Cómo autenticar el VPN 5000 Client al VPN 5000 concentrator con el CiscoSecure NT 2.5 y posterior (RADIUS)

Contenido

Introducción

El Cisco Secure NT (CSNT) 2.5 y posterior (RADIUS) es capaz de volver el Red privada virtual (VPN) 5000 atributos específicos del proveedor para VPN GroupInfo y contraseña de VPN para autenticar un VPN 5000 Client al VPN 5000 concentrator. El documento siguiente asume que la autenticación local está trabajando antes de agregar la autenticación de RADIUS (por lo tanto nuestro usuario, “localuser,” en el grupo “ciscolocal”). Entonces la autenticación se agrega al RADIUS CSNT para usuarios que no existe en la base de datos local (asignan el usuario “csntuser” para agrupar el “csntgroup” en virtud de los atributos vueltos del servidor del CSNT RADIUS).

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

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

- Cisco Secure NT 2.5
- Concentrador 5.2.16.0005 del Cisco VPN 5000
- Cliente Cisco VPN 5000 4.2.7

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.

Convenciones

Para obtener más información sobre las convenciones del documento, consulte las Convenciones de Consejos Técnicos de Cisco.

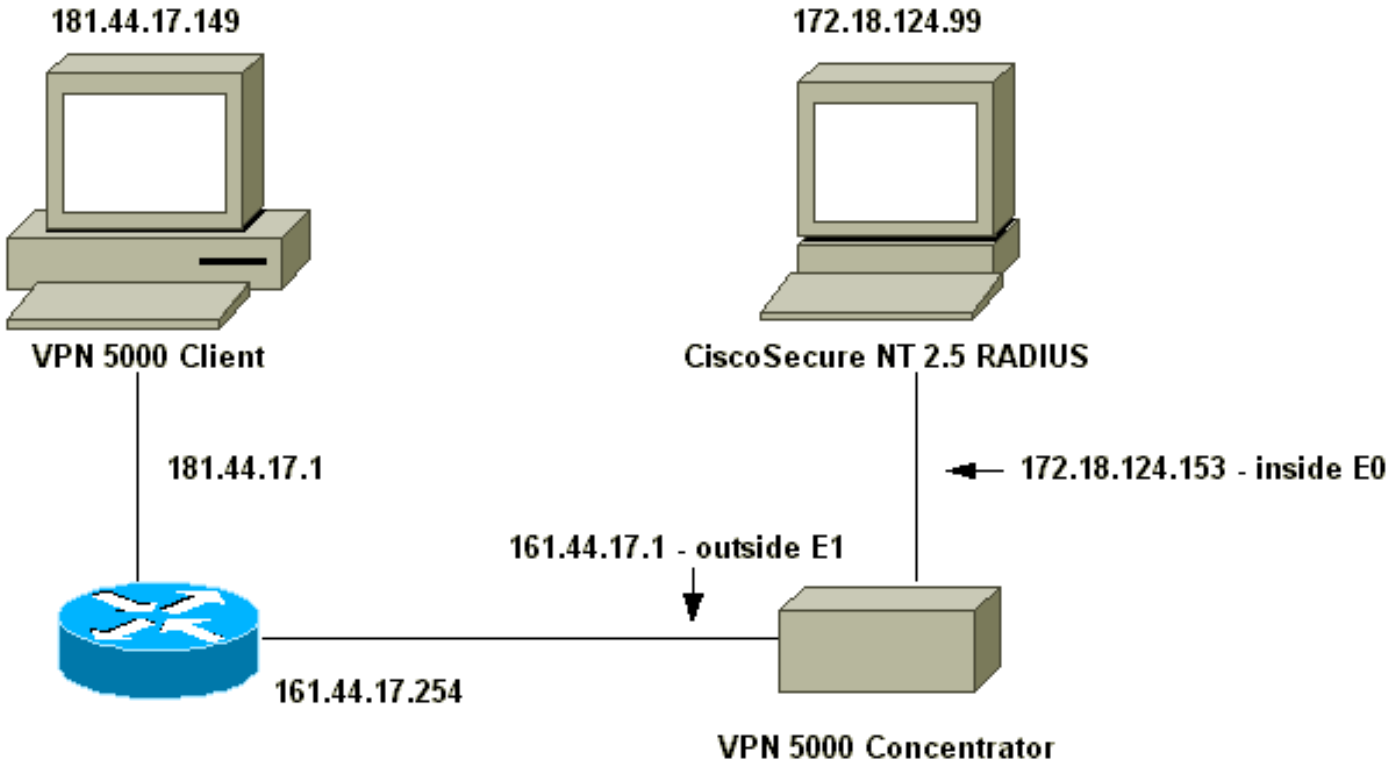
Configurar

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

Nota: Para obtener información adicional sobre los comandos que se utilizan en este documento, use la Command Lookup Tool (solo para clientes registrados).

