Authentifizieren des VPN 5000-Clients für den VPN 500-Konzentrator mit CiscoSecure NT 2.5 und höher (RADIUS)

Inhalt

Einführung

Cisco Secure NT (CSNT) 2.5 und höher (RADIUS) kann anbieterspezifische Attribute Virtual Private Network (VPN) 5000 für VPN GroupInfo und VPN Password zurückgeben, um einen VPN 5000-Client für den VPN 5000-Konzentrator zu authentifizieren. Im folgenden Dokument wird davon ausgegangen, dass die lokale Authentifizierung funktioniert, bevor RADIUS-Authentifizierung hinzugefügt wird (daher wird unser Benutzer, "localuser", in der Gruppe "ciscolocal", "localuser" genannt). Dann wird der CSNT RADIUS-Authentifizierung für Benutzer hinzugefügt, die nicht in der lokalen Datenbank vorhanden sind (der Benutzer "csntuser" wird der Gruppe "csntgroup" anhand der vom CSNT-RADIUS-Server zurückgegebenen Attribute zugewiesen).

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

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

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions.

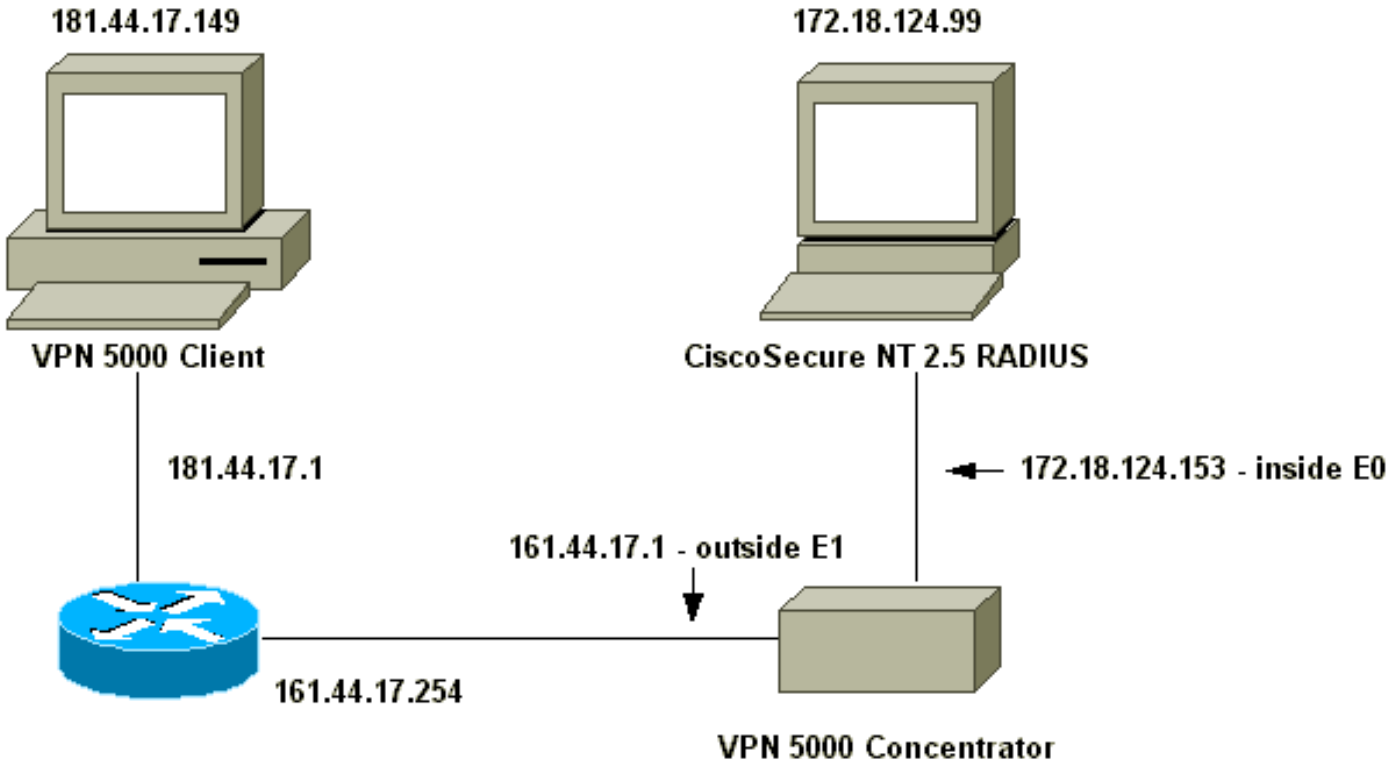
Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Hinweis: Um weitere Informationen zu den in diesem Dokument verwendeten Befehlen zu erhalten, verwenden Sie das Command Lookup Tool (nur registrierte Kunden).

