Cisco Secure PIX Firewall 6.x y Cisco VPN Client 3.5 para Windows con autenticación RADIUS de Microsoft Windows 2000 y 2003 IAS

Contenido

Introducción

Esta configuración de ejemplo muestra cómo configurar Cisco VPN Client versión 3.5 para Windows y Cisco Secure PIX Firewall para su uso con el Servidor RADIUS de Microsoft Windows 2000 y Servicio de Autenticación Internet (IAS). Consulte Microsoft - Lista de verificación: Configuración de IAS para marcación manual y acceso VPN para más información sobre el IAS.

Consulte Ejemplo de Configuración de Autenticación de PIX/ASA 7.x y Cisco VPN Client 4.x para Windows con Microsoft Windows 2003 IAS RADIUS para obtener más información sobre el mismo escenario en PIX/ASA 7.0 con Cisco VPN Client 4.x.

Prerequisites

Requirements

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- La versión 6.0 del software Cisco Secure PIX Firewall admite conexiones VPN de Cisco VPN Client 3.5 para Windows.
- Esta configuración de ejemplo asume que el PIX ya está funcionando con las listas de estática, conductos o acceso apropiadas. El documento actual no pretende ilustrar estos

conceptos básicos, sino mostrar la conectividad con el PIX desde un Cisco VPN Client.

Componentes Utilizados

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

- Software PIX Firewall versión 6.1.1**Nota:** Esto se probó en la versión 6.1.1 del software PIX, pero debería funcionar en todas las versiones 6.x.
- Cisco VPN Client versión 3.5 para Windows
- Windows 2000 y 2003 Server con IAS

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

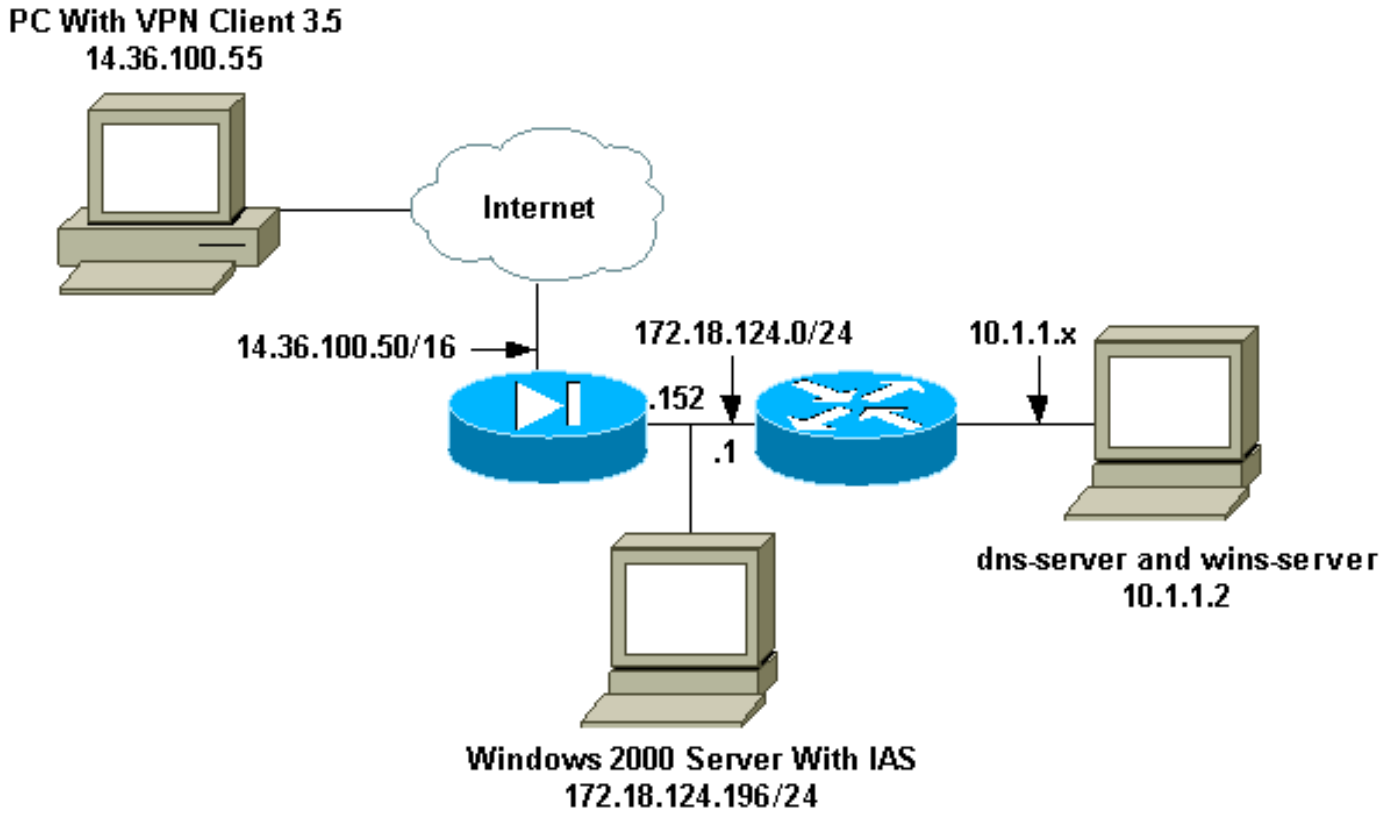
Configurar

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

Nota: Utilice la herramienta Command Lookup (sólo para clientes registrados) para obtener más información sobre los comandos utilizados en esta sección.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Configuraciones

Este documento usa estas configuraciones.

- Firewall PIX
- Cisco VPN Client 3.5 para Windows
- Microsoft Windows 2000 Server con IAS
- Microsoft Windows 2003 Server con IAS

Firewall PIX

Firewall PIX

```
pixfirewall(config)#write terminal
Building configuration...
: Saved
:
PIX Version 6.1(1)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pixfirewall
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
```

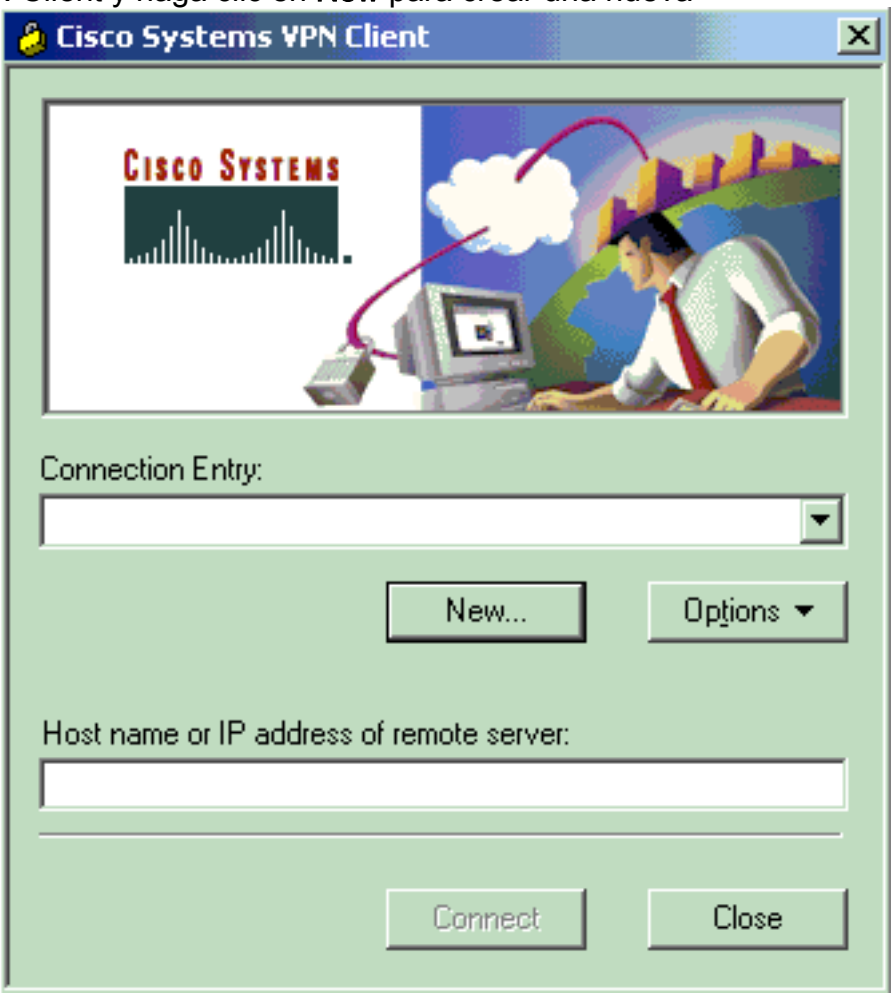
```
names
!--- Issue the access-list command to avoid !--- Network
Address Translation (NAT) on the IPsec packets.

access-list 101 permit ip 10.1.1.0 255.255.255.0
10.1.2.0
  255.255.255.0
pager lines 24
interface ethernet0 auto
interface ethernet1 auto
mtu outside 1500
mtu inside 1500
ip address outside 14.36.100.50 255.255.0.0
ip address inside 172.18.124.152 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
ip local pool ippool 10.1.2.1-10.1.2.254
pdm history enable
arp timeout 14400
global (outside) 1 14.36.100.51
!--- Binding access list 101 to the NAT statement to
avoid !--- NAT on the IPsec packets. nat (inside) 0
access-list 101
Nat (inside) 1 0.0.0.0 0.0.0.0 0 0
route outside 0.0.0.0 0.0.0.0 14.36.1.1 1
route inside 10.1.1.0 255.255.255.0 172.18.124.1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
   rpc 0:10:00 h323 0:05:00 sip 0:30:00 sip_media
0:02:00
timeout uauth 0:05:00 absolute
!--- Enable access to the RADIUS protocol.
aaa-server RADIUS protocol radius
!--- Associate the partnerauth protocol to RADIUS. aaa-
server partnerauth protocol radius
aaa-server partnerauth (inside) host 172.18.124.196
cisco123
   timeout 5
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
!--- Tell PIX to implicitly permit IPsec traffic. sysopt
connection permit-ipsec
no sysopt route dnat
!--- Configure a transform set that defines how the
traffic is protected. crypto ipsec transform-set myset
esp-des esp-md5-hmac
!--- Create a dynamic crypto map and specify which !---
transform sets are allowed for this dynamic crypto map
entry. crypto dynamic-map dynmap 10 set transform-set
myset
!--- Add the dynamic crypto map set into a static crypto
map set. crypto map mymap 10 ipsec-isakmp dynamic dynmap
!--- Enable the PIX to launch the Xauth application on
the VPN Client. crypto map mymap client authentication
partnerauth
!--- Apply the crypto map to the outside interface.
crypto map mymap interface outside
!--- IKE Policy Configuration. isakmp enable outside
isakmp identity address
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption des
```

```
isakmp policy 10 hash md5
isakmp policy 10 group 2
isakmp policy 10 lifetime 86400
!--- IPsec group configuration for VPN Client. vpngroup
vpn3000 address-pool ippool
vpngroup vpn3000 dns-server 10.1.1.2
vpngroup vpn3000 wins-server 10.1.1.2
vpngroup vpn3000 default-domain cisco.com
vpngroup vpn3000 idle-time 1800
vpngroup vpn3000 password ********
telnet timeout 5
ssh timeout 5
terminal width 80
Cryptochecksum:3f9e31533911b8a6bb5c0f06900c2dbc
: end
[OK]
pixfirewall(config)#
```

