Túnel de IPsec dinâmico entre um ASA estaticamente endereçado e um roteador dinamicamente endereçado do Cisco IOS que use o exemplo de configuração CCP

Índice

Introdução

Este documento fornece uma configuração de exemplo para que como permita a ferramenta de segurança PIX/ASA de aceitar conexões de IPSec dinâmica do roteador do ® do Cisco IOS. Nesta encenação, o túnel de IPsec estabelece quando o túnel é iniciado da extremidade do roteador somente. O ASA não podia iniciar um túnel VPN devido à configuração IPSec dinâmica.

Esta configuração permite a ferramenta de segurança PIX de criar um túnel dinâmico do LAN para LAN do IPsec (L2L) com um VPN Router remoto. Este roteador recebe dinamicamente seu endereço IP público exterior de seu provedor de serviço da Internet. O protocolo de configuração dinâmica host (DHCP) fornece este mecanismo a fim atribuir dinamicamente endereços IP de Um ou Mais Servidores Cisco ICM NT do fornecedor. Isto permite que os endereços IP de Um ou Mais Servidores Cisco ICM NT sejam reutilizados quando os anfitriões já não os precisam.

A configuração no roteador é feita com o uso do Cisco Configuration Professional (CCP). O CCP é uma ferramenta de Gerenciamento de dispositivos com base em GUI que permita que você configure roteadores baseado em IOS de Cisco. Refira a configuração de roteador básico usando o Cisco Configuration Professional para obter mais informações sobre de como configurar um

roteador com CCP.

Refira o local para situar VPN (L2L) com o ASA para mais inormation e exemplos de configuração no estabelecimento do túnel de IPsec que usam o Roteadores ASA e de Cisco IOS.

Refira o local para situar VPN (L2L) com IO para mais informação e um exemplo de configuração no estabelecimento dinâmico do túnel de IPsec com o uso do roteador PIX e de Cisco IOS.

Pré-requisitos

Requisitos

Antes que você tente esta configuração, assegure-se de que o ASA e o roteador tenham a conectividade de Internet a fim estabelecer o túnel de IPsec.

Componentes Utilizados

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

- Cisco IOS Router1812 que executa o Cisco IOS Software Release 12.4
- Software Release 8.0.3 de Cisco ASA 5510

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

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Informações de Apoio

Nesta encenação, a rede de 192.168.100.0 é atrás da rede ASA e de 192.168.200.0 é atrás do roteador do Cisco IOS. Supõe-se que o roteador obtém seu endereço público com o DHCP de seu ISP. Porque isto levanta um problema na configuração de um peer estático na extremidade ASA, você precisa de aproximar a maneira de configuração de criptografia dinâmica de estabelecer um túnel de site para site entre o ASA e o roteador do Cisco IOS.

Os usuários do Internet na extremidade ASA obtêm traduzidos ao endereço IP de Um ou Mais Servidores Cisco ICM NT de sua interface externa. Supõe-se que o NAT não está configurado na extremidade do roteador do Cisco IOS.

Agora estas são as etapas principais a ser configuradas na extremidade ASA a fim estabelecer o túnel dinâmico:

1. Configuração relacionada da fase 1 ISAKMP
2. Configuração Nat da isenção
3. Configuração do mapa cripto dinâmico

O roteador do Cisco IOS tem um mapa estático de criptografia configurado porque o ASA é suposto para ter um endereço IP público estático. Agora esta é a lista de etapas principais a ser configuradas na extremidade do roteador do Cisco IOS para estabelecer o túnel de IPsec dinâmico.

1. Configuração relacionada da fase 1 ISAKMP
2. Configuração relacionada do mapa estático de criptografia

Estas etapas são descritas em detalhe nestas configurações.

