Как провести авторизацию VPN 5000 Client для работы с концентратором VPN 5000 с Cisco Secure NT 2.5 и более поздних версий (RADIUS)

Содержание

Введение

Cisco Secure NT (CSNT) 2.5 и позже (RADIUS) способен к возврату Виртуальной частной сети (VPN) 5000 определяемых поставщиком атрибутов для VPN GroupInfo и Пароля VPN для аутентификации VPN 5000 Client на Концентраторе VPN 5000. Следующий документ предполагает, что локальная проверка подлинности работает перед добавляющей Проверкой подлинности RADIUS (следовательно наш пользователь, "localuser", в группе "ciscolocal"). Затем аутентификация добавлена к CSNT RADIUS для пользователей, не существующему в локальной базе данных (пользователь "csntuser" назначают сгруппироваться, "csntgroup" на основании атрибутов возвратился из сервера CSNT RADIUS).

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

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

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Технические рекомендации Cisco. Условные обозначения.

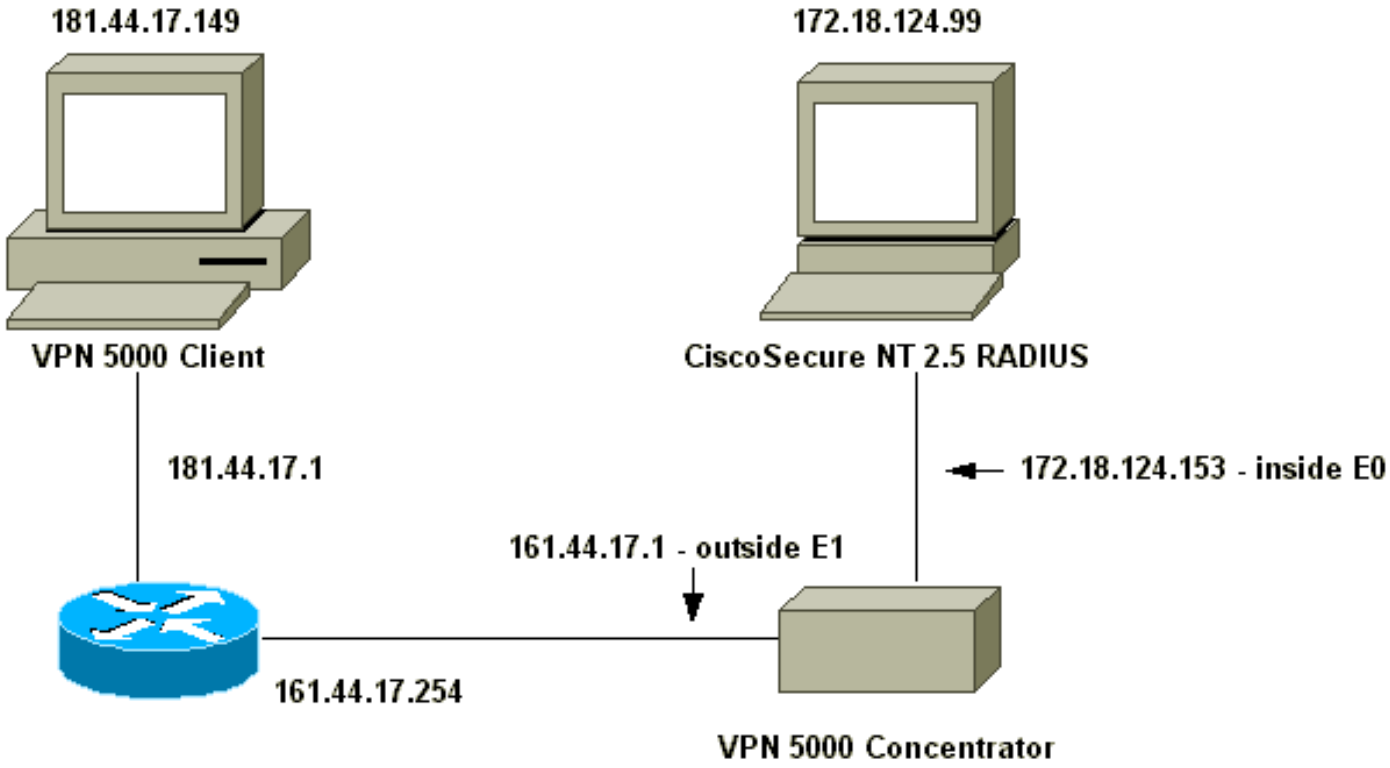
Настройка

В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

Примечание: Поиск дополнительной информации о командах в данном документе можно выполнить с помощью средства "Command Lookup" (Поиск команд) (только для зарегистрированных клиентов).

Схема сети

В настоящем документе используется следующая схема сети:



Конфигурации

Эти конфигурации используются в данном документе:

- Концентратор VPN 5000
- VPN 5000 Client

Концентратор VPN 5000

```
[ 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.
```

