Настройка Cisco IOS и клиентов Windows 2000 для L2TP с использованием Microsoft IAS

Содержание

Введение

Этот документ предоставляет инструкции по тому, как настроить программное обеспечение Cisco IOS и клиентов Windows 2000 для Internet Authentication Server (IAS) Microsoft использования протокола туннелирования на уровне 2 (L2TP).

См. L2TP По IPsec между Windows 2000/XP PC и Использованием примера конфигурации PIX/ASA 7.2 Предварительного общего ключа для получения дополнительной информации о том, как настроить L2TP через IP-безопасность (IPSec) от удаленного Microsoft Windows 2000/2003 и клиентов XP к офису корпорации Устройства безопасности PIX с помощью предварительных общих ключей с Microsoft Windows 2003 сервера RADIUS IAS для проверки подлинности пользователя.

См. L2TP Настройки по IPSec от Windows 2000 или Клиента XP к концентратору Cisco VPN серии 3000 Использование Предварительных общих ключей для получения дополнительной информации о том, как настроить L2TP через IPSec от удаленного Microsoft Windows 2000 и клиентов XP к корпоративному узлу с помощью зашифрованного метода.

Предварительные условия

Требования

Для данного документа отсутствуют предварительные условия.

Используемые компоненты

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

- Дополнительный компонент Microsoft IAS устанавливается на расширенной версии сервера Microsoft 2000 с Active Directory
- Маршрутизатор Cisco 3600
- ПО Cisco IOS версии c3640-io3s56i-mz.121-5. T

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 Условные обозначения технических терминов Cisco.

Настройка

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

Примечание: Чтобы получить подробные сведения о командах в данном документе, используйте Средство поиска команд (только для зарегистрированных клиентов).

Схема сети

В настоящем документе используется следующая схема сети:

Этот документ использует эти пулы IP для клиентов удаленного доступа:

- Маршрутизатор/шлюз: 192.168.1.2 ~ 192.168.1.254
- LNS: 172.16.10.1 ~ 172.16.10.1

Настройка сервера Windows 2000 Advanced Server для Microsoft IAS

Убедитесь, что установлен Microsoft IAS. Для установки Microsoft IAS войдите как администратор и выполните эти шаги:

1. **В разеделе Network Services убедитесь, что сняты все флажки.**
2. Проверьте флажок **Internet Authentication Server (IAS)** и затем нажмите **OK**.
3. **В мастере компонентов Windows нажмите Next.** В случае появления запроса, вставьте CD-диск Windows 2000.
4. Когда необходимые файлы будут скопированы, нажмите **Finish** и затем закройте все окна. Выполнять перезагрузку не нужно.

Настройка клиентов RADIUS

Выполните следующие действия:

1. **В разделе Administrative Tools, откройте консоль Internet Authentication Server ии нажмите Clients.**
2. В **окне Friendly Name** введите IP-адрес сервера доступа к сети (NAS).
3. Нажмите **Use This IP**.
4. В выпадающем списке **Клиента - поставщика** гарантируйте, что выбран **Стандарт RADIUS**.
5. В **Общем секретном ключе** и **Подтверждают** коробки **Общего секретного ключа**, вводят пароль и затем нажимают **Finish**.
6. В дереве консоли щелкните правой кнопкой **по Internet Authentication Service**, и затем нажмите **Start**.
7. Закройте консоль.

Настройка пользователей в IAS

CiscoSecure, база данных пользователей Server (RADIUS) Пользователя с наборным телефонным доступом Удаленной аутентификации Windows 2000 плотно связана с базой данных Пользователя Windows.

- Если Active Directory установлен на вашем Сервере Windows 2000, создайте своих новых пользователей с удаленным доступом от **Пользователей и компьютеров Active Directory**.
- Если Active Directory не установлен, можно использовать **Локальных пользователей и Группы** от **Средств администрирования** для создания новых пользователей.

Настройка пользователей в Active Directory

Выполните эти шаги для настройки пользователей с Active Directory:

1. **На консоли пользователей и компьютеров Active Directory разверните свой домен.**
2. Щелкните правой кнопкой мыши **Пользовательскую Прокрутку** для выбора **New User**.
3. Создайте нового пользователя с именем tac.
4. Введите ваш пароль в **Пароль** и **Подтвердите Диалоговые окна пароля**.
5. **Очистите опцию User Must Change Password at Next Logon и нажмите Next.**
6. Откройте пользовательскую коробку **Свойств** tac. **Перейдите на вкладку Dial-In.**

7. **В разделе Remote Access Permission (Dial-in or VPN), нажмите Allow Access, затем нажмите "OK".**

Настройка пользователей, если не установлен Active Directory

Выполните эти шаги для настройки пользователей, если не установлен Active Directory:

1. От **Средств администрирования** щелкните **по Computer Management**.
2. **Разверните консоль Computer Management и щелкните Local Users and Groups.**
3. Щелкните правой кнопкой мыши **Пользовательскую Прокрутку** для выбора **New User**.
4. Введите пароль в **Пароле** и **Подтвердите Диалоговые окна пароля**.
5. **Очистите опцию User Must Change Password at Next Logon и нажмите Next.**
6. Откройте коробку **Свойств** tac нового пользователя. **Перейдите на вкладку Dial-In.**
7. **В разделе Remote Access Permission (Dial-in or VPN), нажмите Allow Access, затем нажмите "OK".**

Применение политики удаленного доступа к пользователю Windows

Выполните эти шаги для применения политики удаленного доступа:

1. От **Средств администрирования**, открытых консоль **Internet Authentication Server** и, нажимают **Remote Access Policies**.
2. **Нажмите кнопку Add в Specify the Conditions to Match и добавьте Service-Type.** Выберите доступный тип в качестве **Обрамленного**. Добавьте его к выбранным типам и нажмите **OK**.
3. **Нажмите кнопку Add в Specify the Conditions to Match и добавьте Framed Protocol.** Выберите доступный тип в качестве **PPP**. Добавьте его к выбранным типам и нажмите **OK**.
4. **Нажмите кнопку Add в Specify the Conditions to Match и добавьте Windows-Groups, чтобы добавить группу пользователей Windows, к которой принадлежит пользователь.** Выберите группу и добавьте его к выбранным типам. **Нажмите OK.**
5. На **Предоставляют Доступ, если Полномочиями для удаленного доступа по телефонной линии являются Включенные свойства**, выберите **Grant Remote Access Permission**.
6. Закройте консоль.

Настройка клиента Windows 2000 для L2TP

Выполните эти шаги для настройки клиента Windows 2000 для L2TP:

1. От **Меню Пуск** выберите **Settings**, и затем придерживайтесь одного из этих путей:**Панель управления> Сеть и Подключения удаленного доступа***Или***Сеть и Подключения удаленного доступа> Make New Connection**
2. Используйте Мастера для создания соединения, названного **L2TP**. Это подключение соединяется с частной сетью через Интернет. Также необходимо задать туннельный IP-адрес шлюза L2TP или название.
3. **Новое подключение появляется в окне Network и Dial-up Connections в Control Panel.** Отсюда, щелкните по правильной кнопке мыши для редактирования свойств.

4. Под **Вкладкой Сеть** удостоверьтесь, что **Type of Server I Am Calling** установлен в L2TP.
5. Если вы планируете выделить динамический внутренний адрес этому клиенту от шлюза, или через локальный пул или через DHCP, выберите **протокол TCP/IP**. Удостоверьтесь, что клиент настроен для получения IP-адреса автоматически. Можно также выполнить Информацию DNS автоматически.Кнопка **Advanced** позволяет вам определять статический WINS и Информацию DNS.**Вкладка Options позволяет выключать IPSec или назначать другую политику для подключения.**Под **Вкладкой Безопасность** можно определить параметры аутентификации пользователя, такие как PAP, CHAP или MS-CHAP или вход в систему Домена Windows.
6. Когда соединение настроено, можно дважды нажать на нем для запуска экрана входа в систему, затем **Подключение**.

Отключение IPSec для клиента Windows 2000

1. Отредактируйте свойства L2TP подключения удаленного доступа, который вы только что создали. Щелкните правой кнопкой мыши **L2TP** нового соединения для получения **Окна свойств L2TP**.
2. Под **Вкладкой Сеть** нажмите **свойства Internet Protocol (TCP/IP)**. Дважды нажмите **Вкладку Дополнительно**. Перейдите к вкладке **Options**, нажмите **Ip Security Properties** и, если **Do not use IPSEC** выбран, перепроверьте его.

