CiscoSecure NT 2.5 이상(RADIUS)을 사용하여 VPN 5000 클라이언트를 VPN 5000 Concentrator에 인증하는 방법

목차

소개

Cisco CSNT(Secure NT) 2.5 이상(RADIUS)은 VPN GroupInfo 및 VPN Password에 대한 VPN(Virtual Private Network) 5000 벤더별 특성을 반환하여 VPN 5000 Concentrator에 VPN 5000 클라이언트를 인증할 수 있습니다. 다음 문서에서는 로컬 인증이 RADIUS 인증을 추가하기 전에 작동 중임을 전제로 합니다(따라서 "ciscollocal" 그룹의 "localuser" 사용자). 그런 다음 로컬 데이터베이스에 존재하지 않는 사용자에 대해 CSNT RADIUS에 인증이 추가됩니다(사용자 "csntuser"는 CSNT RADIUS 서버에서 반환된 특성을 통해 그룹 "csntgroup"에 할당됩니다.)

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

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

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참조하십시오.

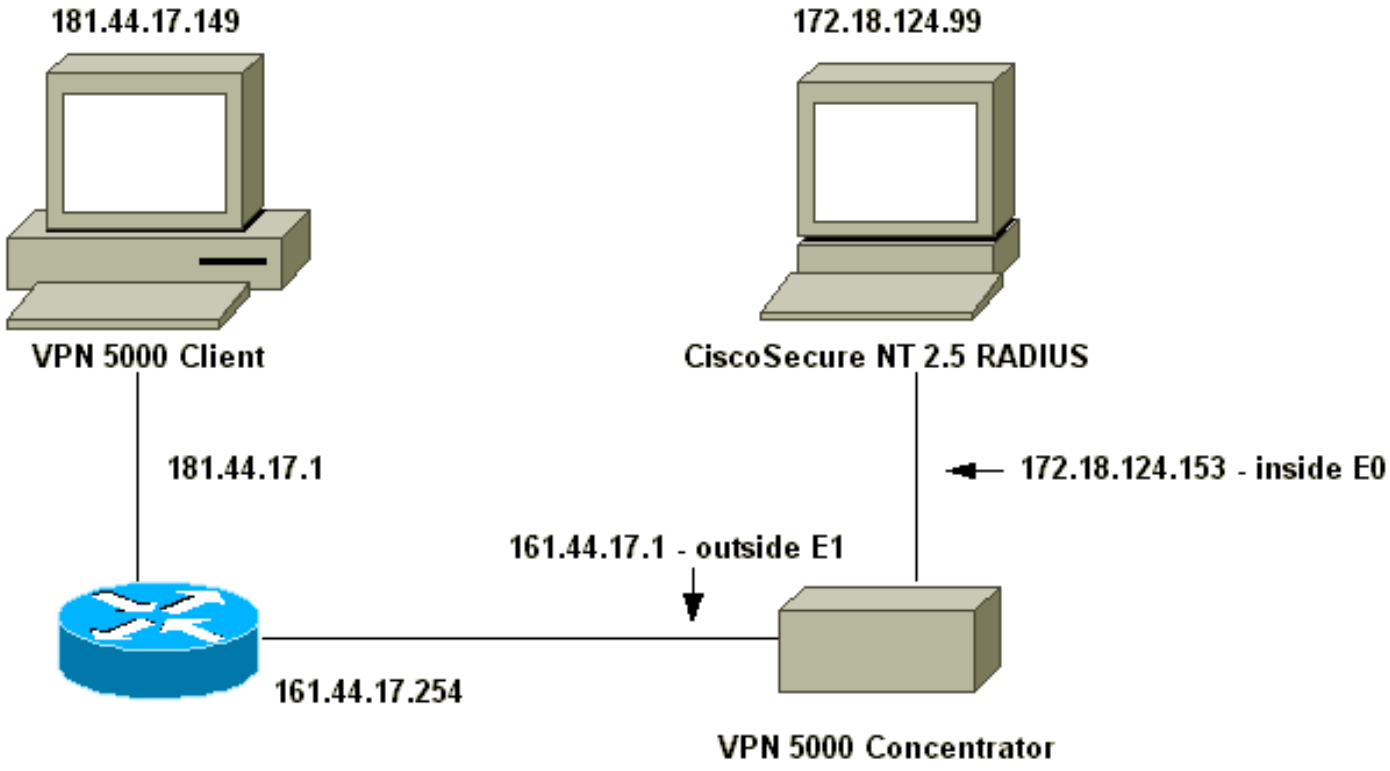
구성

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

참고: 이 문서에 사용된 명령에 대한 추가 정보를 찾으려면 명령 조회 도구(등록된 고객만 해당)를 사용합니다.

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



구성

이 문서에서는 다음 구성을 사용합니다.

- VPN 5000 Concentrator
- VPN 5000 클라이언트

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 클라이언트

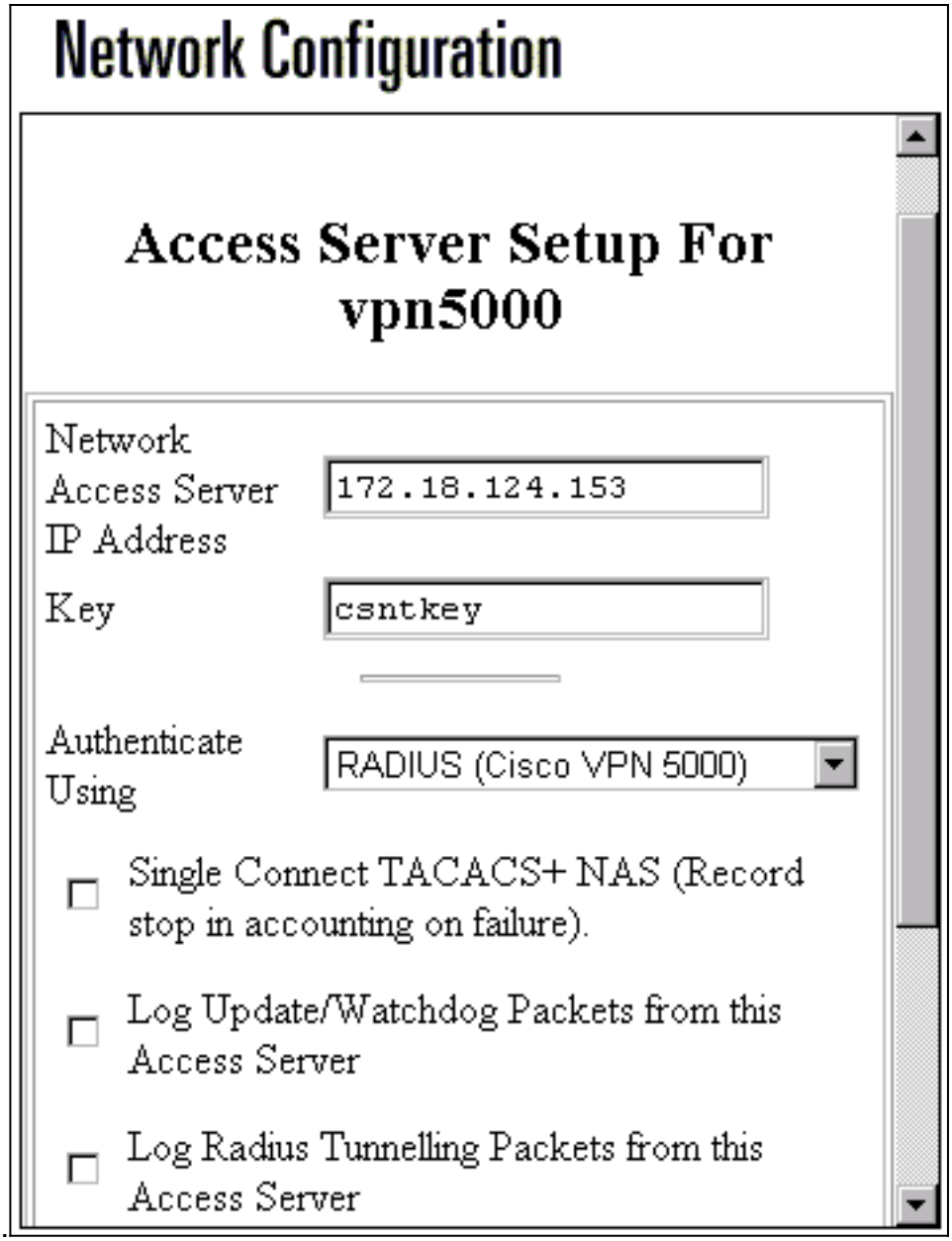
Note: None of the defaults have been changed. Two users were added, and
the appropriate passwords were entered when prompted after clicking Connect:

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

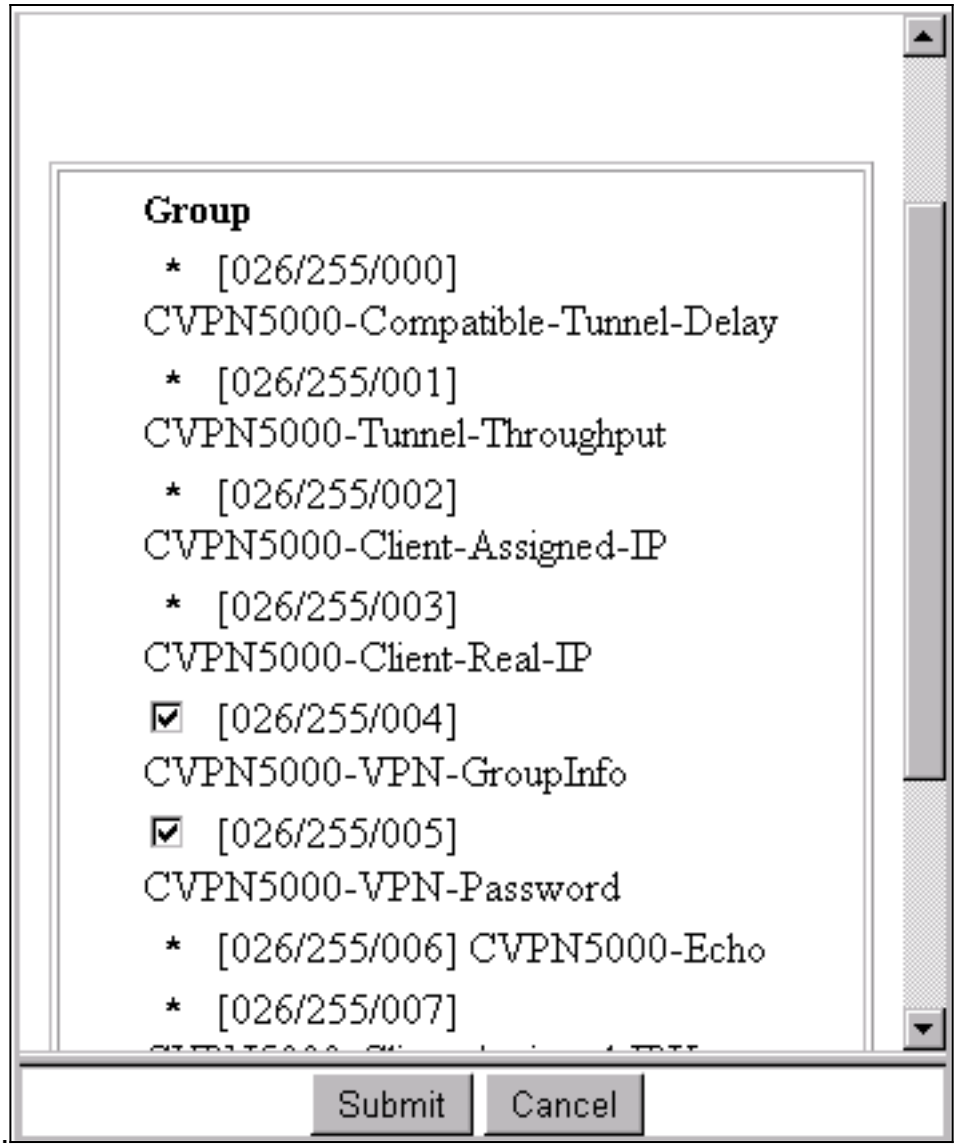
Cisco Secure NT 2.5 구성

다음 절차를 수행합니다.