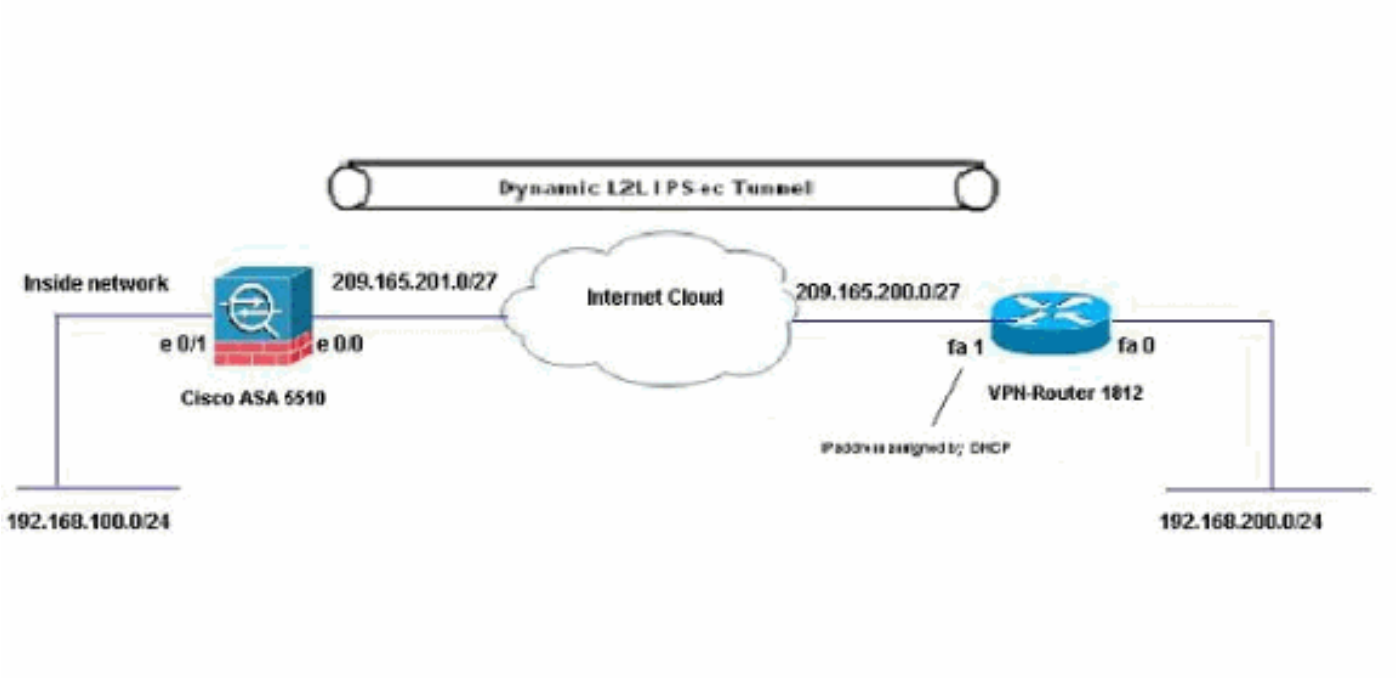
Configurar

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

Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Diagrama de Rede

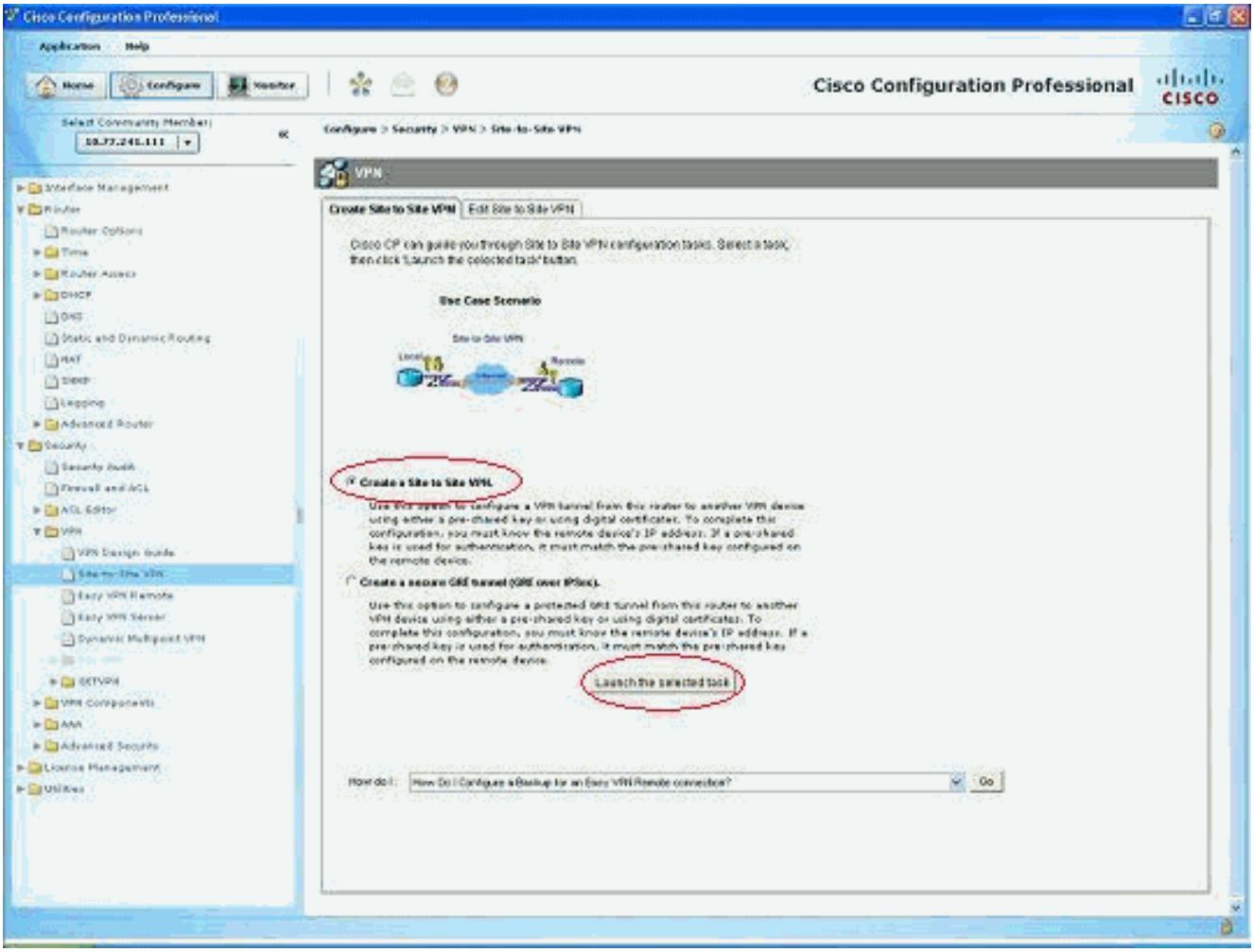
Este documento utiliza a seguinte configuração de rede:



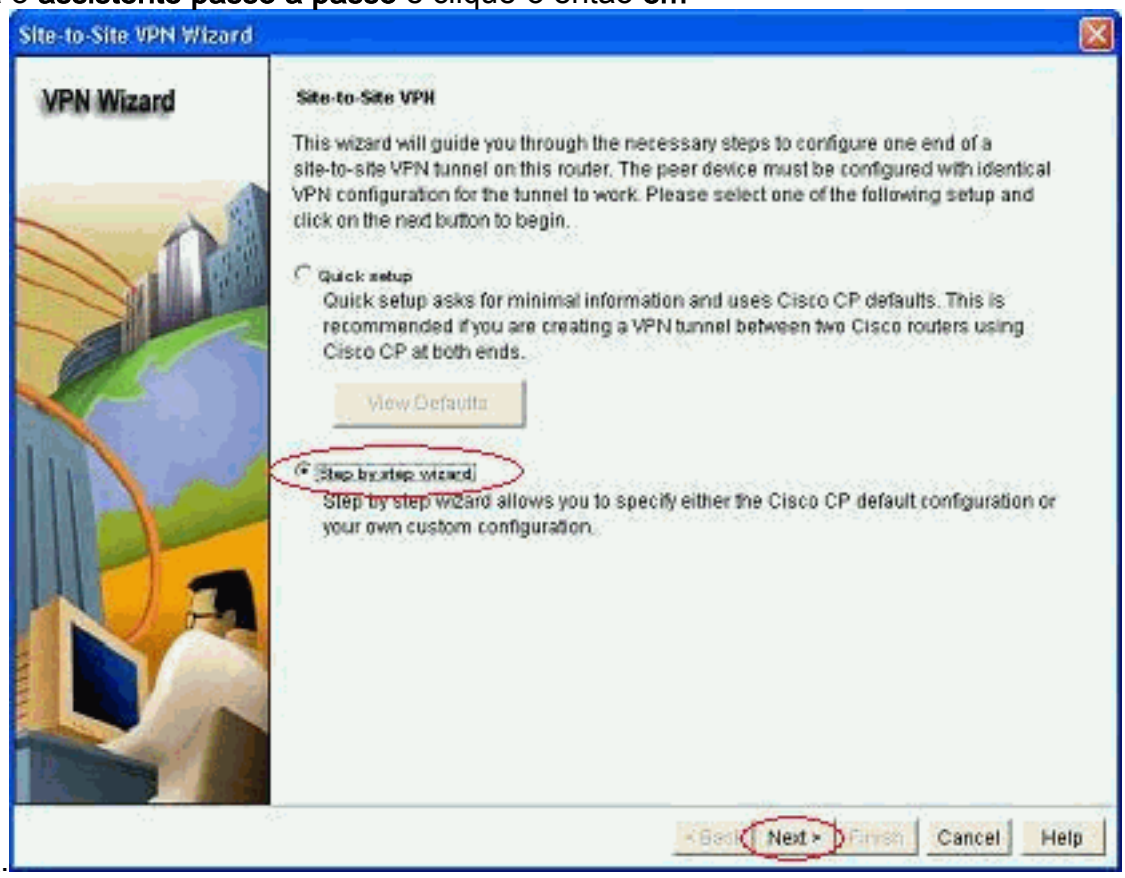
Configurações

Esta é a configuração do IPSec VPN no VPN Router com CCP. Conclua estes passos:

1. Abra o aplicativo CCP e escolha-o **configuram o > segurança > o VPN > o local para situar o VPN**. Clique o **lançamento a aba selecionada**.