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Configuraciones

En este documento, se utilizan estas configuraciones:

- Concentrador VPN 5000
- VPN 5000 Client

Concentrador VPN 5000

```
[ IP Ethernet 0 ]
SubnetMask                  = 255.255.255.0
Mode                        = Routed
IPAddress                   = 172.18.124.153

[ IP Ethernet 1 ]
Mode                        = Routed
SubnetMask                  = 255.255.255.0
IPAddress                   = 161.44.17.1

[ VPN Group "ciscolocal" ]
IPNet                       = 172.18.124.0/24
Transform                   = esp(md5,des)
StartIPAddress              = 172.18.124.250
MaxConnections              = 4
BindTo                      = "ethernet0"
[ General ]
EthernetAddress             = 00:00:a5:f0:c9:00
DeviceType                  = VPN 5001 Concentrator
ConfiguredOn                = Timeserver not configured
ConfiguredFrom              = Command Line, from
172.18.124.99
IPSecGateway                = 161.44.17.254

[ Logging ]
Level                       = 7
Enabled                     = On
LogToAuxPort                = On
```

```
LogToSysLog               = On
SyslogIPAddress           = 172.18.124.114
SyslogFacility            = Local5

[ IKE Policy ]
Protection                = MD5_DES_G1

[ VPN Users ]
localuser Config="ciscolocal" SharedKey="localike"

[ Radius ]
Accounting                = Off
PrimAddress               = "172.18.124.99"
Secret                    = "csntkey"
ChallengeType             = CHAP
BindTo                    = "ethernet0"
Authentication            = On

[ VPN Group "csnt" ]
BindTo                    = "ethernet0"
Transform                 = ESP(md5,Des)
MaxConnections            = 2
IPNet                     = 172.18.124.0/24
StartIPAddress            = 172.18.124.245

AssignIPRADIUS            = Off
BindTo                    = "ethernet0"
StartIPAddress            = 172.18.124.243
IPNet                     = 172.18.124./24
StartIPAddress            = 172.18.124.242
Transform                 = ESP(md5,Des)
BindTo                    = "ethernet0"
MaxConnections            = 1

[ VPN Group "csntgroup" ]
MaxConnections            = 2
StartIPAddress            = 172.18.124.242
BindTo                    = "ethernet0"
Transform                 = ESP(md5,Des)
IPNet                     = 172.18.124.0/24

Configuration size is 2045 out of 65500 bytes.
```

