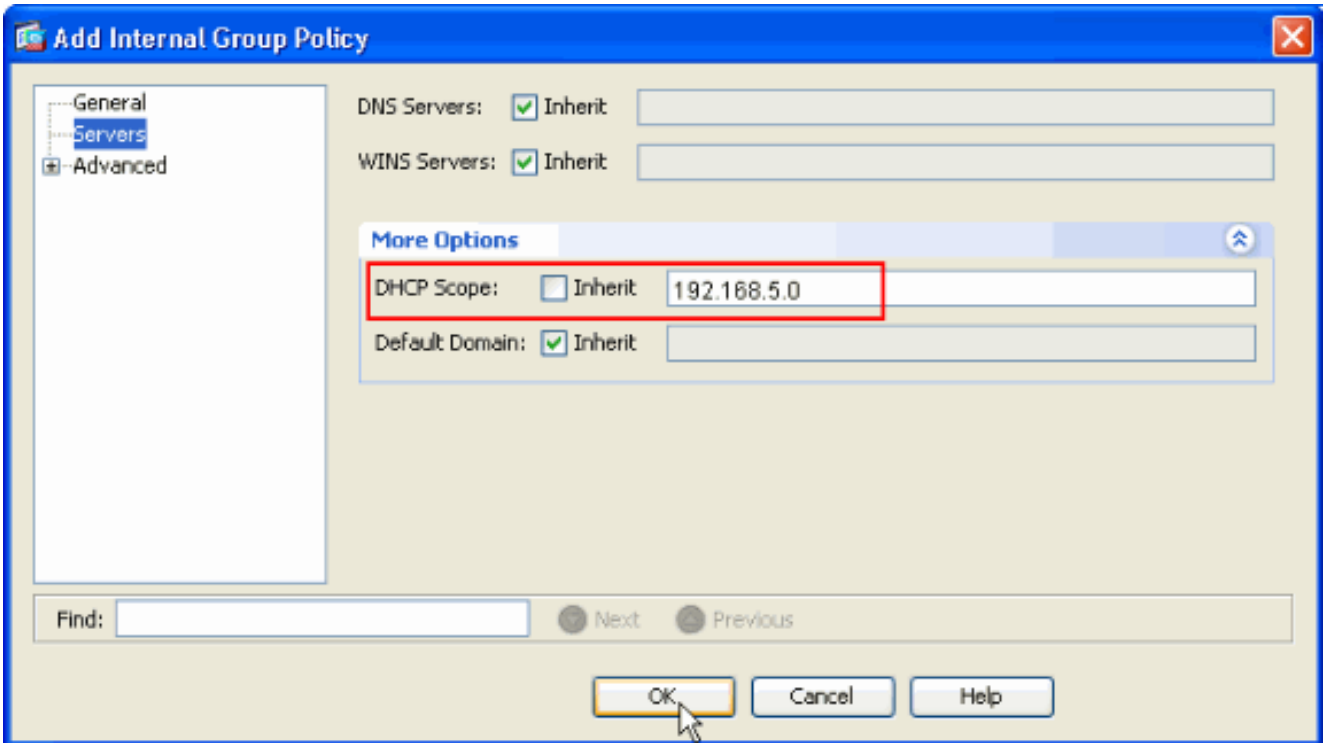
Clique a **APROVAÇÃO** e **aplique-a**.

4. Escolha a **configuração > o acesso do acesso remoto VPN > da rede (cliente) > avançou > políticas do grupo > políticas do grupo de Add>Internal** a fim criar uma política do grupo (por exemplo **GroupPloicy1**), como mostrado.



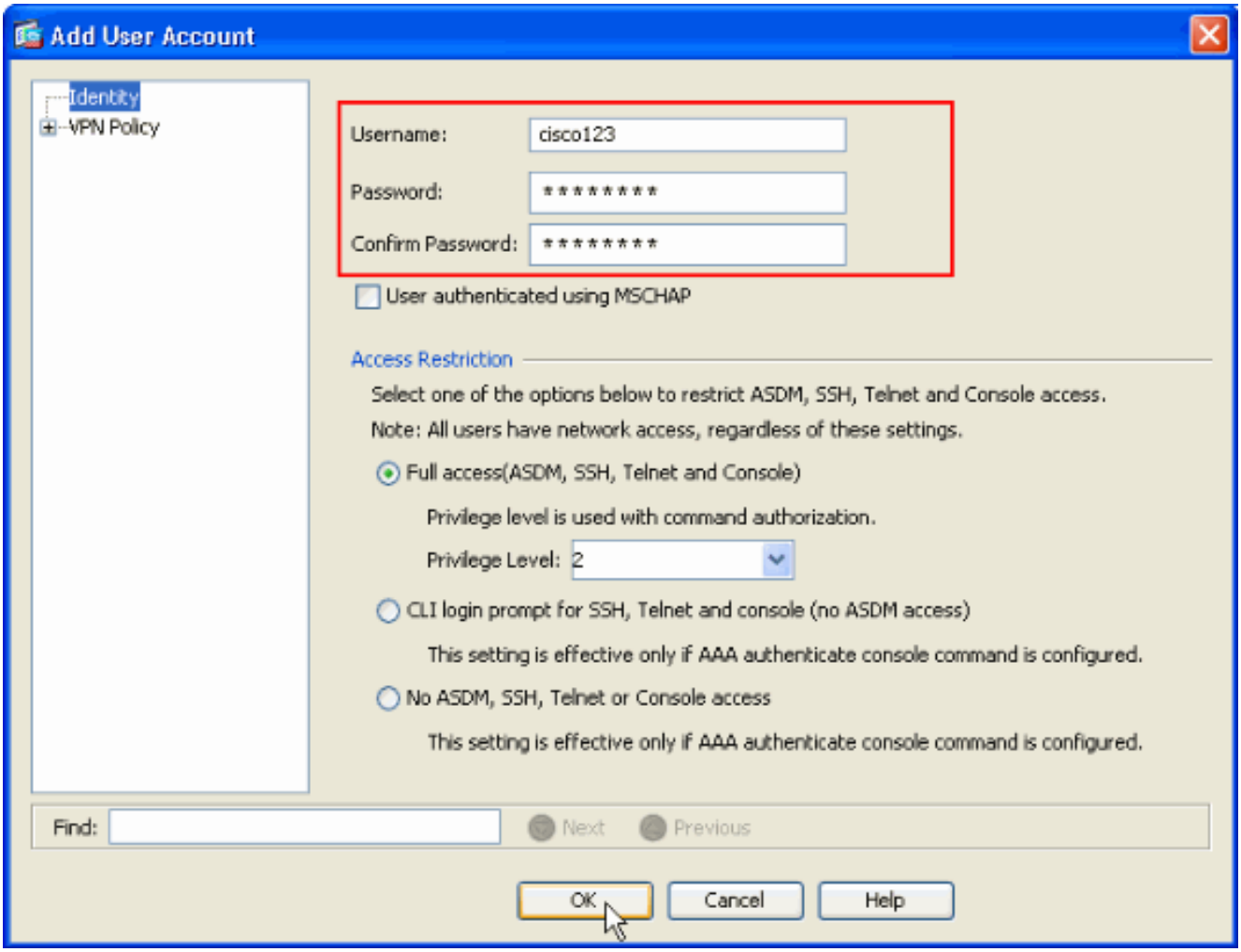
Clique a **APROVAÇÃO** e **aplique-a**.

5. Escolha a **configuração > o acesso do acesso remoto VPN > da rede (cliente) > avançou > políticas do grupo > grupo Policies>Servers>> de Add>Internal** a fim configurar o **escopo de DHCP** para que os usuários de cliente VPN sejam atribuídos dinamicamente.



