使用CCP配置示例在静态寻址的ASA和一个动态地寻址的Cisco IOS路由器之间的动态IPSec隧道

Contents

Introduction

本文为如何给enable (event)接受从Cisco IOS路由器的动态IPSec连接的PIX/ASA安全工具提供一配置示例。在此方案中，当隧道从路由器末端仅被发起时， IPSec隧道设立。ASA不能发起VPN隧道由于动态IPSec配置。

通过此配置，PIX 安全设备可以创建到远程 VPN 路由器的动态 IPsec LAN 到 LAN (L2L) 隧道。此路由器从其互联网服务提供商动态地收到其外部公共IP地址。动态主机配置协议 (DHCP) 可提供此机制，以便动态地分配提供商提供的 IP 地址。这样，当主机不再需要这些 IP 地址时，就可以重用它们。

在路由器的配置执行与使用Cisco Configuration Professional (CCP)。CCP是允许您配置基于Cisco IOS的路由器的一个基于GUI的设备管理管理工具。参考基本路由器配置使用Cisco Configuration Professional关于如何用CCP配置路由器的更多信息。

参考Site to Site VPN (L2L)与使用ASA和Cisco IOS路由器的更多inormation和配置示例的ASA在IPsec隧道建立。

参考Site to Site VPN (L2L)与IOS欲知更多信息和配置示例关于动态IPSec隧道建立与使用PIX和Cisco IOS路由器。

Prerequisites

Requirements

在您尝试此配置前，请保证ASA和路由器有互联网连通性为了设立IPSec隧道。

Components Used

本文档中的信息基于以下软件和硬件版本：

- Cisco IOS运行Cisco IOS Software Release 12.4的Router1812
- Cisco ASA 5510软件版本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

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

背景信息

在此方案中， 192.168.100.0网络是在ASA和192.168.200.0网络后是在Cisco IOS路由器后。假设，路由器通过DHCP得到其公共地址从其ISP。因为这提出在一个静态对等体的配置的一个问题ASA末端的，您需要接近动态加密配置方式设立在ASA和Cisco IOS路由器之间的一条站点到站点隧道。

ASA末端的互联网用户被转换对其外部接口的IP地址。假设， NAT在Cisco IOS路由器末端没有被配置。

现在这些是在ASA末端将配置的主要步骤为了设立动态隧道：

1. 阶段1 ISAKMP相关的配置
2. nat免税配置
3. 动态加密映射配置

因为ASA假设有一个静态公共IP地址， Cisco IOS路由器有被配置的一个静态加密映射。现在这是在Cisco IOS路由器末端将配置的主要步骤列表设立动态IPSec隧道。

