使用CCP配置的靜態定址ASA和動態定址Cisco IOS路由器之間的動態IPsec隧道示例

目錄

簡介

本文檔提供了如何啟用PIX/ASA安全裝置以接受來自Cisco IOS®路由器的動態IPsec連線的示例配置。在此案例中，IPsec通道會在通道僅從路由器端啟動時建立。由於動態IPsec配置，ASA無法啟動VPN隧道。

此配置使PIX安全裝置能夠與遠端VPN路由器建立動態IPsec LAN到LAN(L2L)隧道。此路由器從其Internet服務提供商動態接收其外部公有IP地址。動態主機設定通訊協定(DHCP)提供此機制，以便從提供者動態分配IP位址。這樣，當主機不再需要時，就可以重新使用IP地址。

路由器上的配置使用Cisco Configuration Professional(CCP)完成。CCP是一種基於GUI的裝置管理工具，可用於配置基於Cisco IOS的路由器。有關如何使用CCP配置路由器的詳細資訊，請參閱使用思科配置專業版進行基本路由器配置。

有關使用ASA和Cisco IOS路由器的IPsec隧道建立的詳細資訊和配置示例，請參閱使用ASA的站點到站點VPN(L2L)以及ASA。

有關使用PIX和Cisco IOS路由器建立動態IPSec隧道的詳細資訊和配置示例，請參閱使用IOS的站點到站點VPN(L2L)。

必要條件

需求

在嘗試此配置之前，請確保ASA和路由器均具有Internet連線以建立IPSEC隧道。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 執行Cisco IOS軟體版本12.4的Cisco IOS路由器1812
- Cisco ASA 5510軟體版本8.0.3

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

背景資訊

在此場景中，192.168.100.0網路位於ASA之後，192.168.200.0網路位於Cisco IOS路由器之後。假設路由器通過DHCP從其ISP獲取其公有地址。由於這會在ASA端配置靜態對等體時出現問題，因此需要採用動態加密配置的方法來建立ASA和Cisco IOS路由器之間的站點到站點隧道。

ASA端的Internet使用者將被轉換為其外部介面的IP地址。假設Cisco IOS路由器端未配置NAT。

現在，在ASA端上配置以下主要步驟以建立動態隧道：

1. 階段1 ISAKMP相關配置
2. Nat免除配置
3. 動態加密對映配置

由於ASA假定具有靜態公共IP地址，因此Cisco IOS路由器已配置靜態加密對映。現在，這是要在Cisco IOS路由器端配置以建立動態IPSEC隧道的主要步驟清單。

