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

Contents

Introduction

Este documento fornece uma configuração de exemplo de como habilitar o PIX/ASA Security Appliance a aceitar conexões IPsec dinâmicas do roteador Cisco IOS®. Neste cenário, o túnel de IPsec é estabelecido quando o túnel é iniciado somente da extremidade do Roteador. O ASA não pôde iniciar um túnel VPN devido à configuração de IPSec dinâmica.

Essa configuração permite que o PIX Security Appliance crie um túnel dinâmico de LAN para LAN (L2L) IPsec com um roteador VPN remoto. Esse roteador recebe dinamicamente seu endereço IP público externo de seu provedor de serviços de Internet. O Dynamic Host Configuration Protocol (DHCP) fornece esse mecanismo para alocar endereços IP dinamicamente do provedor. Isso permite que os endereços IP sejam reutilizados quando os hosts não precisarem mais deles.

A configuração no Roteador é feita com o uso do Cisco Configuration Professional (CCP). O CCP é uma ferramenta de gerenciamento de dispositivos baseada em GUI que permite configurar roteadores baseados em Cisco IOS. Consulte Configuração Básica do Roteador Usando o Cisco Configuration Professional para obter mais informações sobre como configurar um roteador com CCP.

Consulte VPN site a site (L2L) com ASA para obter mais informações e exemplos de configuração no estabelecimento de túnel IPsec que usam ASA e Cisco IOS Routers.

Consulte VPN site a site (L2L) com IOS para obter mais informações e um exemplo de configuração no estabelecimento de túnel de IPSec dinâmico com o uso de PIX e Cisco IOS Router.

Prerequisites

Requirements

Antes de tentar essa configuração, verifique se o ASA e o roteador têm conectividade com a Internet para estabelecer o túnel 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 Cisco ASA 5510 versão 8.0.3

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

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

Informações de Apoio

Neste cenário, a rede 192.168.100.0 está atrás do ASA e a rede 192.168.200.0 está atrás do Cisco IOS Router. Pressupõe-se que o Roteador obtenha seu endereço público através do DHCP de seu ISP. Como isso coloca um problema na configuração de um peer estático na extremidade do ASA, você precisa abordar o modo de configuração de criptografia dinâmica para estabelecer um túnel site a site entre o ASA e o Cisco IOS Router.

Os usuários da Internet na extremidade do ASA são convertidos para o endereço IP de sua interface externa. Pressupõe-se que o NAT não esteja configurado na extremidade do roteador do Cisco IOS.

Agora, estes são os principais passos a serem configurados na extremidade do ASA para estabelecer um túnel dinâmico:

1. Fase 1 Configuração relacionada ao ISAKMP
2. configuração de isenção de NAT
3. Configuração de mapa de criptografia dinâmico

O roteador do Cisco IOS tem um mapa de criptografia estático configurado porque se supõe que o ASA tenha um endereço IP público estático. Esta é a lista dos principais passos a serem

configurados na extremidade do Cisco IOS Router para estabelecer um túnel IPSEC dinâmico.

1. Fase 1 Configuração relacionada ao ISAKMP
2. Configuração relacionada ao mapa de criptografia estático

Essas etapas são descritas em detalhes nessas configurações.