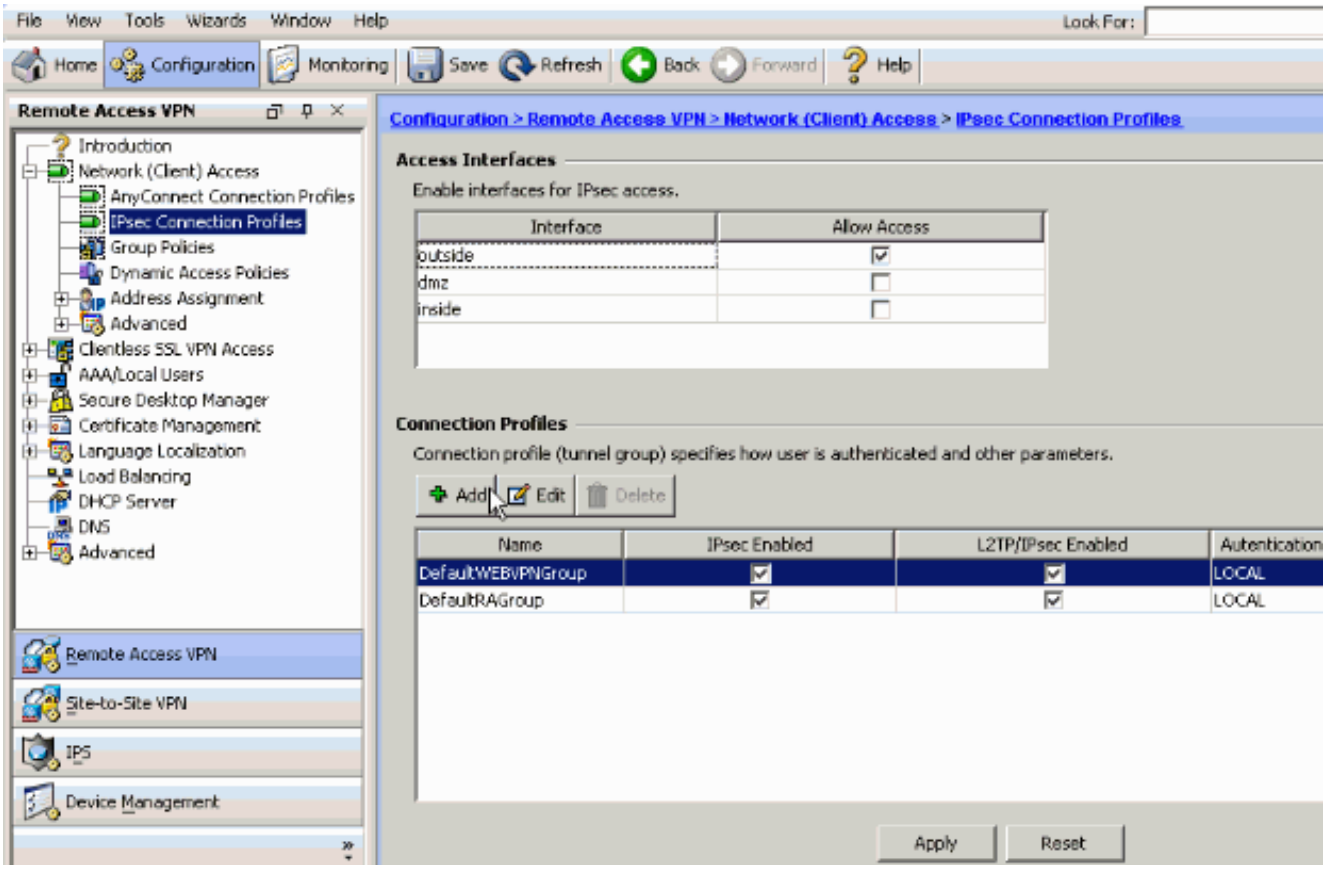
Clique a **APROVAÇÃO** e **aplique-a**.**Nota:** A configuração do escopo de DHCP é opcional. Refira configurar o endereçamento de DHCP para mais informação.

6. Escolha a **configuração > o acesso remoto VPN > o AAA Setup > > Add dos usuários locais** a fim criar a conta de usuário (por exemplo, username - cisco123 e senha - cisco123) para o acesso de cliente
VPN.

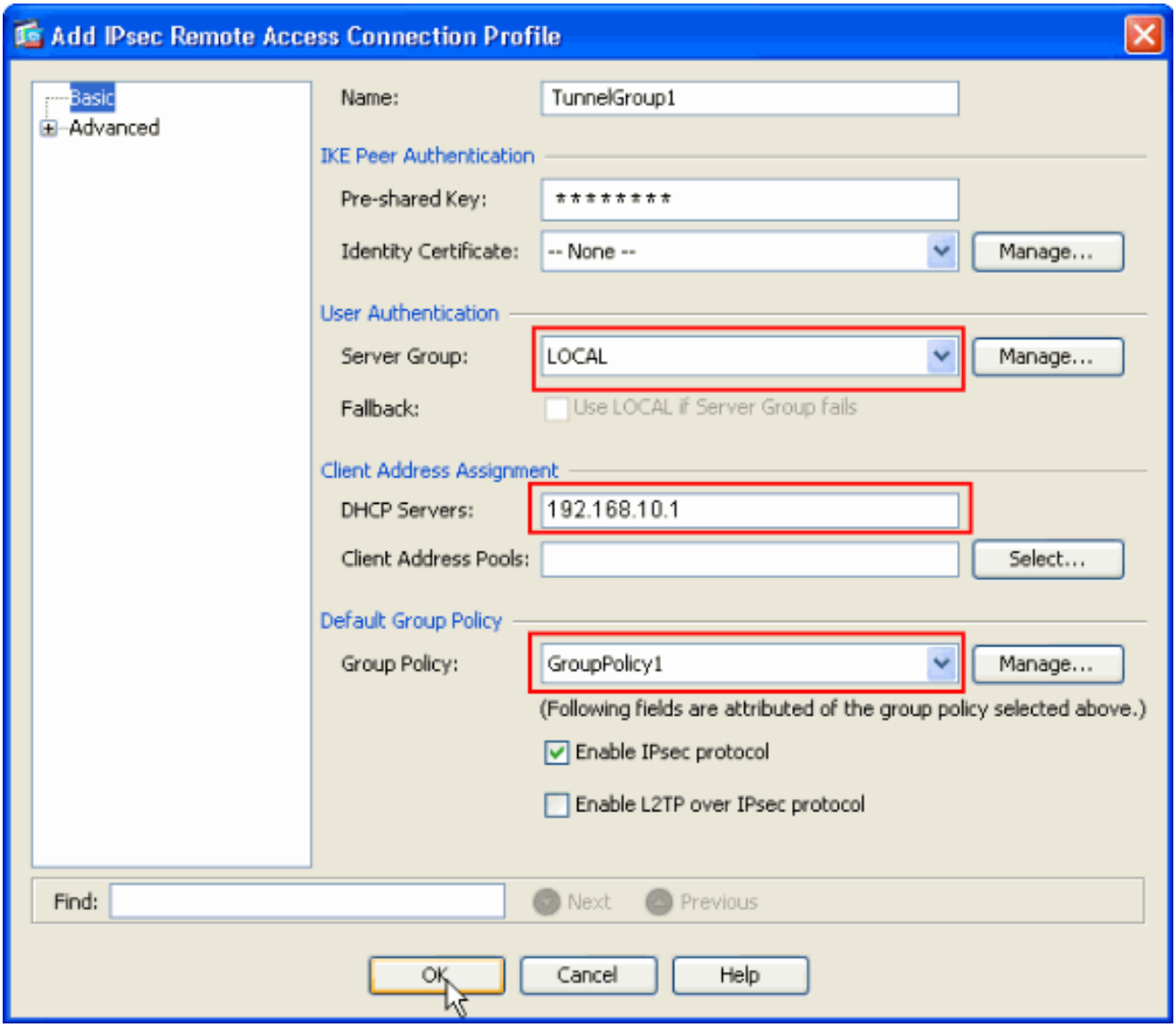


7. Escolha a **configuração > o acesso remoto VPN > o acesso > a conexão IPSec da rede**

(cliente) perfila > Add> a fim adicionar um grupo de túneis (por exemplo, **TunnelGroup1** e a chave Preshared como o cisco123), como
mostrado.

