Настройка VPDN отдельных пользователей без информации о домене или DNIS

Содержание

Введение
Предварительные условия
Требования
Используемые компоненты
Условные обозначения
Общие сведения
Настройка
Схема сети
Конфигурации
Конфигурация сервера RADIUS
Проверка
Пример выходных данных команды show
Устранение неполадок
Команды для устранения неполадок
Пример результата отладки
Дополнительные сведения

Введение

Этот документ предоставляет пример конфигурации для VPDN для каждого пользователя без домена или данных DNIS.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

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

- Релиз 12.1 Программного обеспечения Cisco IOS (4) или позже.
- Программное обеспечение Cisco IOS версии 12.1(4)T или позже.

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 в документах см. Cisco Technical Tips Conventions.

Общие сведения

В сценариях виртуальной частной коммутируемой сети (VPDN) сервер доступа к сети (NAS) (Концентратор доступа L2TP или LAC) устанавливает туннель VPDN к Домашнему шлюзу (LNS) на основе информации по данному пользователю. Этим туннелем VPDN может быть Level 2 Forwarding (L2F) или протокол туннелирования на уровне 2 (L2TP). Чтобы определить, должен ли пользователь использовать туннель VPDN, проверьте:

- Включено ли доменное имя как часть имени пользователя. Например, с именем пользователя tunnelme@cisco.com, NAS вперед этот пользователь в туннель для cisco.com.
- Dialed Number Information Service (DNIS). Это - переадресация вызовов на основе вызываемого номера. Это означает, что NAS может перевести все вызовы с определенным вызываемым номером в соответствующий туннель. Например, если входящий вызов имеет вызываемый номер 5551111, вызов может быть переведен в туннель VPDN, в то время как не переведен вызов к 5552222. Эта функция требует, чтобы Сеть telco отправила информацию о вызываемом номере.

Для получения дополнительной информации о конфигурации VPDN, посмотрите VPDN Понимания.

В некоторых ситуациях можно потребовать, чтобы туннель VPDN был intiated на основе на имя пользователя, с или без потребности в domain-name вообще. В то время как другие пользователи могут быть завершены локально на NAS, например **пользователь ciscouser** может быть туннелирован к **cisco.com**.

Примечание: Это имя пользователя не включает информацию домена как в предыдущем примере.

Функция настройки на базе отдельных пользователей VPDN передает все структурированное имя пользователя к аутентификации, авторизации и учету (AAA) первоначально, маршрутизатор связывается с AAA-сервером. Это позволяет программному обеспечению Cisco IOS настроить атрибуты туннеля для отдельных пользователей, которые используют общее доменное имя или DNIS.

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

Единственные команды VPDN, необходимые на NAS (LAC) для поддержки VPDN для каждого пользователя, являются **vpdn enable** команд глобальной кофигурации и **vpdn authen-before-forward**. **Команда vpdn authen-before-forward** дает NAS команду (LAC) аутентифицировать завершенное имя пользователя, прежде чем это сделает решение по перенаправлению. Туннель VPDN тогда установлен, на основе информации, возвращенной AAA-сервером для этого отдельного пользователя; если никакие сведения о VPDN не возвращены из AAA-сервера, пользователь завершен локально. Конфигурация в этом разделе показывает команды, требуемые поддерживать туннели без информации домена в имени пользователя.

Примечание: Эта конфигурация не является полной. Только соответствующая VPDN, интерфейс и команды AAA включены.

Примечание: Это выходит за рамки этого документа для обсуждения каждого возможного протокола туннелирования и протокола AAA (проверка подлинности, авторизация и учет). Следовательно, эта конфигурация внедряет туннель L2TP с сервером AAA RADIUS. Адаптируйте принципы и конфигурацию, обсужденную здесь для настройки других типов туннеля или протоколов AAA (проверка подлинности, авторизация и учет).

