Настройка PPTP концентратора VPN 3000 с Cisco Secure ACS lkz аутентификации Windows RADIUS

Содержание

Введение

Cisco VPN 3000 Concentrator поддерживает метод туннелирования PPTP для Windows-клиентов. Поддержки концентратора 40-разрядное и 128-разрядное шифрование для защищенного надежного соединения. Этот документ описывает, как настроить PPTP на VPN 3000 Concentrator с Cisco Secure ACS для Windows для Проверки подлинности RADIUS.

См. Настройку межсетевой экран Cisco Secure PIX для Использования PPTP для настройки подключений PPTP к PIX.

См. Cisco Secure ACS Настройки для Аутентификации PPTP маршрутизатора Windows для устанавливания Подключения ПК к маршрутизатору; это предоставляет проверку подлинности пользователя системе управления доступом Cisco Secure Access Control System (ACS) 3.2 для Windows Server, прежде чем вы позволите пользователю в сеть.

Перед началом работы

Условные обозначения

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

Предварительные условия

Этот документ предполагает, что локальная аутентификация PPTP работает перед добавляющим Cisco Secure ACS для аутентификации Windows RADIUS. Посмотрите, Как Настроить PPTP концентратора VPN 3000 с Локальной проверкой подлинности для получения дополнительной информации о локальной аутентификации PPTP. Для полного списка требований и ограничений, см. то, Когда Шифрование PPTP Поддерживается на Cisco VPN 3000 Concentrator?

Используемые компоненты

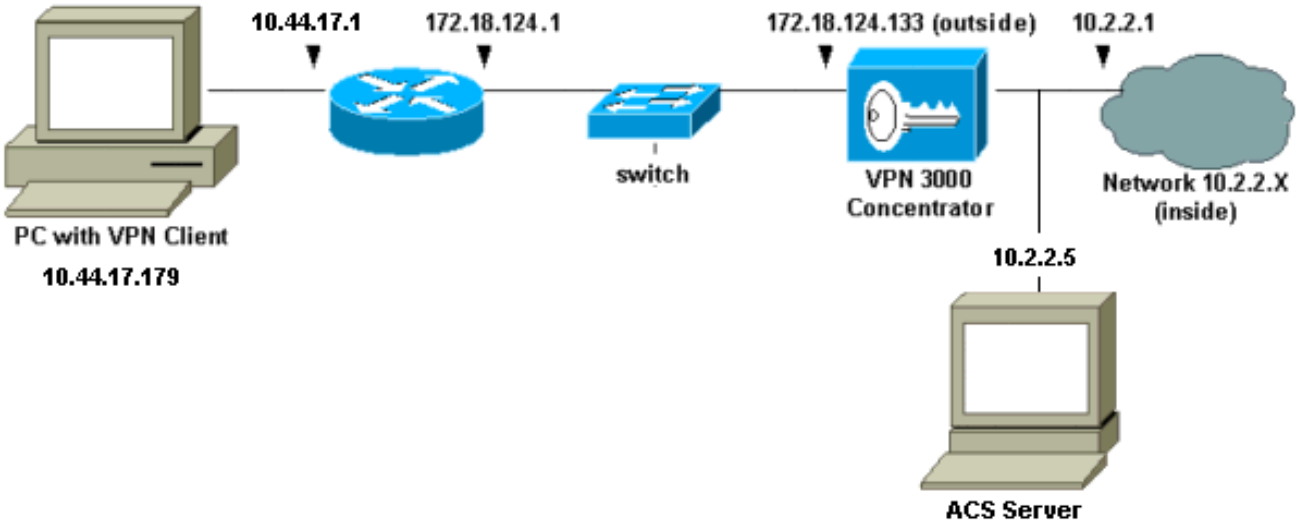
Сведения в этом документе основаны на версиях оборудования и программного обеспечения, указанных ниже.

- Cisco Secure ACS для Версий Windows 2.5 и позже
- Версии 2.5.2. С VPN 3000 Concentrator и позже (Эта конфигурация была проверена с версией 4.0. x.)

Сведения, содержащиеся в данном документе, были получены с устройств в специальной лабораторной среде. Все устройства, описанные в данном документе, были запущены с конфигурацией по умолчанию. При работе с реальной сетью необходимо полностью осознавать возможные результаты использования всех команд.

Схема сети

В данном документе используется сетевая установка, показанная на следующей схеме.