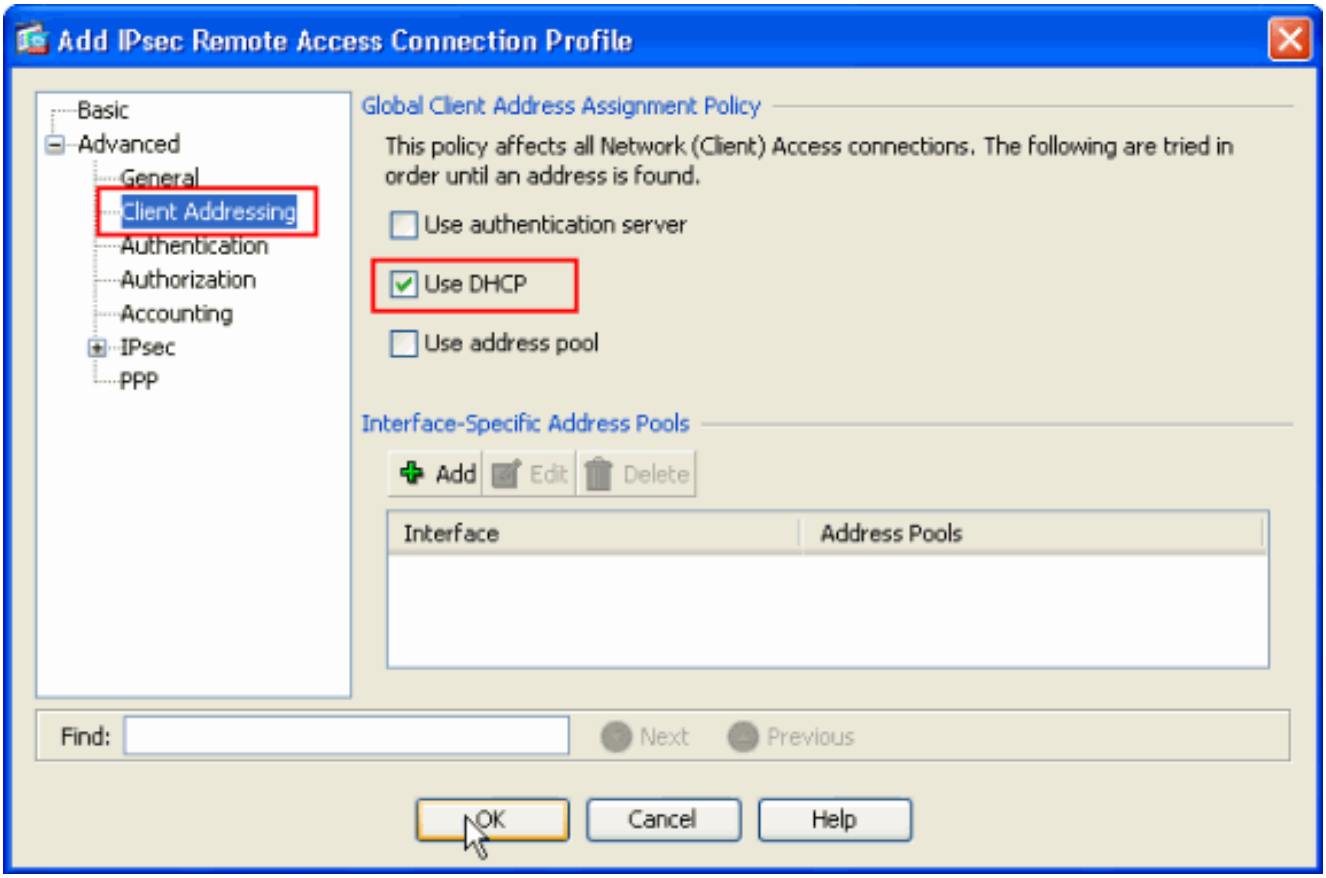


Sob a aba **básica** escolha o grupo de servidor como o **LOCAL** para o campo da autenticação de usuário.Escolha **Grouppolicy1** como a política do grupo para o campo da política do grupo padrão.Forneça o endereço IP de servidor DHCP no espaço fornecido para **servidores DHCP**.



Clique em **OK**.

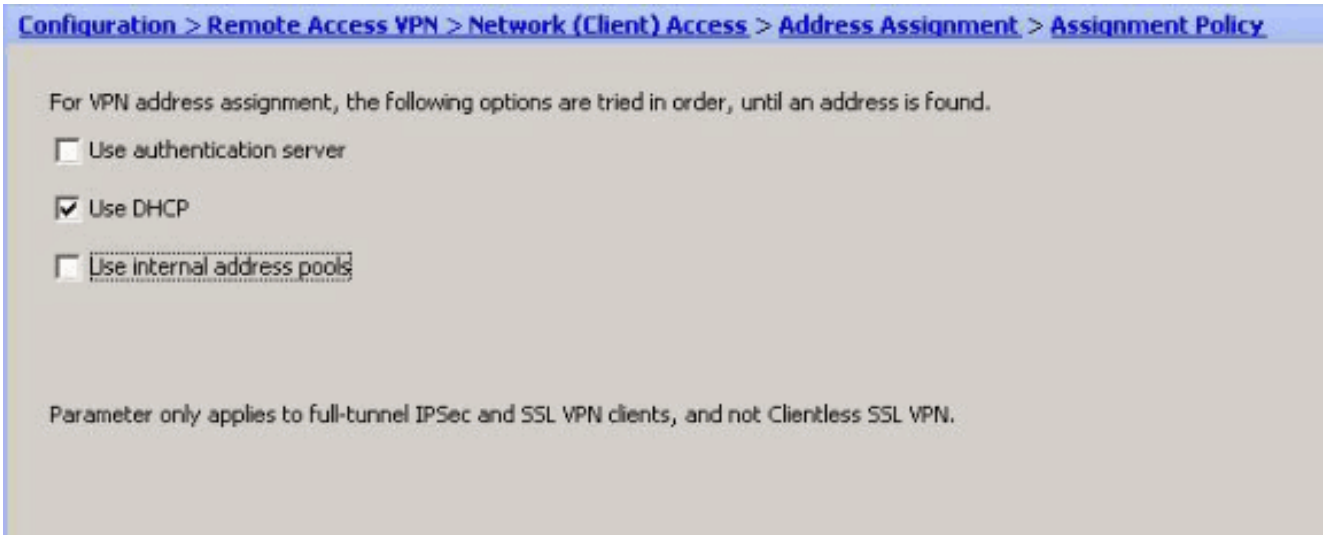
8. Escolha **avançado > endereçamento do cliente >** e verifique a caixa de seleção do **uso DHCP** para ver se há o servidor DHCP para atribuir o endereço IP de Um ou Mais Servidores Cisco ICM NT aos clientes VPN.**Nota:** Certifique-se desmarcar as caixas de seleção para o **Authentication Server do uso** e **usar o conjunto de endereços**.



Configuração para ASDM 6.x

A mesma configuração ASDM trabalha muito bem com a versão 6.x ASDM, à exceção de algumas modificações pequenas em termos dos trajetos ASDM. Os trajetos ASDM a determinados campos tiveram uma variação da versão 6.2 e mais recente ASDM. As alterações junto com os trajetos existentes estão listadas abaixo. As imagens gráficas não são anexadas aqui nos casos onde permanecem as mesmas para todas as versões principais ASDM.

1. A configuração > o acesso do acesso remoto VPN > da rede (cliente) > avançaram > > Add do IPsec > das políticas de IKE
2. A configuração > o acesso do acesso remoto VPN > da rede (cliente) > avançaram > IPsec > IPsec transformam o > Add dos grupos
3. A configuração > o acesso do acesso remoto VPN > da rede (cliente) > avançaram > > Add do IPsec > dos crypto map
4. Escolha a configuração > o acesso remoto VPN > do acesso > do grupo da rede (cliente) > Add > Políticas internas de grupo das políticas
5. Escolha a configuração > o acesso remoto VPN > do acesso > do grupo da rede (cliente) políticas > server do grupo do >Internal do > Add das políticas
6. Escolha a configuração > o acesso remoto VPN > o AAA > Add Setup/usuários locais > dos usuários locais
7. A configuração > o acesso remoto VPN > o acesso > a conexão IPSec da rede (cliente) perfilam o > Add
8. Escolha a configuração > o acesso remoto VPN > do acesso > da atribuição de endereço > da atribuição da rede (cliente)
   política



Todas estas três opções são permitidas à revelia. Cisco ASA segue a mesma ordem para atribuir endereços aos clientes VPN. Quando você desmarca outras duas opções, Cisco ASA não verifica as opções do server e do conjunto local aaa. As opções permitidas padrão podem ser verificadas pela **mostra executam tudo | em VPN-adicionar o** comando. Este é um exemplo de saída para sua referência:

```
vpn-addr-assign aaa
vpn-addr-assign dhcp
vpn-addr-assign local reuse-delay 0
```

Para obter mais informações sobre deste comando, consulte VPN-ADDR-para atribuir.

Configurar o ASA/PIX usando o 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 configurar referências adaptáveis do Dispositivo-comando da Segurança do 5500 Series dos acessos remoto VPN ou do Cisco ASA para obter mais informações sobre de cada comando que é usado.

Configuração running no dispositivo ASA

```
ASA# sh run
ASA Version 8.0(2)
!
!--- Specify the hostname for the Security Appliance.
hostname ASA enable password 8Ry2YjIyt7RRXU24 encrypted
names ! !--- Configure the outside and inside
interfaces. interface Ethernet0/0 nameif inside
security-level 100 ip address 10.1.1.1 255.255.255.0 !
interface Ethernet0/1 nameif outside security-level 0 ip
address 192.168.1.1 255.255.255.0 ! interface
Ethernet0/2 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 access-list 101
extended permit ip 10.1.1.0 255.255.255.0 192.168.5.0
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-613.bin no asdm history enable arp timeout
14400 global (outside) 1 192.168.1.5 nat (inside) 0
```

