如何使用CiscoSecure NT 2.5及以上版本 (RADIUS) 为VPN 5000客户端到VPN 5000集中器做认证

目录

[简介](#)
[先决条件](#)
[要求](#)
[使用的组件](#)
[规则](#)
[配置](#)
[网络图](#)
[配置](#)
[Cisco Secure NT 2.5 配置](#)
[改为 PAP 认证](#)
[VPN 5000 RADIUS 配置文件更改](#)
[添加 IP 地址分配](#)
[增加记账功能](#)
[验证](#)
[故障排除](#)
[Cisco Secure NT 服务器不可达](#)
[身份认证失败](#)
[用户输入的 VPN 组密码与 VPNPassword 不一致](#)
[RADIUS 服务器发送的组名在 VPN 5000 中不存在](#)
[相关信息](#)

简介

Cisco Secure NT (CSNT) 2.5 及更高版本 (RADIUS) 能够为 VPN GroupInfo 和 VPN Password 返回虚拟私有网络 (VPN) 5000 供应商特定的属性以在 VPN 5000 集中器中对 VPN 5000 客户端进行身份验证。以下文档假设在添加 RADIUS 身份验证之前已使用本地身份验证（因此我们的用户“localuser”在组“ciscolocal”中）。 然后，针对本地数据库中不存在的用户，将身份验证添加到 CSNT RADIUS 中（利用从 CSNT RADIUS 服务器返回的属性，将用户“csntuser”分配到组“csntgroup”中）。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco Secure NT 2.5
- Cisco VPN 5000 集中器 5.2.16.0005
- Cisco VPN 5000 Client 4.2.7