1. 階段1 ISAKMP相關配置
2. 靜態加密對映相關配置

這些配置中將詳細介紹這些步驟。

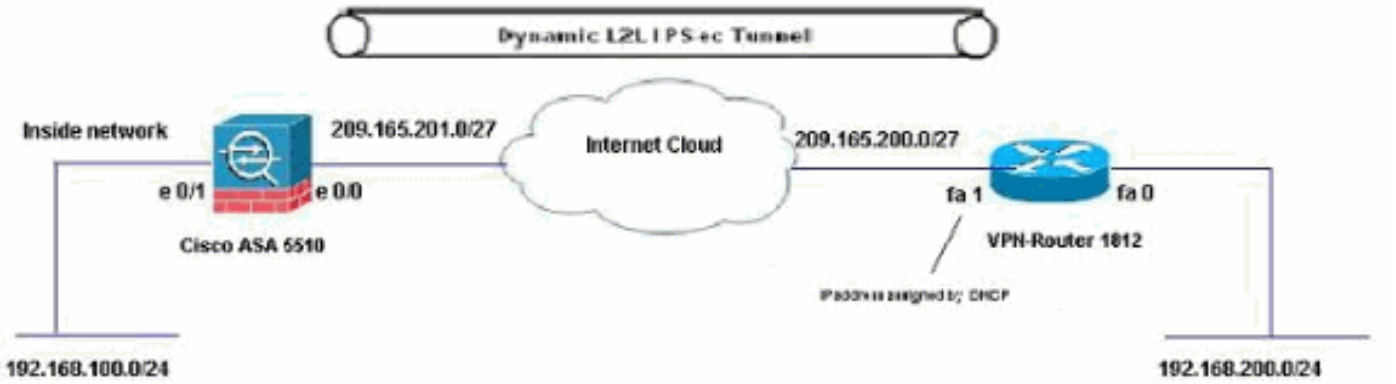
設定

本節提供用於設定本文件中所述功能的資訊。

註：使用Command Lookup Tool(僅供已註冊客戶使用)可獲取本節中使用的命令的詳細資訊。

網路圖表

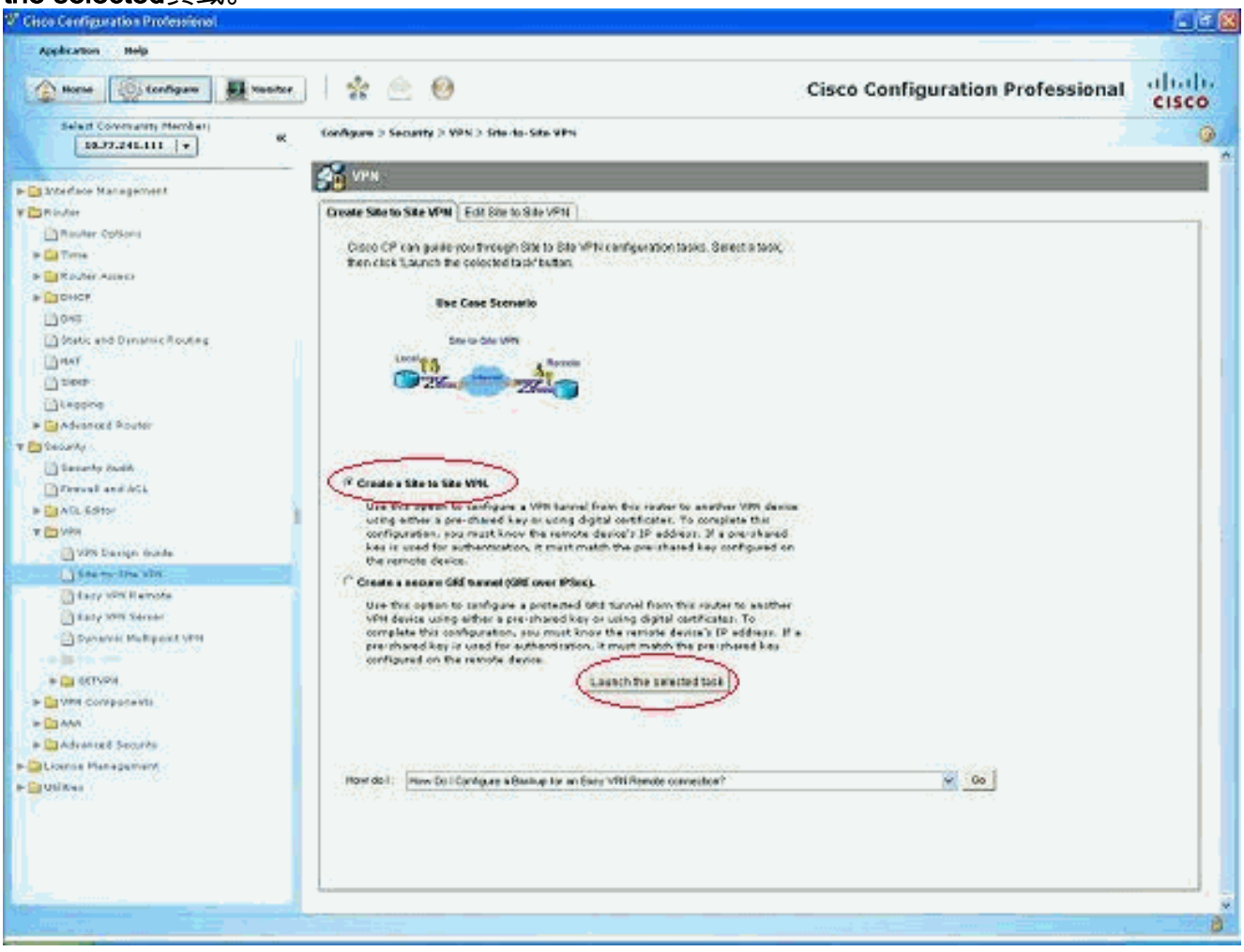
本檔案會使用以下網路設定：



