Configuring GRE over IPSec Between a Cisco IOS Router and a VPN 5000 Concentrator Using Static Routing

Índice

Introdução

Este documento descreve como configurar o Generic Routing Encapsulation (GRE) sobre o IPsec entre um concentrador da Cisco VPN 5000 Series e um roteador Cisco que executam o software de Cisco IOS®. O recurso GRE sobre IPSec foi incorporado no release do software VPN 5000 Concentrator 6.0(19).

Neste exemplo, o roteamento estático é usado aos pacotes de rota através do túnel.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco IOS Software Release 12.2(3)

- Versão de software do concentrador do Cisco VPN 5000 6.0(19)

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 a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

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

Configurar

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

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

Diagrama de Rede

Este documento utiliza a configuração de rede mostrada neste diagrama.

O GRE sobre o IPsec é configurado entre o Cisco IOS Software running do 1720-1 Router e o VPN 5002 concentrator. Atrás do roteador e do concentrador VPN, há as redes múltiplas que são anunciadas com o Open Shortest Path First (OSPF). O OSPF é executado dentro do túnel GRE entre o roteador e o concentrador VPN.

- Estas redes são atrás do 1720-1 Router.10.1.1.0/2410.1.2.0/2410.1.3.0/24
- Estas redes são atrás do VPN 5002 concentrator.20.1.1.0/2420.1.2.0/2420.1.3.0/24

Configurações

Este documento utiliza estas configurações.

- 1720-1 Router
- VPN 5002 concentrator

Note: Com Cisco IOS Software Release 12.2(13)T e Mais Recente (códigos numerados mais altos, 12.3 e códigos mais recente do T-trem), você deve aplicar o crypto map configurado do IPsec à interface física somente. Você já não tem que aplicar o crypto map na interface do túnel GRE. Ter o crypto map no exame e nas interfaces de túnel quando você usa os Cisco IOS Software Release 12.2.(13)T e mais tarde deve ainda trabalhar, mas o Cisco Systems recomenda que você aplica o crypto map na interface física somente.

1720-1 Router

```
Current configuration : 1305 bytes
!
version 12.2
service timestamps debug uptime
```

```
service timestamps log uptime
no service password-encryption
!
hostname 1720-1
!
no logging buffered
no logging monitor
enable secret 5 $1$vIzI$RqD0LqlqbSFCCjVELFLfH/
!
memory-size iomem 15
ip subnet-zero
no ip domain-lookup
!
ip audit notify log
ip audit po max-events 100
ip ssh time-out 120
ip ssh authentication-retries 3
!
crypto isakmp policy 1
 hash md5
 authentication pre-share
crypto isakmp key cisco123 address 172.16.172.21
!
!
crypto ipsec transform-set myset esp-des esp-md5-hmac
 mode transport
!
crypto map vpn 10 ipsec-isakmp
 set peer 172.16.172.21
 set transform-set myset
 match address 102
!
cns event-service server
!
!
!
interface Tunnel0
 ip address 50.1.1.1 255.255.255.252
 tunnel source FastEthernet0
 tunnel destination 172.16.172.21
 crypto map vpn
!
interface FastEthernet0
 ip address 172.16.172.39 255.255.255.240
 speed auto
 crypto map vpn
!
interface Serial0
 ip address 10.1.1.2 255.255.255.0
 encapsulation ppp
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.16.172.33
ip route 10.1.0.0 255.255.0.0 10.1.1.1
ip route 20.1.0.0 255.255.0.0 Tunnel0
no ip http server
!
access-list 102 permit gre host 172.16.172.39 host
172.16.172.21
!
line con 0
line aux 0
line vty 0 4
 password cisco
```

```
 login
!
no scheduler allocate
end
```