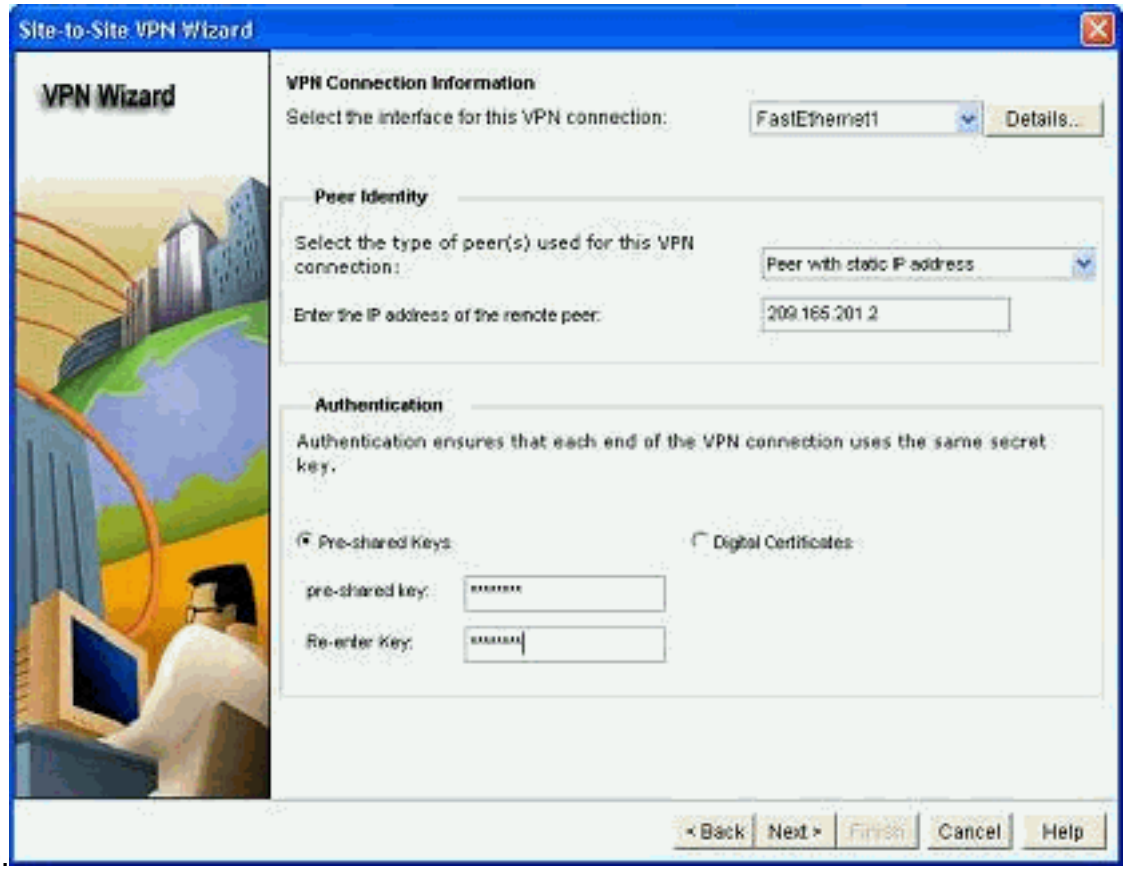
2. Escolha o **assistente passo a passo** e clique-o então **em**



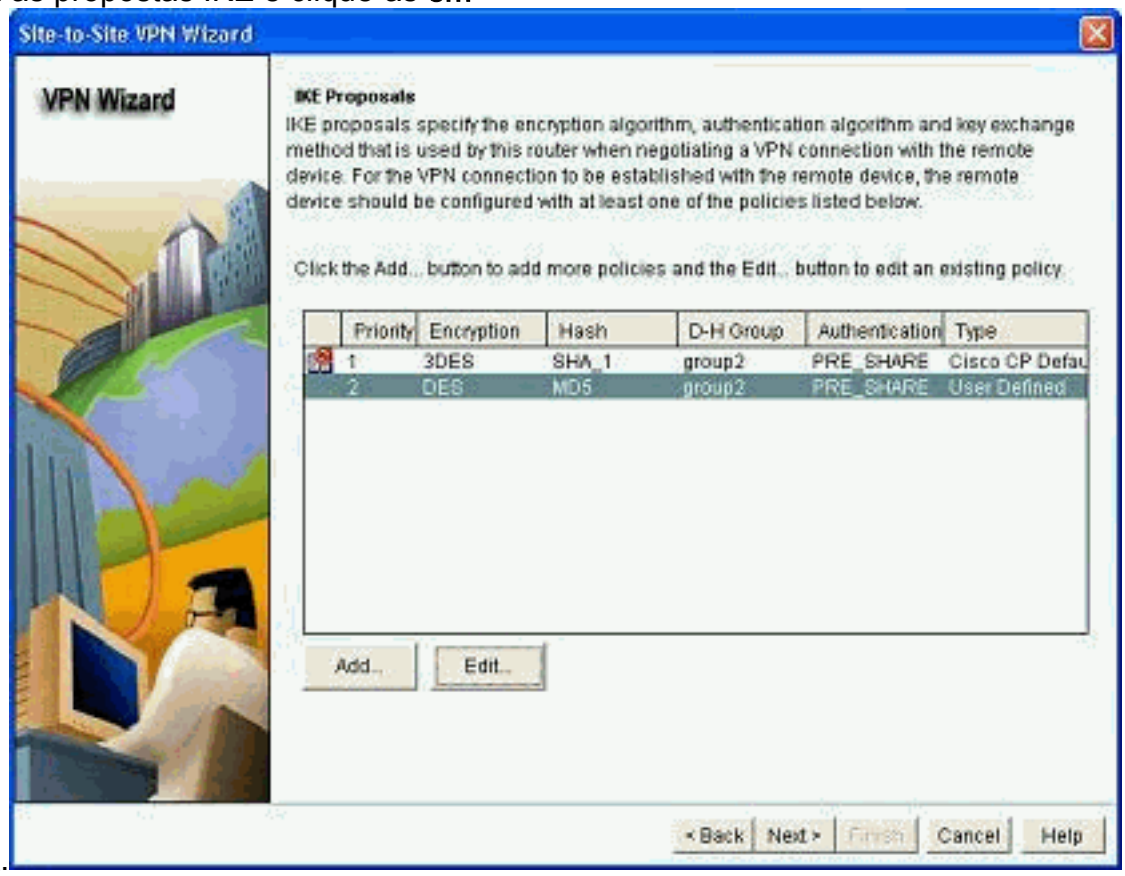
seguida.