Примечание: У клиентов Microsoft Windows 2000 есть Удаленный доступ по умолчанию и Сервисы агента политики, которые, по умолчанию, создают политику для трафика L2TP. Эта политика по умолчанию не позволяет трафик L2TP без IPSec и шифрования. Можно отключить поведение по умолчанию Microsoft путем редактирования Редактора реестра клиента Microsoft. Процедура к реестру окон редактирования и отключить политику по умолчанию IPSec для трафика L2TP дана в этом разделе. См. документацию microsoft для Реестра окон редактирования.

Используйте Редактор реестра (Regedt32.exe) для добавления новой записи реестра для отключения IPSec. См. документацию Microsoft или Раздел справки Microsoft для Regedt32.exe для получения дополнительной информации.

Необходимо добавить Значение ключа ProhibitIPSec в реестре к каждому основанному на Windows 2000 оконечному компьютеру L2TP или IP - безопасного соединения для предотвращения автоматического фильтра для L2TP и Трафика IPSec от того, чтобы быть созданным. Когда Значение ключа ProhibitIPSec в реестре установлено в одно, ваш основанный на Windows 2000 компьютер не создает автоматический фильтр, который использует аутентификацию CA. Вместо этого это проверяет для локальной переменной или Активной политики IPSec каталога. Для добавления Значения ключа ProhibitIPSec в реестре к основанному на Windows 2000 компьютеру используйте Regedt32.exe для определения местоположения этого ключа в реестре:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Rasman\Parameters
```

Добавьте это значение регистрации к следующему ключу:

```
Value Name: ProhibitIpSec
Data Type: REG_DWORD
Value: 1
```

Примечание: Необходимо перезапустить основанный на Windows 2000 компьютер для изменений для вступления в силу. См. эти статьи microsoft для получения дальнейшей информации:

- Q258261 - Отключение политики IPsec, используемой с L2TP
- Q240262 - Как Настроить Соединение L2TP/IPSec Использование Предварительного общего ключа

Cisco IOS Настройки для L2TP

Эти конфигурации выделяют команды, требуемые для L2TP без IPSec. Как только эта базовая конфигурация работает, можно также настроить IPSec.

angela

```
Building configuration...
Current configuration : 1595 bytes
!
version 12.1
no service single-slot-reload-enable
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname angela
!
logging rate-limit console 10 except errors
!--- Enable AAA services here. aaa new-model aaa
authentication login default group radius local aaa
authentication login console none aaa authentication ppp
default group radius local aaa authorization network
default group radius local enable password ww ! memory-
size iomem 30 ip subnet-zero ! ! no ip finger no ip
domain-lookup ip host rund 172.17.247.195 ! ip audit
notify log ip audit po max-events 100 ip address-pool
local ! ! !--- Enable VPN/VPDN services and define
groups and !--- specific variables required for the
group. vpdn enable no vpdn logging ! vpdn-group
L2TP_Windows 2000Client !--- Default L2TP VPDN group. !-
-- Allow the Router to accept incoming requests. accept-
dialin protocol L2TP virtual-template 1 no L2TP tunnel
authentication !--- Users are authenticated at the NAS
or LNS !--- before the tunnel is established. This is
not !--- required for client-initiated tunnels. ! ! call
rsvp-sync ! ! ! ! ! ! controller E1 2/0 ! ! interface
Loopback0 ip address 172.16.10.100 255.255.255.0 !
interface Ethernet0/0 ip address 10.200.20.2
255.255.255.0 half-duplex ! interface Virtual-Template1
ip unnumbered Loopback0 peer default ip address pool
default ppp authentication ms-chap ! ip local pool
default 172.16.10.1 172.16.10.10 ip classless ip route
0.0.0.0 0.0.0.0 10.200.20.1 ip route 192.168.1.0
255.255.255.0 10.200.20.250 no ip http server ! radius-
server host 10.200.20.245 auth-port 1645 acct-port 1646
radius-server retransmit 3 radius-server key cisco !
dial-peer cor custom ! ! ! ! ! line con 0 exec-timeout 0
0 login authentication console transport input none line
33 50 modem InOut line aux 0 line vty 0 4 exec-timeout 0
0 password ww ! end angela# *Mar 12 23:10:54.176: L2TP:
I SCCRQ from RSHANMUG-W2K1.cisco.com tnl 5 *Mar 12
23:10:54.176: Tnl 8663 L2TP: New tunnel created for
remote RSHANMUG-W2K1.cisco.com, address 192.168.1.56
*Mar 12 23:10:54.176: Tnl 8663 L2TP: O SCCRP to
RSHANMUG-W2K1.cisco.com tnlid 5 *Mar 12 23:10:54.180:
Tnl 8663 L2TP: Tunnel state change from idle to wait-
```

```
ctl-reply *Mar 12 23:10:54.352: Tnl 8663 L2TP: I SCCCN
from RSHANMUG-W2K1.cisco.com tnl 5 *Mar 12 23:10:54.352:
Tnl 8663 L2TP: Tunnel state change from wait-ctl-reply
to established *Mar 12 23:10:54.352: Tnl 8663 L2TP: SM
State established *Mar 12 23:10:54.356: Tnl 8663 L2TP: I
ICRQ from RSHANMUG-W2K1.cisco.com tnl 5 *Mar 12
23:10:54.356: Tnl/Cl 8663/44 L2TP: Session FS enabled
*Mar 12 23:10:54.356: Tnl/Cl 8663/44 L2TP: Session state
change from idle to wait-connect *Mar 12 23:10:54.356:
Tnl/Cl 8663/44 L2TP: New session created *Mar 12
23:10:54.356: Tnl/Cl 8663/44 L2TP: O ICRP to RSHANMUG-
W2K1.cisco.com 5/1 *Mar 12 23:10:54.544: Tnl/Cl 8663/44
L2TP: I ICCN from RSHANMUG-W2K1.cisco.com tnl 5, cl 1
*Mar 12 23:10:54.544: Tnl/Cl 8663/44 L2TP: Session state
change from wait-connect to established *Mar 12
23:10:54.544: Vi1 VPDN: Virtual interface created for
*Mar 12 23:10:54.544: Vi1 PPP: Phase is DOWN, Setup [0
sess, 0 load] *Mar 12 23:10:54.544: Vi1 VPDN: Clone from
Vtemplate 1 filterPPP=0 blocking *Mar 12 23:10:54.620:
Tnl/Cl 8663/44 L2TP: Session with no hwidb *Mar 12
23:10:54.624: %LINK-3-UPDOWN: Interface Virtual-Access1,
changed state to up *Mar 12 23:10:54.624: Vi1 PPP: Using
set call direction *Mar 12 23:10:54.624: Vi1 PPP:
Treating connection as a callin *Mar 12 23:10:54.624:
Vi1 PPP: Phase is ESTABLISHING, Passive Open [0 sess, 0
load] *Mar 12 23:10:54.624: Vi1 LCP: State is Listen
*Mar 12 23:10:54.624: Vi1 VPDN: Bind interface
direction=2 *Mar 12 23:10:56.556: Vi1 LCP: I CONFREQ
[Listen] id 1 len 44 *Mar 12 23:10:56.556: Vi1 LCP:
MagicNumber 0x595E7636 (0x0506595E7636) *Mar 12
23:10:56.556: Vi1 LCP: PFC (0x0702) *Mar 12
23:10:56.556: Vi1 LCP: ACFC (0x0802) *Mar 12
23:10:56.556: Vi1 LCP: Callback 6 (0x0D0306) *Mar 12
23:10:56.556: Vi1 LCP: MRRU 1614 (0x1104064E) *Mar 12
23:10:56.556: Vi1 LCP: EndpointDisc 1 Local *Mar 12
23:10:56.556: Vi1 LCP:
(0x1317012E07E41982EB4EF790F1BF1862) *Mar 12
23:10:56.556: Vi1 LCP: (0x10D0AC00000002) *Mar 12
23:10:56.556: Vi1 AAA/AUTHOR/FSM: (0): LCP succeeds
trivially *Mar 12 23:10:56.556: Vi1 LCP: O CONFREQ
[Listen] id 1 len 15 *Mar 12 23:10:56.556: Vi1 LCP:
AuthProto MS-CHAP (0x0305C22380) *Mar 12 23:10:56.556:
Vi1 LCP: MagicNumber 0x4E1B09B8 (0x05064E1B09B8) *Mar 12
23:10:56.560: Vi1 LCP: O CONFREJ [Listen] id 1 len 34
*Mar 12 23:10:56.560: Vi1 LCP: Callback 6 (0x0D0306)
*Mar 12 23:10:56.560: Vi1 LCP: MRRU 1614 (0x1104064E)
*Mar 12 23:10:56.560: Vi1 LCP: EndpointDisc 1 Local *Mar
12 23:10:56.560: Vi1 LCP:
(0x1317012E07E41982EB4EF790F1BF1862) *Mar 12
23:10:56.560: Vi1 LCP: (0x10D0AC00000002) *Mar 12
23:10:56.700: Vi1 LCP: I CONFACK [REQsent] id 1 len 15
*Mar 12 23:10:56.700: Vi1 LCP: AuthProto MS-CHAP
(0x0305C22380) *Mar 12 23:10:56.704: Vi1 LCP:
MagicNumber 0x4E1B09B8 (0x05064E1B09B8) *Mar 12
23:10:56.704: Vi1 LCP: I CONFREQ [ACKrcvd] id 2 len 14
*Mar 12 23:10:56.704: Vi1 LCP: MagicNumber 0x595E7636
(0x0506595E7636) *Mar 12 23:10:56.704: Vi1 LCP: PFC
(0x0702) *Mar 12 23:10:56.704: Vi1 LCP: ACFC (0x0802)
*Mar 12 23:10:56.704: Vi1 LCP: O CONFACK [ACKrcvd] id 2
len 14 *Mar 12 23:10:56.708: Vi1 LCP: MagicNumber
0x595E7636 (0x0506595E7636) *Mar 12 23:10:56.708: Vi1
LCP: PFC (0x0702) *Mar 12 23:10:56.708: Vi1 LCP: ACFC
(0x0802) *Mar 12 23:10:56.708: Vi1 LCP: State is Open
*Mar 12 23:10:56.708: Vi1 PPP: Phase is AUTHENTICATING,
```