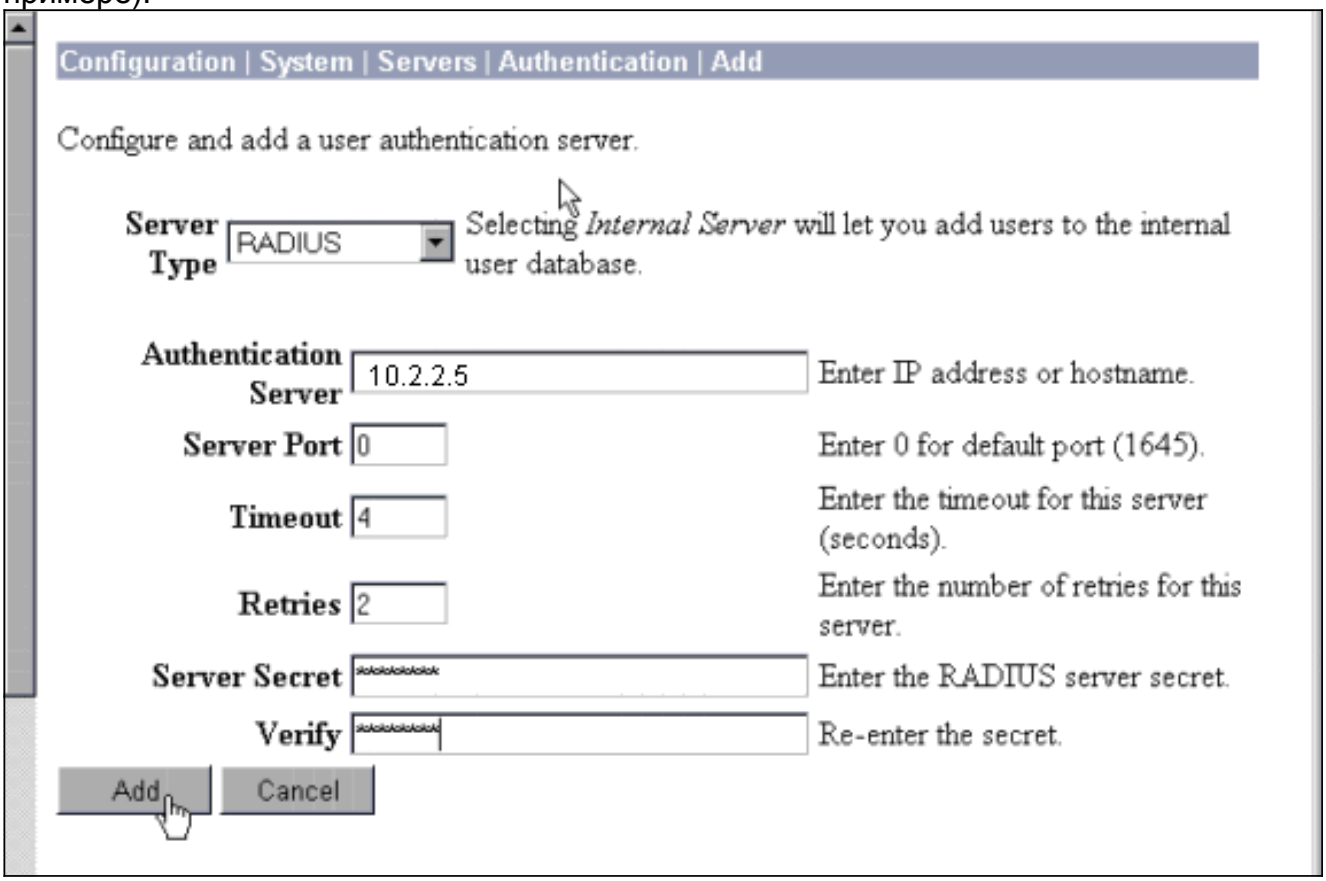


Настройка концентратора VPN 3000

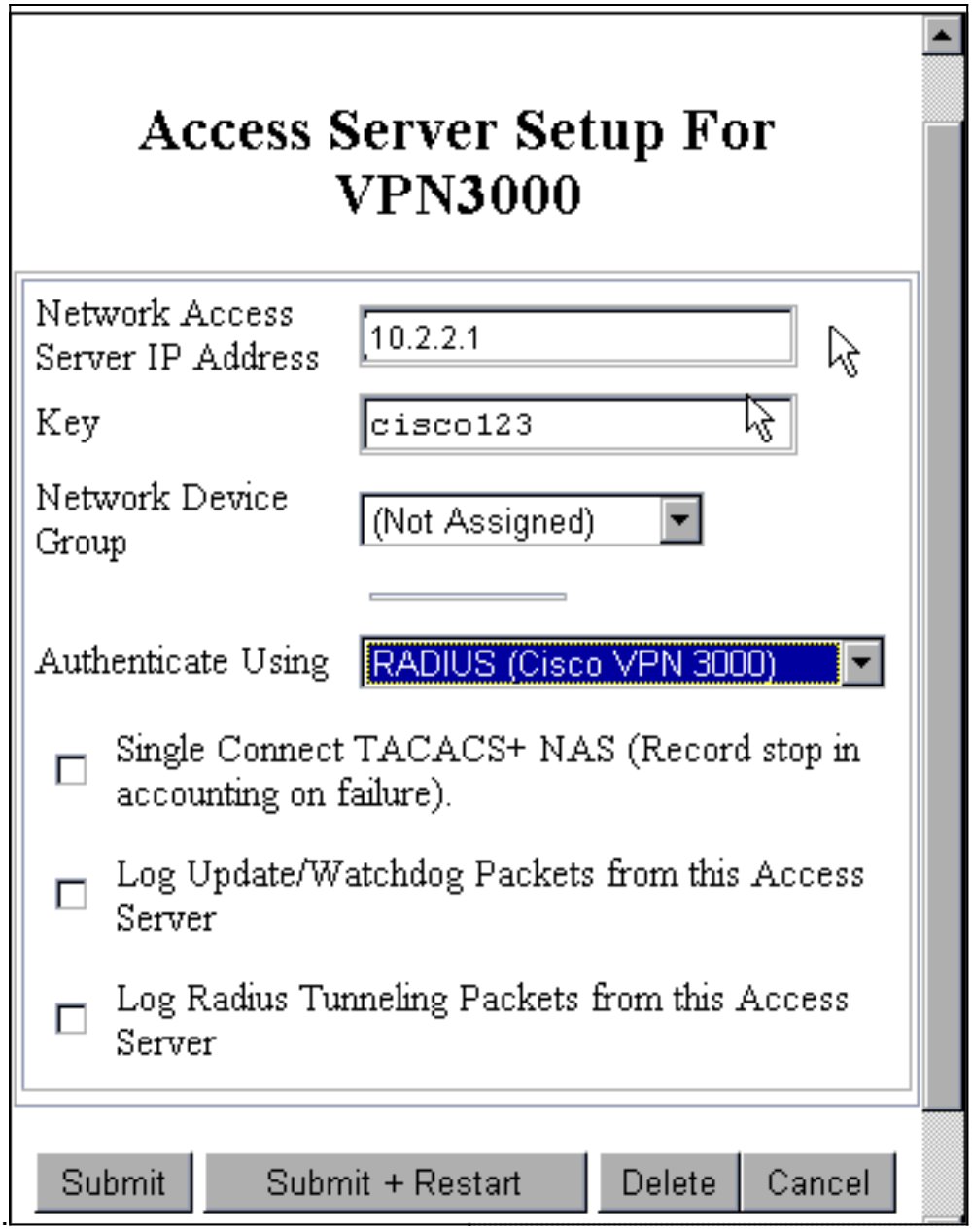
Добавление и Cisco Secure ACS Настройки для Windows

Выполните эти действия для настройки Концентратора VPN для использования Cisco Secure ACS для Windows.

1. На VPN 3000 Concentrator перейдите **к Configuration> System> Servers> Authentication Servers** и добавьте Cisco Secure ACS для Windows Server и ключа ("cisco123" в данном примере).

