如何使用CiscoSecure NT 2.5及更高版本(RADIUS)向VPN 5000集中器驗證VPN 5000客戶端

目錄

簡介

Cisco Secure NT(CSNT)2.5及更高版本(RADIUS)能夠為VPN GroupInfo返回Virtual Private Network(VPN)5000供應商特定屬性和VPN密碼，以向VPN 5000集中器驗證VPN 5000客戶端。以下檔案假設在新增RADIUS驗證之前，本地驗證工作正常（因此組「ciscolocal」中的使用者「localuser」）。 然後為本地資料庫中不存在的使用者向CSNT RADIUS新增身份驗證（通過從CSNT RADIUS伺服器返回的屬性，將使用者「csntuser」分配給組「csntgroup」）。

必要條件

需求

本文件沒有特定需求。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco安全NT 2.5
- Cisco VPN 5000 Concentrator 5.2.16.0005
- Cisco VPN 5000使用者端4.2.7

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

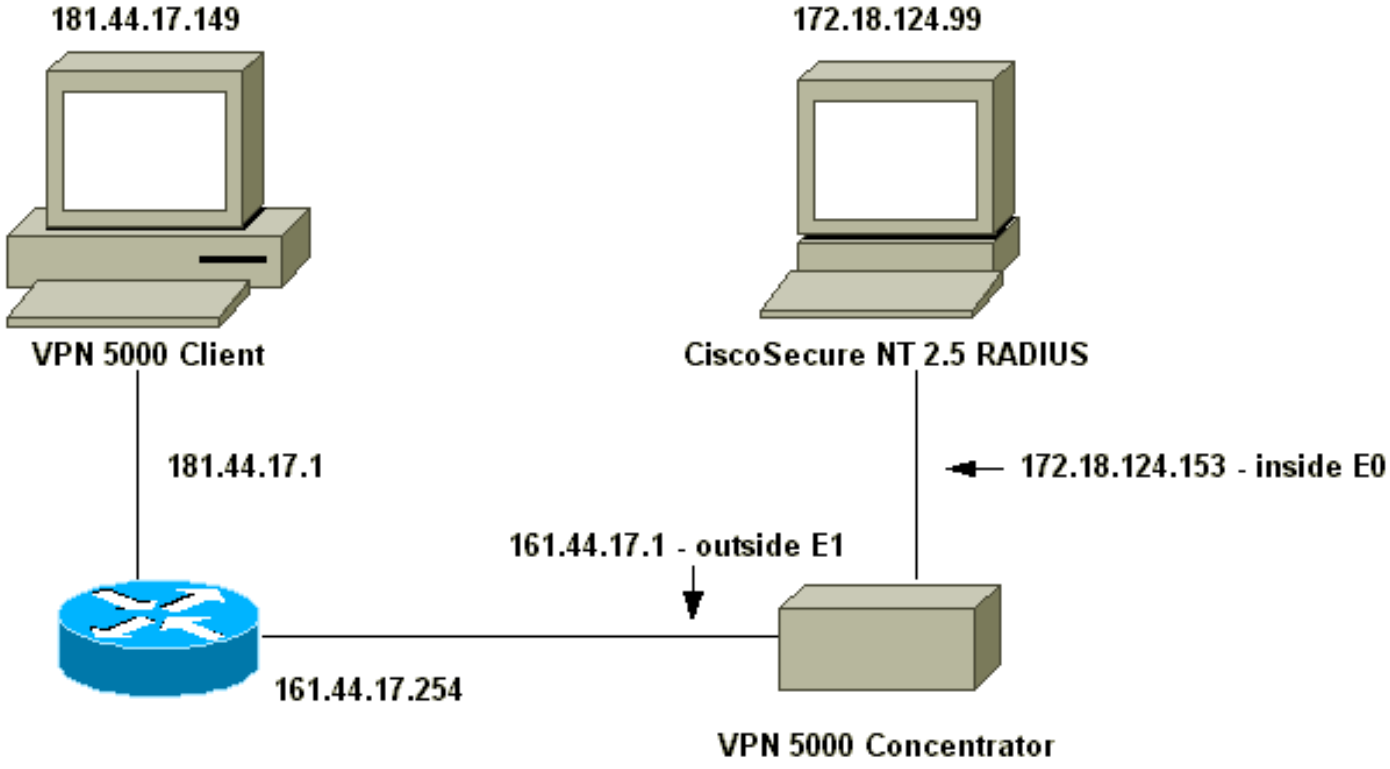
設定

本節提供用於設定本文件中所述功能的資訊。

注意：要查詢有關本文檔中使用的命令的其他資訊，請使用命令查詢工具(僅限註冊客戶)。

網路圖表

本檔案會使用以下網路設定：



組態

本檔案會使用以下設定：

- VPN 5000 Concentrator
- VPN 5000客戶端

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客戶端

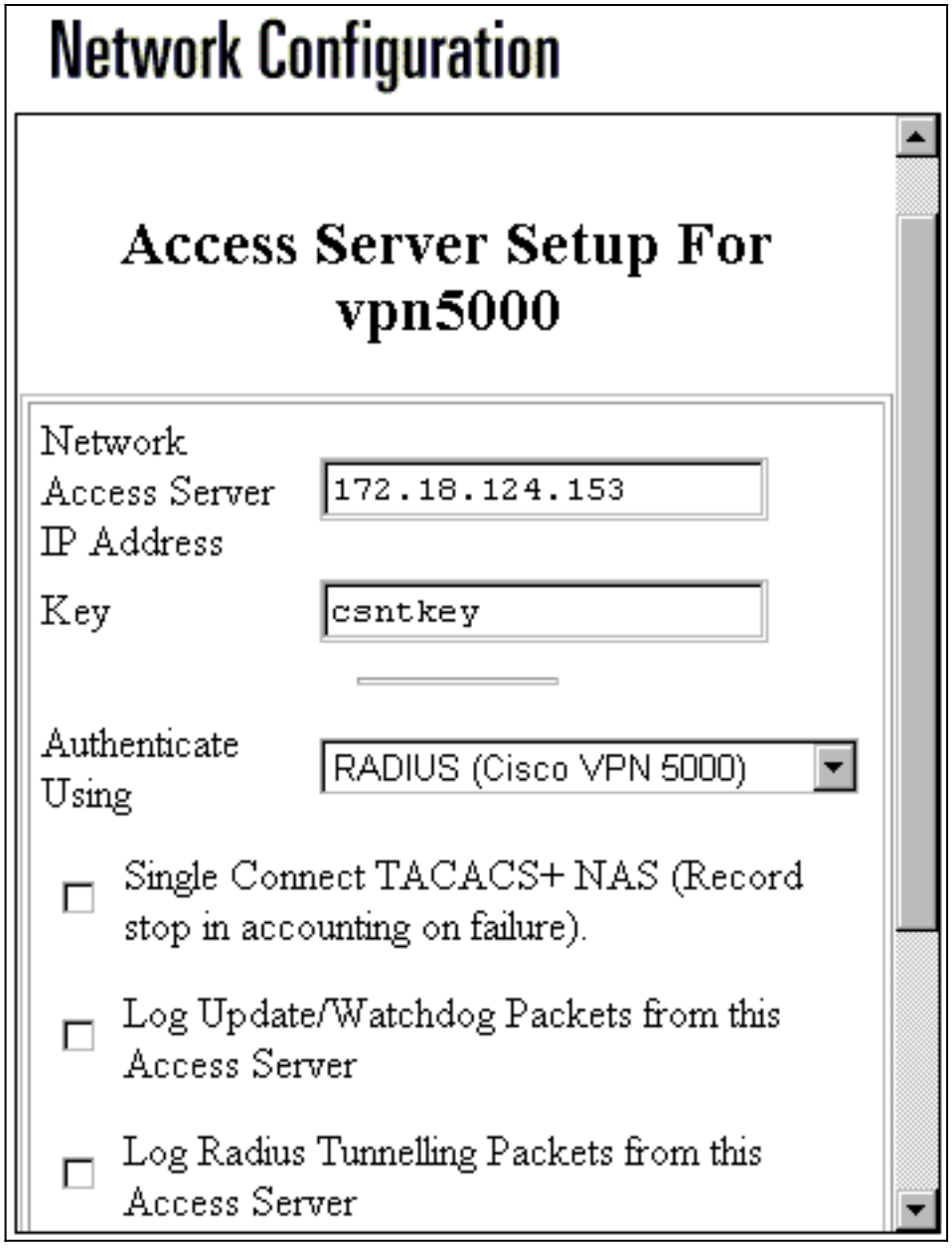
Note: None of the defaults have been changed. Two users were added, and
the appropriate passwords were entered when prompted after clicking Connect:

username	password	radius_password
localuser	localike	N/A
csntuser	grouppass	csntpass