Cisco VPN Client 3.5 para Windows

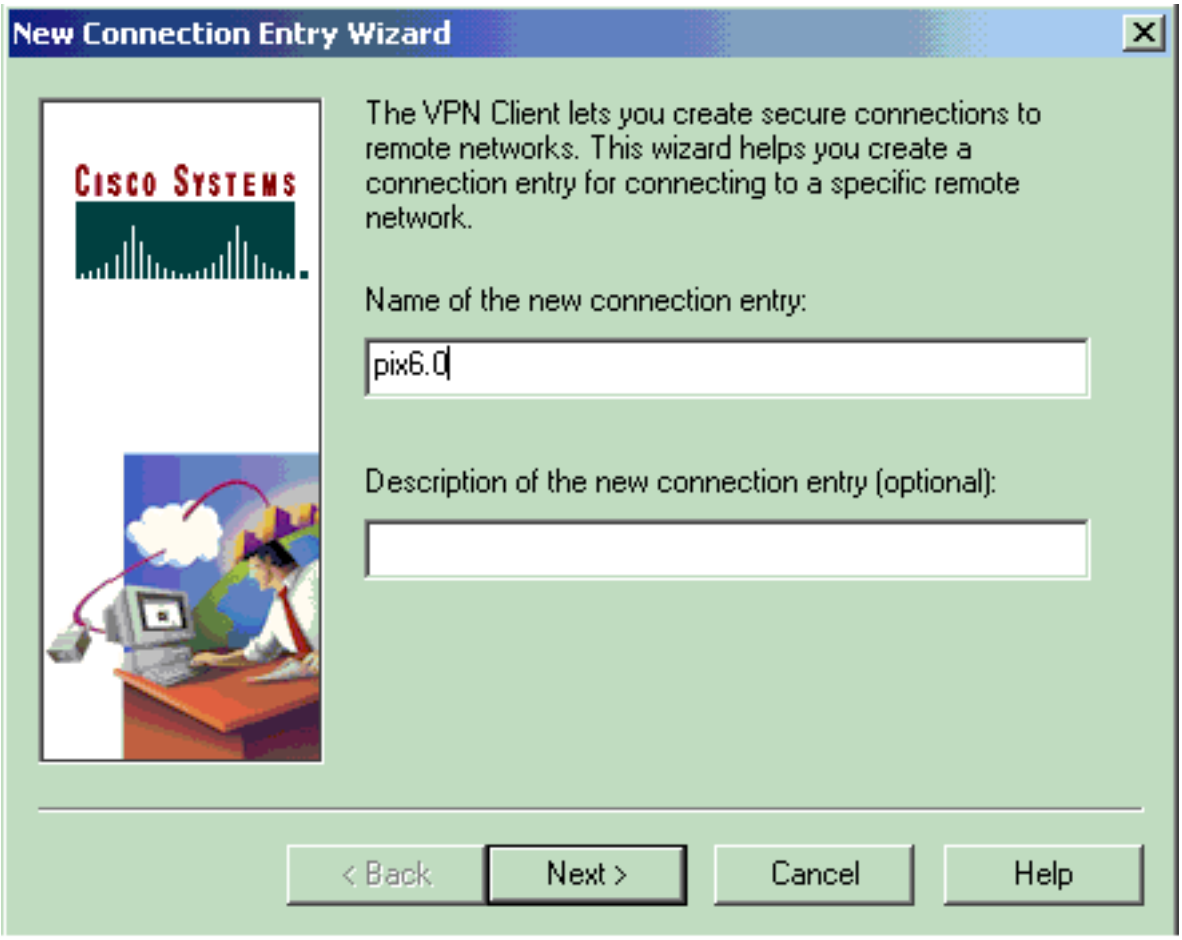
Esta sección explica cómo configurar Cisco VPN Client 3.5 para Windows.

1. Inicie VPN Client y haga clic en **New** para crear una nueva conexión.

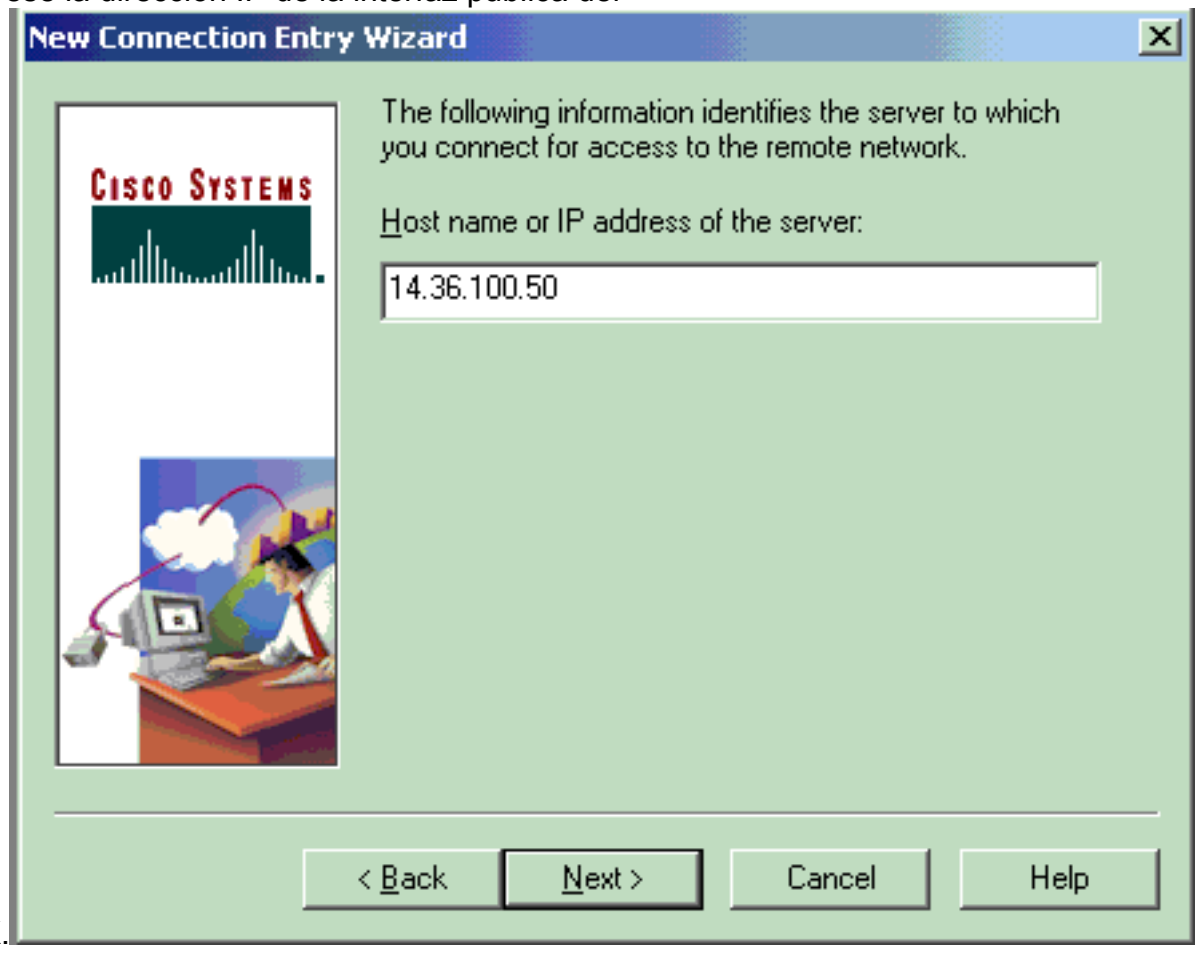


2. En la casilla Connection Entry (Entrada de conexión), asigne un nombre a su

entrada.

