ASA/PIX: IP estático dirigiendo para el cliente del IPSec VPN con el CLI y el ejemplo de la Configuración de ASDM

Contenido

Introducción

Este documento describe cómo configurar el dispositivo de seguridad adaptante de las Cisco 5500 Series (ASA) para proporcionar el IP Address estático al cliente VPN con el Administrador de dispositivos de seguridad adaptante (ASDM) o el 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 ASA de Cisco es completa, puede ser verificada con el Cliente Cisco VPN.

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 de cliente VPN remoto autentica contra el Active Directory con un servidor de RADIUS del Internet Authentication Service de Microsoft Windows 2003 (IAS).

Refiera al PIX/ASA 7.x y al Cliente Cisco VPN 4.x por el ejemplo de la configuración de autenticación del Cisco Secure ACS para configurar una conexión VPN de acceso remoto entre un Cliente Cisco VPN (4.x para Windows) y el dispositivo de seguridad 7.x de la serie PIX 500 con

un Cisco Secure Access Control Server (ACS versión 3.2) para el 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 TécnicosCisco para obtener más información sobre las convenciones del documento.

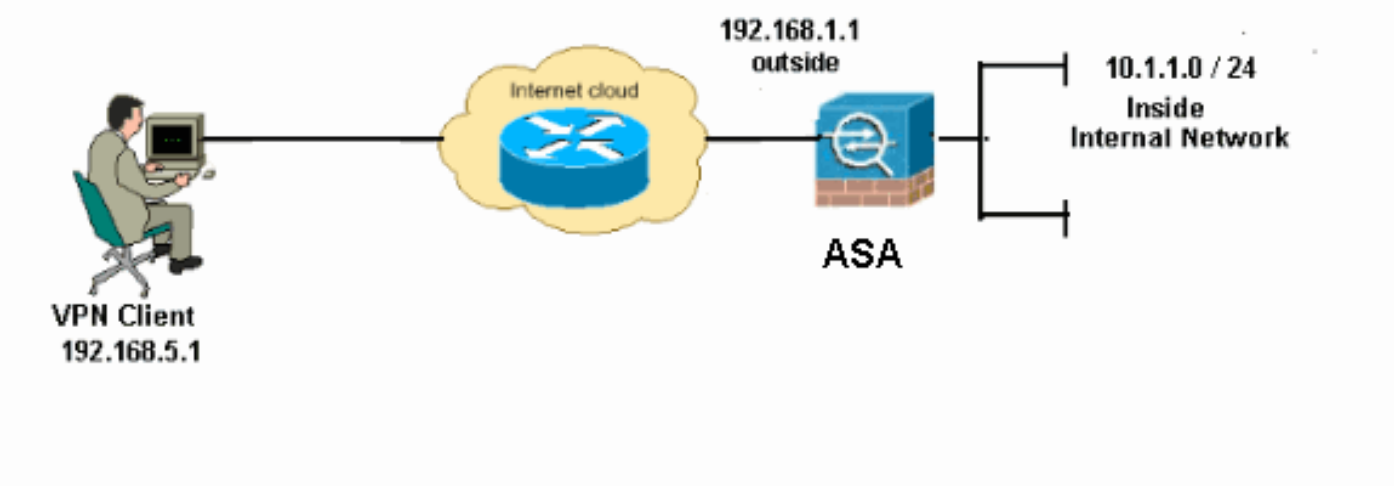
Configurar

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:



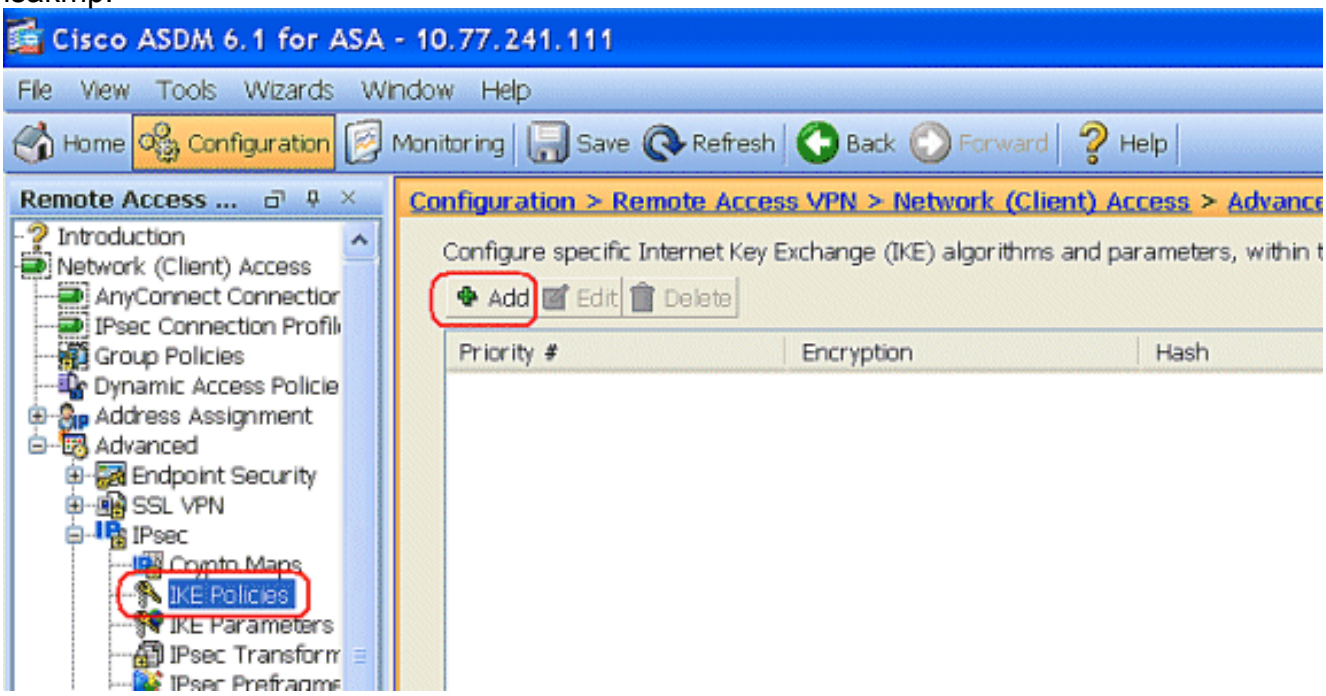
Nota: Los esquemas de direccionamiento IP usados en esta configuración no son legalmente enrutables en Internet. Son los direccionamientos del RFC 1918, que fueron utilizados en un ambiente de laboratorio.

VPN de acceso remoto de la configuración (IPSec)