Cisco Secure NT 2.5配置

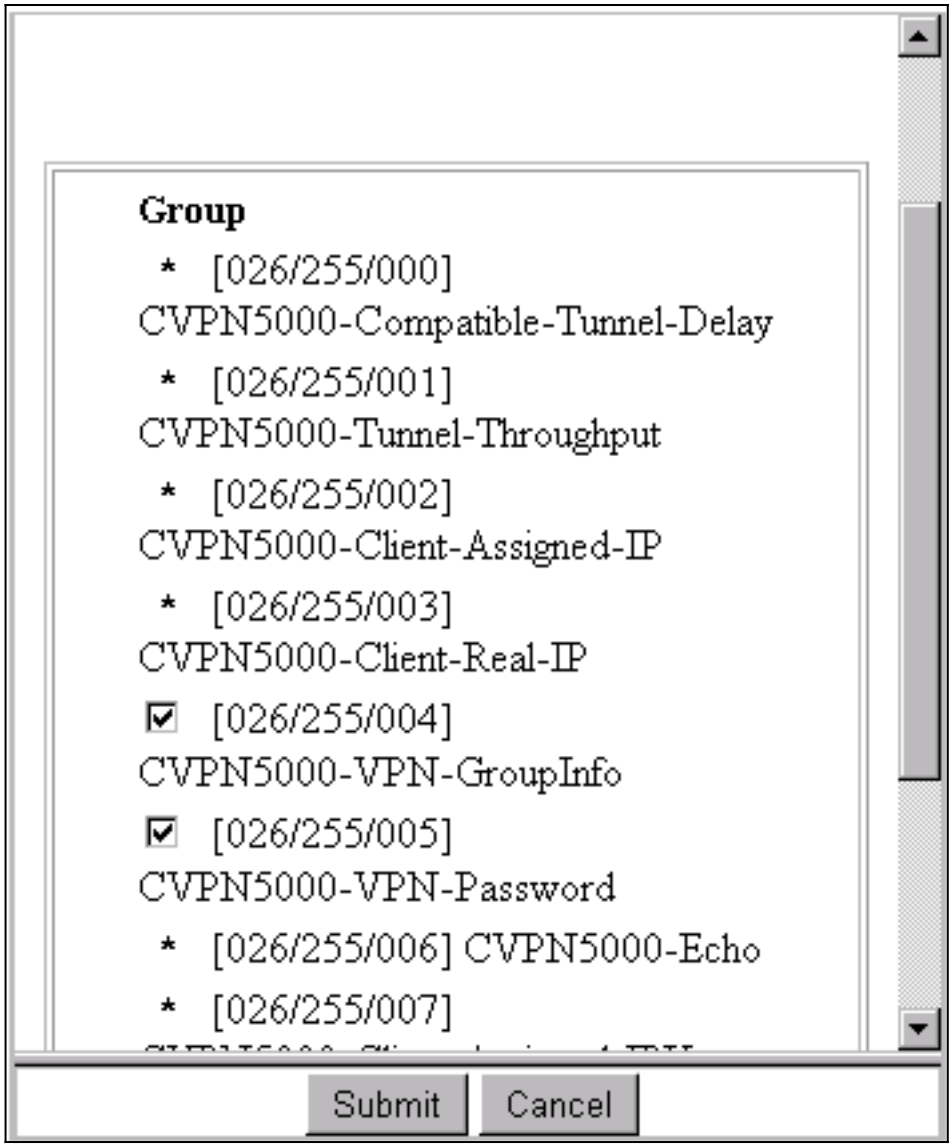
請按照以下步驟操作。

1. 將伺服器配置為與集中器通話



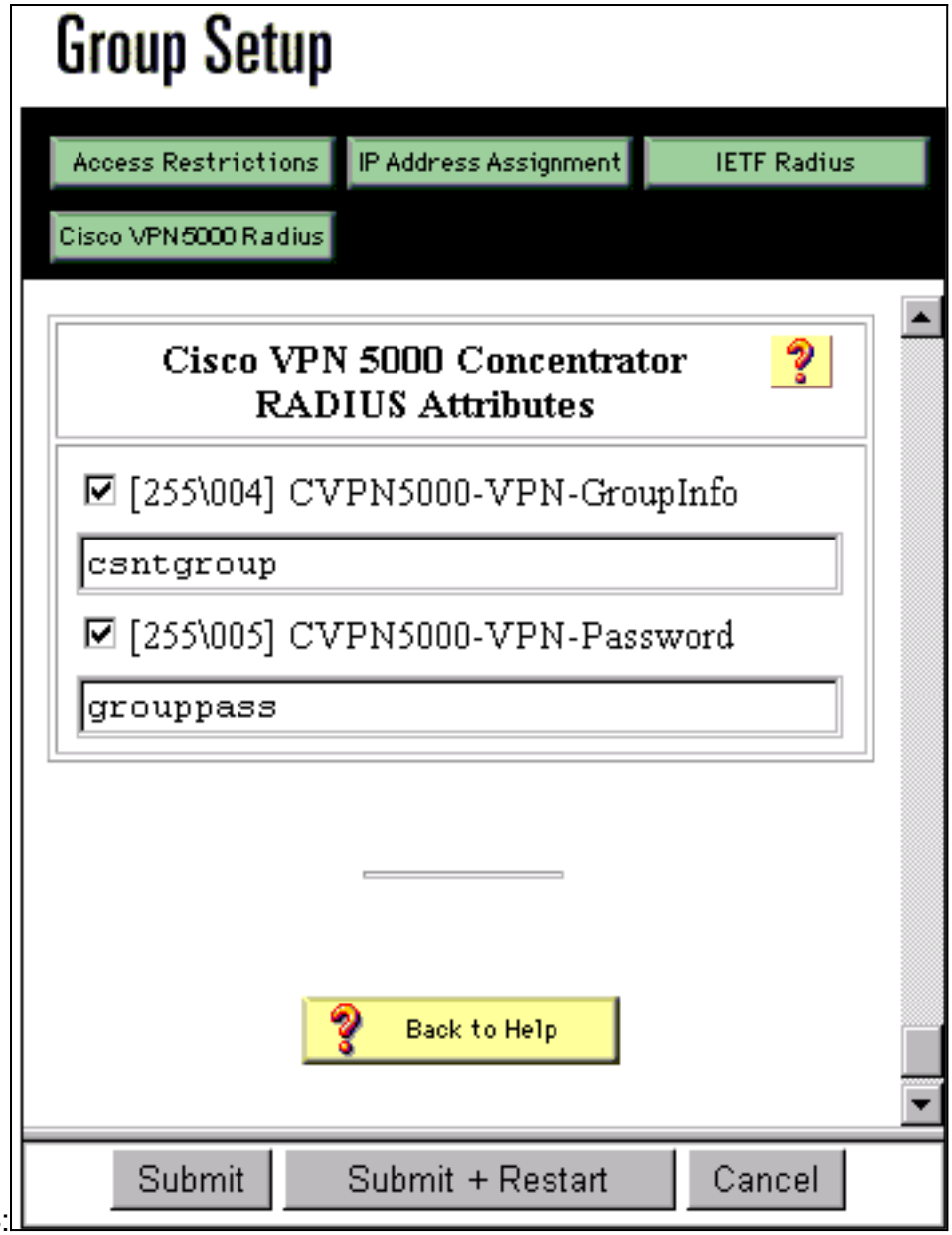
:

2. 前往**Interface Configuration > RADIUS(VPN 5000)**並檢查VPN GroupInfo和VPN密碼



:

3. 在使用者設定中使用密碼(「csntpass」)配置使用者(「csntuser」)並將該使用者置於組13後，在組設定中配置VPN 5000**屬性 |組**

13: 

更改為PAP身份驗證

假設質詢握手身份驗證協定(CHAP)身份驗證有效，您可能希望更改為密碼身份驗證協定(PAP)，這使您能夠讓CSNT使用NT資料庫中的使用者密碼。

VPN 5000 RADIUS設定檔變更

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

注意：CSNT也會配置為使用NT資料庫對該使用者進行身份驗證。

使用者看到的內容（三個密碼框）：

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

新增IP地址分配

如果使用者的CSNT配置檔案在「分配靜態IP地址」中設定為特定值，並且VPN 5000集中器組設定為：

```
AssignIPRADIUS = On
```

然後，從CSNT向下傳送RADIUS IP地址，並將其應用到VPN 5000集中器上的使用者。

新增記帳

如果要將會話記賬記錄傳送到Cisco Secure RADIUS伺服器，則將其新增到VPN 5000集中器RADIUS配置：

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

您必須使用**apply**和**write**命令，然後在VPN 5000上使用**boot**命令以使此更改生效。

來自CSNT的會計記錄

```
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
```

驗證

本節提供的資訊可用於確認您的組態是否正常運作。

輸出直譯器工具(僅供註冊客戶使用)支援某些**show**命令，此工具可讓您檢視show命令輸出的分析。