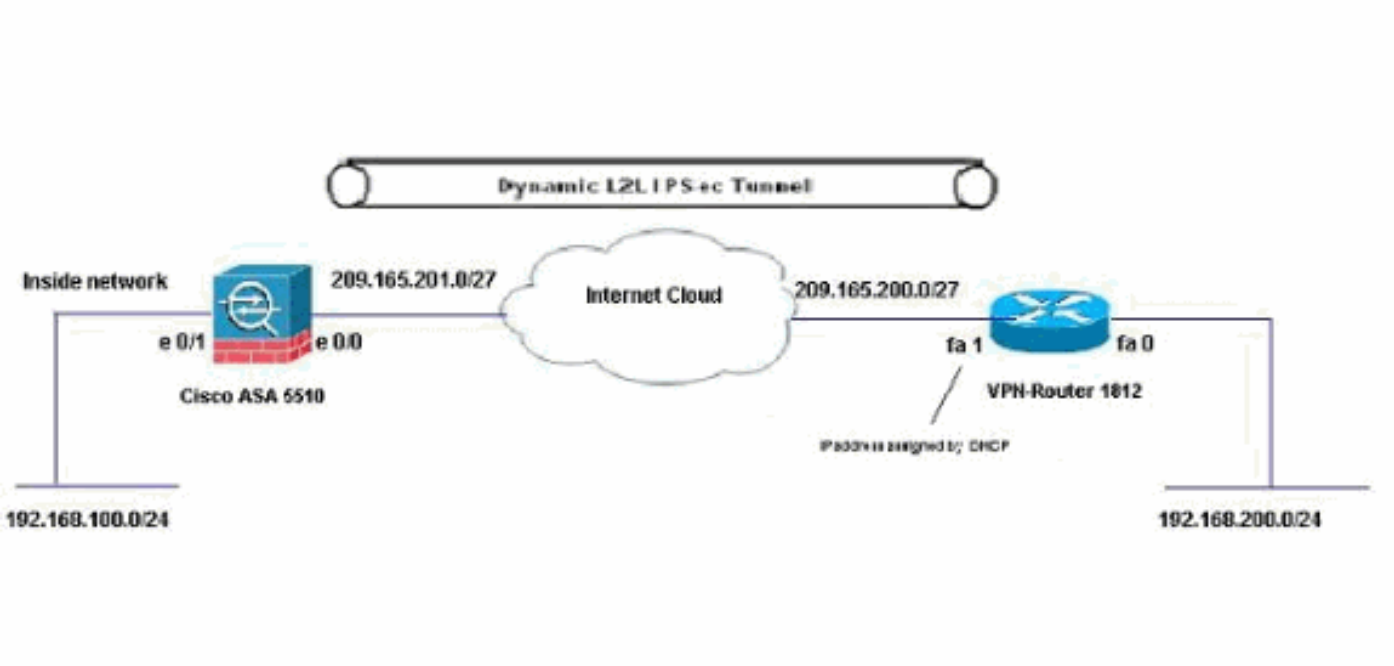
Configurar

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

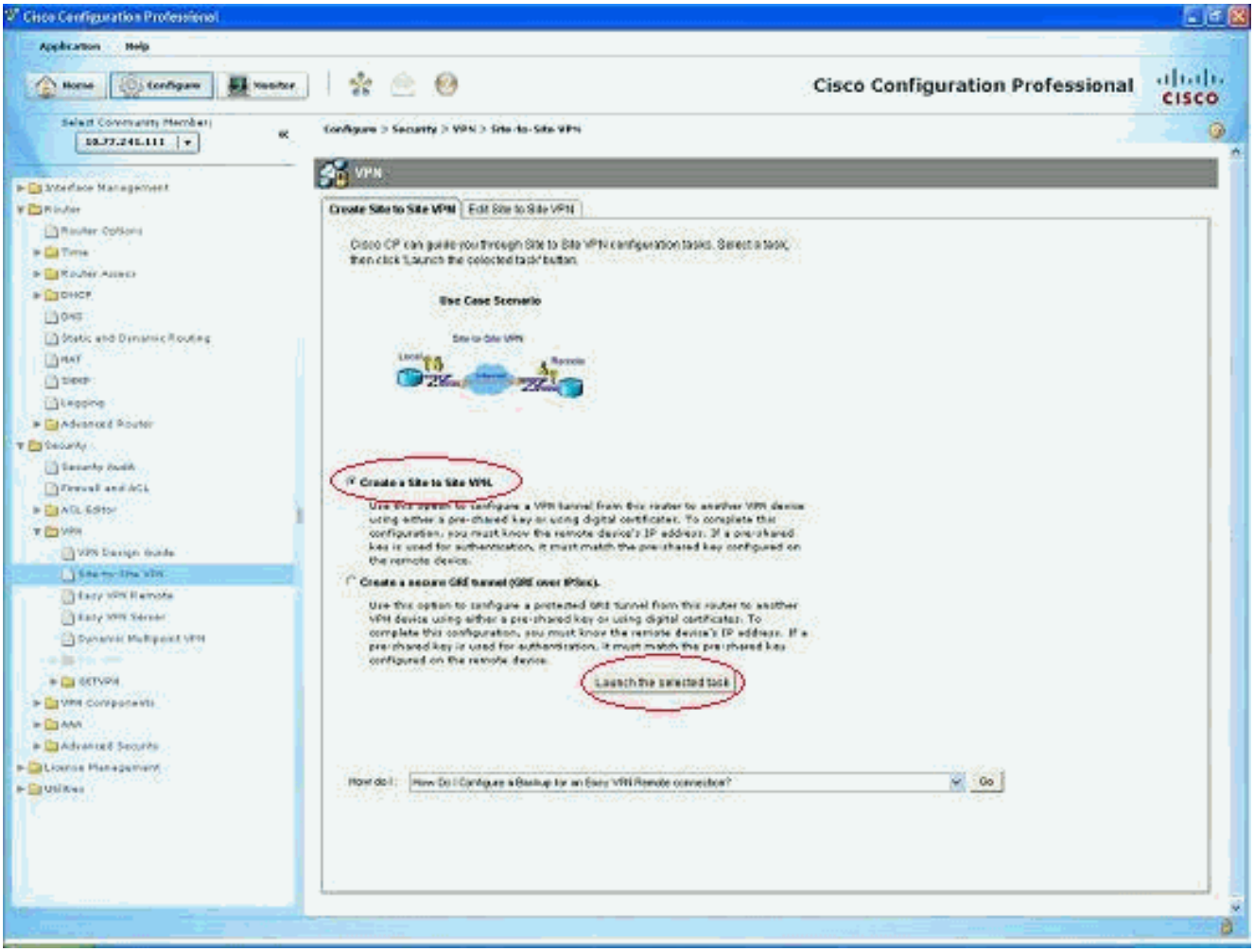
Este documento utiliza a seguinte configuração de rede:



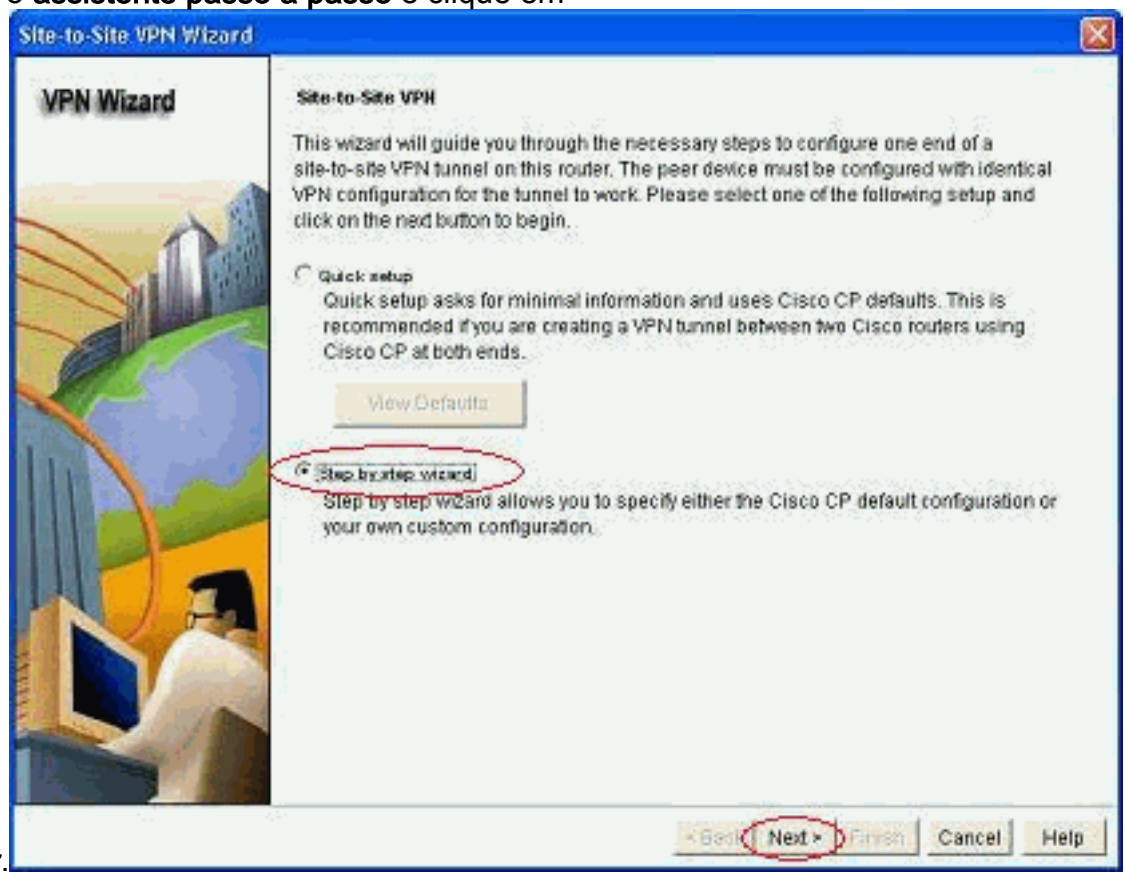
Configurações

Esta é a configuração de VPN IPsec no VPN-Router com CCP. Conclua estes passos:

1. Abra o aplicativo CCP e escolha **Configure > Security > VPN > Site to Site VPN**. Clique na **guia Iniciar selecionada**.

