Настройка Cisco 827 для PPPoE с перегрузкой NAT VPN IPSec

Содержание

Введение

Маршрутизатор Cisco 827 обычно является DSL Customer Premises Equipment (CPE). В этом примере конфигурации Cisco 827 настроен для Протокола PPPoE и используется в качестве узла в Туннеле IPSec между локальными сетями с Маршрутизатором Cisco 3600. Cisco 827 также делает Технологию NAT, перегружающуюся для обеспечения Интернет-соединения для его внутренней сети.

Перед началом работы

Условные обозначения

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

Предварительные условия

При рассмотрении этой конфигурации помните следующее.

- Удостоверьтесь, что PPPoE работает прежде, чем добавить конфигурацию для IPSEC VPN у Cisco 827. Для отладки PPPoE-клиента на Cisco 827 необходимо рассмотреть стек протоколов. Устранение неполадок производится в следующем порядке.Физический уровень DSLУровень ATMУровень EthernetУровень PPP
- В этом примере конфигурации у Cisco 827 есть статический IP - адрес. Если у вашего

Cisco 827 есть динамический IP - адрес, посмотрите Динамический-в-статичный канал IPSec маршрутизатор-маршрутизатор с поддержкой NAT Настройки в дополнение к этому документу.

Используемые компоненты

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

- Cisco 827 12.1 (5) YB4
- Cisco 3600 12.1 (5) T8
- Cisco 6400 12.1 (1) DC1

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.

Настройка

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

Схема сети

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

Конфигурации

В данном документе используются следующие конфигурации.

- Cisco 827 (CPE)
- Маршрутизатор light

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

Cisco 827 (CPE)

```
version 12.1
no service single-slot-reload-enable
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 827
!
logging rate-limit console 10 except errors
!
ip subnet-zero
no ip finger
!
no ip dhcp-client network-discovery
```

```
vpdn enable

no vpdn logging
!
vpdn-group pppoe
 request-dialin
  protocol pppoe
!
!
!
crypto isakmp policy 20
 encr 3des
 authentication pre-share
 group 2
crypto isakmp key sharedkey address 30.30.30.30
!
!
crypto ipsec transform-set dsltest esp-3des esp-md5-hmac
!
crypto map test 10 ipsec-isakmp
 set peer 30.30.30.30
 set transform-set dsltest
 match address 101
!
interface Ethernet0
 ip address 192.168.100.100 255.255.255.0
 ip nat inside
!
interface ATM0
 no ip address
 no atm ilmi-keepalive
 bundle-enable
 dsl operating-mode ansi-dmt
!
interface ATM0.1 point-to-point
 pvc 0/33
!--- This is usually provided by the ISP. protocol pppoe
pppoe-client dial-pool-number 1 ! ! interface Dialer1 ip
address 20.20.20.20 255.255.255.0 !--- This is provided
by the ISP. !--- Another variation is ip address
negotiated. ip mtu 1492 ip Nat outside encapsulation ppp
no ip route-cache no ip mroute-cache dialer pool 1 ppp
authentication chap callin ppp chap hostname testuser
ppp chap password 7 00071A1507545A545C crypto map test !
ip classless ip route 0.0.0.0 0.0.0.0 Dialer1 no ip http
server ! ip Nat inside source route-map nonat interface
Dialer1 overload access-list 1 permit 192.168.100.0
0.0.0.255 access-list 101 permit ip 192.168.100.0
0.0.0.255 192.168.200.0 0.0.0.255 access-list 105 deny
ip 192.168.100.0 0.0.0.255 192.168.200.0 0.0.0.255
access-list 105 permit ip 192.168.100.0 0.0.0.255 any !
route-map nonat permit 10 match ip address 105 ! ! line
con 0 transport input none stopbits 1 line vty 0 4 login
! scheduler max-task-time 5000 end
```

Маршрутизатор light

```
version 12.1
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname light
!
```

```
boot system flash:c3660-jk2s-mz.121-5.T8.bin
logging buffered 4096 debugging
logging rate-limit console 10 except errors
!
ip subnet-zero
!
no ip finger
!
ip cef
!
crypto isakmp policy 20
 encr 3des
 authentication pre-share
 group 2
crypto isakmp key sharedkey address 20.20.20.20
!
crypto ipsec transform-set dsltest esp-3des esp-md5-hmac
!
crypto map test 10 ipsec-isakmp
 set peer 20.20.20.20
 set transform-set dsltest
 match address 101
!
call rsvp-sync
cns event-service server
!
!
!
controller E1 2/0
!
!
interface FastEthernet0/0
 ip address 192.168.200.200 255.255.255.0
 ip Nat inside
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 30.30.30.30 255.255.255.0
 ip Nat outside
 duplex auto
 speed auto
 crypto map test
!
interface Serial1/0
 no ip address
 shutdown
!
interface Serial1/1
 no ip address
 shutdown
!
interface Serial1/2
 no ip address
 shutdown
!
interface Serial1/3
 no ip address
 shutdown
!
interface BRI4/0
 no ip address
 shutdown
!
```

```
interface BRI4/1
 no ip address
 shutdown
!
interface BRI4/2
 no ip address
 shutdown
!
interface BRI4/3
 no ip address
 shutdown
!
ip kerberos source-interface any
ip Nat inside source route-map nonat interface
FastEthernet0/1 overload
ip classless
ip route 0.0.0.0 0.0.0.0 30.30.30.1
ip http server
!
access-list 101 permit ip 192.168.200.0 0.0.0.255
192.168.100.0 0.0.0.255
access-list 105 deny   ip 192.168.200.0 0.0.0.255
192.168.100.0 0.0.0.255
access-list 105 permit ip 192.168.200.0 0.0.0.255 any
!
route-map nonat permit 10
 match ip address 105
!
!
dial-peer cor custom
!
!
line con 0
 exec-timeout 0 0
 transport input none
line 97 108
line aux 0
line vty 0 4
 login
!
end
```

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.