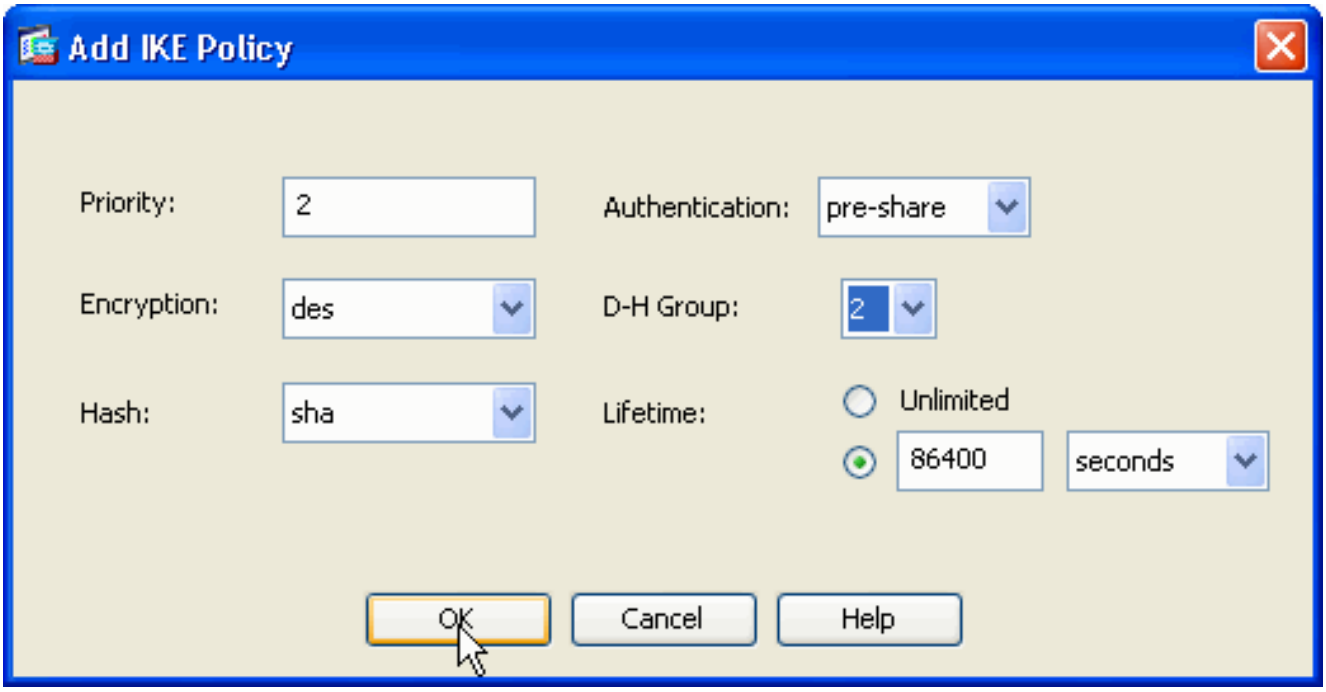
Procedimiento del ASDM

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.

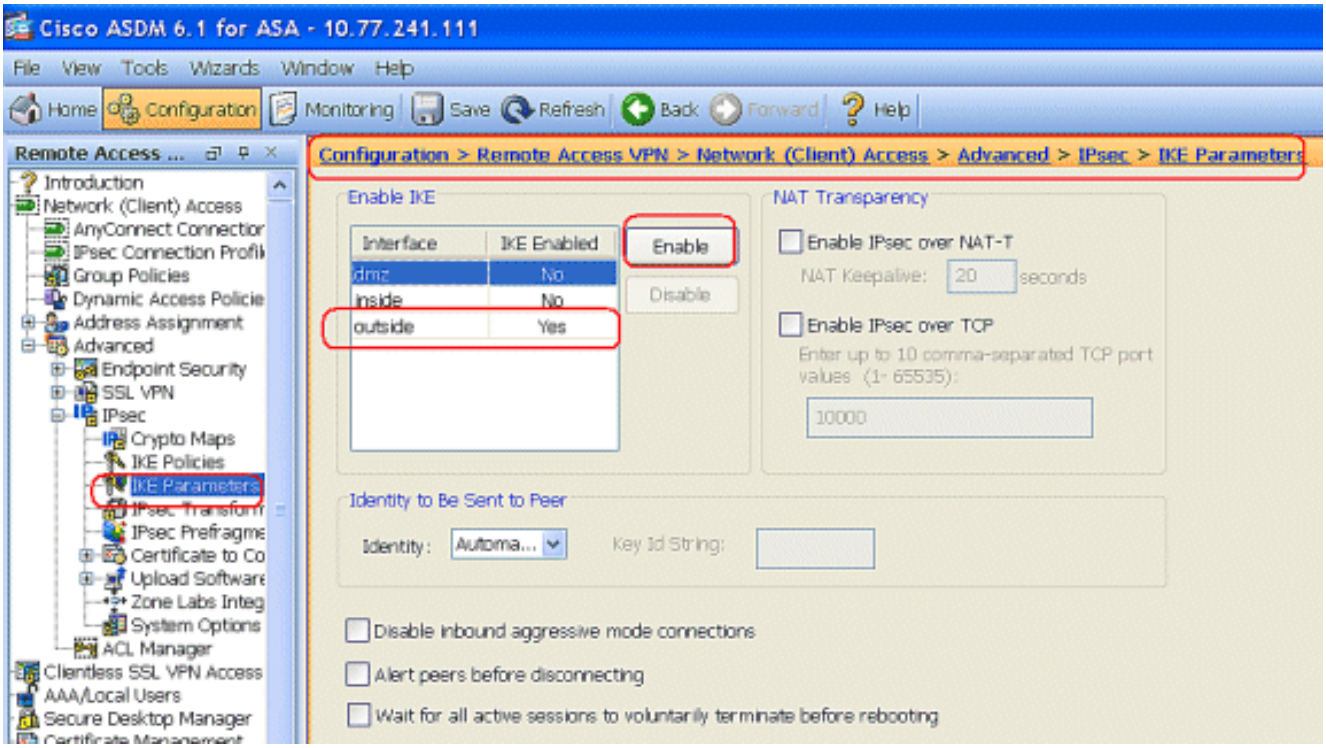


2. Proporcione los detalles de la política isakmp.

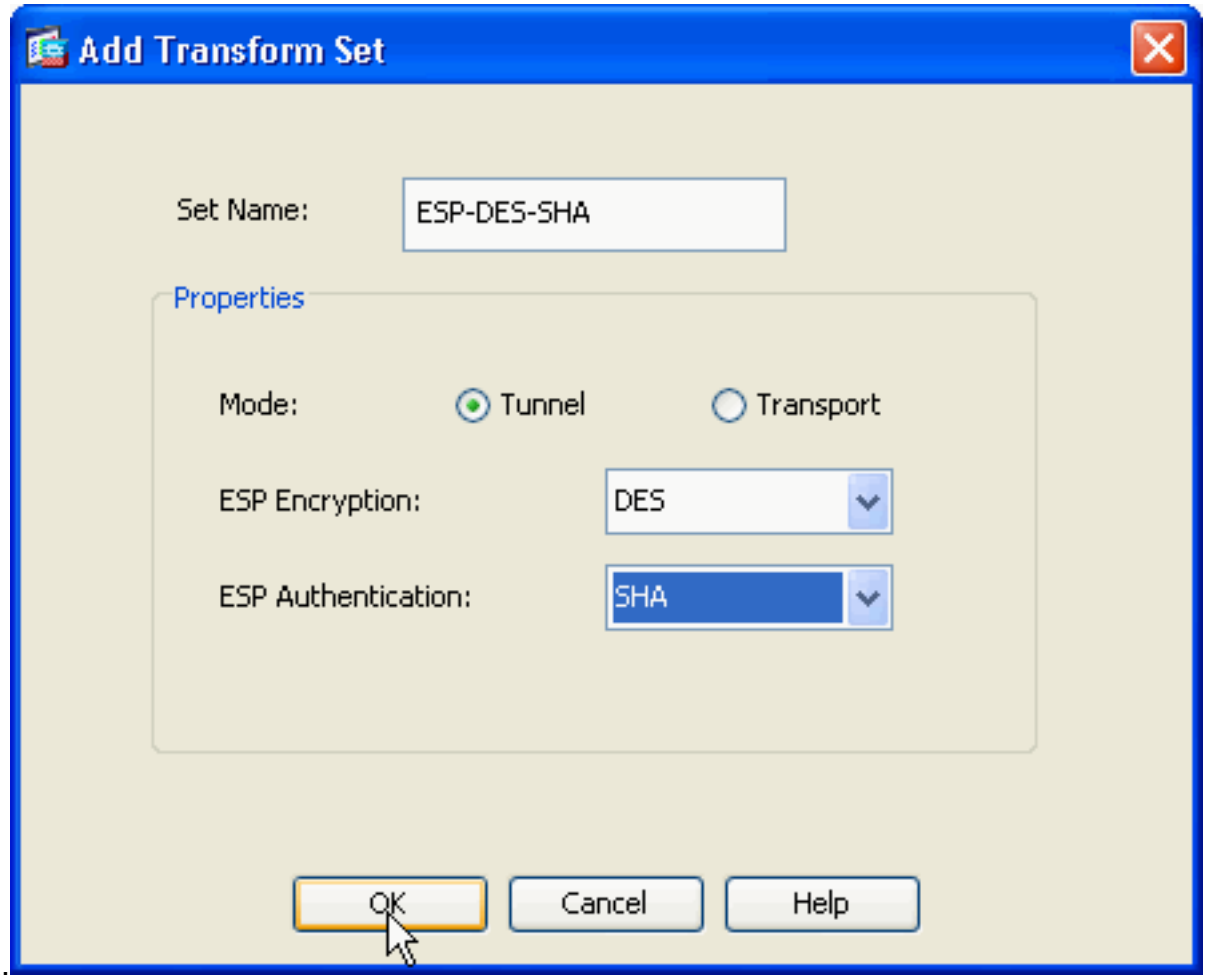


El Haga Click en OK y **se aplica**.