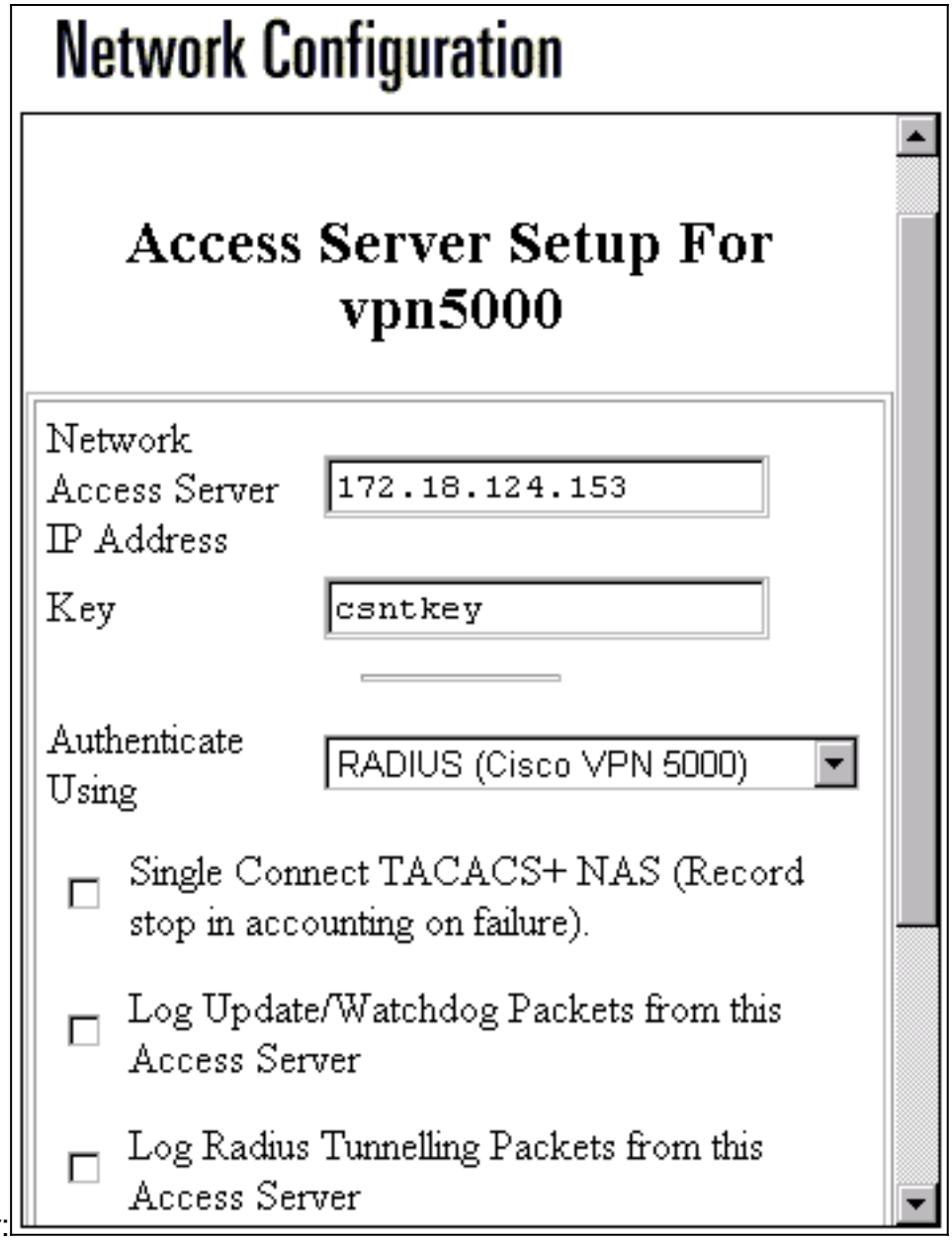
VPN 5000 Client

Note: None of the defaults have been changed. Two users were added, and the appropriate passwords were entered when prompted after clicking Connect: username password radius_password -------- -------- --------------- localuser localike N/A csntuser grouppass csntpass

Configuración de Cisco Secure NT 2.5

Siga este procedimiento.