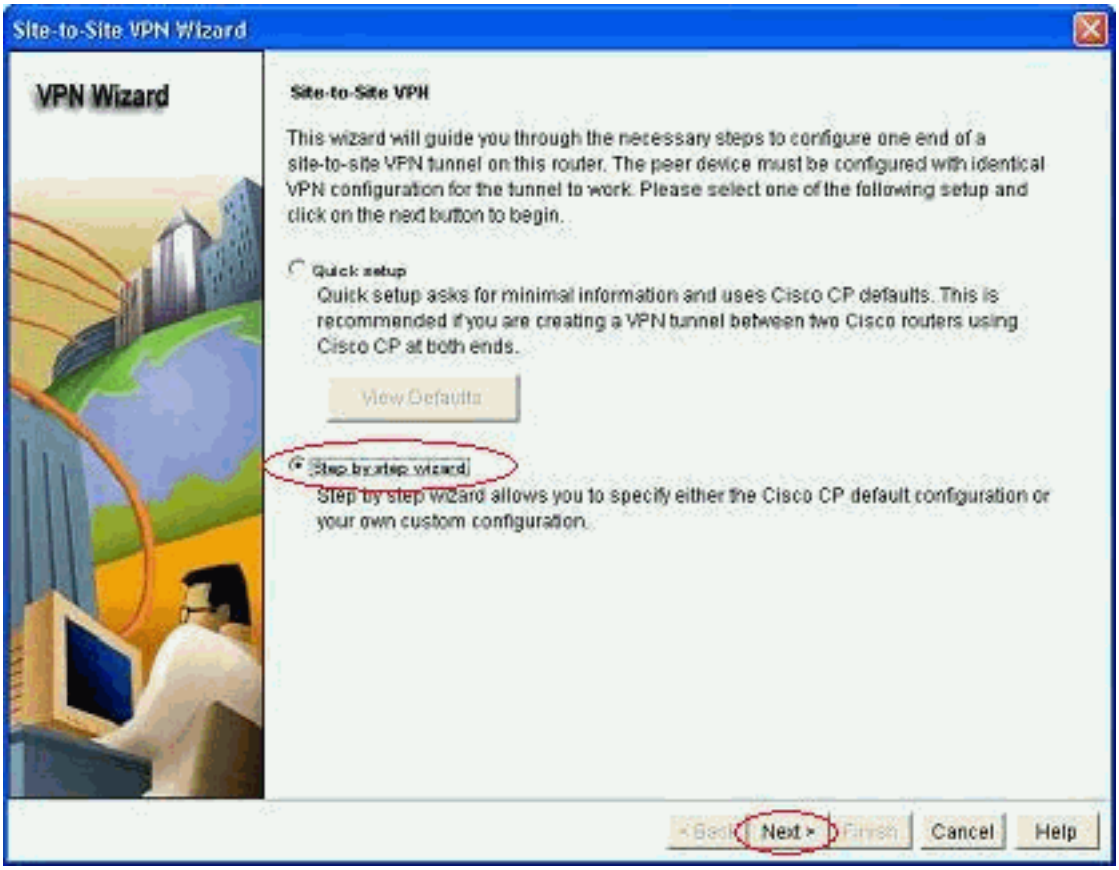
組態

這是使用CCP的VPN路由器上的IPsec VPN配置。請完成以下步驟：

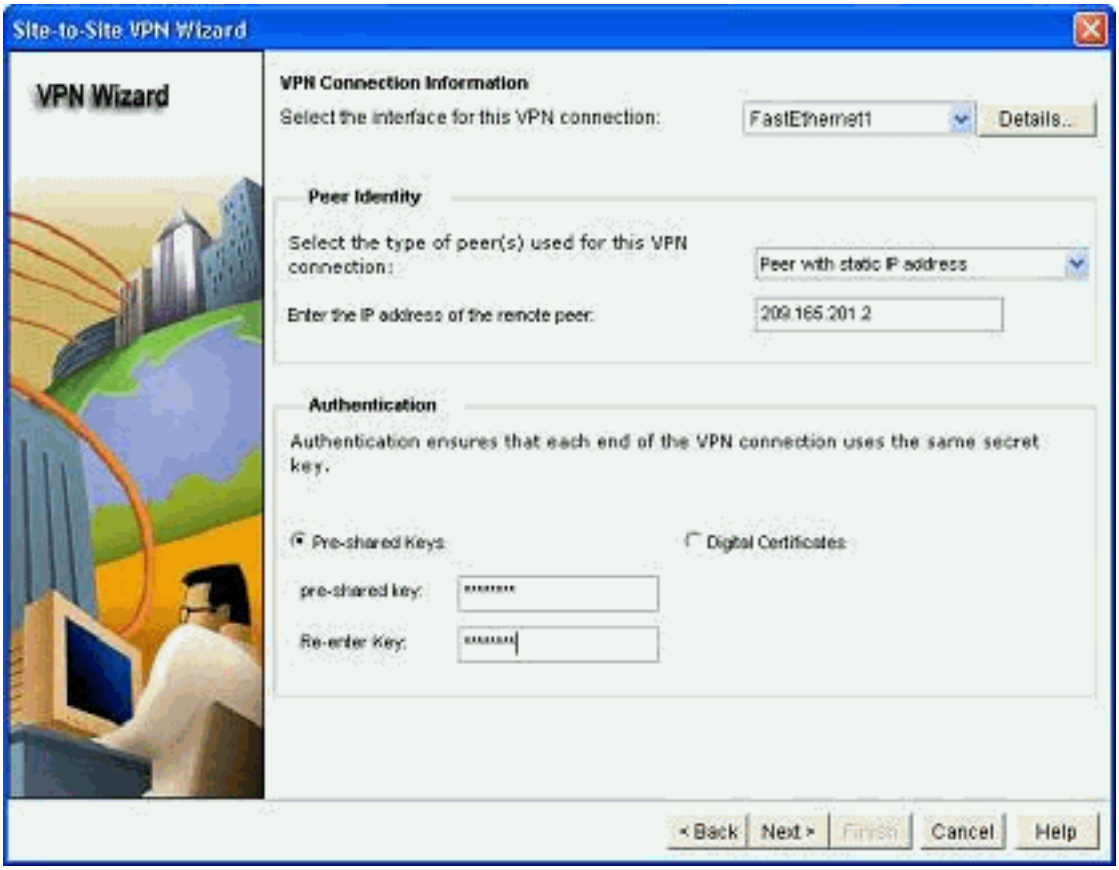
1. 開啟CCP應用程式，然後選擇**Configure > Security > VPN > Site to Site VPN**。按一下**Launch the selected**頁籤。