1. 阶段1 ISAKMP相关的配置
2. 静态加密映射相关的配置

这些步骤在这些配置详细描述。

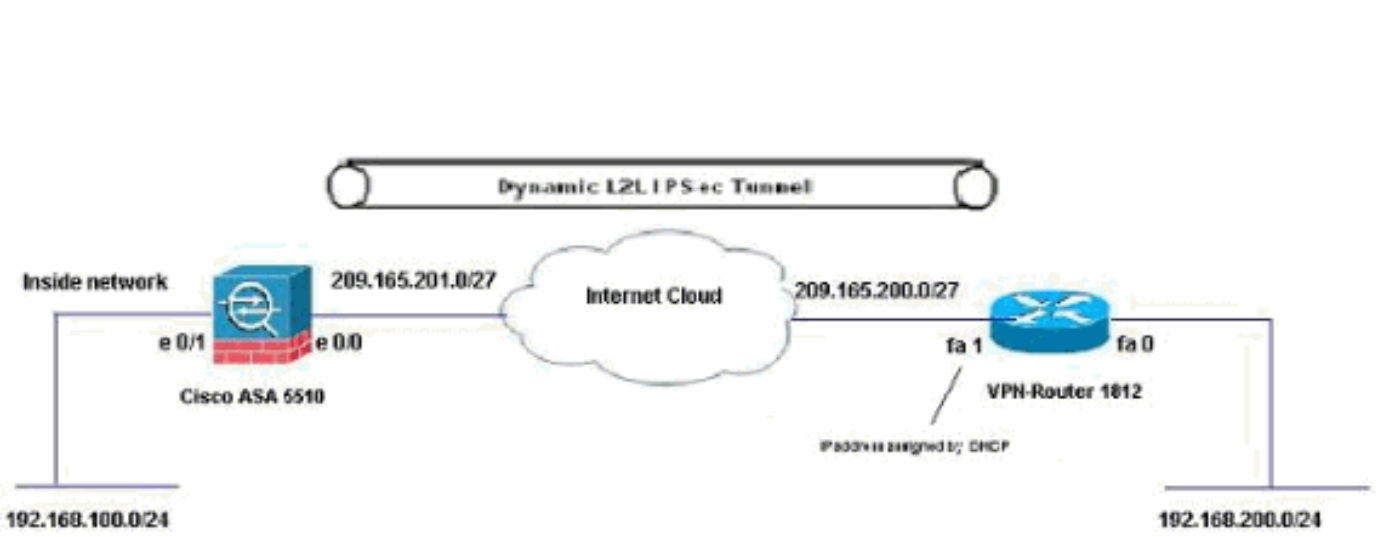
Configure

本部分提供有关如何配置本文档所述功能的信息。

Note: 使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

Network Diagram

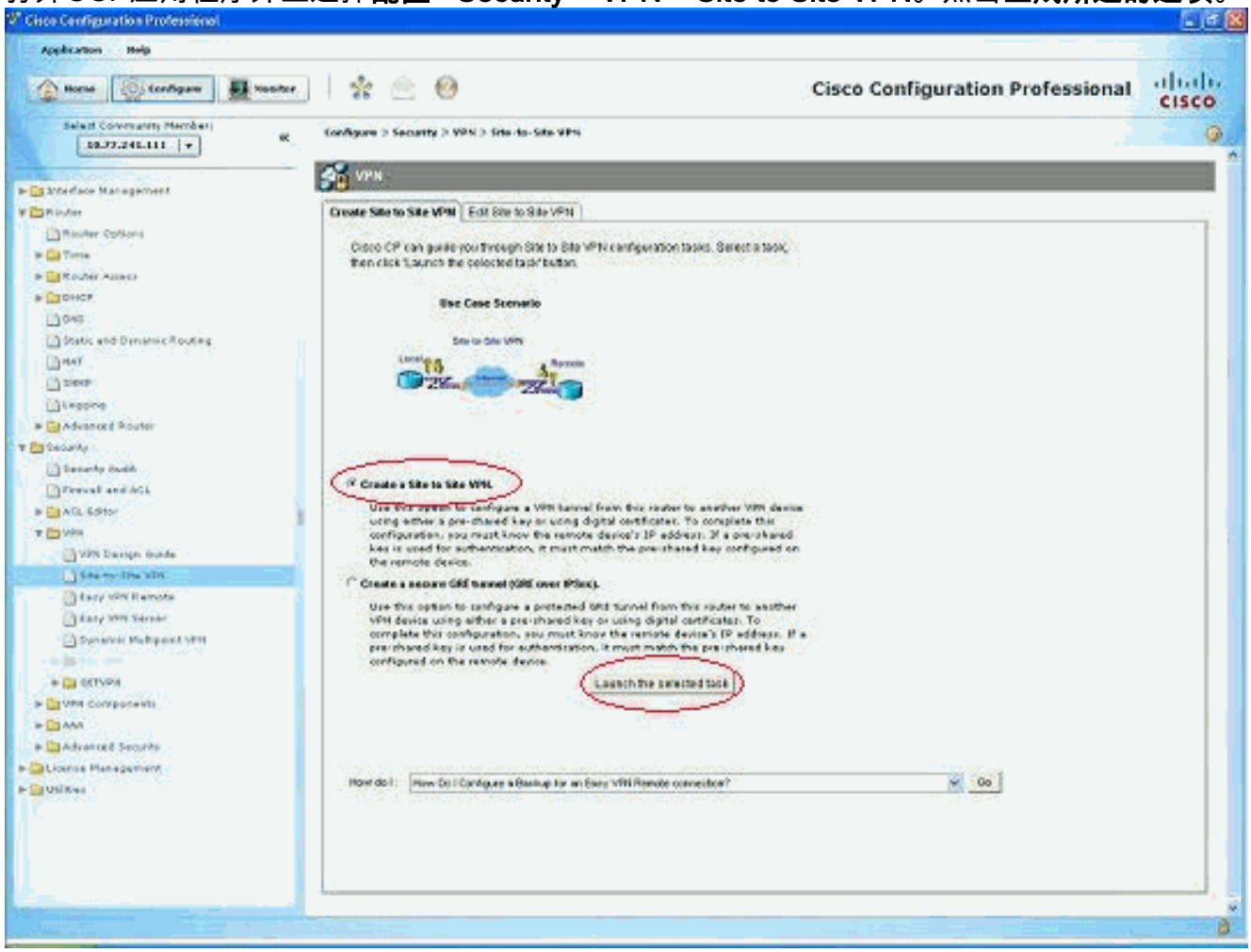
