Hoe u VPN 5000-client verificatie kunt uitvoeren naar de VPN 5000-centrator met Cisco Secure NT 2.5 en hoger (RADIUS)

Inhoud

Inleiding

Cisco Secure NT (CSNT) 2.5 en hoger (RADIUS) kan Virtual Private Network (VPN) 5000 leverancierspecifieke eigenschappen voor VPN GroupInfo en VPN-wachtwoord retourneren om een VPN-client voor 5000 naar de VPN 5000-centrator te controleren. Het volgende document gaat ervan uit dat lokale authenticatie werkt voordat RADIUS-verificatie wordt toegevoegd (dus onze gebruiker, "localuser," in groep "ciscolocal"). Vervolgens wordt de authenticatie toegevoegd aan CSNT RADIUS voor gebruikers die niet in de lokale database aanwezig zijn (gebruiker "verstand" wordt toegewezen aan groep "groep" op grond van de eigenschappen die teruggegeven zijn van de CSNT RADIUS server).

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Secure NT2.5
- Cisco VPN 5000 Concentrator 5.2.16.005
- Cisco VPN 5000 client 4.2.7

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

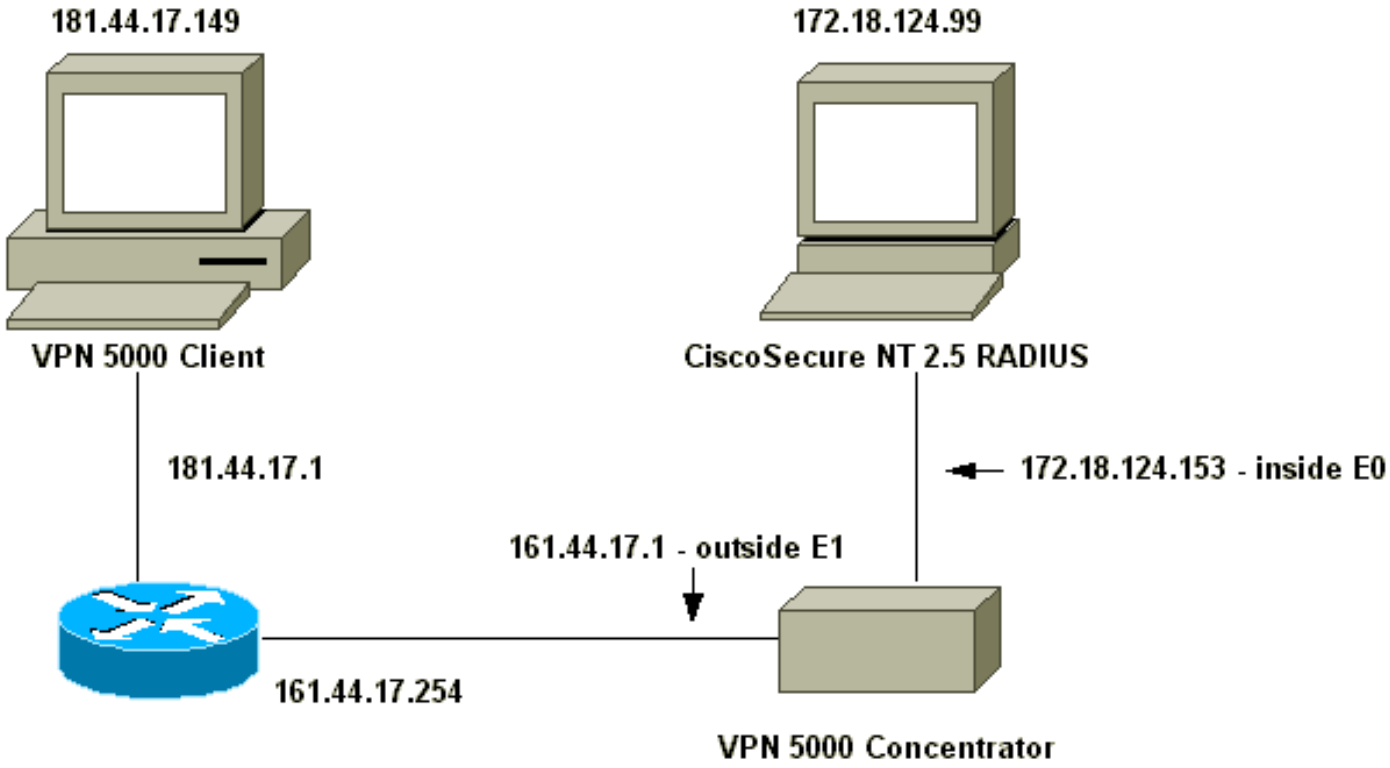
Configureren

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

N.B.: Als u aanvullende informatie wilt vinden over de opdrachten in dit document, gebruikt u het Opdrachtplanningprogramma (alleen geregistreerd klanten).

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:



Configuraties

Dit document gebruikt deze configuraties:

- VPN 5000 Concentrator
- VPN 5000-client

VPN 5000 Concentrator

```
[ 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

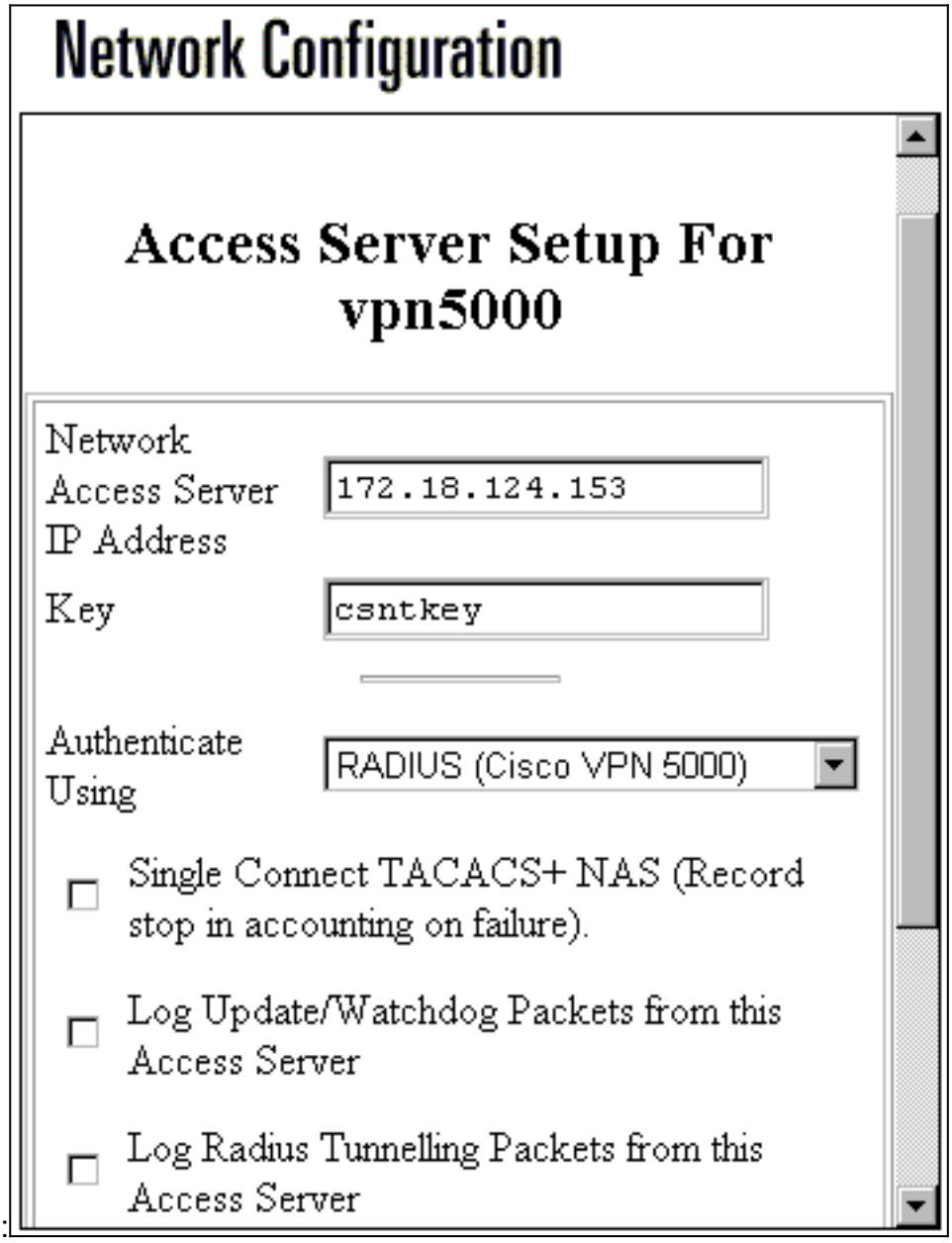
Note: None of the defaults have been changed. Two users were added, and
the appropriate passwords were entered when prompted after clicking Connect:

```
username        password        radius_password
--------        --------        ---------------
localuser       localike        N/A
csntuser        grouppass       csntpass
```

Cisco Secure NT 2.5-configuratie

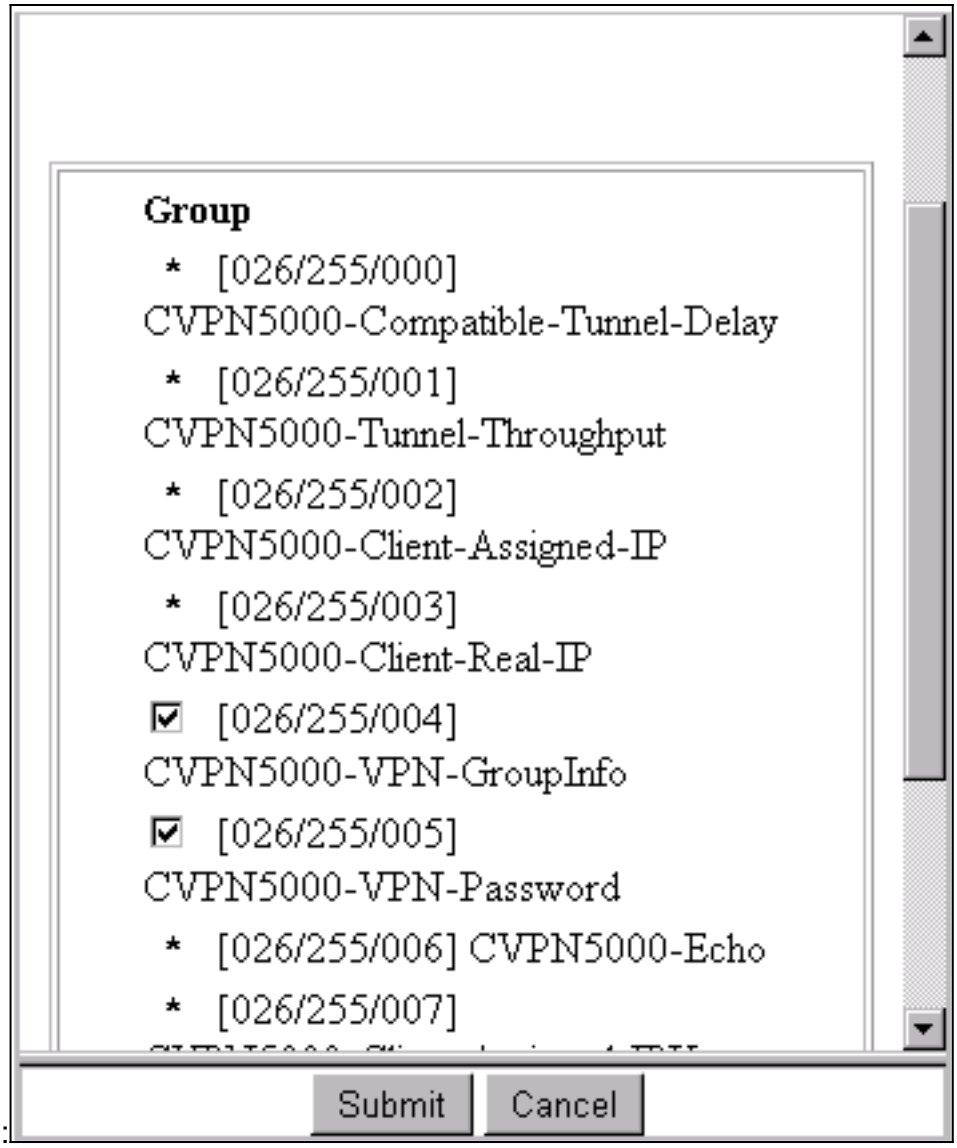
Volg deze procedure.

1. Configuratie van de server om met de Concentrator te spreken:

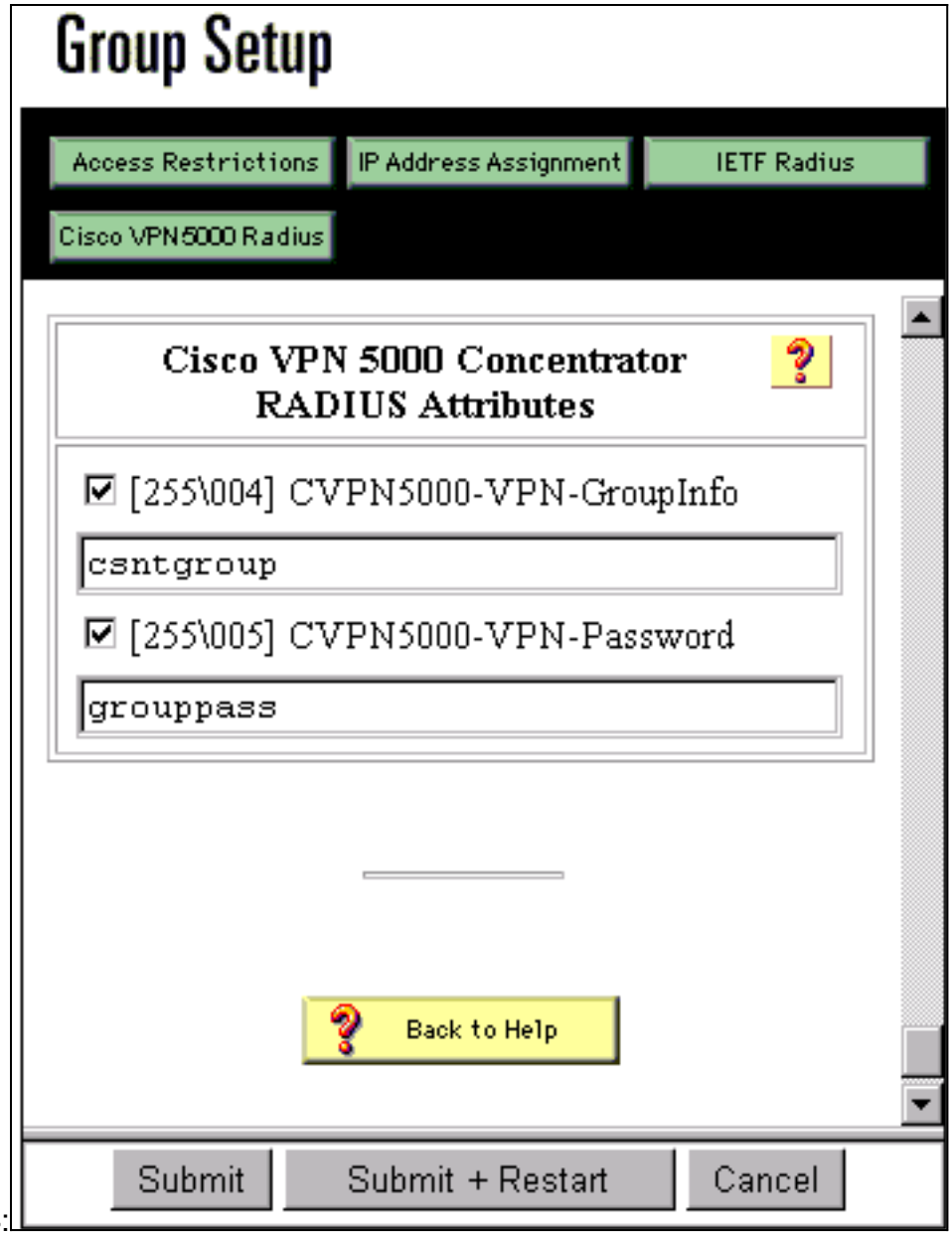


2. Ga naar **interfaceconfiguratie > RADIUS (VPN 5000)** en controleer VPN-groepsinformatie en

VPN-wachtwoord:



3. Na het configureren van de gebruiker ("scanner") met een wachtwoord ("passeren") in de gebruikersinstelling en het plaatsen van de gebruiker in groep 13, moet u de VPN 5000-eigenschappen in **groepsinstellingen** configureren **| Groep**

13: 

Naar PAP-verificatie wijzigen

Aangenomen dat Challenge Handshake Authentication Protocol (CHAP) werkt, kunt u naar Wachtwoord Verificatie Protocol (PAP) wijzigen, waardoor u het wachtwoord van de gebruiker vanuit de NT-database kunt gebruiken.

VPN 5000 RADIUS-profielwijziging

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

Opmerking: CSNT zou ook ingesteld worden om de NT-database te gebruiken voor de verificatie van die gebruiker.

Wat de gebruiker ziet (drie wachtwoordboxen):