VPN 5002 concentrator

```
[ General ]
VPNGateway              = 172.16.172.17
EthernetAddress         = 00:05:32:3e:90:40
DeviceType              = VPN 5002/8 Concentrator
ConfiguredOn            = Timeserver not configured
ConfiguredFrom          = Command Line, from Console

[ IKE Policy ]
Protection              = SHA_DES_G1
Protection              = MD5_DES_G2
Protection              = MD5_DES_G1

[ Tunnel Partner VPN 1 ]
KeyLifeSecs             = 3500
KeepaliveInterval       = 120
TunnelType              = GREinIPSec
InactivityTimeout       = 120
Transform               = ESP(MD5,DES)
BindTo                  = "Ethernet 1:0"
SharedKey               = "cisco123"
Certificates            = Off
Mode                    = Main
KeyManage               = Reliable
Partner                 = 172.16.172.39

[ IP VPN 1 ]
HelloInterval           = 10
SubnetMask              = 255.255.255.252
IPAddress               = 50.1.1.2
DirectedBroadcast       = Off
Numbered                = On
Mode                    = Routed

[ IP Ethernet 1:0 ]
Mode                    = Routed
SubnetMask              = 255.255.255.240
IPBroadcast             = 172.16.172.32
IPAddress               = 172.16.172.21

[ IP Ethernet 0:0 ]
Mode                    = Routed
IPBroadcast             = 20.1.1.255
SubnetMask              = 255.255.255.0
IPAddress               = 20.1.1.1

[ Logging ]
Level                   = Debug
LogToAuxPort            = On
Enabled                 = On

[ Ethernet Interface Ethernet 0:0 ]
DUPLEX                  = half
SPEED                   = 10meg


[ IP Static ]
```

```
0.0.0.0 0.0.0.0 20.1.1.5 1
10.1.1.0 255.255.255.0 VPN 1 1
10.1.2.0 255.255.255.0 VPN 1 1
10.1.3.0 255.255.255.0 VPN 1 1

Configuration size is 1696 out of 65500 bytes.
```

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.

- Estes comandos podem ser executados no roteador do Cisco IOS.**mostre isakmp cripto sa** — Mostra todas as associações de segurança atuais do Internet Security Association and Key Management Protocol (ISAKMP) (SA).**mostre IPsec cripto sa** — Mostra todo o IPSec atual SA.**show crypto engine connection ative** — Mostra o contador da criptografia de pacote de informação/descriptografia para o cada sas de IPSec.
- Você pode executar estes comandos no VPN 5002 concentrator.**Show System Log Buffer** — Mostra a informação do syslog básica.**descarga do traço do vpn** — Mostra a informação detalhada sobre processos VPN.

Troubleshooting

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

Comandos para Troubleshooting

Note: Antes de emitir **comandos debug**, consulte Informações importantes sobre comandos debug.

Você pode executar estes comandos no roteador do Cisco IOS.

- **isakmp do debug crypto** — Mostra-me a informação detalhada sobre a fase de intercâmbio de chave de Internet (IKE) negociação (do modo principal).
- **IPsec do debug crypto** — Mostra a informação detalhada sobre a negociação da fase II IKE (Quick Mode).
- **motor do debug crypto** — Debuga a criptografia de pacote de informação/descriptografia e o processo do Diffie-Hellman (DH).

Exemplo de debug

O exemplo de debug para o roteador e o concentrador VPN é mostrado aqui.

