Come autenticare il client VPN 5000 al concentratore VPN 5000 con Cisco Secure NT 2.5 e versioni successive (RADIUS)

Sommario

Introduzione

Cisco Secure NT (CSNT) 2.5 e versioni successive (RADIUS) è in grado di restituire gli attributi VPN 5000 specifici del fornitore per VPN GroupInfo e VPN Password per autenticare un client VPN 5000 al concentratore VPN 5000. Nel documento seguente si presume che l'autenticazione locale funzioni prima di aggiungere l'autenticazione RADIUS (di conseguenza l'utente, "localuser", nel gruppo "ciscolocal"). L'autenticazione viene quindi aggiunta a CSNT RADIUS per gli utenti non esistenti nel database locale (l'utente "csntuser" viene assegnato al gruppo "csntgroup" in virtù degli attributi restituiti dal server CSNT RADIUS).

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Secure NT 2.5
- Cisco VPN 5000 Concentrator 5.2.16.0005
- Cisco VPN 5000 Client 4.2.7

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

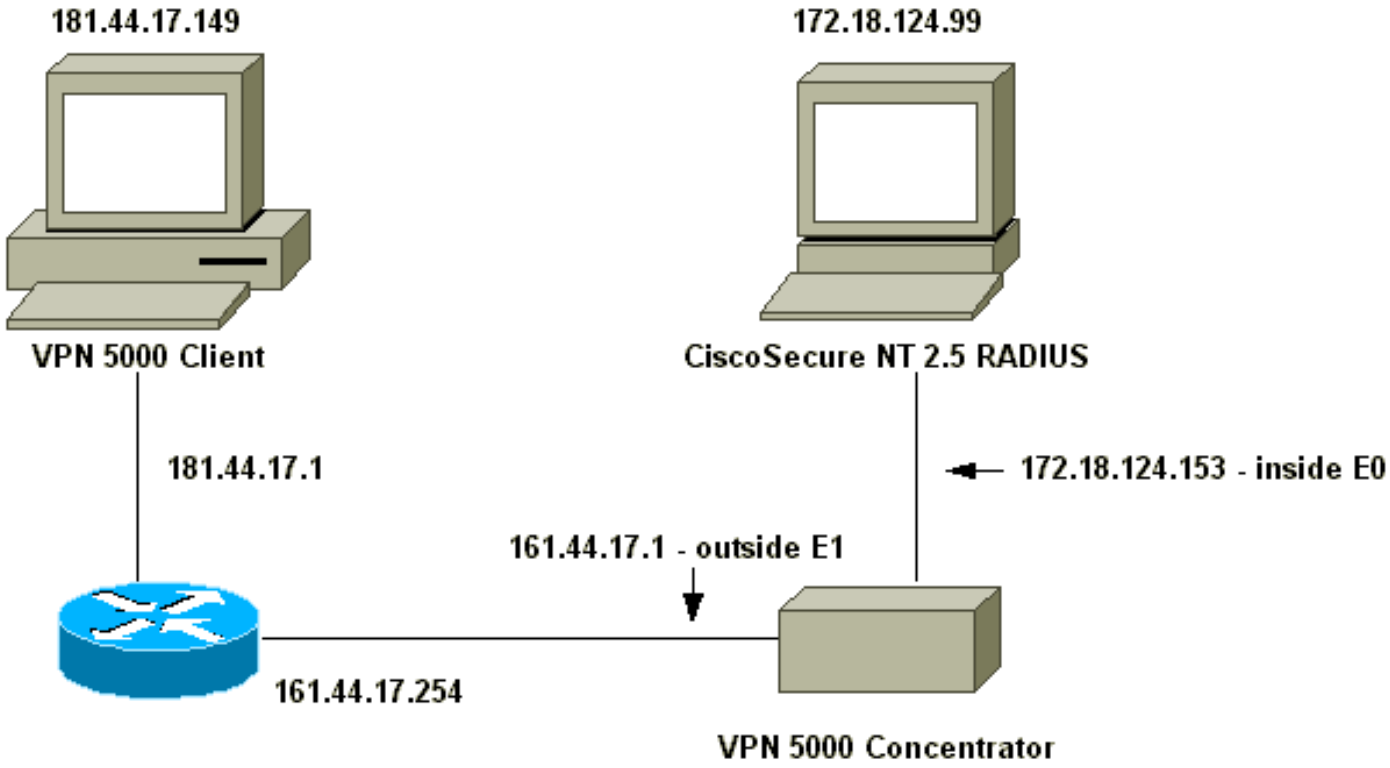
Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Nota: per ulteriori informazioni sui comandi menzionati in questo documento, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Esempio di rete