本文档使用以下网络设置：



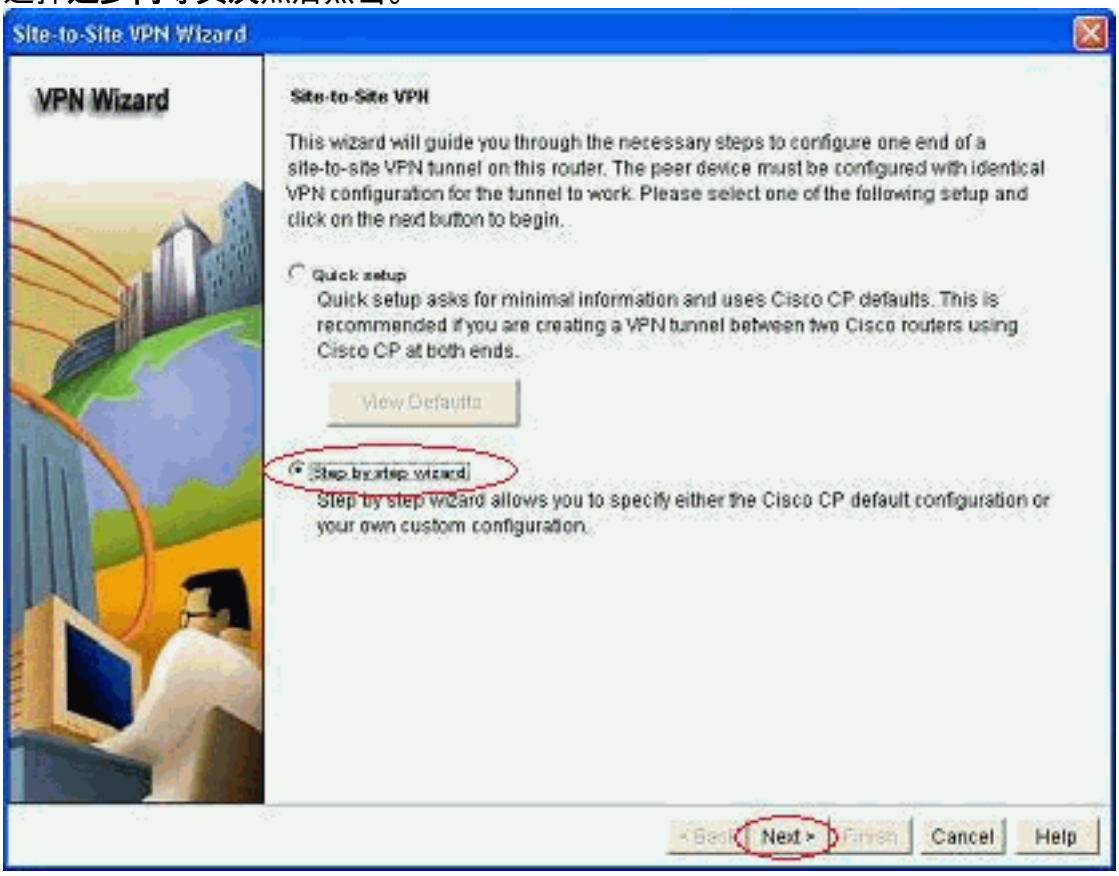
配置

这是在VPN路由器的IPSec VPN配置与CCP。完成这些步骤：

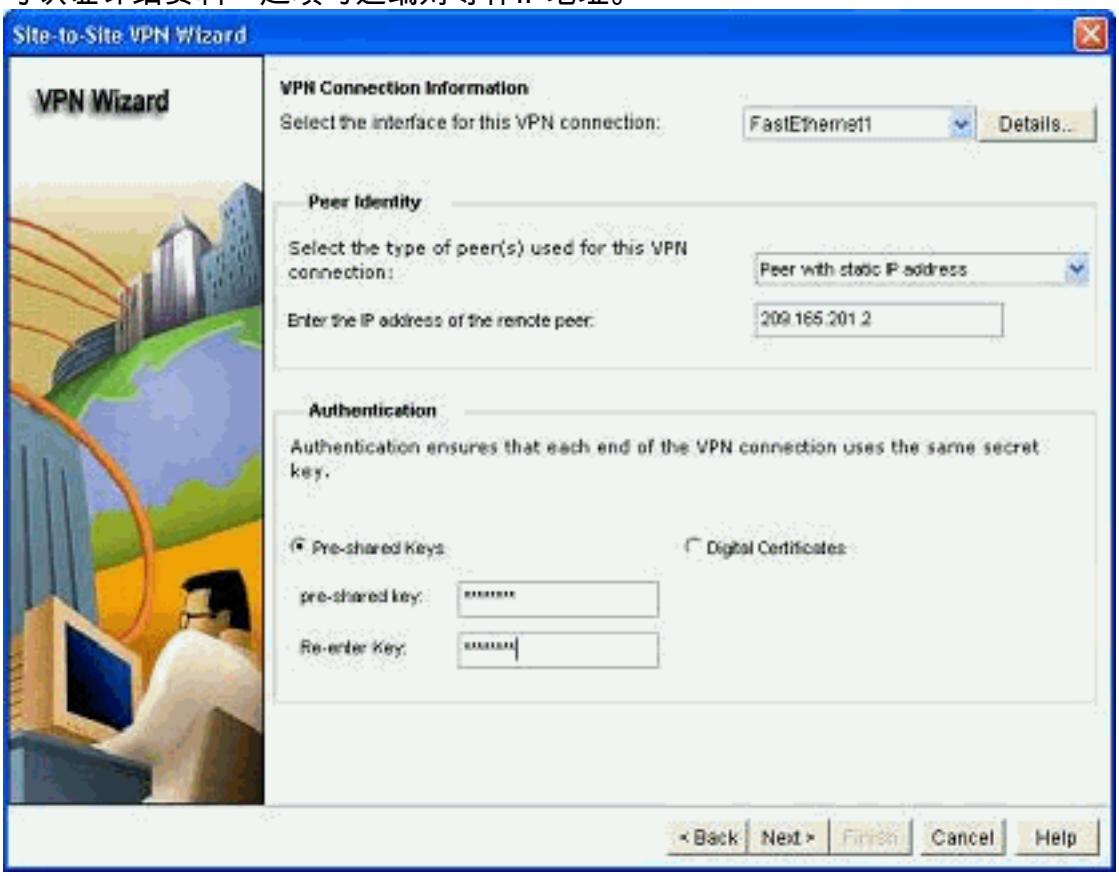
1. 打开CCP应用程序并且选择**配置> Security > VPN > Site to Site VPN**。点击**生成所选的选项**。