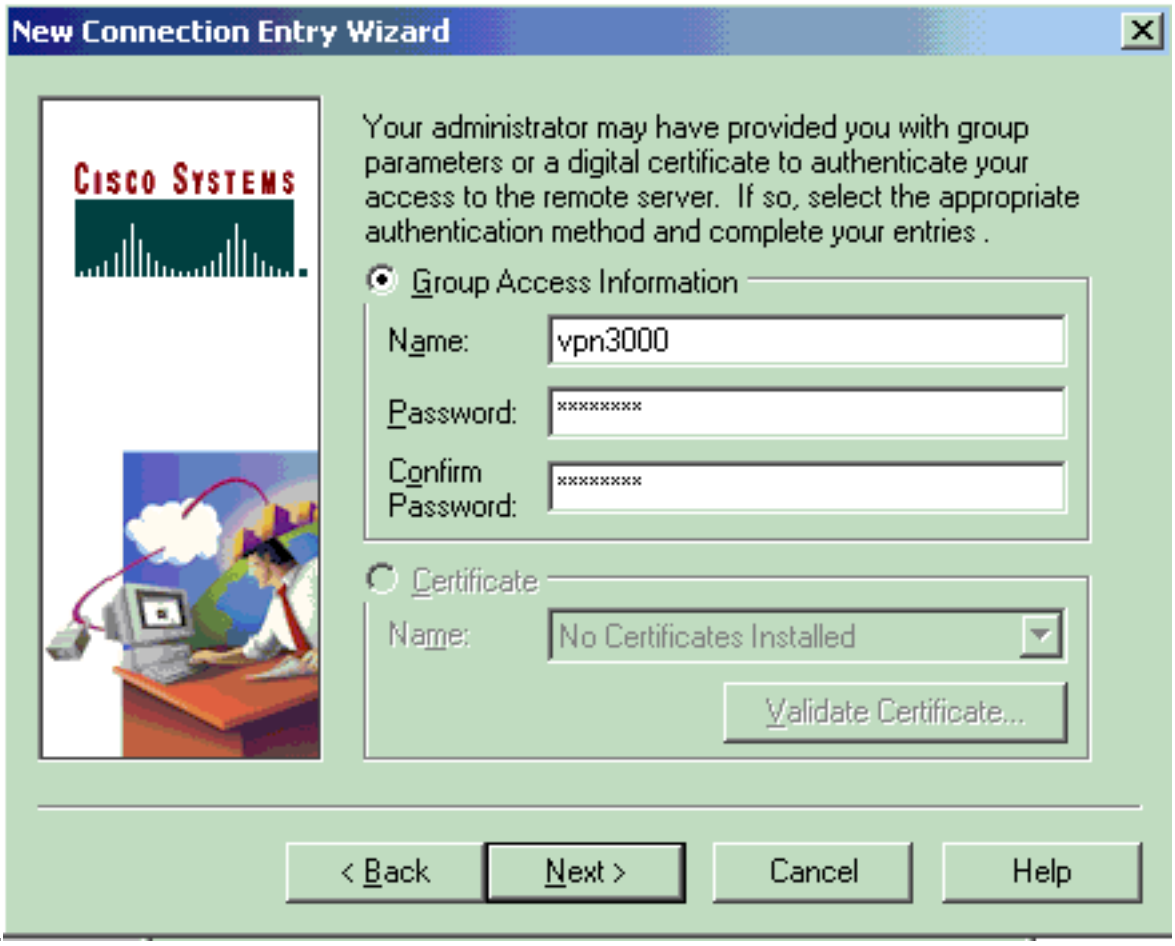


3. Ingrese la dirección IP de la interfaz pública del



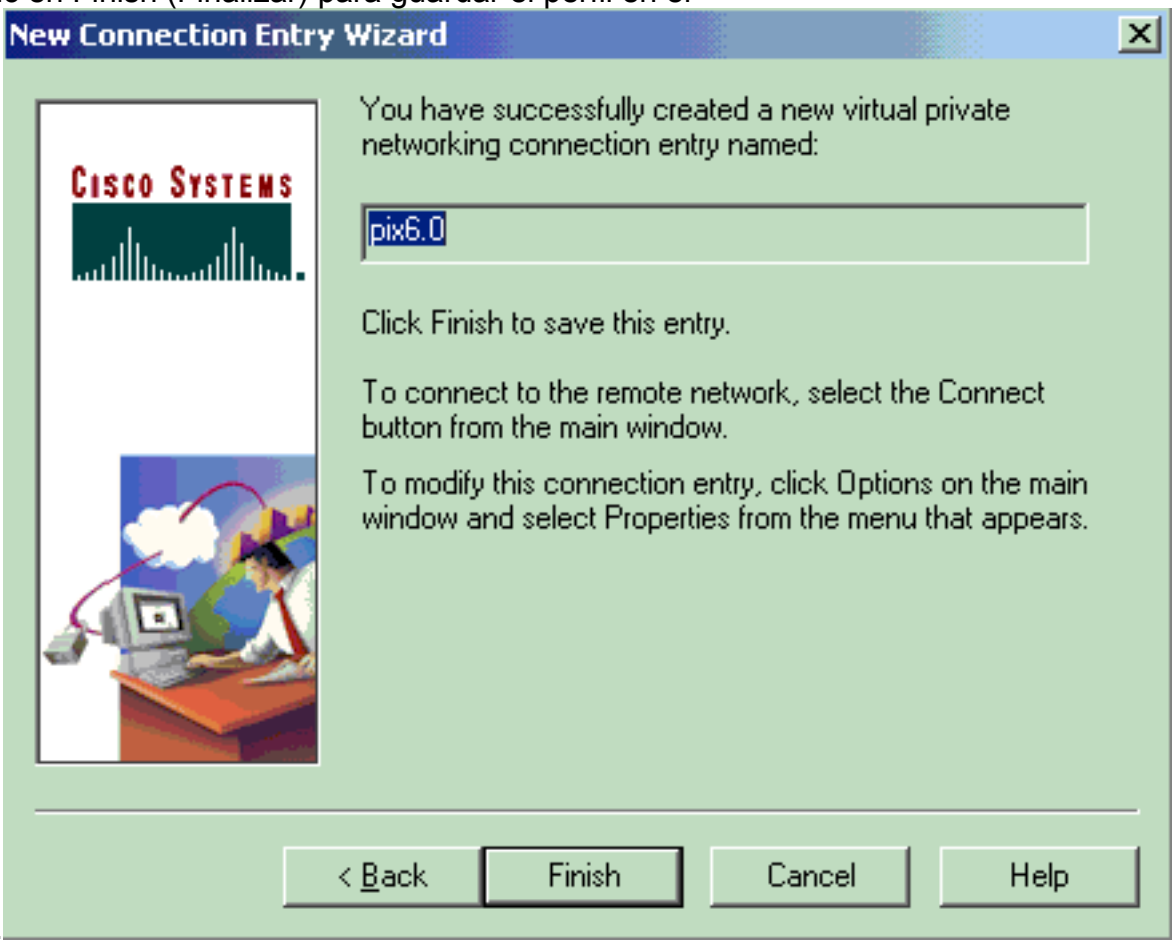
PIX.

4. En **Información de acceso de grupo**, ingrese el nombre de grupo y la contraseña de



grupo.

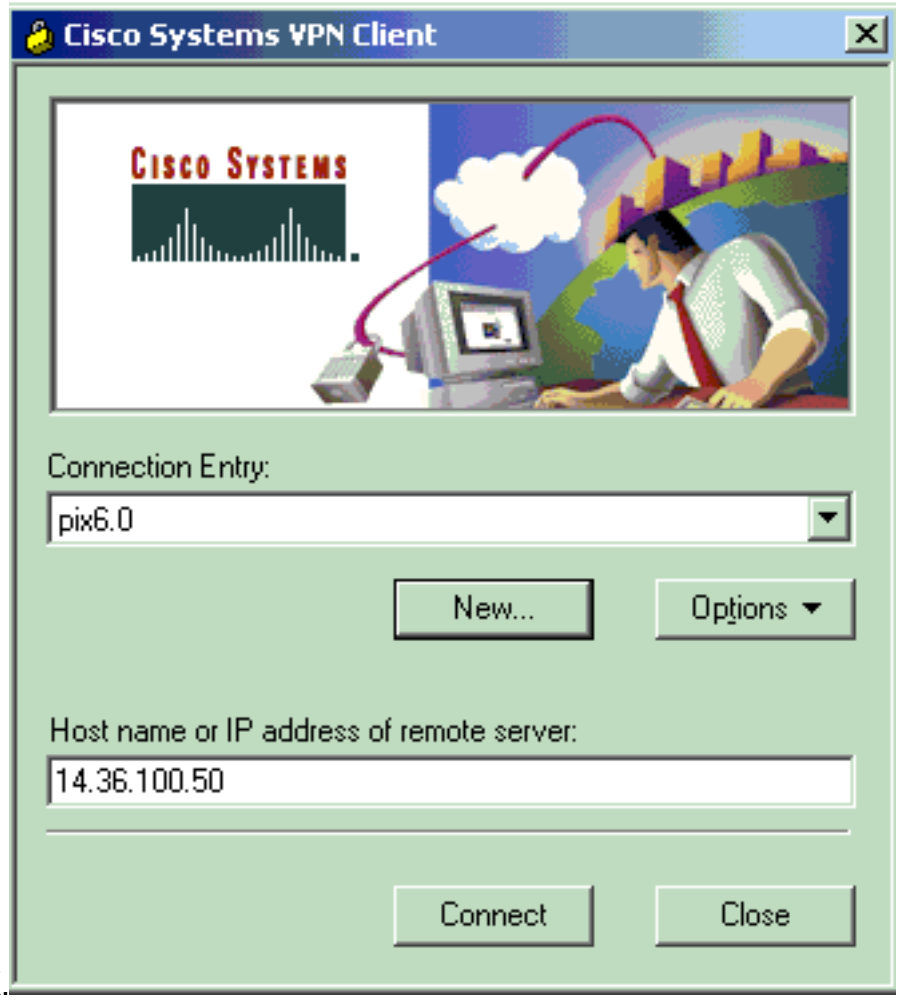
5. Haga clic en Finish (Finalizar) para guardar el perfil en el



registro.

6. Haga clic en Connect (Conectar) para conectar con el

PIX.