- Cisco IOS Router
- VPN 5002 concentrator

Debuga no roteador do Cisco IOS

A saída dos **comandos debug crypto isakmp e debug crypto ipsec no** roteador é mostrada aqui.

```
5d20h: ISAKMP (0:0): received packet from 172.16.172.21 (N) NEW SA
5d20h: ISAKMP: local port 500, remote port 500
5d20h: ISAKMP (0:81): processing SA payload. message ID = 0
5d20h: ISAKMP (0:81): found peer pre-shared key matching 172.16.172.21
5d20h: ISAKMP (0:81): Checking ISAKMP transform 1 against priority 1 policy
5d20h: ISAKMP:      encryption DES-CBC
5d20h: ISAKMP:      hash SHA
5d20h: ISAKMP:      auth pre-share
5d20h: ISAKMP:      default group 1
5d20h: ISAKMP (0:81): atts are not acceptable. Next payload is 3
5d20h: ISAKMP (0:81): Checking ISAKMP transform 2 against priority 1 policy
5d20h: ISAKMP:      encryption DES-CBC
5d20h: ISAKMP:      hash MD5
5d20h: ISAKMP:      auth pre-share
5d20h: ISAKMP:      default group 2
5d20h: ISAKMP (0:81): atts are not acceptable. Next payload is 3
5d20h: ISAKMP (0:81): Checking ISAKMP transform 3 against priority 1 policy
5d20h: ISAKMP:      encryption DES-CBC
5d20h: ISAKMP:      hash MD5
5d20h: ISAKMP:      auth pre-share
5d20h: ISAKMP:      default group 1
5d20h: ISAKMP (0:81): atts are acceptable. Next payload is 0
5d20h: ISAKMP (0:81): processing vendor id payload
5d20h: ISAKMP (0:81): SA is doing pre-shared key authentication
using id type ID_IPV4_ADDR
5d20h: ISAKMP (0:81): sending packet to 172.16.172.21 (R) MM_SA_SETUP
5d20h: ISAKMP (0:81): received packet from 172.16.172.21 (R) MM_SA_SETUP
5d20h: ISAKMP (0:81): processing KE payload. message ID = 0
5d20h: ISAKMP (0:81): processing NONCE payload. message ID = 0
5d20h: ISAKMP (0:81): found peer pre-shared key matching 172.16.172.21
5d20h: ISAKMP (0:81): SKEYID state generated
5d20h: ISAKMP (0:81): sending packet to 172.16.172.21 (R) MM_KEY_EXCH
5d20h: ISAKMP (0:81): received packet from 172.16.172.21 (R) MM_KEY_EXCH
5d20h: ISAKMP (0:81): processing ID payload. message ID = 0
5d20h: ISAKMP (0:81): processing HASH payload. message ID = 0
5d20h: ISAKMP (0:81): SA has been authenticated with 172.16.172.21
5d20h: ISAKMP (81): ID payload
        next-payload : 8
        type         : 1
        protocol     : 17
        port         : 500
        length       : 8
5d20h: ISAKMP (81): Total payload length: 12
5d20h: ISAKMP (0:81): sending packet to 172.16.172.21 (R) QM_IDLE
5d20h: ISAKMP (0:81): received packet from 172.16.172.21 (R) QM_IDLE
5d20h: ISAKMP (0:81): processing HASH payload. message ID = 241
5d20h: ISAKMP (0:81): processing SA payload. message ID = 241
5d20h: ISAKMP (0:81): Checking IPSec proposal 1
5d20h: ISAKMP: transform 1, ESP_DES
5d20h: ISAKMP:   attributes in transform:
5d20h: ISAKMP:      SA life type in seconds
5d20h: ISAKMP:      SA life duration (VPI) of  0x0 0x0 0xD 0xAC
5d20h: ISAKMP:      SA life type in kilobytes
5d20h: ISAKMP:      SA life duration (VPI) of  0x0 0x10 0x0 0x0
5d20h: ISAKMP:      encaps is 2
5d20h: ISAKMP:      authenticator is HMAC-MD5
5d20h: ISAKMP (0:81): atts are acceptable.
```

```
5d20h: IPSEC(validate_proposal_request): proposal part #1,
  (key eng. msg.) dest= 172.16.172.39, src= 172.16.172.21,
    dest_proxy= 172.16.172.39/255.255.255.255/47/0 (type=1),
    src_proxy= 172.16.172.21/255.255.255.255/47/0 (type=1),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x0
5d20h: ISAKMP (0:81): processing NONCE payload. message ID = 241
5d20h: ISAKMP (0:81): processing ID payload. message ID = 241
5d20h: ISAKMP (81): ID_IPV4_ADDR src 172.16.172.21 prot 47 port 0
5d20h: ISAKMP (0:81): processing ID payload. message ID = 241