- **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>
```

疑難排解

以下是您可能會遇到的錯誤。

Cisco Secure NT Server無法訪問

VPN 5000偵錯

```
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.
```

使用者看到的內容：

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

身份驗證失敗

Cisco Secure NT上的使用者名稱或密碼錯誤。

VPN 5000偵錯

```
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.
```

使用者看到的內容：

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

Cisco Secure:

轉到Reports和Activity，失敗嘗試日誌將顯示失敗。

使用者輸入的VPN組密碼與VPN密碼不一致

VPN 5000偵錯

```
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
```

使用者看到的內容：

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

Cisco Secure:

轉到Reports和Activity，失敗嘗試日誌不會顯示失敗。

VPN 5000上不存在RADIUS伺服器傳送的組名

VPN 5000偵錯

```
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)
```

使用者看到的內容：

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

Cisco Secure:

轉到**Reports**和**Activity**，失敗嘗試日誌不會*顯示失敗*。

相關資訊

- Cisco Secure ACS for Windows支援頁
- Cisco VPN 5000系列集中器銷售終止公告
- Cisco VPN 5000集中器支援頁
- Cisco VPN 5000使用者端支援頁面
- IPsec支援頁面
- RADIUS 支援頁面
- 要求建議 (RFC)
- 技術支援與文件 - Cisco Systems