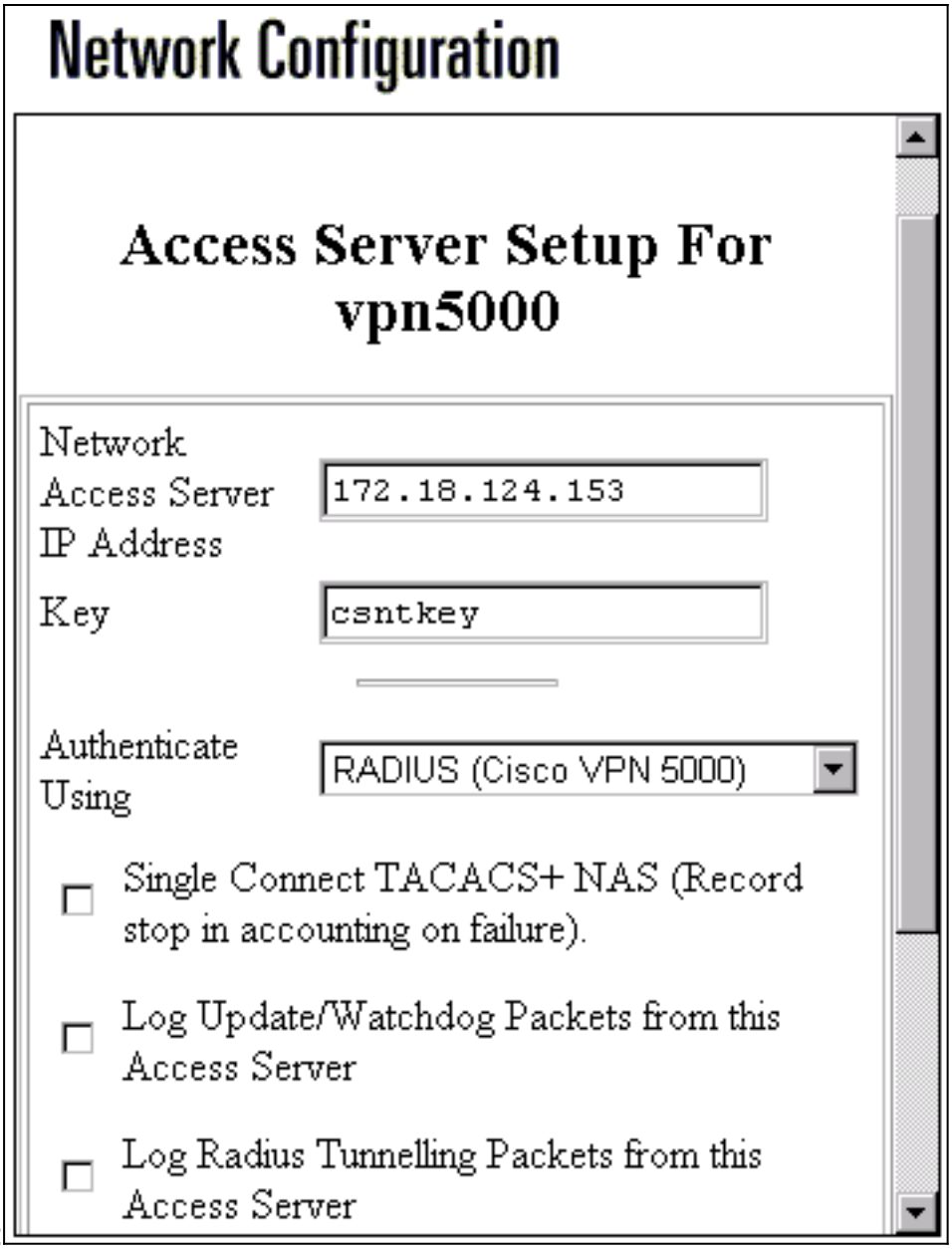
VPN 5000 Client

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