```
by this end [0 sess, 0 load] *Mar 12 23:10:56.708: Vi1
MS-CHAP: O CHALLENGE id 28 len 21 from angela *Mar 12
23:10:56.852: Vi1 LCP: I IDENTIFY [Open] id 3 len 18
magic 0x595E7636 MSRASV5.00 *Mar 12 23:10:56.872: Vi1
LCP: I IDENTIFY [Open] id 4 len 27 magic 0x595E7636
MSRAS-1- RSHANMUG-W2K1 *Mar 12 23:10:56.880: Vi1 MS-
CHAP: I RESPONSE id 28 len 57 from tac *Mar 12
23:10:56.880: AAA: parse name=Virtual-Access1 idb
type=21 tty=-1 *Mar 12 23:10:56.880: AAA: name=Virtual-
Access1 flags=0x11 type=5 shelf=0 slot=0 adapter=0
port=1 channel=0 *Mar 12 23:10:56.884: AAA/MEMORY:
create_user (0x6273D024) user='tac' ruser=''
port='Virtual-Access1' rem_addr='' authen_type=MSCHAP
service=PPP priv=1 *Mar 12 23:10:56.884:
AAA/AUTHEN/START (3634835145): port='Virtual-Access1'
list='' action=LOGIN service=PPP *Mar 12 23:10:56.884:
AAA/AUTHEN/START (3634835145): using default list *Mar
12 23:10:56.884: AAA/AUTHEN/START (3634835145):
Method=radius (radius) *Mar 12 23:10:56.884: RADIUS:
ustruct sharecount=0 *Mar 12 23:10:56.884: RADIUS:
Initial Transmit Virtual-Access1 id 173
10.200.20.245:1645, Access-Request, len 129 *Mar 12
23:10:56.884: Attribute 4 6 0AC81402 *Mar 12
23:10:56.884: Attribute 5 6 00000001 *Mar 12
23:10:56.884: Attribute 61 6 00000001 *Mar 12
23:10:56.884: Attribute 1 5 7461631A *Mar 12
23:10:56.884: Attribute 26 16 000001370B0A0053 *Mar 12
23:10:56.884: Attribute 26 58 0000013701341C01 *Mar 12
23:10:56.884: Attribute 6 6 00000002 *Mar 12
23:10:56.884: Attribute 7 6 00000001 *Mar 12
23:10:56.900: RADIUS: Received from id 173
10.200.20.245:1645, Access-Accept, len 116 *Mar 12
23:10:56.900: Attribute 7 6 00000001 *Mar 12
23:10:56.900: Attribute 6 6 00000002 *Mar 12
23:10:56.900: Attribute 25 32 502605A6 *Mar 12
23:10:56.900: Attribute 26 40 000001370C22F6D5 *Mar 12
23:10:56.900: Attribute 26 12 000001370A061C4E *Mar 12
23:10:56.900: AAA/AUTHEN (3634835145): status = PASS
*Mar 12 23:10:56.900: Vi1 AAA/AUTHOR/LCP: Authorize LCP
*Mar 12 23:10:56.900: Vi1 AAA/AUTHOR/LCP (1995716469):
Port='Virtual-Access1' list='' service=NET *Mar 12
23:10:56.900: AAA/AUTHOR/LCP: Vi1 (1995716469)
user='tac' *Mar 12 23:10:56.900: Vi1 AAA/AUTHOR/LCP
(1995716469): send AV service=ppp *Mar 12 23:10:56.900:
Vi1 AAA/AUTHOR/LCP (1995716469): send AV protocol=lcp
*Mar 12 23:10:56.900: Vi1 AAA/AUTHOR/LCP (1995716469):
found list default *Mar 12 23:10:56.904: Vi1
AAA/AUTHOR/LCP (1995716469): Method=radius (radius) *Mar
12 23:10:56.904: RADIUS: unrecognized Microsoft VSA type
10 *Mar 12 23:10:56.904: Vi1 AAA/AUTHOR (1995716469):
Post authorization status = PASS_REPL *Mar 12
23:10:56.904: Vi1 AAA/AUTHOR/LCP: Processing AV
service=ppp *Mar 12 23:10:56.904: Vi1 AAA/AUTHOR/LCP:
Processing AV
mschap_mppe_keys*1p1T11=1v1O1~11a1W11151\1V1M1#11Z1`1k1}
111 *Mar 12 23:10:56.904: Vi1 MS-CHAP: O SUCCESS id 28
len 4 *Mar 12 23:10:56.904: Vi1 PPP: Phase is UP [0
sess, 0 load] *Mar 12 23:10:56.904: Vi1 AAA/AUTHOR/FSM:
(0): Can we start IPCP? *Mar 12 23:10:56.904: Vi1
AAA/AUTHOR/FSM (2094713042): Port='Virtual-Access1'
list='' service=NET *Mar 12 23:10:56.904:
AAA/AUTHOR/FSM: Vi1 (2094713042) user='tac' *Mar 12
23:10:56.904: Vi1 AAA/AUTHOR/FSM (2094713042): send AV
service=ppp *Mar 12 23:10:56.904: Vi1 AAA/AUTHOR/FSM
```