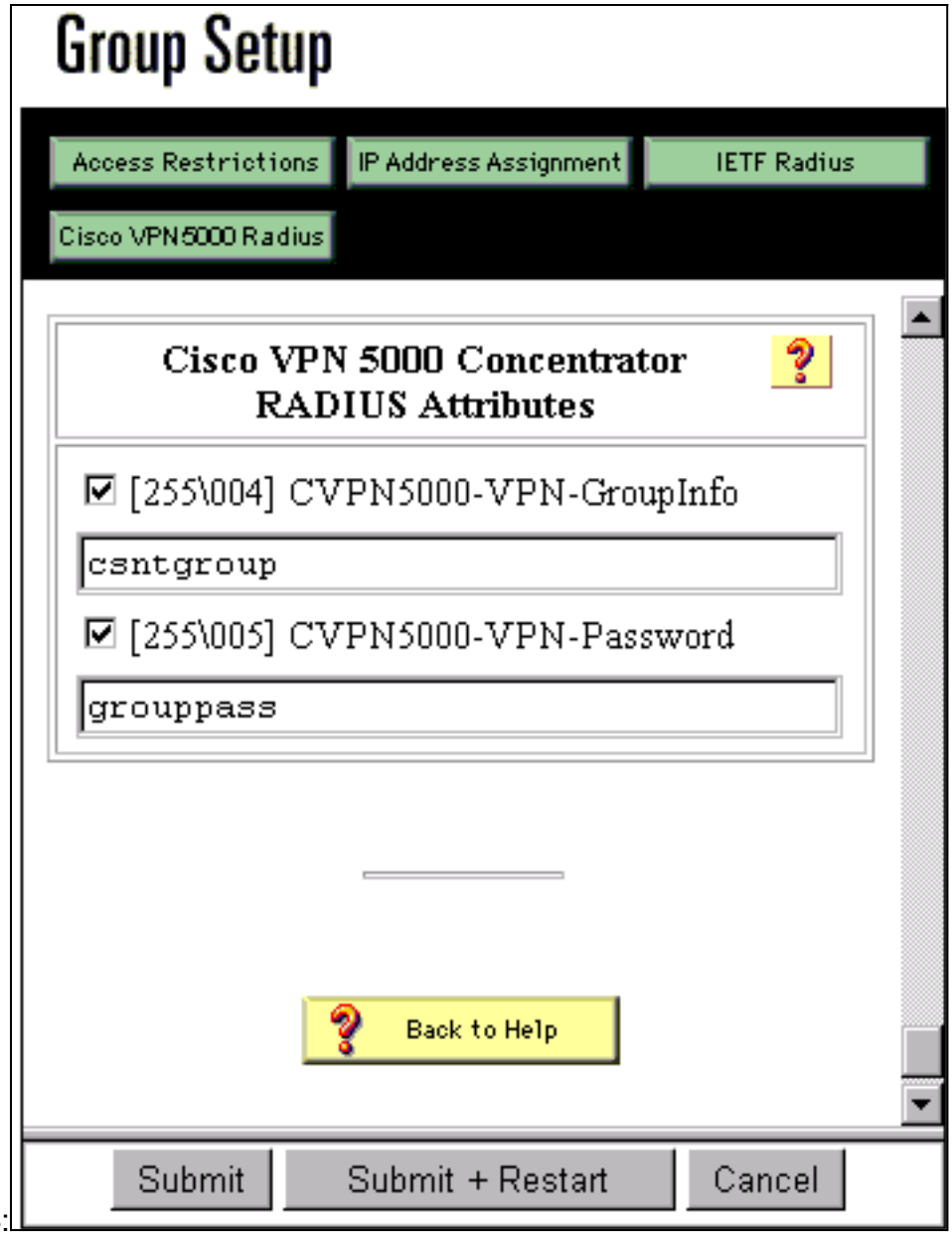
1. Concentrator와 통신하도록 서버를 구성합니다



2. Interface Configuration(**인터페이스 컨피그레이션) > RADIUS(VPN 5000)로 이동하여** VPN GroupInfo 및 VPN Password(VPN 그룹 정보 및 VPN 비밀번호)를 선택합니다