Nel documento viene usata questa impostazione di rete:



Configurazioni

Nel documento vengono usate queste configurazioni:

- 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

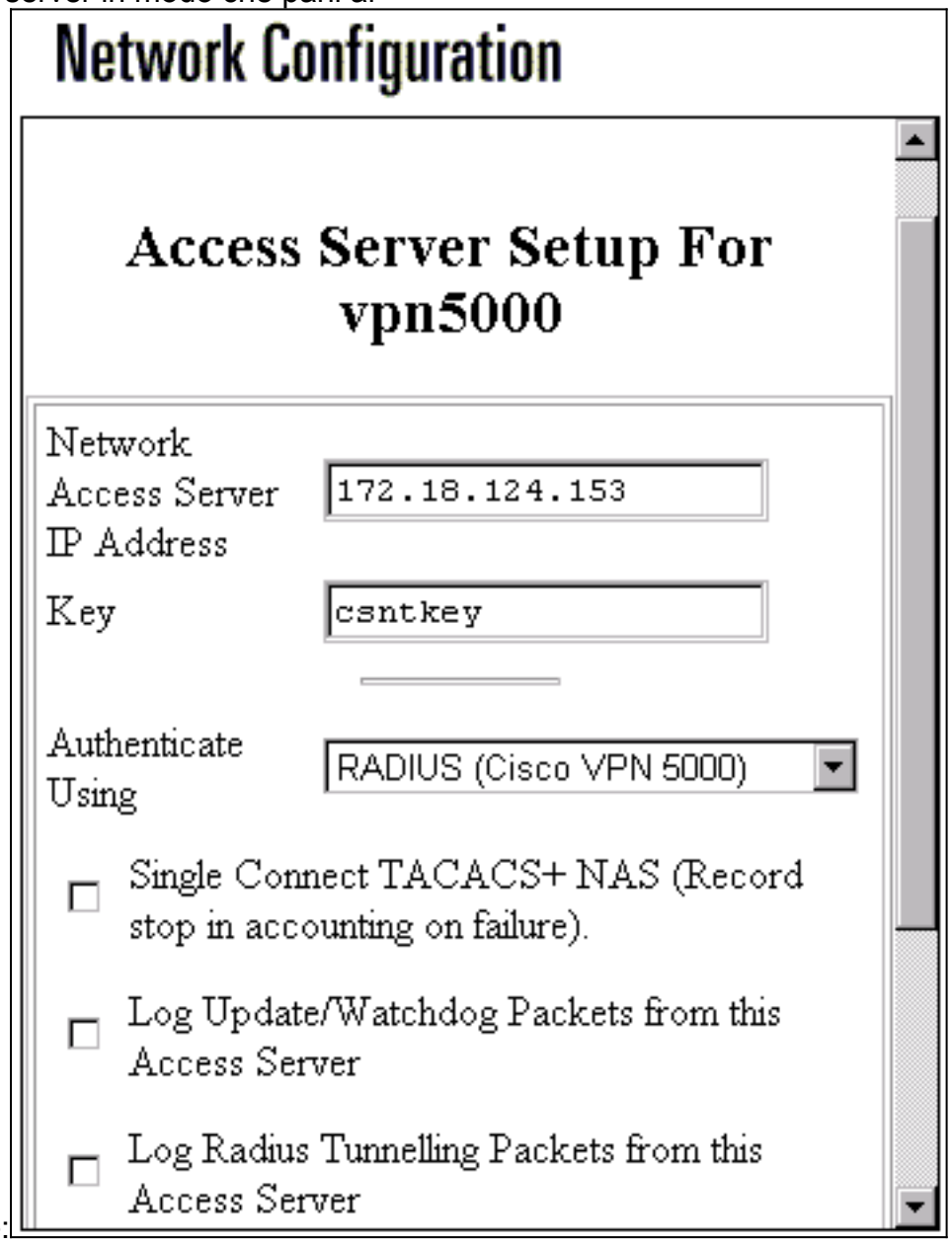
Note: None of the defaults have been changed. Two users were added, and
the appropriate passwords were entered when prompted after clicking Connect:

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

Configurazione di Cisco Secure NT 2.5

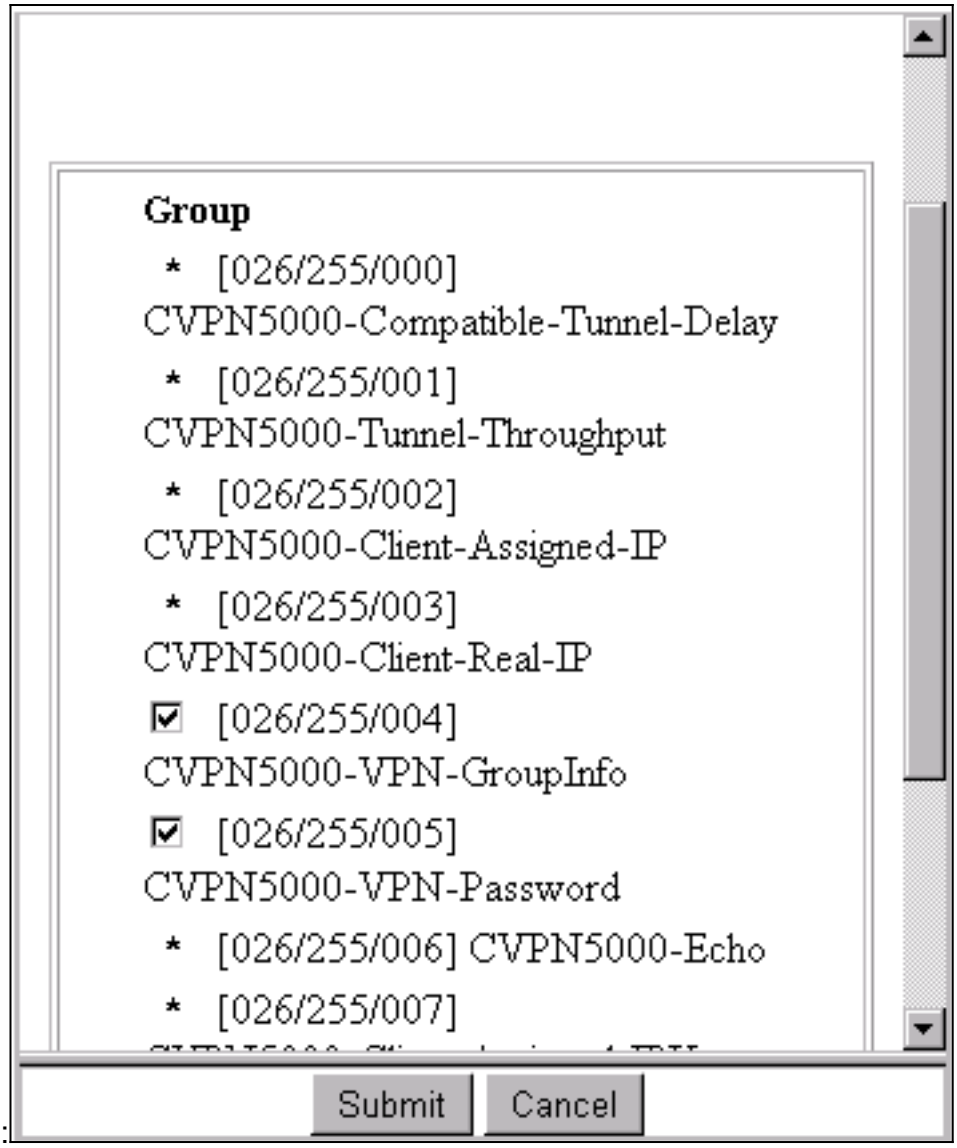
Attenersi alla procedura seguente.