```
(2094713042): send AV protocol=ip *Mar 12 23:10:56.904:
Vi1 AAA/AUTHOR/FSM (2094713042): found list default *Mar
12 23:10:56.904: Vi1 AAA/AUTHOR/FSM (2094713042):
Method=radius (radius) *Mar 12 23:10:56.908: RADIUS:
unrecognized Microsoft VSA type 10 *Mar 12 23:10:56.908:
Vi1 AAA/AUTHOR (2094713042): Post authorization status =
PASS_REPL *Mar 12 23:10:56.908: Vi1 AAA/AUTHOR/FSM: We
can start IPCP *Mar 12 23:10:56.908: Vi1 IPCP: O CONFREQ
[Closed] id 1 len 10 *Mar 12 23:10:56.908: Vi1 IPCP:
Address 172.16.10.100 (0x0306AC100A64) *Mar 12
23:10:57.040: Vi1 CCP: I CONFREQ [Not negotiated] id 5
len 10 *Mar 12 23:10:57.040: Vi1 CCP: MS-PPC supported
bits 0x01000001 (0x120601000001) *Mar 12 23:10:57.040:
Vi1 LCP: O PROTREJ [Open] id 2 len 16 protocol CCP
(0x80FD0105000A120601000001) *Mar 12 23:10:57.052: Vi1
IPCP: I CONFREQ [REQsent] id 6 len 34 *Mar 12
23:10:57.052: Vi1 IPCP: Address 0.0.0.0 (0x030600000000)
*Mar 12 23:10:57.052: Vi1 IPCP: PrimaryDNS 0.0.0.0
(0x810600000000) *Mar 12 23:10:57.052: Vi1 IPCP:
PrimaryWINS 0.0.0.0 (0x820600000000) *Mar 12
23:10:57.052: Vi1 IPCP: SecondaryDNS 0.0.0.0
(0x830600000000) *Mar 12 23:10:57.052: Vi1 IPCP:
SecondaryWINS 0.0.0.0 (0x840600000000) *Mar 12
23:10:57.052: Vi1 AAA/AUTHOR/IPCP: Start. Her address
0.0.0.0, we want 0.0.0.0 *Mar 12 23:10:57.056: Vi1
AAA/AUTHOR/IPCP: Processing AV service=ppp *Mar 12
23:10:57.056: Vi1 AAA/AUTHOR/IPCP: Processing AV
mschap_mppe_keys*1p1T11=1v1O1~11a1W11151\1V1M1#11Z1`1k1}
111 *Mar 12 23:10:57.056: Vi1 AAA/AUTHOR/IPCP:
Authorization succeeded *Mar 12 23:10:57.056: Vi1
AAA/AUTHOR/IPCP: Done. Her address 0.0.0.0, we want
0.0.0.0 *Mar 12 23:10:57.056: Vi1 IPCP: Pool returned
172.16.10.1 *Mar 12 23:10:57.056: Vi1 IPCP: O CONFREJ
[REQsent] id 6 len 28 *Mar 12 23:10:57.056: Vi1 IPCP:
PrimaryDNS 0.0.0.0 (0x810600000000) *Mar 12
23:10:57.056: Vi1 IPCP: PrimaryWINS 0.0.0.0
(0x820600000000) *Mar 12 23:10:57.056: Vi1 IPCP:
SecondaryDNS 0.0.0.0 (0x830600000000) *Mar 12
23:10:57.056: Vi1 IPCP: SecondaryWINS 0.0.0.0
(0x840600000000) *Mar 12 23:10:57.060: Vi1 IPCP: I
CONFACK [REQsent] id 1 len 10 *Mar 12 23:10:57.060: Vi1
IPCP: Address 172.16.10.100 (0x0306AC100A64) *Mar 12
23:10:57.192: Vi1 IPCP: I CONFREQ [ACKrcvd] id 7 len 10
*Mar 12 23:10:57.192: Vi1 IPCP: Address 0.0.0.0
(0x030600000000) *Mar 12 23:10:57.192: Vi1
AAA/AUTHOR/IPCP: Start. Her address 0.0.0.0, we want
172.16.10.1 *Mar 12 23:10:57.192: Vi1 AAA/AUTHOR/IPCP:
Processing AV service=ppp *Mar 12 23:10:57.192: Vi1
AAA/AUTHOR/IPCP: Processing AV
mschap_mppe_keys*1p1T11=1v1O1~11a1W11151\1V1M1#11Z1`1k1}
111 *Mar 12 23:10:57.192: Vi1 AAA/AUTHOR/IPCP:
Authorization succeeded *Mar 12 23:10:57.192: Vi1
AAA/AUTHOR/IPCP: Done. Her address 0.0.0.0, we want
172.16.10.1 *Mar 12 23:10:57.192: Vi1 IPCP: O CONFNAK
[ACKrcvd] id 7 len 10 *Mar 12 23:10:57.192: Vi1 IPCP:
Address 172.16.10.1 (0x0306AC100A01) *Mar 12
23:10:57.324: Vi1 IPCP: I CONFREQ [ACKrcvd] id 8 len 10
*Mar 12 23:10:57.324: Vi1 IPCP: Address 172.16.10.1
(0x0306AC100A01) *Mar 12 23:10:57.324: Vi1
AAA/AUTHOR/IPCP: Start. Her address 172.16.10.1, we want
172.16.10.1 *Mar 12 23:10:57.324: Vi1 AAA/AUTHOR/IPCP
(413757991): Port='Virtual-Access1' list='' service=NET
*Mar 12 23:10:57.324: AAA/AUTHOR/IPCP: Vi1 (413757991)
user='tac' *Mar 12 23:10:57.324: Vi1 AAA/AUTHOR/IPCP
```

```
(413757991): send AV service=ppp *Mar 12 23:10:57.324:
Vi1 AAA/AUTHOR/IPCP (413757991): send AV protocol=ip
*Mar 12 23:10:57.324: Vi1 AAA/AUTHOR/IPCP (413757991):
send AV addr*172.16.10.1 *Mar 12 23:10:57.324: Vi1
AAA/AUTHOR/IPCP (413757991): found list default *Mar 12
23:10:57.324: Vi1 AAA/AUTHOR/IPCP (413757991):
Method=radius (radius) *Mar 12 23:10:57.324: RADIUS:
unrecognized Microsoft VSA type 10 *Mar 12 23:10:57.324:
Vi1 AAA/AUTHOR (413757991): Post authorization status =
PASS_REPL *Mar 12 23:10:57.324: Vi1 AAA/AUTHOR/IPCP:
Reject 172.16.10.1, using 172.16.10.1 *Mar 12
23:10:57.328: Vi1 AAA/AUTHOR/IPCP: Processing AV
service=ppp *Mar 12 23:10:57.328: Vi1 AAA/AUTHOR/IPCP:
Processing AV
mschap_mppe_keys*1p1T11=1v1O1~11a1W11151\1V1M1#11Z1`1k1}
111 *Mar 12 23:10:57.328: Vi1 AAA/AUTHOR/IPCP:
Processing AV addr*172.16.10.1 *Mar 12 23:10:57.328: Vi1
AAA/AUTHOR/IPCP: Authorization succeeded *Mar 12
23:10:57.328: Vi1 AAA/AUTHOR/IPCP: Done. Her address
172.16.10.1, we want 172.16.10.1 *Mar 12 23:10:57.328:
Vi1 IPCP: O CONFACK [ACKrcvd] id 8 len 10 *Mar 12
23:10:57.328: Vi1 IPCP: Address 172.16.10.1
(0x0306AC100A01) *Mar 12 23:10:57.328: Vi1 IPCP: State
is Open *Mar 12 23:10:57.332: Vi1 IPCP: Install route to
172.16.10.1 *Mar 12 23:10:57.904: %LINEPROTO-5-UPDOWN:
Line protocol on Interface Virtual-Access1, changed
state to up *Mar 12 23:11:06.324: Vi1 LCP: I ECHOREP
[Open] id 1 len 12 magic 0x595E7636 *Mar 12
23:11:06.324: Vi1 LCP: Received id 1, sent id 1, line up
```

angela#**show vpdn** L2TP Tunnel and Session Information Total tunnels 1 sessions 1 LocID RemID Remote Name State Remote Address Port Sessions 8663 5 RSHANMUG-W2K1.c est 192.168.1.56 1701 1 LocID RemID TunID Intf Username State Last Chg Fastswitch 44 1 8663 Vi1 tac est 00:00:18 enabled %No active L2F tunnels %No active PPTP tunnels %No active PPPoE tunnels *Mar 12 23:11:16.332: Vi1 LCP: I ECHOREP [Open] id 2 len 12 magic 0x595E7636 *Mar 12 23:11:16.332: Vi1 LCP: Received id 2, sent id 2, line upsh caller ip Line User IP Address Local Number Remote Number <-> Vi1 tac 172.16.10.1 - - in angela#**show ip route** Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area * - candidate default, U - per-user static route, o - ODR P - periodic downloaded static route Gateway of last resort is 10.200.20.1 to network 0.0.0.0 172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks C 172.16.10.0/24 is directly connected, Loopback0 C 172.16.10.1/32 is directly connected, Virtual-Access1 10.0.0.0/24 is subnetted, 1 subnets C 10.200.20.0 is directly connected, Ethernet0/0 S 192.168.1.0/24 [1/0] via 10.200.20.250 S* 0.0.0.0/0 [1/0] via 10.200.20.1 *Mar 12 23:11:26.328: Vi1 LCP: I ECHOREP [Open] id 3 len 12 magic 0x595E7636 *Mar 12 23:11:26.328: Vi1 LCP: Received id 3, sent id 3, line up172.16.10.1 angela#**ping 172.16.10.1** Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 172.16.10.1, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 156/160/168 ms

Чтобы включить шифрование

Добавьте команду **ppp encrypt mppe 40** под **interface virtual-template 1**. Удостоверьтесь, что шифрование выбрано в клиенте Microsoft также.