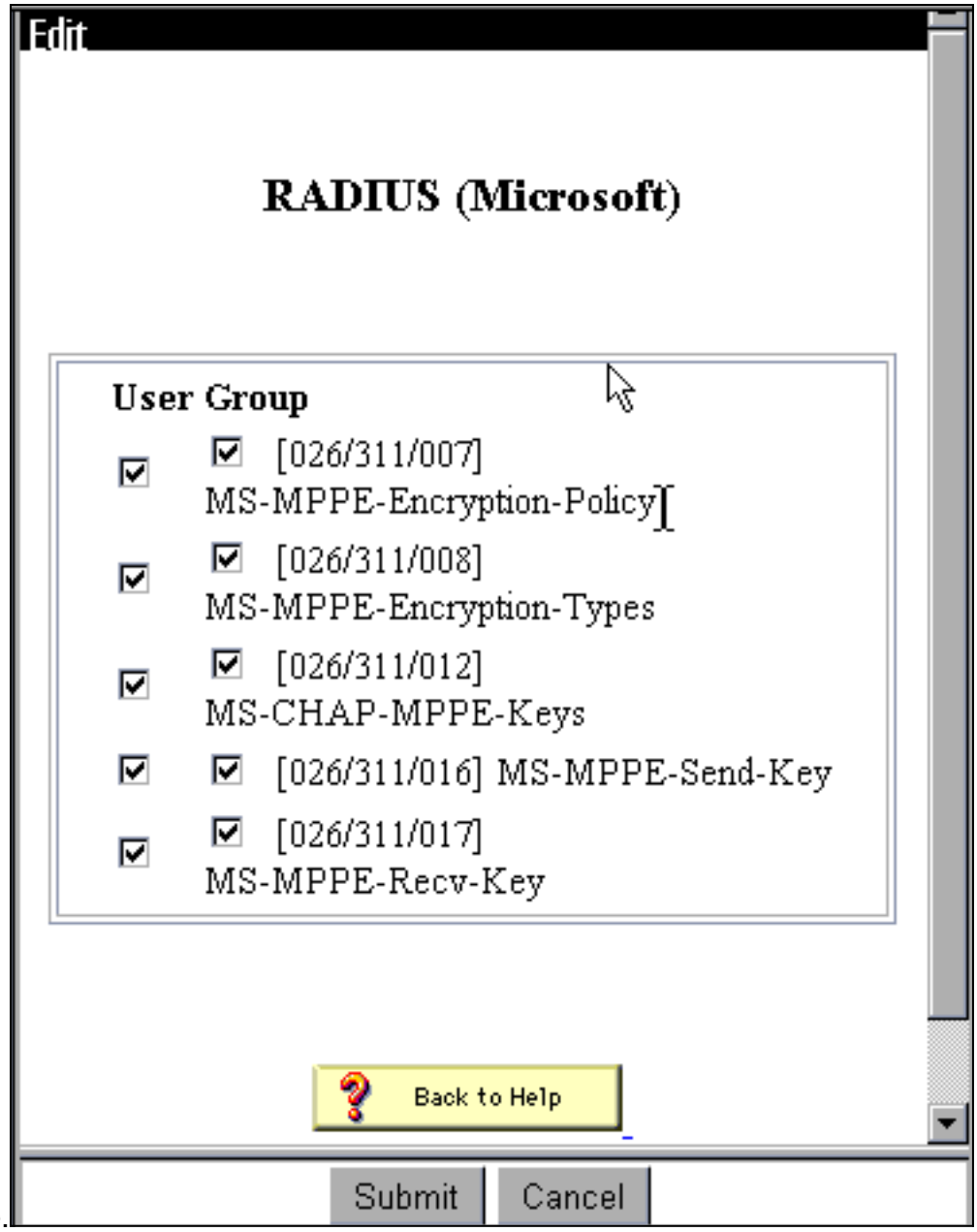


2. В Cisco Secure ACS для Windows добавьте Концентратор VPN к Конфигурации сети сервера ACS и определите тип



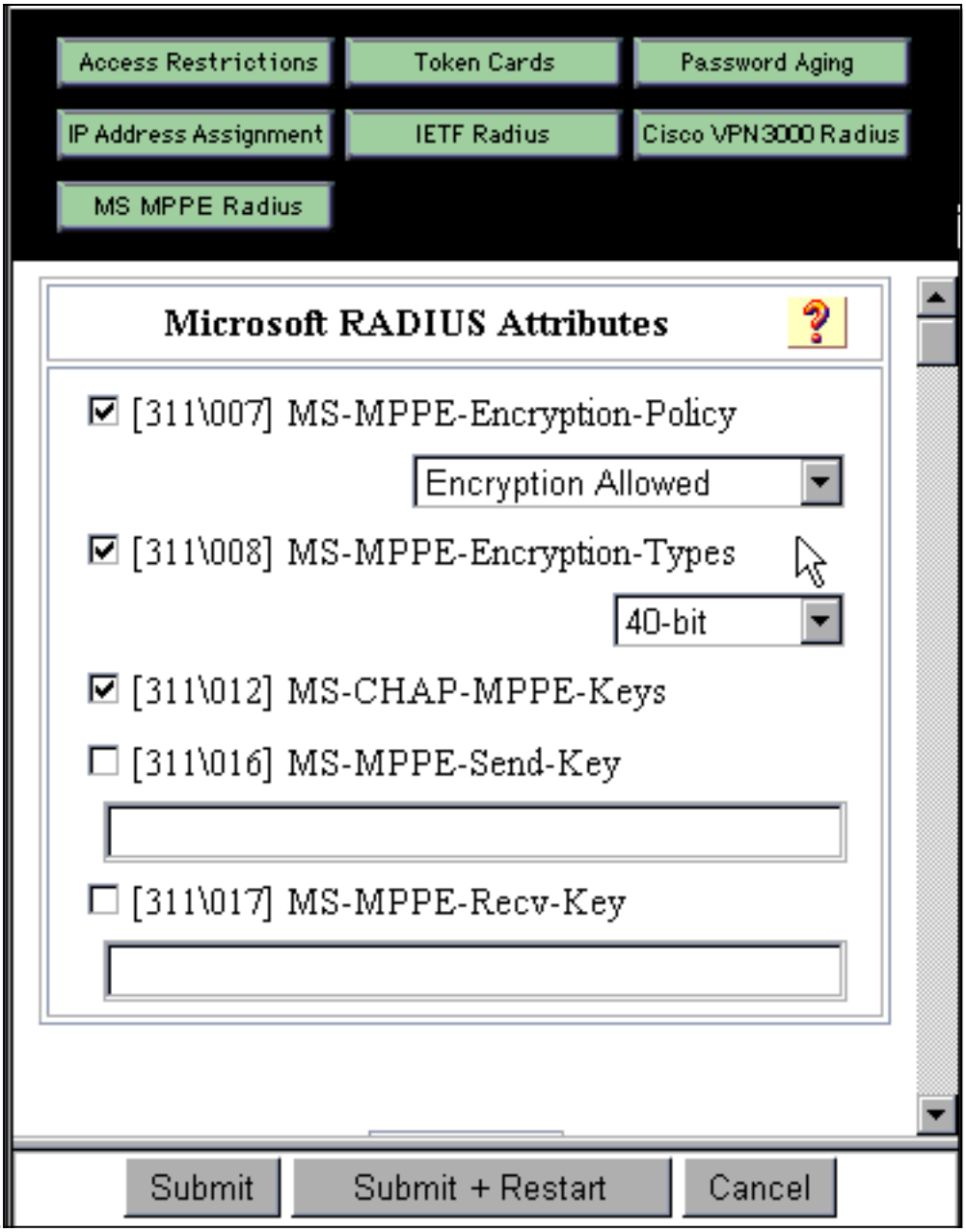
словаря.