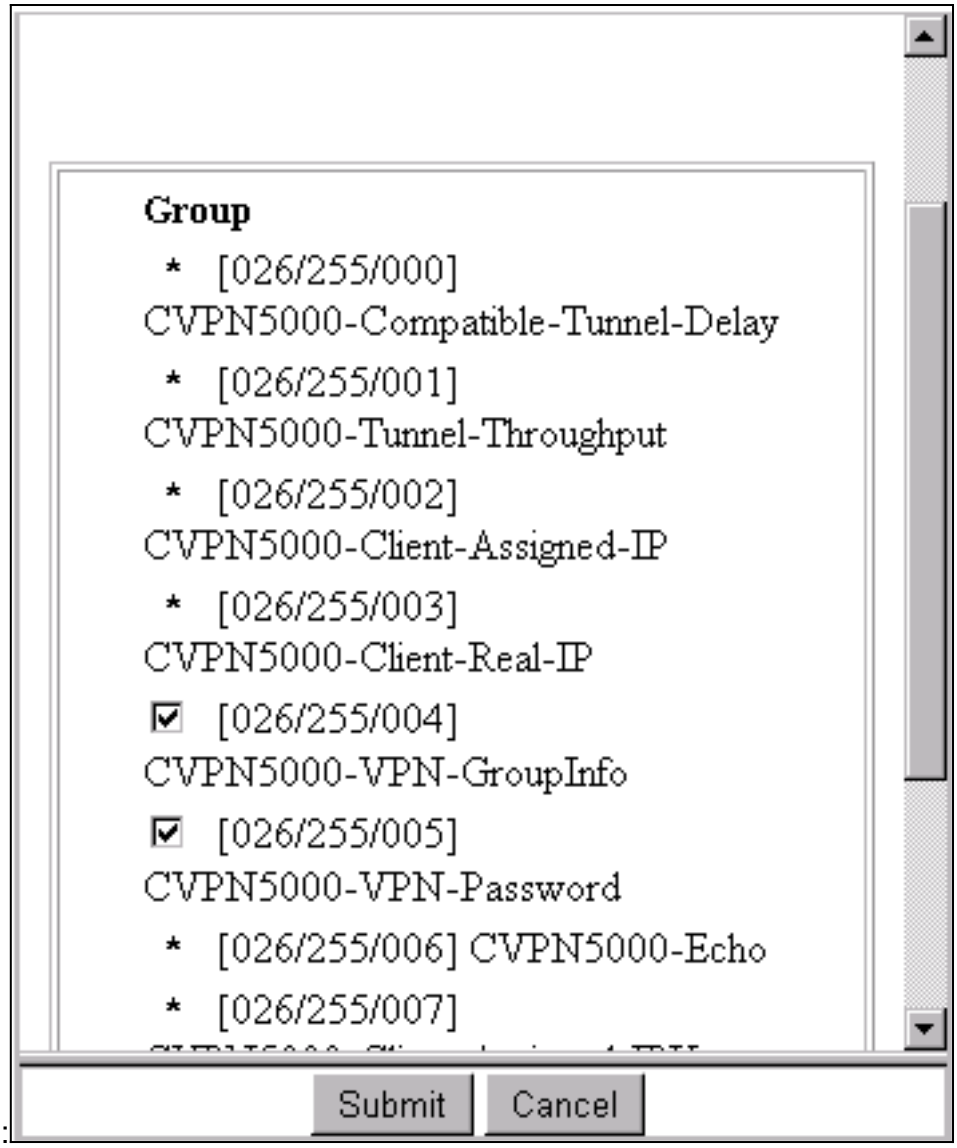
1. Configure el servidor para hablar al



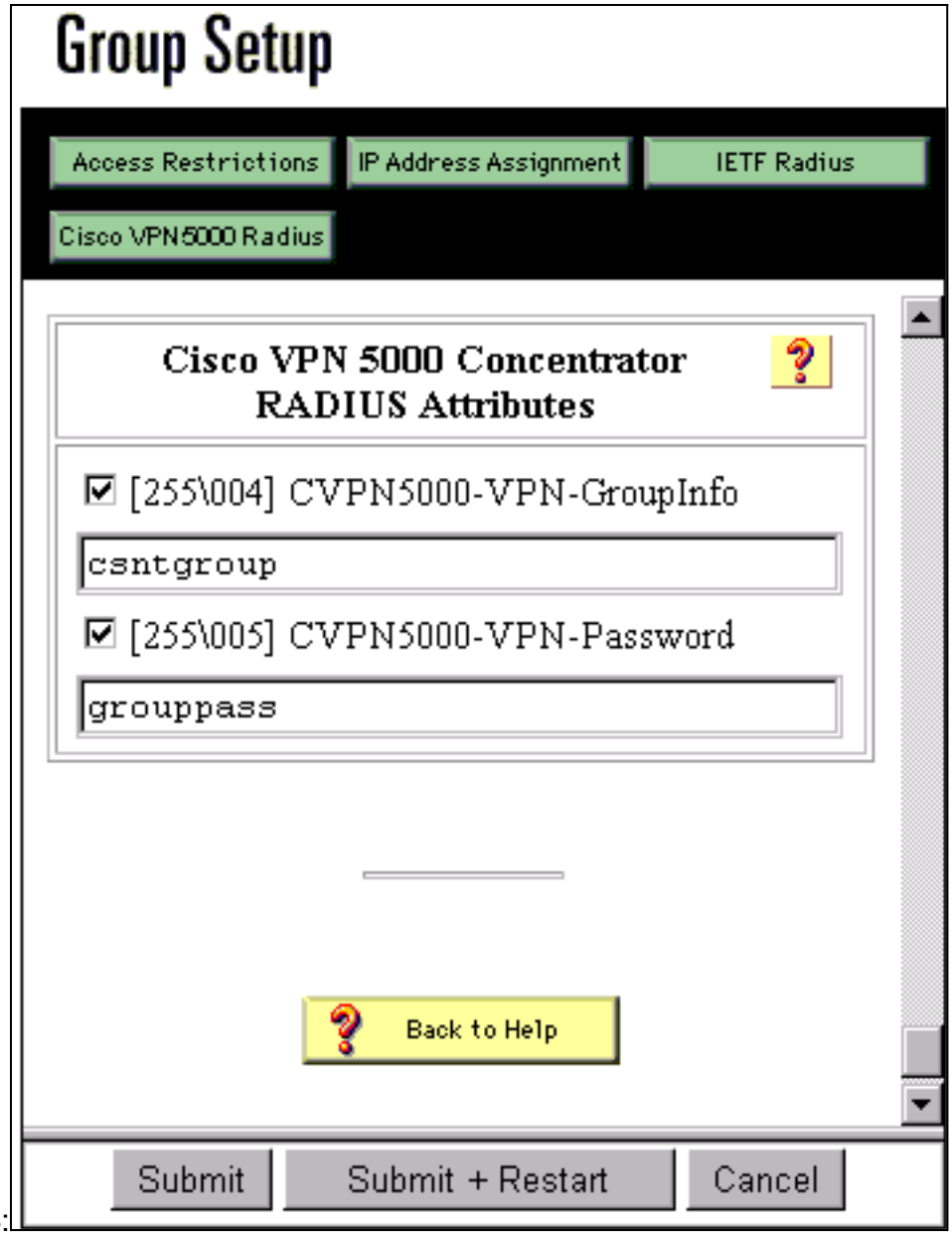
concentrador:

2. Va a la **configuración de la interfaz** > a **RADIUS (VPN5000)** y marca VPN GroupInfo y la

contraseña de VPN:



3. Después de configurar al usuario (“csntuser”) con una contraseña (“csntpass”) en la configuración de usuario y de poner al usuario en el grupo 13, configure los atributos VPN5000 en **configuración de grupo | Grupo**

13: 

Cambio a la autenticación PAP

Los trabajos asumidos de la autenticación del Challenge Handshake Authentication Protocol (CHAP), usted puede desear cambiar al protocolo password authentication (PAP), que le permite para tener la contraseña de usuario CSNT uso de la base de datos de NT.

Cambio de perfil de RADIUS VPN 5000

```
[ Radius ]
PAPAuthSecret           = "abcxyz"
ChallengeType           = PAP
```

Nota: El CSNT también sería configurado para utilizar la base de datos de NT para la esa autenticación de usuario.

Qué el usuario ve (tres casillas de verificación de contraseña):

```
Shared Secret = grouppass
RADIUS Login box - Password = csntpass
RADIUS Login box - Authentication Secret = abcxyz
```

Agregar una asignación de dirección IP

Si el perfil CSNT del usuario se fija en “asigne el IP Address estático” a un valor específico, y si fijan al grupo del VPN 5000 concentrator para:

```
AssignIPRADIUS = On
```

Entonces, la dirección IP RADIUS se envía abajo del CSNT y se aplica al usuario en el VPN 5000 concentrator.

Incorporación de contabilidad

Si usted quiere los registros de contabilidad de la sesión enviados a Cisco aseguran al servidor de RADIUS, después agregan al VPN 5000 concentrator la configuración de RADIUS:

```
[ Radius ]
Accounting = On
```

Usted debe utilizar los **comandos apply y write**, y entonces el **comando boot** en el VPN5000 para que este cambio tome el efecto.

Registros de contabilidad del CSNT

```
11/06/2000,16:02:45,csntuser,Group 13,,Start,077745c5-00000000,,,,,,,,,
   268435456,172.18.124.153
11/06/2000,16:03:05,csntuser,Group 13,,Stop,077745c5-00000000,20,,,
   104,0,1,0,,268435456,172.18.124.153
```

Verificación

En esta sección encontrará información que puede utilizar para confirmar que su configuración esté funcionando correctamente.

La herramienta Output Interpreter (sólo para clientes registrados) permite utilizar algunos comandos “show” y ver un análisis del resultado de estos comandos.