3. Elija la **configuración > el acceso del VPN de acceso remoto > de la red (cliente) > avanzó > IPSec > los parámetros IKE** para habilitar el IKE en la interfaz exterior.

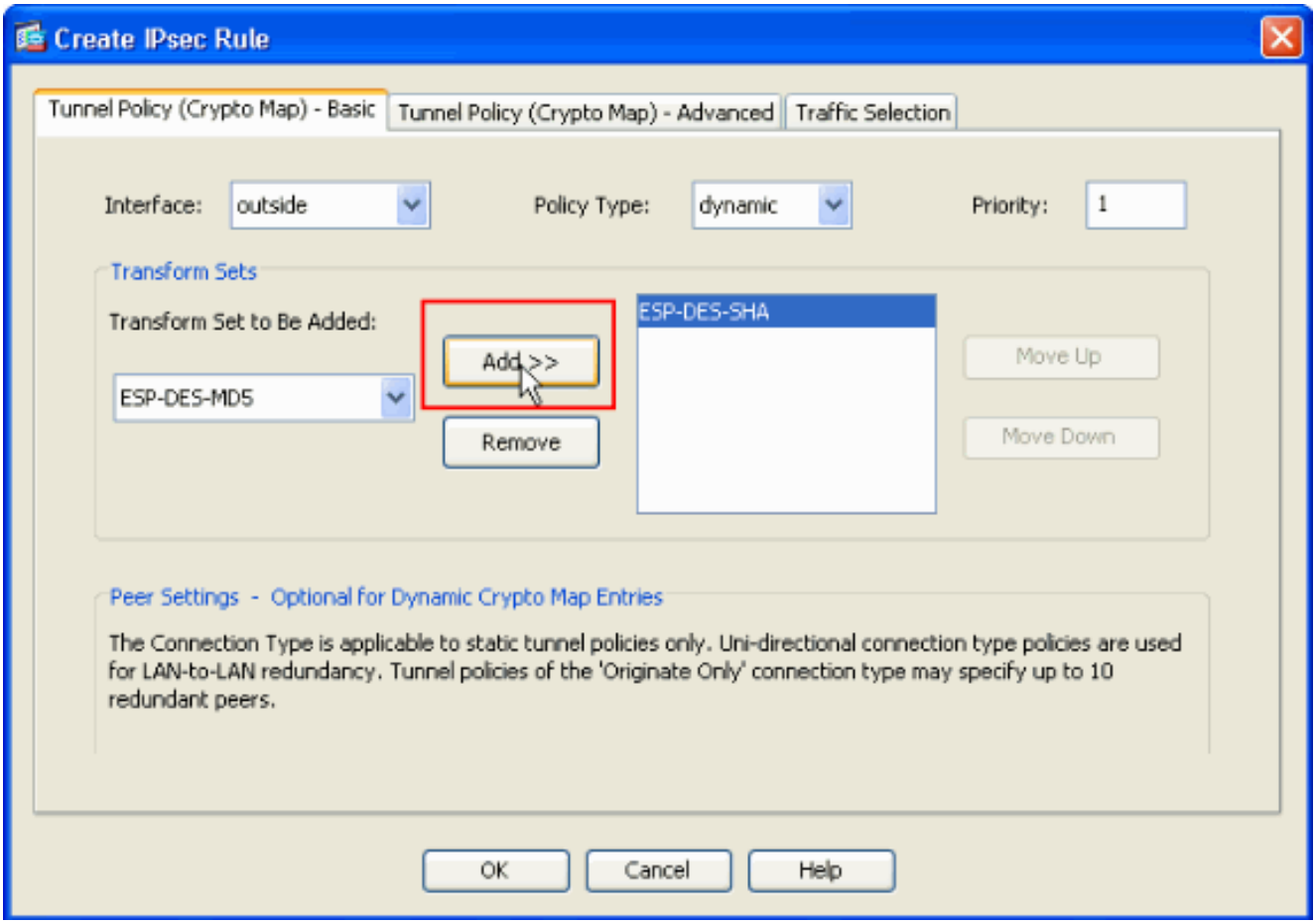


4. Elija la **configuración > el acceso del VPN de acceso remoto > de la red (cliente) > avanzó > IPSec > IPSec transforman los conjuntos > Add** para crear el **ESP-DES-SHA** transforman el conjunto, como se



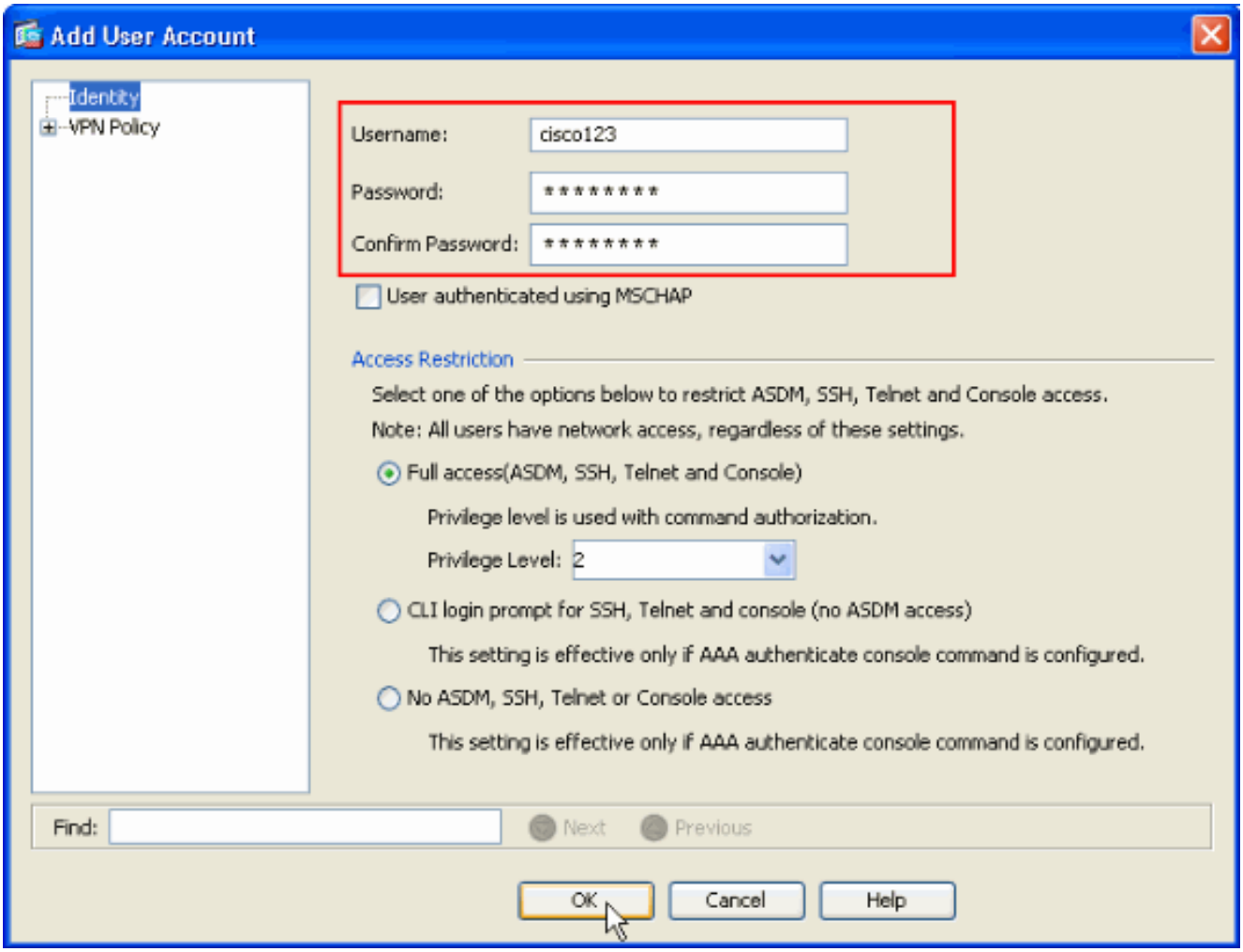
muestra.
El Haga Click en OK y **se aplica**.