3. В Cisco Secure ACS для Windows перейдите **к Interface Configuration> Radius (Microsoft)** и проверьте атрибуты Средств шифрования Microsoft точка-точка (MPPE) так, чтобы атрибуты появились в групповом



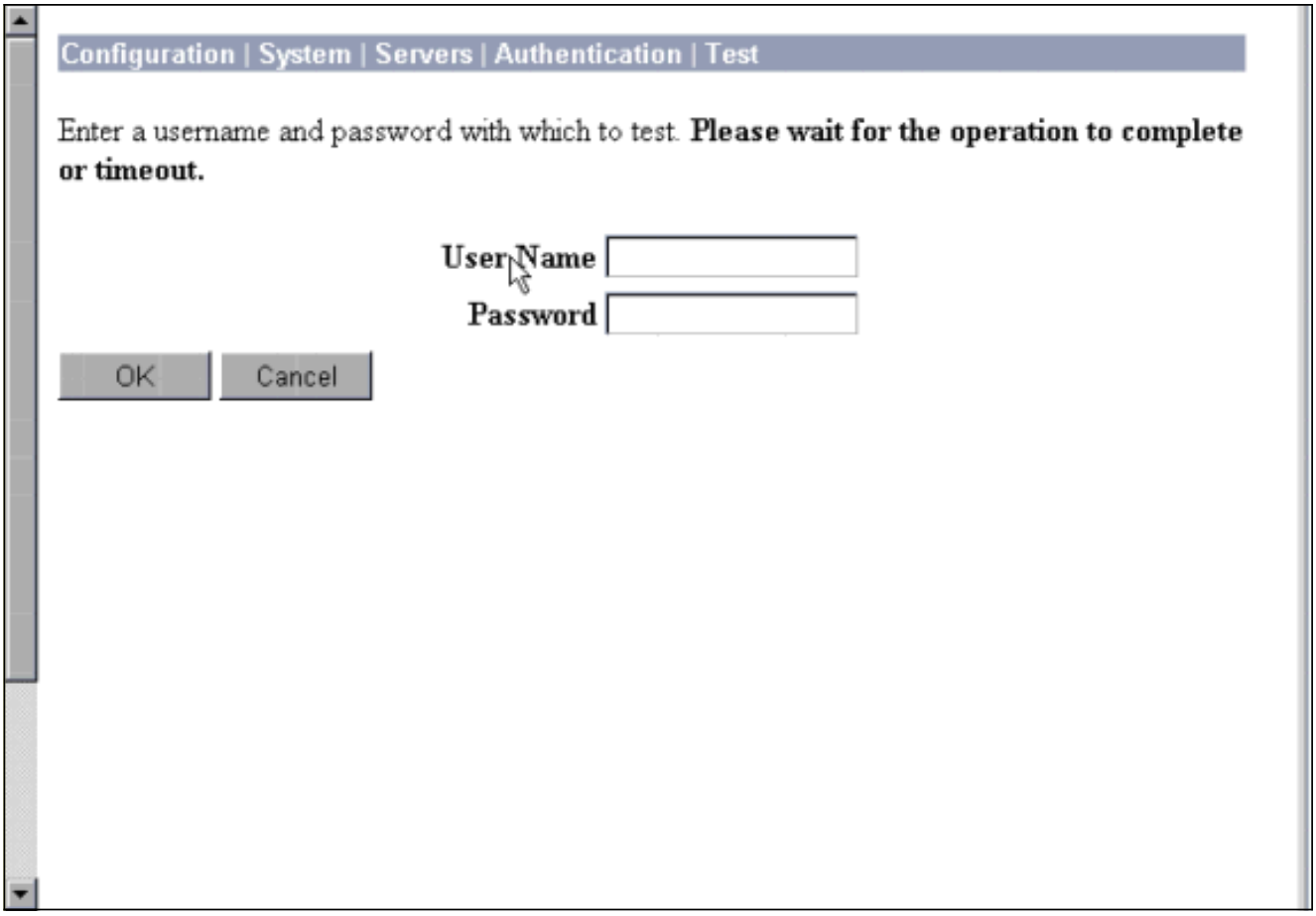
интерфейсе.

4. В Cisco Secure ACS для Windows добавьте пользователя. В группе пользователя добавьте MPPE (Microsoft RADIUS) атрибуты, в случае, если вы требуете шифрования в более позднее

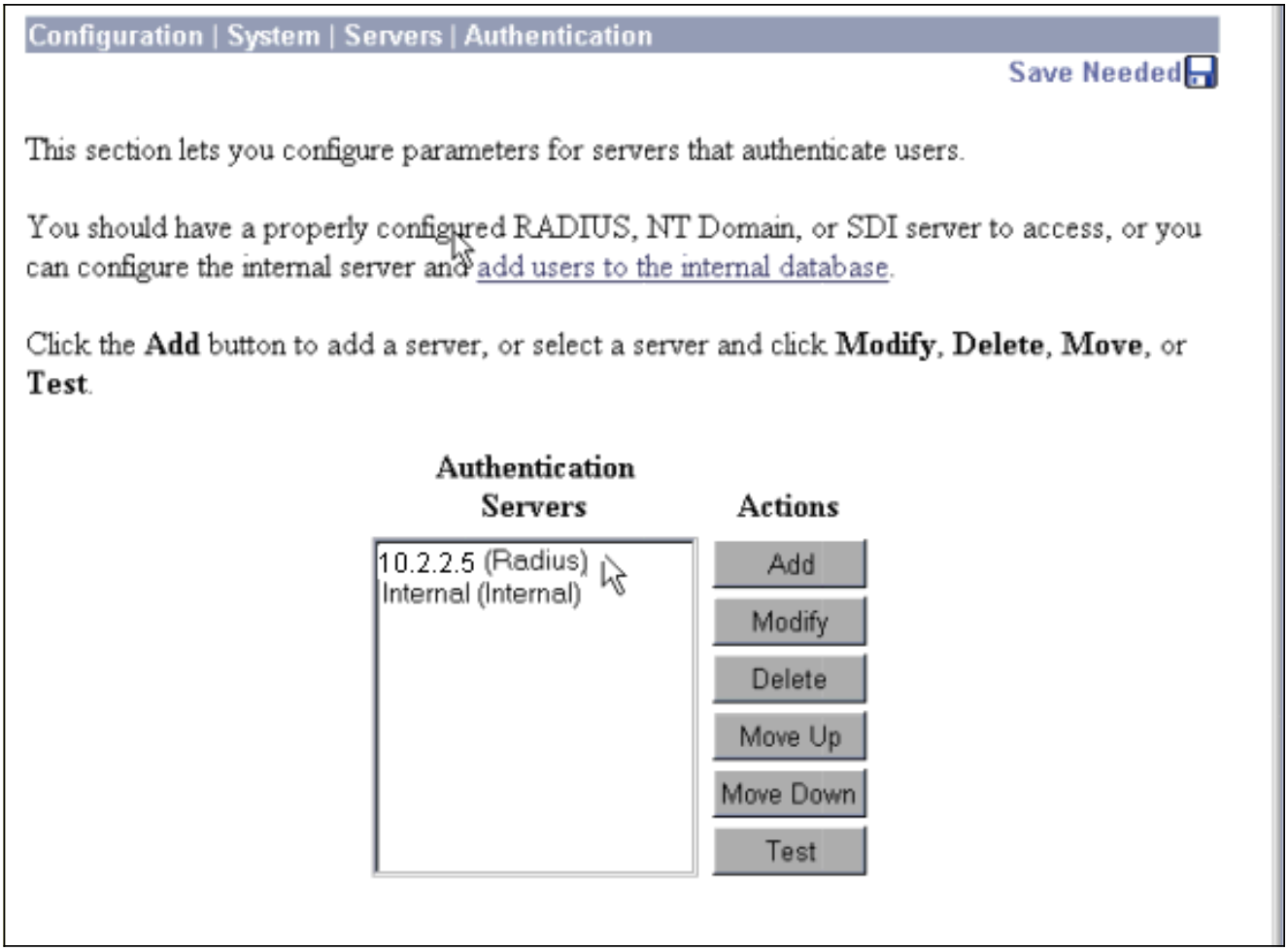


время.