В данном документе используется следующая конфигурация:

- VPDN NAS (LAC)

VPDN NAS (LAC)

```
aaa new-model
aaa authentication ppp default group radius
!--- Use RADIUS authentication for PPP authentication.
aaa authorization network default group radius !---
Obtain authorization information from the Radius server.
!--- This command is required for the AAA server to
provide VPDN attributes. ! vpdn enable !--- VPDN is
enabled. vpdn authen-before-forward !--- Authenticate
the complete username before making a forwarding
decision. !--- The LAC sends the username to the AAA
server for VPDN attributes. ! controller E1 0 pri-group
timeslots 1-31 ! interface Serial0:15 dialer rotary-
group 1 !--- D-channel for E1 0 is a member of the
dialer rotary group 1. ! interface Dialer1 !--- Logical
interface for dialer rotary group 1. ip unnumbered
Ethernet0 encapsulation ppp dialer in-band dialer-group
1 ppp authentication chap pap callin ! radius-server
host 172.22.53.201 !--- The IP address of the RADIUS
server host. !--- This AAA server will supply the
NAS(LAC) with the VPDN attributes for the user. radius-
server key cisco !--- The RADIUS server key.
```

Конфигурация сервера RADIUS

Вот некоторые пользовательские конфигурации на Cisco Secure для Unix (CSU) сервер RADIUS:

1. Пользователь, который должен быть завершен локально на NAS: `user1 Password = "cisco"`
   `Service-Type = Framed-User`
2. Пользователь, для которого должен быть установлен сеанс VPDN:`user2`
   ```
   Password = "cisco"
   Service-Type = Framed-User,
   Cisco-AVPair = "vpdn:ip-addresses=172.22.53.141",
   Cisco-AVPair = "vpdn:l2tp-tunnel-password=cisco",
   Cisco-AVPair = "vpdn:tunnel-type=l2tp"
   ```

NAS (LAC) использует атрибуты, заданные с VPDN Cisco-AVPair к intiate туннель VPDN к Домашнему шлюзу. Гарантируйте настройку Домашнего шлюза для принятия туннелей VPDN от NAS.

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 caller user** — показывает параметры для индивидуального пользователя, такие как используемая линия TTY, асинхронный интерфейс (полка, слот или порт), номер канала DS0, номер модема, назначенный IP-адрес, PPP и параметры пакета PPP, и так далее. **Если данная команда не поддерживается в вашей версии программного обеспечения Cisco IOS, используйте команду "show user command".**
- **show vpdn** об активном L2F и протоколах туннеля L2TP и идентификаторах сообщения в VPDN.

Пример выходных данных команды show

Когда подключения вызова используют команду *show caller user username*, а также **команду show vpdn**, чтобы проверить, что вызов успешен. Ниже представлен результат выборки:

```
maui-nas-02#show caller user vpdn_authen User: vpdn_authen, line tty 12, service Async Active
time 00:09:01, Idle time 00:00:05 Timeouts: Absolute Idle Idle Session Exec Limits: - - 00:10:00
Disconnect in: - - - TTY: Line 12, running PPP on As12 DS0: (slot/unit/channel)=0/0/5 Line: Baud
rate (TX/RX) is 115200/115200, no parity, 1 stopbits, 8 databits Status: Ready, Active, No Exit
Banner, Async Interface Active HW PPP Support Active Capabilities: Hardware Flowcontrol In,
Hardware Flowcontrol Out Modem Callout, Modem RI is CD, Line is permanent async interface,
Integrated Modem Modem State: Ready User: vpdn_authen, line As12, service PPP Active time
00:08:58, Idle time 00:00:05 Timeouts: Absolute Idle Limits: - - Disconnect in: - - PPP: LCP
Open, CHAP (<- AAA) IP: Local 172.22.53.140 VPDN: NAS , MID 4, MID Unknown HGW , NAS CLID 0, HGW
CLID 0, tunnel open !--- The VPDN tunnel is open. Counts: 85 packets input, 2642 bytes, 0 no
buffer 0 input errors, 0 CRC, 0 frame, 0 overrun 71 packets output, 1577 bytes, 0 underruns 0
output errors, 0 collisions, 0 interface resets maui-nas-02#show vpdn L2TP Tunnel and Session
Information Total tunnels 1 sessions 1 LocID RemID Remote Name State Remote Address Port
Sessions 6318 3 HGW est 172.22.53.141 1701 1 LocID RemID TunID Intf Username State Last Chg
Fastswitch 4 3 6318 As12 vpdn_authen est 00:09:33 enabled !--- The tunnel for user vpdn_authen
is in established state. %No active L2F tunnels %No active PPTP tunnels %No active PPPoE tunnel
```

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

Команды для устранения неполадок

Примечание: Прежде чем вызывать команды debug, обратитесь к разделу Важные сведения о командах отладки.