- **show system log buffer**
```
Info 7701.12 seconds Command loop started from 172.18.124.99
on PTY1

Notice 7723.36 seconds New IKE connection: [181.44.17.149]:1041:csntuser
Debug 7723.38 seconds Sending RADIUS CHAP challenge to
   csntuser at 181.44.17.149
Debug 7729.0 seconds Received RADIUS challenge resp. from
   csntuser at 181.44.17.149, contacting server
Notice 7729.24 seconds VPN 0 opened for csntuser from 181.44.17.149.
Debug 7729.26 seconds Client's local broadcast address = 181.44.17.255
Notice 7729.29 seconds User assigned IP address 172.18.124.242
```
- **vpn trace dump all**
```
VPN5001_A5F0C900# vpn trace dump all
         6 seconds -- stepmngr trace enabled --
   new script: ISAKMP primary responder script for <no id> (start)
manage @ 91 seconds :: [181.44.17.149]:1042 (start)
         91 seconds doing irpri_new_conn, (0 @ 0)
         91 seconds doing irpri_pkt_1_recd, (0 @ 0)
   new script: ISAKMP Resp Aggr Shared Secret script for
      [181.44.17.149]:1042 (start)
         91 seconds doing irsass_process_pkt_1, (0 @ 0)
         91 seconds doing irsass_build_rad_pkt, (0 @ 0)
```

```
          91 seconds doing irsass_send_rad_pkt, (0 @ 0)
    manage @ 91 seconds :: [181.44.17.149]:1042 (done)
    manage @ 93 seconds :: [181.44.17.149]:1042:csntuser (start)
          93 seconds doing irsass_radius_wait, (0 @ 0)
          93 seconds doing irsass_send_rad_pkt, (0 @ 0)
    manage @ 93 seconds :: [181.44.17.149]:1042:csntuser (done)
    manage @ 95 seconds :: [181.44.17.149]:1042:csntuser (start)
          95 seconds doing irsass_radius_wait, (0 @ 0)
          95 seconds doing irsass_send_rad_pkt, (0 @ 0)
    manage @ 95 seconds :: [181.44.17.149]:1042:csntuser (done)
    manage @ 95 seconds :: [181.44.17.149]:1042:csntuser (start)
          95 seconds doing irsass_radius_wait, (0 @ 0)
    manage @ 95 seconds :: [181.44.17.149]:1042:csntuser (done)
    manage @ 95 seconds :: [181.44.17.149]:1042:csntuser (start)
          95 seconds doing irsass_rad_serv_wait, (0 @ 0)
          95 seconds doing irsass_build_pkt_2, (0 @ 0)
          96 seconds doing irsass_send_pkt_2, (0 @ 0)
    manage @ 96 seconds :: [181.44.17.149]:1042:csntuser (done)
    manage @ 96 seconds :: [181.44.17.149]:1042:csntuser (start)
          96 seconds doing irsass_check_timeout, (0 @ 0)
          96 seconds doing irsass_check_hash, (0 @ 0)
          96 seconds doing irsass_last_op, (0 @ 0)
       end script: ISAKMP Resp Aggr Shared Secret script for
          [181.44.17.149]:1042:csntuser, (0 @ 0)
       next script: ISAKMP primary responder script for
          [181.44.17.149]:1042:csntuser, (0 @ 0)
             96 seconds doing irpri_phase1_done, (0 @ 0)
             96 seconds doing irpri_phase1_done, (0 @ 0)
             96 seconds doing irpri_start_phase2, (0 @ 0)
       new script: phase 2 initiator for [181.44.17.149]:1042:csntuser (start)
             96 seconds doing iph2_init, (0 @ 0)
             96 seconds doing iph2_build_pkt_1, (0 @ 0)
             96 seconds doing iph2_send_pkt_1, (0 @ 0)
    manage @ 96 seconds :: [181.44.17.149]:1042:csntuser (done)
    manage @ 96 seconds :: [181.44.17.149]:1042:csntuser (start)
          96 seconds doing iph2_pkt_2_wait, (0 @ 0)
          96 seconds doing ihp2_process_pkt_2, (0 @ 0)
          96 seconds doing iph2_build_pkt_3, (0 @ 0)
          96 seconds doing iph2_config_SAs, (0 @ 0)
          96 seconds doing iph2_send_pkt_3, (0 @ 0)
          96 seconds doing iph2_last_op, (0 @ 0)
       end script: phase 2 initiator for [181.44.17.149]:1042:csntuser, (0 @ 0)
       next script: ISAKMP primary responder script for
          [181.44.17.149]:1042:csntuser, (0 @ 0)
             96 seconds doing irpri_open_tunnel, (0 @ 0)
             96 seconds doing irpri_start_i_maint, (0 @ 0)
       new script: initiator maintenance for [181.44.17.149]:1042:csntuser (start)
             96 seconds doing imnt_init, (0 @ 0)
    manage @ 96 seconds :: [181.44.17.149]:1042:csntuser (done)
    <vpn trace dump done, 55 records scanned>
```