```
*Mar 12 23:27:36.608: L2TP: I SCCRQ from  RSHANMUG-W2K1.cisco.com tnl 13
*Mar 12 23:27:36.608: Tnl 31311 L2TP: New tunnel created for remote
RSHANMUG-W2K1.cisco.com, address 192.168.1.56
*Mar 12 23:27:36.608: Tnl 31311 L2TP: O SCCRP  to  RSHANMUG-W2K1.cisco.com
tnlid 13
*Mar 12 23:27:36.612: Tnl 31311 L2TP: Tunnel state change from idle to
wait-ctl-reply
*Mar 12 23:27:36.772: Tnl 31311 L2TP: I SCCCN from  RSHANMUG-W2K1.cisco.com
tnl 13
```

```
*Mar 12 23:27:36.772: Tnl 31311 L2TP: Tunnel state change from
wait-ctl-reply to established
*Mar 12 23:27:36.776: Tnl 31311 L2TP: SM State established
*Mar 12 23:27:36.780: Tnl 31311 L2TP: I ICRQ from  RSHANMUG-W2K1.cisco.com
tnl 13
*Mar 12 23:27:36.780: Tnl/Cl 31311/52 L2TP: Session FS enabled
*Mar 12 23:27:36.780: Tnl/Cl 31311/52 L2TP: Session state change from idle
to wait-connect
*Mar 12 23:27:36.780: Tnl/Cl 31311/52 L2TP: New session created
*Mar 12 23:27:36.780: Tnl/Cl 31311/52 L2TP: O ICRP to
RSHANMUG-W2K1.cisco.com 13/1
*Mar 12 23:27:36.924: Tnl/Cl 31311/52 L2TP: I ICCN from
RSHANMUG-W2K1.cisco.com tnl 13, cl 1
*Mar 12 23:27:36.928: Tnl/Cl 31311/52 L2TP: Session state change from
wait-connect to established
*Mar 12 23:27:36.928: Vi1 VPDN: Virtual interface created for
*Mar 12 23:27:36.928: Vi1 PPP: Phase is DOWN, Setup [0 sess, 0 load]
*Mar 12 23:27:36.928: Vi1 VPDN: Clone from Vtemplate 1 filterPPP=0 blocking
*Mar 12 23:27:36.972: Tnl/Cl 31311/52 L2TP: Session with no hwidb
*Mar 12 23:27:36.976: %LINK-3-UPDOWN: Interface Virtual-Access1, changed
state to up
*Mar 12 23:27:36.976: Vi1 PPP: Using set call direction
*Mar 12 23:27:36.976: Vi1 PPP: Treating connection as a callin
*Mar 12 23:27:36.976: Vi1 PPP: Phase is ESTABLISHING, Passive Open [0 sess,
0 load]
*Mar 12 23:27:36.976: Vi1 LCP: State is Listen
*Mar 12 23:27:36.976: Vi1 VPDN: Bind interface direction=2
*Mar 12 23:27:38.976: Vi1 LCP: TIMEout: State Listen
*Mar 12 23:27:38.976: Vi1 AAA/AUTHOR/FSM: (0): LCP succeeds trivially
*Mar 12 23:27:38.976: Vi1 LCP: O CONFREQ [Listen] id 1 len 15
*Mar 12 23:27:38.976: Vi1 LCP:  AuthProto MS-CHAP (0x0305C22380)
*Mar 12 23:27:38.976: Vi1 LCP:  MagicNumber 0x4E2A5593 (0x05064E2A5593)
*Mar 12 23:27:38.984: Vi1 LCP: I CONFREQ [REQsent] id 1 len 44
*Mar 12 23:27:38.984: Vi1 LCP:  MagicNumber 0x4B4817ED (0x05064B4817ED)
*Mar 12 23:27:38.984: Vi1 LCP:  PFC (0x0702)
*Mar 12 23:27:38.984: Vi1 LCP:  ACFC (0x0802)
*Mar 12 23:27:38.984: Vi1 LCP:  Callback 6  (0x0D0306)
*Mar 12 23:27:38.984: Vi1 LCP:  MRRU 1614 (0x1104064E)
*Mar 12 23:27:38.984: Vi1 LCP:  EndpointDisc 1 Local
*Mar 12 23:27:38.984: Vi1 LCP:   (0x1317012E07E41982EB4EF790F1BF1862)
*Mar 12 23:27:38.984: Vi1 LCP:   (0x10D0AC0000000A)
*Mar 12 23:27:38.984: Vi1 LCP: O CONFREJ [REQsent] id 1 len 34
*Mar 12 23:27:38.984: Vi1 LCP:  Callback 6  (0x0D0306)
*Mar 12 23:27:38.984: Vi1 LCP:  MRRU 1614 (0x1104064E)
*Mar 12 23:27:38.984: Vi1 LCP:  EndpointDisc 1 Local
*Mar 12 23:27:38.988: Vi1 LCP:   (0x1317012E07E41982EB4EF790F1BF1862)
*Mar 12 23:27:38.988: Vi1 LCP:   (0x10D0AC0000000A)
*Mar 12 23:27:39.096: Vi1 LCP: I CONFACK [REQsent] id 1 len 15
*Mar 12 23:27:39.096: Vi1 LCP:  AuthProto MS-CHAP (0x0305C22380)
*Mar 12 23:27:39.096: Vi1 LCP:  MagicNumber 0x4E2A5593 (0x05064E2A5593)
*Mar 12 23:27:39.128: Vi1 LCP: I CONFREQ [ACKrcvd] id 2 len 14
*Mar 12 23:27:39.128: Vi1 LCP:  MagicNumber 0x4B4817ED (0x05064B4817ED)
*Mar 12 23:27:39.128: Vi1 LCP:  PFC (0x0702)
*Mar 12 23:27:39.128: Vi1 LCP:  ACFC (0x0802)
*Mar 12 23:27:39.128: Vi1 LCP: O CONFACK [ACKrcvd] id 2 len 14
*Mar 12 23:27:39.128: Vi1 LCP:  MagicNumber 0x4B4817ED (0x05064B4817ED)
*Mar 12 23:27:39.128: Vi1 LCP:  PFC (0x0702)
*Mar 12 23:27:39.128: Vi1 LCP:  ACFC (0x0802)
*Mar 12 23:27:39.128: Vi1 LCP: State is Open
*Mar 12 23:27:39.128: Vi1 PPP: Phase is AUTHENTICATING, by this end [0
sess, 0 load]
*Mar 12 23:27:39.128: Vi1 MS-CHAP: O CHALLENGE id 32 len 21 from angela
*Mar 12 23:27:39.260: Vi1 LCP: I IDENTIFY [Open] id 3 len 18 magic
0x4B4817ED MSRASV5.00
```