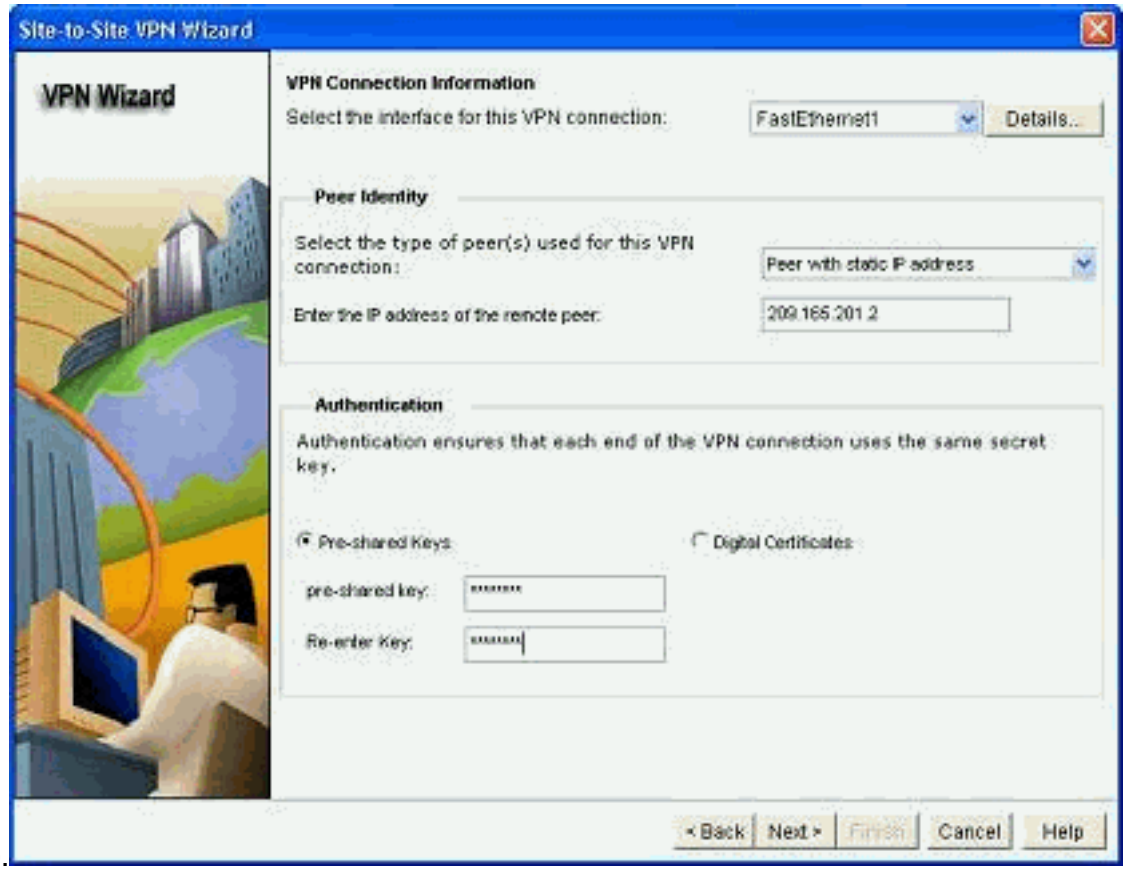


2. Escolha o **assistente passo a passo** e clique em **Avançar**.

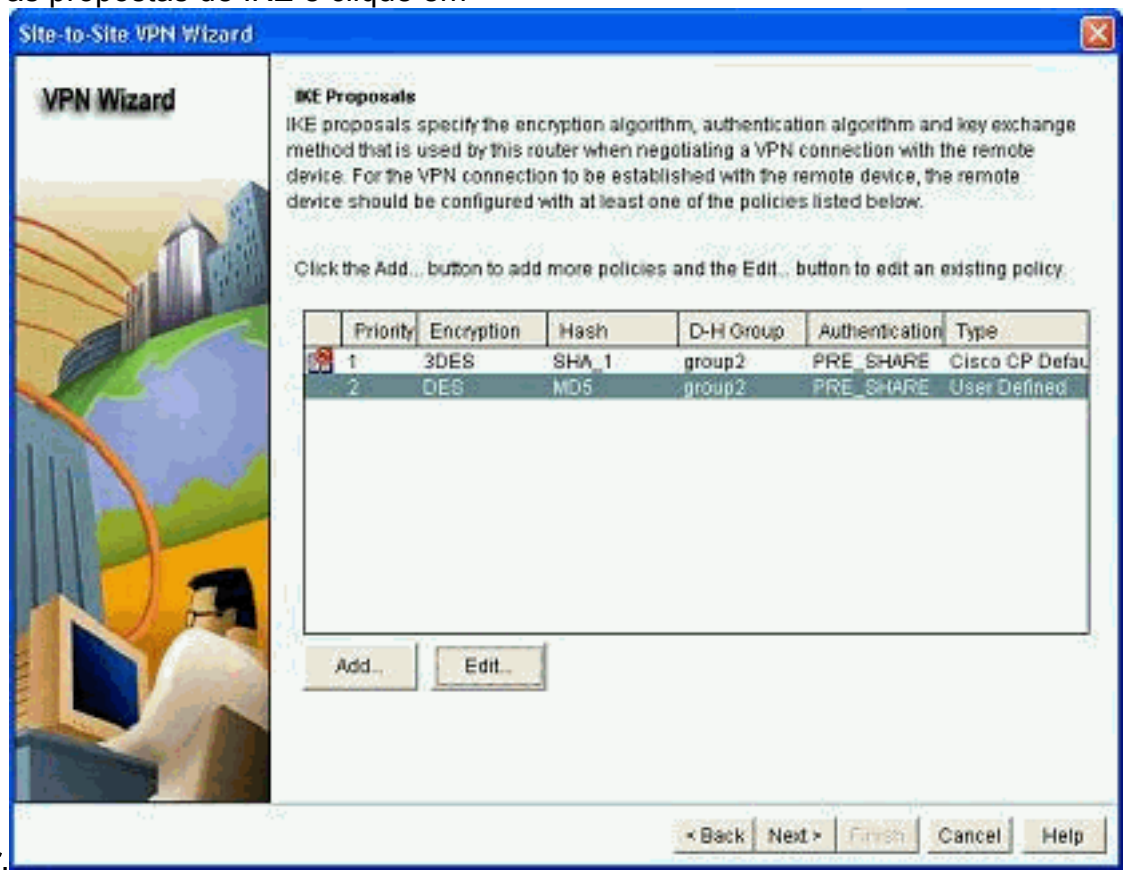