Конфигурация Cisco Secure NT 2.5

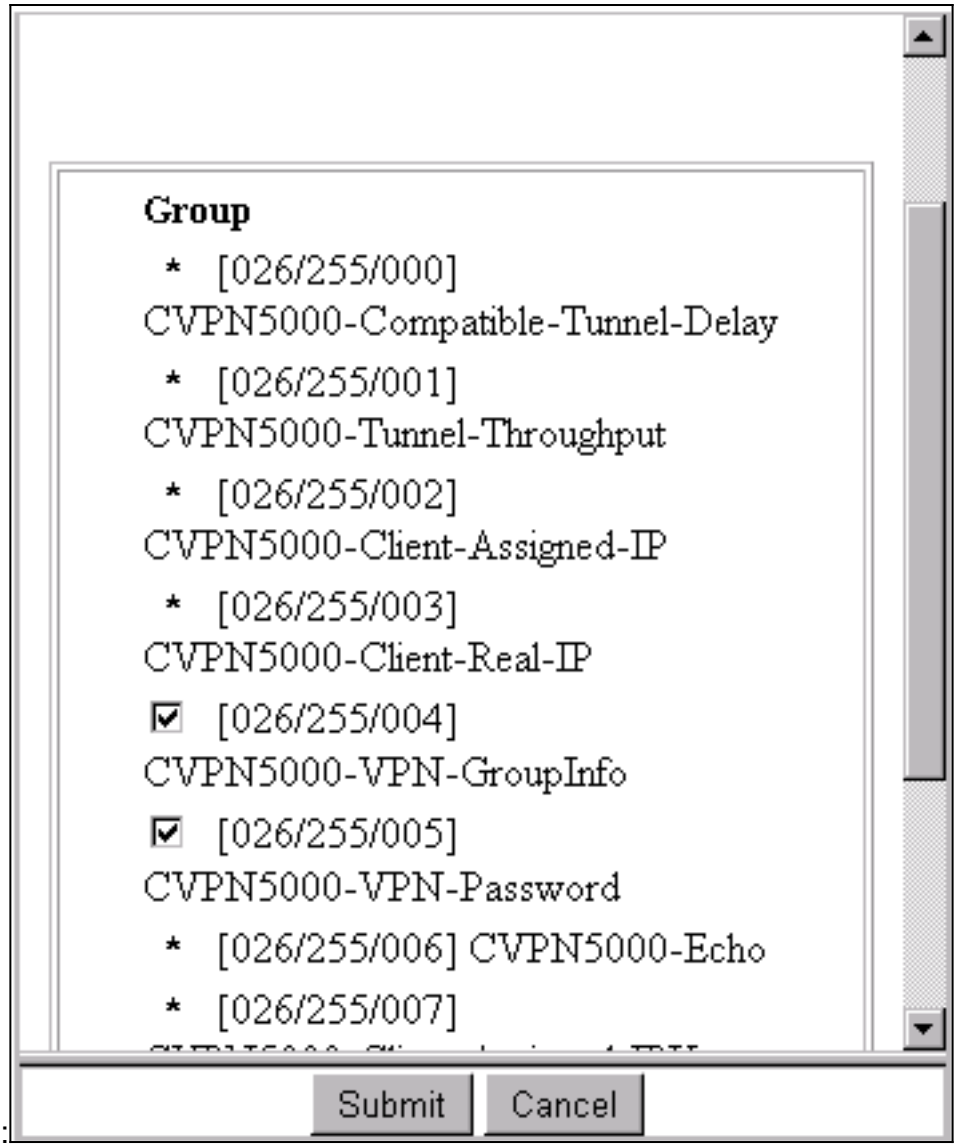
Придерживайтесь следующего порядка действий.