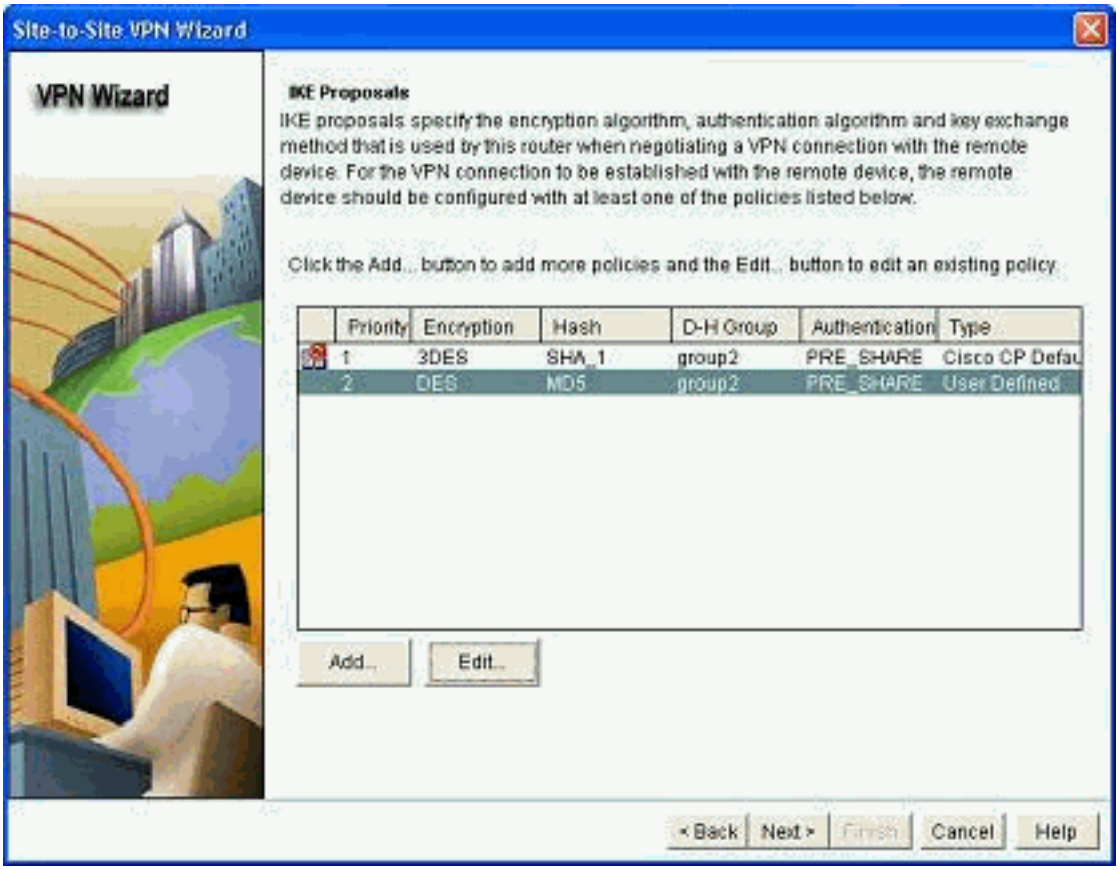
2. 選擇**Step-by-step wizard**，然後按一下**Next**。