5. 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.

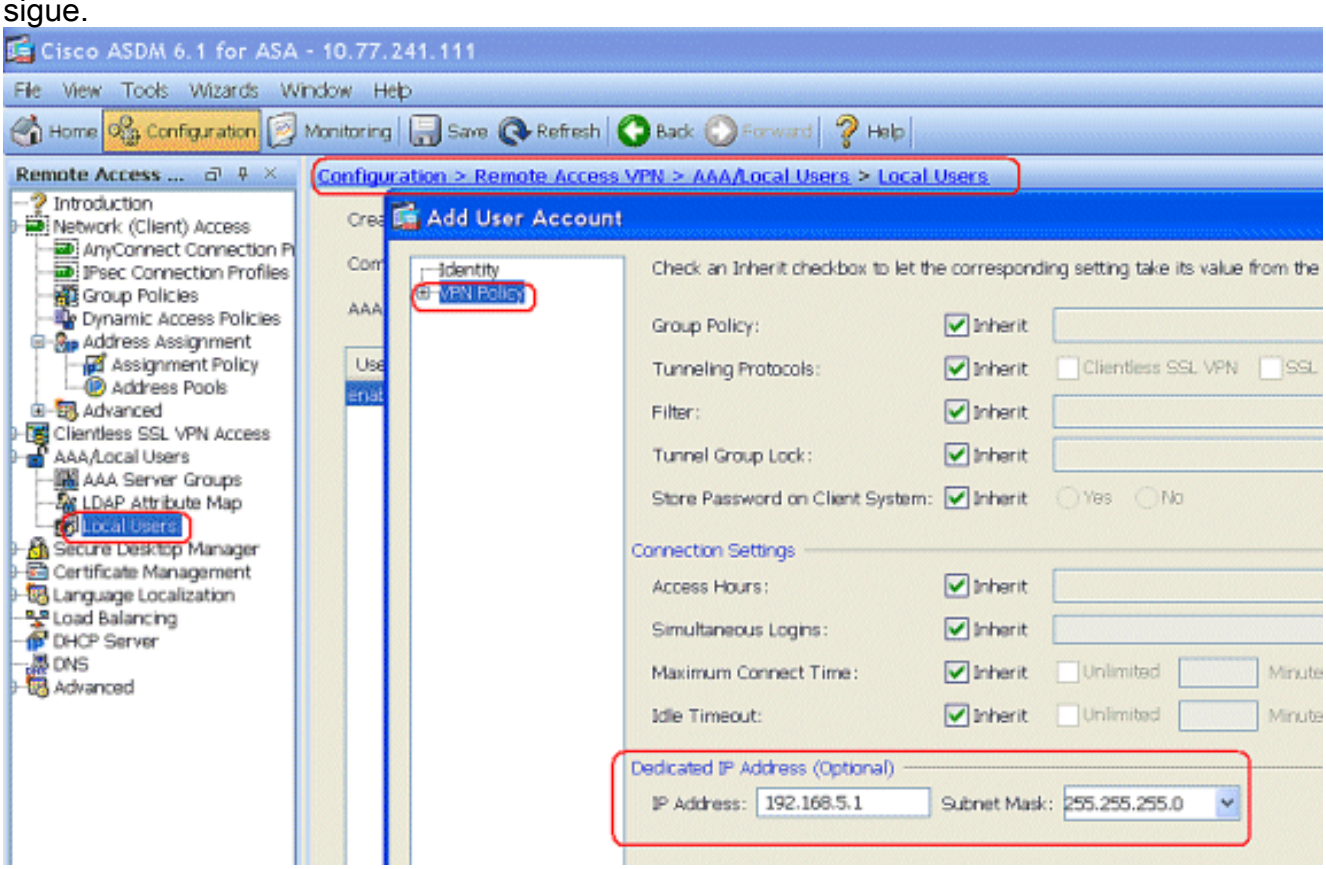


El Haga Click en OK y **se aplica**.

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.

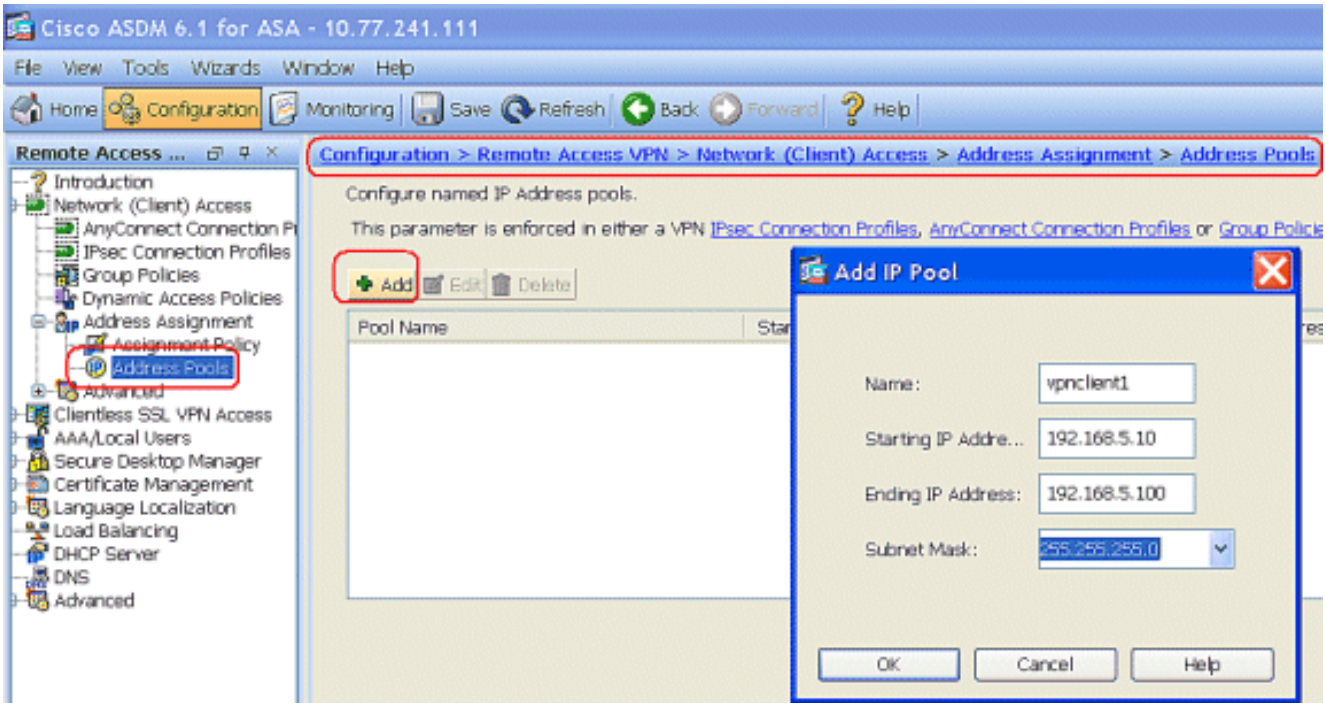


7. Vaya a la **política del VPN** y agregue el **estático/dedicó la dirección IP** para el usuario el "cisco123," como
sigue.