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Konfigurationen

In diesem Dokument werden folgende Konfigurationen verwendet:

- 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

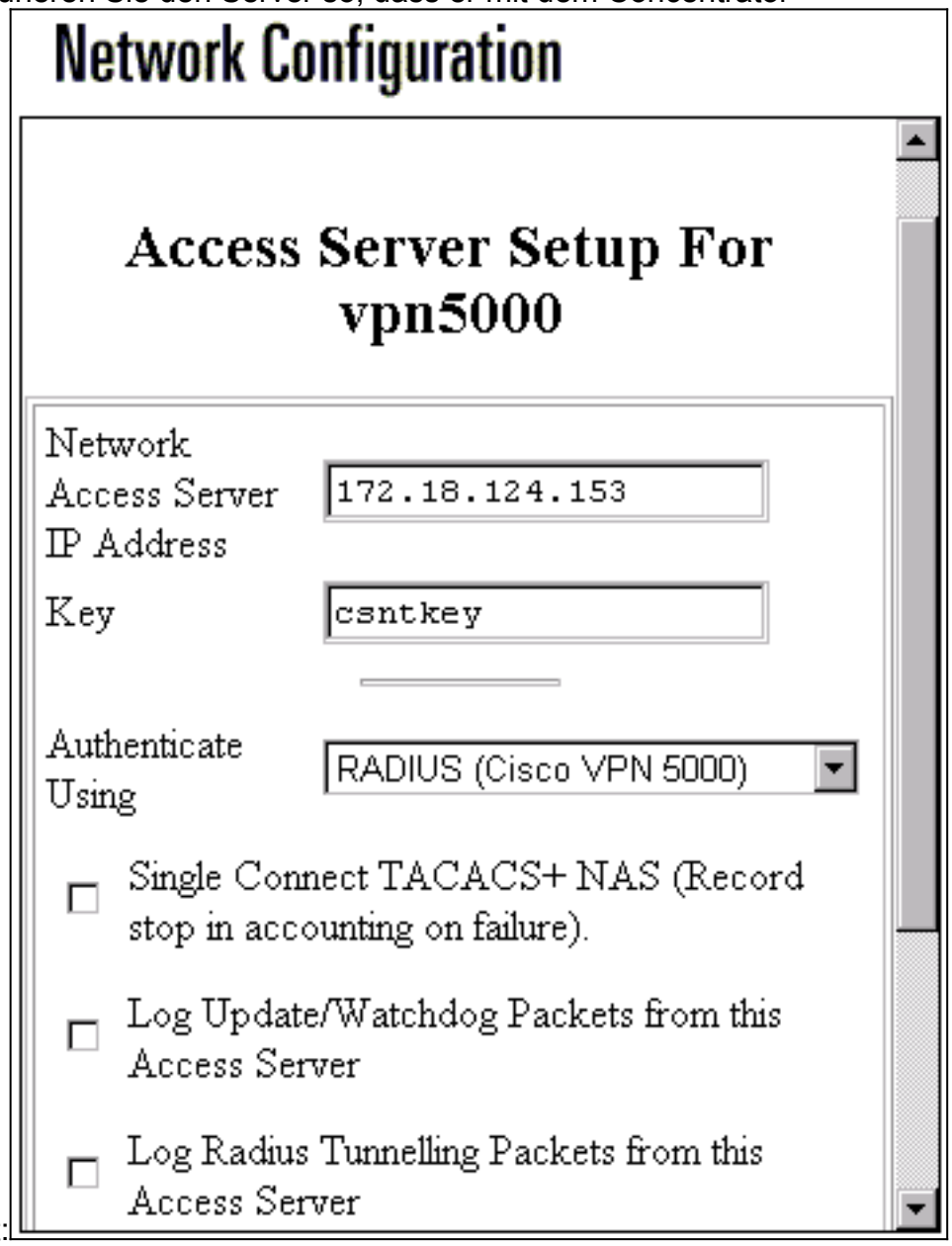
Note: None of the defaults have been changed. Two users were added, and
the appropriate passwords were entered when prompted after clicking Connect:

username	password	radius_password
localuser	localike	N/A
csntuser	grouppass	csntpass