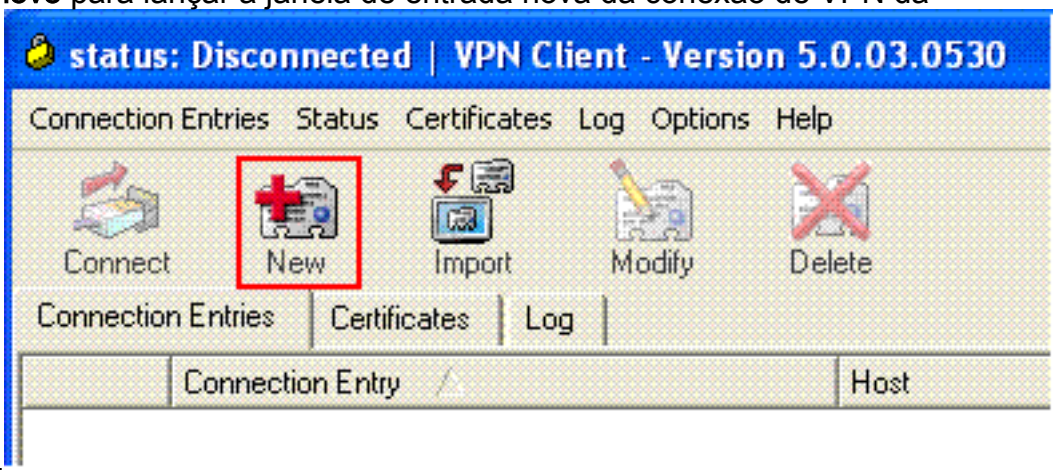
```
access-list 101 nat (inside) 1 0.0.0.0 0.0.0.0 route
outside 0.0.0.0 0.0.0.0 192.168.1.2 1 timeout xlate
3:00:00 timeout conn 1:00:00 half-closed 0:10:00 udp
0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00 h323 0:05:00
h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 timeout sip
0:30:00 sip_media 0:02:00 sip-invite 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 crypto
ipsec transform-set ESP-DES-SHA esp-des esp-sha-hmac
crypto dynamic-map outside_dyn_map 1 set transform-set
ESP-DES-SHA crypto map outside_map 1 ipsec-isakmp
dynamic outside_dyn_map !--- Specifies the interface to
be used with !--- the settings defined in this
configuration. crypto map outside_map interface outside
!--- PHASE 1 CONFIGURATION ---! !--- This configuration
uses ISAKMP policy 2. !--- The configuration commands
here define the Phase !--- 1 policy parameters that are
used. crypto isakmp enable outside crypto isakmp policy
2 authentication pre-share encryption des hash sha group
2 lifetime 86400 no crypto isakmp nat-traversal !---
Specifies that the IP address to the vpn clients are
assigned by the DHCP Server and now by AAA or the Local
pool.The CLI vpn-addr-assign dhcp for VPN address
assignment through DHCP Server is hidden in the CLI
provided by show run command.

no vpn-addr-assign aaa
no vpn-addr-assign local

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
!
```

```
group-policy GroupPolicy1 internal
group-policy GroupPolicy1 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 cisco123
password ffIRPGpDSOJh9YLq encrypted

!--- Create a new tunnel group and set the connection !-
-- type to remote-access. tunnel-group TunnelGroup1 type
remote-access !--- Define the DHCP server address to the
tunnel group. tunnel-group TunnelGroup1 general-
attributes default-group-policy GroupPolicy1 dhcp-server
192.168.10.1

!--- Enter the pre-shared-key to configure the
authentication method. tunnel-group TunnelGroup1 ipsec-
attributes pre-shared-key * prompt hostname context
Cryptochecksum:e0725ca9ccc28af488ded9ee36b7822d : end
ASA#
```

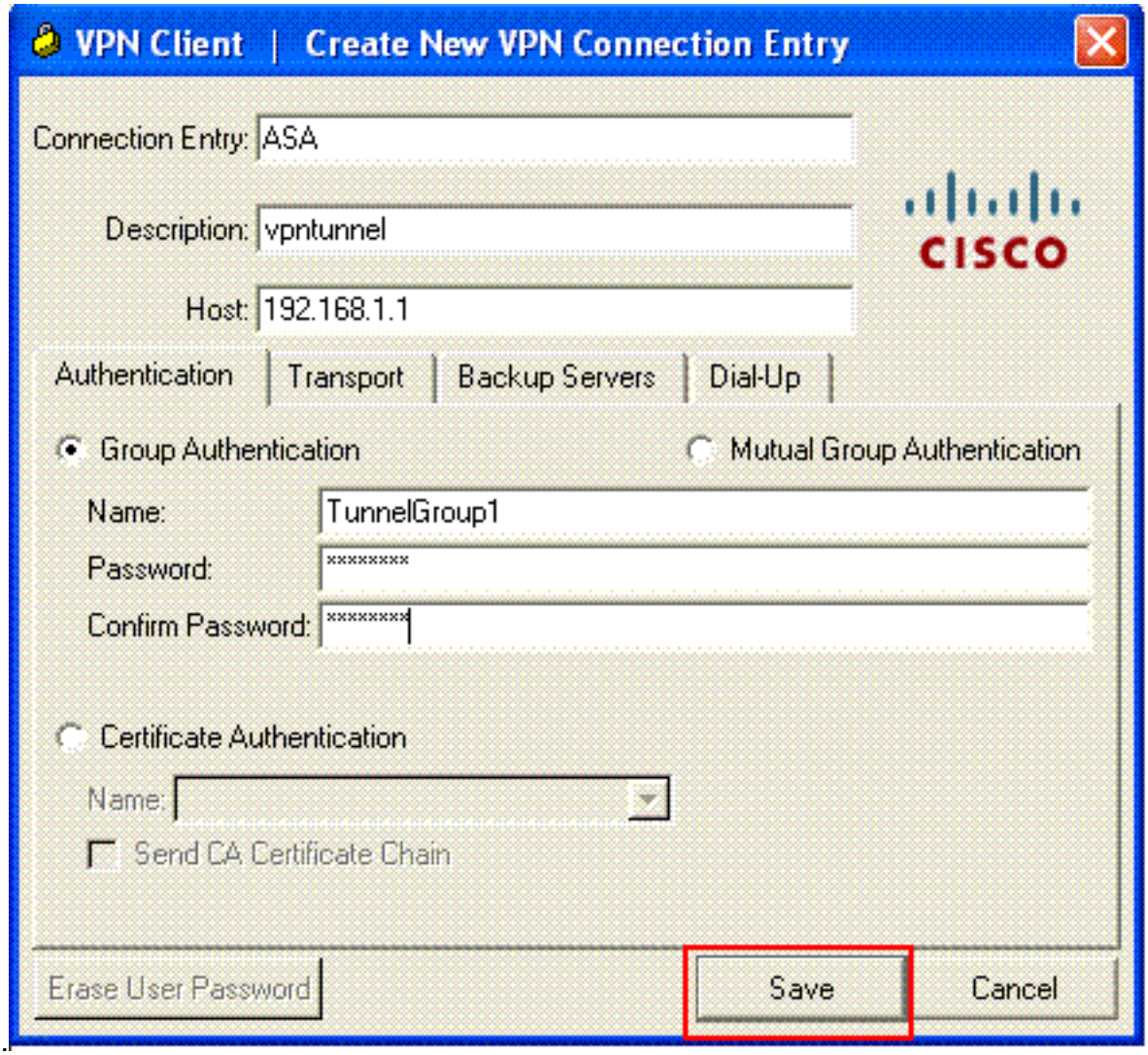
Configuração de Cisco VPN Client

Tente conectar a Cisco ASA usando o Cisco VPN Client a fim verificar que o ASA está configurado com sucesso.

1. Selecione o **Iniciar > Programas > Cliente de VPN de Sistemas Cisco > o cliente VPN**.
2. Clique **novo** para lançar a janela de entrada nova da conexão de VPN da criação.