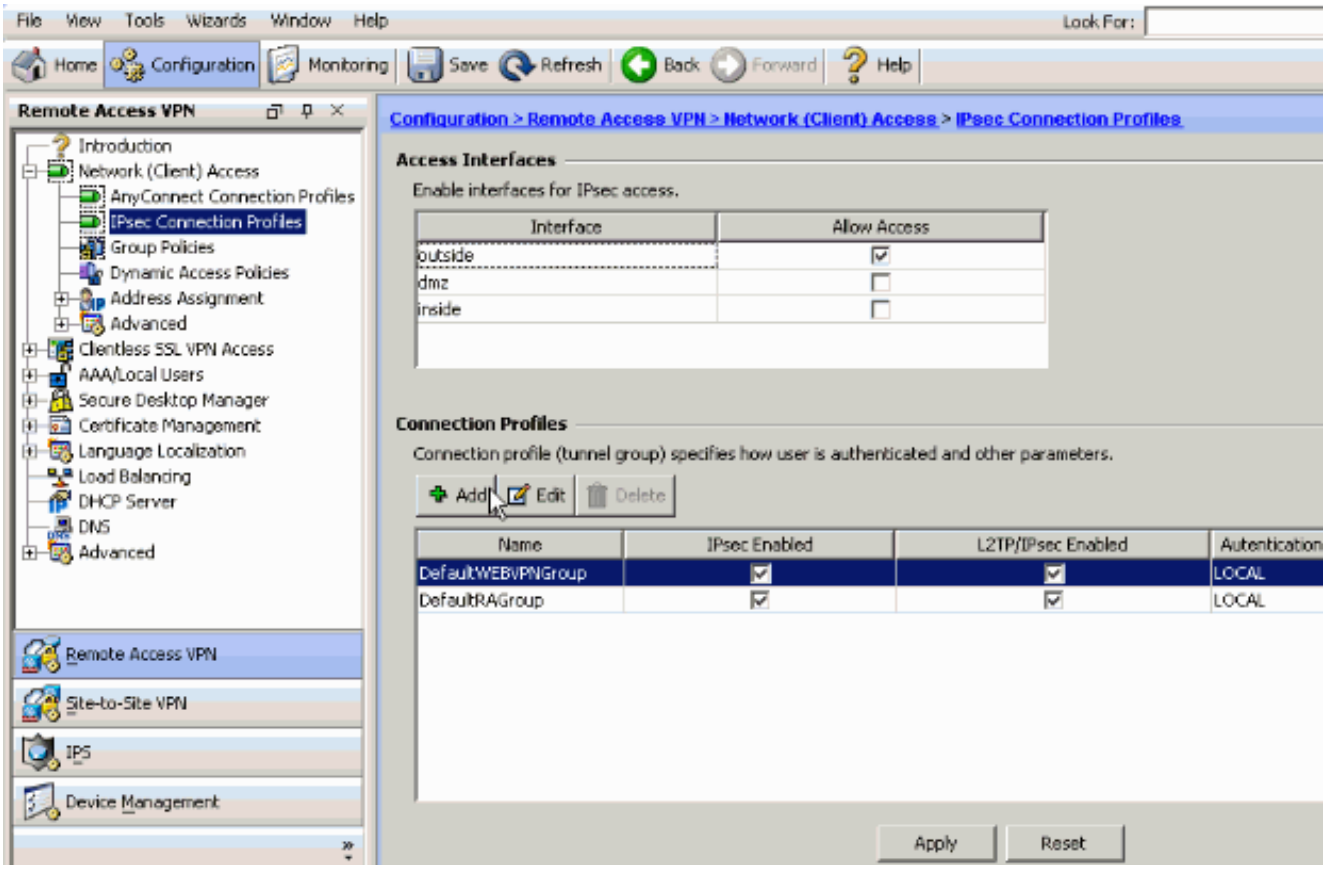


8. Elija la **configuración > el VPN de acceso remoto > el acceso > la asignación de dirección >**

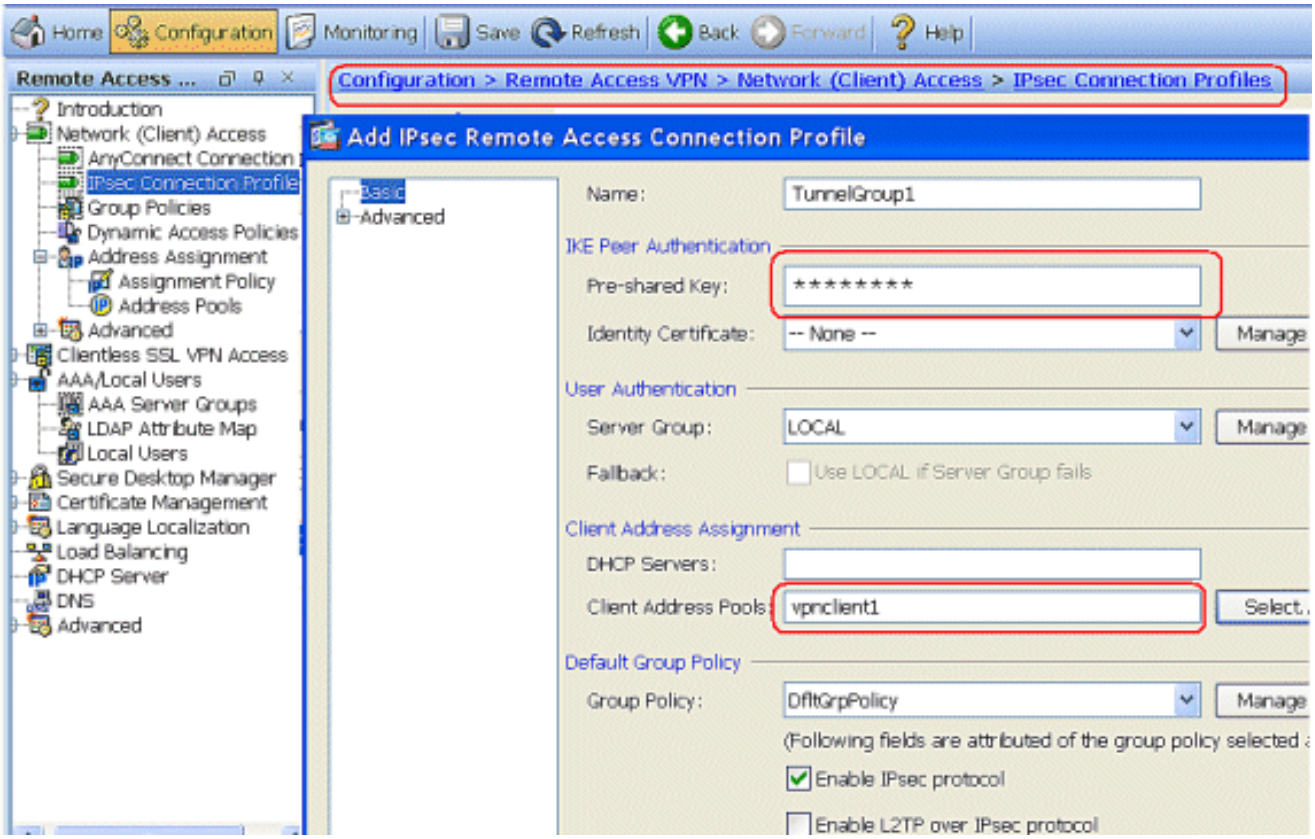
a las agrupaciones de direcciones de la red (cliente) y el tecleo **agrega** para agregar al cliente VPN para los usuarios de cliente
VPN.



9. Elija la **configuración > el acceso del VPN de acceso remoto > de la red (cliente) > conexión IPSec perfila > Add** para agregar a un grupo de túnel (por ejemplo, TunnelGroup1 y el preshared cierran como cisco123), como se
muestra.