```
*Mar 12 23:27:39.288: Vi1 LCP: I IDENTIFY [Open] id 4 len 27 magic
0x4B4817ED MSRAS-1- RSHANMUG-W2K1
*Mar 12 23:27:39.296: Vi1 MS-CHAP: I RESPONSE id 32 len 57 from tac
*Mar 12 23:27:39.296: AAA: parse name=Virtual-Access1 idb type=21 tty=-1
*Mar 12 23:27:39.296: AAA: name=Virtual-Access1 flags=0x11 type=5 shelf=0
slot=0 adapter=0 port=1 channel=0
*Mar 12 23:27:39.296: AAA/MEMORY: create_user (0x6273D528) user='tac'
ruser='' port='Virtual-Access1' rem_addr='' authen_type=MSCHAP service=PPP
priv=1
*Mar 12 23:27:39.296: AAA/AUTHEN/START (2410248116): port='Virtual-Access1'
list='' action=LOGIN service=PPP
*Mar 12 23:27:39.296: AAA/AUTHEN/START (2410248116): using default list
*Mar 12 23:27:39.296: AAA/AUTHEN/START (2410248116): Method=radius (radius)
*Mar 12 23:27:39.296: RADIUS: ustruct sharecount=0
*Mar 12 23:27:39.300: RADIUS: Initial Transmit Virtual-Access1 id 181
10.200.20.245:1645, Access-Request, len 129
*Mar 12 23:27:39.300:      Attribute 4 6 0AC81402
*Mar 12 23:27:39.300:      Attribute 5 6 00000001
*Mar 12 23:27:39.300:      Attribute 61 6 00000001
*Mar 12 23:27:39.300:      Attribute 1 5 7461631A
*Mar 12 23:27:39.300:      Attribute 26 16 000001370B0AFC72
*Mar 12 23:27:39.300:      Attribute 26 58 0000013701342001
*Mar 12 23:27:39.300:      Attribute 6 6 00000002
*Mar 12 23:27:39.300:      Attribute 7 6 00000001
*Mar 12 23:27:39.312: RADIUS: Received from id 181 10.200.20.245:1645,
Access-Accept, len 116
*Mar 12 23:27:39.312:      Attribute 7 6 00000001
*Mar 12 23:27:39.312:      Attribute 6 6 00000002
*Mar 12 23:27:39.312:      Attribute 25 32 502E05AE
*Mar 12 23:27:39.312:      Attribute 26 40 000001370C225042
*Mar 12 23:27:39.312:      Attribute 26 12 000001370A06204E
*Mar 12 23:27:39.312: AAA/AUTHEN (2410248116): status = PASS
*Mar 12 23:27:39.316: Vi1 AAA/AUTHOR/LCP: Authorize LCP
*Mar 12 23:27:39.316: Vi1 AAA/AUTHOR/LCP (2365724222):
Port='Virtual-Access1' list='' service=NET
*Mar 12 23:27:39.316: AAA/AUTHOR/LCP: Vi1 (2365724222) user='tac'
*Mar 12 23:27:39.316: Vi1 AAA/AUTHOR/LCP (2365724222): send AV service=ppp
*Mar 12 23:27:39.316: Vi1 AAA/AUTHOR/LCP (2365724222): send AV protocol=lcp
*Mar 12 23:27:39.316: Vi1 AAA/AUTHOR/LCP (2365724222): found list default
*Mar 12 23:27:39.316: Vi1 AAA/AUTHOR/LCP (2365724222): Method=radius
(radius)
*Mar 12 23:27:39.316: RADIUS: unrecognized Microsoft VSA type 10
*Mar 12 23:27:39.316: Vi1 AAA/AUTHOR (2365724222): Post authorization
status = PASS_REPL
*Mar 12 23:27:39.316: Vi1 AAA/AUTHOR/LCP: Processing AV service=ppp
*Mar 12 23:27:39.316: Vi1 AAA/AUTHOR/LCP: Processing AV
mschap_mppe_keys*1p1T11=1v1O1~11a1W11151\1V1M1#11Z1`1k1}111
*Mar 12 23:27:39.316: Vi1 MS-CHAP: O SUCCESS id 32 len 4
*Mar 12 23:27:39.316: Vi1 PPP: Phase is UP [0 sess, 0 load]
*Mar 12 23:27:39.316: Vi1 AAA/AUTHOR/FSM: (0): Can we start IPCP?
*Mar 12 23:27:39.320: Vi1 AAA/AUTHOR/FSM (1499311111):
Port='Virtual-Access1' list='' service=NET
*Mar 12 23:27:39.320: AAA/AUTHOR/FSM: Vi1 (1499311111) user='tac'
*Mar 12 23:27:39.320: Vi1 AAA/AUTHOR/FSM (1499311111): send AV service=ppp
*Mar 12 23:27:39.320: Vi1 AAA/AUTHOR/FSM (1499311111): send AV protocol=ip
*Mar 12 23:27:39.320: Vi1 AAA/AUTHOR/FSM (1499311111): found list default
*Mar 12 23:27:39.320: Vi1 AAA/AUTHOR/FSM (1499311111): Method=radius
(radius)
*Mar 12 23:27:39.320: RADIUS: unrecognized Microsoft VSA type 10
*Mar 12 23:27:39.320: Vi1 AAA/AUTHOR (1499311111): Post authorization
status = PASS_REPL
*Mar 12 23:27:39.320: Vi1 AAA/AUTHOR/FSM: We can start IPCP
*Mar 12 23:27:39.320: Vi1 IPCP: O CONFREQ [Closed] id 1 len 10
*Mar 12 23:27:39.320: Vi1 IPCP:    Address 172.16.10.100 (0x0306AC100A64)
```

```
*Mar 12 23:27:39.320: Vi1 AAA/AUTHOR/FSM: (0): Can we start CCP?
*Mar 12 23:27:39.320: Vi1 AAA/AUTHOR/FSM (327346364):
Port='Virtual-Access1' list='' service=NET
*Mar 12 23:27:39.324: AAA/AUTHOR/FSM: Vi1 (327346364) user='tac'
*Mar 12 23:27:39.324: Vi1 AAA/AUTHOR/FSM (327346364): send AV service=ppp
*Mar 12 23:27:39.324: Vi1 AAA/AUTHOR/FSM (327346364): send AV protocol=ccp
*Mar 12 23:27:39.324: Vi1 AAA/AUTHOR/FSM (327346364): found list default
*Mar 12 23:27:39.324: Vi1 AAA/AUTHOR/FSM (327346364): Method=radius
(radius)
*Mar 12 23:27:39.324: RADIUS: unrecognized Microsoft VSA type 10
*Mar 12 23:27:39.324: Vi1 AAA/AUTHOR (327346364): Post authorization status
= PASS_REPL
*Mar 12 23:27:39.324: Vi1 AAA/AUTHOR/FSM: We can start CCP
*Mar 12 23:27:39.324: Vi1 CCP: O CONFREQ [Closed] id 1 len 10
*Mar 12 23:27:39.324: Vi1 CCP:  MS-PPC supported bits 0x01000020
(0x120601000020)
*Mar 12 23:27:39.460: Vi1 CCP: I CONFREQ [REQsent] id 5 len 10
*Mar 12 23:27:39.460: Vi1 CCP:  MS-PPC supported bits 0x01000001
(0x120601000001)
*Mar 12 23:27:39.460: Vi1 AAA/AUTHOR/FSM: Check for unauthorized mandatory
AV's
*Mar 12 23:27:39.460: Vi1 AAA/AUTHOR/FSM: Processing AV service=ppp
*Mar 12 23:27:39.460: Vi1 AAA/AUTHOR/FSM: Processing AV
mschap_mppe_keys*1p1T11=1v1O1~11a1W11151\1V1M1#11Z1`1k1}111
*Mar 12 23:27:39.460: Vi1 AAA/AUTHOR/FSM: Succeeded
*Mar 12 23:27:39.464: Vi1 CCP: O CONFNAK [REQsent] id 5 len 10
*Mar 12 23:27:39.464: Vi1 CCP:  MS-PPC supported bits 0x01000020
(0x120601000020)
*Mar 12 23:27:39.472: Vi1 IPCP: I CONFREQ [REQsent] id 6 len 34
*Mar 12 23:27:39.472: Vi1 IPCP:    Address 0.0.0.0 (0x030600000000)
*Mar 12 23:27:39.472: Vi1 IPCP:    PrimaryDNS 0.0.0.0 (0x810600000000)
*Mar 12 23:27:39.472: Vi1 IPCP:    PrimaryWINS 0.0.0.0 (0x820600000000)
*Mar 12 23:27:39.472: Vi1 IPCP:    SecondaryDNS 0.0.0.0 (0x830600000000)
*Mar 12 23:27:39.472: Vi1 IPCP:    SecondaryWINS 0.0.0.0 (0x840600000000)
*Mar 12 23:27:39.472: Vi1 AAA/AUTHOR/IPCP: Start.  Her address 0.0.0.0, we
want 0.0.0.0
*Mar 12 23:27:39.472: Vi1 AAA/AUTHOR/IPCP: Processing AV service=ppp
*Mar 12 23:27:39.472: Vi1 AAA/AUTHOR/IPCP: Processing AV
mschap_mppe_keys*1p1T11=1v1O1~11a1W11151\1V1M1#11Z1`1k1}111
*Mar 12 23:27:39.472: Vi1 AAA/AUTHOR/IPCP: Authorization succeeded
*Mar 12 23:27:39.472: Vi1 AAA/AUTHOR/IPCP: Done.  Her address 0.0.0.0, we
want 0.0.0.0
*Mar 12 23:27:39.472: Vi1 IPCP: Pool returned 172.16.10.1
*Mar 12 23:27:39.476: Vi1 IPCP: O CONFREJ [REQsent] id 6 len 28
*Mar 12 23:27:39.476: Vi1 IPCP:    PrimaryDNS 0.0.0.0 (0x810600000000)
*Mar 12 23:27:39.476: Vi1 IPCP:    PrimaryWINS 0.0.0.0 (0x820600000000)
*Mar 12 23:27:39.476: Vi1 IPCP:    SecondaryDNS 0.0.0.0 (0x830600000000)
*Mar 12 23:27:39.476: Vi1 IPCP:    SecondaryWINS 0.0.0.0 (0x840600000000)
*Mar 12 23:27:39.480: Vi1 IPCP: I CONFACK [REQsent] id 1 len 10
*Mar 12 23:27:39.484: Vi1 IPCP:    Address 172.16.10.100 (0x0306AC100A64)
*Mar 12 23:27:39.488: Vi1 CCP: I CONFACK [REQsent] id 1 len 10
*Mar 12 23:27:39.488: Vi1 CCP:  MS-PPC supported bits 0x01000020
(0x120601000020)
*Mar 12 23:27:39.596: Vi1 CCP: I CONFREQ [ACKrcvd] id 7 len 10
*Mar 12 23:27:39.596: Vi1 CCP:  MS-PPC supported bits 0x01000020
(0x120601000020)
*Mar 12 23:27:39.596: Vi1 AAA/AUTHOR/FSM: Check for unauthorized mandatory
AV's
*Mar 12 23:27:39.596: Vi1 AAA/AUTHOR/FSM: Processing AV service=ppp
*Mar 12 23:27:39.596: Vi1 AAA/AUTHOR/FSM: Processing AV
mschap_mppe_keys*1p1T11=1v1O1~11a1W11151\1V1M1#11Z1`1k1}111
*Mar 12 23:27:39.596: Vi1 AAA/AUTHOR/FSM: Succeeded
*Mar 12 23:27:39.596: Vi1 CCP: O CONFACK [ACKrcvd] id 7 len 10
*Mar 12 23:27:39.596: Vi1 CCP:  MS-PPC supported bits 0x01000020
```

