

# ASA/PIX: Cliente del IPSec VPN que dirige usando el servidor DHCP con el ejemplo de la Configuración de ASDM

## Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Productos Relacionados](#)

[Convenciones](#)

[Antecedentes](#)

[Configurar](#)

[Diagrama de la red](#)

[VPN de acceso remoto de la configuración \(IPSec\)](#)

[Configure ASA/PIX usando el CLI](#)

[Configuración de Cliente Cisco VPN](#)

[Verificación](#)

[Comandos show](#)

[Troubleshooting](#)

[Borre las asociaciones de seguridad](#)

[Comandos para resolución de problemas](#)

[Ejemplo de resultado del comando debug](#)

[Información Relacionada](#)

## [Introducción](#)

Este documento describe cómo configurar Cisco 5500 Series Adaptive Security Appliance (ASA) para hacer que el servidor DHCP proporcione la dirección IP del cliente a todos los clientes VPN que usan Adaptive Security Device Manager (ASDM) o la CLI. El ASDM ofrece administración de seguridad de talla mundial y monitoreo a través de una Interfaz de administración basada en la Web intuitiva, fácil de utilizar. Una vez que la configuración de Cisco ASA es completa, puede ser verificada usando el Cisco VPN Client.

Consulte el Ejemplo de Configuración de Autenticación [PIX/ASA 7.x y Cisco VPN Client 4.x con Windows 2003 IAS RADIUS \(en comparación con Active Directory\)](#) para instalar la conexión VPN de acceso remoto entre Cisco VPN Client (4.x para Windows) y PIX 500 Series Security Appliance 7.x. El usuario remoto de VPN Client se autentica contra el Active Directory usando un servidor RADIUS de Internet Authentication Service de Microsoft Windows 2003 (IAS).

Consulte el Ejemplo de Configuración de Autenticación de [PIX/ASA 7.x y al Cisco VPN Client 4.x](#)

[para Cisco Secure ACS](#) para configurar una conexión VPN de acceso remoto entre un Cisco VPN Client (4.x para Windows) y el PIX 500 Series Security Appliance 7.x usando un Cisco Secure Access Control Server (ACS versión 3.2) para la autenticación ampliada (Xauth).

## prerrequisitos

### Requisitos

Este documento asume que el ASA está completamente operativo y está configurado para permitir que el ASDM de Cisco o el CLI realice los cambios de configuración.

**Nota:** Consulte [Cómo Permitir el Acceso HTTPS para el ASDM](#) o el [PIX/ASA 7.x: SSH en el Ejemplo de Configuración de las Interfaces Interiores y Exteriores](#) para permitir que el dispositivo sea configurado remotamente por el ASDM o el Secure Shell (SSH).

### Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco Adaptive Security Appliance Software Version 7.x y posterior
- Adaptive Security Device Manager Version 5.x y posterior
- Cisco VPN Client Version 4.x y posterior

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

### Productos Relacionados

Esta configuración también se puede usar con Cisco PIX Security Appliance Version 7.x y posterior.

### Convenciones

Consulte [Convenciones de Consejos Técnicos Cisco](#) para obtener más información sobre las convenciones del documento.

## Antecedentes

Los VPN de accesos remotos dirigen el requisito del equipo de trabajo móvil de conectar con seguridad con la red de la organización. Los usuarios ambulantes pueden configurar una conexión segura usando el software cliente VPN instalado en sus PC. El cliente VPN inicia una conexión a un dispositivo del sitio central configurado para validar estas peticiones. En este ejemplo, el dispositivo del sitio central es un dispositivo de seguridad adaptante de las 5500 Series ASA que utiliza las correspondencias cifradas dinámicas.

En administración de direcciones del dispositivo de seguridad tenemos que configurar los IP Addresses que conectan a un cliente con un recurso en la red privada, a través del túnel, y dejan

al cliente funcionar como si fuera conectado directamente con la red privada. Además, nos estamos ocupando solamente de los IP Address privados que consiguen asignados a los clientes. Los IP Addresses asignados a otros recursos en su red privada son parte de sus responsabilidades de la Administración de red, no Administración de VPN de la parte de. Por lo tanto, cuando los IP Addresses se discuten aquí, significamos esos IP Addresses disponibles en su esquema de direccionamiento de la red privada que deje al cliente funcionar como un punto final del túnel.

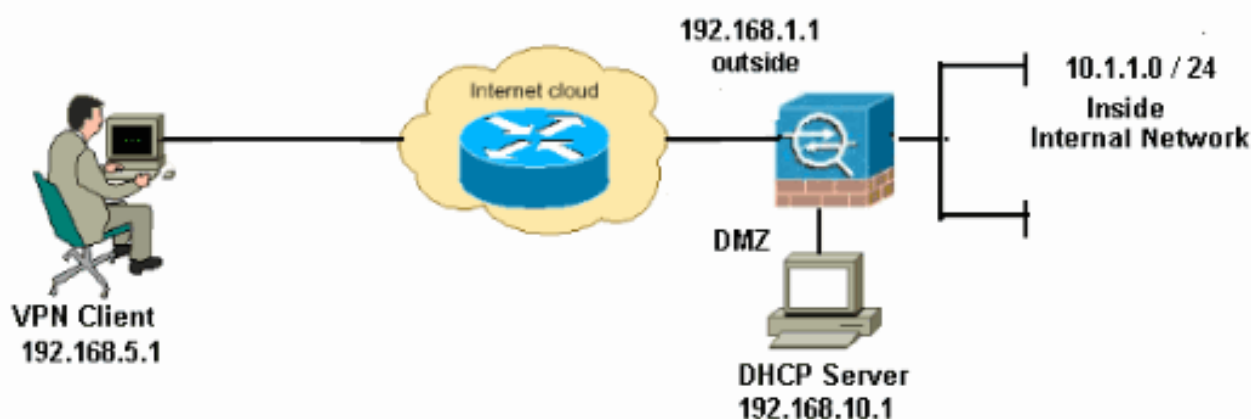
## Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

**Nota:** Use la [Command Lookup Tool \(clientes registrados solamente\)](#) para obtener más información sobre los comandos usados en esta sección.

## Diagrama de la red

En este documento, se utiliza esta configuración de red:



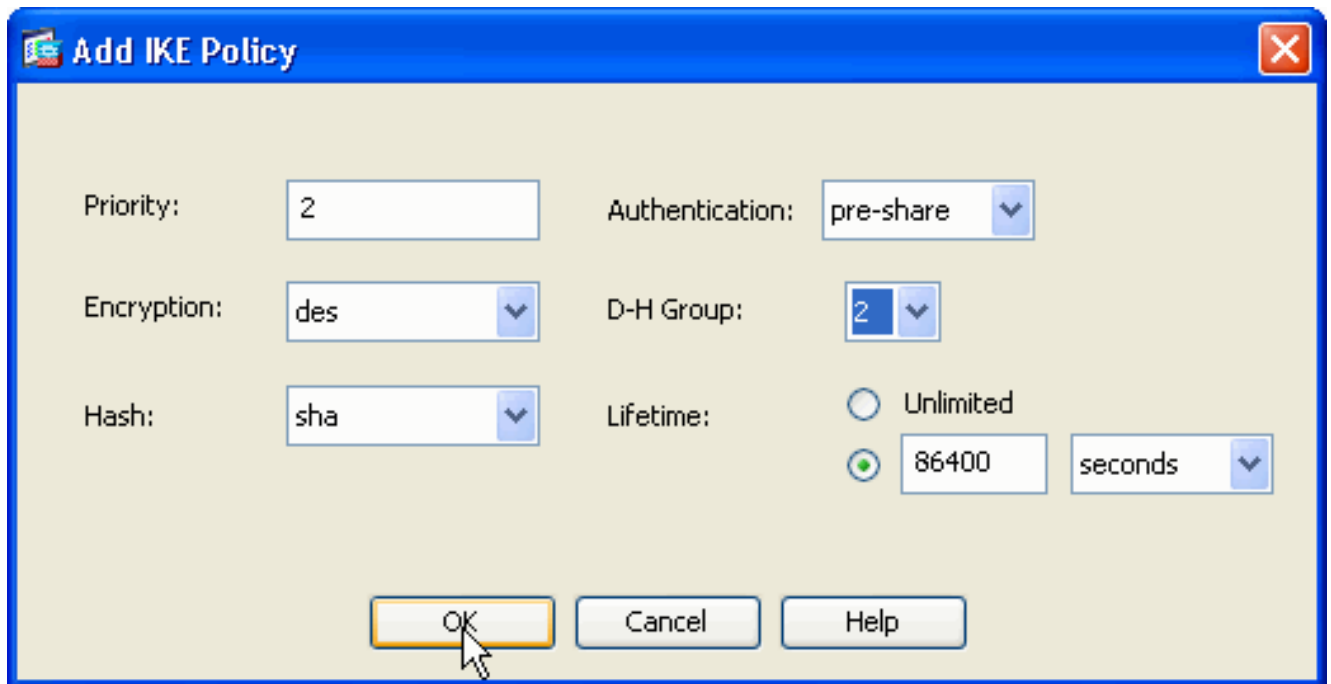
**Nota:** Los esquemas de direccionamiento IP usados en esta configuración no son legalmente enrutables en Internet. Son las direcciones RFC1918 que fueron utilizadas en un entorno de laboratorio.