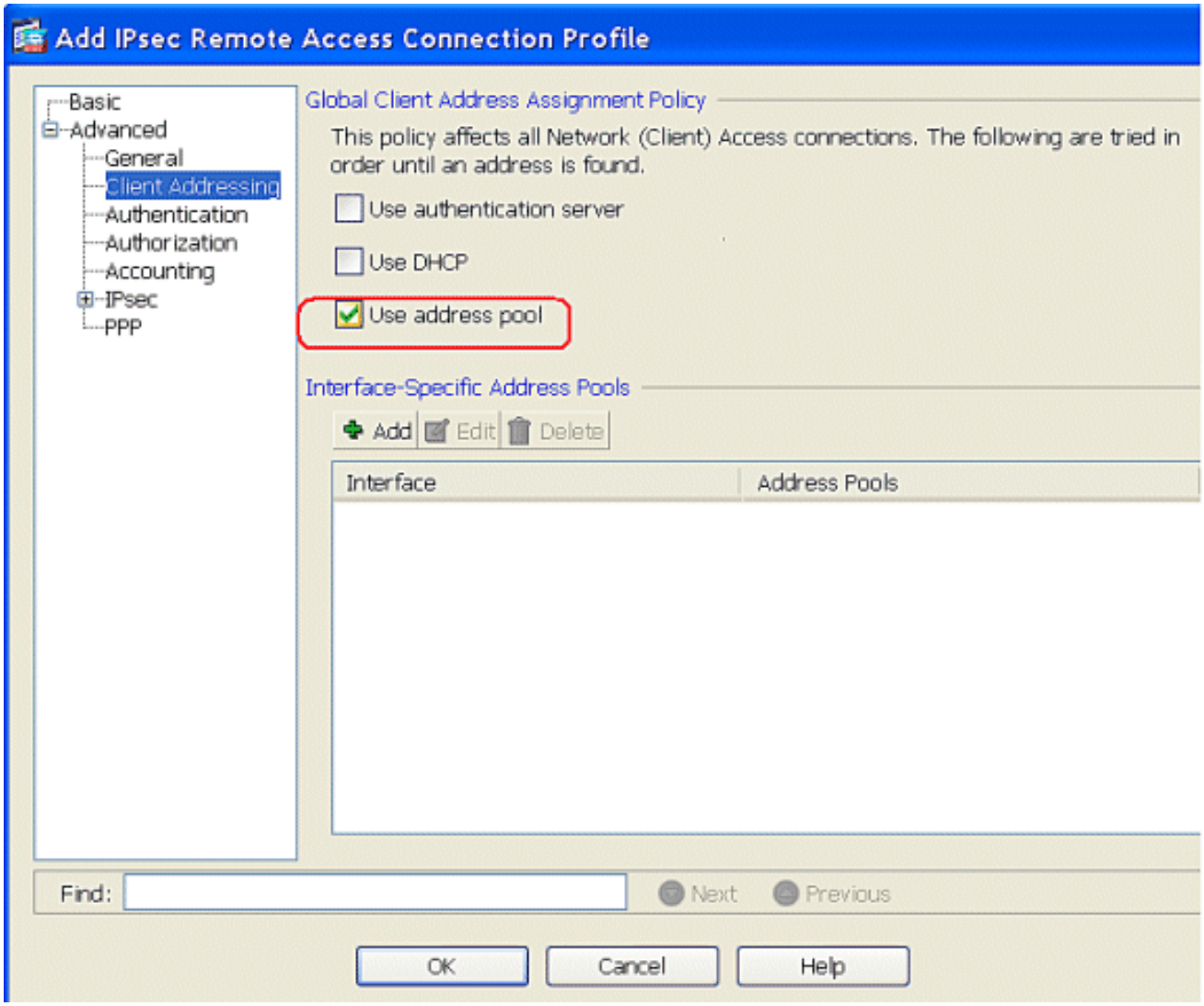


Bajo lengueta **básica**, elija al grupo de servidores como **LOCAL** para el campo de la autenticación de usuario.Elija **vpnclient1** como los pools de la dirección cliente para los usuarios de cliente
VPN.



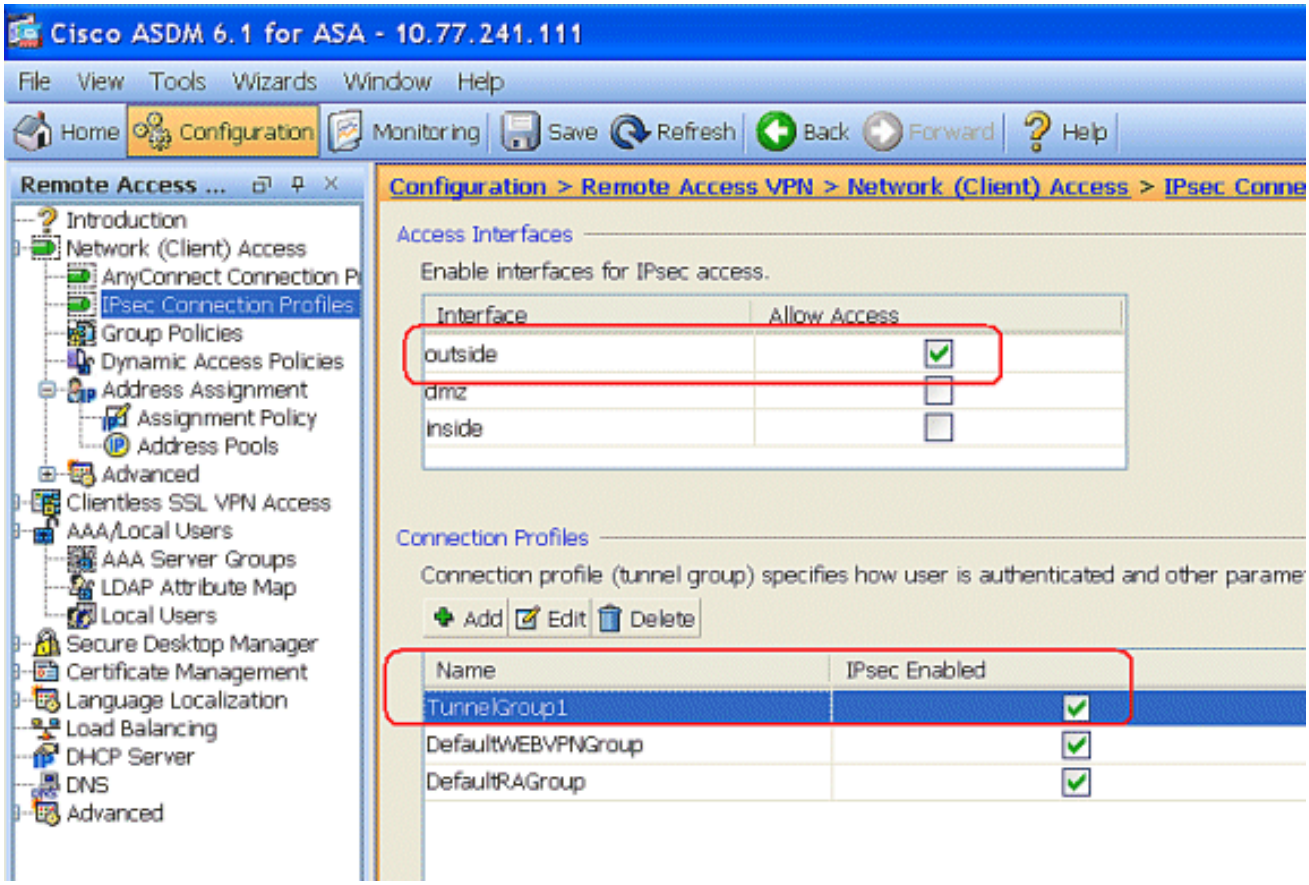
Haga clic en OK.

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



Haga clic en OK.