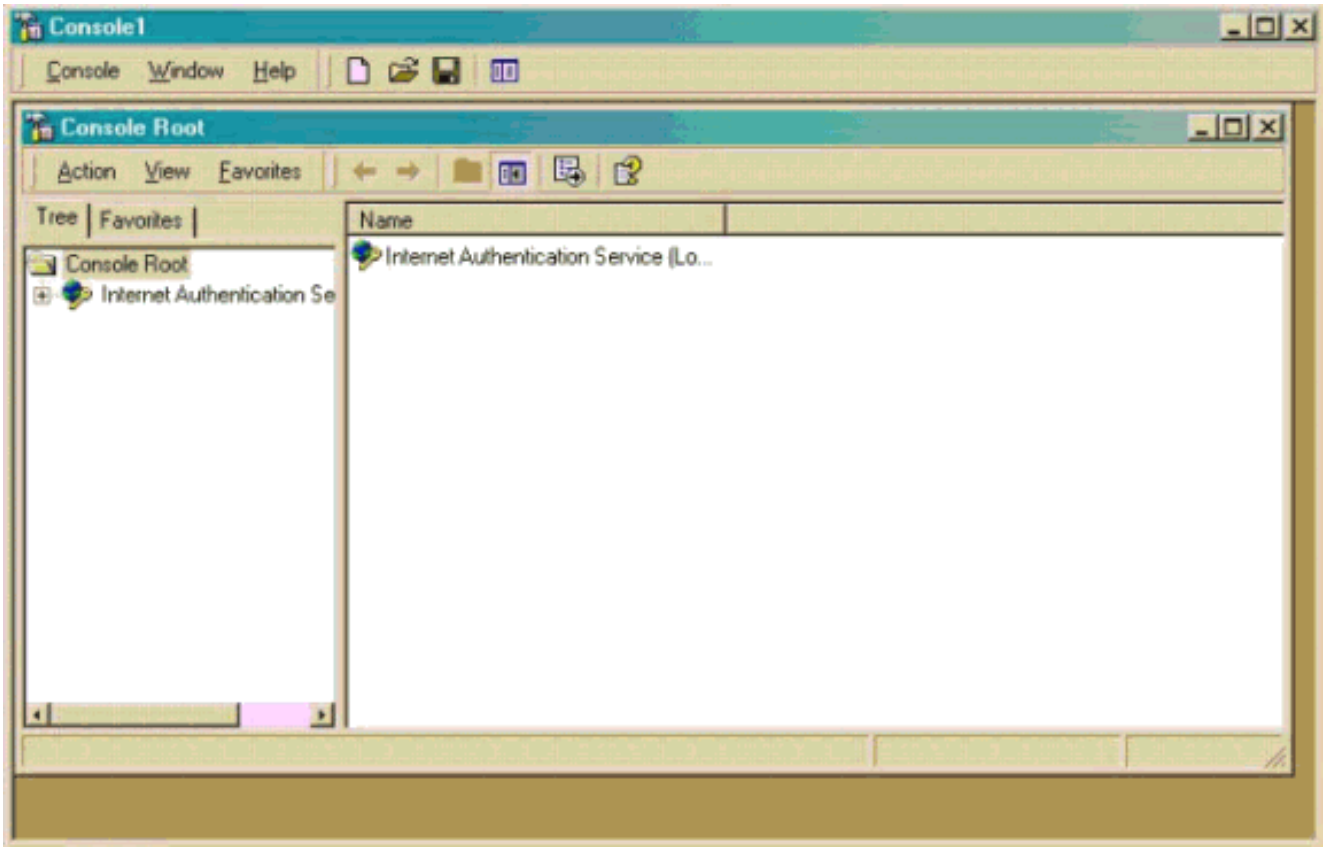


Microsoft Windows 2000 Server con IAS

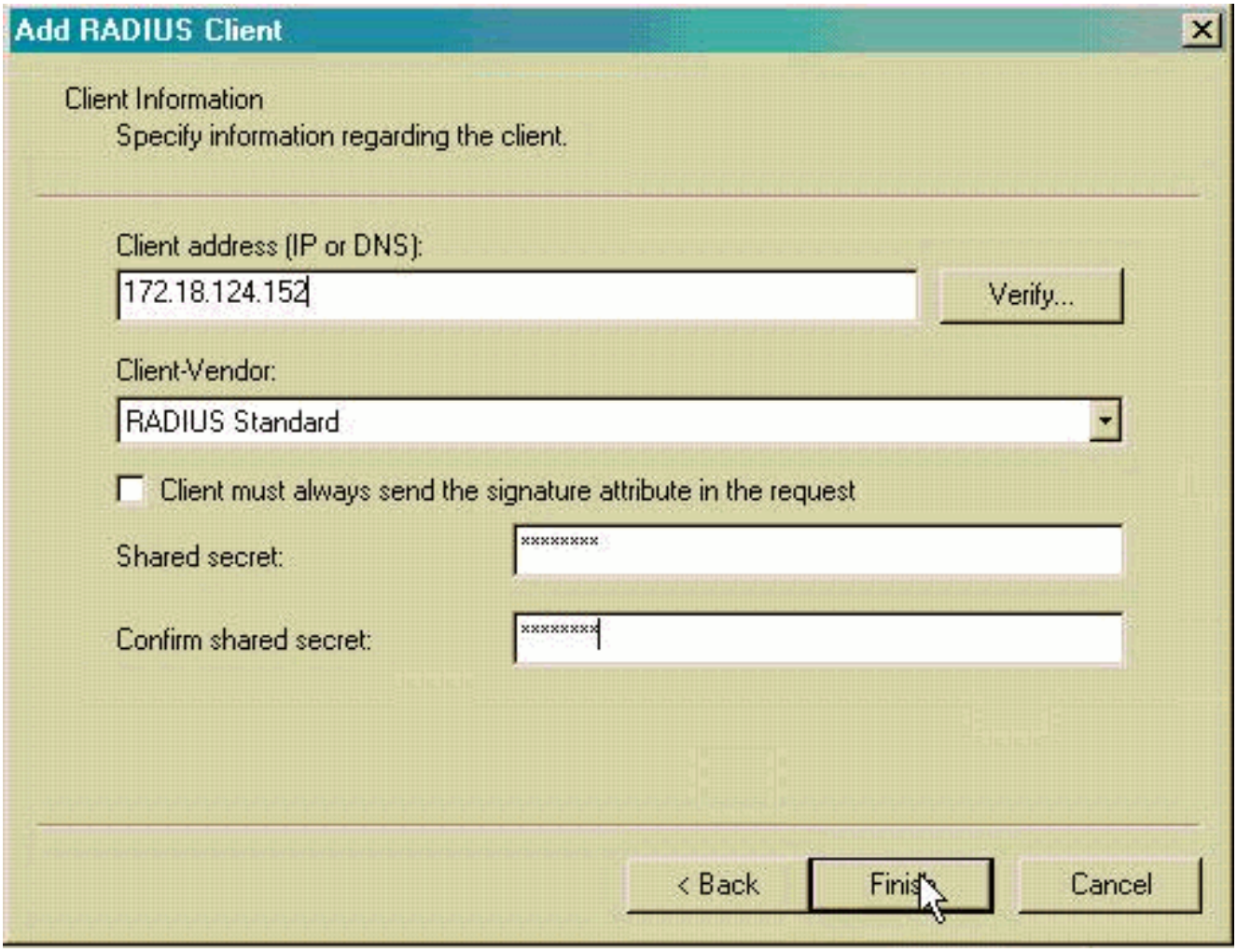
Complete estos pasos para configurar el servidor de Microsoft Windows 2000 con IAS. Se trata de una configuración muy básica para utilizar un servidor IAS de Windows 2000 para la autenticación RADIUS de los usuarios de VPN. Si necesita un diseño más complejo, póngase en contacto con Microsoft para obtener asistencia.

Nota: Estos pasos suponen que IAS ya se ha instalado en la máquina local. De lo contrario, agregue el IAS a través del **Control Panel > Add/Remove Programs**.

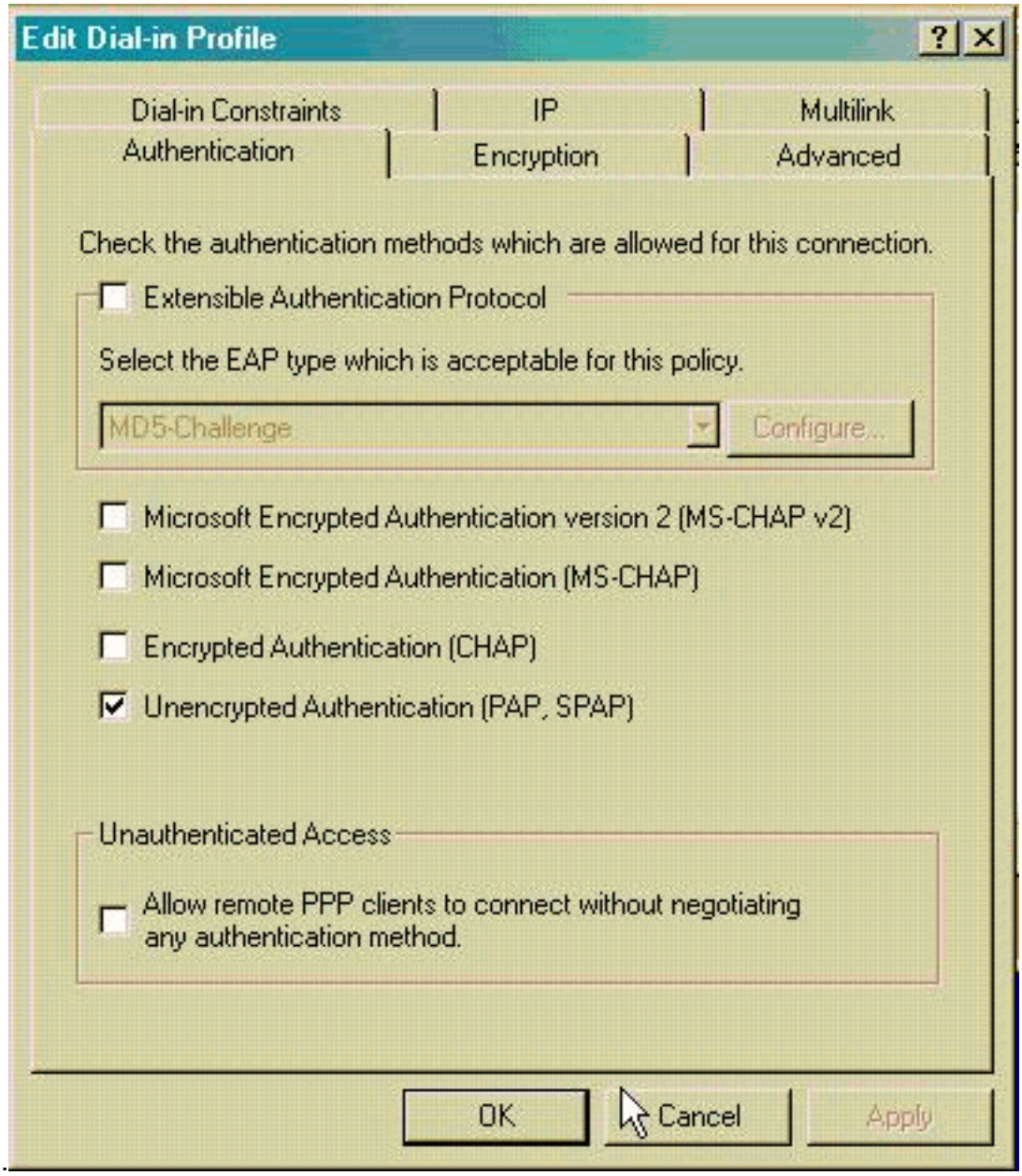
1. Inicie Microsoft Management Console. Elija **Inicio > Ejecutar** y escriba **mmc.** Luego haga clic en OK (Aceptar).
2. Elija **Console > Add Remove Snap-In....** para agregar el servicio IAS a esta consola.
3. Haga clic en **Agregar** para iniciar una nueva ventana con todos los complementos independientes disponibles. Haga clic en **Internet Authentication Service (IAS)** y haga clic en **Add**.
4. Asegúrese de que **Local Computer** esté seleccionado y haga clic en **Finish**. A continuación, haga clic en **Cerrar**.
5. Observe que se ha agregado IAS. Haga clic en **Aceptar** para ver que se ha agregado a la raíz de la
consola.



6. Amplíe el **Servicio de Autenticación de Internet** y haga clic con el botón derecho en **Clientes**. Haga clic en **Nuevo cliente** e introduzca un nombre. La elección del nombre no importa; será lo que verá en esta vista. Asegúrese de seleccionar **RADIUS** y haga clic en **Next**.
7. Rellene la **dirección del cliente** con la dirección de la interfaz PIX a la que está conectado el servidor IAS. Asegúrese de seleccionar **RADIUS Standard** y agregar el secreto compartido para que coincida con el comando que ingresó en el PIX:
   ```
   aaa-server partnerauth (inside) host 172.18.124.196 cisco123 timeout 5
   ```
   Nota: En este ejemplo, "cisco123" es el secreto compartido.