## VPN de acceso remoto de la configuración (IPSec)

### Procedimiento del ASDM

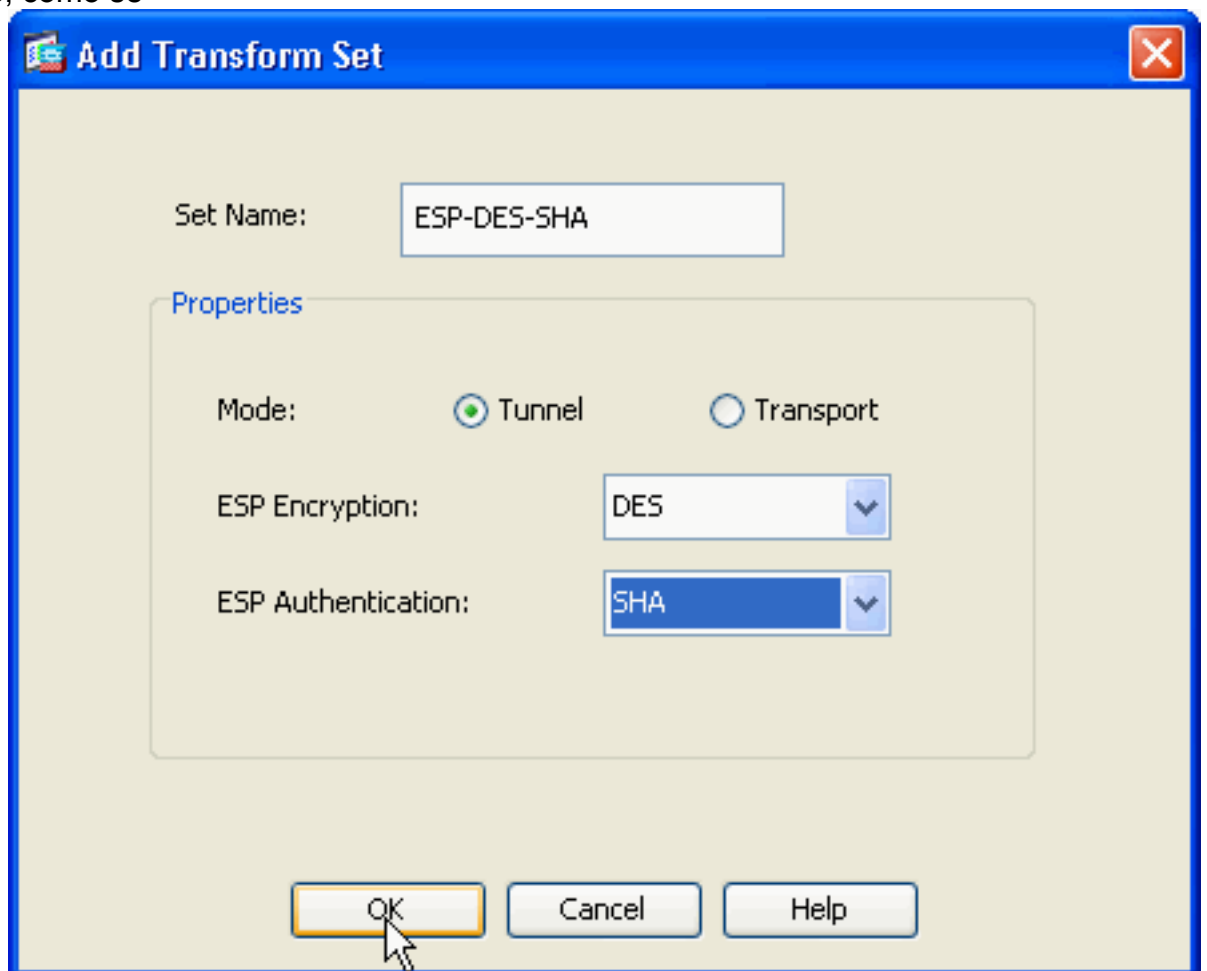
Complete estos pasos para configurar el VPN de acceso remoto:

1. Elija la configuración > el acceso del VPN de acceso remoto > de la red (cliente) > avanzó > IPSec > las políticas IKE > Add para crear una política isakmp 2, como se muestra.



El Haga Click en OK y se aplica.

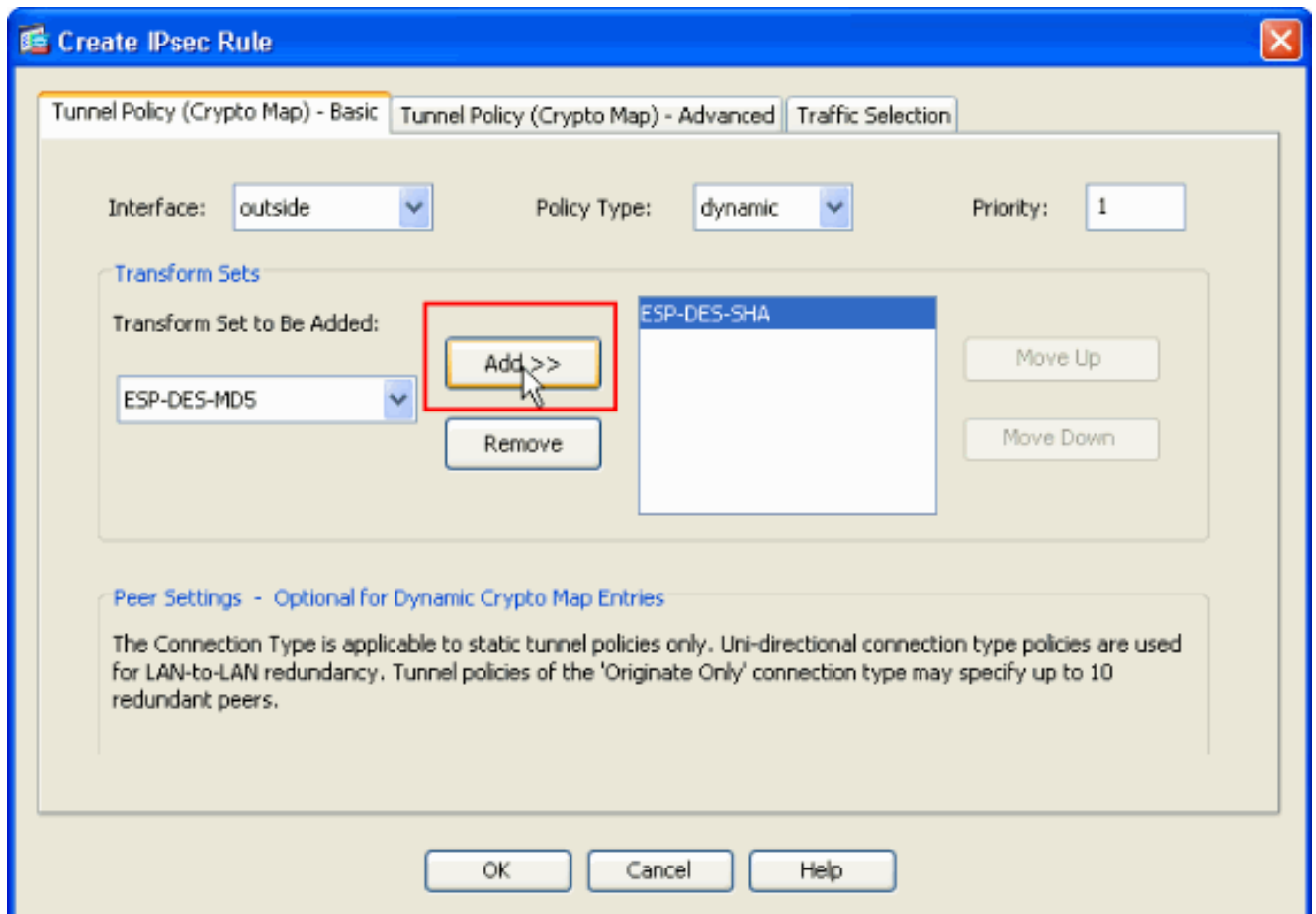
2. Elija la configuración > el acceso del VPN de acceso remoto > de la red (cliente) > avanzó > IPsec > IPsec transforman los conjuntos > Add para crear el ESP-DES-SHA transforman el conjunto, como se



muestra.

