

目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[関連製品](#)

[表記法](#)

[設定](#)

[ネットワーク図](#)

[VPN トンネル ASDM の設定](#)

[ルータ SDM の設定](#)

[ASA CLI 設定](#)

[ルータ CLI 設定](#)

[確認](#)

[ASA/PIX セキュリティ アプライアンス - show コマンド](#)

[リモート IOS ルータ : show コマンド](#)

[トラブルシューティング](#)

[関連情報](#)

概要

このドキュメントでは、Cisco セキュリティ アプライアンス (ASA/PIX) と Cisco IOS ルータとの間の LAN-to-LAN (サイトツーサイト) IPsec トンネルの設定例を紹介しています。話を簡単にするため、スタティック ルートを使用します。

PIX/ASA セキュリティ アプライアンスでバージョン 7.x のソフトウェアが実行される場合と同じシナリオの詳細は、『[IOS ルータの LAN-to-LAN IPsec トンネルに対する PIX/ASA 7.x セキュリティ アプライアンスの設定例](#)』を参照してください。

前提条件

要件

この設定を行う前に、次の要件が満たされていることを確認します。

- この設定を開始する前に、エンドツーエンドの IP 接続を確立する必要があります。
- Data Encryption Standard (DES; データ暗号標準) の暗号化 (最小限の暗号化レベル) でセキュリティ アプライアンスのライセンスを有効にする必要があります。

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くものです。

- バージョン 8.x 以降が稼働する Cisco Adaptive Security Appliance (ASA; 適応型セキュリティ アプライアンス)
- ASDM バージョン 6.x 以降
- Cisco IOS® ソフトウェア リリース 12.3 が稼働する Cisco 1812 ルータ
- Cisco Security Device Manager (SDM) バージョン 2.5

注ASA を ASDM で設定できるようにするには、『[ASDM 用の HTTPS アクセスの許可](#)』を参照してください。

注ルータを SDM で設定できるようにするには、『[SDM を使用した基本的なルータ設定](#)』を参照してください。

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たものです。このドキュメントで使用するすべてのデバイスは、クリアな (デフォルト) 設定で作業を開始しています。ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

注ASA 関連の設定が ASDM GUI を使用して表示され、ルータ関連の設定が Cisco CP GUI を使用して表示される同様のシナリオについては、『[Configuration Professional: ルータの Cisco Configuration Professional \(CCP \) を使用した同じような設定のための ASA/PIX と IOSルータ 設定例間のサイト間の IPsec VPN](#)』。