```
Shared Secret = grouppass
```

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

IP-adrestoewijzing toevoegen

Als het CSNT-profiel van de gebruiker is ingesteld in "Toewijzen statische IP-adres" op een bepaalde waarde en als de VPN 5000 Concentrator-groep is ingesteld voor:

```
AssignIPRADIUS = On
```

Vervolgens wordt het RADIUS IP-adres verzonden vanuit CSNT en toegepast op de gebruiker in VPN 5000 Concentrator.

Boekhouding toevoegen

Als u sessieaccounting records wilt die naar de Cisco Secure RADIUS-server worden verzonden, dan toevoegen aan de VPN 5000 Concentrator RADIUS-configuratie:

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

U moet de opdrachten **toepassen** en **schrijven**, en vervolgens de laars opdracht op VPN 5000 gebruiken om deze wijziging in werking te stellen.

Boekhoudkundige gegevens van 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
```

Verifiëren

Deze sectie verschaft informatie die u kunt gebruiken om te bevestigen dat uw configuratie correct werkt.

Bepaalde opdrachten met **show worden ondersteund door de tool** Output Interpreter (alleen voor geregistreerde klanten). Hiermee kunt u een analyse van de output van opdrachten met **show genereren.**

- **systeemlog-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-scan**

```
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>
```

Problemen oplossen

Het volgende zijn mogelijke fouten u kunt tegenkomen.

Cisco Secure NT Server is onbereikbaar

VPN 5000 debug

```
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.
```

Wat de gebruiker ziet:

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

Verificatiefouten

De gebruikersnaam of het wachtwoord op Cisco Secure NT is slecht.

VPN 5000 debug

```
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.
```

Wat de gebruiker ziet:

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

Cisco Secure:

Ga naar **Rapporten** en **Activiteit**, en het mislukte poging logboek toont de mislukking.

VPN Group Wachtwoord dat door gebruiker is ingevoerd, is niet akkoord met VPN-wachtwoord

VPN 5000 debug

```
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
```

Wat de gebruiker ziet:

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

Cisco Secure:

Ga naar **Rapporten** en **Activiteit**, en het mislukte poging logboek toont de mislukking niet.

De groepsnaam die door de RADIUS-server is verstuurd, bestaat niet op VPN 5000

VPN 5000 debug

```
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)
```

Wat de gebruiker ziet:

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

Cisco Secure:

Ga naar **Rapporten** en **Activiteit**, en het mislukte poging logbestand *toont* de mislukking niet.

Gerelateerde informatie

- Cisco Secure ACS voor Windows-ondersteuningspagina
- Cisco VPN 5000 Series Concentrators end-of-sale aankondiging
- Ondersteuning van Cisco VPN 5000 Concentrator-pagina
- Cisco VPN 5000 clientondersteuningspagina
- Ondersteuning van IPsec
- RADIUS-ondersteuningspagina
- Verzoeken om opmerkingen (RFC's)
- Technische ondersteuning en documentatie – Cisco Systems