3. Preencha o endereço IP de Um ou Mais Servidores Cisco ICM NT do peer remoto junto com os detalhes da

autenticação.

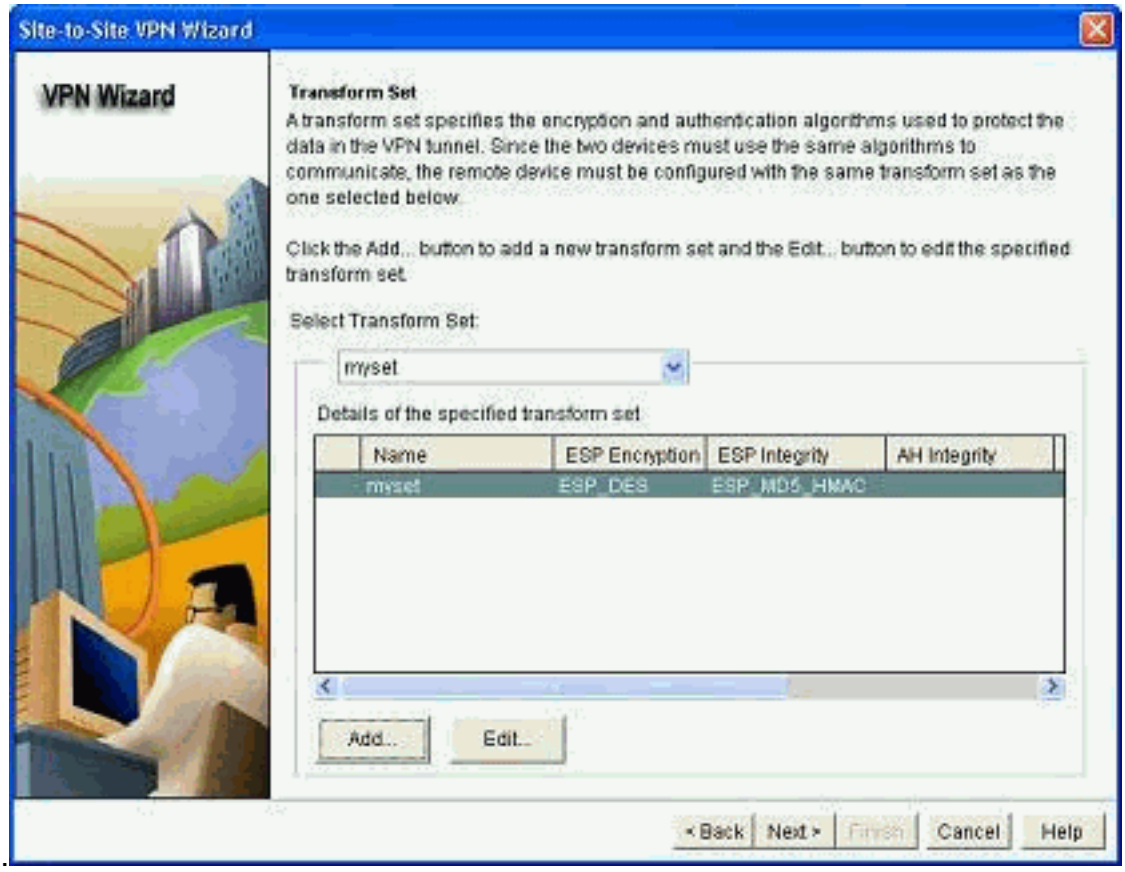


4. Escolha as propostas IKE e clique-as em



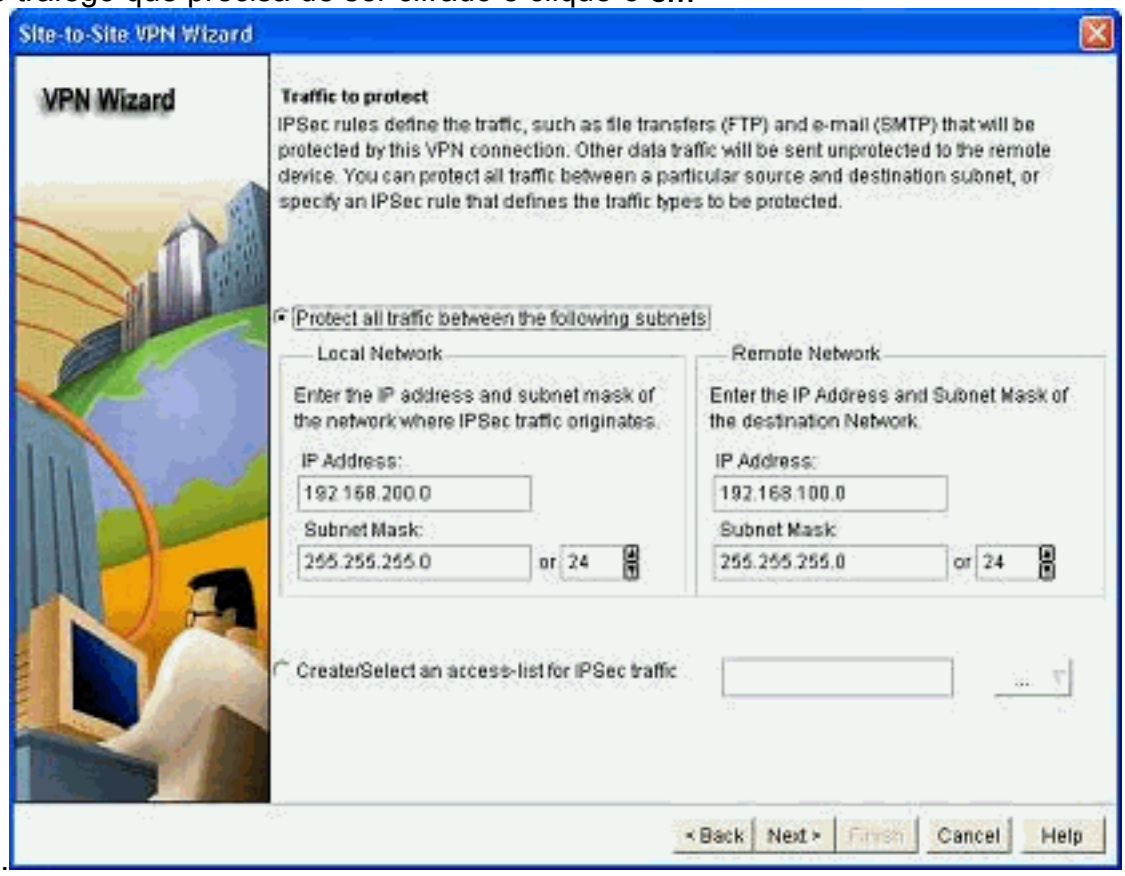
seguida.