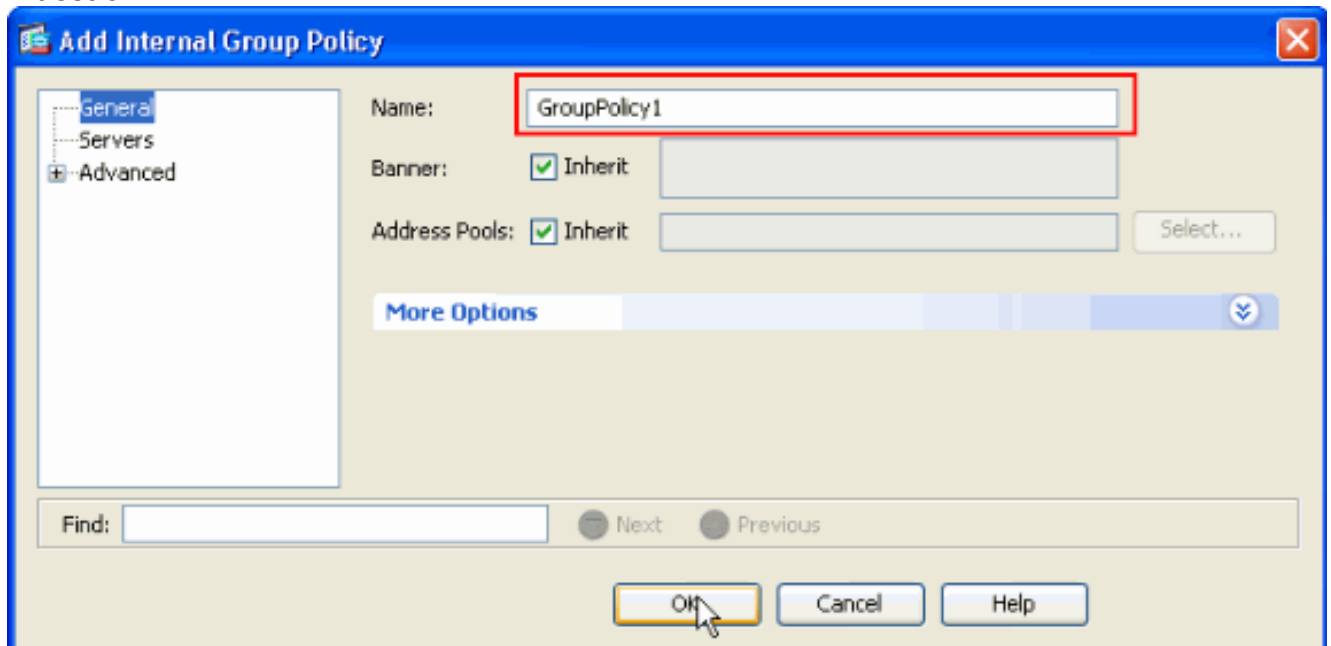
El Haga Click en OK y se aplica.

3. Elija la configuración > el acceso del VPN de acceso remoto > de la red (cliente) > avanzó > IPsec > las correspondencias de criptografía > Add para crear una correspondencia de criptografía con la directiva dinámica de la prioridad 1, como se muestra.



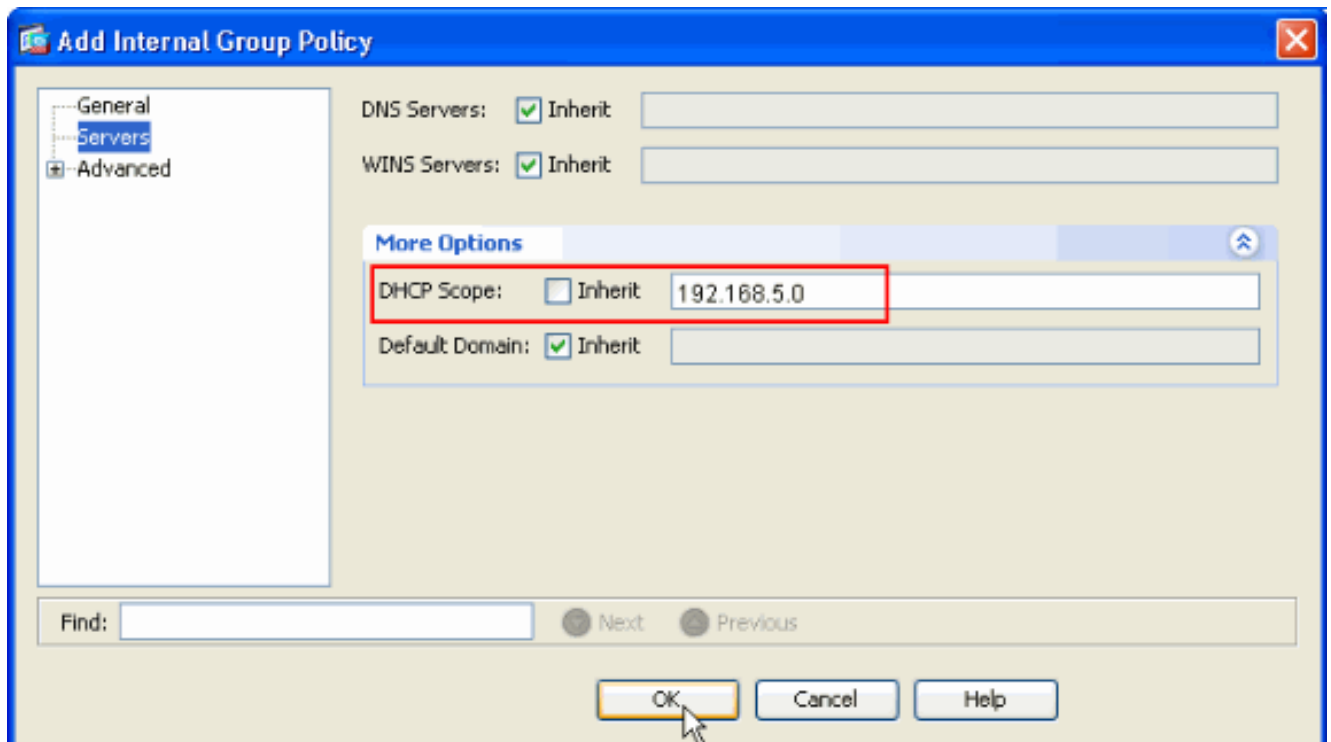
El Haga Click en OK y se aplica.

4. Elija la configuración > el acceso del VPN de acceso remoto > de la red (cliente) > avanzó > las directivas del grupo > las directivas del grupo de Add>Internal para crear una directiva del grupo (por ejemplo GroupPloicy1), como se muestra.



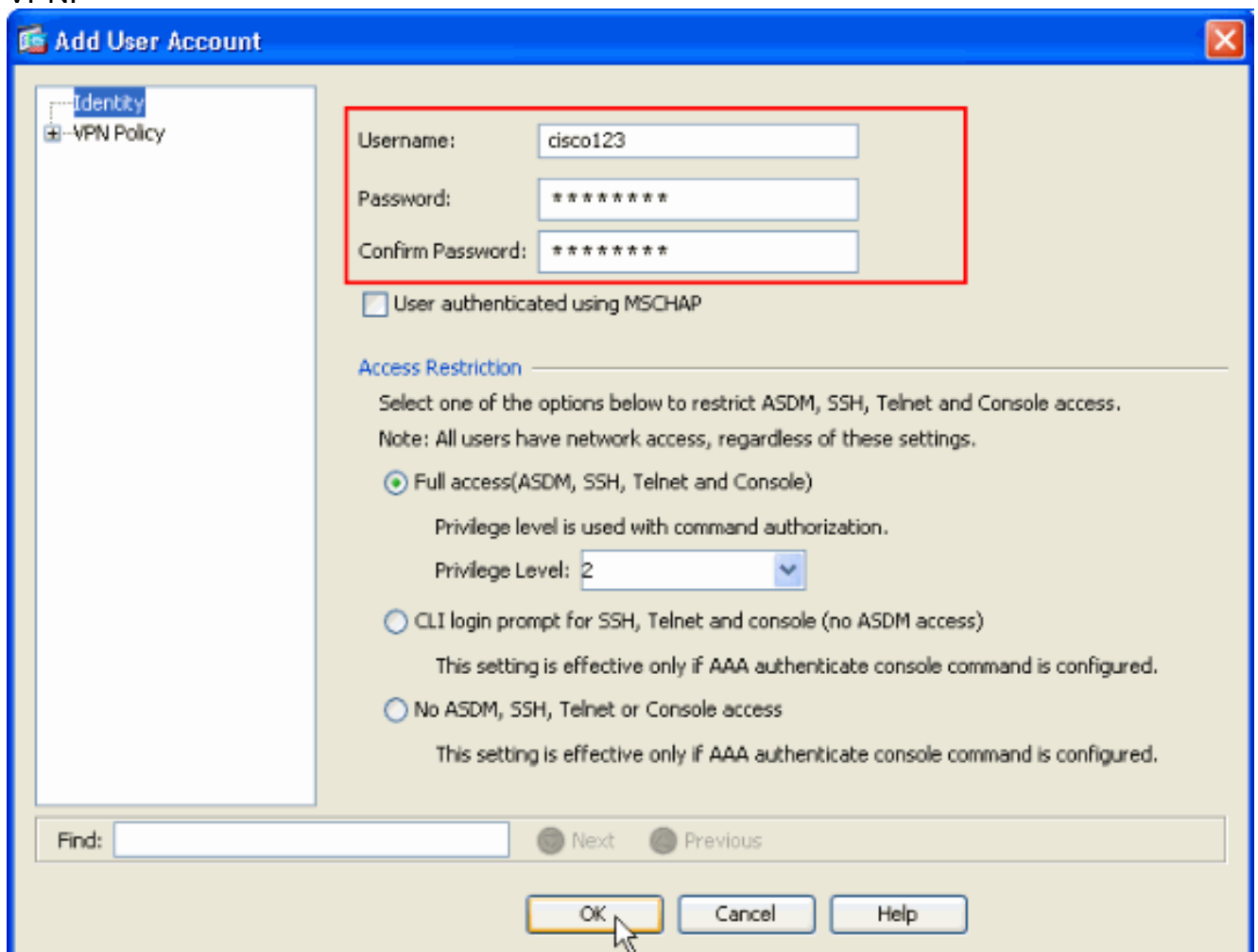
El Haga Click en OK y se aplica.

5. Elija la configuración > el acceso del VPN de acceso remoto > de la red (cliente) > avanzó > las directivas del grupo > grupo Policies>Servers>> de Add>Internal para configurar el alcance de DHCP para que los usuarios de cliente VPN sean asignados dinámicamente.