Примечание: Понять точно, на что следующие **команды показа** указывают см. Устранение проблем системы безопасности IP - Понимание и Использование Команд отладки.

- **show crypto isakmp sa— показывает ассоциацию безопасности (SA) протокола ISAKMP, построенную между двумя одноранговыми узлами.**
- **show crypto ipsec sa— показывает ассоциации безопасности IPSec, установленные между узлами.**

- **show crypto engine connections active – Показывает все встроенные сопоставления безопасности второго этапа и объем отправленного трафика.**

IPSec маршрутизатора Хорошая команда показа

- **show crypto isakmp sa**Cisco 827 (CPE)Маршрутизатор light
- **show crypto engine connections active**Cisco 827 (CPE)Маршрутизатор light
- **show crypto ipsec sa**

```
827#show crypto ipsec sa interface: Dialer1 Crypto map tag: test, local addr. 20.20.20.20 local
ident (addr/mask/prot/port): (192.168.100.0/255.255.255.0/0/0) remote ident
(addr/mask/prot/port): (192.168.200.0/255.255.255.0/0/0) current_peer: 30.30.30.30 PERMIT,
flags={origin_is_acl,} #pkts encaps: 208, #pkts encrypt: 208, #pkts digest 208 #pkts decaps:
208, #pkts decrypt: 208, #pkts verify 208 #pkts compressed: 0, #pkts decompressed: 0 #pkts not
compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0 #send errors 2, #recv errors 0
local crypto endpt.: 20.20.20.20, remote crypto endpt.: 30.30.30.30 path mtu 1500, media mtu
1500 current outbound spi: 4FE59EF2 inbound esp sas: spi: 0x3491ACD6(881962198) transform: esp-
3des esp-md5-hmac , in use settings ={Tunnel, } slot: 0, conn id: 2000, flow_id: 1, crypto map:
test sa timing: remaining key lifetime (k/sec): (4607840/3301) IV size: 8 bytes replay detection
support: Y inbound ah sas: inbound pcp sas: outbound esp sas: spi: 0x4FE59EF2(1340448498)
transform: esp-3des esp-md5-hmac , in use settings ={Tunnel, } slot: 0, conn id: 2001, flow_id:
2, crypto map: test sa timing: remaining key lifetime (k/sec): (4607837/3301) IV size: 8 bytes
replay detection support: Y outbound ah sas: outbound pcp sas: interface: Virtual-Access1 Crypto
map tag: test, local addr. 20.20.20.20 local ident (addr/mask/prot/port):
(192.168.100.0/255.255.255.0/0/0) remote ident (addr/mask/prot/port):
(192.168.200.0/255.255.255.0/0/0) current_peer: 30.30.30.30 PERMIT, flags={origin_is_acl,} #pkts
encaps: 208, #pkts encrypt: 208, #pkts digest 208 #pkts decaps: 208, #pkts decrypt: 208, #pkts
verify 208 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 0, #pkts compr.
failed: 0, #pkts decompress failed: 0 #send errors 2, #recv errors 0 local crypto endpt.:
20.20.20.20, remote crypto endpt.: 30.30.30.30 path mtu 1500, media mtu 1500 current outbound
spi: 4FE59EF2 inbound esp sas: spi: 0x3491ACD6(881962198) transform: esp-3des esp-md5-hmac , in
use settings ={Tunnel, } slot: 0, conn id: 2000, flow_id: 1, crypto map: test sa timing:
remaining key lifetime (k/sec): (4607840/3301) IV size: 8 bytes replay detection support: Y
inbound ah sas: inbound pcp sas: outbound esp sas: spi: 0x4FE59EF2(1340448498) transform: esp-
3des esp-md5-hmac , in use settings ={Tunnel, } slot: 0, conn id: 2001, flow_id: 2, crypto map:
test sa timing: remaining key lifetime (k/sec): (4607837/3301) IV size: 8 bytes replay detection
support: Y outbound ah sas: outbound pcp sas:
```

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

Команды для устранения неполадок

Примечание: Прежде, чем выполнить **команды отладки**, посмотрите раздел Важные сведения о командах отладки и Устранение проблем системы безопасности IP - Понимание и Использование Команд отладки.

- **команда debug crypto ipsec отображает согласование IPSec на втором этапе.**
- **debug crypto isakmp – вывод данных о согласовании ISAKMP в фазе 1.**
- **"debug crypto engine" - отображается зашифрованный трафик.**
- **ping - служит для определения состояния соединения через туннель VPN и может использоваться в сочетании с командами debug и show.**

```
827#ping Protocol [ip]: Target IP address: 192.168.200.200 Repeat count [5]: 100 Datagram size
[100]: 1600 Timeout in seconds [2]: Extended commands [n]: y Source address or interface:
```

```
192.168.100.100 Type of service [0]: Set DF bit in IP header? [no]: Validate reply data? [no]:
Data pattern [0xABCD]: Loose, Strict, Record, Timestamp, Verbose[none]: Sweep range of sizes
[n]: Type escape sequence to abort. Sending 100, 1600-byte ICMP Echos to 192.168.200.200,
timeout is 2 seconds: !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!! Success rate is 100 percent (100/100), round-trip min/avg/max =
264/266/276 ms
```

Дополнительные сведения

- Страницы поддержки IPSec
- Страницы поддержки IP-маршрутизации
- Введение к IP - безопасному шифрованию
- Устранение неполадок для маршрутизатора Cisco 827
- Техническая поддержка - Cisco Systems