5. Defina os detalhes do conjunto de transformação e clique-os em



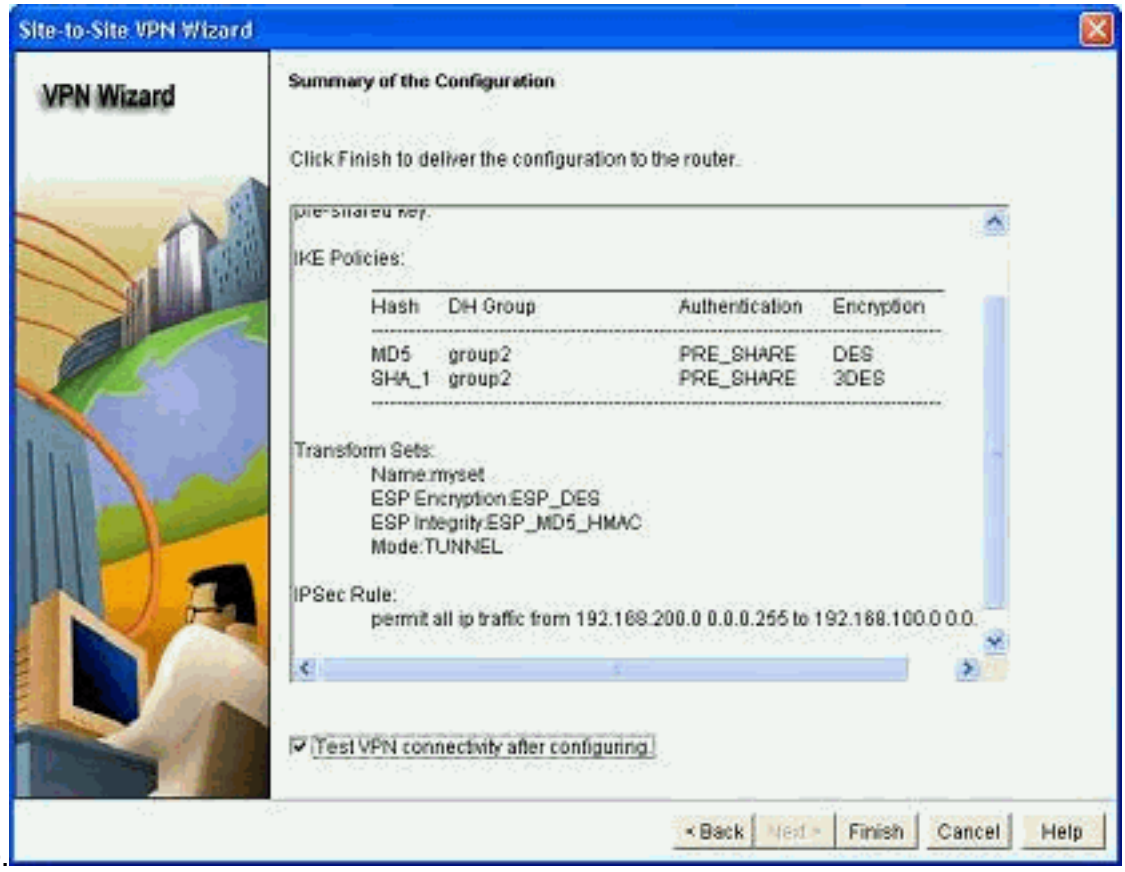
seguida.

6. Defina o tráfego que precisa de ser cifrado e clique-o **em**



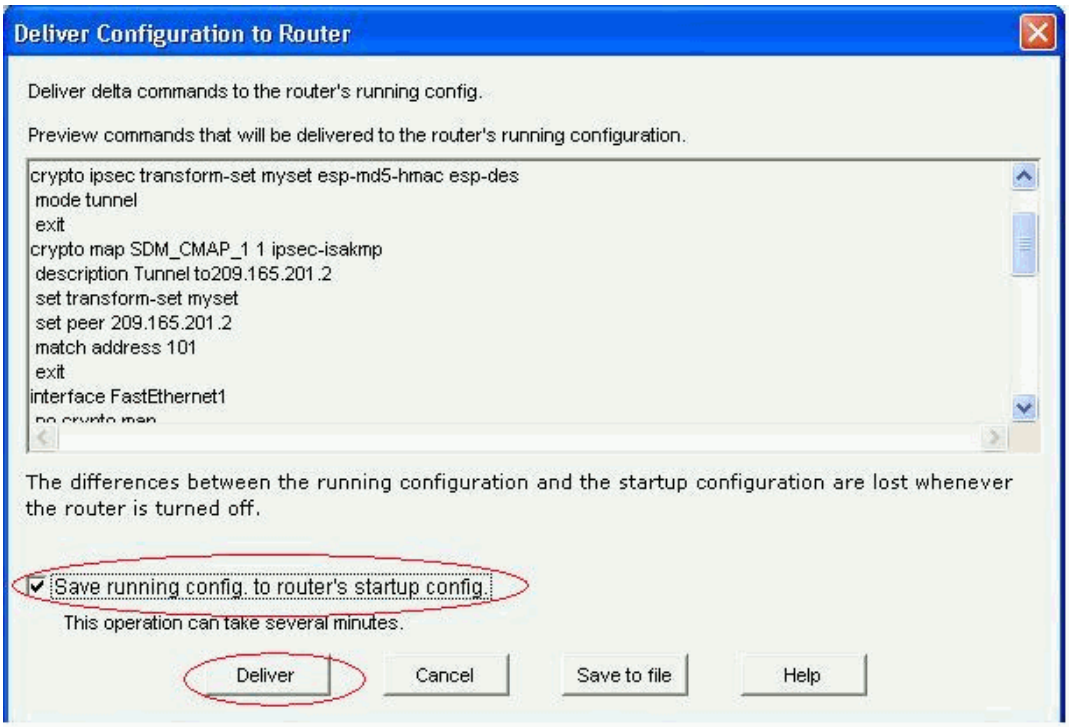
seguida.