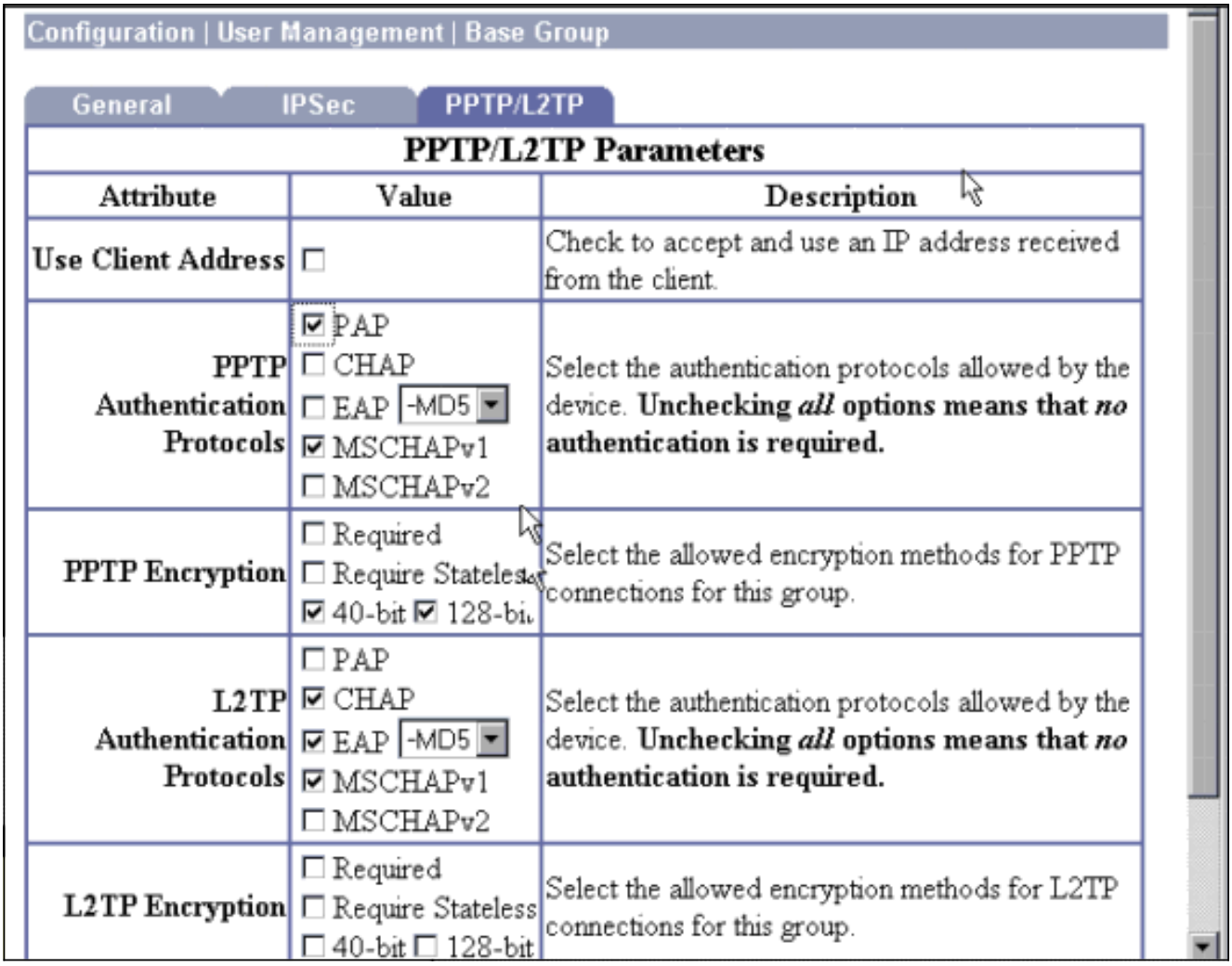
5. На VPN 3000 Concentrator перейдите **к Configuration> System> Servers> Authentication Servers**. Выберите сервер проверки подлинности из списка, и затем выберите **Test**. Тестовая аутентификация от Концентратора VPN до Cisco Secure ACS для Windows Server путем ввода имени пользователя и пароля.На успешной проверке подлинности Концентратор VPN должен показать Сообщение "authentication successful". Сбои в Cisco Secure ACS для Windows зарегистрированы в **Отчётах и Действии> Неудачные попытки**. В установке по умолчанию эти отчёты сохранены на диске в C:\Program Files\CiscoSecure ACS v2.5\Logs\Failed
Attempts.



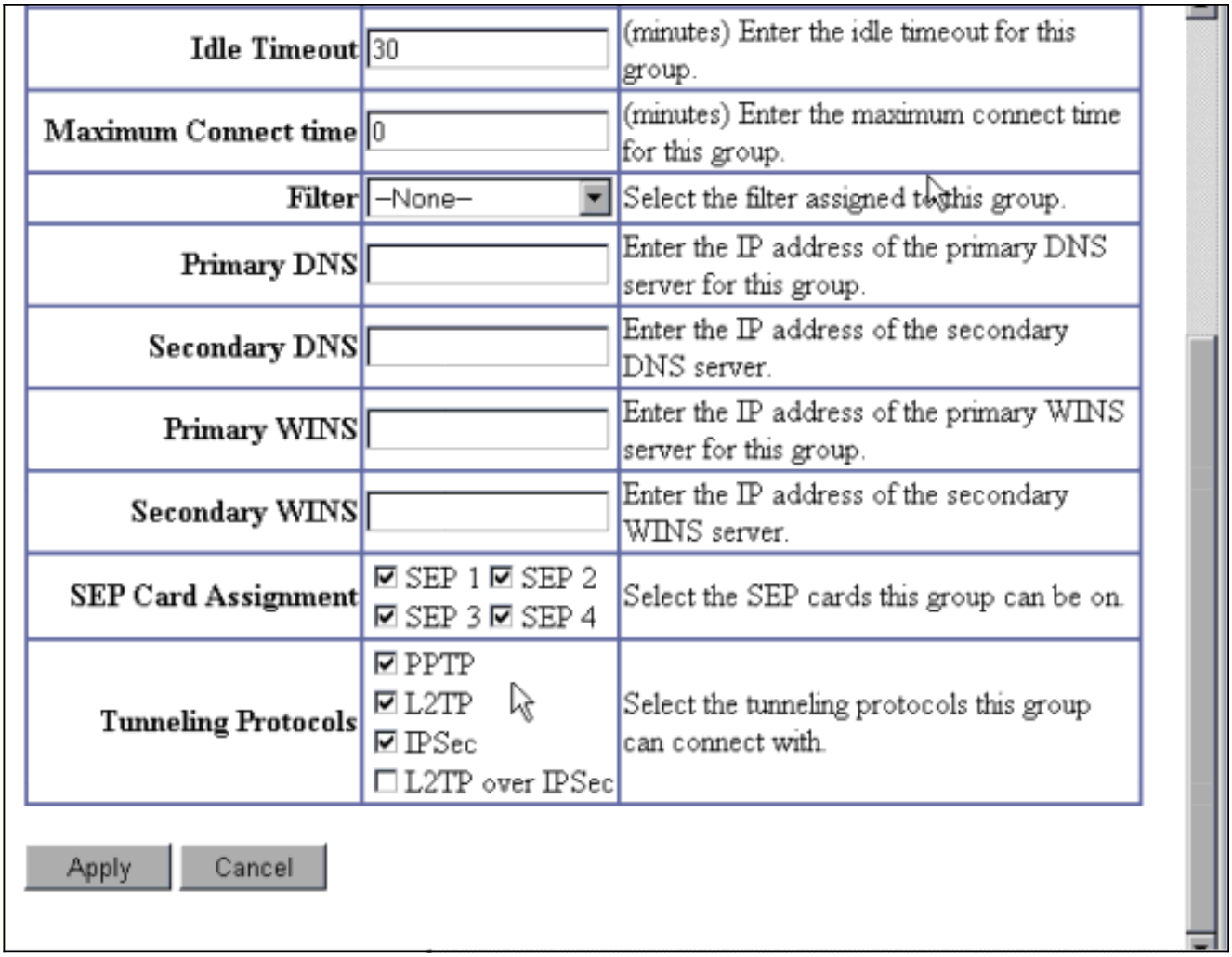
6. Так как вы теперь проверили, что аутентификация от ПК до Концентратора VPN работает и от концентратора до Cisco Secure ACS для Windows Server, можно реконфигурировать Концентратор VPN, чтобы передать пользователям PPTP к Cisco Secure ACS для Windows RADIUS путем перемещения Cisco Secure ACS для Windows Server к вершине списка серверов. Чтобы сделать это на Концентраторе VPN, перейдите **к Configuration> System> Servers> Authentication Servers**.



