スタティックにアドレス指定された ASA と、CCP を使用するダイナミックにアドレス指定された Cisco IOS ルータ間における、ダイナミック IPSec トンネルの設定例

内容

概要

このドキュメントでは、PIX/ASA セキュリティ アプライアンスが Cisco IOS® ルータからのダイナミック IPSec 接続の受け入れを可能にする方法の設定例を示します。このシナリオでは、ルータ側からトンネルが開始された場合にのみ IPSec トンネルが確立されます。ダイナミック IPSec 設定のため、ASA は VPN トンネルを開始できません。

この設定は、PIX セキュリティ アプライアンスが VPN ルータを使用してダイナミック IPsec LAN-to-LAN（L2L）トンネルを作成できるようにします。このルータは、インターネット サービス プロバイダーから外部のパブリック IP アドレスをダイナミックに受信します。プロバイダーからダイナミックに IP アドレスを割り当てる目的で、Dynamic Host Configuration Protocol（DHCP）がこのメカニズムを提供します。これにより、ホストで使用されなくなった IP アドレスを再利用できます。

ルータ上の設定は、Cisco Configuration Professional（CCP）を使用して実行されます。CCP とは、Cisco IOS ベースのアクセス ルータを設定する GUI ベースのデバイス管理ツールです。CCP を使用したルータの設定方法の詳細については、『Cisco Configuration Professional を使用した基本的なルータ設定』を参照してください。

ASA および Cisco IOS ルータを使用する IPSec トンネルの確立に関する情報および設定例については、『ASA によるサイト間 VPN（L2L）』を参照してください。

PIX および Cisco IOS ルータを使用する IPSec トンネルの確立に関する情報および設定例については、『IOS によるサイト間 VPN（L2L）』を参照してください。

前提条件

要件

この設定を実行する前に、IPSec トンネルを確立するためのインターネット接続が ASA およびルータに用意されていることを確認します。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco IOS ソフトウェア リリース 12.4 が稼働する Cisco IOS ルータ 1812
- Cisco ASA 5510 ソフトウェア リリース 8.0.3

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細については、『シスコ テクニカル ティップスの表記法』を参照してください。

背景説明

このシナリオでは、192.168.100.0 ネットワークが ASA の背後にあり、192.168.200.0 ネットワークは Cisco IOS ルータの背後にあります。ルータは ISP から DHCP を使用してパブリック アドレスを取得することを前提とします。ASA 側ではスタティック ピアの設定に問題が発生するため、ASA と Cisco IOS ルータ間のサイト間トンネルを確立するには、ダイナミック クリプト設定を使用する必要があります。

ASA 側のインターネット ユーザは、その outside インターフェイスの IP アドレスに変換されます。NAT は Cisco IOS 側に設定されないものとします。

次に、ダイナミック トンネルを確立するために ASA 側で設定する主なステップを示します。

1. フェーズ 1 の ISAKMP 関連の設定
2. NAT 免除の設定
3. ダイナミック クリプト マップの設定

ASA がスタティックなパブリック IP アドレスを保持していると見なされるため、Cisco IOS ルータにはスタティック クリプト マップが設定されています。次に、ダイナミック IPSec トンネルを確立するために Cisco IOS ルータ側で設定する主なステップのリストを示します。