3. Preencha o endereço IP do peer remoto junto com os detalhes da

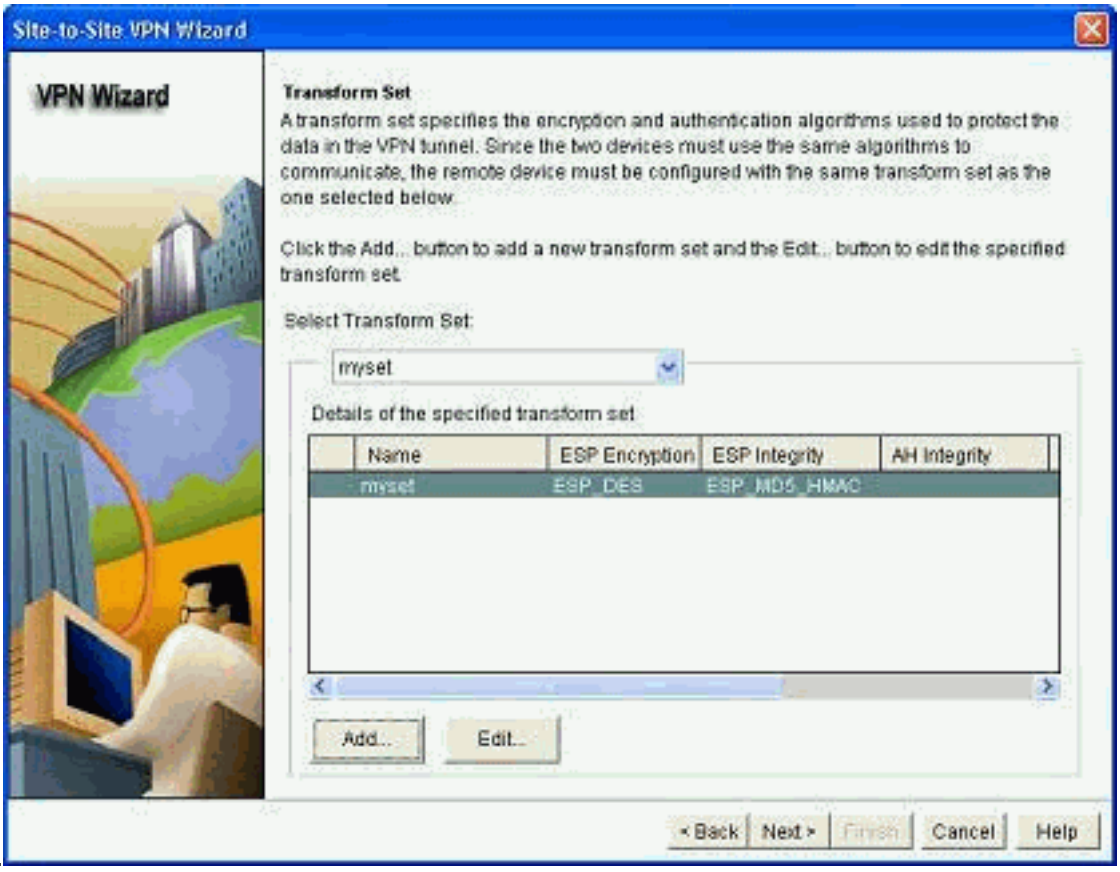
autenticação.