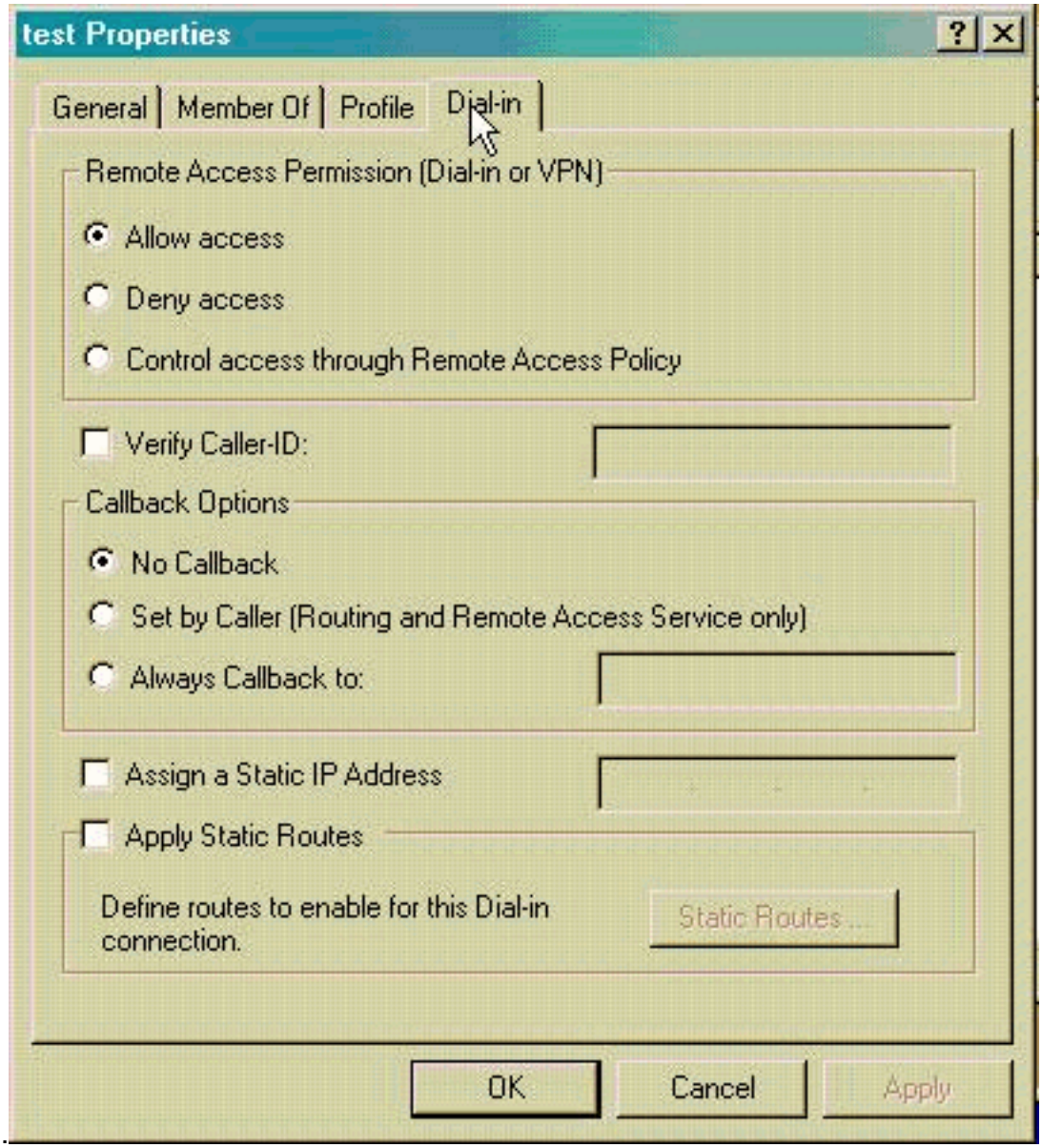


8. Haga clic en **Finalizar** para volver a la raíz de la consola.
9. Haga clic en **Políticas de acceso remoto** en el panel izquierdo y haga doble clic en la política denominada **Permitir acceso si el permiso de marcado está habilitado**.
10. Haga clic en **Editar perfil** y vaya a la ficha Autenticación. En **Métodos de Autenticación**, asegúrese de que sólo **esté marcada la autenticación no cifrada (PAP, SPAP)**.**Nota:** El VPN Client sólo puede utilizar este método para la



autenticación.

11. Haga clic en **Aplicar** y luego **Aceptar** dos veces.
12. Para modificar los usuarios para permitir la conexión, elija **Console > Add/Remove Snap-in**. Haga clic en **Agregar** y, a continuación, seleccione el **complemento Usuarios y grupos locales**. Haga clic en Add (Agregar). Asegúrese de seleccionar **Local Computer** y haga clic en **Finish**. Click OK.
13. Expanda **Usuario y grupos locales** y haga clic en la carpeta **Usuarios** en el panel izquierdo. En el panel derecho, haga doble clic en el usuario al que desea permitir el acceso.
14. Haga clic en la ficha Marcar y seleccione **Permitir acceso** en **Permiso de acceso remoto (Marcado o**



VPN).

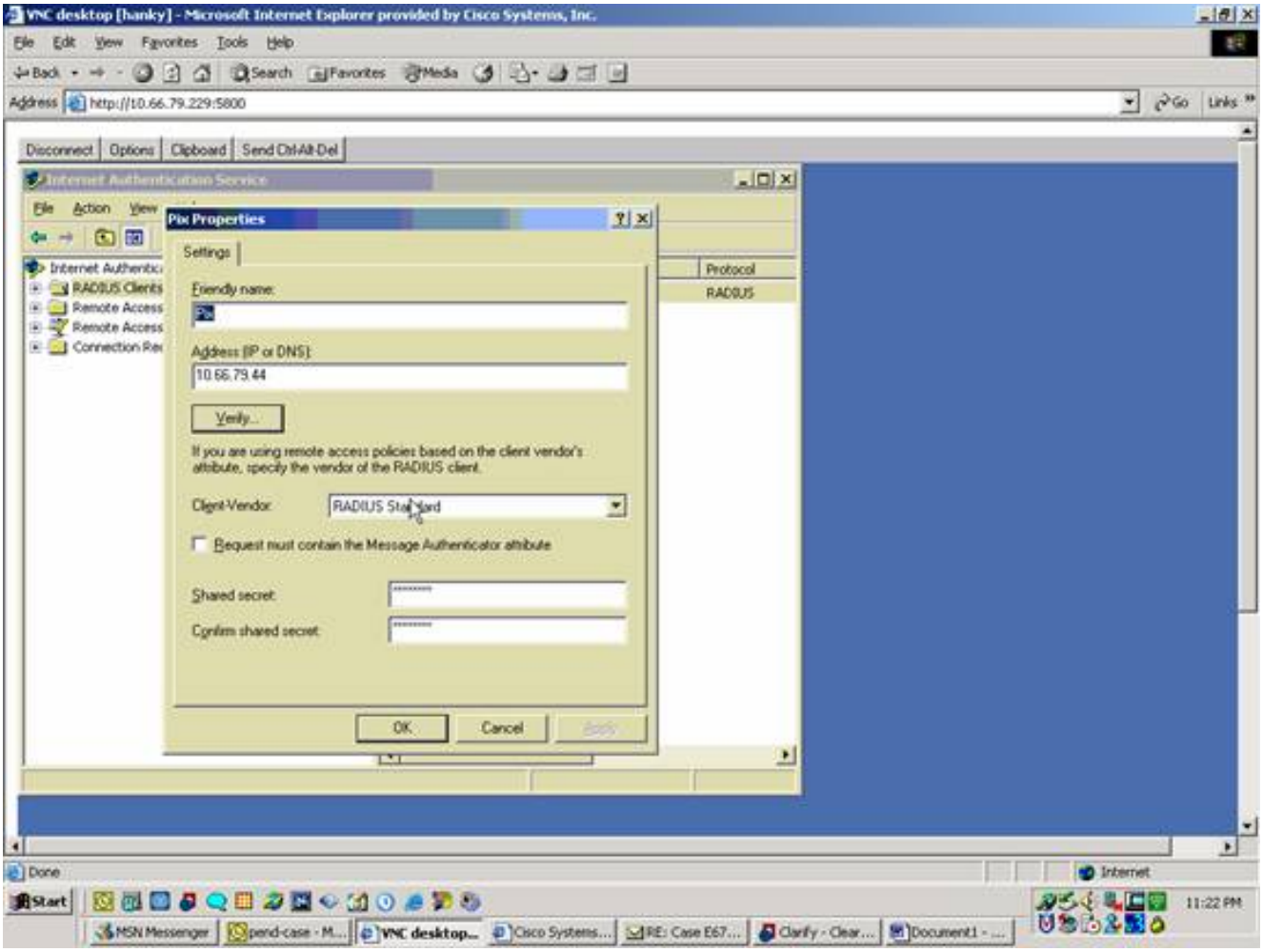
15. Haga clic en **Aplicar** y **Aceptar** para completar la acción. Puede cerrar la pantalla **Administración de la consola** y guardar la sesión, si lo desea.
16. Los usuarios que modificó ahora deberían poder acceder al PIX con el VPN Client 3.5. Tenga en cuenta que el servidor IAS sólo autentica la información del usuario. El PIX todavía hace la autenticación de grupo.

Microsoft Windows 2003 Server con IAS

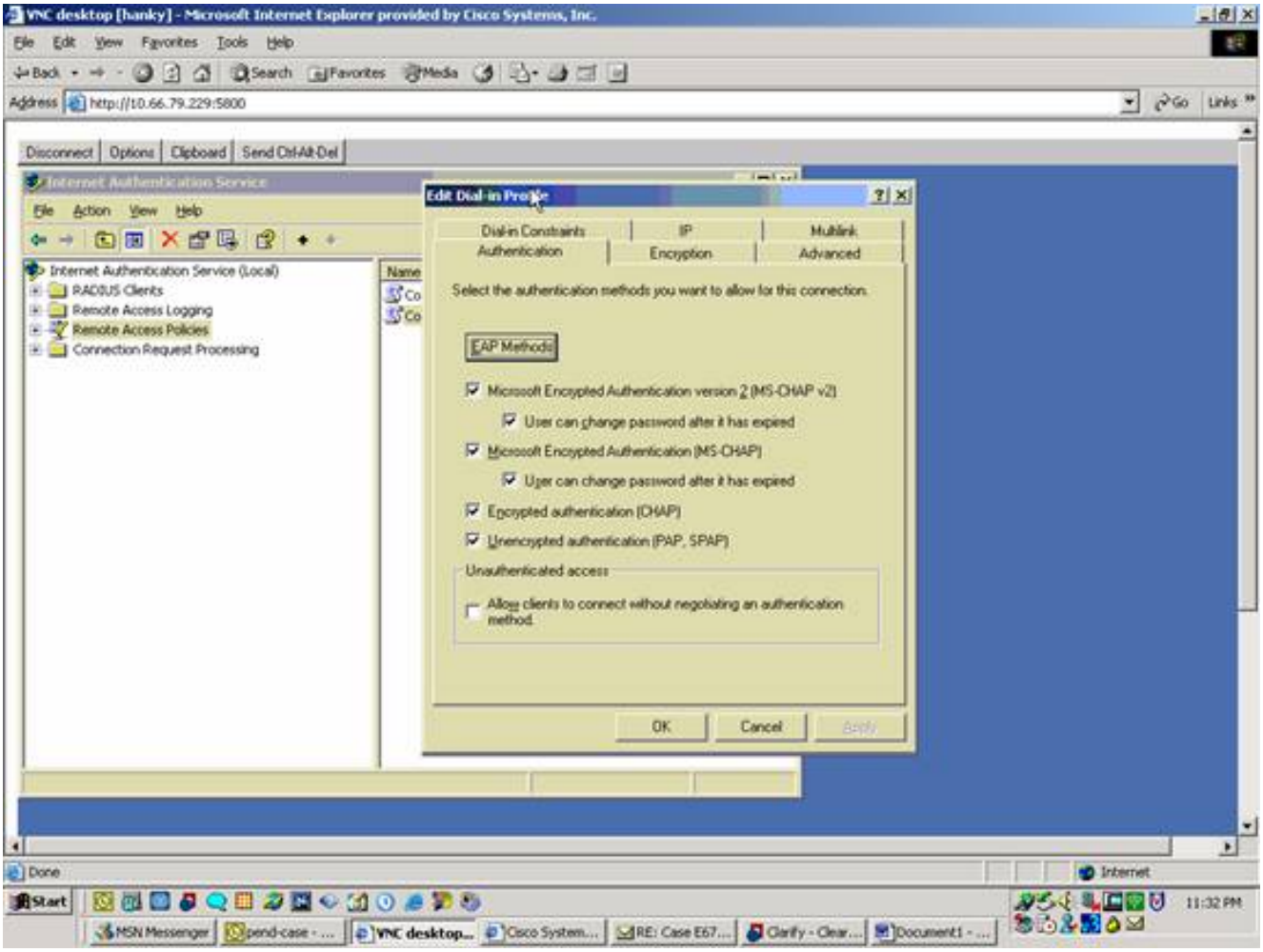
Complete estos pasos para configurar el servidor de Microsoft Windows 2003 con IAS.