1. フェーズ 1 の ISAKMP 関連の設定
2. スタティック クリプト マップ関連の設定

これらのステップは、下記の設定で詳しく説明します。

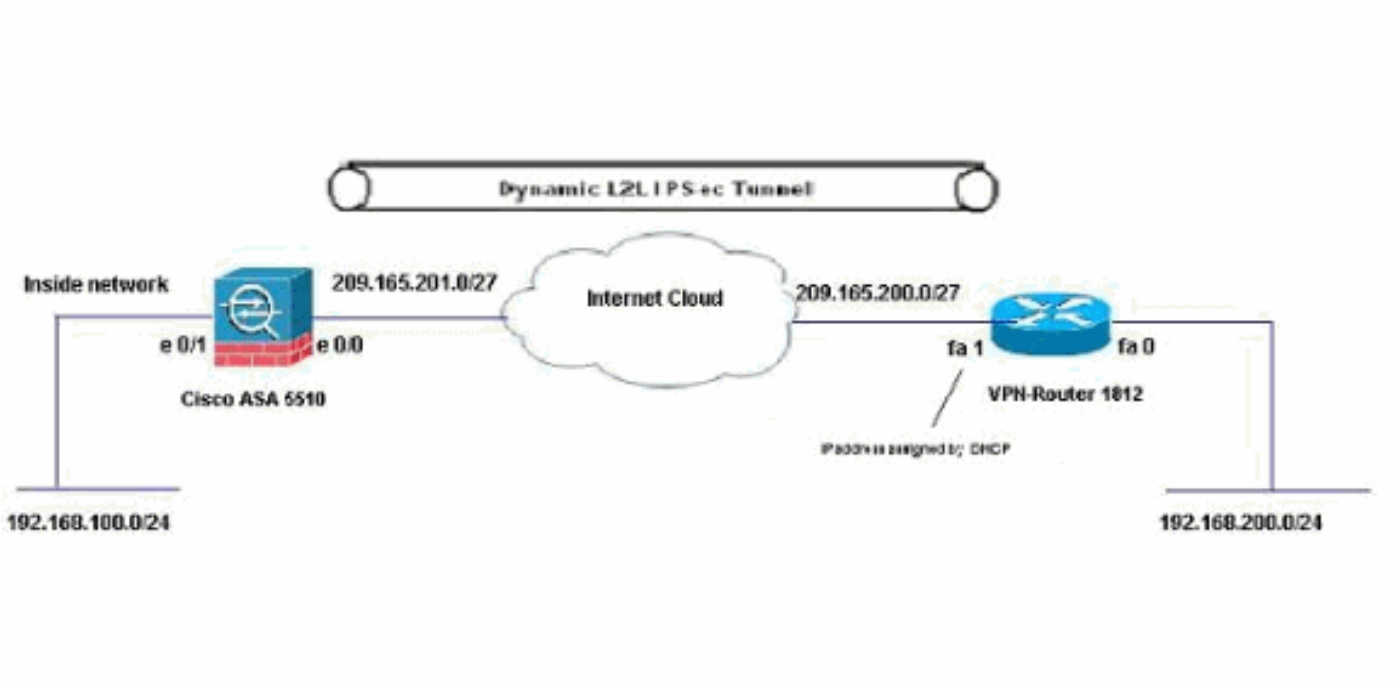
設定

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

注：このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を参照してください。一部ツールについては、ゲスト登録のお客様にはアクセスできない場合がありますことをご了承ください。