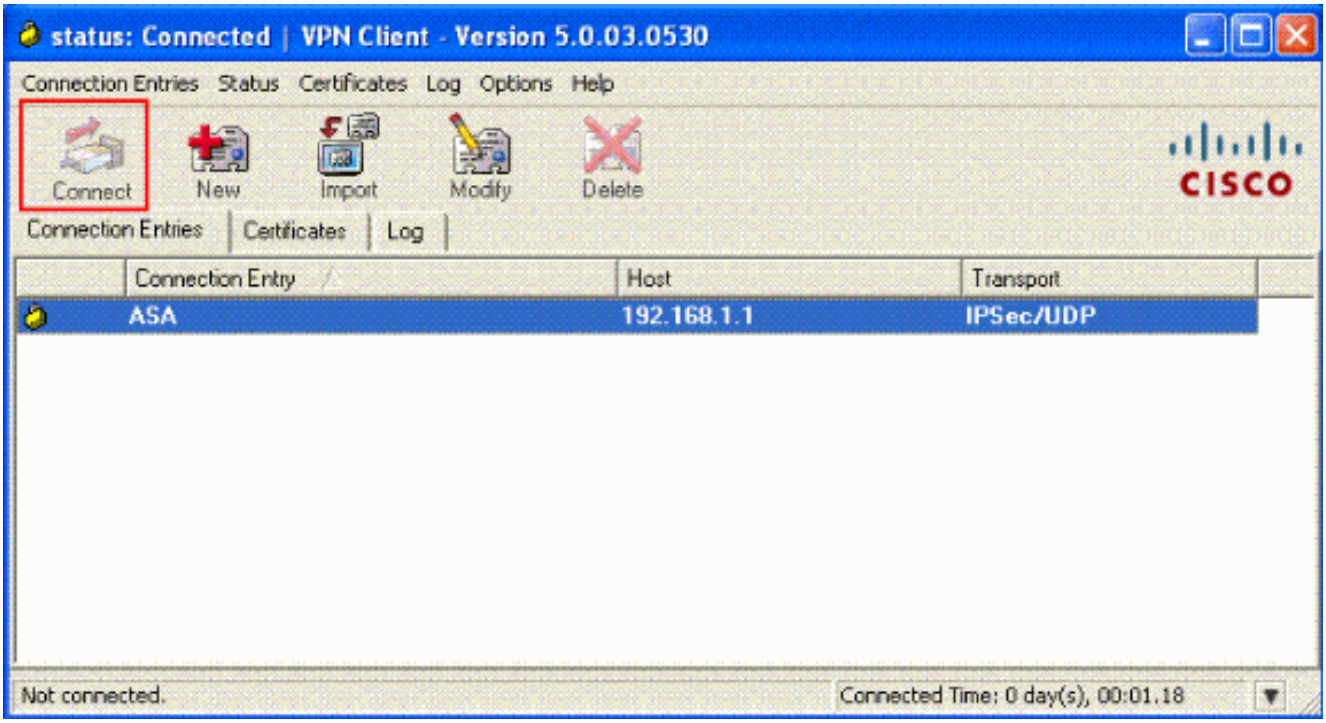


3. Preencha os detalhes de sua nova conexão.Dê entrada com o nome da entrada de conexão junto com uma descrição. Incorpore o **endereço IP externo do ASA à** caixa do host. Incorpore então o grupo de túneis VPN name(TunnelGroup1) e a senha (chave pré-compartilhada - cisco123) como configurado no ASA. Click

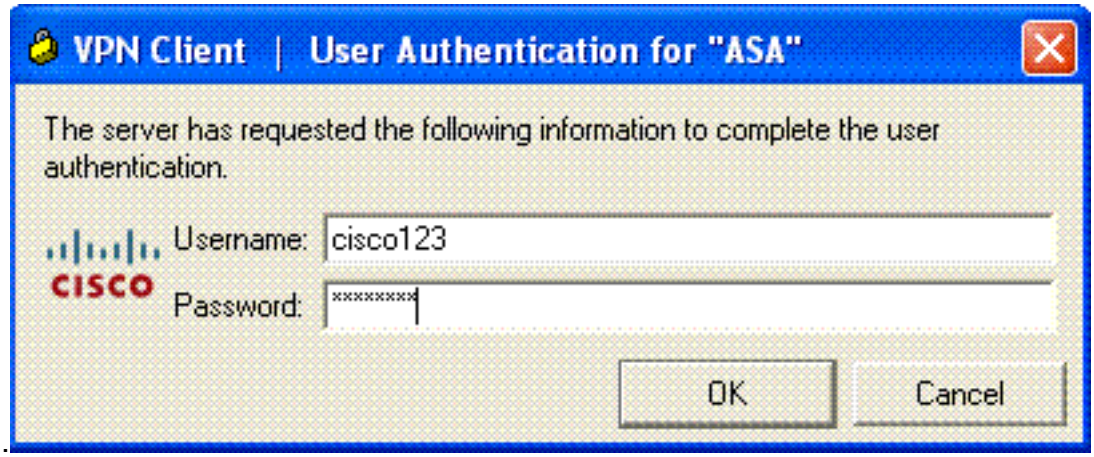


Save.

4. Clique sobre a conexão que você quer se usar e o clique **conecta da** janela principal do cliente
VPN.

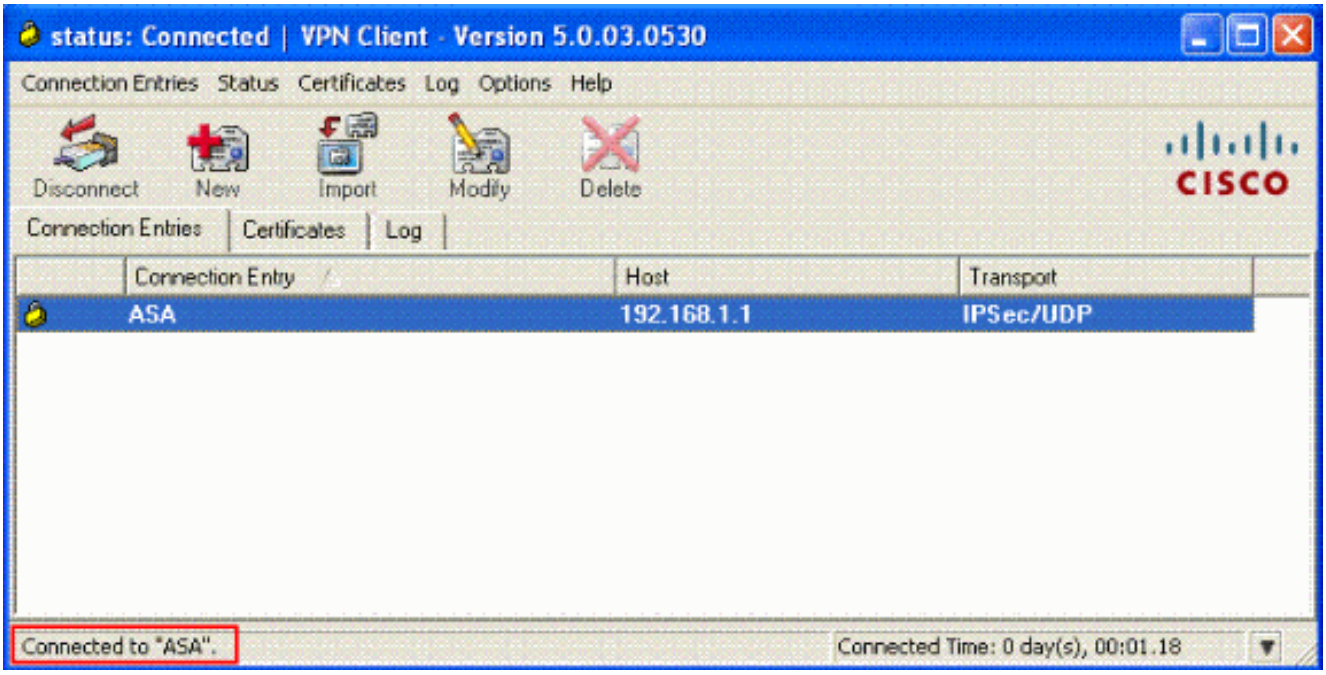


5. Quando alertado, incorpore o **username: cisco123** e **senha: cisco123** como configurado no ASA acima para o Xauth, e **APROVAÇÃO do** clique a conectar à rede

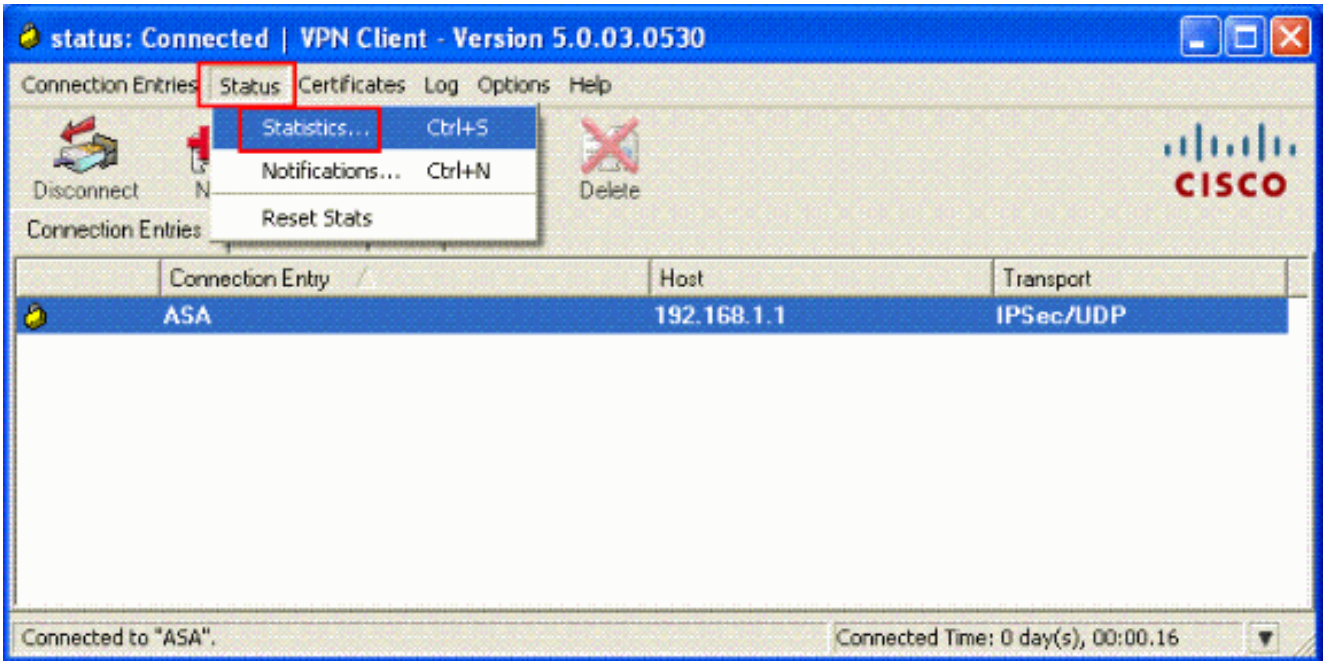


remota.