11. Habilite la **interfaz exterior** para el acceso del IPSec. El tecleo **se aplica** para proceder.



Configurar ASA/PIX con la CLI

Complete estos pasos para configurar al servidor DHCP para proporcionar los IP Addresses 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 corriente 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 ip local pool vpnclient1 192.168.5.10-192.168.5.100
mask 255.255.255.0

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 local and not by
AAA or dhcp. The CLI vpn-addr-assign local for VPN
address assignment through ASA is hidden in the CLI
provided by show run command.

no vpn-addr-assign aaa
no vpn-addr-assign dhcp

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
```

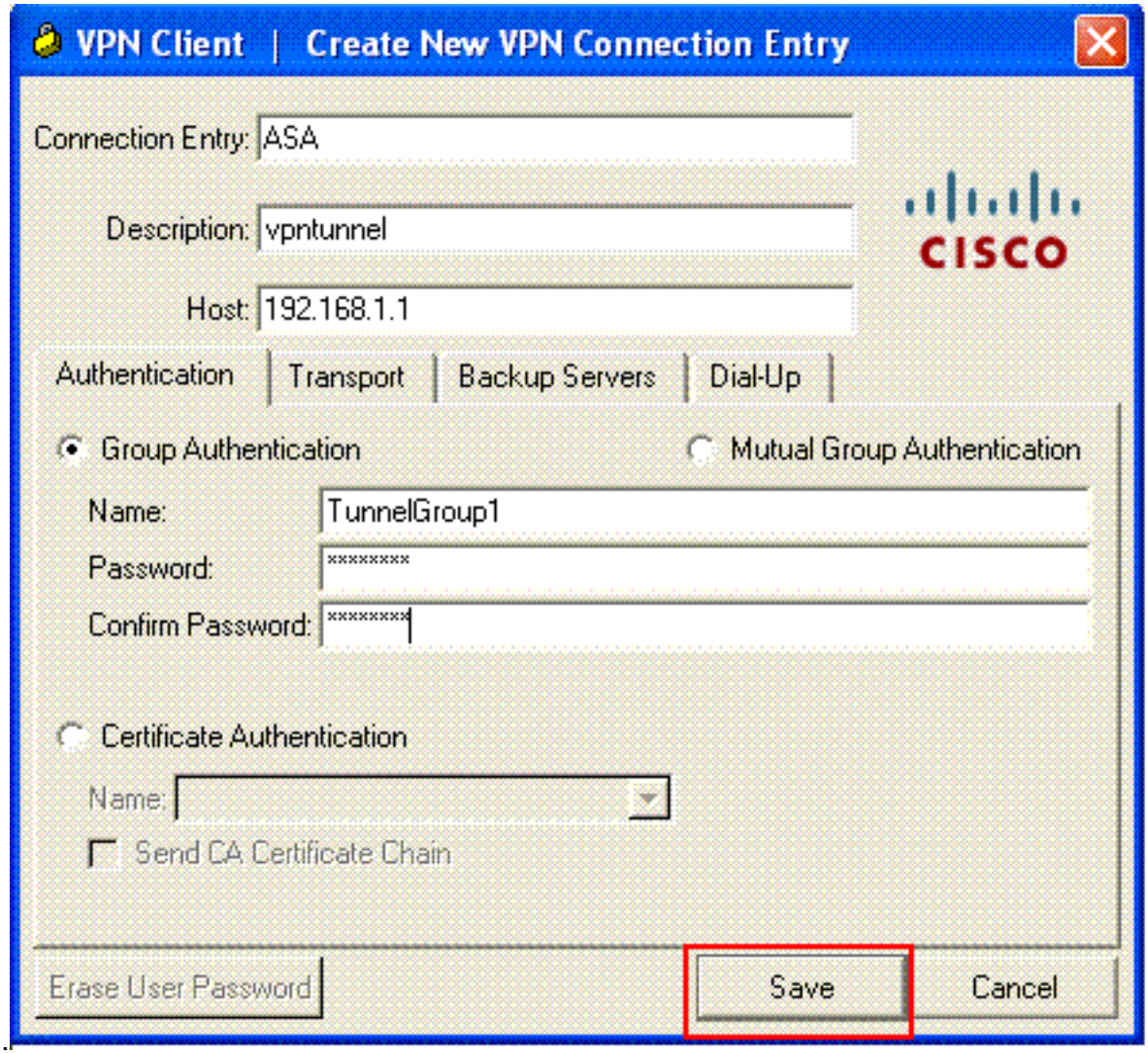
```
  inspect xdmcp
!
service-policy global_policy global
!
group-policy DfltGrpPolicy attributes
 vpn-tunnel-protocol IPSec webvpn
group-policy GroupPolicy1 internal

!--- In order to identify remote access users to the
Security Appliance, !--- you can also configure
usernames and passwords on the device. !--- specify the
IP address to assign to a particular user, use the vpn-
framed-ip-address command !--- in username mode

username cisco123 password ffIRPGpDSOJh9YLq encrypted
username cisco123 attributes
  vpn-framed-ip-address 192.168.5.1 255.255.255.0
!--- Create a new tunnel group and set the connection !-
-- type to remote-access. tunnel-group TunnelGroup1 type
remote-access tunnel-group TunnelGroup1 general-
attributes address-pool vpnclient1 !--- 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 conectar con Cisco ASA con el Cliente Cisco VPN para verificar que el ASA está configurado con éxito.

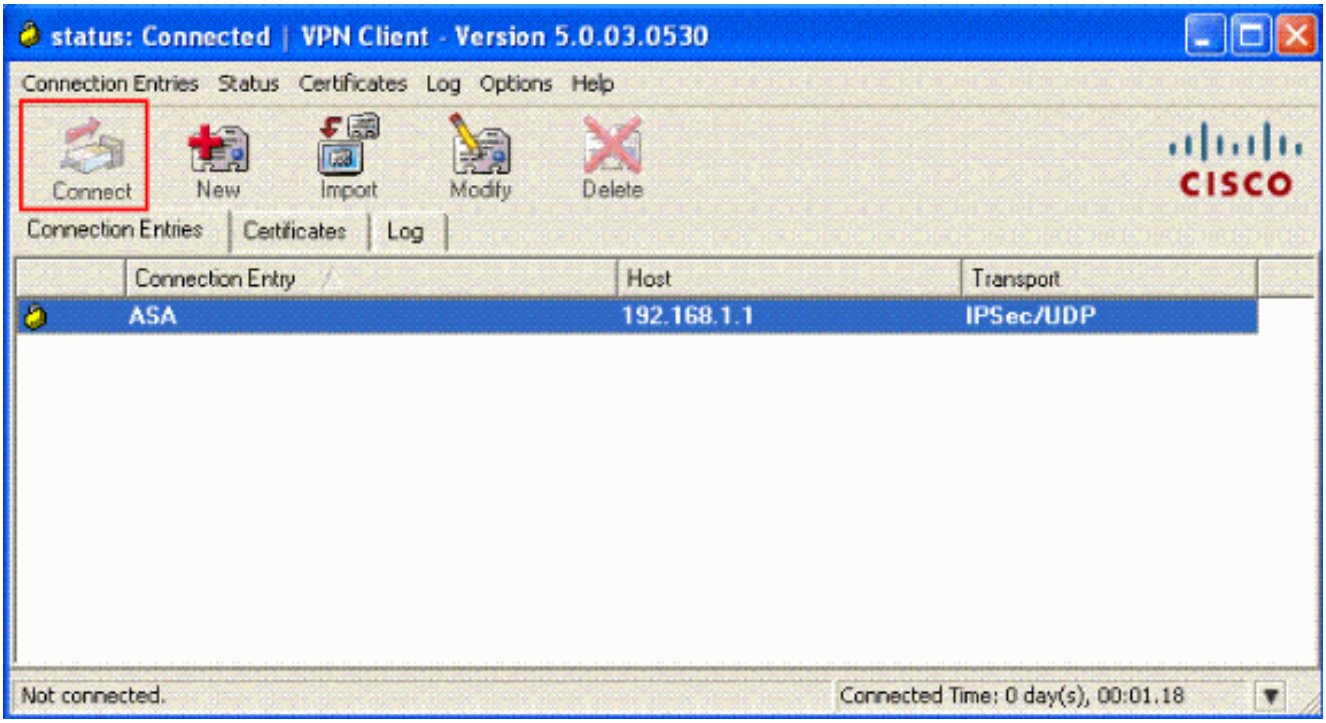
1. Elija el **Start (Inicio) > Programs (Programas) > Cisco Systems VPN Client (VPN Client de Cisco Systems) > al cliente VPN**.
2. Tecleo **nuevo** iniciar la nueva ventana de entrada de la conexión VPN del crear.