7. Verifique o sumário da configuração IPSec cripto e clique o

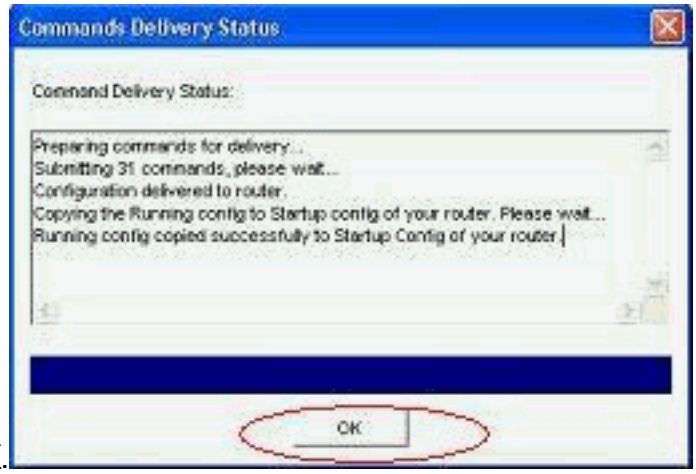


revestimento.

8. O clique **entrega** a fim enviar a configuração ao VPN Router.



9. Clique em **OK**.



Configuração de CLI

- Ciscoasa
- VPN Router

Ciscoasa

```
ciscoasa(config)#show run : Saved : ASA Version 8.0(3) !
hostname ciscoasa enable password 8Ry2YjIyt7RRXU24
encrypted names ! interface Ethernet0/0 nameif outside
security-level 0 ip address 209.165.201.2
255.255.255.224 ! interface Ethernet0/1 nameif inside
security-level 100 ip address 192.168.100.1
255.255.255.0 ! interface Ethernet0/2 shutdown no nameif
no security-level no ip address ! interface Ethernet0/3
shutdown no nameif no security-level no ip address !
interface Management0/0 shutdown no nameif no security-
level no ip address ! passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive !--- Output suppressed access-list
nonat extended permit ip 192.168.100.0 255.255.255.0
192.168.200.0 255.255.255.0 no pager mtu outside 1500
mtu inside 1500 icmp unreachable rate-limit 1 burst-size
1 asdm image disk0:/asdm-613.bin no asdm history enable
arp timeout 14400 ! !--- Define the nat-translation for
Internet users global (outside) 1 interface nat (inside)
1 192.168.100.0 255.255.255.0 ! ! !--- Define the nat-
exemption policy for VPN traffic nat (inside) 0 access-
list nonat ! route outside 0.0.0.0 0.0.0.0 209.165.201.1
1 ! timeout xlate 3:00:00 timeout conn 1:00:00 half-
closed 0:10:00 udp 0:02:00 icmp 0:00:02 timeout sunrpc
0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat
0:05:00 timeout sip 0:30:00 sip_media 0:02:00 sip-invite
0:03:00 sip-disconnect 0:02:00 timeout uauth 0:05:00
absolute dynamic-access-policy-record DfltAccessPolicy
no snmp-server location no snmp-server contact snmp-
server enable traps snmp authentication linkup linkdown
coldstart ! !--- Configure the IPsec transform-set
crypto ipsec transform-set myset esp-des esp-md5-hmac !
! !--- Configure the dynamic crypto map crypto dynamic-
map mymap 1 set transform-set myset crypto dynamic-map
mymap 1 set reverse-route crypto map dyn-map 10 IPSec-
isakmp dynamic mymap crypto map dyn-map interface
outside ! !--- Configure the phase I ISAKMP policy
crypto isakmp policy 10 authentication pre-share
encryption des hash md5 group 2 lifetime 86400 ! ! !---
Configure the default L2L tunnel group parameters
tunnel-group DefaultL2LGroup IPSec-attributes pre-
shared-key * ! class-map inspection_default match
```

```
default-inspection-traffic ! ! policy-map type inspect
dns preset_dns_map parameters message-length maximum 512
policy-map global_policy class inspection_default
inspect dns preset_dns_map inspect ftp inspect h323 h225
inspect h323 ras inspect netbios inspect rsh inspect
rtsp inspect skinny inspect esmtp inspect sqlnet inspect
sunrpc inspect tftp inspect sip inspect xdmcp ! service-
policy global_policy global prompt hostname context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e : end
ciscoasa(config)#
```

O CCP cria esta configuração no VPN Router.

VPN Router

```
VPN-Router#show run Building configuration... ! version
12.4 service timestamps debug datetime msec service
timestamps log datetime msec no service password-
encryption ! hostname VPN-Router ! ! username cisco
privilege 15 secret 5 $1$UQxM$WvwDZbfDhK3wS26C9xYns/
username test12 privilege 15 secret 5
$1$LC0U$ex3tp4hM8CYD.HJSRDfQO1 ! ! !--- Output
suppressed no aaa new-model ip subnet-zero ! ip cef !
crypto isakmp enable outside ! crypto isakmp policy 1
encrypt 3des authentication pre-share group 2 ! crypto
isakmp policy 2 hash md5 authentication pre-share group
2 ! ! crypto isakmp key cisco123 address 209.165.201.2 !
! crypto ipsec transform-set myset esp-des esp-md5-hmac
! ! crypto map SDM_CMAP_1 1 IPSec-isakmp description
Tunnel to209.165.201.2 set peer 209.165.201.2 set
transform-set myset match address 101 ! ! ! interface
BRI0 no ip address shutdown ! interface Dot11Radio0 no
ip address shutdown speed basic-1.0 basic-2.0 basic-5.5
6.0 9.0 basic-11.0 12.0 18.0 24.0 36.0 48.0 54.0
station-role root ! interface Dot11Radio1 no ip address
shutdown speed basic-6.0 9.0 basic-12.0 18.0 basic-24.0
36.0 48.0 54.0 station-role root ! interface
FastEthernet0 ip address 192.168.200.1 255.255.255.0
duplex auto speed auto ! interface FastEthernet1 ip
address dhcp duplex auto speed auto crypto map
SDM_CMAP_1 ! interface FastEthernet2 no ip address
shutdown ! interface FastEthernet3 no ip address
shutdown ! interface FastEthernet4 no ip address
shutdown ! interface FastEthernet5 no ip address
shutdown ! interface FastEthernet6 no ip address
shutdown ! interface FastEthernet7 no ip address
shutdown ! interface FastEthernet8 no ip address
shutdown ! interface FastEthernet9 no ip address
shutdown ! interface Vlan1 no ip address ! ip classless
ip route 0.0.0.0 0.0.0.0 209.165.200.1 ! ! !--- Output
suppressed ! ip http server ip http authentication local
ip http secure-server ! access-list 100 permit ip
0.0.0.0 255.255.255.0 0.0.0.0 255.255.255.0 access-list
101 remark CCP_ACL Category=4 access-list 101 remark
IPSEC Rule access-list 101 permit ip 192.168.200.0
0.0.0.255 192.168.100.0 0.0.0.255 ! ! ! ! control-plane
! ! line con 0 line aux 0 line vty 0 4 privilege level
15 login local transport input telnet ssh line vty 5 15
privilege level 15 login local transport input telnet
ssh ! no scheduler allocate end
```