ネットワーク図

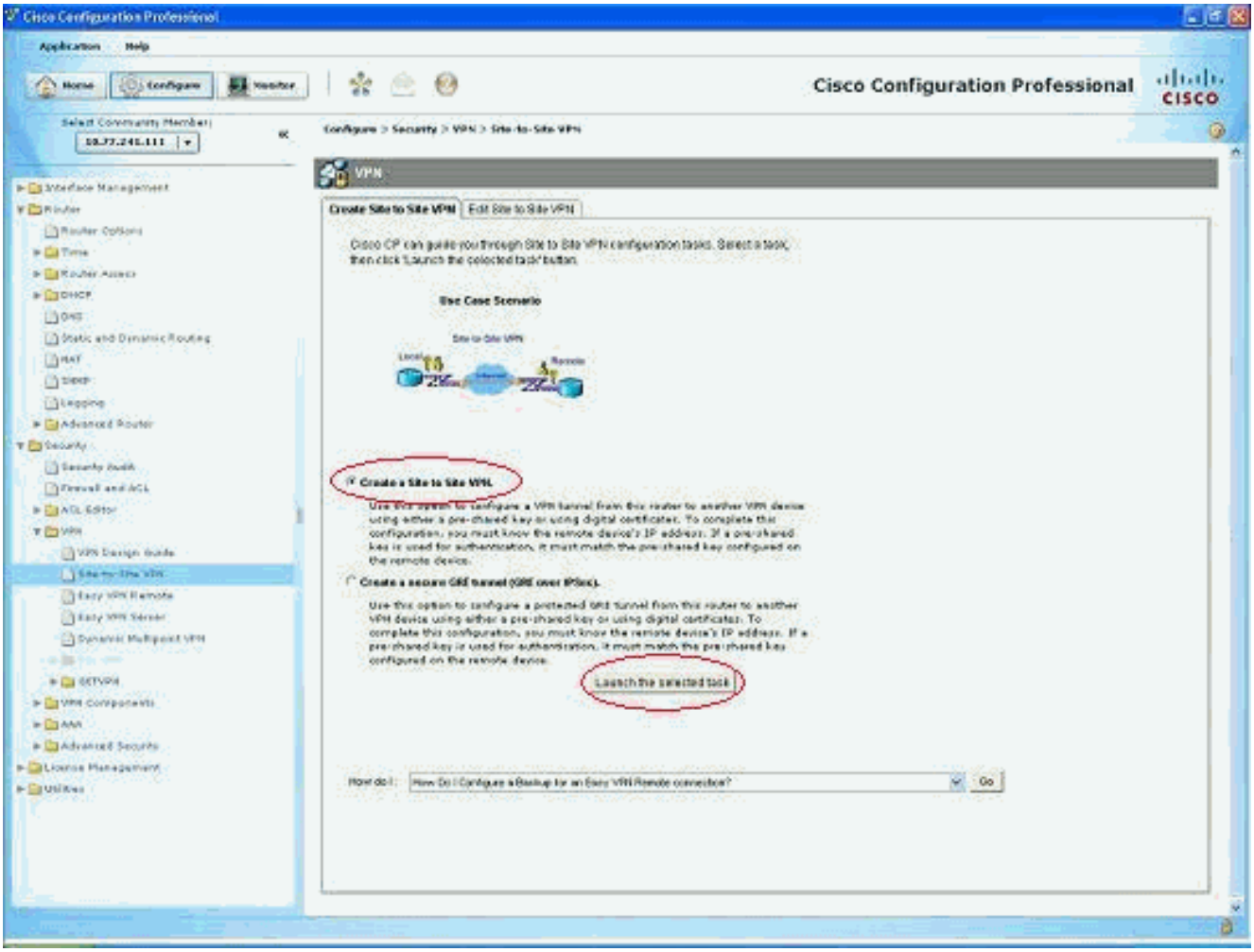
このドキュメントでは、次のネットワーク セットアップを使用します。



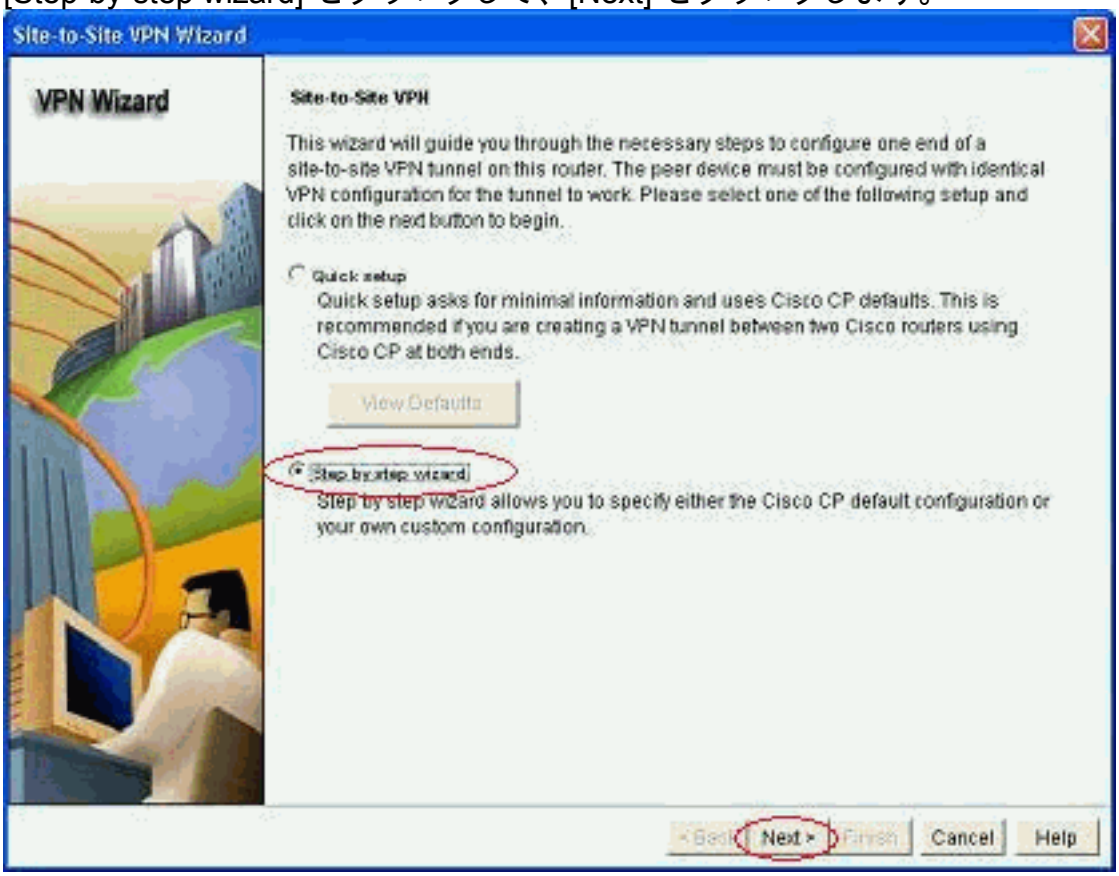
設定

これは、CCP を使用した VPN ルータ上の IPsec VPN 設定です。次のステップを実行します。

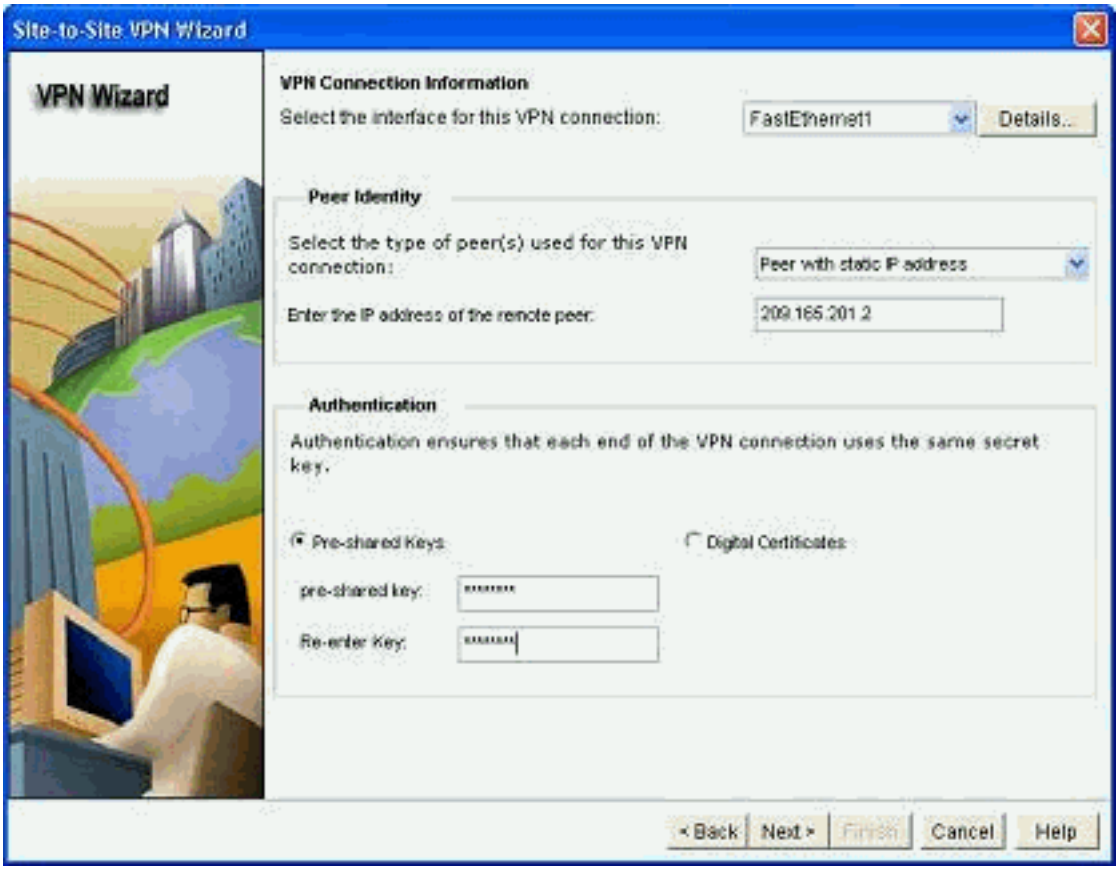
1. CCP アプリケーションを起動し、[Configure] > [Security] > [VPN] > [Site to Site VPN] の順に選択します。[Launch the selected tab] をクリックします。