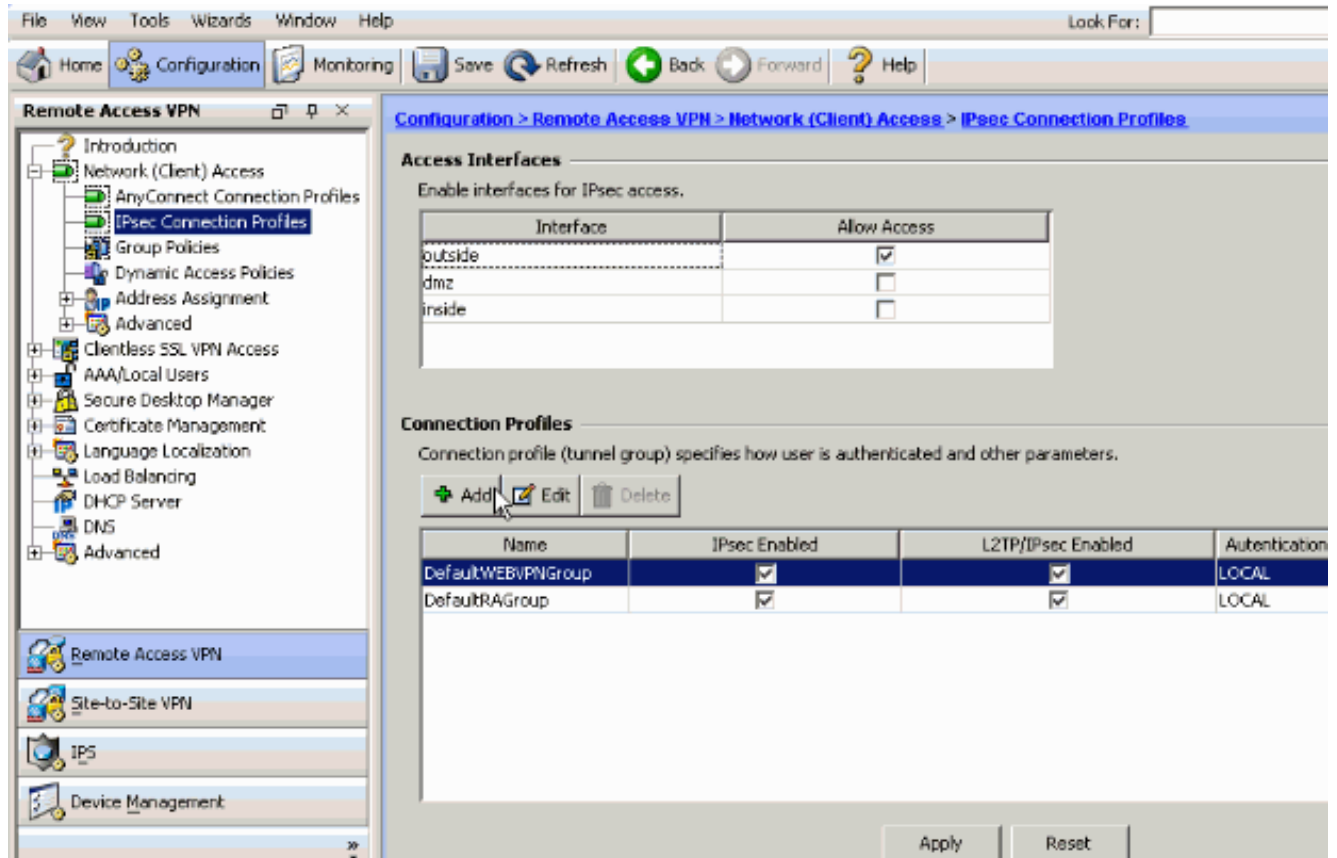
El Haga Click en OK y se aplica. **Nota:** La configuración del alcance de DHCP es opcional. Refiera a [configurar el direccionamiento DHCP](#) para más información.

6. Elija la configuración > el VPN de acceso remoto > AAA ponen > los usuarios locales > Add para crear la cuenta de usuario (por ejemplo, nombre de usuario - cisco123 y contraseña - cisco123) para el acceso de cliente VPN.

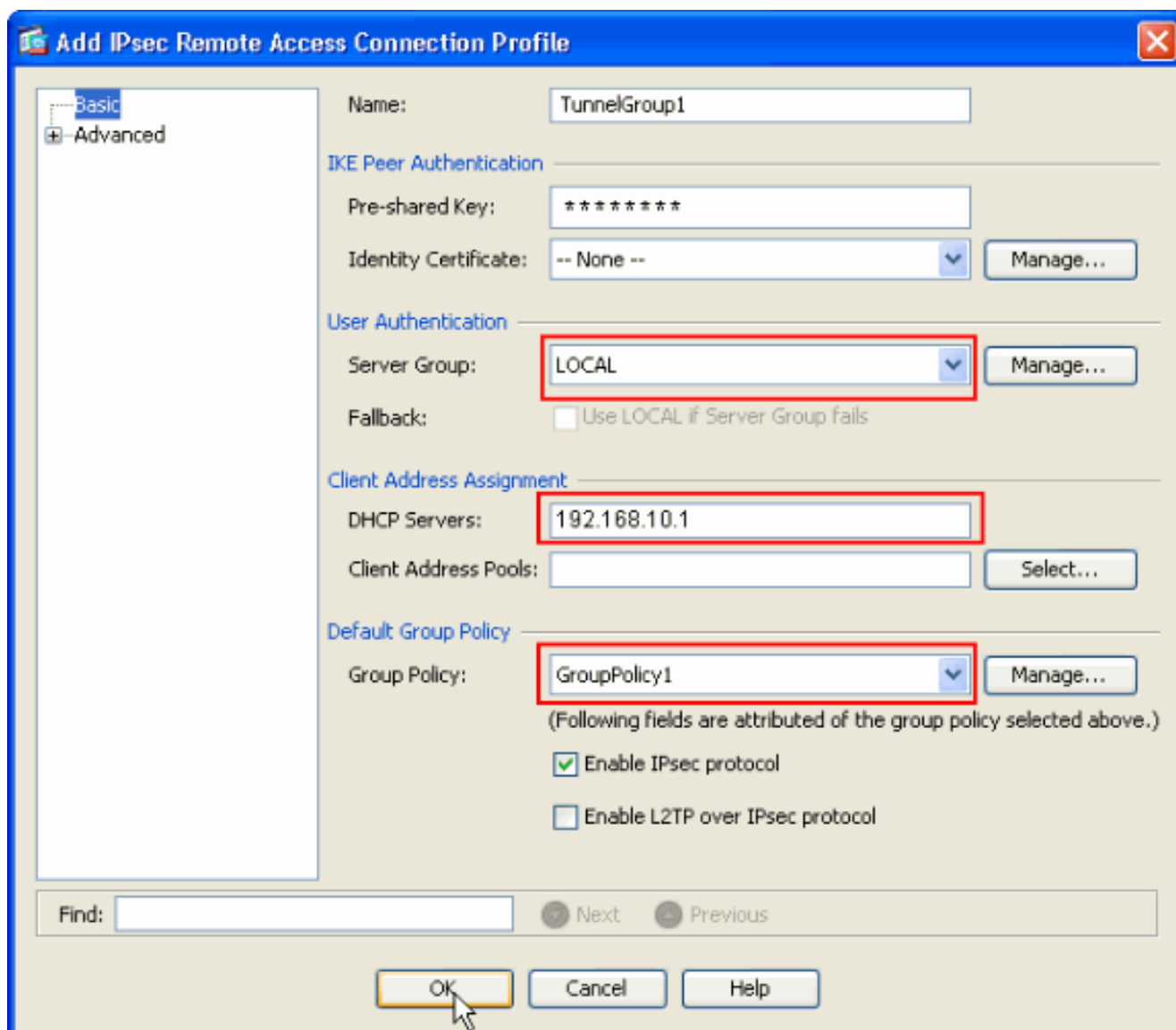


7. Elija la configuración > el acceso del VPN de acceso remoto > de la red (cliente) > conexión

**IPSec los perfiles > Add>** para agregar a un grupo de túnel (por ejemplo, **TunnelGroup1** y el preshared cierran como **cisco123**), como se muestra.