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文件规则的更多信息请参见“ Cisco技术提示规则”。

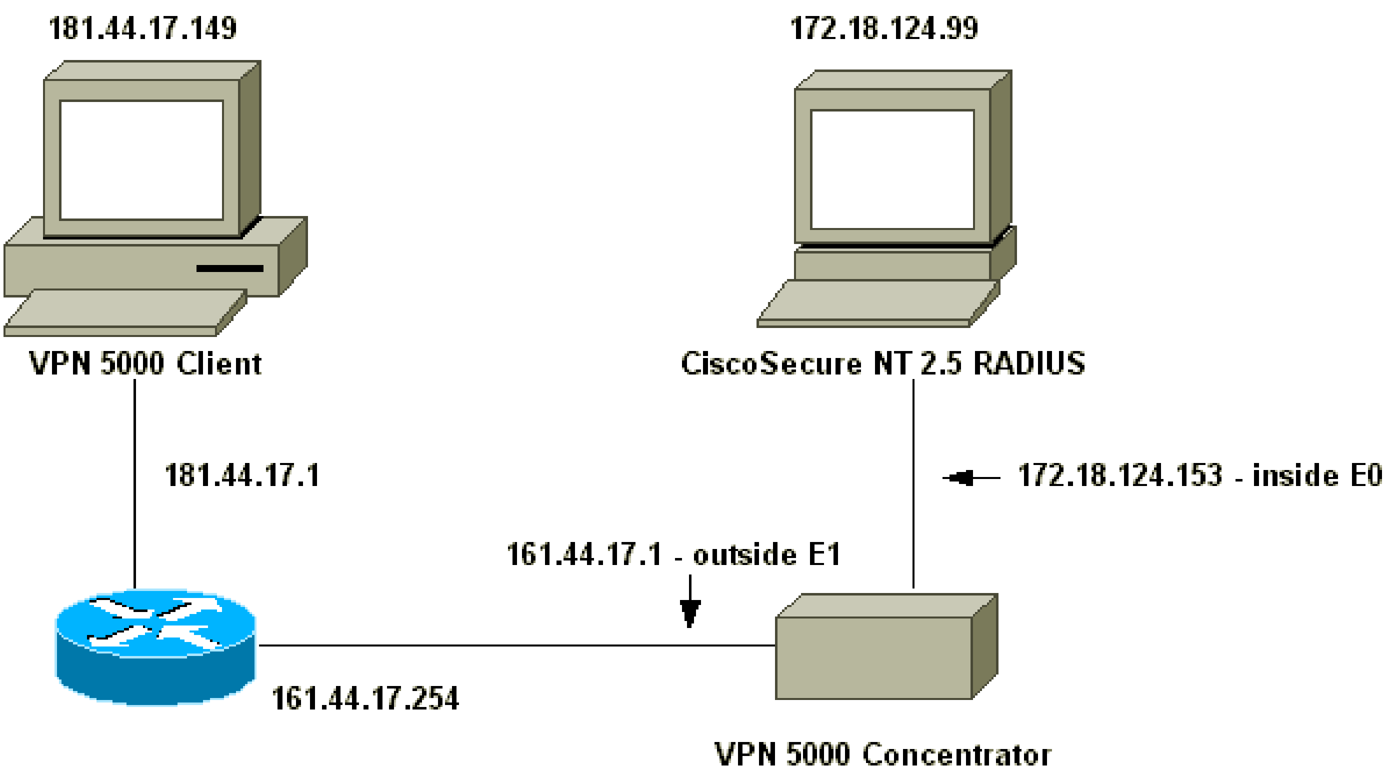
配置

本部分提供有关如何配置本文档所述功能的信息。

注：要查找有关本文档中使用的命令的其他信息，请使用命令查找工具(仅注册客户)。

网络图

本文档使用以下网络设置：



配置

本文档使用以下配置：

- VPN 5000 集中器
- VPN 5000 客户端