```
(0x120601000020)
*Mar 12 23:27:39.596: Vi1 CCP: State is Open
*Mar 12 23:27:39.600: Vi1 MPPE: Generate keys using RADIUS data
*Mar 12 23:27:39.600: Vi1 MPPE: Initialize keys
*Mar 12 23:27:39.600: Vi1 MPPE: [40 bit encryption]  [stateless mode]
*Mar 12 23:27:39.620: Vi1 IPCP: I CONFREQ [ACKrcvd] id 8 len 10
*Mar 12 23:27:39.620: Vi1 IPCP:    Address 0.0.0.0 (0x030600000000)
*Mar 12 23:27:39.620: Vi1 AAA/AUTHOR/IPCP: Start.  Her address 0.0.0.0, we
want 172.16.10.1
*Mar 12 23:27:39.620: Vi1 AAA/AUTHOR/IPCP: Processing AV service=ppp
*Mar 12 23:27:39.620: Vi1 AAA/AUTHOR/IPCP: Processing AV
mschap_mppe_keys*1p1T11=1v1O1~11a1W11151\1V1M1#11Z1`1k1}111
*Mar 12 23:27:39.620: Vi1 AAA/AUTHOR/IPCP: Authorization succeeded
*Mar 12 23:27:39.620: Vi1 AAA/AUTHOR/IPCP: Done.  Her address 0.0.0.0, we
want 172.16.10.1
*Mar 12 23:27:39.624: Vi1 IPCP: O CONFNAK [ACKrcvd] id 8 len 10
*Mar 12 23:27:39.624: Vi1 IPCP:    Address 172.16.10.1 (0x0306AC100A01)
*Mar 12 23:27:39.756: Vi1 IPCP: I CONFREQ [ACKrcvd] id 9 len 10
*Mar 12 23:27:39.756: Vi1 IPCP:    Address 172.16.10.1 (0x0306AC100A01)
*Mar 12 23:27:39.756: Vi1 AAA/AUTHOR/IPCP: Start.  Her address 172.16.10.1,
we want 172.16.10.1
*Mar 12 23:27:39.756: Vi1 AAA/AUTHOR/IPCP (2840659706):
Port='Virtual-Access1' list='' service=NET
*Mar 12 23:27:39.756: AAA/AUTHOR/IPCP: Vi1 (2840659706) user='tac'
*Mar 12 23:27:39.756: Vi1 AAA/AUTHOR/IPCP (2840659706): send AV service=ppp
*Mar 12 23:27:39.756: Vi1 AAA/AUTHOR/IPCP (2840659706): send AV protocol=ip
*Mar 12 23:27:39.756: Vi1 AAA/AUTHOR/IPCP (2840659706): send AV
addr*172.16.10.1
*Mar 12 23:27:39.756: Vi1 AAA/AUTHOR/IPCP (2840659706): found list
default
*Mar 12 23:27:39.756: Vi1 AAA/AUTHOR/IPCP (2840659706): Method=radius
(radius)
*Mar 12 23:27:39.756: RADIUS: unrecognized Microsoft VSA type 10
*Mar 12 23:27:39.756: Vi1 AAA/AUTHOR (2840659706): Post authorization
status = PASS_REPL
*Mar 12 23:27:39.756: Vi1 AAA/AUTHOR/IPCP: Reject 172.16.10.1, using
172.16.10.1
*Mar 12 23:27:39.760: Vi1 AAA/AUTHOR/IPCP: Processing AV service=ppp
*Mar 12 23:27:39.760: Vi1 AAA/AUTHOR/IPCP: Processing AV
mschap_mppe_keys*1p1T11=1v1O1~11a1W11151\1V1M1#11Z1`1k1}111
*Mar 12 23:27:39.760: Vi1 AAA/AUTHOR/IPCP: Processing AV addr*172.16.10.1
*Mar 12 23:27:39.760: Vi1 AAA/AUTHOR/IPCP: Authorization succeeded
*Mar 12 23:27:39.760: Vi1 AAA/AUTHOR/IPCP: Done.  Her address 172.16.10.1,
we want 172.16.10.1
*Mar 12 23:27:39.760: Vi1 IPCP: O CONFACK [ACKrcvd] id 9 len 10
*Mar 12 23:27:39.760: Vi1 IPCP:    Address 172.16.10.1 (0x0306AC100A01)
*Mar 12 23:27:39.760: Vi1 IPCP: State is Open
*Mar 12 23:27:39.764: Vi1 IPCP: Install route to 172.16.10.1
*Mar 12 23:27:40.316: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Virtual-Access1, changed state to up
*Mar 12 23:27:46.628: Vi1 LCP: I ECHOREP [Open] id 1 len 12 magic
0x4B4817ED
*Mar 12 23:27:46.628: Vi1 LCP: Received id 1, sent id 1, line up
*Mar 12 23:27:56.636: Vi1 LCP: I ECHOREP [Open] id 2 len 12 magic
0x4B4817ED
*Mar 12 23:27:56.636: Vi1 LCP: Received id 2, sent id 2, line upcaller ip
Line     UserIP AddressLocal NumberRemote Number<->
Vi1     tac172.16.10.1--in

angela#show ppp mppe virtual-Access 1 Interface Virtual-Access1 (current connection) Software
encryption, 40 bit encryption, Stateless mode packets encrypted = 0 packets decrypted = 16 sent
CCP resets = 0 receive CCP resets = 0 next tx coherency = 0 next rx coherency = 16 tx key
changes = 0 rx key changes = 16 rx pkt dropped = 0 rx out of order pkt= 0 rx missed packets = 0
*Mar 12 23:28:06.604: Vi1 LCP: I ECHOREP [Open] id 3 len 12 magic 0x4B4817ED *Mar 12
```

```
23:28:06.604: Vi1 LCP: Received id 3, sent id 3, line up angela#ping 172.16.10.1 Type escape
sequence to abort. Sending 5, 100-byte ICMP Echos to 172.16.10.1, timeout is 2 seconds: !!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 188/196/204 ms angela#show ppp mppe
virtual-Access 1 Interface Virtual-Access1 (current connection) Software encryption, 40 bit
encryption, Stateless mode packets encrypted = 5 packets decrypted = 22 sent CCP resets = 0
receive CCP resets = 0 next tx coherency = 5 next rx coherency = 22 tx key changes = 5 rx key
changes = 22 rx pkt dropped = 0 rx out of order pkt= 0 rx missed packets = 0 angela#ping
172.16.10.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 172.16.10.1,
timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max =
184/200/232 ms angela#ping 172.16.10.1sh ppp mppe virtual-Access 1 Interface Virtual-Access1
(current connection) Software encryption, 40 bit encryption, Stateless mode packets encrypted =
10 packets decrypted = 28 sent CCP resets = 0 receive CCP resets = 0 next tx coherency = 10 next
rx coherency = 28 tx key changes = 10 rx key changes = 28 rx pkt dropped = 0 rx out of order
pkt= 0 rx missed packets = 0 angela#
```

команды "debug" и "show"

Прежде чем выполнять какие-либо команды отладки , ознакомьтесь с документом "Важные сведения о командах отладки".

Средство Output Interpreter (OIT) (только для зарегистрированных клиентов) поддерживает определенные команды show. **Посредством OIT можно анализировать выходные данные команд show.**

Если вещи не работают, минимальная **отладка** включает эти команды:

- **debug aaa authentication - Вывод сведений об аутентификации AAA/TACACS+.**
- **debug aaa authorization — отображаются данные авторизации AAA/TACACS+.**
- **"debug ppp negotiation" – отображаются PPP-пакеты, передаваемые при запуске PPP с согласованием параметров.**
- **debug ppp authenticaion** — Отображает сообщения протокола аутентификации, который включает Протокол аутентификации проблемы (CHAP) обмены Протокола аутентификации пароля (PAP) и обмены пакетами.
- **debug radius– выводит подробные данные об отладке сервера RADIUS.**

Если аутентификация работает, но существуют проблемы с шифрованием Средств шифрования Microsoft точка-точка (MPPE), используют одну из этих команд:

- **debug ppp mppe packet - Отображает весь входящий и исходящий трафик MPPE.**
- **debug ppp mppe event – отображаются основные события MPPE.**
- **debug ppp mppe detailed - отображает подробные сведения об MPPE.**
- **debug vpdn l2x-packet** — Отображают сообщения о заголовках протокола Level 2 Forwarding (L2F) и статусе.
- **debug vpdn events –отображает сообщения о событиях, являющихся частью нормального туннельного открытия или закрытия.**
- **debug vpdn errors – отображает ошибки, которые мешают установке туннеля, или ошибки, которые вызывают закрытие установленного туннеля.**
- **команда debug vpdn packets отображает замененные пакеты данных для всех протоколов.** Этот параметр может вызвать существенное увеличение числа отладочных сообщений, поэтому его следует использовать только в конфигурации отладки с одним активным сеансом.
- **show vpdn** об активном туннеле Протокола 12f и идентификаторах сообщения в Виртуальной частной коммутируемой сети (VPDN).

Можно ли также использовать **show vpdn?** команда для наблюдения других специфичных для vpdn **команд показа**.

Раздельное туннелирование

Предположите, что маршрутизатор/шлюз является маршрутизатором интернет-провайдера (ISP). Когда туннель Протокола PPTP подходит на ПК, маршрут PPTP установлен с более высокой метрикой, чем предыдущий по умолчанию, таким образом, мы теряем интернет-соединение. Для исправления этого модифицируйте Организацию маршрутизации Microsoft, чтобы удалить по умолчанию и повторно установить маршрут по умолчанию (это требуемое знание IP-адреса, клиенту PPTP назначили; для текущего примера это 172.16.10.1):