5d20h: ISAKMP (81): ID_IPV4_ADDR dst 172.16.172.39 prot 47 port 0
5d20h: ISAKMP (0:81): asking for 1 spis from ipsec
5d20h: IPSEC(key_engine): got a queue event...
5d20h: IPSEC(spi_response): getting spi 895566248 for SA
        from 172.16.172.21   to 172.16.172.39   for prot 3
5d20h: ISAKMP: received ke message (2/1)
5d20h: ISAKMP (0:81): sending packet to 172.16.172.21 (R) QM_IDLE
5d20h: ISAKMP (0:81): received packet from 172.16.172.21 (R) QM_IDLE
5d20h: ISAKMP (0:81): Creating IPSec SAs
5d20h:         inbound SA from 172.16.172.21 to 172.16.172.39
        (proxy 172.16.172.21 to 172.16.172.39)
5d20h:         has spi 0x356141A8 and conn_id 362 and flags 0
5d20h:         lifetime of 3500 seconds
5d20h:         lifetime of 1048576 kilobytes
5d20h:         outbound SA from 172.16.172.39   to 172.16.172.21
(proxy 172.16.172.39   to 172.16.172.21  )
5d20h:         has spi 337 and conn_id 363 and flags 0
5d20h:         lifetime of 3500 seconds
5d20h:         lifetime of 1048576 kilobytes
5d20h: ISAKMP (0:81): deleting node 241 error FALSE reason
"quick mode done (await()"
5d20h: IPSEC(key_engine): got a queue event...
5d20h: IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 172.16.172.39, src= 172.16.172.21,
    dest_proxy= 172.16.172.39/0.0.0.0/47/0 (type=1),
    src_proxy= 172.16.172.21/0.0.0.0/47/0 (type=1),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 3500s and 1048576kb,
    spi= 0x356141A8(895566248), conn_id= 362, keysize= 0, flags= 0x0
5d20h: IPSEC(initialize_sas): ,
  (key eng. msg.) src= 172.16.172.39, dest= 172.16.172.21,
    src_proxy= 172.16.172.39/0.0.0.0/47/0 (type=1),
    dest_proxy= 172.16.172.21/0.0.0.0/47/0 (type=1),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 3500s and 1048576kb,
    spi= 0x151(337), conn_id= 363, keysize= 0, flags= 0x0
5d20h: IPSEC(create_sa): sa created,
  (sa) sa_dest= 172.16.172.39, sa_prot= 50,
    sa_spi= 0x356141A8(895566248),
    sa_trans= esp-des esp-md5-hmac , sa_conn_id= 362
5d20h: IPSEC(create_sa): sa created,
  (sa) sa_dest= 172.16.172.21, sa_prot= 50,
    sa_spi= 0x151(337),
    sa_trans= esp-des esp-md5-hmac , sa_conn_id= 363
5d20h: IPSEC(add_sa): peer asks for new SAs -- expire current in 120 sec.,
  (sa) sa_dest= 172.16.172.21, sa_prot= 50,
    sa_spi= 0x150(336),
    sa_trans= esp-des esp-md5-hmac , sa_conn_id= 361,
  (identity) local= 172.16.172.39, remote= 172.16.172.21,
    local_proxy= 172.16.172.39/255.255.255.255/47/0 (type=1),
    remote_proxy= 172.16.172.21/255.255.255.255/47/0 (type=1)
1720-1#
```

```
1720-1#show crypto isakmp sa
dst             src             state          conn-id    slot
172.16.172.39   172.16.172.21   QM_IDLE             81       0

1720-1#show crypto ipsec sa

interface: FastEthernet0
    Crypto map tag: vpn, local addr. 172.16.172.39

   local  ident (addr/mask/prot/port): (172.16.172.39/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port): (172.16.172.21/255.255.255.255/0/0)
   current_peer: 172.16.172.21
     PERMIT, flags={transport_parent,}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0,
    #pkts decompress failed: 0, #send errors 0, #recv errors 0

     local crypto endpt.: 172.16.172.39, remote crypto endpt.: 172.16.172.21
     path mtu 1514, media mtu 1514
     current outbound spi: 0

     inbound esp sas:

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:

     outbound ah sas:

     outbound pcp sas:

   local  ident (addr/mask/prot/port): (172.16.172.39/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (172.16.172.21/255.255.255.255/47/0)
   current_peer: 172.16.172.21