VPN 5000 集中器

```
[ 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 客户端

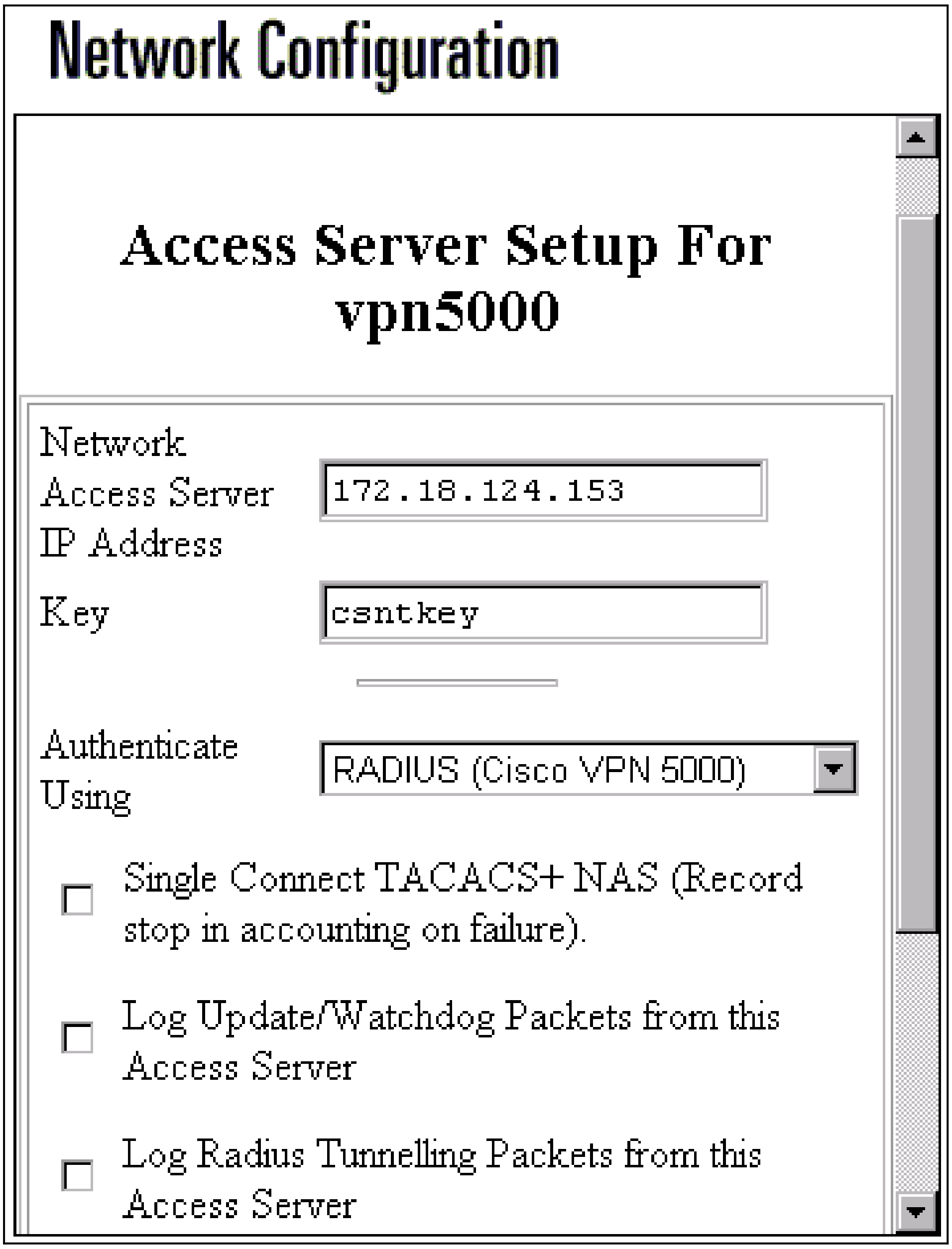
```
Note: None of the defaults have been changed. Two users
were added, and
the appropriate passwords were entered when prompted
after clicking Connect:

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

Cisco Secure NT 2.5 配置

遵循该步骤。

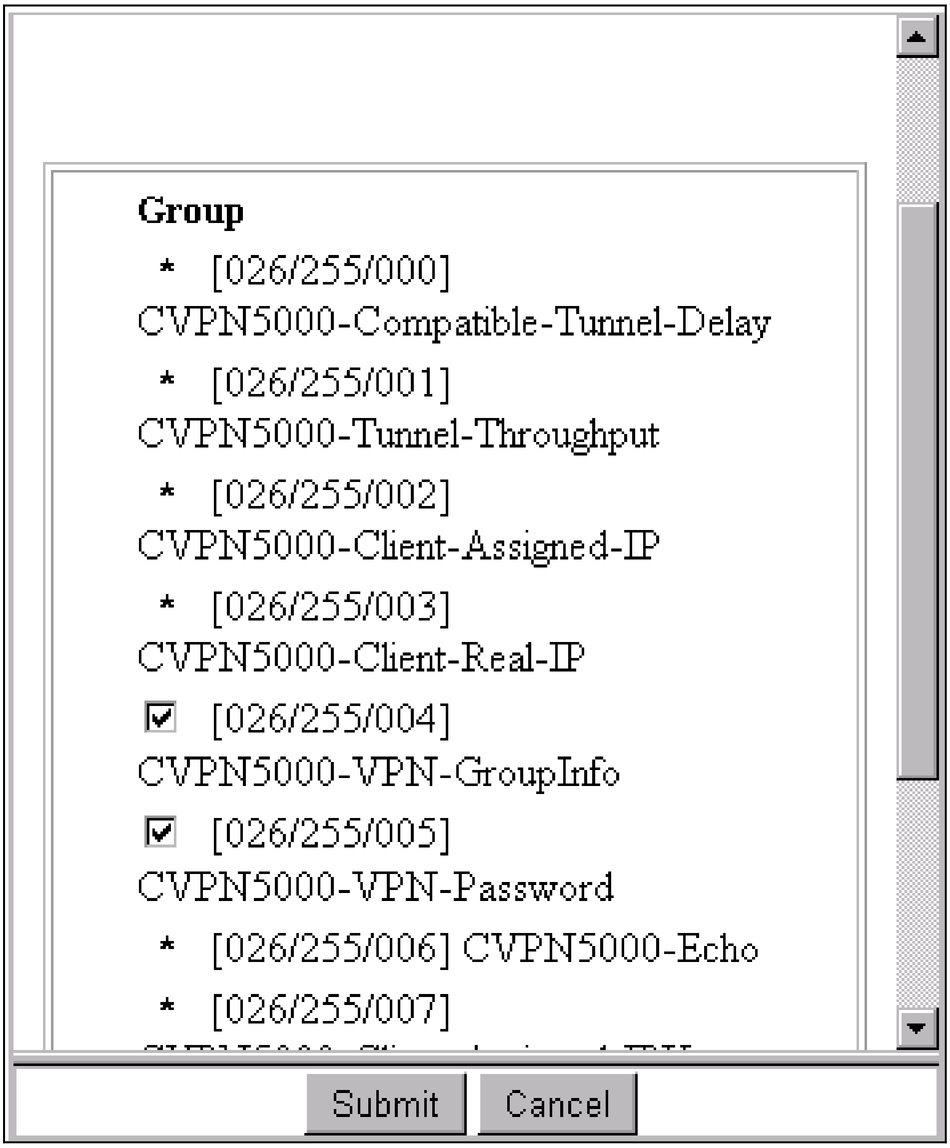
1. 配置服务器以与集中器通信



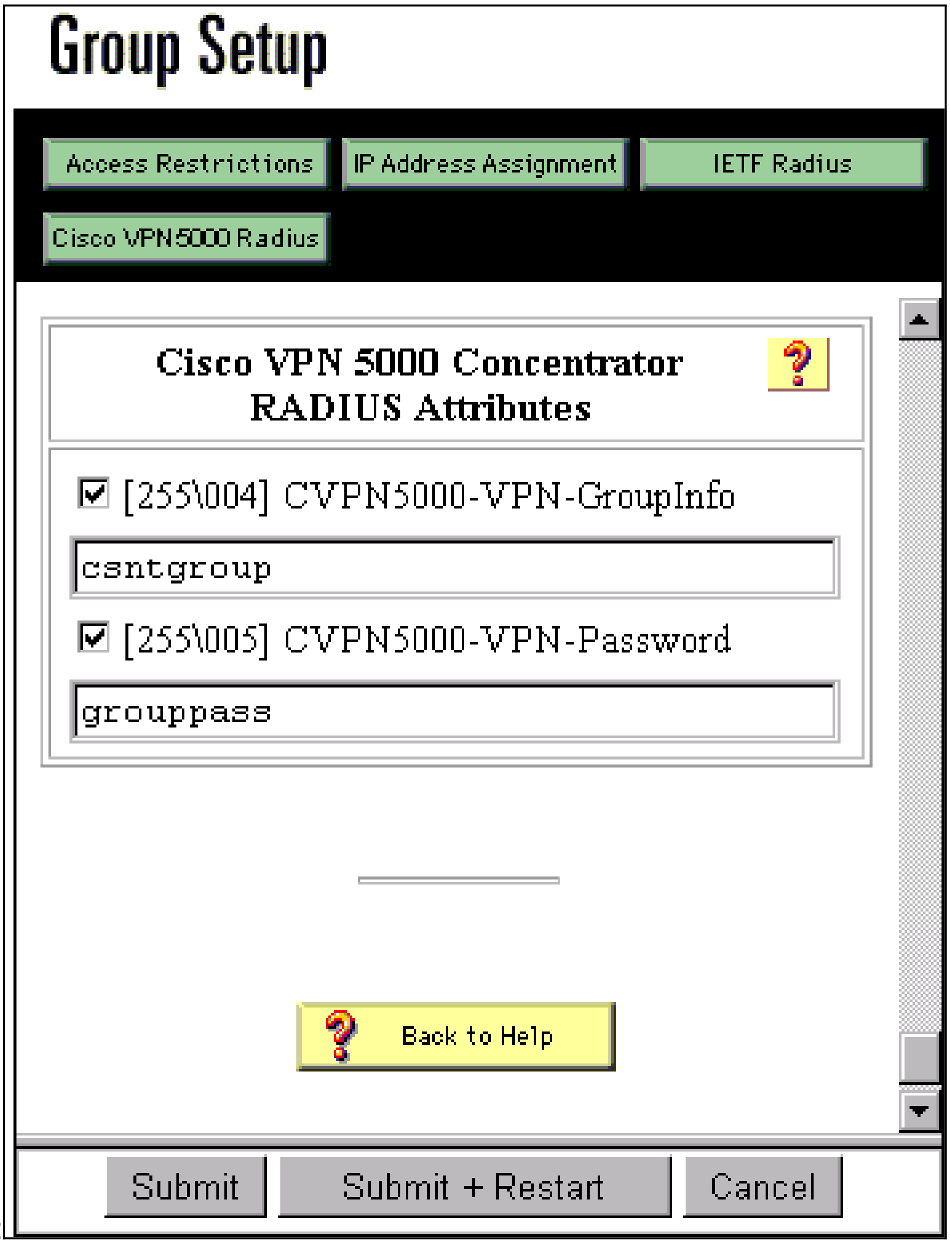
:

2. 转到 **Interface Configuration > RADIUS (VPN 5000) 并检查 VPN GroupInfo 和 VPN**

Password：



3. 在 User Setup 中使用密码（“csntpass”）配置用户（“csntuser”）并将该用户放置在 Group 13 中后，在 **Group Setup |组**



13:

改为 PAP 认证

假设已使用质询握手身份验证协议 (CHAP) 身份验证，您可能希望更改为密码身份验证协议 (PAP)，这使您能够让 CSNT 使用 NT 数据库中的用户密码。

VPN 5000 RADIUS 配置文件更改

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

注意：CSNT也将配置为使用NT数据库进行该用户的身份验证。

用户看到的内容（三个密码框）：

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

添加 IP 地址分配

如果用户的 CSNT 配置文件在“Assign static IP Address”中设置为特定值，并且 VPN 5000 Concentrator 组设置为：

```
AssignIPRADIUS = On
```

那么，从 CSNT 向下发送 RADIUS IP 地址并将其应用于 VPN 5000 集中器上的用户。

增加记账功能

如果您希望将会话记帐记录发送给 Cisco Secure RADIUS 服务器，请添加到 VPN 5000 集中器 RADIUS 配置：

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

您必须在 VPN 5000 上使用 **apply 和 write 命令，然后使用 boot 命令才能使此更改生效。**

CSNT 的记帐记录

```
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
```

验证

本部分所提供的信息可用于确认您的配置是否正常工作。

命令输出解释程序工具（仅限注册用户）支持某些 **show 命令，使用此工具可以查看对 show 命令输出的分析。**

- **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>
```

故障排除

下面是您可能遇到的可能错误。

Cisco Secure NT 服务器不可达

VPN 5000 调试

```
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.
```

用户看见什么：

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

身份认证失败

Cisco Secure NT 上的用户名或密码错误。

VPN 5000 调试

```
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.
```

用户看见什么：

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

Cisco Secure：

转到 **Reports 和 Activity**，并且失败的尝试日志显示失败。

用户输入的 VPN 组密码与 VPNPassword 不一致

VPN 5000 调试

```
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
```

用户看见什么：

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

Cisco Secure：

转到 **Reports 和 Activity**，并且失败的尝试日志没有显示失败。

RADIUS 服务器发送的组名在 VPN 5000 中不存在

VPN 5000 调试

```
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)
```

用户看见什么：

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

Cisco Secure：

转到 **Reports 和** *Activity*，并且失败的尝试日志没有显示失败。

相关信息

- Cisco Secure ACS for Windows 支持页
- Cisco VPN 5000 系列集中器终止销售公告
- Cisco VPN 5000 集中器支持页
- Cisco VPN 5000 客户端支持页
- IPSec 支持页面
- RADIUS 支持页
- 请求注解 (RFC)
- 技术支持和文档 - Cisco Systems