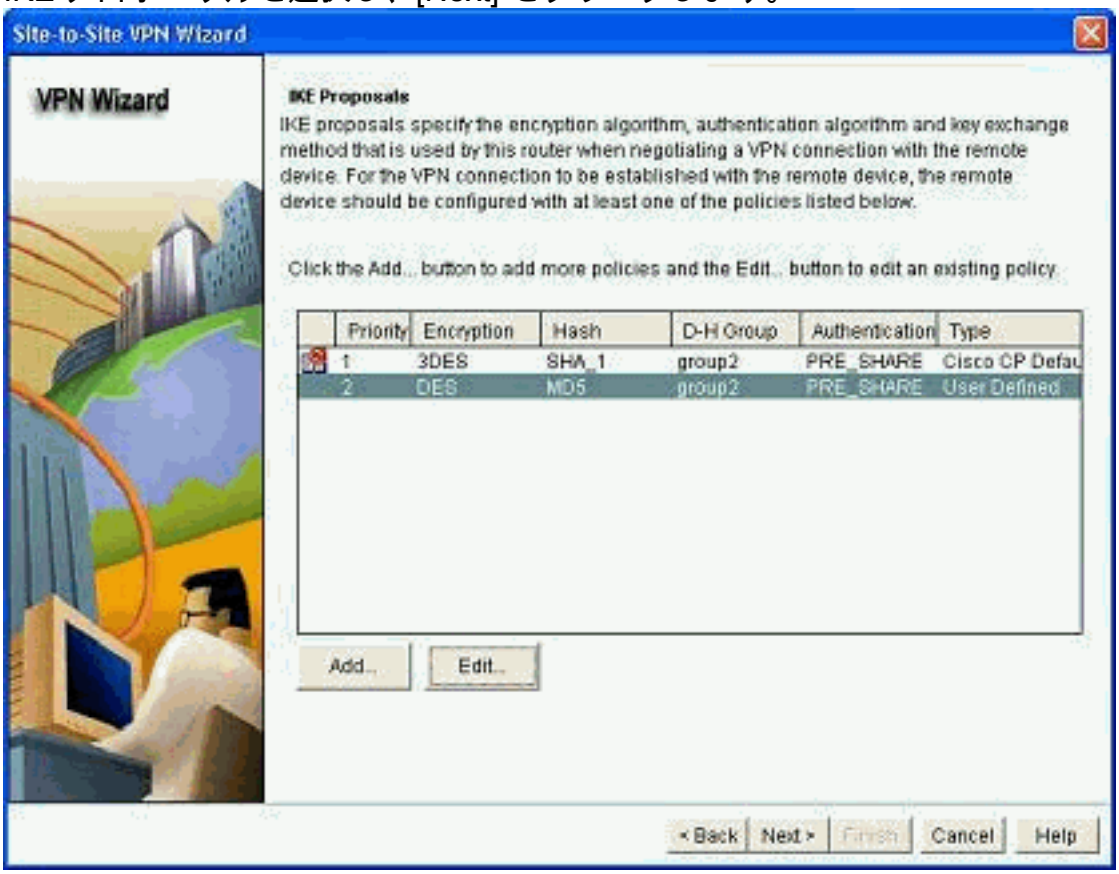
2. [Step-by-step wizard] をクリックして、[Next] をクリックします。