     PERMIT, flags={origin_is_acl,transport_parent,parent_is_transport,}
    #pkts encaps: 34901, #pkts encrypt: 34901, #pkts digest 34901
    #pkts decaps: 34900, #pkts decrypt: 34900, #pkts verify 34900
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0,
    #pkts decompress failed: 0, #send errors 0, #recv errors 0

     local crypto endpt.: 172.16.172.39, remote crypto endpt.: 172.16.172.21
     path mtu 1500, media mtu 1500
     current outbound spi: 151

     inbound esp sas:
      spi: 0x356141A8(895566248)
        transform: esp-des esp-md5-hmac ,
        in use settings ={Transport, }
        slot: 0, conn id: 362, flow_id: 163, crypto map: vpn
        sa timing: remaining key lifetime (k/sec): (1046258/3306)
        IV size: 8 bytes
        replay detection support: Y

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x151(337)
```

```
        transform: esp-des esp-md5-hmac ,
        in use settings ={Transport, }
        slot: 0, conn id: 363, flow_id: 164, crypto map: vpn
        sa timing: remaining key lifetime (k/sec): (1046258/3306)
        IV size: 8 bytes
        replay detection support: Y

      outbound ah sas:

      outbound pcp sas:



interface: Tunnel0
    Crypto map tag: vpn, local addr. 172.16.172.39

   local  ident (addr/mask/prot/port): (172.16.172.39/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port): (172.16.172.21/255.255.255.255/0/0)
   current_peer: 172.16.172.21
     PERMIT, flags={transport_parent,}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0,
    #pkts decompress failed: 0, #send errors 0, #recv errors 0

     local crypto endpt.: 172.16.172.39, remote crypto endpt.: 172.16.172.21
     path mtu 1514, media mtu 1514
     current outbound spi: 0

     inbound esp sas:

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:

     outbound ah sas:

     outbound pcp sas:



   local  ident (addr/mask/prot/port): (172.16.172.39/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (172.16.172.21/255.255.255.255/47/0)
   current_peer: 172.16.172.21
     PERMIT, flags={origin_is_acl,transport_parent,parent_is_transport,}
    #pkts encaps: 35657, #pkts encrypt: 35657, #pkts digest 35657
    #pkts decaps: 35656, #pkts decrypt: 35656, #pkts verify 35656
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0,
    #pkts decompress failed: 0, #send errors 0, #recv errors 0

     local crypto endpt.: 172.16.172.39, remote crypto endpt.: 172.16.172.21
     path mtu 1500, media mtu 1500
     current outbound spi: 151

     inbound esp sas:
      spi: 0x356141A8(895566248)
        transform: esp-des esp-md5-hmac ,
        in use settings ={Transport, }
        slot: 0, conn id: 362, flow_id: 163, crypto map: vpn
        sa timing: remaining key lifetime (k/sec): (1046154/3302)
```

```
        IV size: 8 bytes
        replay detection support: Y

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x151(337)
        transform: esp-des esp-md5-hmac ,
        in use settings ={Transport, }
        slot: 0, conn id: 363, flow_id: 164, crypto map: vpn
        sa timing: remaining key lifetime (k/sec): (1046154/3302)
        IV size: 8 bytes
        replay detection support: Y

     outbound ah sas:

     outbound pcp sas:

1720-1#show crypto engine connections active

  ID Interface             IP-Address    State  Algorithm    Encrypt Decrypt
  81 FastEthernet0  172.16.172.39   set  HMAC_MD5+DES_56_CB      0       0
 362 FastEthernet0  172.16.172.39   set  HMAC_MD5+DES_56_CB      0   23194
 363 FastEthernet0  172.16.172.39   set  HMAC_MD5+DES_56_CB  23195       0
```