Nota: Estos pasos suponen que IAS ya se ha instalado en la máquina local. De lo contrario, agregue el IAS a través del **Control Panel > Add/Remove Programs**.

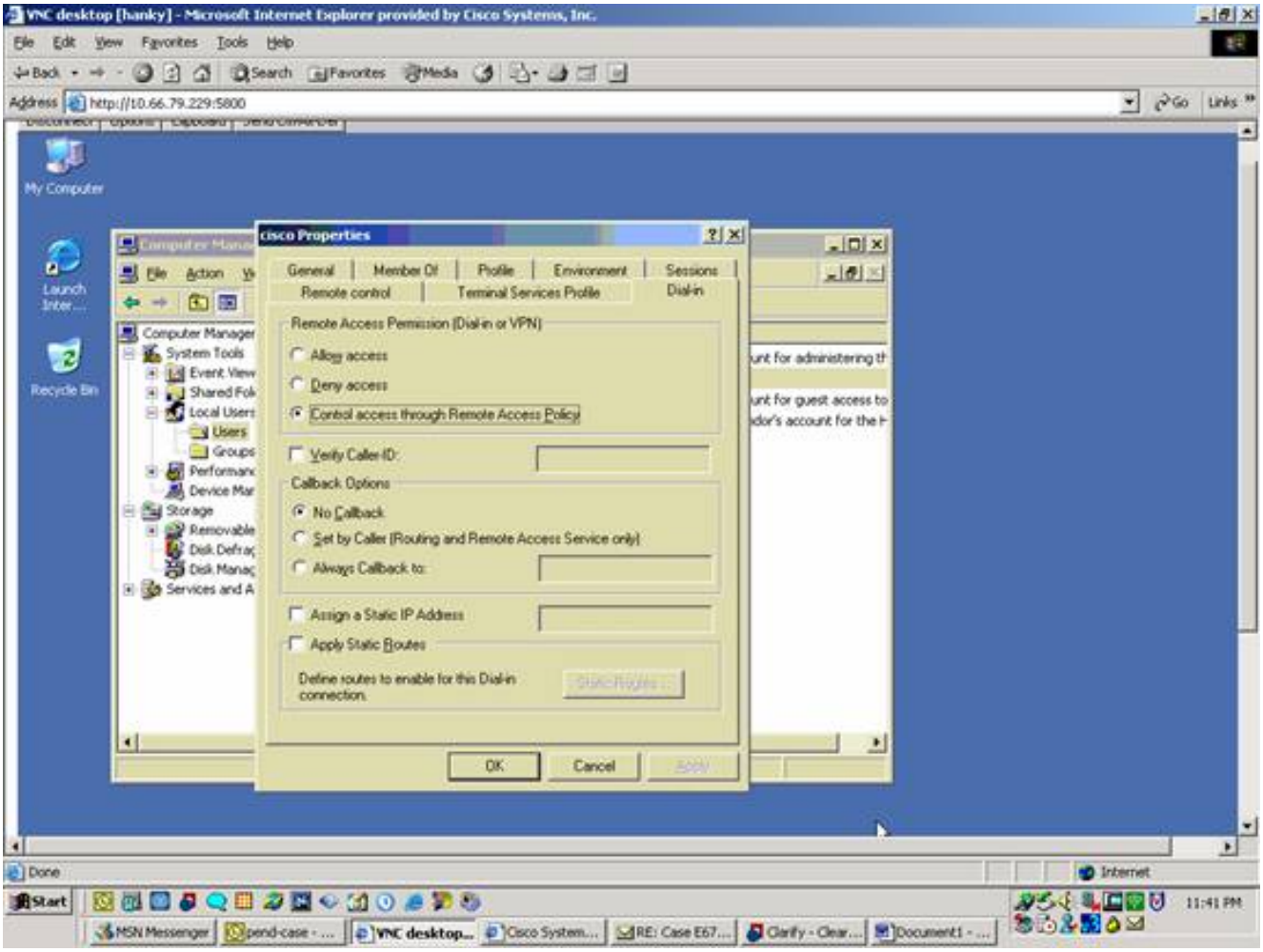
1. Elija **Administrative Tools > Internet Authentication Service** y haga clic con el botón derecho en **RADIUS Client** para agregar un nuevo cliente RADIUS. Luego de escribir la información del cliente, haga clic en **OK**.Este ejemplo muestra un cliente denominado “Pix” con una dirección IP de 10.66.79.44. Client-Vendor se establece en RADIUS Standard y el secreto compartido es
"cisco123".



2. Vaya a **Políticas de acceso remoto**, haga clic con el botón derecho en **Conexiones a otros servidores de acceso** y seleccione **Propiedades**.
3. Asegúrese de que la opción Grant Remote Access Permissions esté seleccionada.
4. Haga clic en **Editar perfil** y verifique estas configuraciones.En la pestaña Autentication, marque **Unencrypted authentication (PAP, SPAP)**.En la pestaña Encryption, asegúrese de de que esté seleccionada la opción No Encryption .Haga clic en **Aceptar** cuando haya terminado.



5. Agregue un usuario a la cuenta de equipo local. Para hacer esto, elija **Administrative Tools > Computer Management > System Tools > Local Users and Groups.**. Haga clic con el botón derecho en **Usuarios** y seleccione **Nuevos Usuarios**.
6. Agregue el usuario con la contraseña de Cisco "cisco123" y verifique esta información de perfil.En la pestaña General, asegúrese de que esté seleccionada la opción Password Never Expired en vez de la opción User Must Change Password.En la ficha Marcar, seleccione la opción **Permitir acceso** (o deje la configuración predeterminada Control access a través de Remote Access Policy).Haga clic en **Aceptar** cuando haya terminado.



Verificación

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 de seguridad (SA) IKE actuales en un par.
- **show crypto ipsec sa**: muestra la configuración utilizada por las asociaciones de seguridad actuales.

Troubleshoot

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración. Para obtener información adicional, consulte Solución de Problemas de PIX para Pasar el Tráfico de Datos en un Túnel IPSec Establecido.

Comandos para resolución de problemas

Ciertos comandos son soportados por la herramienta Output Interpreter Tool (clientes registrados solamente), que le permite ver un análisis de la salida del comando show.

Nota: Consulte Información Importante sobre Comandos Debug antes de utilizar los comandos **debug** y consulte Solución de Problemas de Seguridad IP - Introducción y Uso de Comandos debug.

- **debug crypto ipsec**: vea las negociaciones IPSec de la fase 2.
- **debug crypto isakmp**: vea las negociaciones ISAKMP de la fase 1.
- **debug crypto engine**: vea el tráfico cifrado.