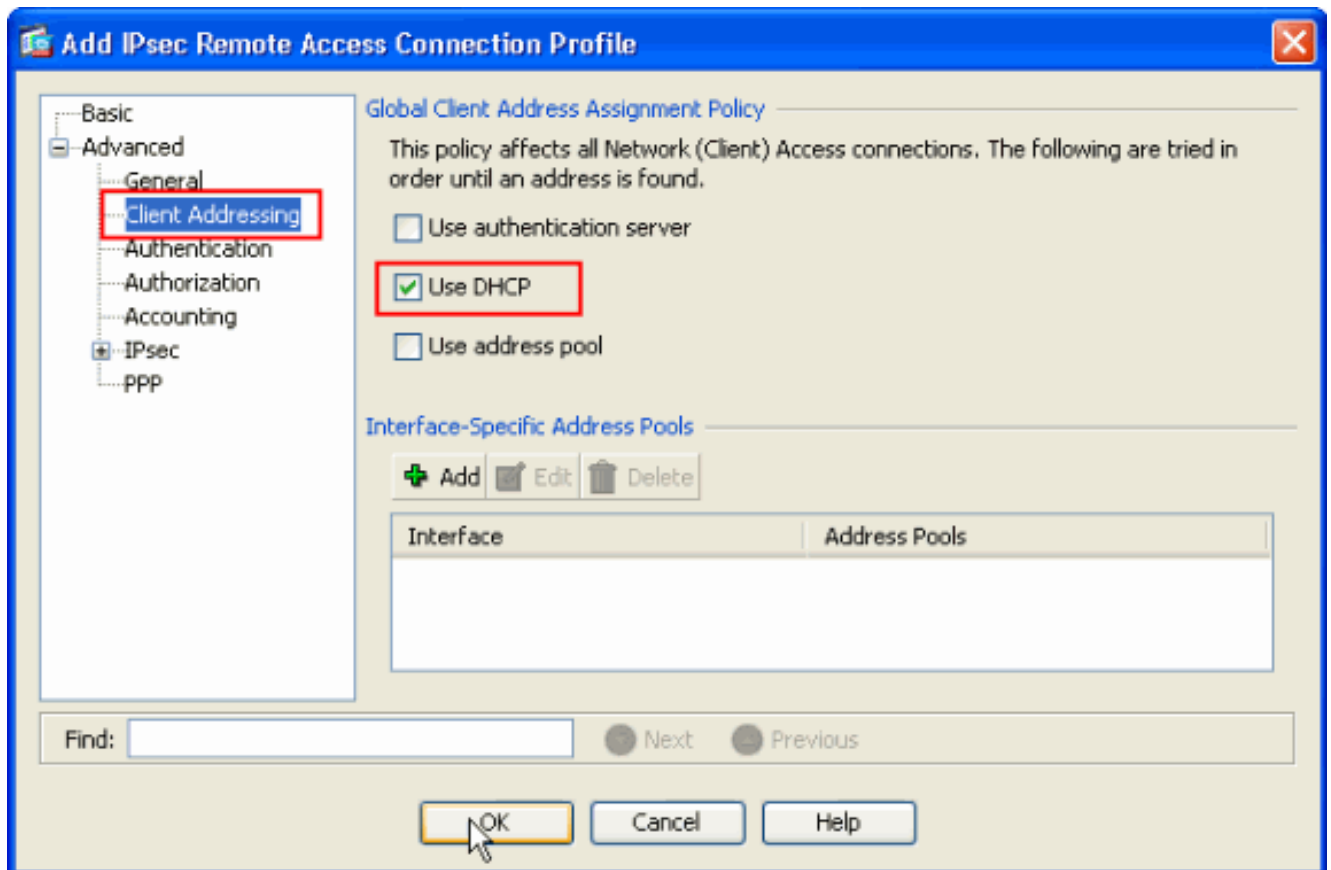
Bajo lengüeta **básica** elija al grupo de servidores como **LOCAL** para el campo de la autenticación de usuario. Elija **Grouppolicy1** como la directiva del grupo para el campo de la directiva del grupo predeterminado. Proporcione el IP Address del servidor DHCP en el espacio proporcionado para los **servidores DHCP**.



Click OK.

8. Elija **avanzado > cliente que dirige >** y marque el checkbox del **DHCP del uso** para que el servidor DHCP asigne la dirección IP a los clientes VPN. **Nota:** Asegurese desmarcar las casillas de verificación para el **servidor de autenticación del uso** y utilizar a la **agrupación de direcciones**.





### Configuración para el ASDM 6.x

La misma Configuración de ASDM trabaja muy bien con la versión 6.x del ASDM, a excepción de algunas modificaciones menores en términos de trayectorias del ASDM. Las trayectorias del ASDM a ciertos campos tenían una variación de la versión 6.2 y posterior del ASDM. Las modificaciones junto con los trayectos existentes son mencionadas abajo. Aquí las imágenes gráficas no se asocian en los casos donde siguen siendo lo mismo para todas las versiones importantes del ASDM.

1. La configuración > el acceso del VPN de acceso remoto > de la red (cliente) > avanzaron > IPsec > las políticas IKE > Add
2. La configuración > el acceso del VPN de acceso remoto > de la red (cliente) > avanzaron > IPsec > IPsec transforman los conjuntos > Add
3. La configuración > el acceso del VPN de acceso remoto > de la red (cliente) > avanzaron > IPsec > las correspondencias de criptografía > Add
4. Elija la configuración > el VPN de acceso remoto > las directivas del acceso > del grupo de la red (cliente) > Add > los Internal group policyes (política grupal interna)
5. Elija la configuración > el VPN de acceso remoto > las directivas > los servidores del grupo del >Internal de las directivas del acceso > del grupo de la red (cliente) > Add
6. Elija la configuración > el VPN de acceso remoto > AAA ponen/los usuarios locales > los usuarios locales > Add
7. La configuración > el acceso del VPN de acceso remoto > de la red (cliente) > conexión IPsec perfila > Add
8. Elija la configuración > el VPN de acceso remoto > directiva del acceso > de la asignación de dirección > de la asignación de la red (cliente)

For VPN address assignment, the following options are tried in order, until an address is found.

- Use authentication server
- Use DHCP
- Use internal address pools

Parameter only applies to full-tunnel IPSec and SSL VPN clients, and not Clientless SSL VPN.

Todas estas tres opciones se habilitan por abandono. Cisco ASA sigue la misma orden para asignar los direccionamientos a los clientes VPN. Cuando usted desmarca las otras dos opciones, Cisco ASA no verifica las opciones del servidor y de la agrupación local aaa. Las opciones habilitadas predeterminadas se pueden verificar por la **demostración funcionan con todos | en VPN-agregue el comando**. Esto es una salida de muestra para su referencia:

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

Para más información sobre este comando, refiérase VPN-addr-[asignan](#).

## [Configure ASA/PIX usando el CLI](#)

Complete estos pasos para configurar al servidor DHCP para proporcionar la dirección IP a los clientes VPN de la línea de comando. Consulte [Configuración de VPN de Acceso Remoto](#) o Referencias de Comandos de [Cisco ASA 5500 Series Adaptive Security Appliance](#) para obtener más información sobre cada uno de los comandos.