Debuga no VPN 5002 concentrator

As saídas de SYSLOG no concentrador VPN são mostradas aqui.

```
VPN5002_8_323E9040: Main# VPN 0:1 opened for 172.16.172.39 from 172.16.172.39.
User assigned IP address 50.1.1.2

VPN5002_8_323E9040: Main#show vpn partner verbose


Port        Partner         Partner  Default  Bindto          Connect
Number      Address         Port     Partner  Address         Time
-------------------------------------------------------------------------
VPN 0:1     172.16.172.39   500      No       172.16.172.21   00:00:13:26
     Auth/Encrypt: MD5e/DES  User Auth: Shared Key
     Access: Static Peer: 172.16.172.39    Local: 172.16.172.21
     Start:14518 seconds Managed:15299 seconds State:imnt_maintenance


IOP slot 1:
No active connections found.


VPN5002_8_323E9040: Main#show vpn statistics verbose

          Current  In       High     Running  Script   Script   Script
          Active   Negot    Water    Total    Starts   OK       Error
          ---------------------------------------------------------------
Users     0        0        0        0        0        0        0
Partners  1        0        1        81       81       1        158
Total     1        0        1        81       81       1        158

Stats             VPN0:1
Wrapped            79733
Unwrapped          79734
```

```
BadEncap                0
BadAuth                 0
BadEncrypt              0
rx IP               79749
rx IPX                  0
rx Other                0
tx IP               79761
tx IPX                  0
tx Other                0
IKE rekey               0

Input VPN pkts dropped due to no SA: 0

Input VPN pkts dropped due to no free queue entries: 0

IOP slot 1:

          Current  In       High     Running  Script   Script   Script
          Active   Negot    Water    Total    Starts   OK       Error
          ------------------------------------------------------------
Users     0        0        0        0        0        0        0
Partners  0        0        0        0        0        0        0
Total     0        0        0        0        0        0        0
Stats
Wrapped
Unwrapped
BadEncap
BadAuth
BadEncrypt
rx IP
rx IPX
rx Other
tx IP
tx IPX
tx Other
IKE rekey

Input VPN pkts dropped due to no SA: 0

Input VPN pkts dropped due to no free queue entries: 0
```

Misconfiguration do modo de túnel

O VPN 5000 concentrator propõe o modo de transporte à revelia quando o GRE sobre o IPsec é usado. Quando o roteador do Cisco IOS é desconfigurado para o modo de túnel, a seguir este os erros ocorrem.