```
route delete 0.0.0.0
route add 0.0.0.0 mask 0.0.0.0 192.168.1.47 metric 1
route add 172.16.10.1 mask 255.255.255.0 192.168.1.47 metric 1
```

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

Проблема 1: IPSec не отключен

Признак

Пользователь ПК видит это сообщение:

```
Error connecting to L2TP:
Error 781: The encryption attempt failed because
no valid certificate was found.
```

Решение

Перейдите к разделу **Свойств** окна **Virtual Private Connection** и щелкните **по Вкладке Безопасность**. Отключите опцию **Require Data Encryption**.

Проблема 2: Ошибка 789

Признак

Попытка подключения L2TP отказывает, потому что уровень безопасности встретился с ошибкой обработки во время начальных согласований с удаленным компьютером.

Microsoft Remote Access и Сервисы агента политики создают политику, которая используется для трафика L2TP, потому что L2TP не предоставляет шифрование. Это применимо для Microsoft Windows 2000 Advanced Server, Сервера Microsoft Windows 2000 и Microsoft Windows 2000 Professional.

Решение

Используйте Редактор реестра (Regedt32.exe) для добавления новой записи реестра для отключения IPSec. См. документацию Microsoft или Раздел справки Microsoft для

Regedt32.exe.

Необходимо добавить Значение ключа ProhibitIPSec в реестре к каждому основанному на Windows 2000 оконечному компьютеру L2TP или IP - безопасного соединения для предотвращения автоматического фильтра для L2TP и Трафика IPSec от того, чтобы быть созданным. Когда Значение ключа ProhibitIPSec в реестре установлено в одно, ваш основанный на Windows 2000 компьютер не создает автоматический фильтр, который использует аутентификацию CA. Вместо этого это проверяет для локальной переменной или Активной политики IPSec каталога. Для добавления Значения ключа ProhibitIPSec в реестре к основанному на Windows 2000 компьютеру используйте Regedt32.exe для определения местоположения этого ключа в реестре:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Rasman\Parameters
```

Добавьте это значение регистрации к следующему ключу:

```
Value Name: ProhibitIpSec
Data Type: REG_DWORD
Value: 1
```

Примечание: Необходимо перезапустить основанный на Windows 2000 компьютер для изменений для вступления в силу.

Проблема 3: Проблема с аутентификацией туннелирования

Пользователи аутентифицируются в NAS или LNS, прежде чем будет установлен туннель. Это не требуется для инициированных клиентом туннелей как L2TP от клиента Microsoft.

Пользователь ПК видит это сообщение:

```
Connecting to 10.200.20.2..
Error 651: The modem(or other connecting device) has reported an error.
Router debugs:

*Mar 12 23:03:47.124: L2TP: I SCCRQ from  RSHANMUG-W2K1.cisco.com tnl 1
*Mar 12 23:03:47.124: Tnl 30107 L2TP: New tunnel created for remote
RSHANMUG-W2K1.cisco.com, address 192.168.1.56
*Mar 12 23:03:47.124: Tnl 30107 L2TP: O SCCRP  to  RSHANMUG-W2K1.cisco.com
tnlid 1
*Mar 12 23:03:47.124: Tnl 30107 L2TP: Tunnel state change from idle to
wait-ctl-reply
*Mar 12 23:03:47.308: Tnl 30107 L2TP: I SCCCN from  RSHANMUG-W2K1.cisco.com
tnl 1
*Mar 12 23:03:47.308: Tnl 30107 L2TP: Got a Challenge Response in SCCCN
from  RSHANMUG-W2K1.cisco.com
*Mar 12 23:03:47.308: AAA: parse name= idb type=-1 tty=-1
*Mar 12 23:03:47.308: AAA/MEMORY: create_user (0x6273D528) user='angela'
ruser='' port='' rem_addr='' authen_type=CHAP service=PPP priv=1
*Mar 12 23:03:47.308: AAA/AUTHEN/START (4077585132): port='' list='default'
action=SENDAUTH service=PPP
*Mar 12 23:03:47.308: AAA/AUTHEN/START (4077585132): found list default
*Mar 12 23:03:47.308: AAA/AUTHEN/START (4077585132): Method=radius (radius)
*Mar 12 23:03:47.308: AAA/AUTHEN/SENDAUTH (4077585132): no authenstruct
hwidb
*Mar 12 23:03:47.308: AAA/AUTHEN/SENDAUTH (4077585132): Failed sendauthen
for angela
*Mar 12 23:03:47.308: AAA/AUTHEN (4077585132): status = FAIL
*Mar 12 23:03:47.308: AAA/AUTHEN/START (4077585132): Method=LOCAL
*Mar 12 23:03:47.308: AAA/AUTHEN (4077585132): SENDAUTH no password for
angela
```

```
*Mar 12 23:03:47.308: AAA/AUTHEN (4077585132): status = ERROR
*Mar 12 23:03:47.308: AAA/AUTHEN/START (4077585132): no methods left to try
*Mar 12 23:03:47.308: AAA/AUTHEN (4077585132): status = ERROR
*Mar 12 23:03:47.308: AAA/AUTHEN/START (4077585132): failed to authenticate
*Mar 12 23:03:47.308: VPDN: authentication failed, couldn't find user
information for angela
*Mar 12 23:03:47.308: AAA/MEMORY: free_user (0x6273D528) user='angela'
ruser='' port='' rem_addr='' authen_type=CHAP service=PPP priv=1
*Mar 12 23:03:47.312: Tnl 30107 L2TP: O StopCCN  to
RSHANMUG-W2K1.cisco.com tnlid 1
*Mar 12 23:03:47.312: Tnl 30107 L2TP: Tunnel state change from
wait-ctl-reply to shutting-down
*Mar 12 23:03:47.320: Tnl 30107 L2TP: Shutdown tunnel
*Mar 12 23:03:47.320: Tnl 30107 L2TP: Tunnel state change from
shutting-down to idle
*Mar 12 23:03:47.324: L2TP: Could not find tunnel for tnl 30107, discarding
ICRQ ns 3 nr 1
*Mar 12 23:03:47.448: L2TP: Could not find tunnel for tnl 30107, discarding
ICRQ ns 3 nr 2
```

Дополнительные сведения

- Уровень два протокола туннелирования (L2TP)
- Пример конфигурации L2TP по IPsec между Windows 2000 и концентратором VPN 3000 с использованием цифровых сертификатов
- Настройка L2TP по IPSec между межсетевым экраном PIX и Windows 2000 PC с помощью сертификатов
- Протокол туннелирования 2-го уровня
- Настройка виртуальных частных сетей (VPN)
- Настройка аутентификации по протоколу L2TP с использованием RADIUS
- Cisco Systems – техническая поддержка и документация