Configurando um Cisco 827 para o PPPoE com sobrecarga NAT do IPSec de VPN

Índice

Introdução

O roteador Cisco 827 é geralmente um equipamento local do cliente (CPE). Nesta configuração de exemplo, o Cisco 827 é configurado para o protocolo ponto a ponto em Ethernet (PPPoE) e é usado como um par em um túnel IPSec de LAN para LAN com um roteador Cisco 3600. O Cisco 827 também faz a sobrecarga da conversão de endereço de rede (NAT) para fornecer a conexão com a Internet para sua rede interna.

Antes de Começar

Convenções

Para obter mais informações sobre convenções de documento, consulte as Convenções de dicas técnicas Cisco.

Pré-requisitos

Ao considerar essa configuração, lembre-se do seguinte.

- Certifique-se de que o PPPoE está trabalhando antes de adicionar uma configuração para o IPSec VPN no Cisco 827. Para debugar o PPPoE Client no Cisco 827, você deve considerar a pilha de protocolos. Você deve solucionar o problema na seqüência a seguir.Camada física DSLCamada ATMCamada de EthernetCamada PPP
- Nesta configuração de exemplo, o Cisco 827 tem um endereço IP estático. Se seu Cisco 827

tem um endereço IP dinâmico, veja por favor configurar o IPSec dinâmico a estático de roteador a roteador com NAT além do que este documento.

Componentes Utilizados

As informações neste documento são baseadas nas versões de software e hardware abaixo.

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

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se você estiver trabalhando em uma rede ativa, certifique-se de que entende o impacto potencial de qualquer comando antes de utilizá-lo.

Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Diagrama de Rede

Este documento utiliza a instalação de rede mostrada no diagrama abaixo.

Configurações

Este documento utiliza as configurações mostradas abaixo.

- Cisco 827 (CPE)
- Luz do Roteador

Nota: Para localizar informações adicionais sobre os comandos usados neste documento, utilize a Ferramenta Command Lookup (somente clientes registrados).

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
```

Luz do Roteador

```
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
```

Verificar

Esta seção fornece informações que você pode usar para confirmar se sua configuração está funcionando adequadamente.

A Output Interpreter Tool (somente clientes registrados) oferece suporte a determinados comandos show, o que permite exibir uma análise da saída do comando show.

Nota: Para compreender exatamente o que os seguintes **comandos show** indicam, satisfaça referem o Troubleshooting de Segurança IP - compreendendo e usando comandos Debug.

- **mostre isakmp cripto sa** - Mostra a associação de segurança do protocolo internet security association management (ISAKMP) (SA) construída entre pares.
- show crypto ipsec sa - Mostra o SA de IPSec criado entre os correspondentes.
- show crypto engine connections active – Mostra cada fase 2 SA embutida e a quantidade de tráfego enviado.

Bom comando show do IPSec de roteador

- show crypto isakmp saCisco 827 (CPE)Luz do Roteador
- **show crypto engine connections active**Cisco 827 (CPE)Luz do Roteador
- **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:
```

Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Comandos para Troubleshooting

Nota: Antes de emitir **comandos debug**, veja por favor a informação importante em comandos Debug e em Troubleshooting de Segurança IP - compreendendo e usando comandos Debug.

- **o IPsec do debug crypto** mostra as negociações de IPSEC de fase 2.
- debug crypto isakmp Exibe as negociações ISAKMP da fase 1.
- **motor do debug crypto** - Mostra o tráfego que é cifrado.
- ping - mostra a conectividade pelo túnel de VPN e pode ser usado juntamente com os comandos debug e 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
```

Informações Relacionadas

- Páginas de Suporte do IPSec
- Páginas de Suporte ao IP Routing
- Uma introdução à criptografia IPSec
- Troubleshooting o Cisco 827 Router
- Suporte Técnico - Cisco Systems