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 nombre de grupo de túnel VPN (TunnelGroup1) y la contraseña (clave previamente compartida - cisco123) como está configurado en el ASA. Haga clic en Save



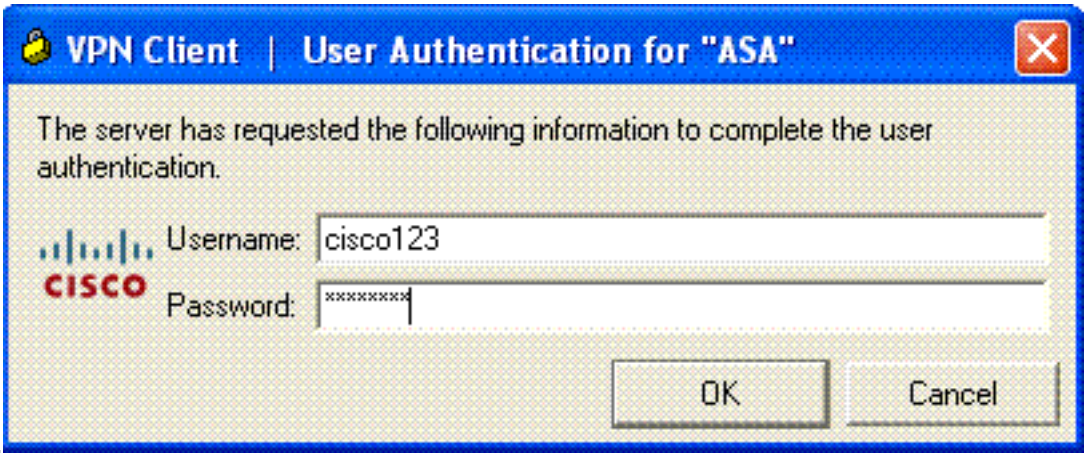
(Guardar).

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

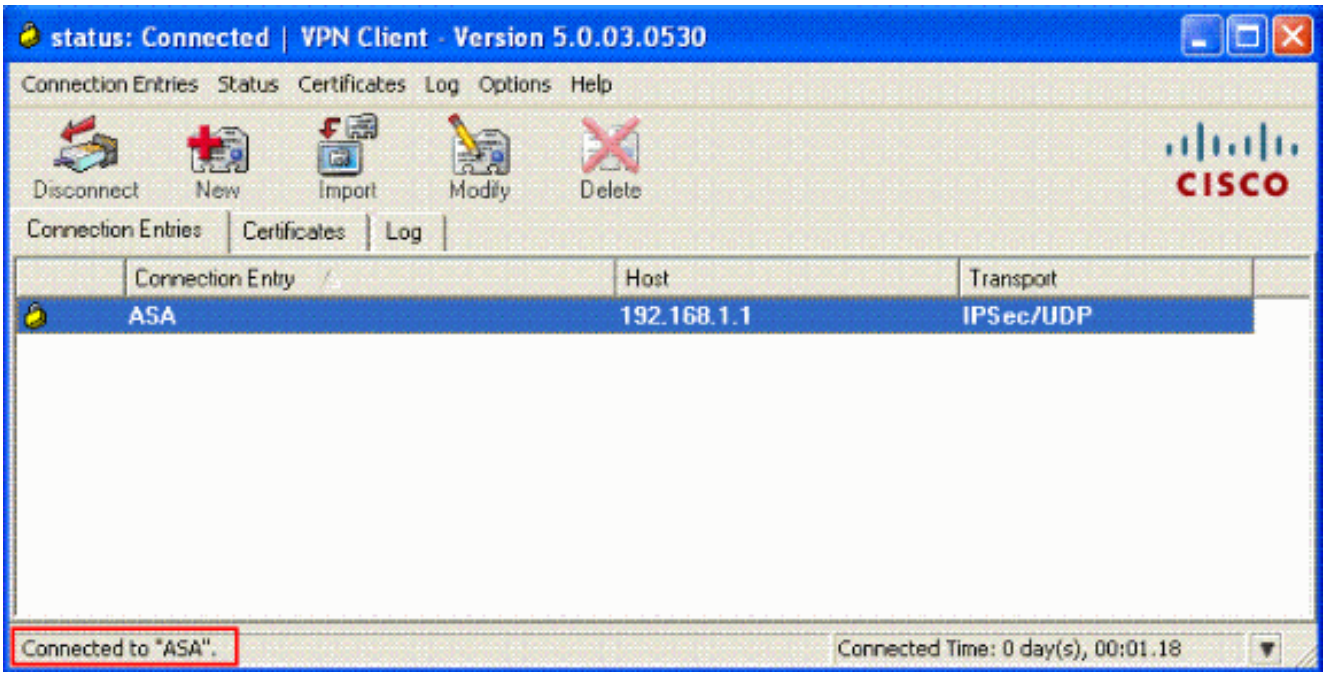


5. Cuando se le pregunte, ingrese el **nombre de usuario: cisco123** y **contraseña: cisco123** como está configurado en el ASA para el Xauth, y **AUTORIZACIÓN del** tecleo a conectar

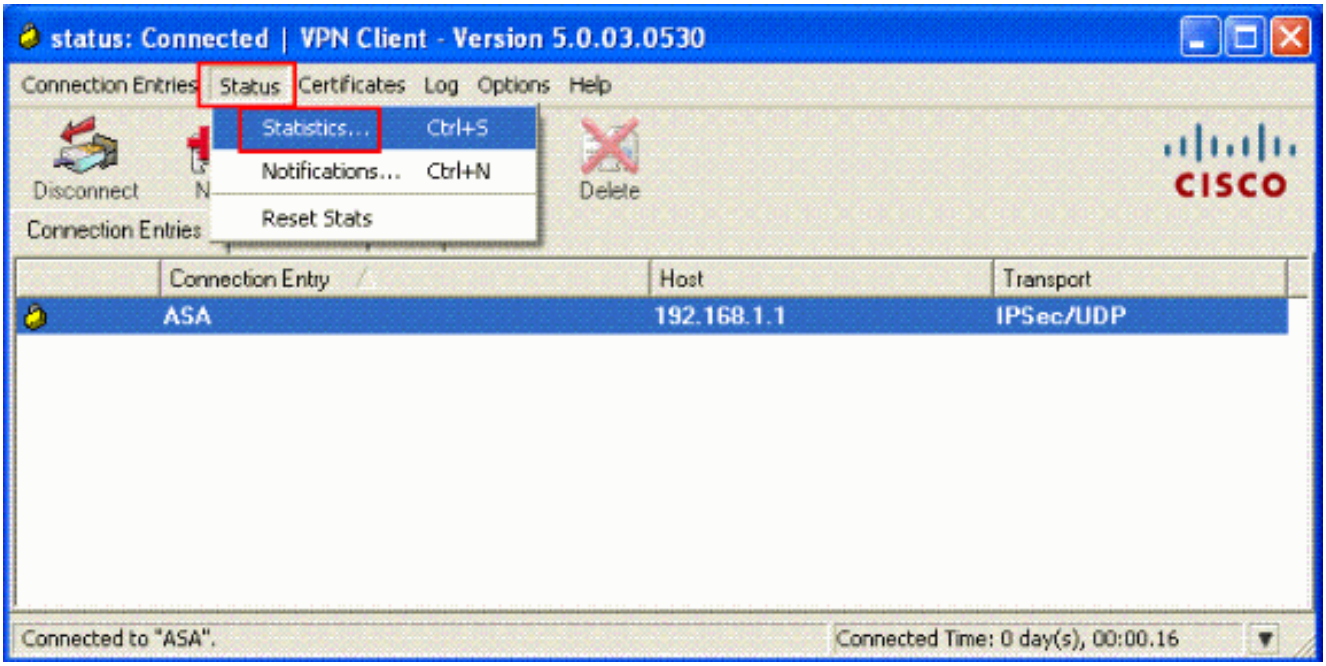
con la red remota.



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



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



Verificación

Comandos show

Use esta sección para confirmar que su configuración funciona 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.

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, aseegurese 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.

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
- Página de soporte para cliente Cisco VPN
- Cisco PIX Firewall Software
- Referencias de Comandos de Cisco Secure PIX Firewall
- Avisos de campos de productos de seguridad (incluido PIX)
- Solicitudes de Comentarios (RFC)
- Soporte Técnico y Documentación - Cisco Systems