Ejemplo de resultado del comando debug

- Firewall PIX
- VPN Client 3.5 para Windows

Firewall PIX

```
pixfirewall(config)#
crypto_isakmp_process_block: src 14.36.100.55, dest 14.36.100.50
VPN Peer: ISAKMP: Added new peer: ip:14.36.100.55 Total VPN Peers:1
VPN Peer: ISAKMP: Peer ip:14.36.100.55 Ref cnt incremented to:1
   Total VPN Peers:1
OAK_AG exchange
ISAKMP (0): processing SA payload. message ID = 0

ISAKMP (0): Checking ISAKMP transform 1 against priority 10 policy
ISAKMP:      encryption 3DES-CBC
ISAKMP:      hash SHA
ISAKMP:      default group 2
ISAKMP:      extended auth pre-share
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 2 against priority 10 policy
ISAKMP:      encryption 3DES-CBC
ISAKMP:      hash MD5
ISAKMP:      default group 2
ISAKMP:      extended auth pre-share
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 3 against priority 10 policy
ISAKMP:      encryption 3DES-CBC
ISAKMP:      hash SHA
ISAKMP:      default group 2
ISAKMP:      auth pre-share
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 4 against priority 10 policy
ISAKMP:      encryption 3DES-CBC
ISAKMP:      hash MD5
ISAKMP:      default group 2
ISAKMP:      auth pre-share
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 5 against priority 10 policy
ISAKMP:      encryption DES-CBC
ISAKMP:      hash SHA
```

```
ISAKMP:      default group 2
ISAKMP:      extended auth pre-share
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 6 against priority 10 policy
ISAKMP:      encryption DES-CBC
ISAKMP:      hash MD5
ISAKMP:      default group 2
ISAKMP:      extended auth pre-share
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are acceptable. Next payload is 3
ISAKMP (0): processing KE payload. message ID = 0

ISAKMP (0): processing NONCE payload. message ID = 0

ISAKMP (0): processing ID payload. message ID = 0
ISAKMP (0): processing vendor id payload

ISAKMP (0): processing vendor id payload

ISAKMP (0): remote peer supports dead peer detection

ISAKMP (0): processing vendor id payload

ISAKMP (0): speaking to a Unity client

ISAKMP: Created a peer node for 14.36.100.55
ISAKMP (0): ID payload
        next-payload : 10
        type         : 1
        protocol     : 17
        port         : 500
        length       : 8
ISAKMP (0): Total payload length: 12
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 14.36.100.55, dest 14.36.100.50
OAK_AG exchange
ISAKMP (0): processing HASH payload. message ID = 0
ISAKMP (0): processing NOTIFY payload 24578 protocol 1
        spi 0, message ID = 0
ISAKMP (0): processing notify INITIAL_CONTACTIPSEC(key_engine): got
   a queue event...
IPSEC(key_engine_delete_sas): rec'd delete notify from ISAKMP
IPSEC(key_engine_delete_sas): delete all SAs shared with 14.36.100.55

ISAKMP (0): SA has been authenticated
return status is IKMP_NO_ERROR
ISAKMP/xauth: request attribute XAUTH_TYPE
ISAKMP/xauth: request attribute XAUTH_USER_NAME
ISAKMP/xauth: request attribute XAUTH_USER_PASSWORD
ISAKMP (0:0): initiating peer config to 14.36.100.55. ID = 3870616596
   (0xe6b4ec14)
crypto_isakmp_process_block: src 14.36.100.55, dest 14.36.100.50
ISAKMP_TRANSACTION exchange
ISAKMP (0:0): processing transaction payload from 14.36.100.55.
   message ID = 84
ISAKMP: Config payload CFG_REPLY
return status is IKMP_ERR_NO_RETRANS
ISAKMP (0:0): initiating peer config to 14.36.100.55. ID = 3612718114
   (0xd755b422)
crypto_isakmp_process_block: src 14.36.100.55, dest 14.36.100.50
ISAKMP_TRANSACTION exchange
```

```
ISAKMP (0:0): processing transaction payload from 14.36.100.55.
   message ID = 60
ISAKMP: Config payload CFG_ACK
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 14.36.100.55, dest 14.36.100.50
ISAKMP_TRANSACTION exchange
ISAKMP (0:0): processing transaction payload from 14.36.100.55.
   message ID = 0
ISAKMP: Config payload CFG_REQUEST
ISAKMP (0:0): checking request:
ISAKMP: attribute    IP4_ADDRESS (1)
ISAKMP: attribute    IP4_NETMASK (2)
ISAKMP: attribute    IP4_DNS (3)
ISAKMP: attribute    IP4_NBNS (4)
ISAKMP: attribute    ADDRESS_EXPIRY (5)
        Unsupported Attr: 5
ISAKMP: attribute    APPLICATION_VERSION (7)
        Unsupported Attr: 7
ISAKMP: attribute    UNKNOWN (28672)
        Unsupported Attr: 28672
ISAKMP: attribute    UNKNOWN (28673)
        Unsupported Attr: 28673
ISAKMP: attribute    UNKNOWN (28674)
ISAKMP: attribute    UNKNOWN (28676)
ISAKMP: attribute    UNKNOWN (28679)
        Unsupported Attr: 28679
ISAKMP: attribute    UNKNOWN (28680)
        Unsupported Attr: 28680
ISAKMP: attribute    UNKNOWN (28677)
        Unsupported Attr: 28677
ISAKMP (0:0): responding to peer config from 14.36.100.55.
   ID = 3979868003
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 14.36.100.55, dest 14.36.100.50
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID = 1527320241

ISAKMP : Checking IPSec proposal 1

ISAKMP: transform 1, ESP_3DES
ISAKMP:   attributes in transform:
ISAKMP:      authenticator is HMAC-MD5
ISAKMP:      encaps is 1
ISAKMP:      SA life type in seconds
ISAKMP:      SA life duration (VPI) of  0x0 0x20 0xc4 0x9b
   IPSEC(validate_proposal): transform proposal (prot 3, trans
3, hmac_alg 1) not supported

ISAKMP (0): atts not acceptable. Next payload is 0
ISAKMP (0): skipping next ANDed proposal (1)
ISAKMP : Checking IPSec proposal 2

ISAKMP: transform 1, ESP_3DES
ISAKMP:   attributes in transform:
ISAKMP:      authenticator is HMAC-SHA
ISAKMP:      encaps is 1
ISAKMP:      SA life type in seconds
ISAKMP:      SA life duration (VPI) of  0x0 0x20 0xc4 0x9b
   IPSEC(validate_proposal): transform proposal (prot 3, trans
3, hmac_alg 2) not supported

ISAKMP (0): atts not acceptable. Next payload is 0
```

```
ISAKMP (0): skipping next ANDed proposal (2)
ISAKMP : Checking IPSec proposal 3

ISAKMP: transform 1, ESP_3DES
ISAKMP:   attributes in transform:
ISAKMP:      authenticator is HMAC-MD5
ISAKMP:      encaps is 1
ISAKMP:      SA life type in seconds
ISAKMP:      SA life duration (VPI) of  0x0 0x20 0xc4 0x9b
   IPSEC(validate_proposal): transform proposal (prot 3, trans
3, hmac_alg 1) not supported

ISAKMP (0): atts not acceptable. Next payload is 0
ISAKMP : Checking IPSec proposal 4

ISAKMP: transform 1, ESP_3DES
ISAKMP:   attributes in transform:
ISAKMP:      authenticator is HMAC-SHA
ISAKMP:      encaps is 1
ISAKMP:      SA life type in seconds
ISAKMP:      SA life duration (VPI) of  0x0 0x20 0xc4 0x9b
   IPSEC(validate_proposal): transform proposal (prot 3, trans
3, hmac_alg 2) not supported

ISAKMP (0): atts not acceptable. Next payload is 0
ISAKMP : Checking IPSec proposal 5

ISAKMP: transform 1, ESP_DES
ISAKMP:   attributes in transform:
ISAKMP:      authenticator is HMAC-MD5
ISAKMP:      encaps is 1
ISAKMP:      SA life type in seconds
ISAKMP:      SA life duration (VPI) of  0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are acceptable.
ISAKMP (0): bad SPI size of 2 octets!
ISAKMP : Checking IPSec proposal 6

ISAKMP: transform 1, ESP_DES
ISAKMP:   attributes in transform:
ISAKMP:      authenticator is HMAC-SHA
ISAKMP:      encaps is 1
ISAKMP:      SA life type in seconds
ISAKMP:      SA life duration (VPI) of  0x0 0x20 0xc4 0x9b
   IPSEC(validate_proposal): transform proposal (prot 3, trans
2, hmac_alg 2) not supported

ISAKMP (0): atts not acceptable. Next payload is 0
ISAKMP (0): skipping next ANDed proposal (6)
ISAKMP : Checking IPSec proposal 7

ISAKMP: transform 1, ESP_DES
ISAKMP:   attributes in transform:
ISAKMP:      authenticator is HMAC-MD5
ISAKMP:      encaps is 1
ISAKMP:      SA life type in seconds
ISAKMP:      SA life duration (VPI) of  0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are acceptable.IPSEC(validate_proposal_request):
   proposal part #1,
  (key eng. msg.) dest= 14.36.100.50, src= 14.36.100.55,
    dest_proxy= 14.36.100.50/255.255.255.255/0/0 (type=1),
    src_proxy= 10.1.2.1/255.255.255.255/0/0 (type=1),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
```

```
ISAKMP (0): processing NONCE payload. message ID = 1527320241

ISAKMP (0): processing ID payload. message ID = 1527320241
ISAKMP (0): ID_IPV4_ADDR src 10.1.2.1 prot 0 port 0
ISAKMP (0): processing ID payload. message ID = 1527320241
ISAKMP (0): ID_IPV4_ADDR dst 14.36.100.50 prot 0 port
   0IPSEC(key_engine): got a queue event...
IPSEC(spi_response): getting spi 0xf39c2217(4087095831) for SA
        from    14.36.100.55 to    14.36.100.50 for prot 3

return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 14.36.100.55, dest 14.36.100.50
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID = 3487980779

ISAKMP : Checking IPSec proposal 1

ISAKMP: transform 1, ESP_3DES
ISAKMP:   attributes in transform:
ISAKMP:      authenticator is HMAC-MD5
crypto_isakmp_process_block: src 14.36.100.55, dest 14.36.100.50
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_AUTH_AWAIT
ISAKMP (0): Creating IPSec SAs
        inbound SA from    14.36.100.55 to    14.36.100.50
             (proxy        10.1.2.1 to    14.36.100.50)
        has spi 4087095831 and conn_id 1 and flags 4
        lifetime of 2147483 seconds
        outbound SA from    14.36.100.50 to    14.36.100.55
             (proxy    14.36.100.50 to        10.1.2.1)
        has spi 1929305241 and conn_id 2 and flags 4
        lifetime of 2147483 secondsIPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 14.36.100.50, src= 14.36.100.55,
    dest_proxy= 14.36.100.50/0.0.0.0/0/0 (type=1),
    src_proxy= 10.1.2.1/0.0.0.0/0/0 (type=1),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 2147483s and 0kb,
    spi= 0xf39c2217(4087095831), conn_id= 1, keysize= 0, flags= 0x4
IPSEC(initialize_sas): ,
  (key eng. msg.) src= 14.36.100.50, dest= 14.36.100.55,
    src_proxy= 14.36.100.50/0.0.0.0/0/0 (type=1),
    dest_proxy= 10.1.2.1/0.0.0.0/0/0 (type=1),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 2147483s and 0kb,
    spi= 0x72fedc99(1929305241), conn_id= 2, keysize= 0, flags= 0x4

VPN Peer: IPSEC: Peer ip:14.36.100.55 Ref cnt incremented to:2
   Total VPN Peers:1
VPN Peer: IPSEC: Peer ip:14.36.100.55 Ref cnt incremented to:3
   Total VPN Peers:1
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 14.36.100.55, dest 14.36.100.50
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_AUTH_AWAIT
ISAKMP (0): Creating IPSec SAs
        inbound SA from    14.36.100.55 to    14.36.100.50
             (proxy        10.1.2.1 to         0.0.0.0)
        has spi 1791135440 and conn_id 3 and flags 4
```

```
        lifetime of 2147483 seconds
        outbound SA from    14.36.100.50 to    14.36.100.55
             (proxy         0.0.0.0 to        10.1.2.1)
        has spi 173725574 and conn_id 4 and flags 4
        lifetime of 2147483 secondsIPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 14.36.100.50, src= 14.36.100.55,
    dest_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
    src_proxy= 10.1.2.1/0.0.0.0/0/0 (type=1),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 2147483s and 0kb,
    spi= 0x6ac28ed0(1791135440), conn_id= 3, keysize= 0, flags= 0x4
IPSEC(initialize_sas): ,
  (key eng. msg.) src= 14.36.100.50, dest= 14.36.100.55,
    src_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
    dest_proxy= 10.1.2.1/0.0.0.0/0/0 (type=1),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 2147483s and 0kb,
    spi= 0xa5ad786(173725574), conn_id= 4, keysize= 0, flags= 0x4

VPN Peer: IPSEC: Peer ip:14.36.100.55 Ref cnt incremented to:4
   Total VPN Peers:1
VPN Peer: IPSEC: Peer ip:14.36.100.55 Ref cnt incremented to:5
   Total VPN Peers:1
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 14.36.100.55, dest 14.36.100.50
ISAKMP (0): processing NOTIFY payload 36136 protocol 1
        spi 0, message ID = 3443334051
ISAMKP (0): received DPD_R_U_THERE from peer 14.36.100.55
ISAKMP (0): sending NOTIFY message 36137 protocol 1
return status is IKMP_NO_ERR_NO_TRANS
```