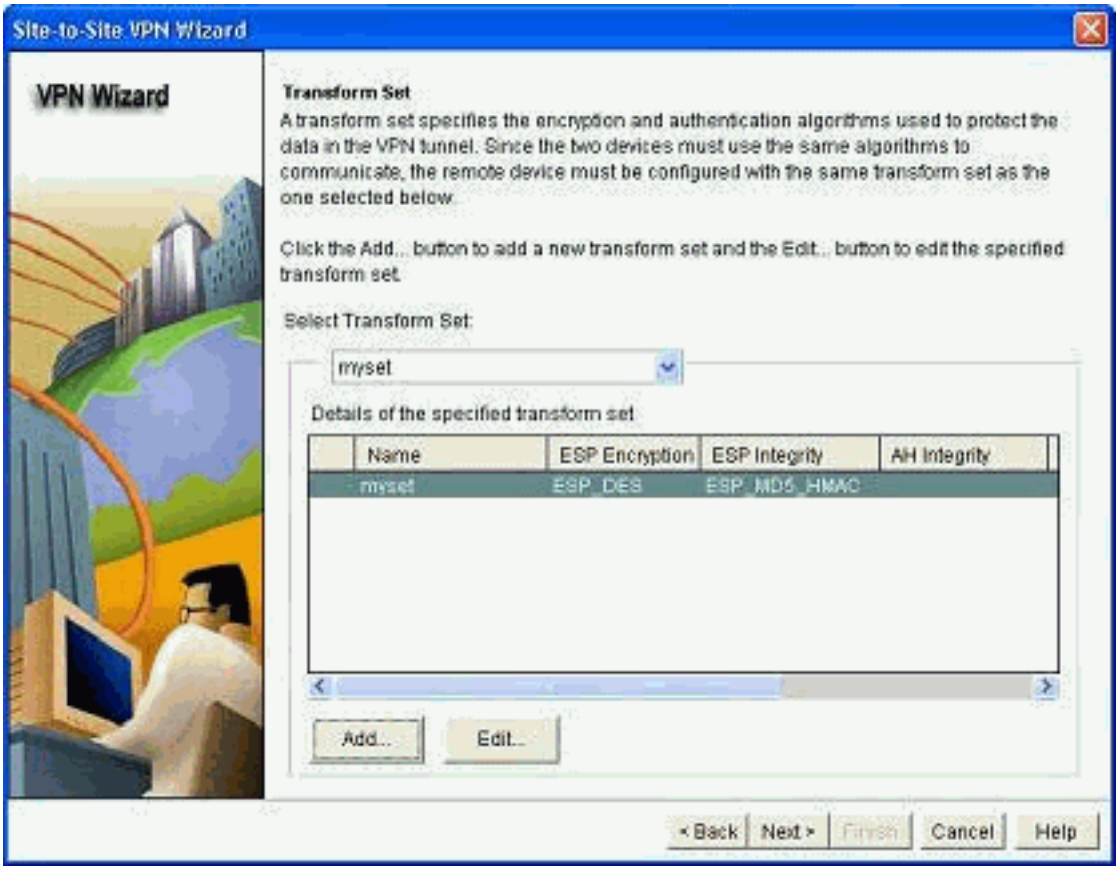
3. 認証についての詳細に従って、リモート ピアの IP アドレスを入力します。