7. Перейдите к **Configuration> User Management> Base Group** и выберите вкладку **PPTP/L2TP**. В базовой группе Концентратора VPN гарантируйте, что включены опции для PAP и
MSCHAPv1.



8. Выберите **Вкладку Общие** и гарантируйте, что PPTP разрешен в разделе Протоколов туннелирования.

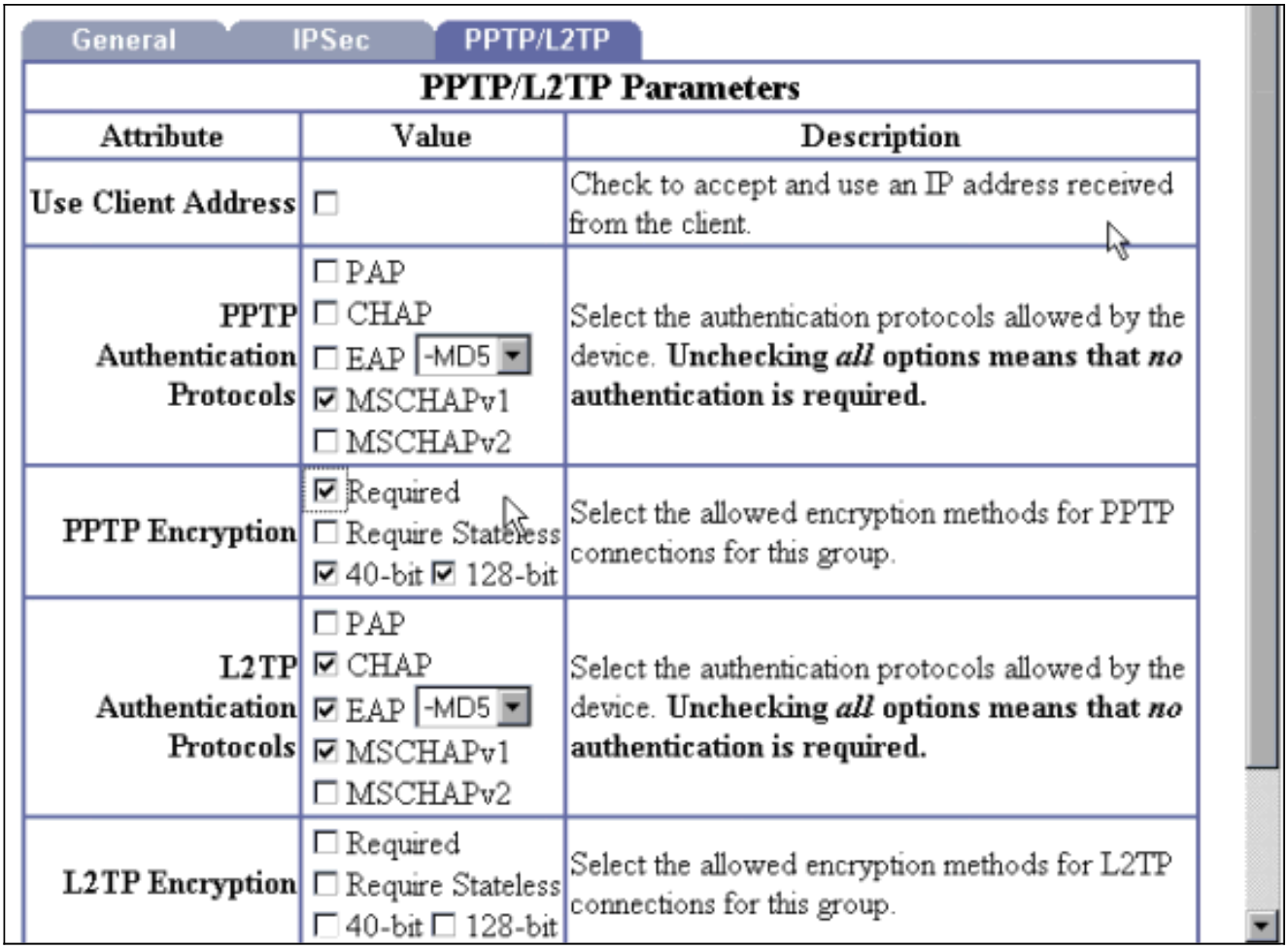


9. Тестовая аутентификация PPTP с пользователем в Cisco Secure ACS для Сервера Windows Radius. Если это не работает, посмотрите Раздел отладки.

Добавление протокола MPPE (шифрование)

Если Cisco Secure ACS для аутентификации PPTP Windows RADIUS работает без шифрования, можно добавить MPPE к VPN 3000 Concentrator.

1. На Концентраторе VPN перейдите **к Configuration> User Management> Base Group**.
2. Под разделом для Шифрования PPTP проверьте опции для **Требуемого**, **40-разрядного**, и **128-разрядный**. С тех пор не все PC поддерживают и 40-разрядное и 128-разрядное шифрование, проверяют обе опции для учета согласования.
3. Под разделом для Протоколов Аутентификации PPTP проверьте опцию для **MSCHAPv1**. (Вы уже настроили Cisco Secure ACS для атрибутов пользователя Windows 2.5 для шифрования в более раннем
шаге.)