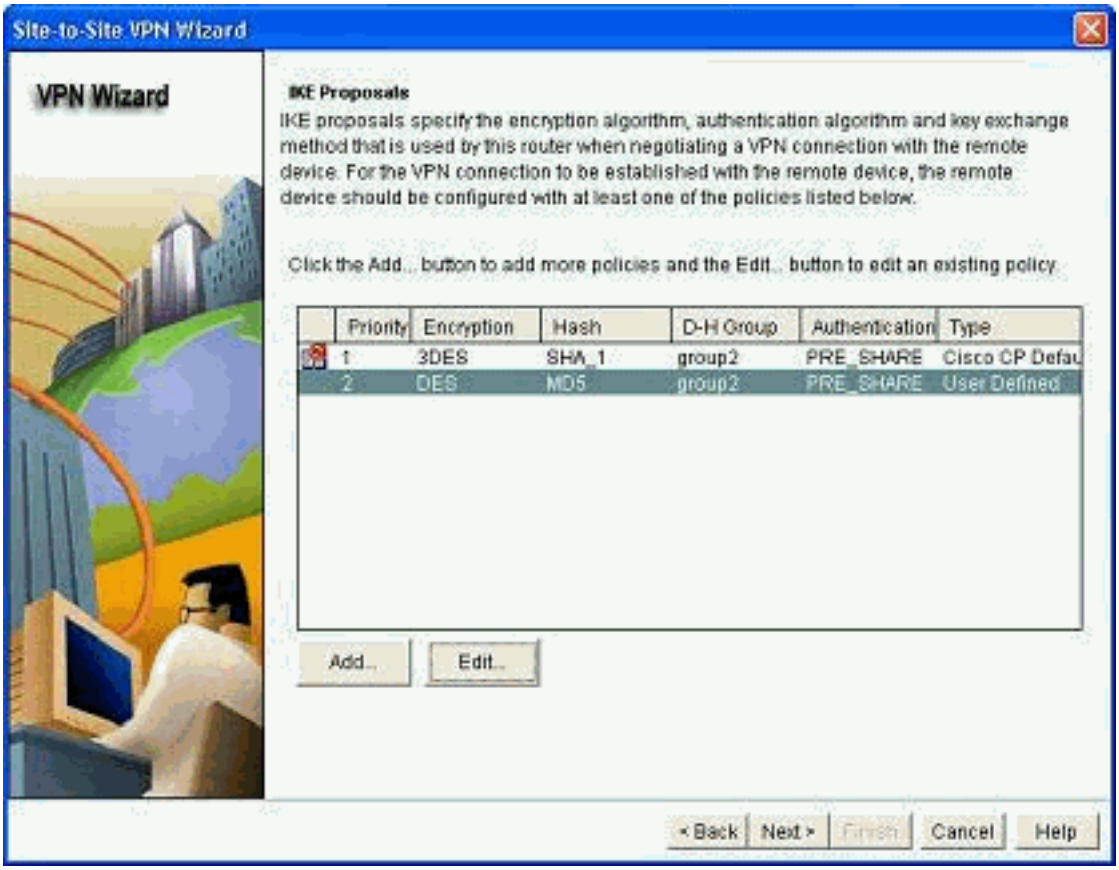
2. 选择**逐步向导**其次然后点击。



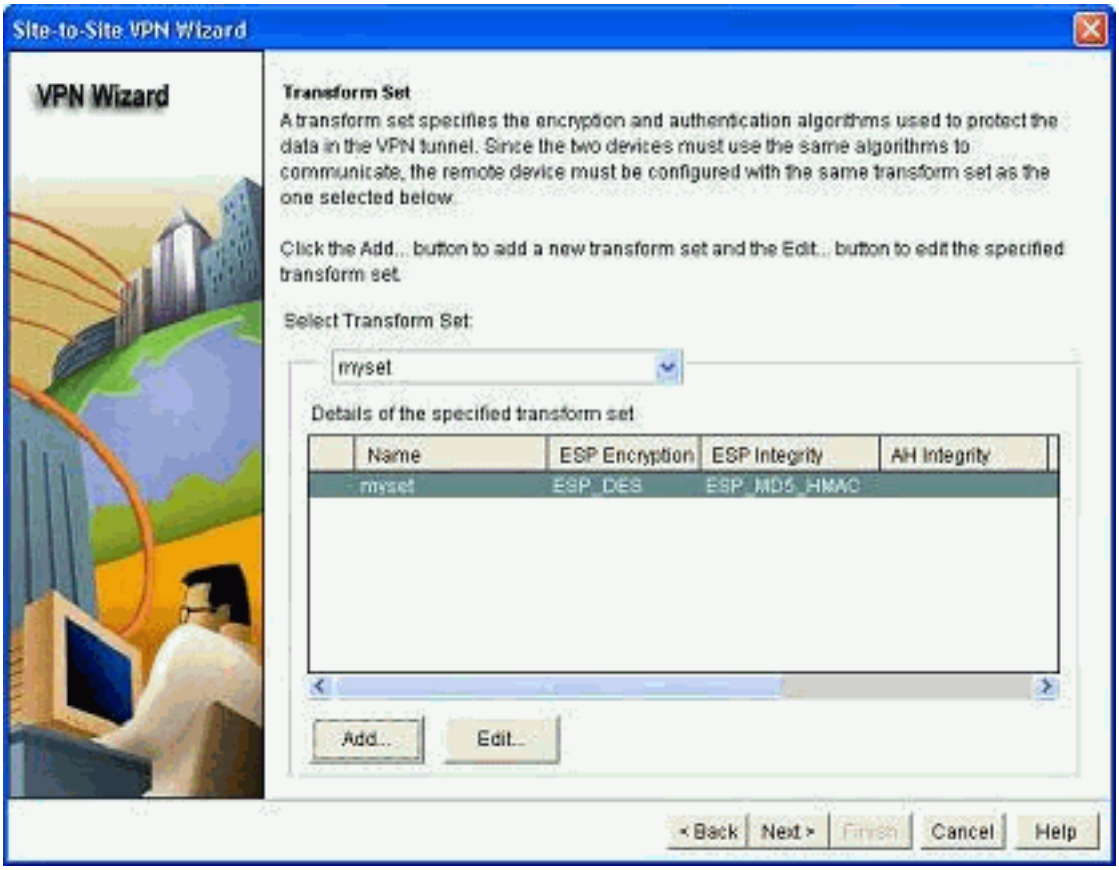
3. 与认证详细资料一起填写远端对等体IP地址。



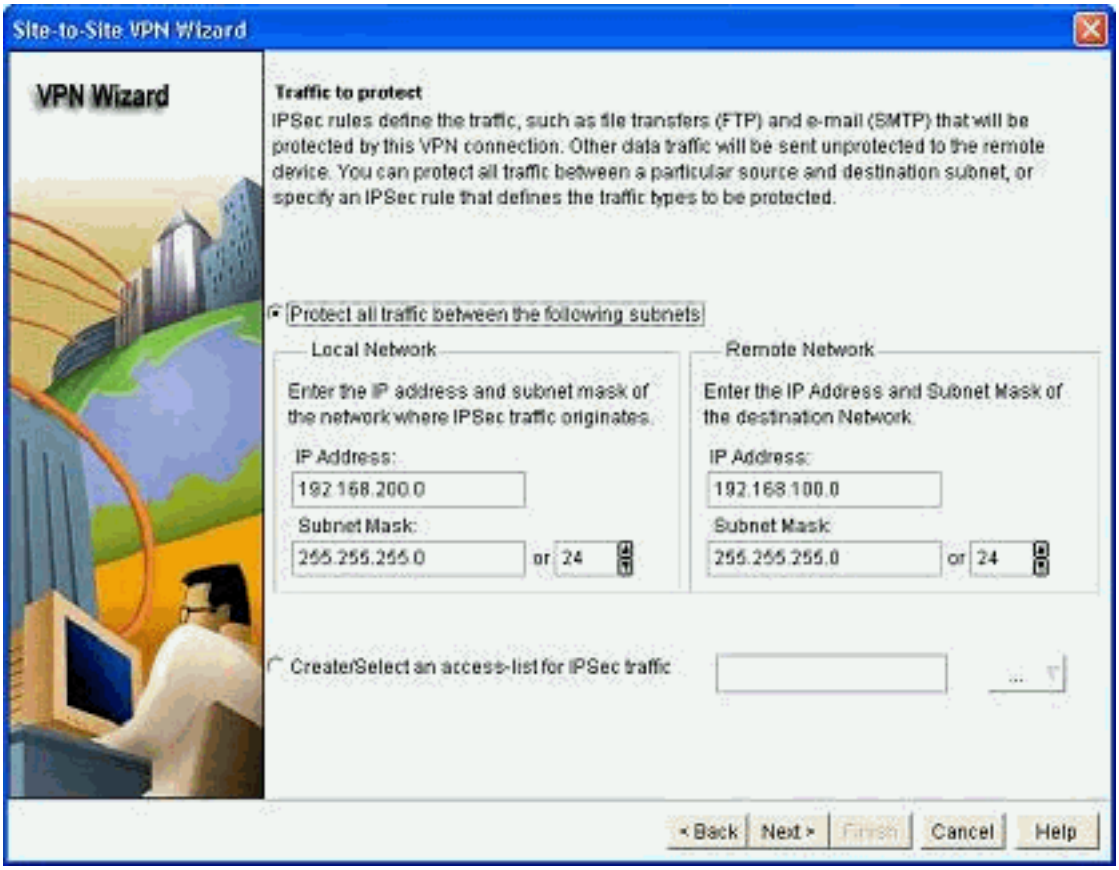
4. 选择IKE建议并且**其次**点击。