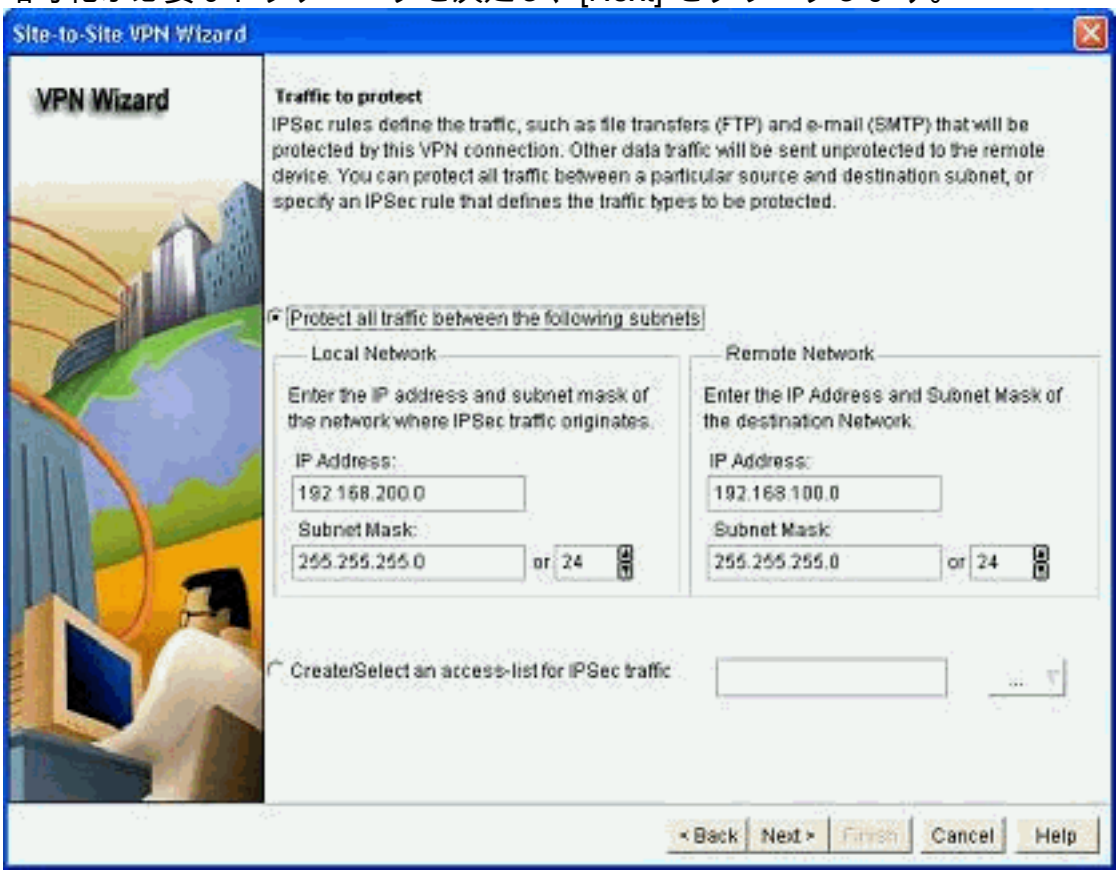
4. IKE プロポーザルを選択し、[Next] をクリックします。



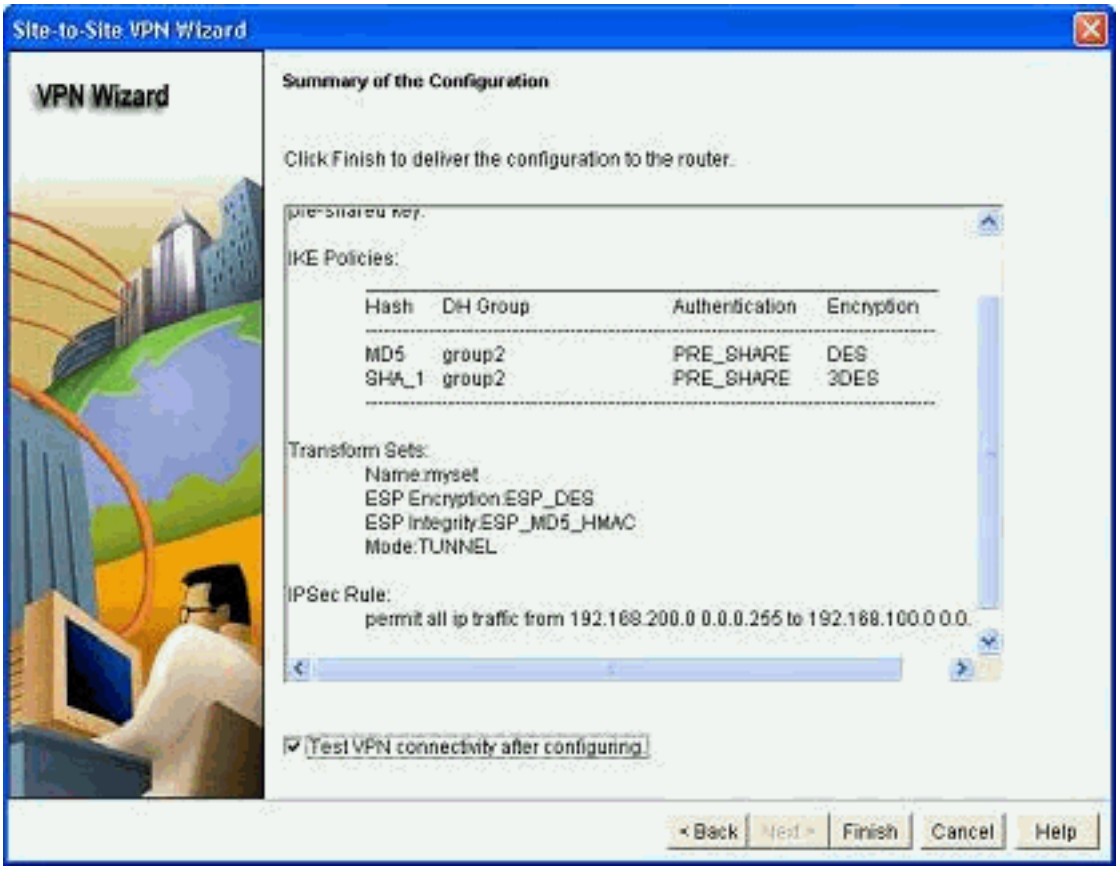
5. トランスフォーム セットの詳細を決定し、[Next] をクリックします。



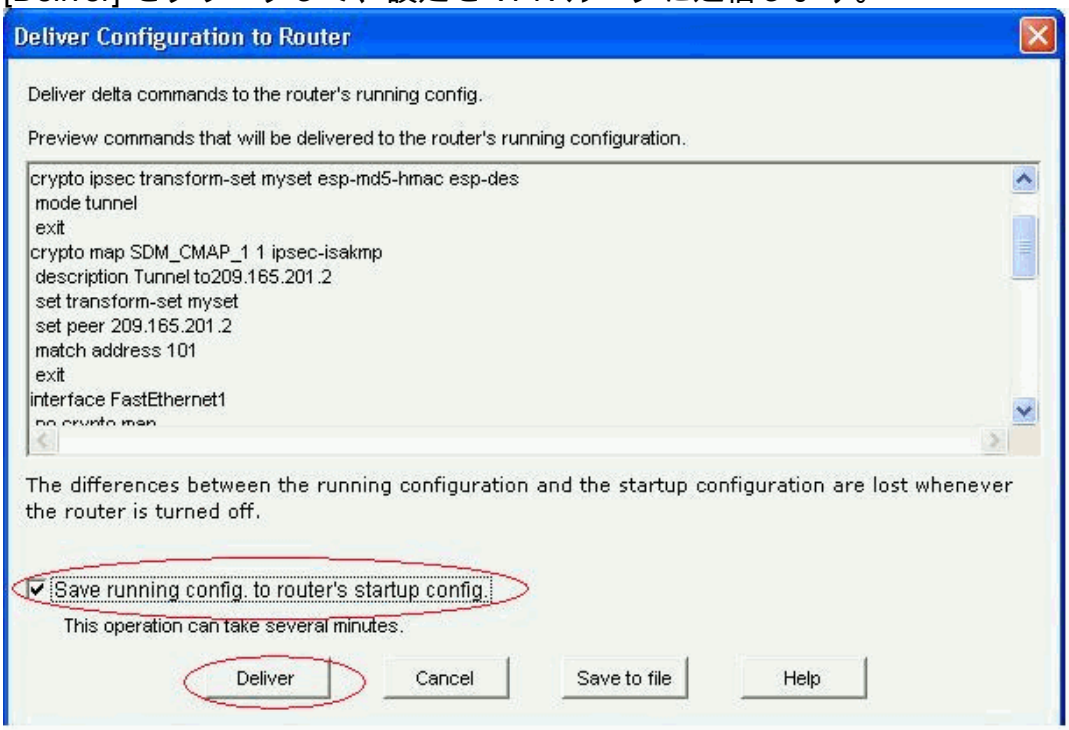
6. 暗号化が必要なトラフィックを決定し、[Next] をクリックします。

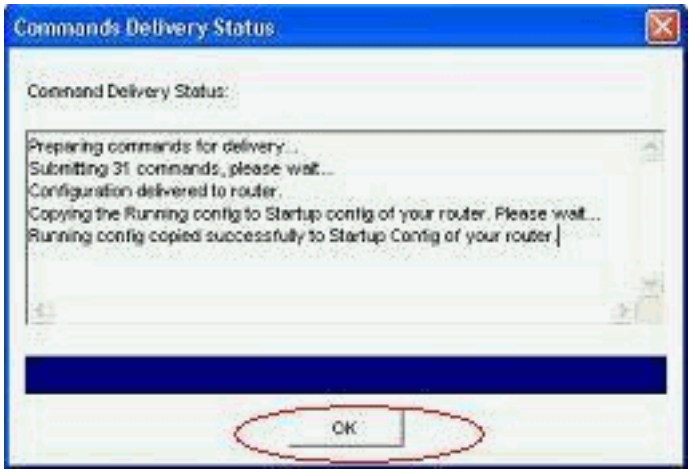


7. crypto IPsec 設定のサマリーを確認し、[Finish] をクリックします。



8. [Deliver] をクリックして、設定を VPN ルータに送信します。