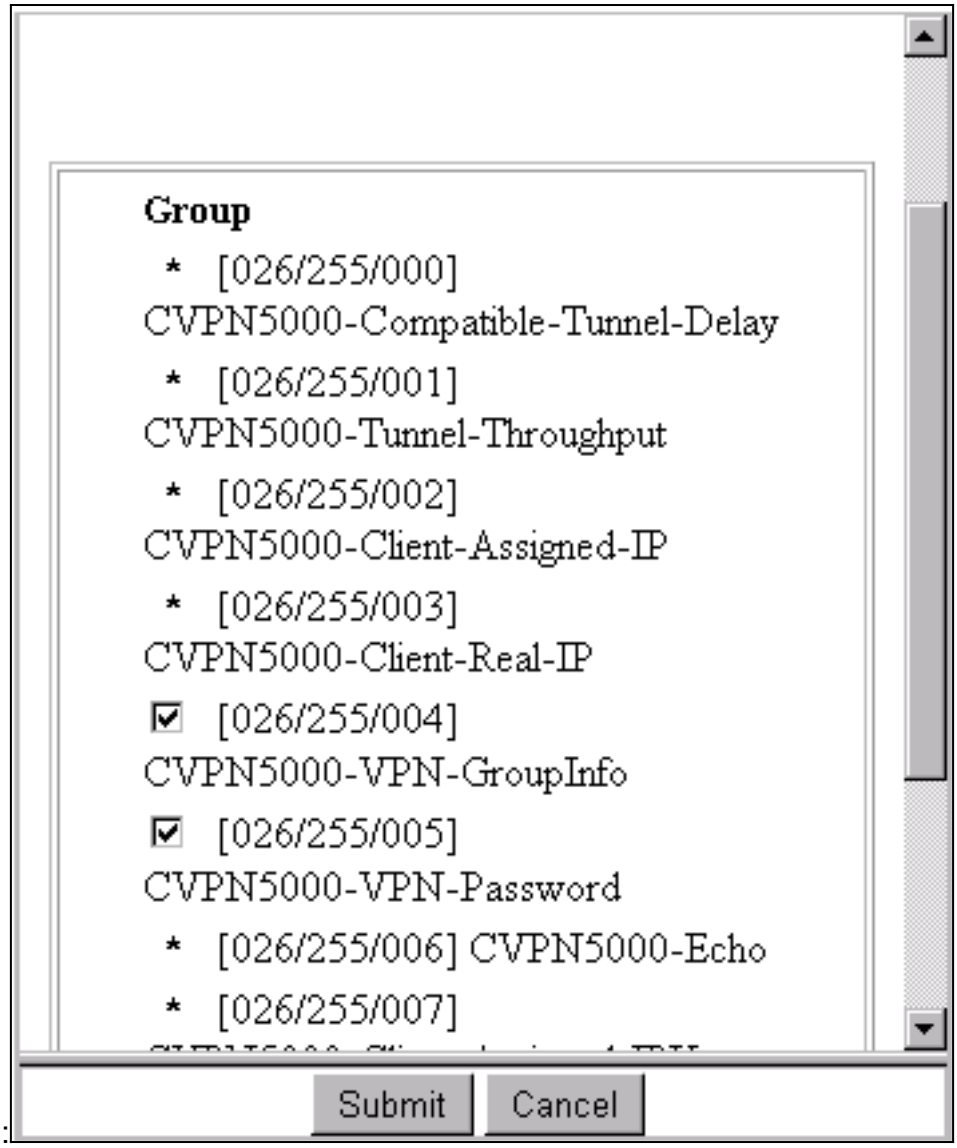
Konfiguration von Cisco Secure NT 2.5

Befolgen Sie dieses Verfahren.