1. Configurare il server in modo che parli al concentratore:

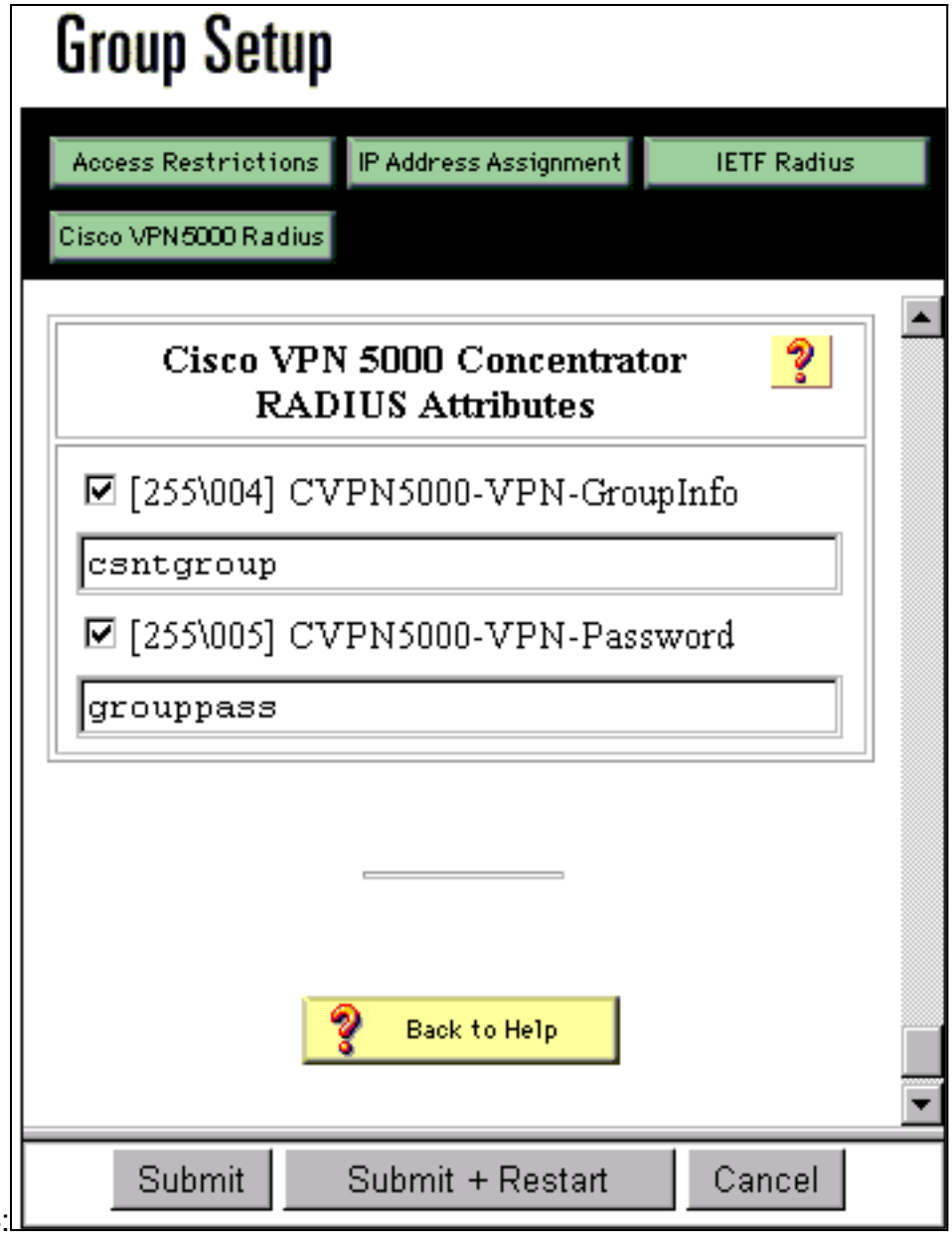


2. Andare a **Interface Configuration** > RADIUS (VPN 5000) e selezionare VPN GroupInfo e

VPN Password:



3. Dopo aver configurato l'utente ("csntuser") con una password ("csntpass") nella configurazione utente e aver inserito l'utente nel gruppo 13, configurare gli attributi VPN 5000 nella **configurazione gruppo | Gruppo**

13: 

Passaggio all'autenticazione PAP

Se l'autenticazione CHAP (Challenge Handshake Authentication Protocol) funziona, è possibile passare al protocollo PAP (Password Authentication Protocol), che consente a CSNT di utilizzare la password dell'utente del database NT.

Modifica profilo VPN 5000 RADIUS

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

Nota: CSNT verrà inoltre configurato per utilizzare il database NT per l'autenticazione dell'utente.

Elementi visualizzati dall'utente (tre caselle per la password):

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

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

Aggiunta assegnazione indirizzo IP

Se il profilo CSNT dell'utente è impostato in "Assegna indirizzo IP statico" su un valore particolare e se il gruppo VPN 5000 Concentrator è impostato su:

```
AssignIPRADIUS = On
```

Quindi, l'indirizzo IP RADIUS viene inviato dal CSNT e applicato all'utente sul concentratore VPN 5000.

Aggiunta di accounting

Per inviare i record di accounting delle sessioni al server Cisco Secure RADIUS, aggiungere alla configurazione VPN 5000 Concentrator RADIUS:

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

Per rendere effettiva la modifica, è necessario utilizzare i comandi **apply** e **write** e quindi il comando **boot** sulla VPN 5000.

Record contabili da 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
```

Verifica

Le informazioni contenute in questa sezione permettono di verificare che la configurazione funzioni correttamente.