1. Настройте сервер для разговора с



Концентратором:

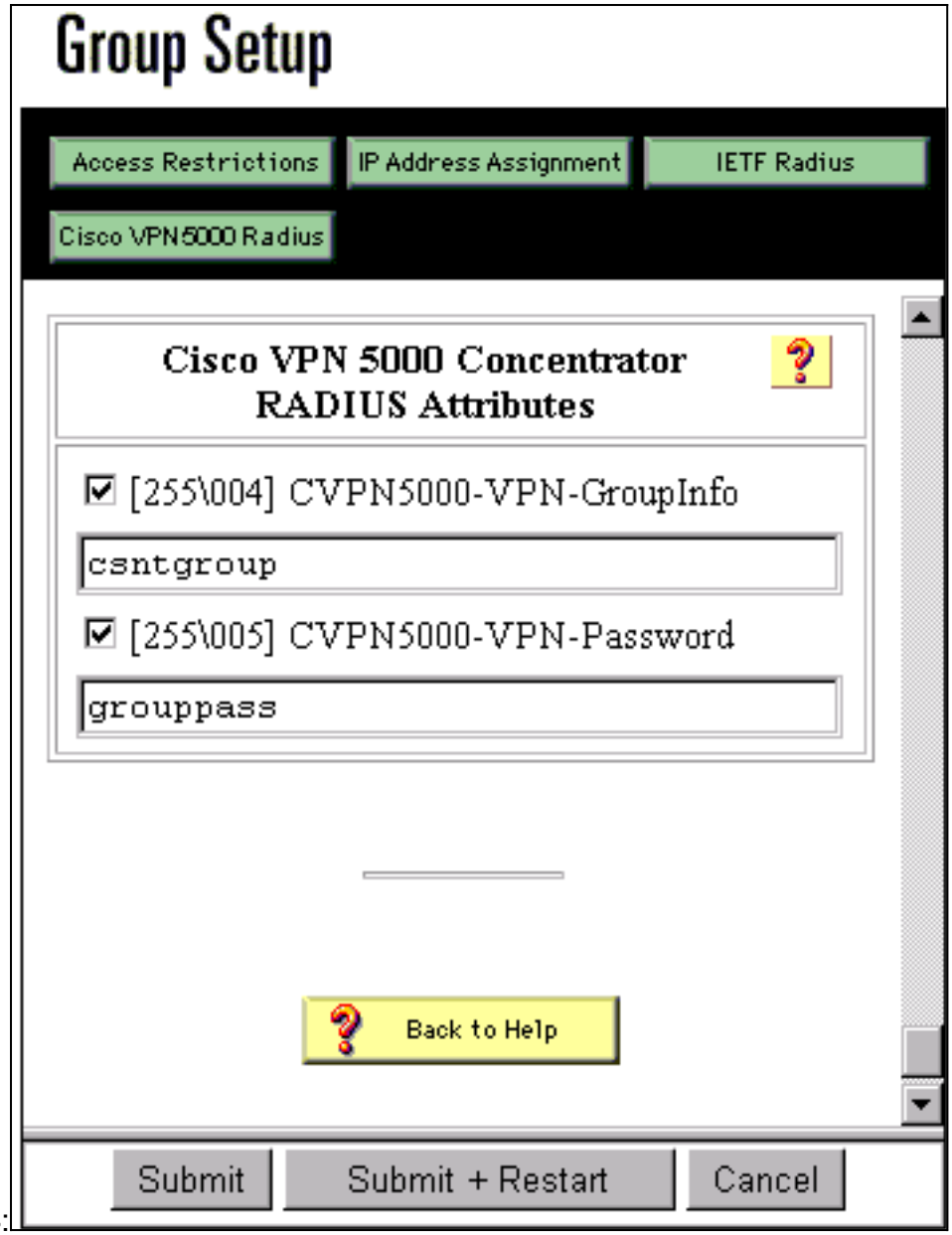
2. Перейдите **к Конфигурации интерфейса> RADIUS (VPN 5000)** и проверьте VPN