1. Konfigurieren Sie den Server so, dass er mit dem Concentrator spricht:

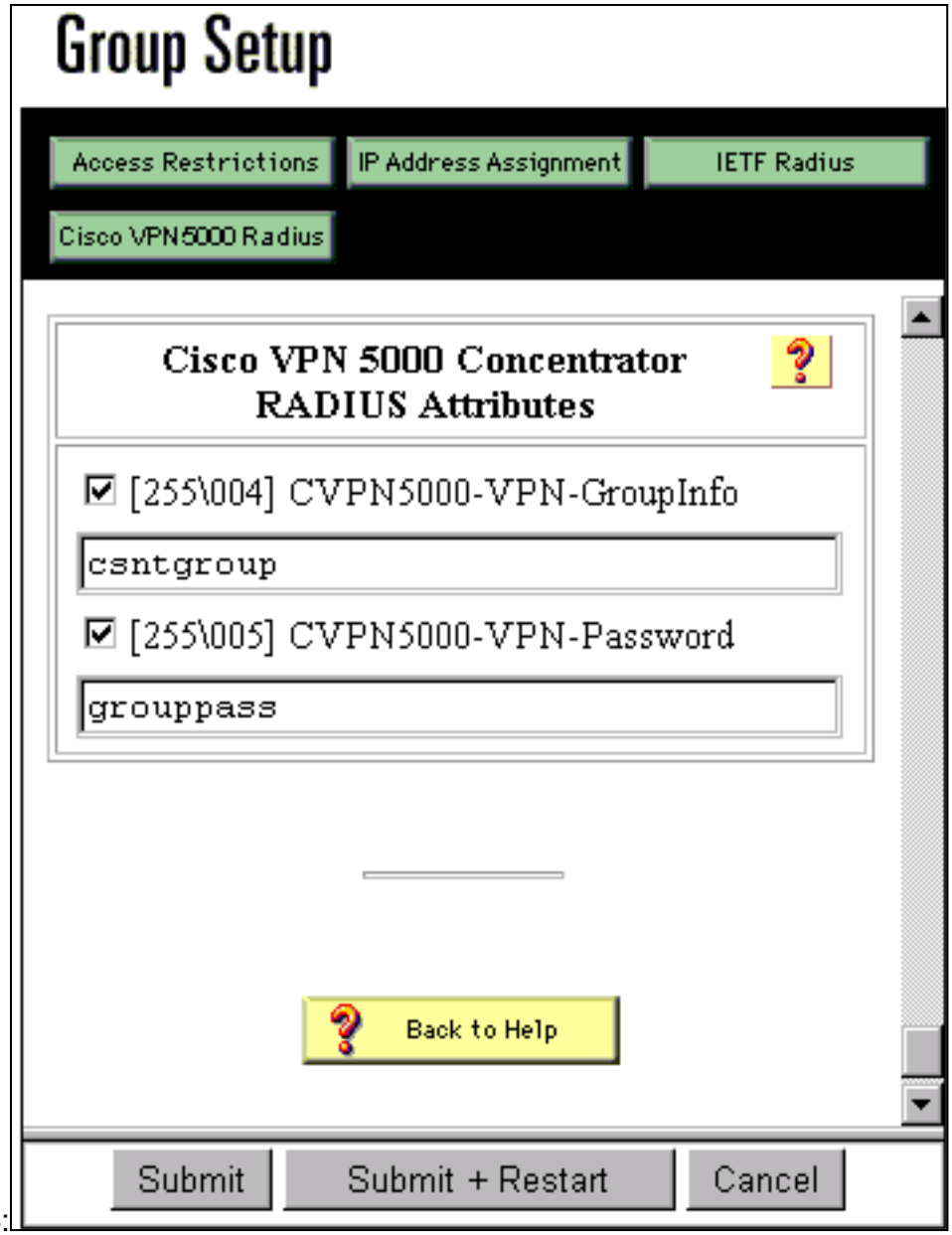


2. Gehen Sie zu **Schnittstellenkonfiguration > RADIUS (VPN 5000)**, und aktivieren Sie VPN GroupInfo und VPN



Password:

3. Nachdem der Benutzer ("csntuser") im User Setup mit einem Kennwort ("csntpass") konfiguriert und der Benutzer in Gruppe 13 eingeordnet wurde, konfigurieren Sie die VPN 500-Attribute im **Group Setup. | Gruppe**

13: 

Ändern zur PAP-Authentifizierung

Wenn die CHAP-Authentifizierung (Challenge Handshake Authentication Protocol) funktioniert, können Sie zu Password Authentication Protocol (PAP) wechseln, mit dem Sie festlegen können, dass das Kennwort des Benutzers von der NT-Datenbank aus vom CSNT verwendet wird.

Änderung des VPN 5000-RADIUS-Profils

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

Hinweis: CSNT würde auch so konfiguriert, dass die NT-Datenbank für die Authentifizierung dieses Benutzers verwendet wird.

Was der Benutzer sieht (drei Kennwortfelder):

```
Shared Secret = grouppass
```

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

Hinzufügen der IP-Adressenzuweisung

Wenn das CSNT-Profil des Benutzers in "Assign static IP Address" (Statische IP-Adresse zuweisen) auf einen bestimmten Wert festgelegt ist und wenn die VPN 5000 Concentrator-Gruppe für Folgendes festgelegt ist:

```
AssignIPRADIUS = On
```

Anschließend wird die RADIUS-IP-Adresse aus CSNT versendet und auf den Benutzer im VPN 5000-Konzentrator angewendet.

Hinzufügen von Buchhaltung

Wenn Sie Datensätze zur Sitzungsabrechnung an den Cisco Secure RADIUS-Server senden möchten, fügen Sie diese zur RADIUS-Konfiguration des VPN 500 Concentrator hinzu:

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

Sie müssen die **Befehle zum Anwenden** und **Schreiben** und anschließend den Befehl **boot** auf dem VPN 5000 verwenden, damit diese Änderung wirksam wird.

Buchhaltungsaufzeichnungen von 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
```

Überprüfen

Dieser Abschnitt enthält Informationen, mit denen Sie überprüfen können, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Bestimmte **show**-Befehle werden vom Output Interpreter Tool unterstützt (nur registrierte Kunden), mit dem Sie eine Analyse der **show**-Befehlsausgabe anzeigen können.

- **Systemprotokollspeicher anzeigen**

```
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-Ablaufverfolgungsdump alle**

```
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>
```

Fehlerbehebung

Folgende Fehler können auftreten.

Cisco Secure NT Server ist nicht erreichbar

VPN 5000-Fehlersuche

```
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.
```

Was der Benutzer sieht:

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

Authentifizierungsfehler

Der Benutzername oder das Kennwort in Cisco Secure NT sind ungültig.

VPN 5000-Fehlersuche

```
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.
```

Was der Benutzer sieht:

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

Cisco Secure:

Gehen Sie zu **Berichte** und **Aktivität**, und das Fehlerprotokoll zeigt den Fehler an.

Das vom Benutzer eingegebene VPN-Gruppenkennwort stimmt nicht mit dem VPN-Kennwort überein.

VPN 5000-Fehlersuche

```
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
```

Was der Benutzer sieht:

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

Cisco Secure:

Gehen Sie zu **Berichte** und **Aktivität**, und das Fehlerprotokoll zeigt den Fehler nicht an.

Der vom RADIUS-Server gesendete Gruppenname existiert auf dem VPN 5000 nicht.

VPN 5000-Fehlersuche

```
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)
```

Was der Benutzer sieht:

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

Cisco Secure:

Gehen Sie zu **Berichte** und **Aktivität**, und das Fehlerprotokoll *zeigt* den Fehler *nicht* an.

Zugehörige Informationen

- Support-Seite für Cisco Secure ACS für Windows
- Cisco VPN Concentrators der Serie 5000 - Ankündigung des Vertriebsendes
- Support-Seite für Cisco VPN 500 Concentrator
- Support-Seite für Cisco VPN 5000-Client
- IPsec-Support-Seite
- RADIUS-Support-Seite
- Anforderungen für Kommentare (RFCs)
- Technischer Support und Dokumentation - Cisco Systems