9. [OK] をクリックします。

CLI での設定

- Ciscoasa
- VPN ルータ

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 により、VPN ルータにこの内容が設定されます。

VPN ルータ

```
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
```

確認

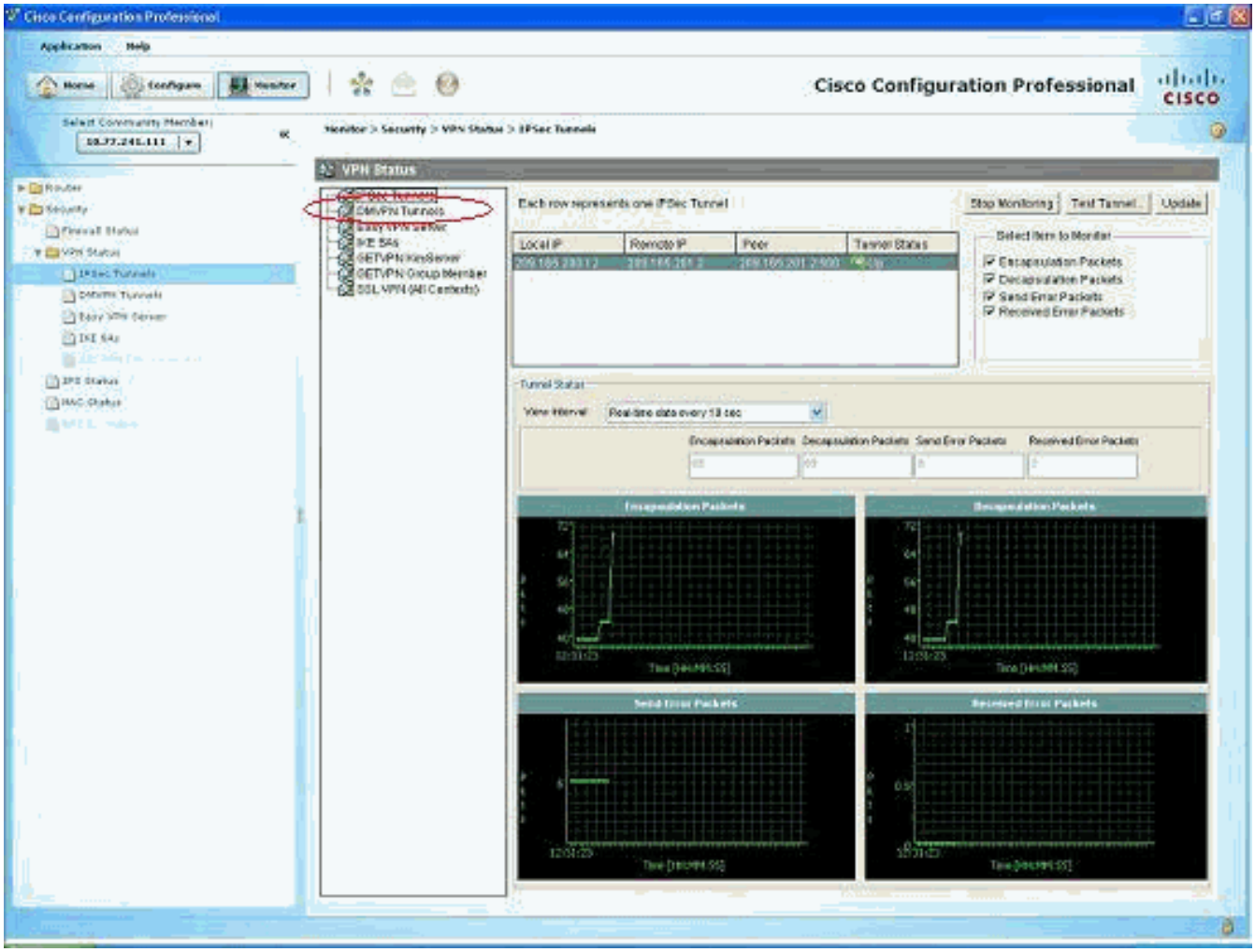
ここでは、設定が正常に機能しているかどうかを確認します。

アウトプット インタープリタ ツール（登録ユーザ専用）（OIT）は、特定の show コマンドをサポートします。OIT を使用して、show コマンドの出力の分析を表示します。