- **debug ppp authenticaion** — отображает сообщения протокола аутентификации PPP и включает обмены пакетами Протокола аутентификации по квитированию вызова (CHAP) и обмены Протокола аутентификации пароля (PAP).
- **debug aaa authentication** — отображает информацию на аутентификации AAA/RADIUS.
- **debug aaa authorization** — отображает информацию на авторизации AAA/RADIUS.
- **debug radius– выводит подробные данные об отладке сервера RADIUS.** Используйте Средство интерпретации выходных данных (только зарегистрированные клиенты) для декодирования сообщений debug radius. Например, обратитесь к разделу Примера отладочных выходных данных. Используйте информацию от **debug radius** для определения, о каких атрибутах выполняют согласование.
- **debug tacacs** — подробная отладочная информация показов связалась с TACACS +.
- **debug vpdn event** — отображает ошибки L2x и события, которые являются частью обычного создания туннеля или завершением для VPDN.
- **debug vpdn error** — отображает ошибки протокола VPDN.
- **debug vpdn l2x-event** — отображает подробные ошибки L2x и события, которые являются частью обычного создания туннеля или завершением для VPDN.
- **debug vpdn l2x-error** — отображает ошибки протокола L2x VPDN.

Пример результата отладки

Вот **выходные данные отладки** для успешного вызова. В данном примере обратите внимание, что NAS получает атрибуты для туннеля VPDN от сервера RADIUS.

```
maui-nas-02#show debug General OS: AAA Authentication debugging is on AAA Authorization
debugging is on PPP: PPP authentication debugging is on VPN: L2X protocol events debugging is on
L2X protocol errors debugging is on VPDN events debugging is on VPDN errors debugging is
onRadius protocol debugging is on maui-nas-02# *Jan 21 19:07:26.752: %ISDN-6-CONNECT: Interface
Serial0:5 is now connected to N/A N/A !--- Incoming call. *Jan 21 19:07:55.352: %LINK-3-UPDOWN:
Interface Async12, changed state to up *Jan 21 19:07:55.352: As12 PPP: Treating connection as a
dedicated line *Jan 21 19:07:55.352: As12 AAA/AUTHOR/FSM: (0): LCP succeeds trivially *Jan 21
19:07:55.604: As12 CHAP: O CHALLENGE id 1 len 32 from "maui-nas-02" *Jan 21 19:07:55.732: As12
CHAP: I RESPONSE id 1 len 32 from "vpdn_authen" !--- Incoming CHAP response from user
vpdn_authen. *Jan 21 19:07:55.732: AAA: parse name=Async12 idb type=10 tty=12 *Jan 21
19:07:55.732: AAA: name=Async12 flags=0x11 type=4 shelf=0 slot=0 adapter=0 port=12 channel=0
*Jan 21 19:07:55.732: AAA: parse name=Serial0:5 idb type=12 tty=-1 *Jan 21 19:07:55.732: AAA:
name=Serial0:5 flags=0x51 type=1 shelf=0 slot=0 adapter=0 port=0 channel=5 *Jan 21 19:07:55.732:
AAA/ACCT/DS0: channel=5, ds1=0, t3=0, slot=0, ds0=5 *Jan 21 19:07:55.732: AAA/MEMORY:
create_user (0x628C79EC) user='vpdn_authen' ruser='' port='Async12' rem_addr='async/81560'
authen_type=CHAP service=PPP priv=1 *Jan 21 19:07:55.732: AAA/AUTHEN/START (4048817807):
port='Async12' list='' action=LOGIN service=PPP *Jan 21 19:07:55.732: AAA/AUTHEN/START
(4048817807): using "default" list *Jan 21 19:07:55.732: AAA/AUTHEN/START (4048817807):
Method=radius (radius) *Jan 21 19:07:55.736: RADIUS: ustruct sharecount=1 *Jan 21 19:07:55.736:
RADIUS: Initial Transmit Async12 id 6 172.22.53.201:1645, Access-Request, len 89 *Jan 21
19:07:55.736: Attribute 4 6 AC16358C *Jan 21 19:07:55.736: Attribute 5 6 0000000C *Jan 21
```