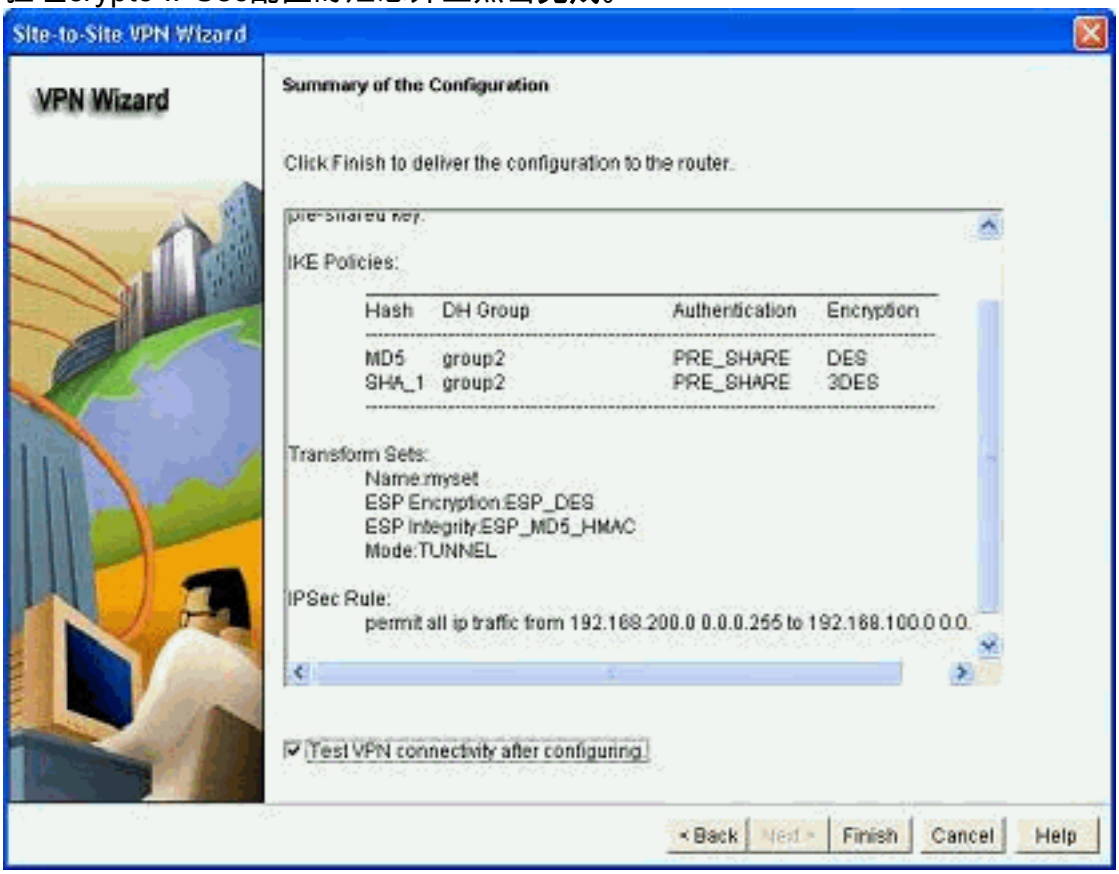
5. 定义变换设置详细资料并且**其次**点击。



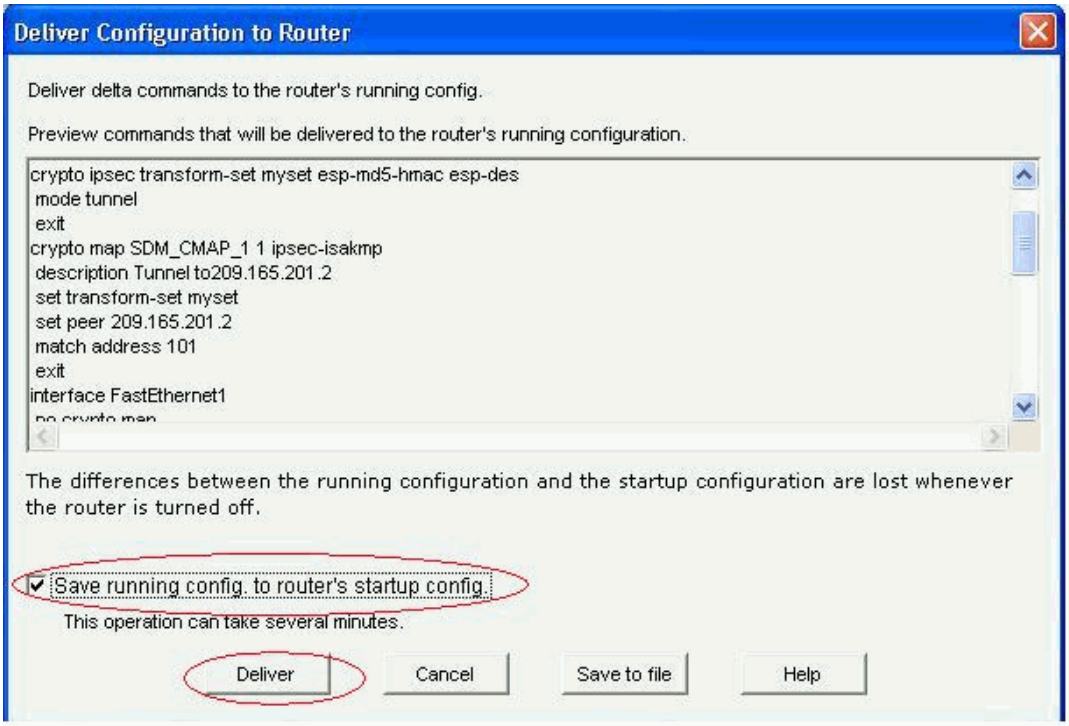
6. 定义需要被加密的数据流并且**其次**点击。



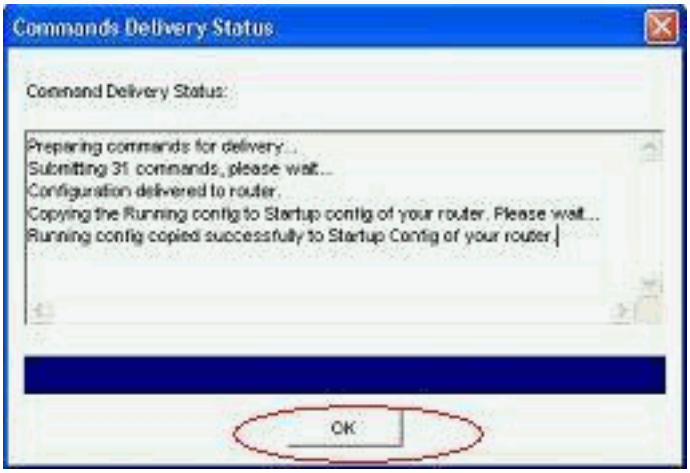
7. 验证crypto IPSec配置的汇总并且点击**完成**。



8. 点击**传送**为了发送配置到VPN路由器。



9. 单击 **Ok**。



CLI 配置

- Ciscoasa
- VPN路由器

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)#
```

CCP创建在VPN路由器的此配置。

VPN路由器