4. Escolha as propostas de IKE e clique em **Avançar**.

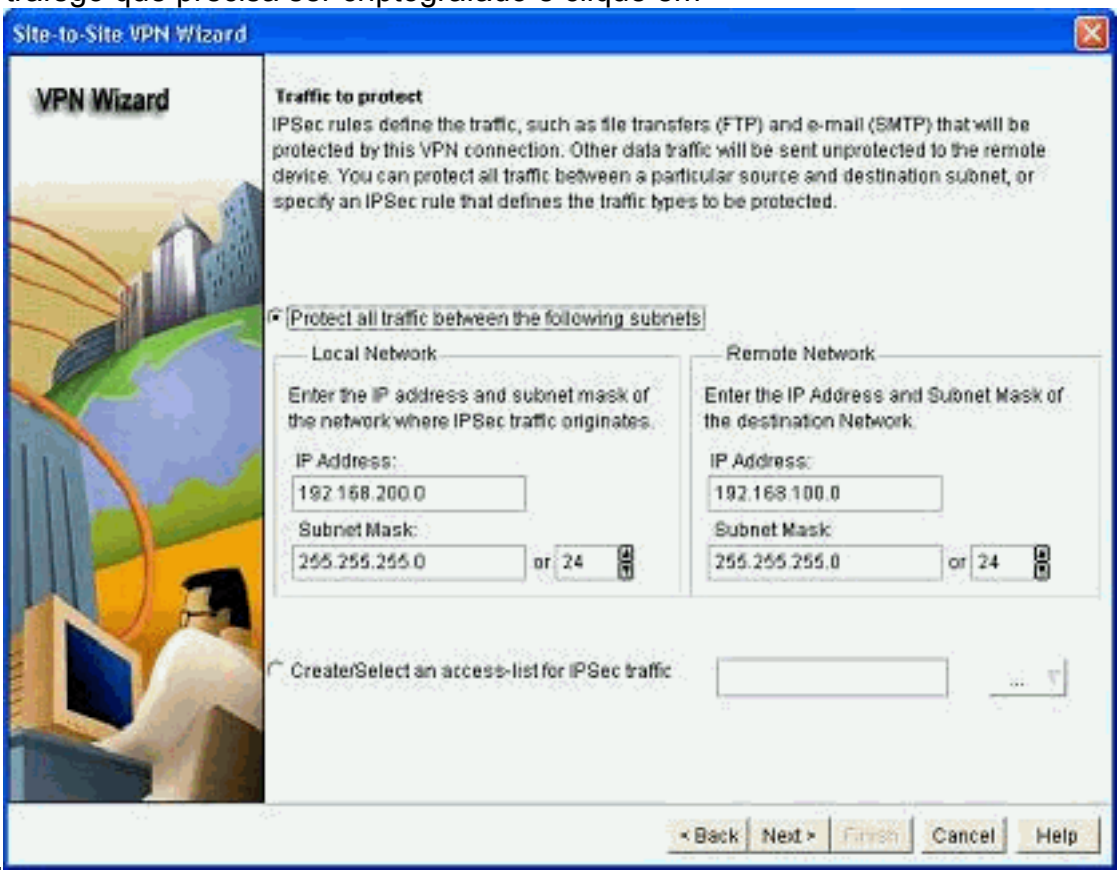


5. Defina os detalhes do conjunto de transformações e clique em



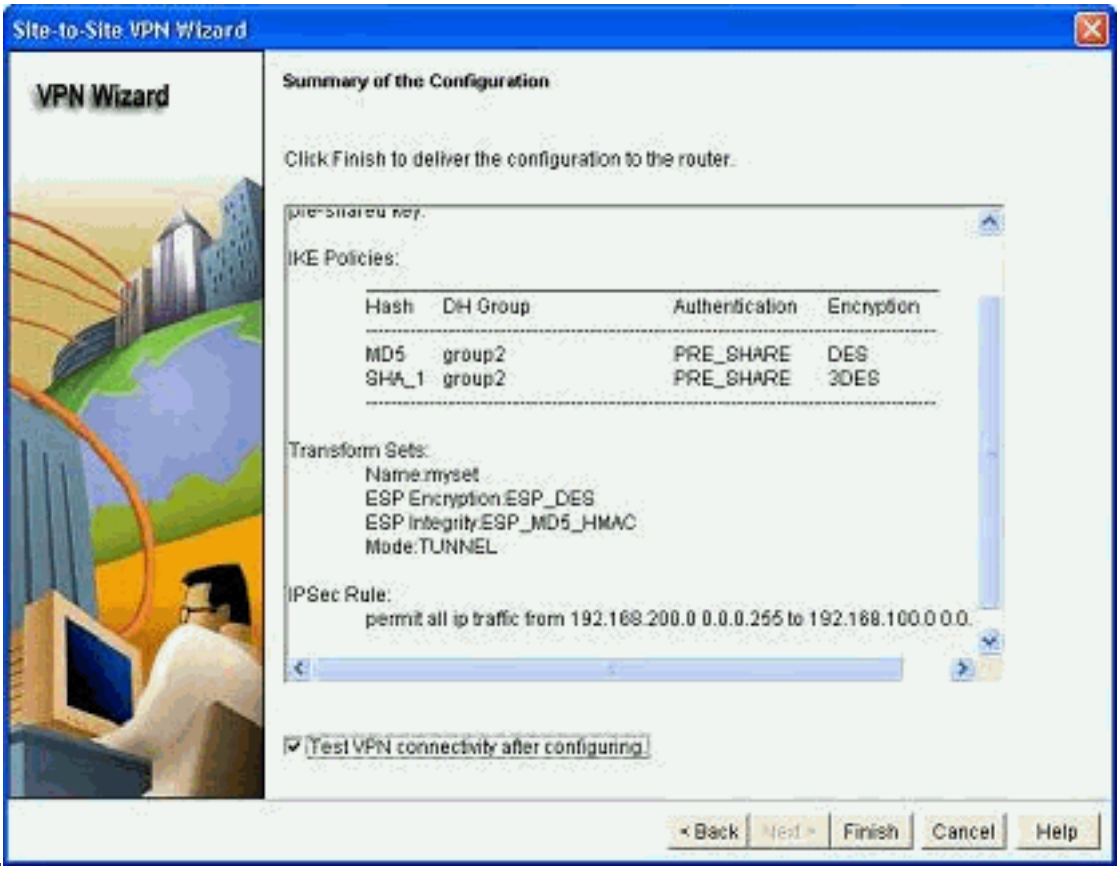
Avançar.

6. Defina o tráfego que precisa ser criptografado e clique em



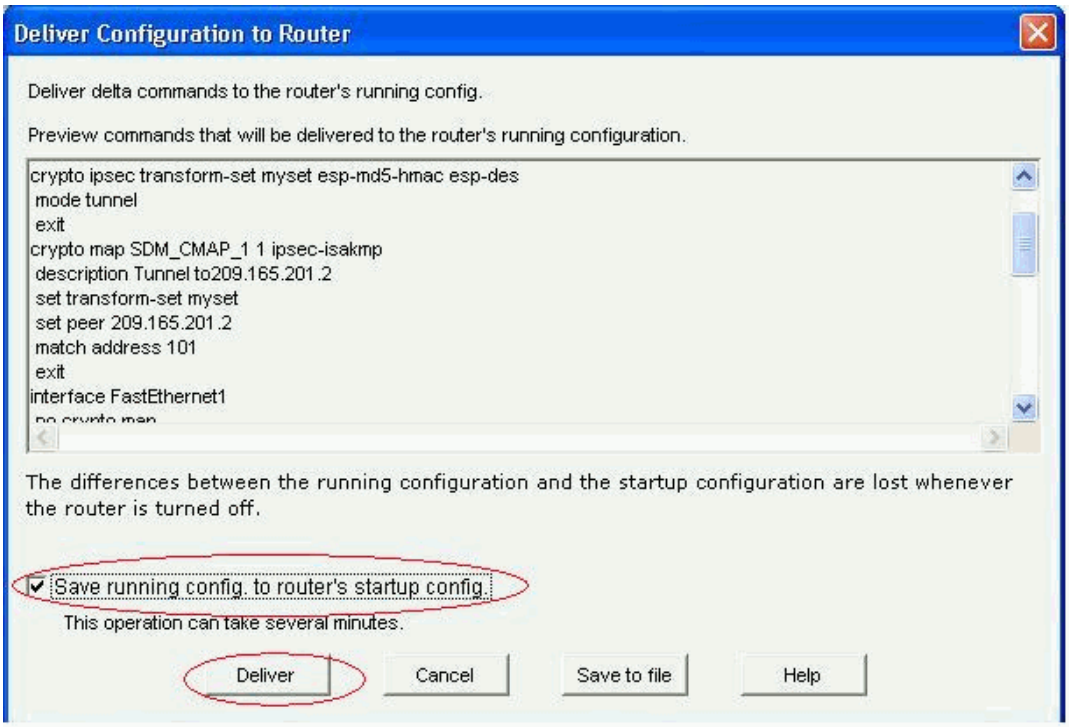
Avançar.