19:07:55.736: Attribute 61 6 00000000 *Jan 21 19:07:55.736: Attribute 1 13 7670646E *Jan 21 19:07:55.736: Attribute 30 7 38313536 *Jan 21 19:07:55.736: Attribute 3 19 014CF9D6 *Jan 21 19:07:55.736: Attribute 6 6 00000002 *Jan 21 19:07:55.736: Attribute 7 6 00000001 *Jan 21 19:07:55.740: RADIUS: Received from id 6 172.22.53.201:1645, Access-Accept, len 136 *Jan 21 19:07:55.740: Attribute 6 6 00000002 *Jan 21 19:07:55.740: Attribute 26 40 0000000901227670 *Jan 21 19:07:55.740: Attribute 26 40 0000000901227670 *Jan 21 19:07:55.740: Attribute 26 30 0000000901187670

Пары значений атрибутов (AVP), необходимые для туннеля VPDN, оттолкнуты от сервера RADIUS. Однако **debug radius** производит закодированные выходные данные, указывающие на AVP и их значения. Можно вставить выходные данные, показанные **полужирным** шрифт выше в Средство интерпретации выходных данных (только зарегистрированные клиенты). Следующий результат полужирным является декодируемыми выходными данными, полученными из программного средства:

Access-Request 172.22.53.201:1645 id 6 Attribute Type 4: NAS-IP-Address is 172.22.53.140 Attribute Type 5: NAS-Port is 12 Attribute Type 61: NAS-Port-Type is Asynchronous Attribute Type 1: User-Name is vpdn Attribute Type 30: Called-Station-ID(DNIS) is 8156 Attribute Type 3: CHAP-Password is (encoded) Attribute Type 6: Service-Type is Framed Attribute Type 7: Framed-Protocol is PPP Access-Accept 172.22.53.201:1645 id 6 Attribute Type 6: Service-Type is Framed Attribute Type 26: Vendor is Cisco Attribute Type 26: Vendor is Cisco Attribute Type 26: Vendor is Cisco
*Jan 21 19:07:55.740: AAA/AUTHEN (4048817807): status = PASS ... ... *Jan 21 19:07:55.744: RADIUS: cisco AVPair "vpdn:ip-addresses=172.22.53.141" *Jan 21 19:07:55.744: RADIUS: cisco AVPair "vpdn:l2tp-tunnel-password=cisco" *Jan 21 19:07:55.744: RADIUS: cisco AVPair "vpdn:tunnel-type=l2tp" *Jan 21 19:07:55.744: AAA/AUTHOR (733932081): Post authorization status = PASS_REPL *Jan 21 19:07:55.744: AAA/AUTHOR/VPDN: Processing AV service=ppp *Jan 21 19:07:55.744: AAA/AUTHOR/VPDN: Processing AV ip-addresses=172.22.53.141 *Jan 21 19:07:55.744: AAA/AUTHOR/VPDN: Processing AV l2tp-tunnel-password=cisco *Jan 21 19:07:55.744: AAA/AUTHOR/VPDN: Processing AV tunnel-type=l2tp *!--- Tunnel information. !--- The VPDN Tunnel will now be established and the call will be authenticated. !--- Since the debug information is similar to that for a normal VPDN call, !--- the VPDN tunnel establishment debug output is omitted.*

Дополнительные сведения

- Общие сведения о VPDN (виртуальная частная коммутируемая сеть)
- Виртуальные частные коммутируемые сети Настройки
- Инструкция настраивает проверку подлинности протокола туннелирования уровня 2 с RADIUS
- Настройка протокола туннелирования второго уровня, используя TACACS+
- Страницы поддержки технологии доступа
- Техническая поддержка - Cisco Systems