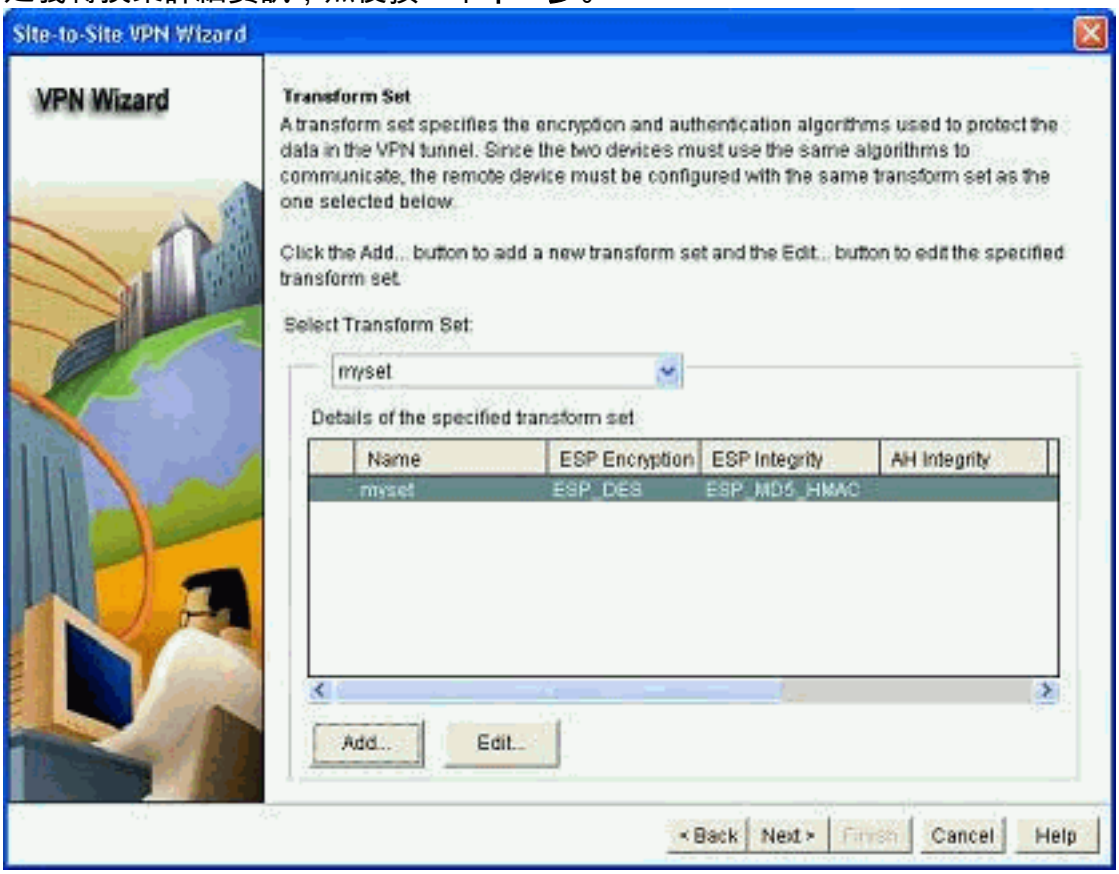
3. 填寫遠端對等IP地址以及身份驗證詳細資訊。



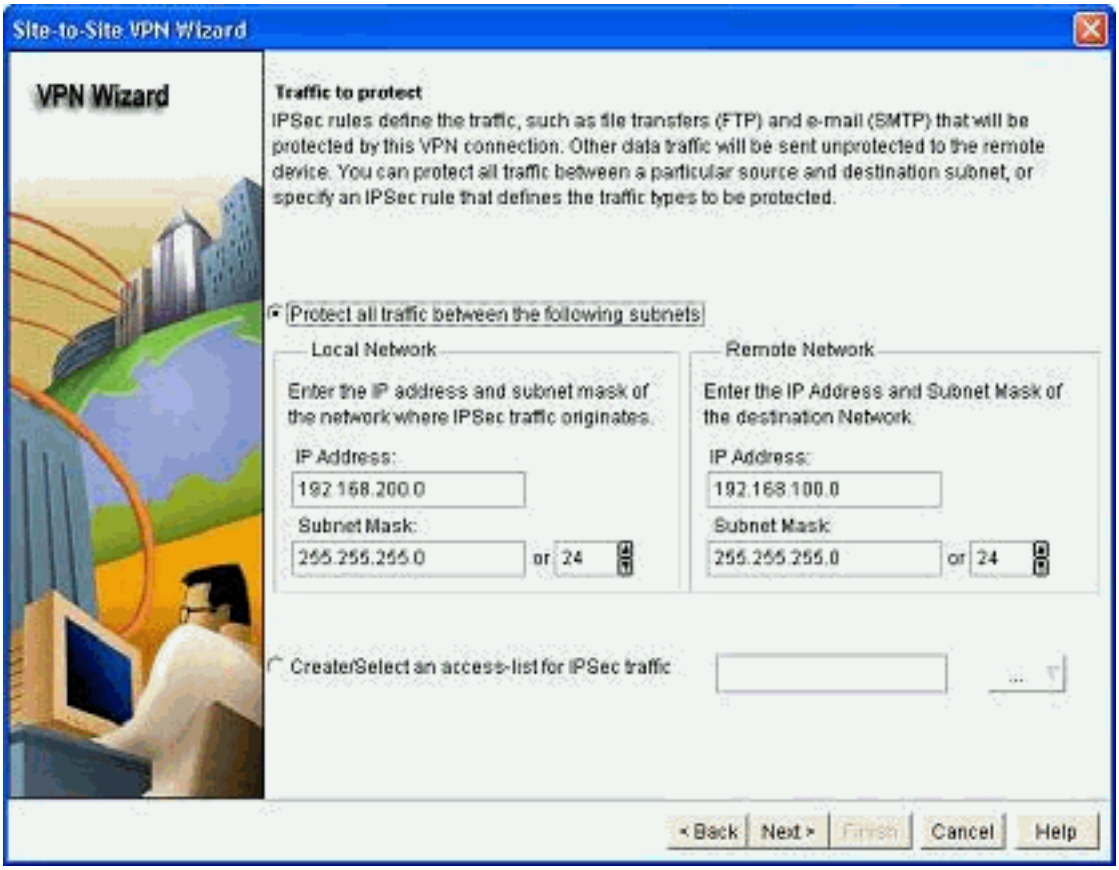
4. 選擇IKE建議並按一下**下一步**。



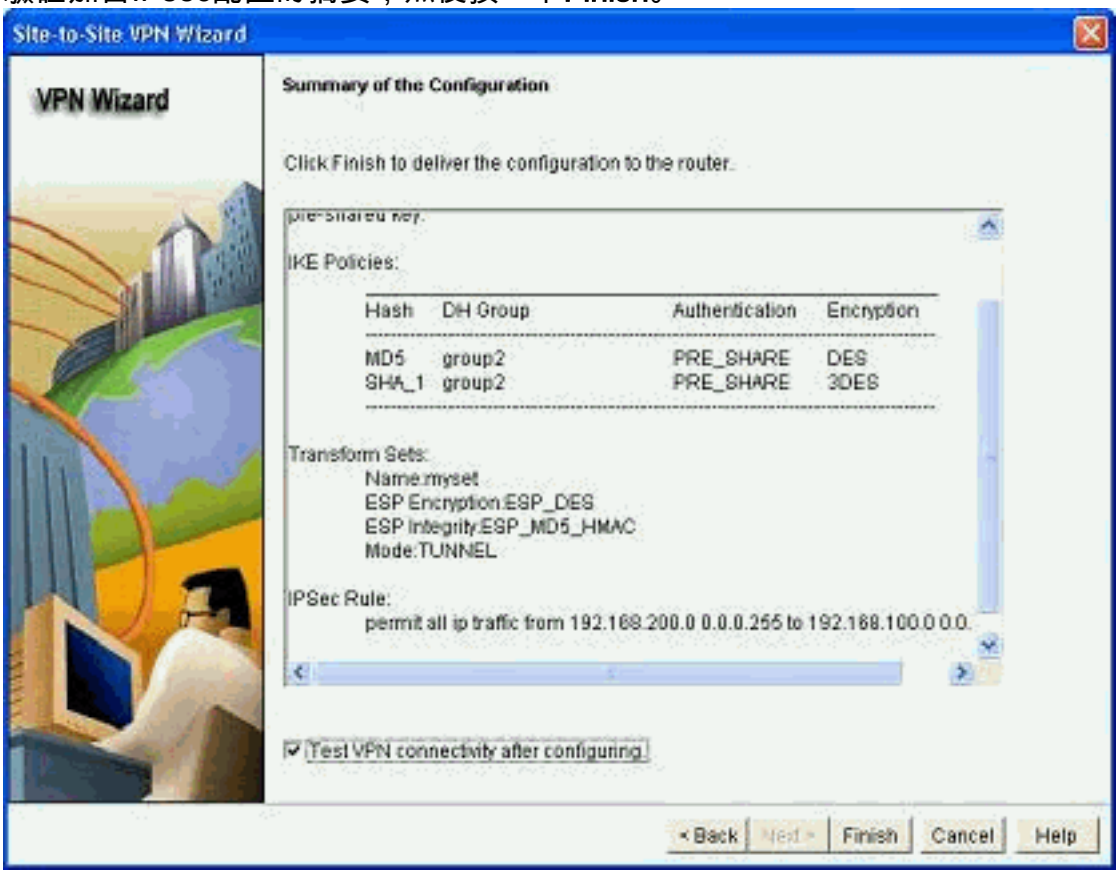
5. 定義轉換集詳細資訊，然後按一下**下一步**。



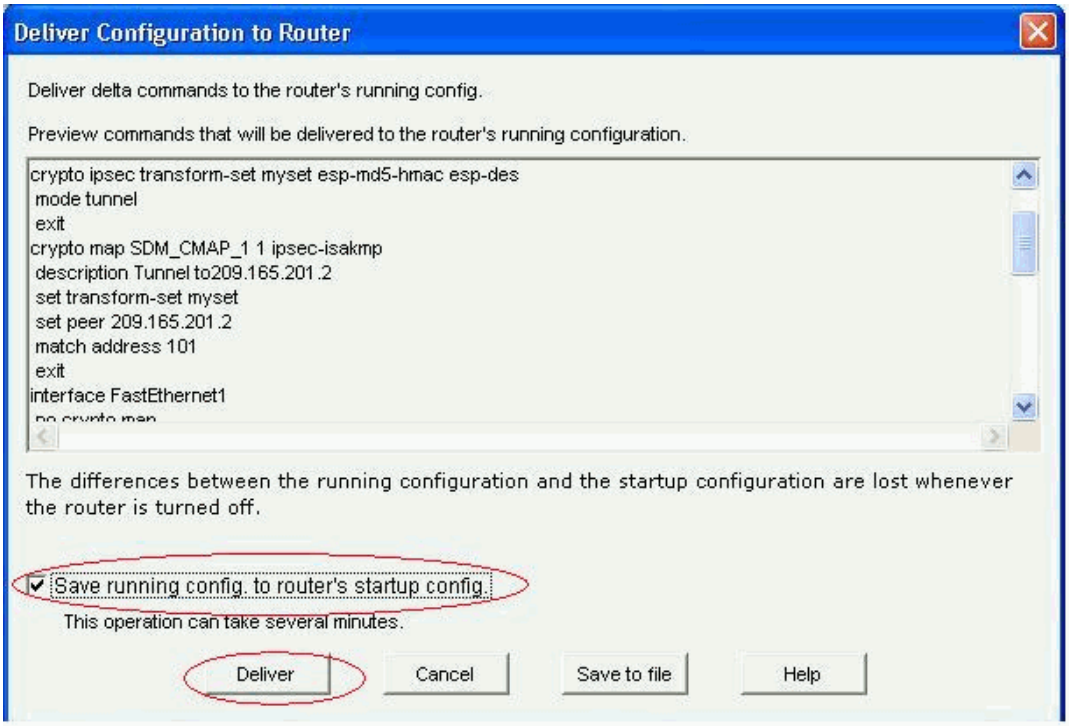
6. 定義需要加密的流量，然後按一下**Next**。

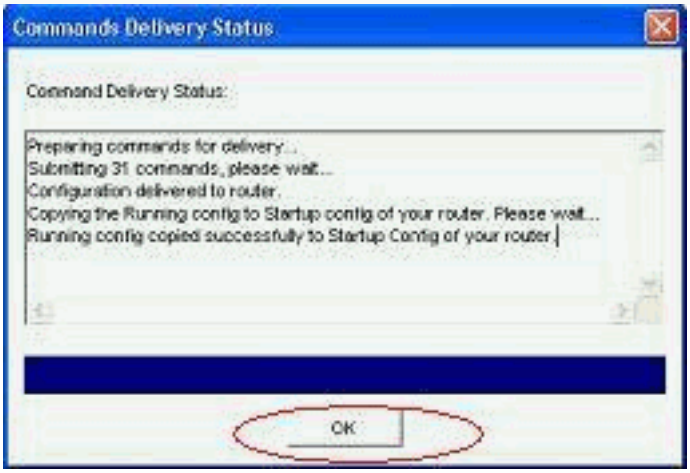


7. 驗證加密IPsec配置的摘要，然後按一下**Finish**。



8. 按一下「**Deliver**」將組態傳送到VPN路由器。





9. 按一下「**OK**」（確定）。

CLI組態