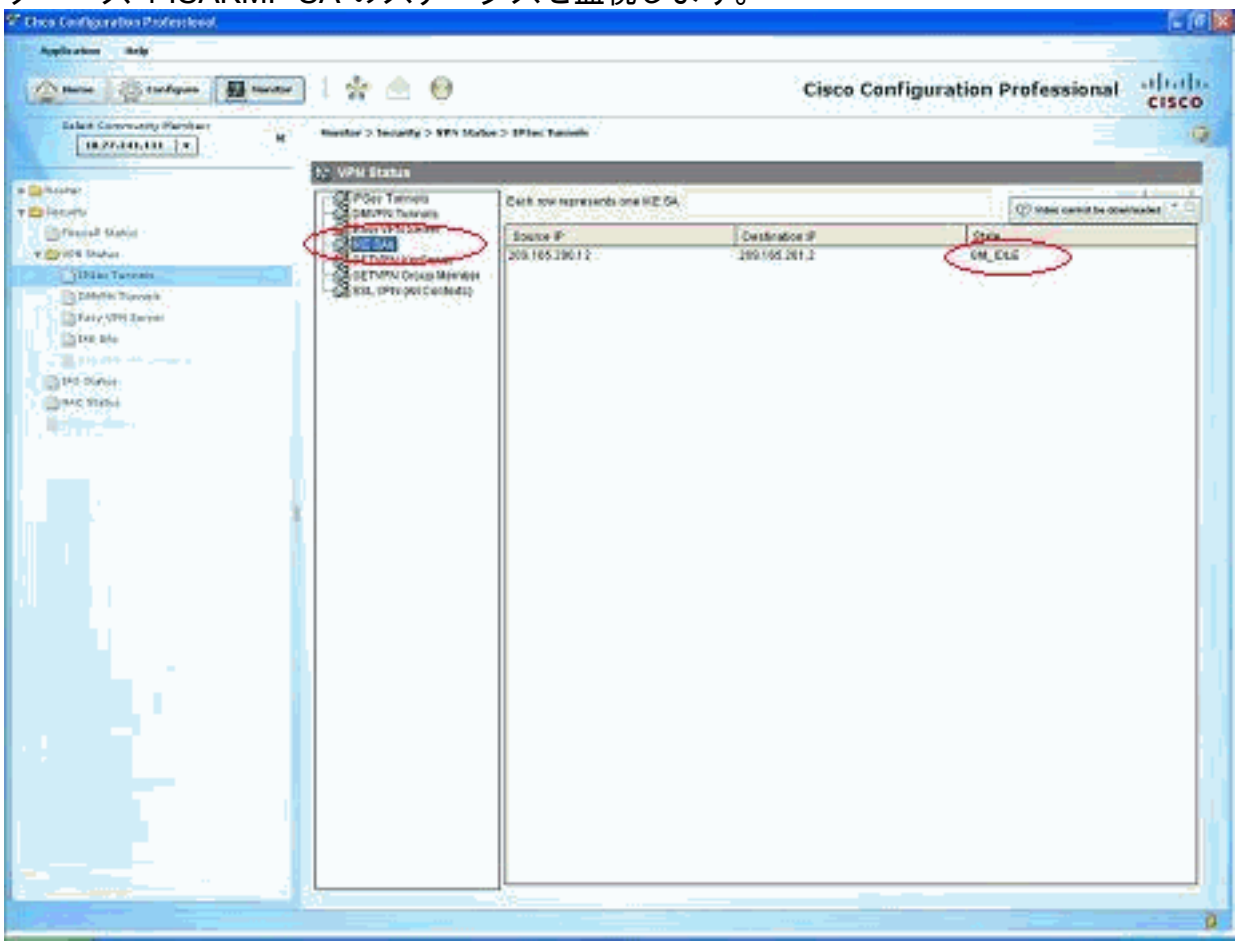
- CCP を使用したトンネル パラメータの確認
- ASA CLI を使用したトンネル ステータスの確認
- ルータの CLI を使用したトンネルパラメータの確認

CCP を使用したトンネル パラメータの確認

- トラフィックが IPSec トンネルを通過することを監視します。



- フェーズ 1 ISAKMP SA のステータスを監視します。



ASA CLI を使用したトンネル ステータスの確認

- フェーズ 1 ISAKMP SA のステータスを確認します。

```
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：応答側の役割を確認します。この役割は、このトンネルの発信側がもう一方の端（VPNルータなど）にあることを示します。

- フェーズ 2 IPSEC SA のパラメータを確認します。

```
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
```

ルータの CLI を使用したトンネルパラメータの確認

- フェーズ 1 ISAKMP SA のステータスを確認します。

```
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
```

- フェーズ 2 IPSEC SA のパラメータを確認します。

```
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:
```

トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

- 既存のクリプト接続を切断します。

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

VPN-Router#clear crypto isakmp
```

- VPN トンネルに関する問題をトラブルシューティングするには、debug コマンドを使用します。**注：デバッグ**を有効にすると、インターネットワークで高負荷状態が発生したときにルータの動作が中断する可能性があります。debugコマンド**は使用注意してください。一般に、これらのコマンドは、特定の障害をトラブルシューティングする場合に限り、必ずルータの技術サポート担当者の指示に従って使用することをお勧めします。**

```
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#
```

debug コマンドの詳細については、『debug コマンドの説明と使用』の「debug crypto isakmp」を参照してください。

関連情報

- IPsec ネゴシエーション/IKE プロトコルに関するサポート ページ
- Cisco ASA セキュリティ アプライアンス OS ソフトウェアに関するドキュメント
- 最も一般的な IPSec VPN のトラブルシューティング方法
- Requests for Comments (RFCs)