### Configuración que se está ejecutando en el 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

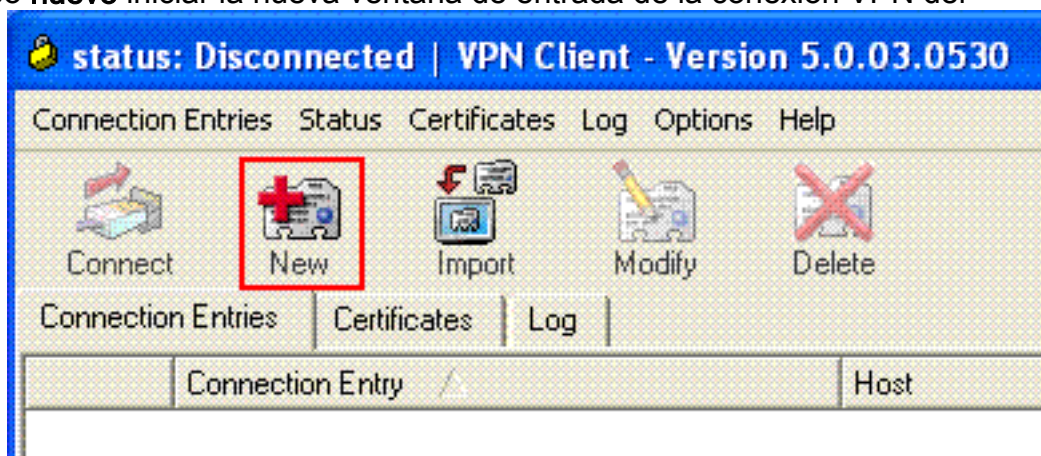
!--- Enter the pre-shared-key to configure the
authentication method. tunnel-group TunnelGroup1 ipsec-
attributes pre-shared-key * prompt hostname context
Cryptochecksum:e0725ca9ccc28af488ded9ee36b7822d : end
ASA#

```

## Configuración de Cliente Cisco VPN

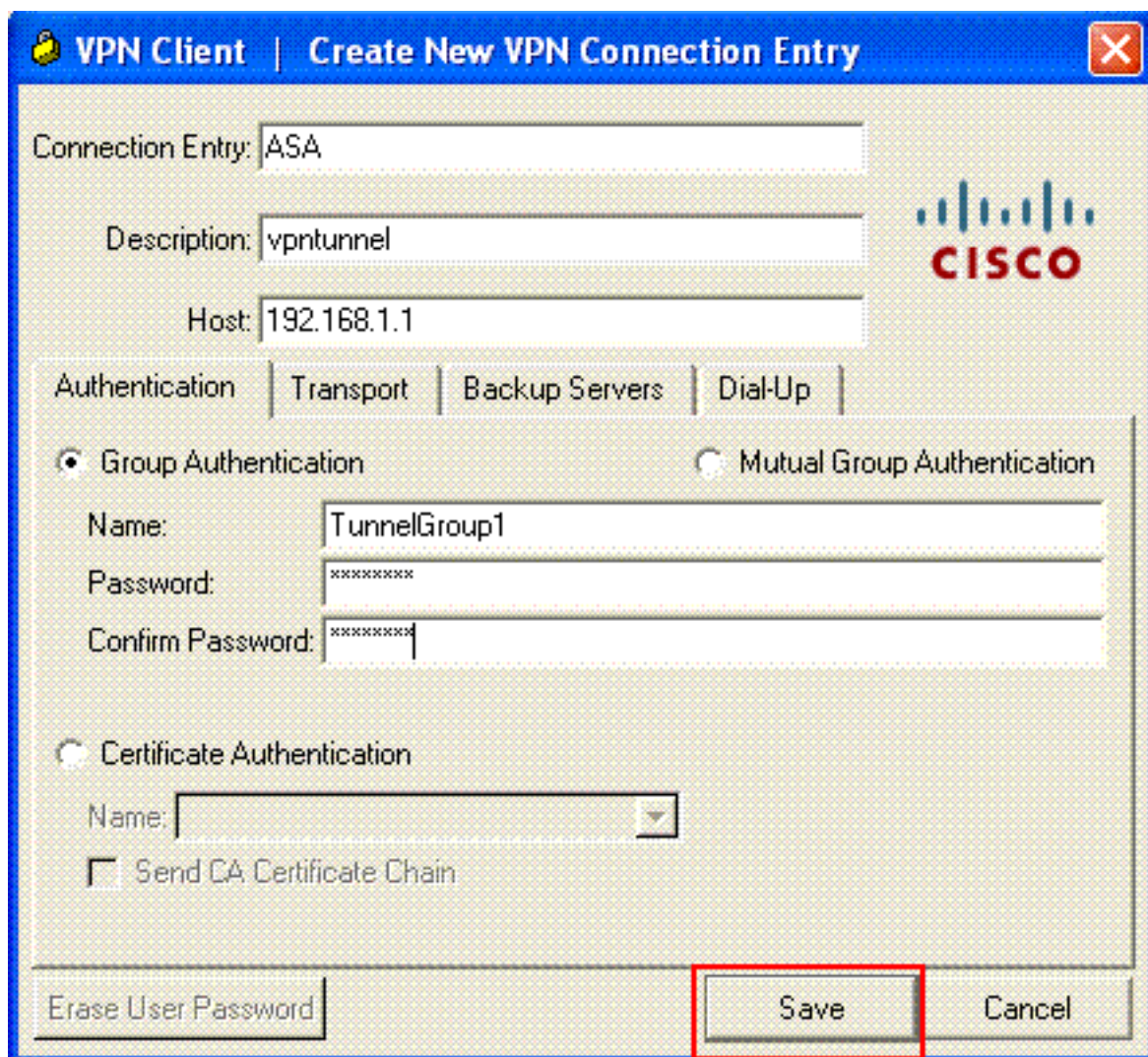
Intente conectarse con Cisco ASA usando el Cisco VPN Client para verificar que el ASA esté configurado con éxito.

1. Seleccione el **Start (Inicio) > Programs (Programas) > Cisco Systems VPN Client (VPN Client de Cisco Systems) > al cliente VPN.**
2. Tecleo **nuevo** iniciar la nueva ventana de entrada de la conexión VPN del



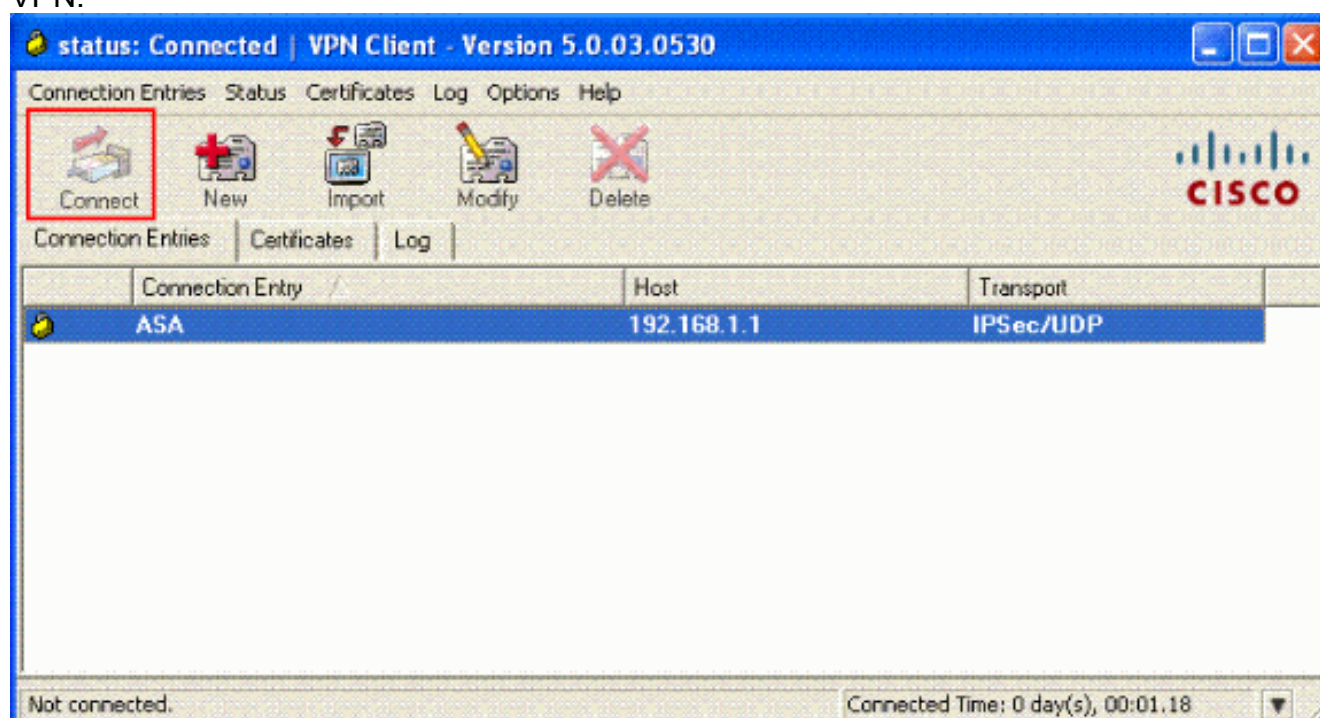
crear.

3. Complete la información de su nueva conexión. Ingrese el nombre del Entrada de conexión junto con una descripción. Ingrese el **IP Address externo del ASA** en el rectángulo del host. Entonces ingrese el grupo de túnel VPN name(TunnelGroup1) y la contraseña (clave previamente compartida - cisco123) como está configurado en el ASA. Click



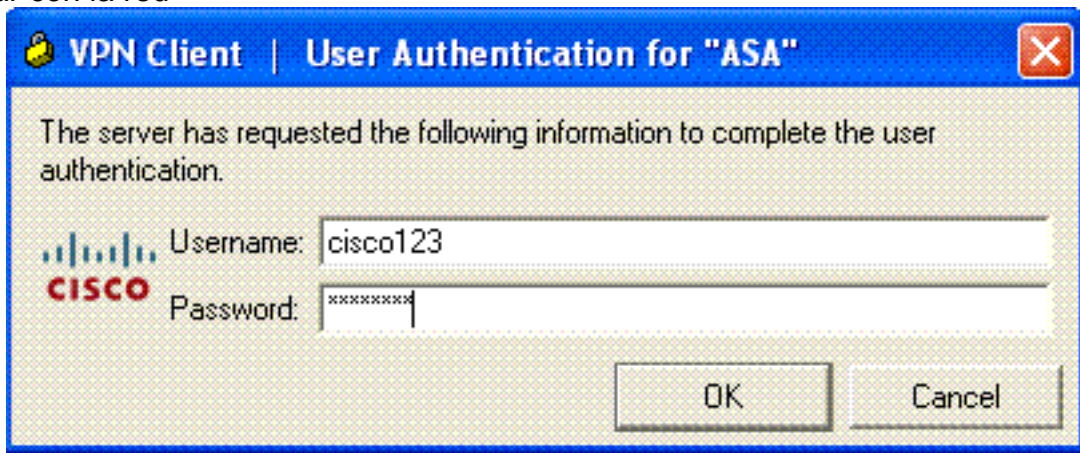
Save.

- Haga clic en la conexión que usted quiere utilizar y el tecleo **conecta de la ventana principal del cliente VPN.**



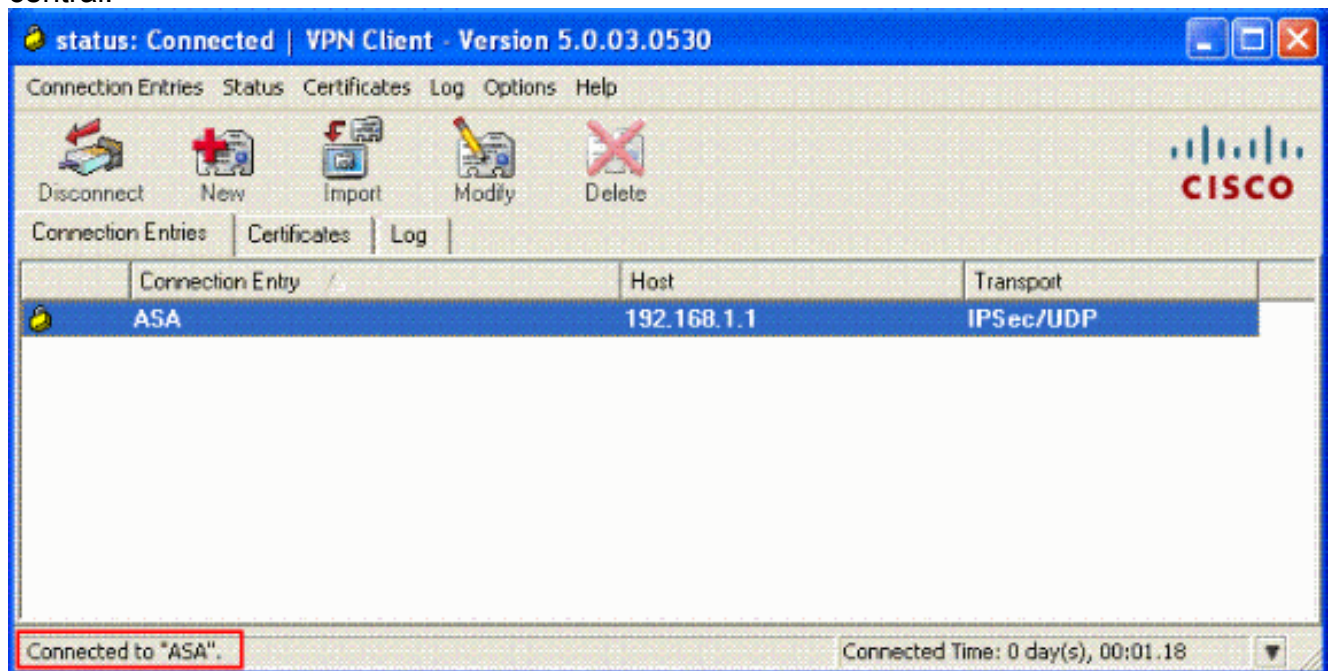
- Cuando se le pregunte, ingrese el **nombre de usuario: cisco123** y **contraseña: cisco123** como está configurado en el ASA arriba para el Xauth, y **AUTORIZACIÓN** del tecleo a

conectar con la red

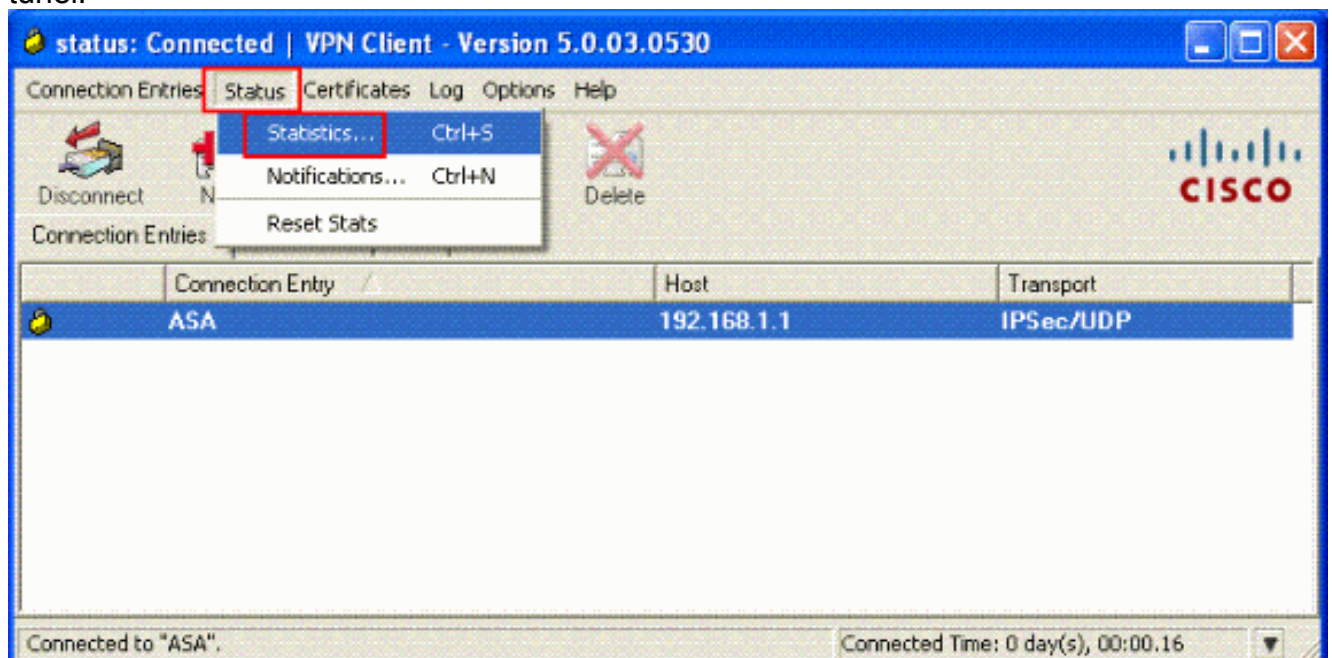


remota.

6. El cliente VPN está conectado con el ASA en el sitio central.



7. Una vez que la conexión se establece con éxito, seleccione las **estadísticas** del menú Status (Estado) para verificar los detalles del túnel.



# Verificación

## Comandos show

Utilice esta sección para confirmar sus trabajos de la configuración correctamente.

[La herramienta Output Interpreter Tool \(clientes registrados solamente\)](#) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

- **show crypto isakmp sa**: muestra todas las asociaciones actuales de seguridad IKE (SA) de un par.
- **muestre IPsec crypto sa** — Muestra las configuraciones usadas por los SA actuales.