- 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在VPN路由器上建立此配置。

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
```

驗證

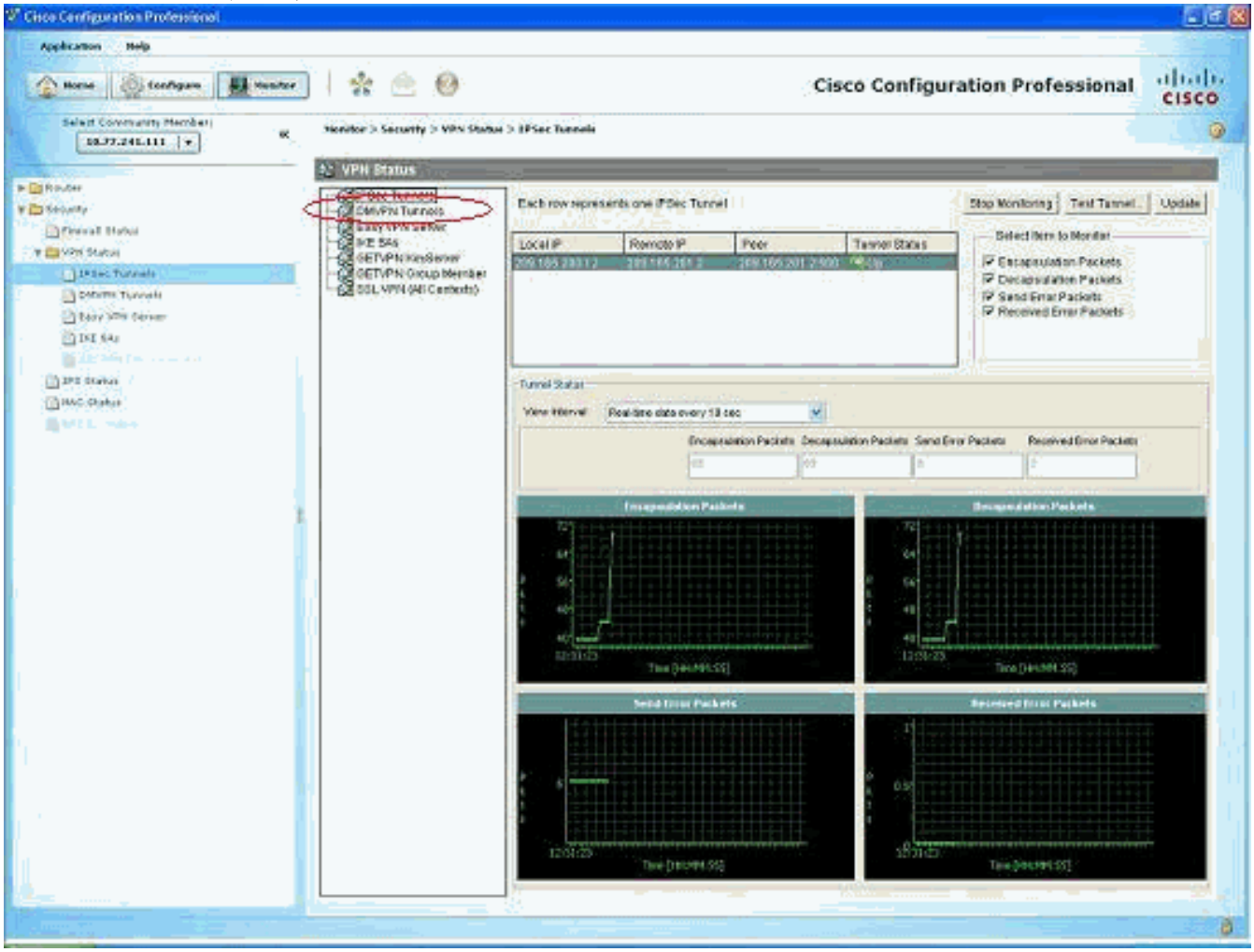
使用本節內容，確認您的組態是否正常運作。

輸出直譯器工具(僅供已註冊客戶使用)(OIT)支援某些show命令。使用OIT檢視show命令輸出的分析。

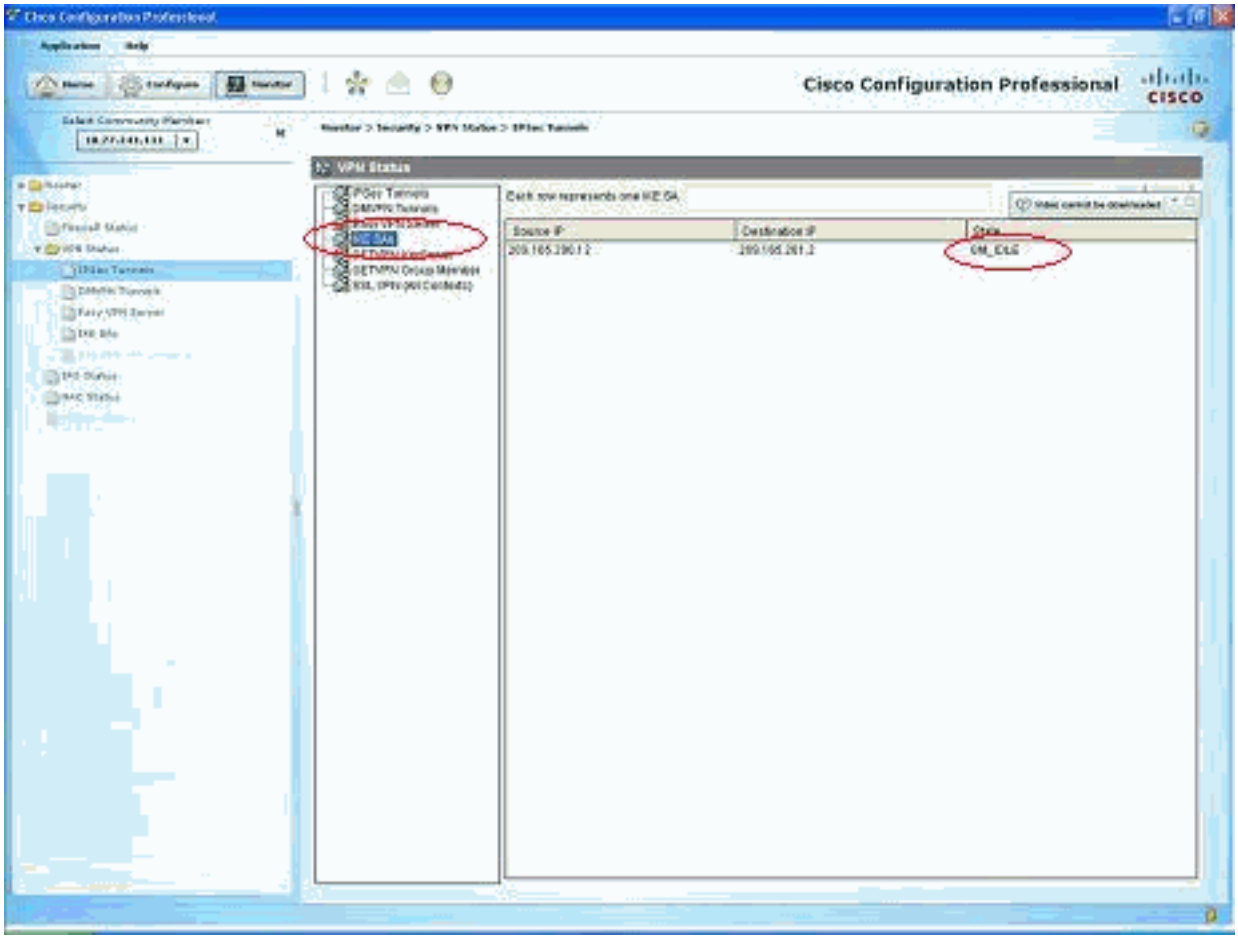
- 通過CCP驗證隧道引數
- 通過ASA CLI驗證隧道狀態
- 通過路由器CLI驗證隧道引數

通過CCP驗證隧道引數

- 監控通過IPsec隧道的流量。



- 監控I階段ISAKMP SA的狀態。



通過ASA CLI驗證隧道狀態

- 驗證階段I ISAKMP SA的狀態。

```
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#
```

注意：觀察作為響應方的角色，該角色表明此隧道的發起方位於另一端，例如VPN路由器。

- 驗證階段II IPSEC SA的引數。

```
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
```

通過路由器CLI驗證通道引數

- 驗證階段I ISAKMP SA的狀態。

```
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
```

- 驗證階段II IPSEC SA的引數。

```
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:
```

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

- 拆除現有的加密連線。

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

VPN-Router#clear crypto isakmp
```

- 使用debug命令以疑難排解VPN通道的問題。**注意：如**果啟用調試，則當網際網路遇到高負載條件時，這可能會中斷路由器的運行。**請謹慎使用debug命令。通常，在排除特定故障時，建議僅在路由器技術支援代表的指導下使用這些命令。**

```
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#
```

有關debug命令的詳細資訊，請參閱瞭解和使用debug命令中的debug crypto isakmp。

相關資訊

- IPSEC協商/IKE通訊協定支援頁面
- Cisco ASA安全裝置OS軟體文檔
- 最常見的IPSEC VPN故障排除解決方案
- 要求建議 (RFC)