VPN Client 3.5 para Windows

```
193    19:00:56.073  01/24/02  Sev=Info/6       DIALER/0x63300002
Initiating connection.

194    19:00:56.073  01/24/02  Sev=Info/4       CM/0x63100002
Begin connection process

195    19:00:56.083  01/24/02  Sev=Info/4       CM/0x63100004
Establish secure connection using Ethernet

196    19:00:56.083  01/24/02  Sev=Info/4       CM/0x63100026
Attempt connection with server "14.36.100.50"

197    19:00:56.083  01/24/02  Sev=Info/6       IKE/0x6300003B
Attempting to establish a connection with 14.36.100.50.

198    19:00:56.124  01/24/02  Sev=Info/4       IKE/0x63000013
SENDING >>> ISAKMP OAK AG (SA, KE, NON, ID, VID, VID, VID)
to 14.36.100.50

199    19:00:56.774  01/24/02  Sev=Info/4       IPSEC/0x63700014
Deleted all keys

200    19:00:59.539  01/24/02  Sev=Info/5       IKE/0x6300002F
Received ISAKMP packet: peer = 14.36.100.50

201    19:00:59.539  01/24/02  Sev=Info/4       IKE/0x63000014
RECEIVING <<< ISAKMP OAK AG (SA, VID, VID, VID, KE, ID, NON, HASH)
from 14.36.100.50
```

```
202    19:00:59.539  01/24/02  Sev=Info/5       IKE/0x63000059
Vendor ID payload = 12F5F28C457168A9702D9FE274CC0100

203    19:00:59.539  01/24/02  Sev=Info/5       IKE/0x63000001
Peer is a Cisco-Unity compliant peer

204    19:00:59.539  01/24/02  Sev=Info/5       IKE/0x63000059
Vendor ID payload = AFCAD71368A1F1C96B8696FC77570100

205    19:00:59.539  01/24/02  Sev=Info/5       IKE/0x63000001
Peer supports DPD

206    19:00:59.539  01/24/02  Sev=Info/5       IKE/0x63000059
Vendor ID payload = 6D761DDC26ACECA1B0ED11FABBB860C4

207    19:00:59.569  01/24/02  Sev=Info/4       IKE/0x63000013
SENDING >>> ISAKMP OAK AG *(HASH, NOTIFY:STATUS_INITIAL_CONTACT)
to 14.36.100.50

208    19:00:59.569  01/24/02  Sev=Info/5       IKE/0x6300002F
Received ISAKMP packet: peer = 14.36.100.50

209    19:00:59.569  01/24/02  Sev=Info/4       IKE/0x63000014
RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from 14.36.100.50

210    19:00:59.569  01/24/02  Sev=Info/4       CM/0x63100015
Launch xAuth application

211    19:01:04.236  01/24/02  Sev=Info/4       CM/0x63100017
xAuth application returned

212    19:01:04.236  01/24/02  Sev=Info/4       IKE/0x63000013
SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 14.36.100.50

213    19:01:04.496  01/24/02  Sev=Info/5       IKE/0x6300002F
Received ISAKMP packet: peer = 14.36.100.50

214    19:01:04.496  01/24/02  Sev=Info/4       IKE/0x63000014
RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from 14.36.100.50

215    19:01:04.496  01/24/02  Sev=Info/4       CM/0x6310000E
Established Phase 1 SA.  1 Phase 1 SA in the system

216    19:01:04.506  01/24/02  Sev=Info/4       IKE/0x63000013
SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 14.36.100.50

217    19:01:04.516  01/24/02  Sev=Info/5       IKE/0x6300005D
Client sending a firewall request to concentrator

218    19:01:04.516  01/24/02  Sev=Info/5       IKE/0x6300005C
Firewall Policy: Product=Cisco Integrated Client, Capability=
(Centralized Policy Push).

219    19:01:04.516  01/24/02  Sev=Info/4       IKE/0x63000013
SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 14.36.100.50

220    19:01:04.586  01/24/02  Sev=Info/5       IKE/0x6300002F
Received ISAKMP packet: peer = 14.36.100.50

221    19:01:04.586  01/24/02  Sev=Info/4       IKE/0x63000014
RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from 14.36.100.50

222    19:01:04.586  01/24/02  Sev=Info/5       IKE/0x63000010
MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_ADDRESS: ,
```

```
value = 10.1.2.1

223    19:01:04.586  01/24/02  Sev=Info/5       IKE/0x63000010
MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_DNS(1): ,
value = 10.1.1.2

224    19:01:04.586  01/24/02  Sev=Info/5       IKE/0x63000010
MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_NBNS(1) (a.k.a. WINS)
: , value = 10.1.1.2

225    19:01:04.586  01/24/02  Sev=Info/5       IKE/0x6300000E
MODE_CFG_REPLY: Attribute = MODECFG_UNITY_DEFDOMAIN: ,
value = cisco.com

226    19:01:04.586  01/24/02  Sev=Info/4       CM/0x63100019
Mode Config data received

227    19:01:04.606  01/24/02  Sev=Info/5       IKE/0x63000055
Received a key request from Driver for IP address 14.36.100.50,
GW IP = 14.36.100.50

228    19:01:04.606  01/24/02  Sev=Info/4       IKE/0x63000013
SENDING >>> ISAKMP OAK QM *(HASH, SA, NON, ID, ID) to 14.36.100.50

229    19:01:04.606  01/24/02  Sev=Info/5       IKE/0x63000055
Received a key request from Driver for IP address 10.10.10.255,
GW IP = 14.36.100.50

230    19:01:04.606  01/24/02  Sev=Info/4       IKE/0x63000013
SENDING >>> ISAKMP OAK QM *(HASH, SA, NON, ID, ID) to 14.36.100.50

231    19:01:04.786  01/24/02  Sev=Info/4       IPSEC/0x63700014
Deleted all keys

232    19:01:05.948  01/24/02  Sev=Info/5       IKE/0x6300002F
Received ISAKMP packet: peer = 14.36.100.50

233    19:01:05.948  01/24/02  Sev=Info/4       IKE/0x63000014
RECEIVING <<< ISAKMP OAK QM *(HASH, SA, NON, ID, ID,
NOTIFY:STATUS_RESP_LIFETIME) from 14.36.100.50

234    19:01:05.948  01/24/02  Sev=Info/5       IKE/0x63000044
RESPONDER-LIFETIME notify has value of 28800 seconds

235    19:01:05.948  01/24/02  Sev=Info/5       IKE/0x63000045
RESPONDER-LIFETIME notify has value of 4608000 kb

236    19:01:05.948  01/24/02  Sev=Info/4       IKE/0x63000013
SENDING >>> ISAKMP OAK QM *(HASH) to 14.36.100.50

237    19:01:05.948  01/24/02  Sev=Info/5       IKE/0x63000058
Loading IPsec SA (Message ID = 0x5B090EB1 OUTBOUND SPI =
0xF39C2217 INBOUND SPI = 0x72FEDC99)

238    19:01:05.948  01/24/02  Sev=Info/5       IKE/0x63000025
Loaded OUTBOUND ESP SPI: 0xF39C2217

239    19:01:05.948  01/24/02  Sev=Info/5       IKE/0x63000026
Loaded INBOUND ESP SPI: 0x72FEDC99

240    19:01:05.948  01/24/02  Sev=Info/4       CM/0x6310001A
One secure connection established

241    19:01:05.988  01/24/02  Sev=Info/6       DIALER/0x63300003
```

```
Connection established.

242    19:01:06.078  01/24/02  Sev=Info/6       DIALER/0x63300008
MAPI32 Information - Outlook not default mail client

243    19:01:06.118  01/24/02  Sev=Info/5       IKE/0x6300002F
Received ISAKMP packet: peer = 14.36.100.50

244    19:01:06.118  01/24/02  Sev=Info/4       IKE/0x63000014
RECEIVING <<< ISAKMP OAK QM *(HASH, SA, NON, ID, ID,
NOTIFY:STATUS_RESP_LIFETIME) from 14.36.100.50

245    19:01:06.118  01/24/02  Sev=Info/5       IKE/0x63000044
RESPONDER-LIFETIME notify has value of 28800 seconds

246    19:01:06.118  01/24/02  Sev=Info/5       IKE/0x63000045
RESPONDER-LIFETIME notify has value of 4608000 kb

247    19:01:06.118  01/24/02  Sev=Info/4       IKE/0x63000013
SENDING >>> ISAKMP OAK QM *(HASH) to 14.36.100.50

248    19:01:06.118  01/24/02  Sev=Info/5       IKE/0x63000058
Loading IPsec SA (Message ID = 0xCFE65CEB OUTBOUND SPI =
0x6AC28ED0 INBOUND SPI = 0x0A5AD786)

249    19:01:06.118  01/24/02  Sev=Info/5       IKE/0x63000025
Loaded OUTBOUND ESP SPI: 0x6AC28ED0

250    19:01:06.118  01/24/02  Sev=Info/5       IKE/0x63000026
Loaded INBOUND ESP SPI: 0x0A5AD786

251    19:01:06.118  01/24/02  Sev=Info/4       CM/0x63100022
Additional Phase 2 SA established.

252    19:01:07.020  01/24/02  Sev=Info/4       IPSEC/0x63700010
Created a new key structure

253    19:01:07.020  01/24/02  Sev=Info/4       IPSEC/0x6370000F
Added key with SPI=0x17229cf3 into key list

254    19:01:07.020  01/24/02  Sev=Info/4       IPSEC/0x63700010
Created a new key structure

255    19:01:07.020  01/24/02  Sev=Info/4       IPSEC/0x6370000F
Added key with SPI=0x99dcfe72 into key list

256    19:01:07.020  01/24/02  Sev=Info/4       IPSEC/0x63700010
Created a new key structure

257    19:01:07.020  01/24/02  Sev=Info/4       IPSEC/0x6370000F
Added key with SPI=0xd08ec26a into key list

258    19:01:07.020  01/24/02  Sev=Info/4       IPSEC/0x63700010
Created a new key structure

259    19:01:07.020  01/24/02  Sev=Info/4       IPSEC/0x6370000F
Added key with SPI=0x86d75a0a into key list

260    19:01:15.032  01/24/02  Sev=Info/6       IKE/0x6300003D
Sending DPD request to 14.36.100.50, seq# = 152233542

261    19:01:15.032  01/24/02  Sev=Info/4       IKE/0x63000013
SENDING >>> ISAKMP OAK INFO *(HASH, NOTIFY:DPD_REQUEST)
to 14.36.100.50
```

```
262    19:01:15.032  01/24/02  Sev=Info/5       IKE/0x6300002F
Received ISAKMP packet: peer = 14.36.100.50

263    19:01:15.032  01/24/02  Sev=Info/4       IKE/0x63000014
RECEIVING <<< ISAKMP OAK INFO *(HASH, NOTIFY:DPD_ACK)
from 14.36.100.50

264    19:01:15.032  01/24/02  Sev=Info/5       IKE/0x6300003F
Received DPD ACK from 14.36.100.50, seq# received = 152233542,
seq# expected = 152233542
```

Información Relacionada

- Página de Soporte de PIX
- Referencias de Comando PIX
- Página de soporte de RADIUS
- Página de soporte del concentrador de la serie Cisco VPN 3000
- Página de soporte al cliente Serie Cisco VPN 3000
- Página de Soporte del Protocolo IKE/la Negociación de IPSec
- Solicitudes de Comentarios (RFC)
- Soporte Técnico - Cisco Systems