Verificar

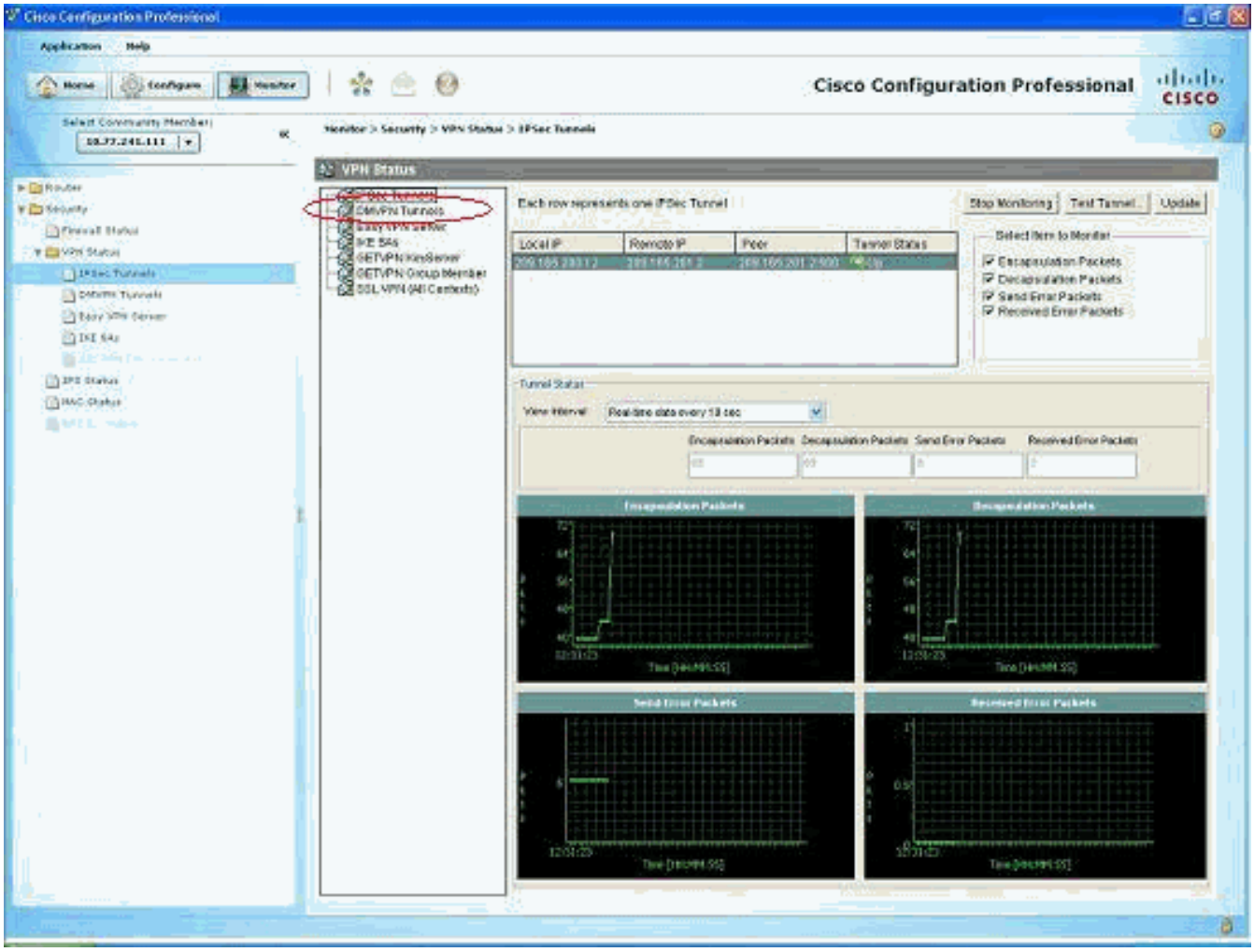
Use esta seção para confirmar se a sua configuração funciona corretamente.

A Output Interpreter Tool (apenas para clientes registrados) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

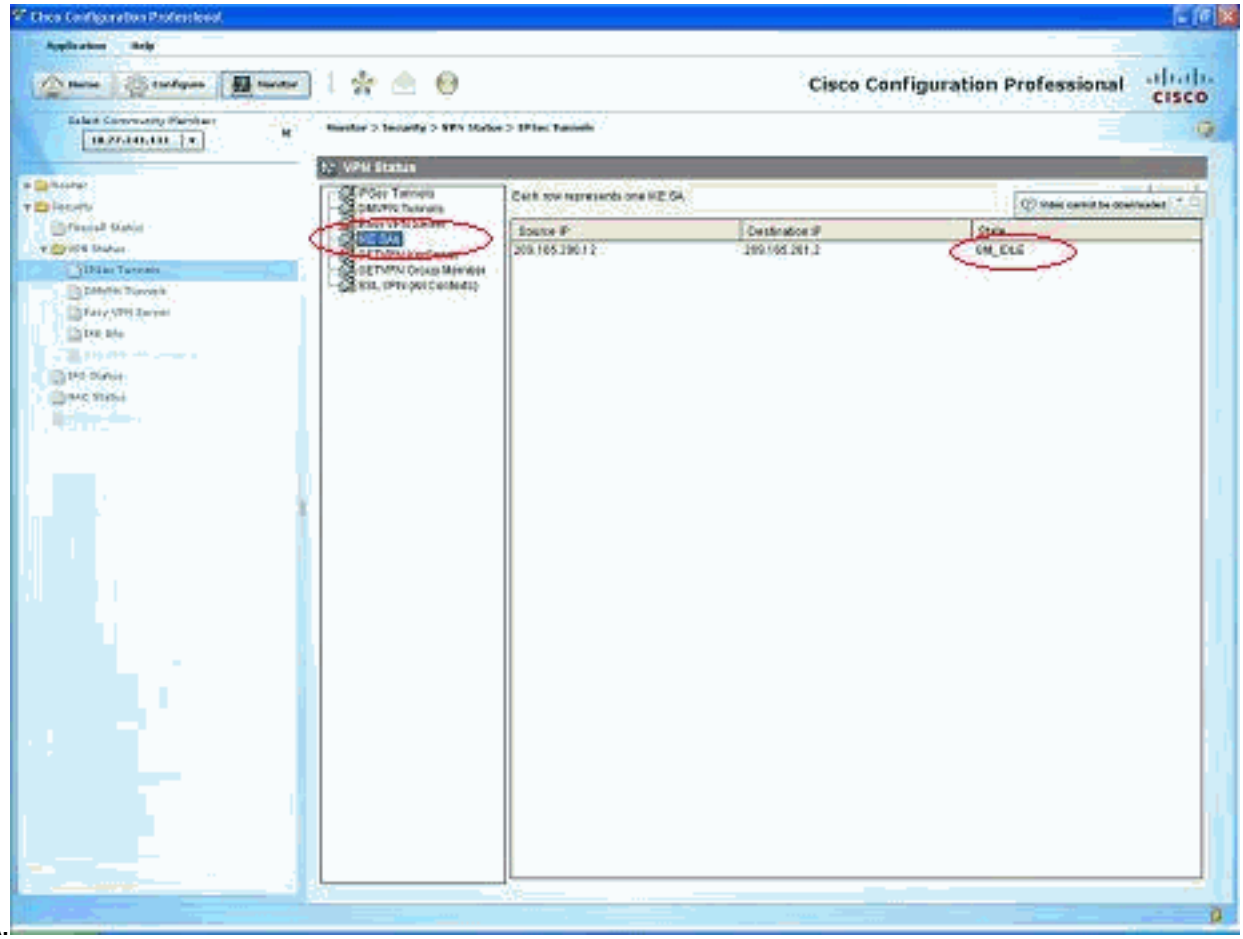
- Verificando os parâmetros do túnel com o CCP
- Verificando o status de túnel com ASA CLI
- Verificando os parâmetros do túnel através do roteador CLI