Troubleshooting

Los siguientes son errores posibles que usted puede encontrar.

El servidor Cisco Secure NT es inalcanzable

Depuración VPN 5000

```
Notice 359.36 seconds New IKE connection: [181.44.17.149]:1044:csntuser
```

```
Debug 359.38 seconds Sending RADIUS CHAP challenge to csntuser at 181.44.17.149
Debug 363.18 seconds Received RADIUS challenge resp. From
   csntuser at 181.44.17.149, contacting server
Notice 423.54 seconds <no ifp> (csntuser) reset: RADIUS server never responded.
```

Qué el usuario ve:

```
VPN Server Error (14) User Access Denied
```

Falla la autenticación

El nombre de usuario o la contraseña en el Cisco Secure NT es mala.

Depuración VPN 5000

```
Notice 506.42 seconds New IKE connection: [181.44.17.149]:1045:csntuser
Debug 506.44 seconds Sending RADIUS CHAP challenge to csntuser
   at 181.44.17.149
Debug 511.24 seconds Received RADIUS challenge resp. From csntuser
  at 181.44.17.149, contacting server
Debug 511.28 seconds Auth request for csntuser rejected by RADIUS server
Notice 511.31 seconds <no ifp> (csntuser) reset due to RADIUS authentication
failure.
```

Qué el usuario ve:

```
VPN Server Error (14) User Access Denied
```

Cisco seguro:

Vaya a los **informes** y a la **actividad**, y el registro de los intentos fallidos muestra el error.

La contraseña de grupo VPN ingresada por el usuario no coincide con VPNPassword

Depuración VPN 5000

```
Notice 545.0 seconds New IKE connection: [181.44.17.149]:1046:csntuser
Debug 545.6 seconds Sending RADIUS CHAP challenge to csntuser at 181.44.17.149
Debug 550.6 seconds Received RADIUS challenge resp. From csntuser at 181.44.17.149,
contacting server
```

Qué el usuario ve:

```
IKE ERROR: Authentication Failed.
```

Cisco seguro:

Vaya a los **informes** y a la **actividad**, y el registro de los intentos fallidos no muestra el error.

El nombre de grupo expulsado por el servidor RADIUS no existe en la VPN 5000

Depuración VPN 5000

```
Notice 656.18 seconds New IKE connection: [181.44.17.149]:1047:csntuser
Debug 656.24 seconds Sending RADIUS CHAP challenge to csntuser at 181.44.17.149
Debug 660.12 seconds Received RADIUS challenge resp. From csntuser at 181.44.17.149,
contacting server
Warnin 660.16 seconds User, "csntuser", has an invalid VPN Group config, "junkgroup"
Notice 660.20 seconds  (csntuser) reset: connection script finished.
Notice 660.23 seconds -- reason: S_NO_POLICY (220@772)
```

Qué el usuario ve:

```
VPN Server Error (6): Bad user configuration on IntraPort server.
```

Cisco seguro:

Vaya a los **informes** y a la **actividad**, y el registro de los intentos fallidos no muestra el error.

Información Relacionada

- Página de soporte de Cisco Secure ACS para Windows
- Anuncio de fin de venta de los concentradores Serie VPN 5000 de Cisco
- Página de soporte del concentrador VPN 5000 de Cisco
- Página de soporte para Cisco VPN 5000 Client
- Página de soporte de IPSec
- Página de soporte de RADIUS
- Solicitudes de Comentarios (RFC)
- Soporte Técnico y Documentación - Cisco Systems