6. O cliente VPN é conectado com o ASA na instalação central.



7. Uma vez que a conexão é estabelecida com sucesso, selecione **estatísticas do** menu de status para verificar os detalhes do túnel.



Verificar

comandos show

Use esta seção para confirmar corretamente seus trabalhos da configuração.

A Output Interpreter Tool (apenas para clientes registrados) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

- show crypto isakmp sa – Mostra todas as associações de segurança (SAs) IKE atuais no correspondente.
- **mostre IPsec cripto sa** — Mostra os ajustes usados por SA atuais.

```
ASA #show crypto ipsec sa
interface: outside
    Crypto map tag: dynmap, seq num: 10, local addr: 192.168.1.1

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.5.1/255.255.255.255/0/0)
      current_peer: 192.168.1.2, username: cisco123
      dynamic allocated peer ip: 192.168.5.1

      #pkts encaps: 55, #pkts encrypt: 55, #pkts digest: 55
      #pkts decaps: 55, #pkts decrypt: 55, #pkts verify: 55
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 192.168.1.1, remote crypto endpt.: 192.168.1.2

      path mtu 1500, ipsec overhead 58, media mtu 1500
      current outbound spi: C2C25E2B

    inbound esp sas:
      spi: 0x69F8C639 (1777911353)
         transform: esp-des esp-md5-hmac none
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 40960, crypto-map: dynmap
         sa timing: remaining key lifetime (sec): 28337
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xC2C25E2B (3267517995)
         transform: esp-des esp-md5-hmac none
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 40960, crypto-map: dynmap
         sa timing: remaining key lifetime (sec): 28337
         IV size: 8 bytes
         replay detection support: Y

ASA #show crypto isakmp sa

   Active SA: 1
    Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1
```

```
1   IKE Peer: 192.168.1.2
    Type    : user            Role    : responder
    Rekey   : no              State   : AM_ACTIVE
```

Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração. O exemplo de debug é mostrado igualmente.

Nota: Para obter mais informações sobre do IPSec VPN do Acesso remoto do Troubleshooting consulte a maioria de IPSec VPN comum L2L e de Acesso remoto que pesquisa defeitos soluções

Cancele associações de segurança

Quando você pesquisa defeitos, certifique-se cancelar associações de segurança existentes depois que você faz uma mudança. No modo privilegiado do PIX, use estes comandos:

- **clear [crypto] ipsec sa** — Suprime do IPSec ativo SA. As palavras-chave crypto são opcionais.
- **clear [crypto] isakmp sa** — Suprime do IKE ativo SA. As palavras-chave crypto são opcionais.

Comandos para Troubleshooting

A Output Interpreter Tool (apenas para clientes registrados) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

Nota: Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos **debug**.

- **IPsec 7 do debug crypto** — Indica as negociações de IPSEC de fase 2.
- **isakmp 7 do debug crypto** — Indica as negociações de ISAKMP de fase 1.

Exemplo de debug

- ASA 8.0
- Cliente VPN 5.0 para Windows

ASA 8.0

```
ASA#debug crypto isakmp 7
Jan 22 22:21:24 [IKEv1]: IP = 192.168.1.2, IKE_DECODE RECEIVED Message
 (msgid=0) with payloads : HDR + SA (1) + KE (4) + NONCE (10) + ID (5) + VENDOR
(13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NONE (0) total le
ngth : 856
Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, processing SA payload
Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, processing ke payload
Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, processing ISA_KE payload
Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, processing nonce payload
Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, processing ID payload
Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, processing VID payload
```

```
Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, Received xauth V6 VID
Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, processing VID payload
Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, Received DPD VID
Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, processing VID payload
Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, Received Fragmentation VID
Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, IKE Peer included IKE fragmenta
tion capability flags:  Main Mode:        True  Aggressive Mode:  False
Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, processing VID payload
Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, Received NAT-Traversal ver 02 V
ID
Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, processing VID payload
Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, Received Cisco Unity client VID
Jan 22 22:21:24 [IKEv1]: IP = 192.168.1.2, Connection landed on tunnel_group Tun
nelGroup1
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, processin
g IKE SA payload
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, IKE SA Pr
oposal # 1, Transform # 13 acceptable  Matches global IKE entry # 2
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct
ing ISAKMP SA payload
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct
ing ke payload
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct
ing nonce payload
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, Generatin
g keys for Responder...
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct
ing ID payload
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct
ing hash payload
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, Computing
 hash for ISAKMP
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct
ing Cisco Unity VID payload
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct
ing xauth V6 VID payload
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct
ing dpd vid payload
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct
ing Fragmentation VID + extended capabilities payload
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct
ing VID payload
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, Send Alti
ga/Cisco VPN3000/Cisco ASA GW VID
Jan 22 22:21:24 [IKEv1]: IP = 192.168.1.2, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + SA (1) + KE (4) + NONCE (10) + ID (5) + HASH (8) + VENDOR
(13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NONE (0) total le
ngth : 368
Jan 22 22:21:24 [IKEv1]: IP = 192.168.1.2, IKE_DECODE RECEIVED Message (msgid=0)
 with payloads : HDR + HASH (8) + NOTIFY (11) + VENDOR (13) + VENDOR (13) + NONE
 (0) total length : 116
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, processin
g hash payload
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, Computing
 hash for ISAKMP
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, processin
g notify payload
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, processin
g VID payload
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, Processin
g IOS/PIX Vendor ID payload (version: 1.0.0, capabilities: 00000408)
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, processin
g VID payload
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, Received
```

```
Cisco Unity client VID
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct
ing blank hash payload
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct
ing qm hash payload
Jan 22 22:21:24 [IKEv1]: IP = 192.168.1.2, IKE_DECODE SENDING Message (msgid=e8a
1816d) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 68
Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE_DECODE RECEIVED Message (msgid=e8
a1816d) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 84
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, process_a
ttr(): Enter!
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, Processin
g MODE_CFG Reply attributes.
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, IKEGetUserAttributes: primary DNS = cleared
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, IKEGetUserAttributes: secondary DNS = cleared
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, IKEGetUserAttributes: primary WINS = cleared
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, IKEGetUserAttributes: secondary WINS = cleared
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, IKEGetUserAttributes: IP Compression = disabled
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, IKEGetUserAttributes: Split Tunneling Policy = Disabled
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, IKEGetUserAttributes: Browser Proxy Setting = no-modify
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, IKEGetUserAttributes: Browser Proxy Bypass Local = disable
Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168
.1.2, User (cisco123) authenticated.
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, constructing blank hash payload
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, constructing qm hash payload
Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE_DECODE SENDING Message (msgid=143
60de6) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 60
Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE_DECODE RECEIVED Message (msgid=14
360de6) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 56
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, process_attr(): Enter!
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, Processing cfg ACK attributes
Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE_DECODE RECEIVED Message (msgid=26
63a1dd) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 193
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, process_attr(): Enter!
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, Processing cfg Request attributes
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, MODE_CFG: Received request for IPV4 address!
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, MODE_CFG: Received request for IPV4 net mask!
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, MODE_CFG: Received request for DNS server address!
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, MODE_CFG: Received request for WINS server address!
Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168
.1.2, Received unsupported transaction mode attribute: 5
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, MODE_CFG: Received request for Banner!
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, MODE_CFG: Received request for Save PW setting!
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
```