関連製品

この設定は、バージョン 7.x 以降で稼働する Cisco PIX 500 シリーズ セキュリティ アプライアンスでも使用できます。

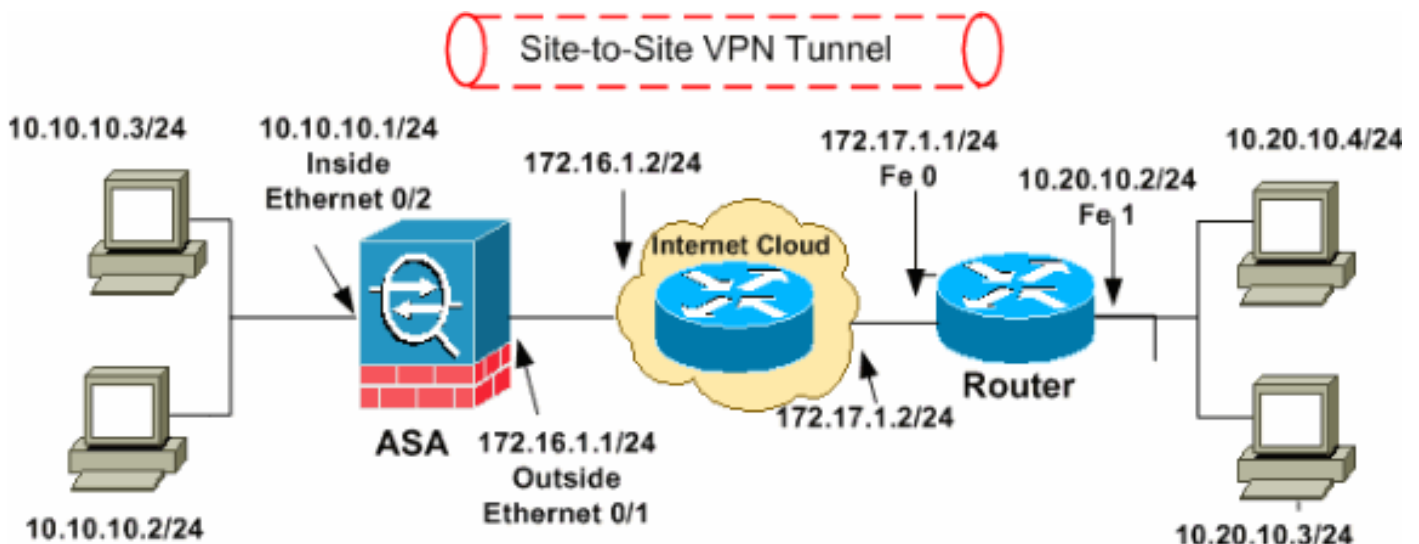
表記法

ドキュメント表記の詳細は、『[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。

設定

ネットワーク図

このドキュメントでは、次の図で示されるネットワーク構成を使用しています。



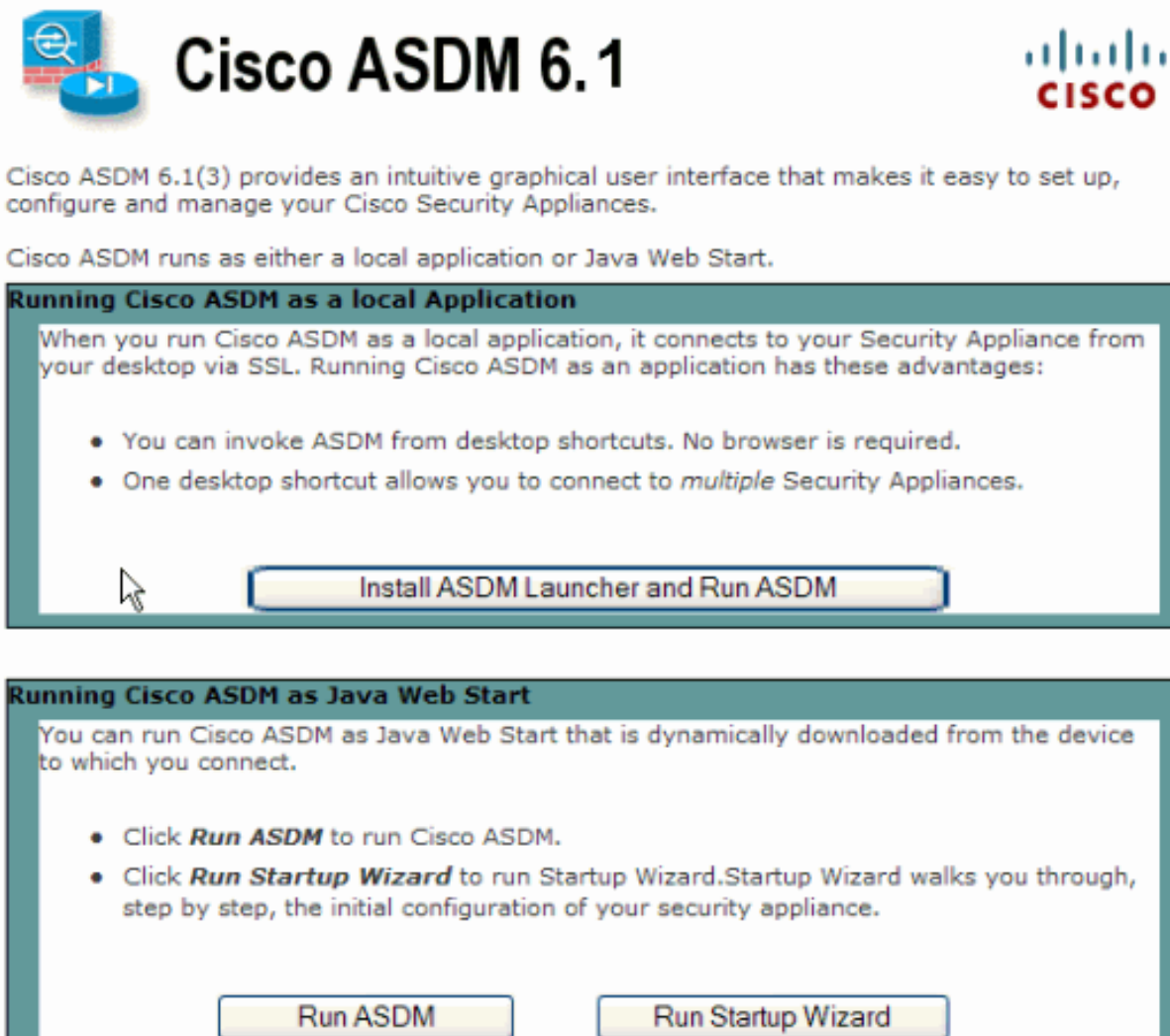
注この設定で使用している IP アドレス スキームは、インターネット上で正式にルーティング可能なものではありません。これらはラボ環境で使用された [RFC 1918](#) のアドレスです。 [🔗](#)