Verifique parâmetros do túnel com o CCP

- Monitore as passagens do tráfego através do túnel de IPsec.



- Monitore o estado da fase MIM ISAKMP

SA. 

Verifique o status de túnel com ASA CLI

- Verifique o estado da fase MIM ISAKMP SA.`ciscoasa#`**`show crypto isakmp sa`** `Active SA: 1 Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey) Total IKE SA: 1 1 IKE Peer: 209.165.200.12 Type : L2L Role :` **`responder`** `Rekey : no State :` **`MM_ACTIVE`** `ciscoasa#`

  Nota: Observe o papel para ser o que responde, que indica que o iniciador deste túnel é no extremo oposto, por exemplo, o VPN Router.
- Verifique os parâmetros IPSEC SA da fase II.`ciscoasa#`**`show crypto ipsec sa`** `interface: outside Crypto map tag: mymap, seq num: 1, local addr: 209.165.201.2` **`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: 209.165.200.12` **`#pkts encaps: 29, #pkts encrypt: 29, #pkts digest: 29 #pkts decaps: 29, #pkts decrypt: 29, #pkts verify: 29`** `#pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 29, #pkts comp failed: 0, #pkts decomp failed: 0 #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0 #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0 #send errors: 0, #recv errors: 0 local crypto endpt.: 209.165.201.2, remote crypto endpt.: 209.165.200.12 path mtu 1500, IPSec overhead 58, media mtu 1500 current outbound spi: E7B37960 inbound esp sas: spi: 0xABB49C64 (2880740452) transform: esp-des esp-md5-hmac none in use settings ={L2L, Tunnel, } slot: 0, conn_id: 4096, crypto-map: mymap sa timing: remaining key lifetime (kB/sec): (4274997/3498) IV size: 8 bytes replay detection support: Y outbound esp sas: spi: 0xE7B37960 (3887298912) transform: esp-des esp-md5-hmac none in use settings ={L2L, Tunnel, } slot: 0, conn_id: 4096, crypto-map: mymap sa timing: remaining key lifetime (kB/sec): (4274997/3498) IV size: 8 bytes replay detection support: Y`

Verifique os parâmetros do túnel através do roteador CLI

- Verifique o estado da fase MIM ISAKMP SA.`VPN-Router#`**`show crypto isakmp sa`** `dst src state conn-id slot status 209.165.201.2 209.165.200.12` **`QM_IDLE`** `1 0` **`ACTIVE`**
- Verifique os parâmetros IPSEC SA da fase II.`VPN-Router#`**`show crypto ipsec sa`** `interface:`

```
FastEthernet1 Crypto map tag: SDM_CMAP_1, local addr 209.165.200.12 protected vrf: (none)
local ident (addr/mask/prot/port): (192.168.200.0/255.255.255.0/0/0) remote ident
(addr/mask/prot/port): (192.168.100.0/255.255.255.0/0/0) current_peer 209.165.201.2 port 500
PERMIT, flags={origin_is_acl,} #pkts encaps: 39, #pkts encrypt: 39, #pkts digest: 39 #pkts
decaps: 39, #pkts decrypt: 39, #pkts verify: 39 #pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0 #pkts not decompressed: 0, #pkts decompress
failed: 0 #send errors 6, #recv errors 0 local crypto endpt.: 209.165.200.12, remote crypto
endpt.: 209.165.201.2 path mtu 1500, ip mtu 1500 current outbound spi:
0xABB49C64(2880740452) inbound esp sas: spi: 0xE7B37960(3887298912) transform: esp-des esp-
md5-hmac , in use settings ={Tunnel, } conn id: 2001, flow_id: C18XX_MBRD:1, crypto map:
SDM_CMAP_1 sa timing: remaining key lifetime (k/sec): (4481818/3375) IV size: 8 bytes replay
detection support: Y Status: ACTIVE inbound ah sas: inbound pcp sas: outbound esp sas: spi:
0xABB49C64(2880740452) transform: esp-des esp-md5-hmac , in use settings ={Tunnel, } conn
id: 2002, flow_id: C18XX_MBRD:2, crypto map: SDM_CMAP_1 sa timing: remaining key lifetime
(k/sec): (4481818/3371) IV size: 8 bytes replay detection support: Y Status: ACTIVE outbound
ah sas: outbound pcp sas:
```

Troubleshooting

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

- Rasgando para baixo as conexões criptos existentes.`ciscoasa#clear crypto ipsec sa ciscoasa#clear crypto isakmp sa VPN-Router#clear crypto isakmp`
- Use **comandos debug** a fim pesquisar defeitos os problemas com túnel VPN.**Nota:** Se você permite a eliminação de erros, esta puder interromper o funcionamento do roteador quando condições de carga elevada da experiência das inter-redes. Use comandos debug com cuidado. Geralmente, recomenda-se que esses comandos sejam somente utilizados sob a coordenação do representante de suporte técnico do roteador quando Troubleshooting problemas específicos.`ciscoasa#debug crypto engine ciscoasa#debug crypto isakmp ciscoasa#debug crypto IPSec ciscoasa# VPN-Router#debug crypto engine Crypto Engine debugging is on VPN-Router#debug crypto isakmp Crypto ISAKMP debugging is on VPN-Router#debug crypto ipsec Crypto IPSEC debugging is on VPN-Router#`

Refira o isakmp do debug crypto na compreensão e os comandos debug de utilização para obter mais informações sobre de debugam commangs.

Informações Relacionadas

- Página de Suporte de Negociação IPSec/Protocolos IKE
- Documentação para o OS Software da ferramenta de segurança de Cisco ASA
- A maioria de soluções do Troubleshooting do IPSec comum VPN
- Solicitações de Comentários (RFCs)
- Suporte Técnico e Documentação - Cisco Systems