O resultado do debug no roteador do Cisco IOS é mostrado aqui.

```
VPN5002_8_323E9040: Main# VPN 0:1 opened for 172.16.172.39 from 172.16.172.39.
User assigned IP address 50.1.1.2

VPN5002_8_323E9040: Main#show vpn partner verbose


Port        Partner         Partner  Default  Bindto          Connect
Number      Address         Port     Partner  Address         Time
-------------------------------------------------------------------------
VPN 0:1     172.16.172.39   500      No       172.16.172.21   00:00:13:26
     Auth/Encrypt: MD5e/DES  User Auth: Shared Key
     Access: Static Peer: 172.16.172.39    Local: 172.16.172.21
```

```
     Start:14518 seconds Managed:15299 seconds State:imnt_maintenance


IOP slot 1:
No active connections found.


VPN5002_8_323E9040: Main#show vpn statistics verbose

          Current  In       High     Running  Script   Script   Script
          Active   Negot    Water    Total    Starts   OK       Error
          -----------------------------------------------------------
Users     0        0        0        0        0        0        0
Partners  1        0        1        81       81       1        158
Total     1        0        1        81       81       1        158

Stats             VPN0:1
Wrapped            79733
Unwrapped          79734
BadEncap               0
BadAuth                0
BadEncrypt             0
rx IP              79749
rx IPX                 0
rx Other               0
tx IP              79761
tx IPX                 0
tx Other               0
IKE rekey              0

Input VPN pkts dropped due to no SA: 0

Input VPN pkts dropped due to no free queue entries: 0

IOP slot 1:

          Current  In       High     Running  Script   Script   Script
          Active   Negot    Water    Total    Starts   OK       Error
          -----------------------------------------------------------
Users     0        0        0        0        0        0        0
Partners  0        0        0        0        0        0        0
Total     0        0        0        0        0        0        0
Stats
Wrapped
Unwrapped
BadEncap
BadAuth
BadEncrypt
rx IP
rx IPX
rx Other
tx IP
tx IPX
tx Other
IKE rekey

Input VPN pkts dropped due to no SA: 0

Input VPN pkts dropped due to no free queue entries: 0
```

O fazer logon o VPN 5002 concentrator mostra uma entrada similar a esta saída.

```
VPN5002_8_323E9040: Main# VPN 0:1 opened for 172.16.172.39 from 172.16.172.39.
```

```
User assigned IP address 50.1.1.2

VPN5002_8_323E9040: Main#show vpn partner verbose


Port        Partner         Partner  Default  Bindto          Connect
Number      Address         Port     Partner  Address         Time
-------------------------------------------------------------------------
VPN 0:1     172.16.172.39   500      No       172.16.172.21   00:00:13:26
     Auth/Encrypt: MD5e/DES  User Auth: Shared Key
     Access: Static Peer: 172.16.172.39    Local: 172.16.172.21
     Start:14518 seconds Managed:15299 seconds State:imnt_maintenance


IOP slot 1:
No active connections found.


VPN5002_8_323E9040: Main#show vpn statistics verbose

          Current  In       High     Running  Script   Script   Script
          Active   Negot    Water    Total    Starts   OK       Error
          ---------------------------------------------------------------
Users     0        0        0        0        0        0        0
Partners  1        0        1        81       81       1        158
Total     1        0        1        81       81       1        158

Stats             VPN0:1
Wrapped            79733
Unwrapped          79734
BadEncap               0
BadAuth                0
BadEncrypt             0
rx IP              79749
rx IPX                 0
rx Other               0
tx IP              79761
tx IPX                 0
tx Other               0
IKE rekey              0

Input VPN pkts dropped due to no SA: 0

Input VPN pkts dropped due to no free queue entries: 0

IOP slot 1:

          Current  In       High     Running  Script   Script   Script
          Active   Negot    Water    Total    Starts   OK       Error
          ---------------------------------------------------------------
Users     0        0        0        0        0        0        0
Partners  0        0        0        0        0        0        0
Total     0        0        0        0        0        0        0
Stats
Wrapped
Unwrapped
BadEncap
BadAuth
BadEncrypt
rx IP
rx IPX
rx Other
tx IP
tx IPX
```

```
tx Other
IKE rekey

Input VPN pkts dropped due to no SA: 0

Input VPN pkts dropped due to no free queue entries: 0
```

Informações Relacionadas

- Anúncio End-of-Life de concentradores do Cisco VPN 5000 Series
- Página de suporte do Cisco VPN 5000 Concentrator
- Página de suporte ao cliente do Cisco VPN 5000
- Página de suporte do IPSec
- Suporte Técnico - Cisco Systems