92.168.1.2, MODE_CFG: Received request for Default Domain Name!
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, MODE_CFG: Received request for Split Tunnel List!
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, MODE_CFG: Received request for Split DNS!
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, MODE_CFG: Received request for PFS setting!
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, MODE_CFG: Received request for Client Browser Proxy Setting!
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, MODE_CFG: Received request for backup ip-sec peer list!
Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168
.1.2, Received unknown transaction mode attribute: 28684
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, MODE_CFG: Received request for Application Version!
Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168
.1.2, Client Type: WinNT Client Application Version: 5.0.03.0530
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, MODE_CFG: Received request for FWTYPE!
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, MODE_CFG: Received request for DHCP hostname for DDNS is: Wireless12
3!
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, MODE_CFG: Received request for UDP Port!
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, Obtained IP addr (192.168.5.1) prior to initiating Mode Cfg (XAuth e
nabled)
Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168
.1.2, Assigned private IP address 192.168.5.1 to remote user
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, constructing blank hash payload
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, Send Client Browser Proxy Attributes!
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, Browser Proxy set to No-Modify. Browser Proxy data will NOT be inclu
ded in the mode-cfg reply
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, constructing qm hash payload
Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE_DECODE SENDING Message (msgid=266
3a1dd) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 158
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, Delay Quick Mode processing, Cert/Trans Exch/RM DSID in progress
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, Resume Quick Mode processing, Cert/Trans Exch/RM DSID completed
Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168
.1.2, **PHASE 1 COMPLETED**
Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, Keep-alive type for this connection:
DPD
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, Starting P1 rekey timer: 950 seconds.
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, sending notify message
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, constructing blank hash payload
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, constructing qm hash payload
Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE_DECODE SENDING Message (msgid=f44
35669) with payloads : HDR + HASH (8) + NOTIFY (11) + NONE (0) total length : 84
Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE_DECODE RECEIVED Message (msgid=54
1f8e43) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) +
 NONE (0) total length : 1022
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, processing hash payload
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1

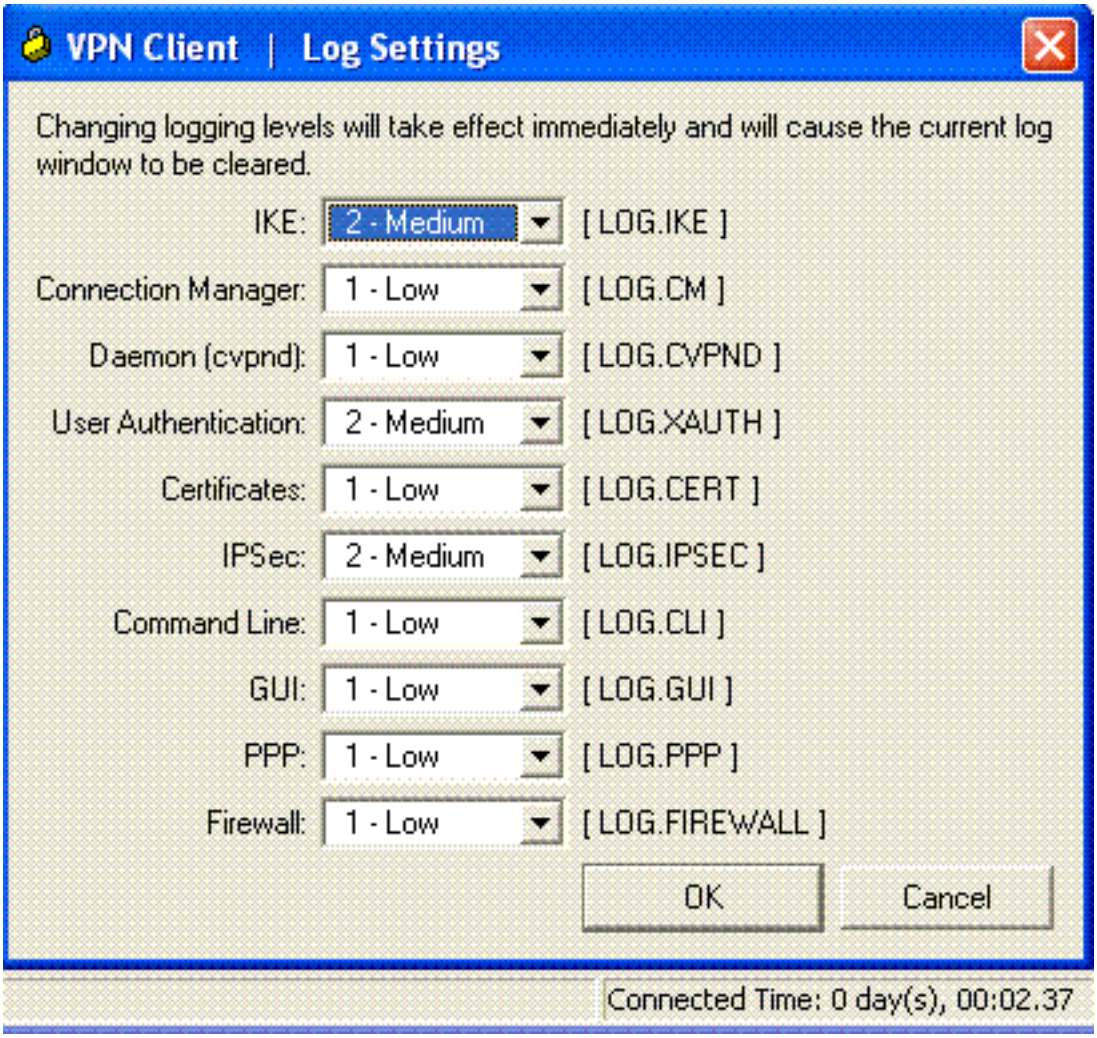
```
92.168.1.2, processing SA payload
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, processing nonce payload
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, processing ID payload
Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168
.1.2, Received remote Proxy Host data in ID Payload:  Address 192.168.5.1, Proto
col 0, Port 0
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, processing ID payload
Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168
.1.2, Received local IP Proxy Subnet data in ID Payload:   Address 0.0.0.0, Mask
 0.0.0.0, Protocol 0, Port 0
Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168
.1.2, QM IsRekeyed old sa not found by addr
Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168
.1.2, IKE Remote Peer configured for crypto map: dynmap
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, processing IPSec SA payload
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, IPSec SA Proposal # 14, Transform # 1 acceptable  Matches global IPS
ec SA entry # 10
Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168
.1.2, IKE: requesting SPI!
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, IKE got SPI from key engine: SPI = 0x31de01d8
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, oakley constucting quick mode
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, constructing blank hash payload
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, constructing IPSec SA payload
Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168
.1.2, Overriding Initiator's IPSec rekeying duration from 2147483 to 28800 secon
ds
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, constructing IPSec nonce payload
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, constructing proxy ID
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, Transmitting Proxy Id:
  Remote host: 192.168.5.1  Protocol 0  Port 0
  Local subnet:  0.0.0.0  mask 0.0.0.0 Protocol 0  Port 0
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, Sending RESPONDER LIFETIME notification to Initiator
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, constructing qm hash payload
Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE_DECODE SENDING Message (msgid=541
f8e43) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) +
NOTIFY (11) + NONE (0) total length : 176
Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE_DECODE RECEIVED Message (msgid=54
1f8e43) with payloads : HDR + HASH (8) + NONE (0) total length : 48
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, processing hash payload
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, loading all IPSEC SAs
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, Generating Quick Mode Key!
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, Generating Quick Mode Key!
Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168
.1.2, Security negotiation complete for User (cisco123)  Responder, Inbound SPI
= 0x31de01d8, Outbound SPI = 0x8b7597a9
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
```

```
92.168.1.2, IKE got a KEY_ADD msg for SA: SPI = 0x8b7597a9
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, Pitcher: received KEY_UPDATE, spi 0x31de01d8
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, Starting P2 rekey timer: 27360 seconds.
Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168
.1.2, Adding static route for client address: 192.168.5.1
Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168
.1.2, PHASE 2 COMPLETED (msgid=541f8e43)
Jan 22 22:21:41 [IKEv1]: IP = 192.168.1.2, IKE_DECODE RECEIVED Message (msgid=78
f7d3ae) with payloads : HDR + HASH (8) + NOTIFY (11) + NONE (0) total length : 8
0
```