```
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

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración. También se muestra un ejemplo de salida del debug .

**Nota:** Para más información sobre el IPsec VPN del Acceso Remoto del troubleshooting refiera [la mayoría del IPsec VPN común L2L y del Acceso Remoto que resuelve problemas las soluciones](#)

### Borre las asociaciones de seguridad

Cuando usted resuelve problemas, asegúrese borrar las asociaciones de seguridad existentes después de que usted realice un cambio. En el modo privilegiado del PIX, utilice estos comandos:

- **clear [crypto] ipsec sa** — Borra el IPsec activo SA. La palabra clave crypto es opcional.
- **clear [crypto] isakmp sa** — Borra el IKE activo SA. La palabra clave crypto es opcional.

### Comandos para resolución de problemas

[La herramienta Output Interpreter Tool \(clientes registrados solamente\)](#) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

**Nota:** Consulte [Información Importante sobre Comandos de Debug](#) antes de usar un **comando debug**.

- **debug crypto ipsec 7** — Muestra negociaciones IPsec de la Fase 2.
- **debug crypto isakmp 7** — Muestra negociaciones ISAKMP de la Fase 1.

### Ejemplo de resultado del comando 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, constructing qm hash payload

Jan 22 22:21:24 [IKEv1]: IP = 192.168.1.2, IKE\_DECODE SENDING Message (msgid=e8a1816d) 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=e8a1816d) 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\_attr(): Enter!

Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, Processing MODE\_CFG Reply attributes.

Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, IKEGetUserAttributes: primary DNS = cleared

Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, IKEGetUserAttributes: secondary DNS = cleared

Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, IKEGetUserAttributes: primary WINS = cleared

Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, IKEGetUserAttributes: secondary WINS = cleared

Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, IKEGetUserAttributes: IP Compression = disabled

Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, IKEGetUserAttributes: Split Tunneling Policy = Disabled

Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, IKEGetUserAttributes: Browser Proxy Setting = no-modify

Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, 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 = 192.168.1.2, constructing blank hash payload

Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, constructing qm hash payload

Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE\_DECODE SENDING Message (msgid=14360de6) 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=14360de6) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 56

Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, process\_attr(): Enter!

Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, Processing cfg ACK attributes

Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE\_DECODE RECEIVED Message (msgid=2663aldd) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 193

Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, process\_attr(): Enter!

Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, Processing cfg Request attributes

Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, MODE\_CFG: Received request for IPV4 address!

Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, MODE\_CFG: Received request for IPV4 net mask!

Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, MODE\_CFG: Received request for DNS server address!

Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, 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 = 192.168.1.2, MODE\_CFG: Received request for Banner!

Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, MODE\_CFG: Received request for Save PW setting!

Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, MODE\_CFG: Received request for Default Domain Name!

Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, MODE\_CFG: Received request for Split Tunnel List!

Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, MODE\_CFG: Received request for Split DNS!

Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, MODE\_CFG: Received request for PFS setting!

Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, MODE\_CFG: Received request for Client Browser Proxy Setting!

Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, 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 = 192.168.1.2, 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 = 192.168.1.2, MODE\_CFG: Received request for FWTYPE!

Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, MODE\_CFG: Received request for DHCP hostname for DDNS is: Wireless123!

Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, MODE\_CFG: Received request for UDP Port!

Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, Obtained IP addr (192.168.5.1) prior to initiating Mode Cfg (XAuth enabled)

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 = 192.168.1.2, constructing blank hash payload

Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, Send Client Browser Proxy Attributes!

Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, Browser Proxy set to No-Modify. Browser Proxy data will NOT be included in the mode-cfg reply

Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, constructing qm hash payload

Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE\_DECODE SENDING Message (msgid=2663a1dd) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 158

Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, Delay Quick Mode processing, Cert/Trans Exch/RM DSID in progress

Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, 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 = 192.168.1.2, Starting P1 rekey timer: 950 seconds.

Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, sending notify message

Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, constructing blank hash payload

Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, constructing qm hash payload

Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE\_DECODE SENDING Message (msgid=f4435669) 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=541f8e43) 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 = 192.168.1.2, processing hash payload

Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, processing SA payload

Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, processing nonce payload

Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, 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, Protocol 0, Port 0

Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, 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 = 192.168.1.2, processing IPsec SA payload

Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, IPsec SA Proposal # 14, Transform # 1 acceptable Matches global IPsec 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 = 192.168.1.2, IKE got SPI from key engine: SPI = 0x31de01d8

Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, oakley constructing quick mode

Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, constructing blank hash payload

Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, 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 seconds

Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, constructing IPsec nonce payload

Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, constructing proxy ID

Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, 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 = 192.168.1.2, Sending RESPONDER LIFETIME notification to Initiator

Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, constructing qm hash payload

Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE\_DECODE SENDING Message (msgid=541f8e43) 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=541f8e43) with payloads : HDR + HASH (8) + NONE (0) total length : 48

Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, processing hash payload

Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, loading all IPSEC SAs

Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, Generating Quick Mode Key!

Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, 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 = 192.168.1.2, IKE got a KEY\_ADD msg for SA: SPI = 0x8b7597a9

Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, Pitcher: received KEY\_UPDATE, spi 0x31de01d8

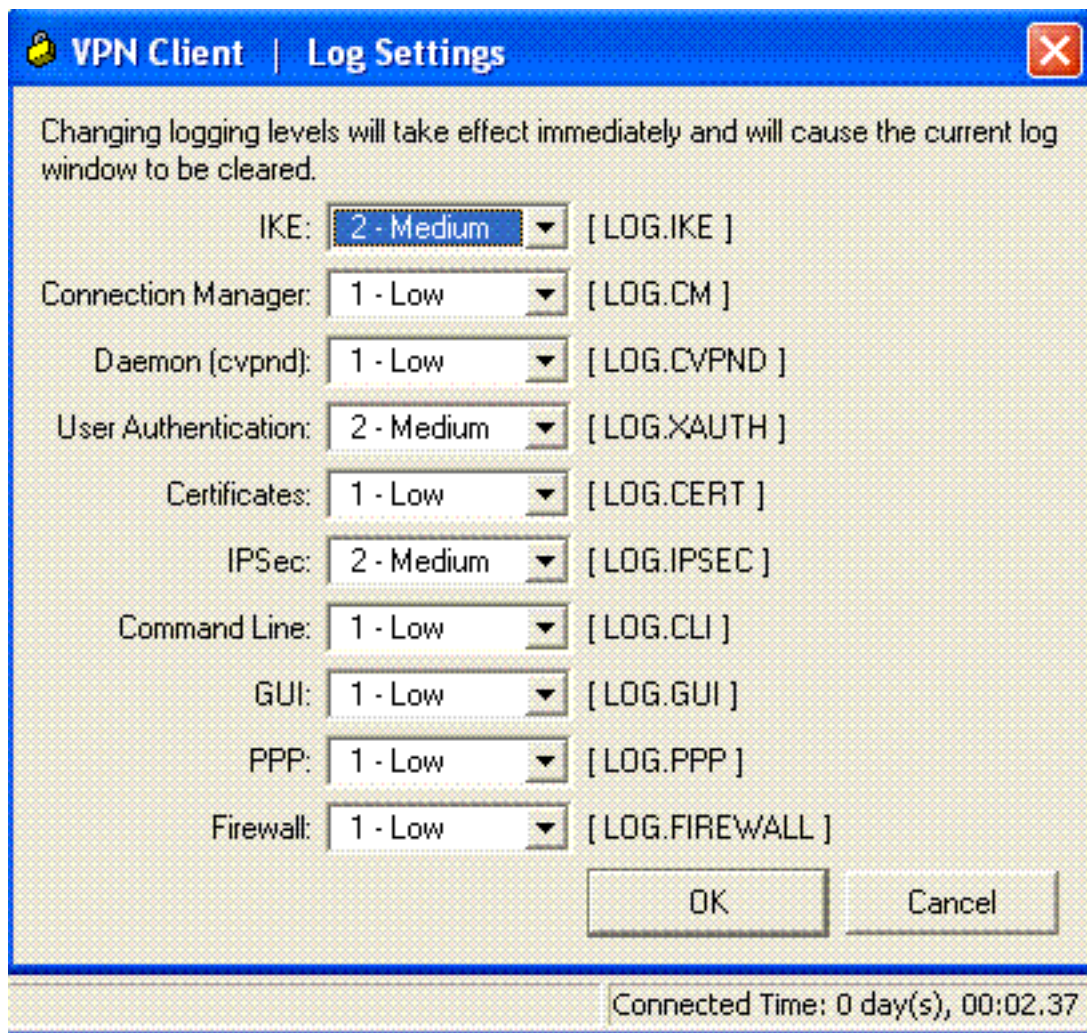
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, Starting P2 rekey timer: 27360 seconds.  
Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, Adding static route for client address: 192.168.5.1  
Jan 22 22:21:31 [IKEv1]: Group = 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=78f7d3ae) with payloads : HDR + HASH (8) + NOTIFY (11) + NONE (0) total length : 80

ASA#debug crypto ipsec 7

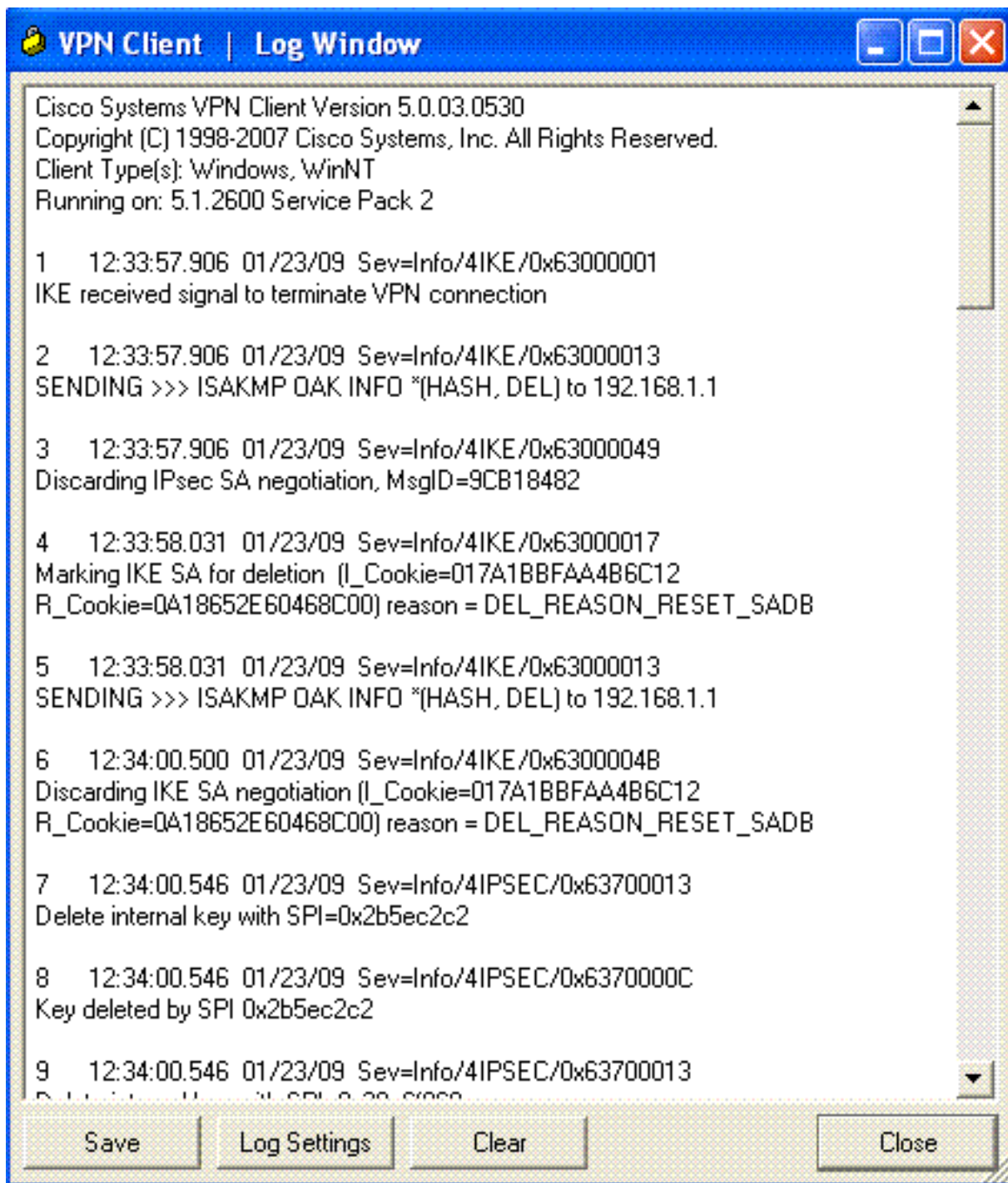
*!--- Deletes the old SAs.* ASA# IPSEC: Deleted inbound decrypt rule, SPI 0x7F3C985A Rule ID: 0xD5567DB0 IPSEC: Deleted inbound permit rule, SPI 0x7F3C985A Rule ID: 0xD4EF1DF0 IPSEC: Deleted inbound tunnel flow rule, SPI 0x7F3C985A Rule ID: 0xD556AF60 IPSEC: Deleted inbound VPN context, SPI 0x7F3C985A 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](#)

Seleccione el registro > las configuraciones de registro para habilitar los niveles del registro en el cliente VPN.



Seleccione el **registro** > **la ventana del registro** para ver las entradas de registro en el cliente VPN.



## [Información Relacionada](#)

- [Página de Soporte de Cisco ASA 5500 Series Adaptive Security Appliances](#)
- [Referencias de comandos del Dispositivos de seguridad adaptable Cisco ASA de la serie 5500](#)
- [Página de Soporte de Cisco PIX 500 Series Security Appliances](#)
- [Referencia de comandos del Dispositivos de seguridad Cisco PIX de la serie 500](#)
- [Cisco Adaptive Security Device Manager](#)
- [Página de Soporte de IPsec Negotiation/IKE Protocols](#)