7. Verifique o resumo da configuração de criptografia IPsec e clique em

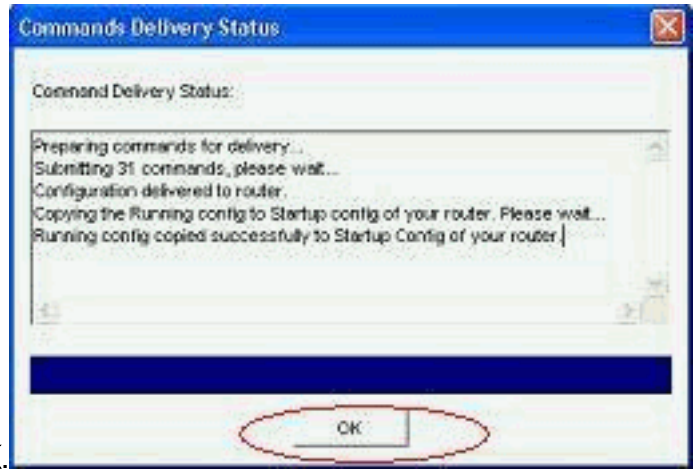


Concluir.

8. Clique em **Deliver** para enviar a configuração para o roteador VPN.



9. Click **OK**.



Configuração de CLI

- Ciscoasa
- Roteador VPN

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 essa configuração no roteador VPN.