Примечание: Клиент PPTP должен быть распознан за оптимальный или обязательное шифрование данных и MSCHAPv1 (если опция).

Добавление автоматического учета

После установления аутентификации можно добавить учет к Концентратору VPN. Перейдите к **Configuration> System> Servers> Accounting Servers** и добавьте Cisco Secure ACS для Windows Server.

В Cisco Secure ACS для Windows учетные записи появляются следующим образом.

```
Date,Time,User-Name,Group-Name,Calling-Station-Id,Acct-Status-Type,Acct-Session-Id,
   Acct-Session-Time,Service-Type,Framed-Protocol,Acct-Input-Octets,Acct-Output-Octets,
   Acct-Input-Packets,Acct-Output-Packets,Framed-IP-Address,NAS-Port,NAS-IP-Address
03/18/2000,08:16:20,CSNTUSER,Default Group,,Start,8BD00003,,Framed,
   PPP,,,,,1.2.3.4,1163,10.2.2.1
03/18/2000,08:16:50,CSNTUSER,Default Group,,Stop,8BD00003,30,Framed,
   PPP,3204,24,23,1,1.2.3.4,1163,10.2.2.1
```

Проверка

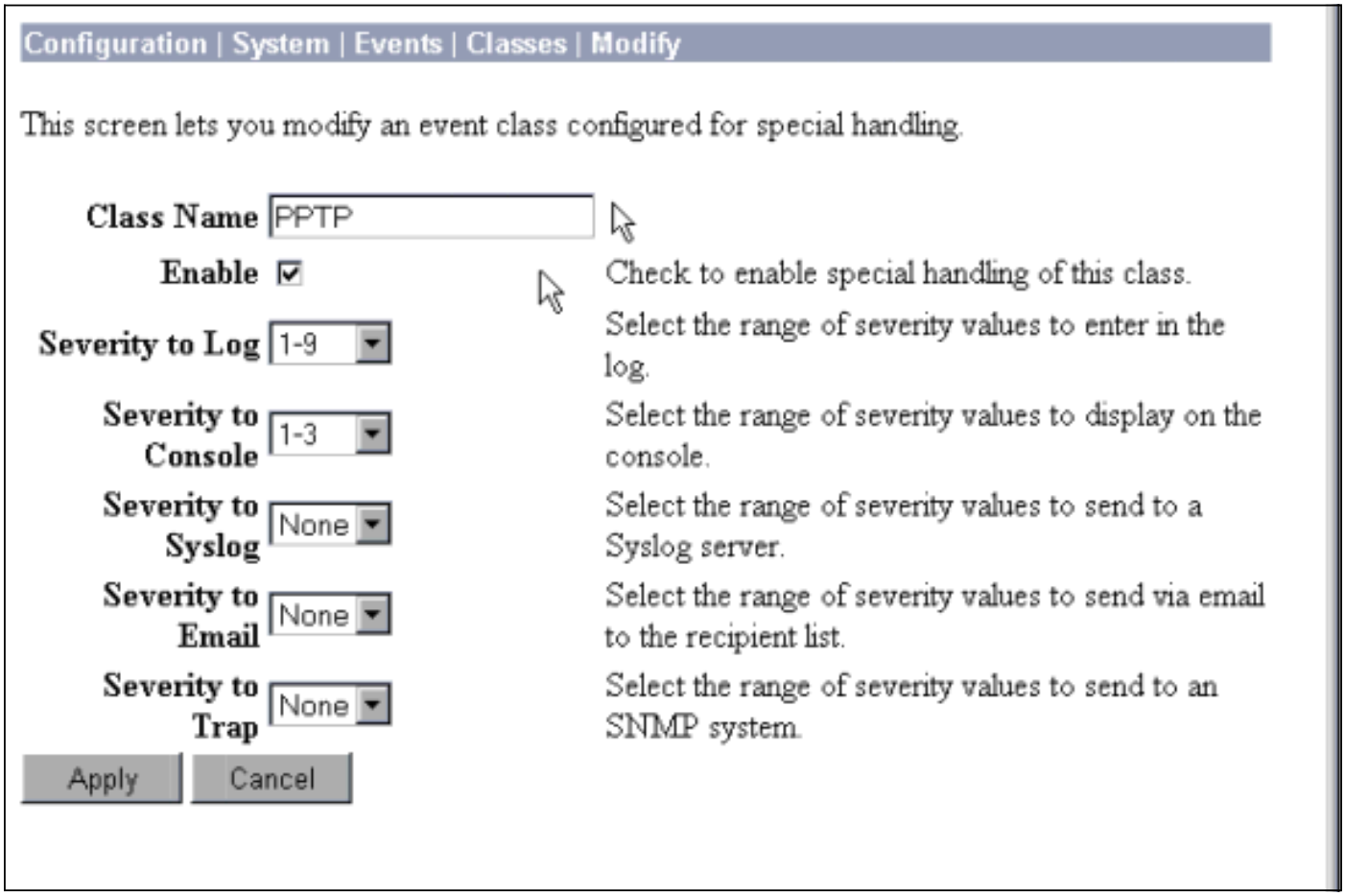
В настоящее время для этой конфигурации нет процедуры проверки.