Alcuni comandi **show sono supportati dallo** strumento Output Interpreter (solo utenti registrati); lo strumento permette di visualizzare un'analisi dell'output del comando **show.**

- **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
```

- **dump di traccia vpn - tutto**

```
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>
```

Risoluzione dei problemi

Di seguito sono riportati i possibili errori che possono verificarsi.

Cisco Secure NT Server non è raggiungibile

Debug 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.
```

Aspetti visualizzati dall'utente:

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

Autenticazione non riuscita

Il nome utente o la password su Cisco Secure NT è errata.

Debug 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.
```

Aspetti visualizzati dall'utente:

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

Cisco Secure:

Andare a **Report** e **attività** e il registro dei tentativi non riusciti mostra l'errore.

La password del gruppo VPN immessa dall'utente non è compatibile con la password VPN

Debug 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
```

Aspetti visualizzati dall'utente:

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

Cisco Secure:

Passare a **Report** e **attività** e il registro dei tentativi non riusciti non visualizza l'errore.

Il nome del gruppo inviato dal server RADIUS non esiste sulla VPN 5000

Debug 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)
```

Aspetti visualizzati dall'utente:

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

Cisco Secure:

Andare a **Report** e **attività** e il registro dei tentativi non riusciti *non* mostra l'errore.

Informazioni correlate

- Pagina di supporto di Cisco Secure ACS per Windows
- Cisco VPN serie 5000 concentrator: annuncio di fine vendita
- Pagina di supporto per Cisco VPN 5000 Concentrator
- Pagina di supporto per i client Cisco VPN 5000
- Pagina di supporto per IPsec
- Pagina di supporto RADIUS
- RFC (Requests for Comments)
- Documentazione e supporto tecnico – Cisco Systems