3. 사용자 설정에서 비밀번호("csntpass")로 사용자("csntuser")를 구성하고 사용자를 그룹 13에 배치한 후 **그룹 설정**에서 VPN 5000 특성을 구성합니다. **| 그룹**

13: 

PAP 인증으로 변경

CHAP(Challenge Handshake Authentication Protocol) 인증이 작동한다고 가정할 때 PAP(Password Authentication Protocol)로 변경할 수 있습니다. 그러면 CSNT에서 NT 데이터베이스에서 사용자의 비밀번호를 사용하도록 할 수 있습니다.

VPN 5000 RADIUS 프로파일 변경

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

참고: CSNT는 해당 사용자의 인증에 NT 데이터베이스를 사용하도록 구성됩니다.

사용자에게 표시되는 항목(3개의 암호 상자):

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

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

IP 주소 할당 추가

사용자의 CSNT 프로파일이 "Assign static IP Address(고정 IP 주소 할당)"에서 특정 값으로 설정된 경우, VPN 5000 Concentrator 그룹이 다음에 대해 설정된 경우

```
AssignIPRADIUS = On
```

그런 다음 RADIUS IP 주소가 CSNT에서 전송되고 VPN 5000 Concentrator의 사용자에게 적용됩니다.

계정 추가

세션 어카운팅 레코드를 Cisco Secure RADIUS 서버로 전송하려면 VPN 5000 Concentrator RADIUS 컨피그레이션에 추가합니다.

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

이 변경 사항을 적용하려면 **apply** 및 **write** 명령을 사용한 다음 VPN 5000에서 boot 명령을 사용해야 합니다.

CSNT의 회계 레코드

```
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
```

다음을 확인합니다.

이 섹션에서는 컨피그레이션이 제대로 작동하는지 확인하는 데 사용할 수 있는 정보를 제공합니다.

일부 **show 명령은** 출력 인터프리터 툴 에서 지원되는데(등록된 고객만), 이 툴을 사용하면 **show 명령 출력의 분석 결과를 볼 수 있습니다.**

- **시스템 로그 버퍼 표시**

```
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 추적 덤프 모두**

```
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>
```

문제 해결

다음과 같은 오류가 발생할 수 있습니다.

Cisco Secure NT Server에 연결할 수 없음

VPN 5000 디버그

```
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.
```

사용자에게 표시되는 내용:

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

인증 실패

Cisco Secure NT의 사용자 이름 또는 암호가 잘못되었습니다.

VPN 5000 디버그

```
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.
```

사용자에게 표시되는 내용:

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

Cisco 보안:

Reports and **Activity로** 이동하면 실패 시도 로그에 오류가 표시됩니다.

사용자가 입력한 VPN 그룹 암호가 VPNnpPassword에 동의하지 않음

VPN 5000 디버그

```
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
```

사용자에게 표시되는 내용:

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

Cisco 보안:

Reports and **Activity(보고서** 및 **작업)**로 이동하면 실패한 시도 로그에 오류가 표시되지 않습니다.

RADIUS 서버에서 보낸 그룹 이름이 VPN 5000에 존재하지 않습니다.

VPN 5000 디버그

```
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)
```

사용자에게 표시되는 내용:

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

Cisco 보안:

Reports and **Activity**(**보고서** 및 **작업**)로 이동하면 실패한 시도 로그에 오류가 표시되지 않습니다.

관련 정보

- Cisco Secure ACS for Windows 지원 페이지
- Cisco VPN 5000 Series Concentrator 판매 중단 발표
- Cisco VPN 5000 Concentrator 지원 페이지
- Cisco VPN 5000 클라이언트 지원 페이지
- IPsec 지원 페이지
- RADIUS 지원 페이지
- RFC(Request for Comments)
- 기술 지원 및 문서 – Cisco Systems