GroupInfo и Пароль VPN:

3. После настройки пользователя ("csntuser") с паролем ("csntpass") в Настройке пользователя и помещении пользователя в Группе 13, настройте атрибуты VPN 5000 в **Настройке групп | Группа**

13:



Переход на проверку подлинности PAP

Принятие аутентификации Протокола аутентификации по квитированию вызова (CHAP) работает, можно хотеть измениться на Протокол аутентификации пароля (PAP), который позволяет вам иметь использование CSNT пароль пользователя от базы данных NT.

Изменение профиля VPN 5000 RADIUS

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

Примечание: CSNT был бы также настроен для использования базы данных NT для аутентификации того пользователя.

Что пользователь видит (три поля пароля):

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

Добавление назначений IP-адресов

Если профиль CSNT пользователя установлен в, "Назначают статический IP - адрес" на определенное значение, и если группа Концентратора VPN 5000 установлена для:

```
AssignIPRADIUS = On
```

Затем IP-адрес RADIUS передан вниз от CSNT и применен к пользователь на Концентраторе VPN 5000.

Добавление автоматического учета

Если вы хотите учетные записи сеанса, передаваемые серверу RADIUS Cisco Secure, то добавьте к Конфигурации RADIUS Концентратора VPN 5000:

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

Необходимо использовать **применение** и **команды write**, и затем **команду загрузки** на VPN 5000 для этого изменения для вступления в силу.

Учетные записи от 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
```

Проверка

В этом разделе содержатся сведения, которые помогают убедиться в надлежащей работе конфигурации.

Некоторые команды show поддерживаются Средством интерпретации выходных данных(только зарегистрированные клиенты), которое позволяет просматривать аналитику выходных данных команды 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
```
- **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>
```

Устранение неполадок

Ниже приводятся возможные ошибки, с которыми можно встретиться.

Сервер Cisco Secure NT недоступен

Отладка 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.
```

Что видно пользователю:

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

Сбой при проверке подлинности

Имя пользователя или пароль на Cisco Secure NT плохо.

Отладка 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.
```

Что видно пользователю:

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

Cisco Secure:

Перейдите **к Отчётам** и **Действию**, и журнал неудачных попыток показывает сбой.

Пароль группы VPN, введенный пользователем, не совпадает с паролем VPNPassword

Отладка 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
```

Что видно пользователю:

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

Cisco Secure:

Перейдите **к Отчётам** и **Действию**, и журнал неудачных попыток не показывает сбой.

Имя группы, отсылаемое сервером RADIUS, не существует в сети VPN 5000

Отладка 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)
```

Что видно пользователю:

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

Cisco Secure:

Перейдите **к Отчётам** и **Действию**, и журнал неудачных попыток *не* показывает сбой.

Дополнительные сведения

- Страница поддержки Cisco Secure ACS для Windows
- Объявление об окончании продажи концентраторов Cisco серии VPN 5000
- Страница поддержки концентратора Cisco VPN 5000
- Страница поддержки Cisco VPN 5000 Client
- Страница поддержки IPSec
- Страница поддержки RADIUS
- Запросы комментариев (RFC)
- Cisco Systems – техническая поддержка и документация