```
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
```

Verify

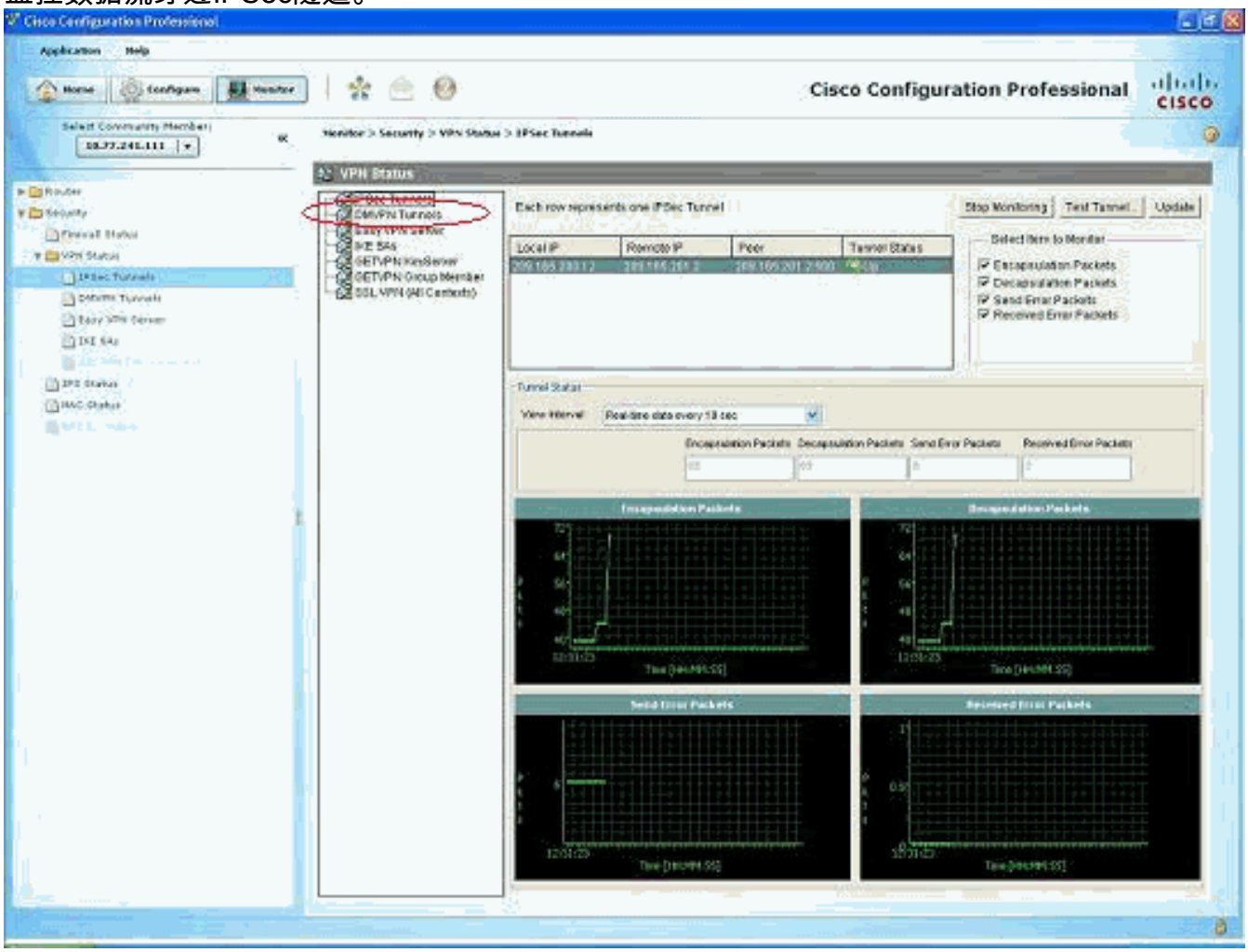
Use this section to confirm that your configuration works properly.

命令输出解释程序（仅限注册用户）(OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输出的分析。

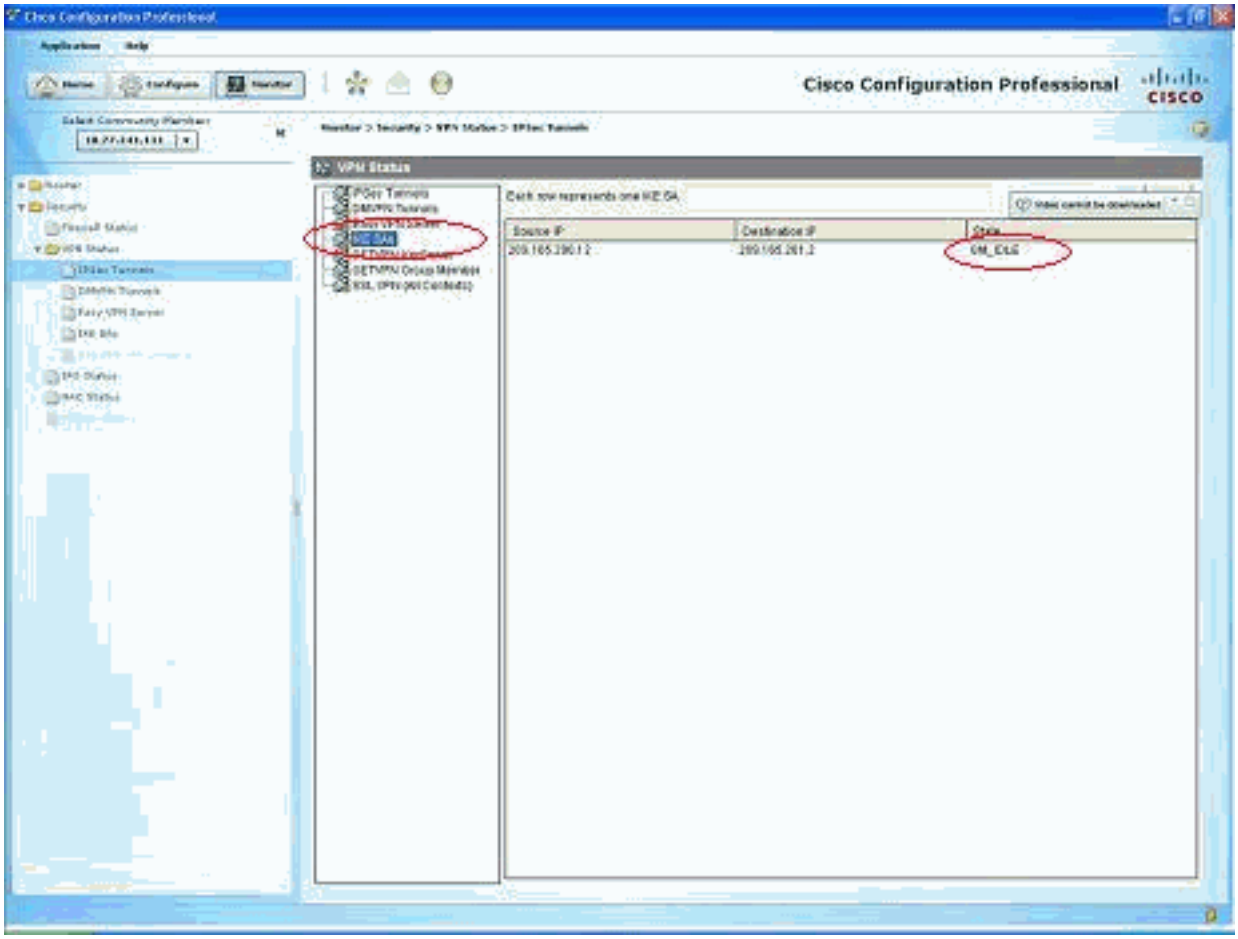
- 验证隧道参数通过CCP
- 验证隧道状态通过ASA CLI
- 验证隧道参数通过路由器CLI

通过CCP验证隧道参数

- 监控数据流穿过IPSec隧道。



- 监控阶段的状况我SA ISAKMP。



通过ASA CLI验证隧道状态

- 验证阶段的状况我SA ISAKMP。

```
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#
```

Note: 观察角色是回应者，阐明，此隧道发起者是在另一边，例如， VPN路由器。

- 验证第II阶段SA IPSEC参数。

```
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
```

通过路由器CLI验证隧道参数

- 验证阶段的状况我SA ISAKMP。

```
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
```

- 验证第II阶段SA IPSEC参数。

```
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

本部分提供的信息可用于对配置进行故障排除。

- 切断现有的crypto连接。

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

VPN-Router#clear crypto isakmp
```

- 请使用调试指令为了用VPN隧道排除问题故障。**Note:** 如果enable (event)调试，这能打乱路由器的操作，当互联网络体验高负载状态。**小心地请使用调试指令**。一般来说，建议仅这些命令使用在您的路由器技术支持代表指导下，当排除特定问题故障时。

```
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#
```

参考在了解和使用调试指令的debug crypto isakmp关于调试commangs的更多信息。

Related Information

- IPsec 协商/IKE 协议支持页
- Cisco ASA安全工具OS软件的文档
- 最常用的 IPSec VPN 故障排除解决方案
- 请求注解 (RFC)