Устранение неполадок

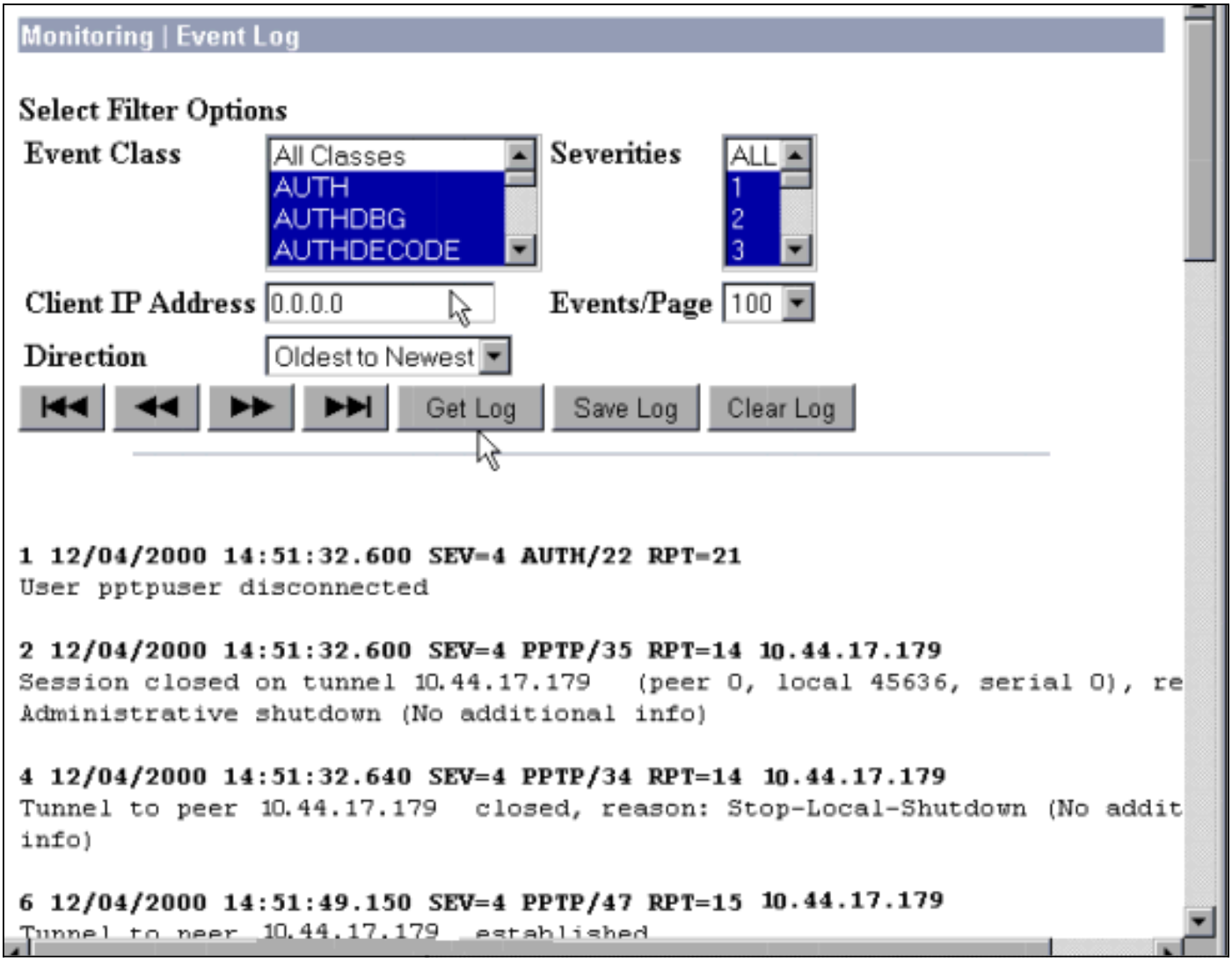
В этом разделе описывается процесс устранения неполадок конфигурации.

Включание отладку

Если соединения не работают, можно добавить PPTP, и Параметры Auth Event Class к Концентратору VPN тем, чтобы переходить **Configuration> System> Events> Classes> Modify**. Можно также добавить PPTPDBG, PPTPDECODE, AUTHDBG и Классы события authdecode, но эти опции могут предоставить слишком много информации.



Можно получить журнал событий, перейдя к **Monitoring> Event Log**.



Отладки - успешная проверка подлинности

Хорошие отладки на Концентраторе VPN будут выглядеть подобными следующему.

```
1 12/06/2000 09:26:16.390 SEV=4 PPTP/47 RPT=20 10.44.17.179
Tunnel to peer 161.44.17.179 established
2 12/06/2000 09:26:16.390 SEV=4 PPTP/42 RPT=20 10.44.17.179
Session started on tunnel 161.44.17.179
3 12/06/2000 09:26:19.400 SEV=7 AUTH/12 RPT=22
Authentication session opened: handle = 22
4 12/06/2000 09:26:19.510 SEV=6 AUTH/4 RPT=17 10.44.17.179
Authentication successful: handle = 22, server = 10.2.2.5,
user = CSNTUSER
5 12/06/2000 09:26:19.510 SEV=5 PPP/8 RPT=17 10.44.17.179
User [ CSNTUSER ]
Authenticated successfully with MSCHAP-V1
6 12/06/2000 09:26:19.510 SEV=7 AUTH/13 RPT=22
Authentication session closed: handle = 22
7 12/06/2000 09:26:22.560 SEV=4 AUTH/21 RPT=30
User CSNTUSER connected
```

Возможные ошибки

Можно встретиться с возможными ошибками как показано ниже.

Неверное имя пользователя или пароль на Cisco Secure ACS для Сервера Windows Radius

- Выходные данные отладки VPN 3000 Concentrator
```
6 12/06/2000 09:33:03.910 SEV=4 PPTP/47
RPT=21 10.44.17.179
Tunnel to peer 10.44.17.179 established

7 12/06/2000 09:33:03.920 SEV=4 PPTP/42 RPT=21 10.44.17.179
Session started on tunnel 10.44.17.179

8 12/06/2000 09:33:06.930 SEV=7 AUTH/12 RPT=23
Authentication session opened: handle = 23

9 12/06/2000 09:33:07.050 SEV=3 AUTH/5 RPT=4 10.44.17.179
Authentication rejected: Reason = Unspecified
handle = 23, server = 10.2.2.5, user = baduser

11 12/06/2000 09:33:07.050 SEV=5 PPP/9 RPT=4 10.44.17.179
User [ baduser ]
disconnected.. failed authentication ( MSCHAP-V1 )

12 12/06/2000 09:33:07.050 SEV=7 AUTH/13 RPT=23
Authentication session closed: handle = 23
```
- Cisco Secure ACS для вывода лога Windows
```
03/18/2000,08:02:47,Authen failed,
baduser,,,CS user
unknown,,,1155,10.2.2.1
```
- Сообщение, что пользователь видит (от Windows 98)
```
Error 691: The computer you have
dialed in to has denied access because
the username and/or password is invalid on the domain.
```

"Шифрование MPPE, Требуемое", выбрано на концентраторе, но Cisco Secure ACS для Windows Server не настроен для MS-CHAP-MPPE-Keys и MS-CHAP-MPPE-Types

- Выходные данные отладки VPN 3000 ConcentratorЕсли AUTHDECODE (Степени серьезности ошибки 1-13) и отладка PPTP (Степени серьезности ошибки 1-9) идет, журнал показывает, что Cisco Secure ACS для Windows Server не передает определяемые производителем характеристика 26 (0x1A) в access-accept от сервера (частичный журнал).
```
2221 12/08/2000 10:01:52.360 SEV=13 AUTHDECODE/0 RPT=545
0000: 024E002C 80AE75F6 6C365664 373D33FE     .N.,..u.l6Vd7=3.
0010: 6DF74333 501277B2 129CBC66 85FFB40C     m.C3P.w....f....
0020: 16D42FC4 BD020806 FFFFFFFF                 ../.........

2028 12/08/2000 10:00:29.570 SEV=5 PPP/13 RPT=12 10.44.17.179
User [ CSNTUSER ] disconnected. Data encrypt required. Auth server
or auth protocol will not support encrypt.
```
- Cisco Secure ACS для вывода лога Windows не показывает сбоев.
- Сообщение, что видит пользователь
```
Error 691: The computer you have dialed in to has
denied access because
the username and/or password is invalid on the domain.
```

Дополнительные сведения

- Страница поддержки концентратора Cisco VPN серии 3000
- Страница поддержки Cisco VPN 3000 Series Client
- Страница поддержки IPSec
- Страница поддержки Cisco Secure ACS для Windows
- Страница поддержки RADIUS
- Страница поддержки PPTP
- RFC 2637: Протокол PPTP

- Запросы комментариев (RFC)
- Cisco Systems – техническая поддержка и документация