Roteador VPN

```
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

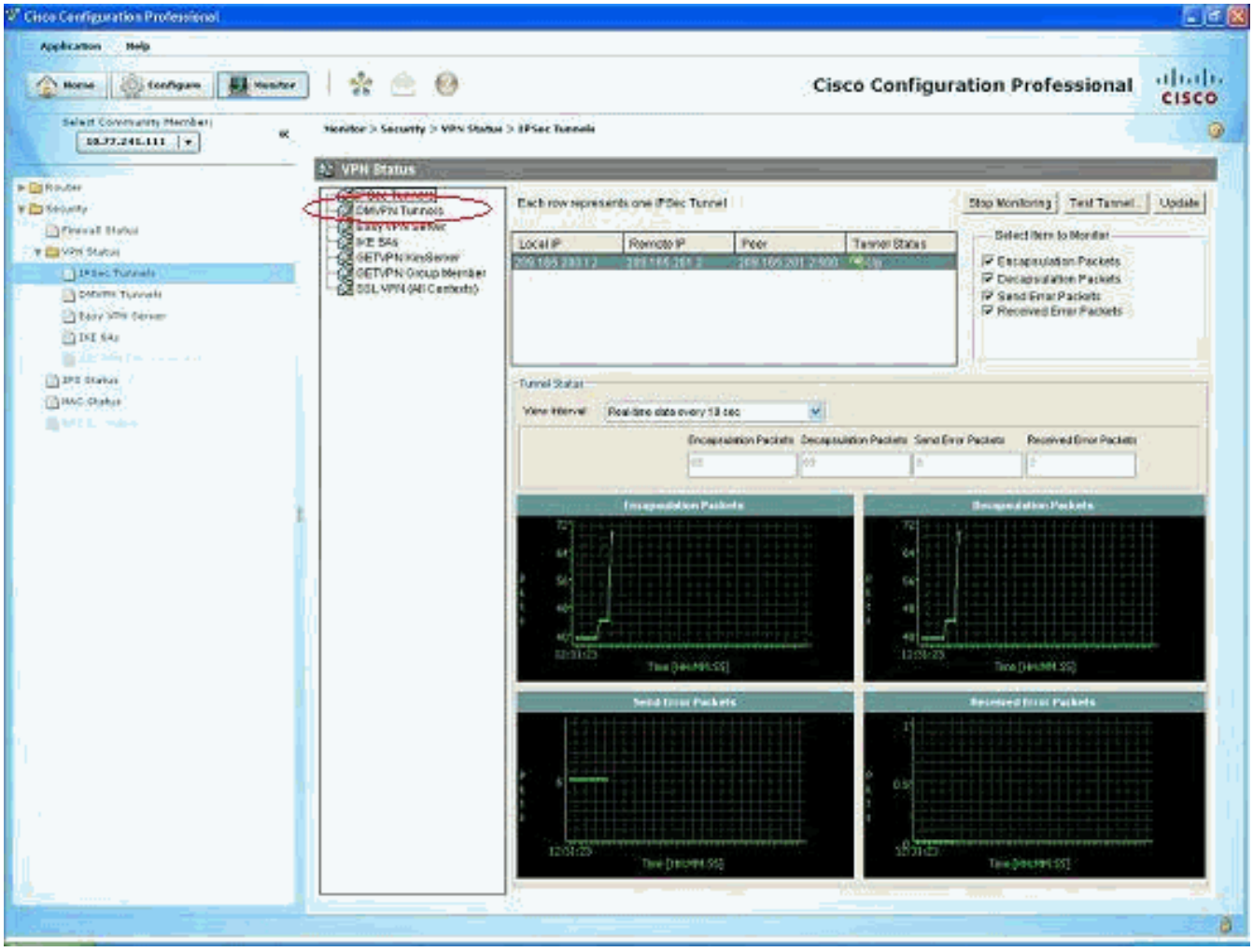
Use esta seção para confirmar se a sua configuração funciona corretamente.

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

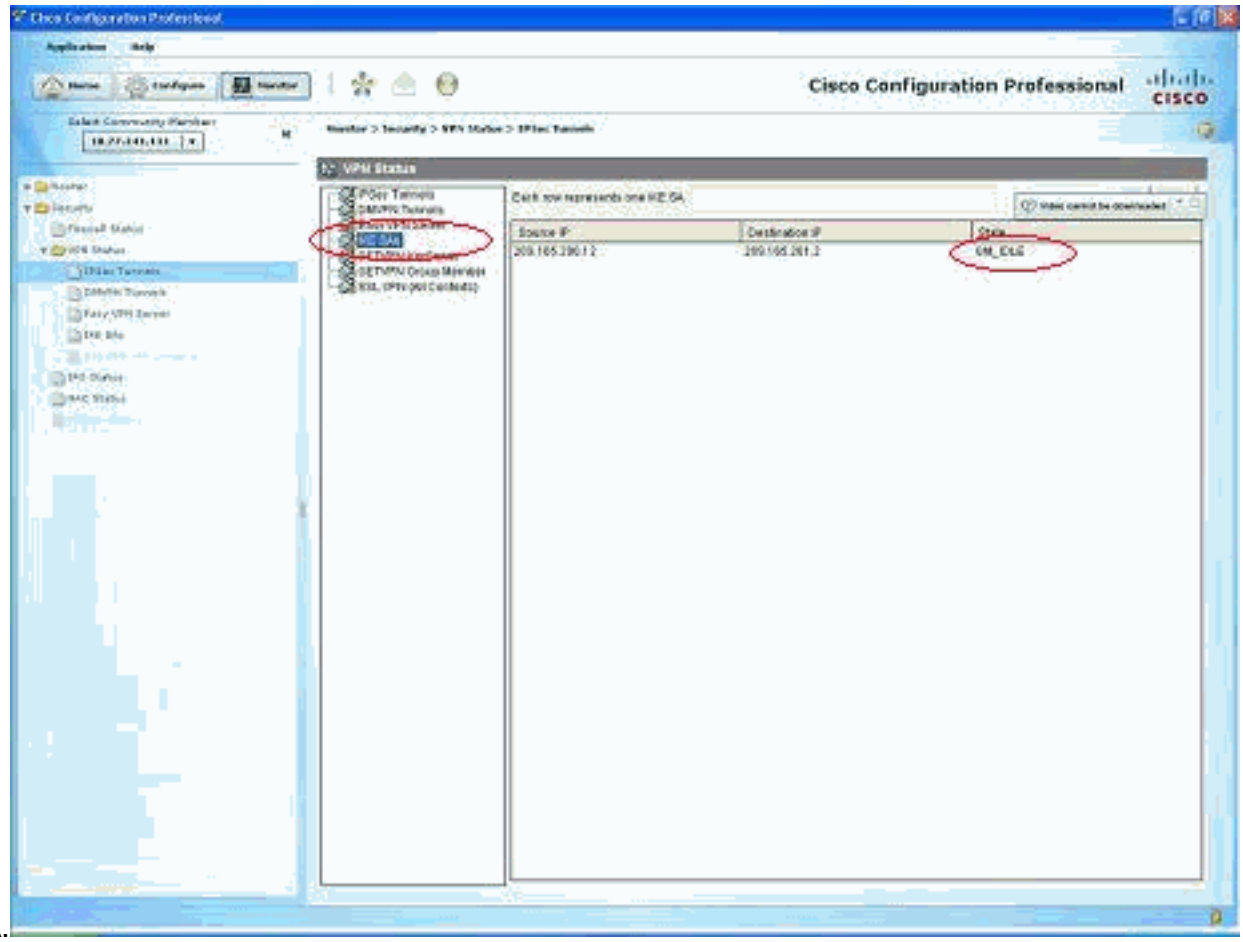
- Verificação dos parâmetros de túnel através do CCP
- Verificando o status do túnel através da CLI do ASA
- Verificação dos parâmetros de túnel através da CLI do roteador

Verificar parâmetros de túnel através do CCP

- Monitore o tráfego que passa pelo túnel IPsec.



- Monitorar o estado da fase I ISAKMP SA.



Verificar o status do túnel através da CLI do ASA

- Verifique o status da fase I 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#
```

Observação: observe a Função para responder, que indica que o iniciador deste túnel está na outra extremidade, por exemplo, o VPN-Roteador.

- Verifique os parâmetros da fase II IPSEC SA.

```
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
```

Verificar os parâmetros do túnel por meio da CLI do roteador

- Verifique o status da fase I 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 da fase II IPSEC SA.

```
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:
```

Troubleshoot

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

- Tocando as conexões de criptografia existentes.

```
ciscoasa#clear crypto ipsec sa
ciscoasa#clear crypto isakmp sa
```

```
VPN-Router#clear crypto isakmp
```

- Use os comandos **debug** para solucionar problemas com o túnel VPN.**Observação:** se você habilitar a depuração, isso poderá interromper a operação do roteador quando as internetworks tiverem condições de alta carga.**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#
```

Consulte debug crypto isakmp em Understanding and Using debug Commands para obter mais informações sobre comandos debug.

Informações Relacionadas

- Página de Suporte de Negociação IPSec/Protocolos IKE
- Documentação do software do SO do Cisco ASA Security Appliance
- Soluções de problemas mais comuns de IPSEC VPN
- Solicitações de Comentários (RFCs)