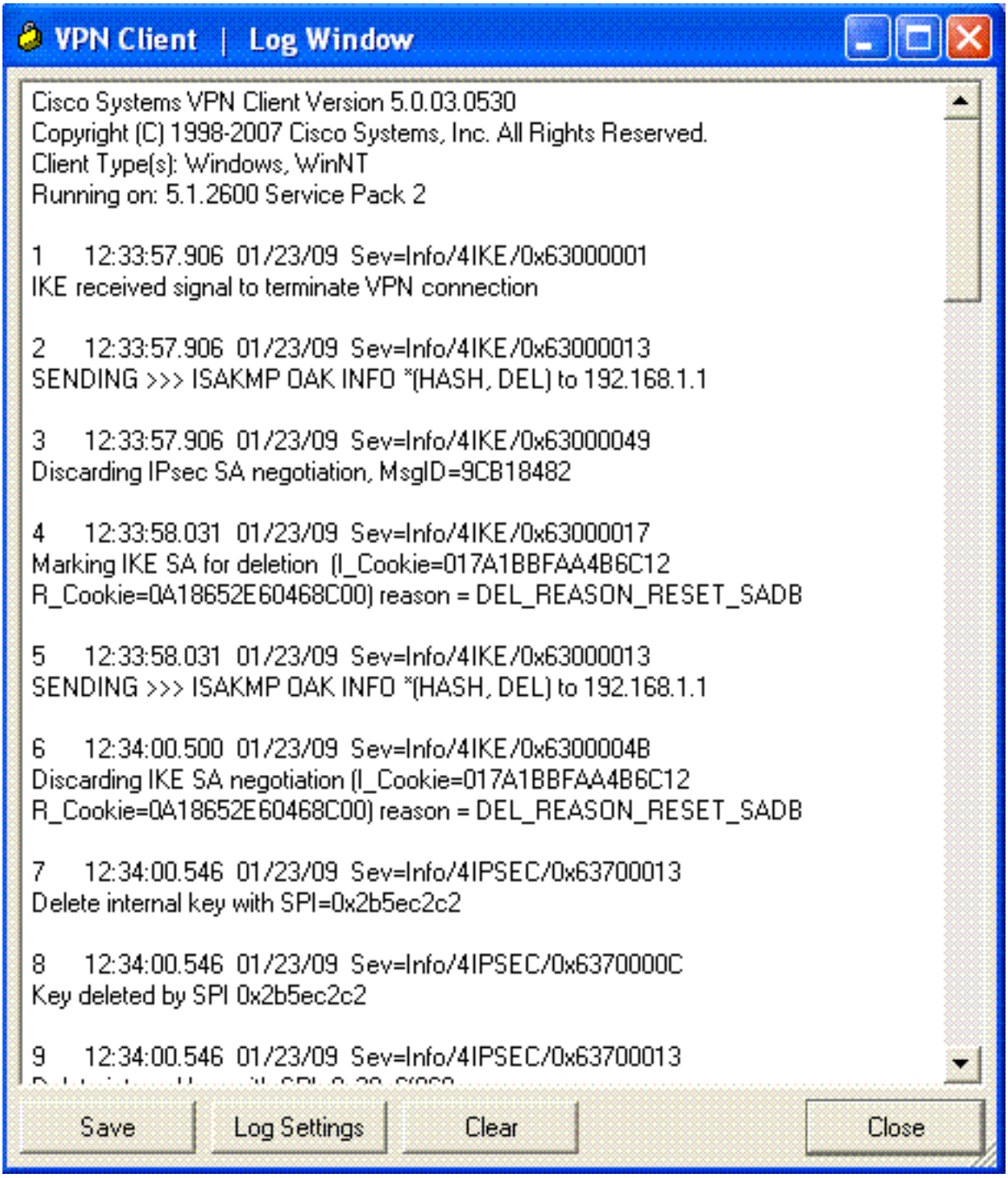
```
ASA#debug crypto ipsec 7

!--- Deletes the old SAs. ASA# IPSEC: Deleted inbound decrypt rule, SPI 0x7F3C985A Rule ID:
0xD5567DB0 IPSEC: Deleted inbound permit rule, SPI 0x7F3C985A Rule ID: 0xD4EF1DF0 IPSEC: Deleted
inbound tunnel flow rule, SPI 0x7F3C985A Rule ID: 0xD556AF60 IPSEC: Deleted inbound VPN context,
SPI 0x7F3C985A VPN handle: 0x0004678C IPSEC: Deleted outbound encrypt rule, SPI 0xC921E280 Rule
ID: 0xD517EE30 IPSEC: Deleted outbound permit rule, SPI 0xC921E280 Rule ID: 0xD5123250 IPSEC:
Deleted outbound VPN context, SPI 0xC921E280 VPN handle: 0x00040AB4 !--- Creates new SAs. ASA#
IPSEC: New embryonic SA created @ 0xD4EF2390, SCB: 0xD4EF22C0, Direction: inbound SPI :
0x7F3C985A Session ID: 0x0000F000 VPIF num : 0x00000002 Tunnel type: ra Protocol : esp Lifetime
: 240 seconds IPSEC: New embryonic SA created @ 0xD556B118, SCB: 0xD556B048, Direction: outbound
SPI : 0xC921E280 Session ID: 0x0000F000 VPIF num : 0x00000002 Tunnel type: ra Protocol : esp
Lifetime : 240 seconds IPSEC: Completed host OBSA update, SPI 0xC921E280 IPSEC: Creating
outbound VPN context, SPI 0xC921E280 Flags: 0x00000005 SA : 0xD556B118 SPI : 0xC921E280 MTU :
1500 bytes VCID : 0x00000000 Peer : 0x00000000 SCB : 0x0133B741 Channel: 0xD4160FA8 IPSEC:
Completed outbound VPN context, SPI 0xC921E280 VPN handle: 0x00040AB4 IPSEC: New outbound
encrypt rule, SPI 0xC921E280 Src addr: 0.0.0.0 Src mask: 0.0.0.0 Dst addr: 192.168.5.1 Dst mask:
255.255.255.255 Src ports Upper: 0 Lower: 0 Op : ignore Dst ports Upper: 0 Lower: 0 Op : ignore
Protocol: 0 Use protocol: false SPI: 0x00000000 Use SPI: false IPSEC: Completed outbound encrypt
rule, SPI 0xC921E280 Rule ID: 0xD517EE30 IPSEC: New outbound permit rule, SPI 0xC921E280 Src
addr: 192.168.1.1 Src mask: 255.255.255.255 Dst addr: 192.168.1.2 Dst mask: 255.255.255.255 Src
ports Upper: 0 Lower: 0 Op : ignore Dst ports Upper: 0 Lower: 0 Op : ignore Protocol: 50 Use
protocol: true SPI: 0xC921E280 Use SPI: true IPSEC: Completed outbound permit rule, SPI
0xC921E280 Rule ID: 0xD5123250 IPSEC: Completed host IBSA update, SPI 0x7F3C985A IPSEC: Creating
inbound VPN context, SPI 0x7F3C985A Flags: 0x00000006 SA : 0xD4EF2390 SPI : 0x7F3C985A MTU : 0
bytes VCID : 0x00000000 Peer : 0x00040AB4 SCB : 0x0132B2C3 Channel: 0xD4160FA8 IPSEC: Completed
inbound VPN context, SPI 0x7F3C985A VPN handle: 0x0004678C IPSEC: Updating outbound VPN context
0x00040AB4, SPI 0xC921E280 Flags: 0x00000005 SA : 0xD556B118 SPI : 0xC921E280 MTU : 1500 bytes
VCID : 0x00000000 Peer : 0x0004678C SCB : 0x0133B741 Channel: 0xD4160FA8 IPSEC: Completed
outbound VPN context, SPI 0xC921E280 VPN handle: 0x00040AB4 IPSEC: Completed outbound inner
rule, SPI 0xC921E280 Rule ID: 0xD517EE30 IPSEC: Completed outbound outer SPD rule, SPI
0xC921E280 Rule ID: 0xD5123250 IPSEC: New inbound tunnel flow rule, SPI 0x7F3C985A Src addr:
192.168.5.1 Src mask: 255.255.255.255 Dst addr: 0.0.0.0 Dst mask: 0.0.0.0 Src ports Upper: 0
Lower: 0 Op : ignore Dst ports Upper: 0 Lower: 0 Op : ignore Protocol: 0 Use protocol: false
SPI: 0x00000000 Use SPI: false IPSEC: Completed inbound tunnel flow rule, SPI 0x7F3C985A Rule
ID: 0xD556AF60 IPSEC: New inbound decrypt rule, SPI 0x7F3C985A Src addr: 192.168.1.2 Src mask:
255.255.255.255 Dst addr: 192.168.1.1 Dst mask: 255.255.255.255 Src ports Upper: 0 Lower: 0 Op :
ignore Dst ports Upper: 0 Lower: 0 Op : ignore Protocol: 50 Use protocol: true SPI: 0x7F3C985A
Use SPI: true IPSEC: Completed inbound decrypt rule, SPI 0x7F3C985A Rule ID: 0xD5567DB0 IPSEC:
New inbound permit rule, SPI 0x7F3C985A Src addr: 192.168.1.2 Src mask: 255.255.255.255 Dst
addr: 192.168.1.1 Dst mask: 255.255.255.255 Src ports Upper: 0 Lower: 0 Op : ignore Dst ports
Upper: 0 Lower: 0 Op : ignore Protocol: 50 Use protocol: true SPI: 0x7F3C985A Use SPI: true
IPSEC: Completed inbound permit rule, SPI 0x7F3C985A Rule ID: 0xD4EF1DF0
```

Cliente VPN 5.0 para Windows

Selecione o **log > as configurações de registro** para permitir os níveis do log no cliente VPN.



Selecione o **log > o indicador do log** para ver as entradas de registro no cliente VPN.



Informações Relacionadas

- Página de Suporte dos Cisco ASA 5500 Series Adaptive Security Appliances
- Referências de comandos do Dispositivos de segurança adaptáveis Cisco ASA série 5500
- Página de Suporte dos Cisco PIX 500 Series Security Appliances
- Referência de comandos do Dispositivos de segurança Cisco PIX série 500
- Cisco Adaptive Security Device Manager
- Página de Suporte de Negociação IPSec/Protocolos IKE