- [VPN トンネル ASDM の設定](#)
- [ルータ SDM の設定](#)
- [ASA CLI 設定](#)
- [ルータ CLI 設定](#)

VPN トンネル ASDM の設定

VPN トンネルを作成するには、次の手順を実行します。

1. ブラウザを開き、<https://<ASDMにアクセスするように設定されたASAのインターフェイスのIPアドレス>> を入力して、ASA 上の ASDM にアクセスします。SSL 証明書の信頼性に関連してブラウザから出力されるすべての警告を承認します。デフォルトのユーザ名とパスワードは、両方とも空白です。ASA がこのウィンドウを表示するのは、ASDM アプリケーションのダウンロードを許可するためです。次の例の場合、アプリケーションはローカル コンピュータにロードされ、Java アプレットでは動作しません。



Cisco ASDM 6.1

Cisco ASDM 6.1(3) provides an intuitive graphical user interface that makes it easy to set up, configure and manage your Cisco Security Appliances.

Cisco ASDM runs as either a local application or Java Web Start.

Running Cisco ASDM as a local Application

When you run Cisco ASDM as a local application, it connects to your Security Appliance from your desktop via SSL. Running Cisco ASDM as an application has these advantages:

- You can invoke ASDM from desktop shortcuts. No browser is required.
- One desktop shortcut allows you to connect to *multiple* Security Appliances.

Install ASDM Launcher and Run ASDM

Running Cisco ASDM as Java Web Start

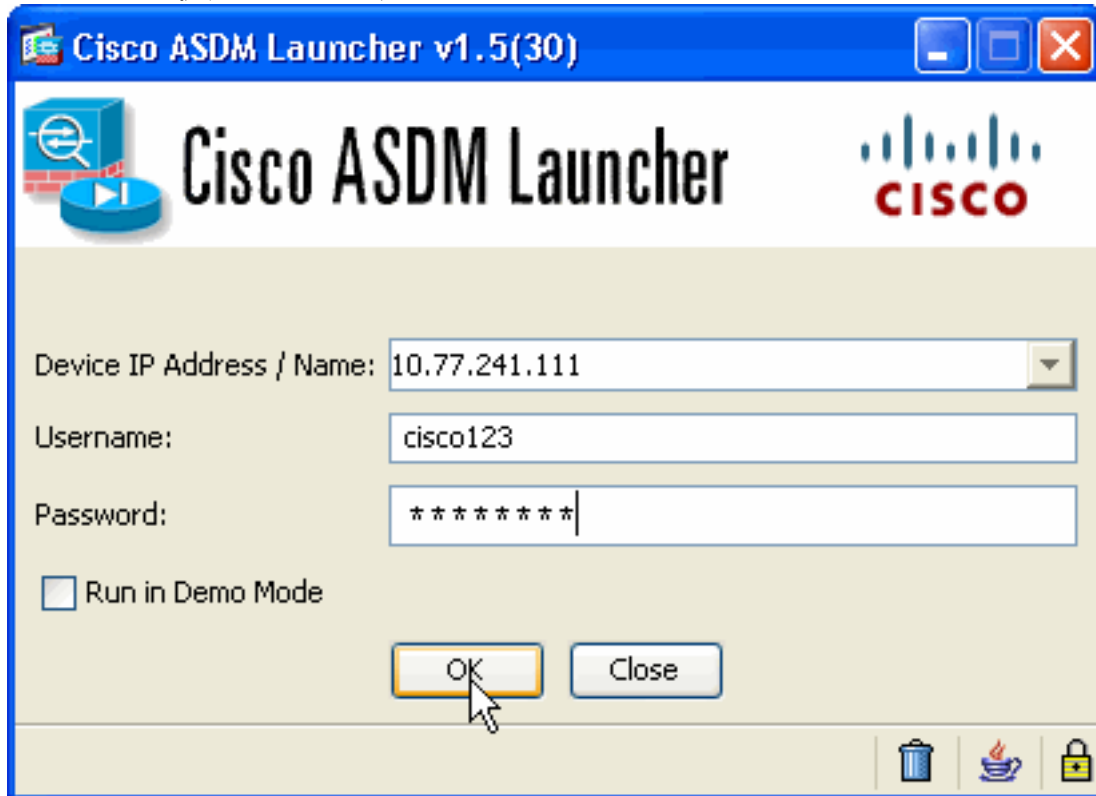
You can run Cisco ASDM as Java Web Start that is dynamically downloaded from the device to which you connect.

- Click **Run ASDM** to run Cisco ASDM.
- Click **Run Startup Wizard** to run Startup Wizard. Startup Wizard walks you through, step by step, the initial configuration of your security appliance.

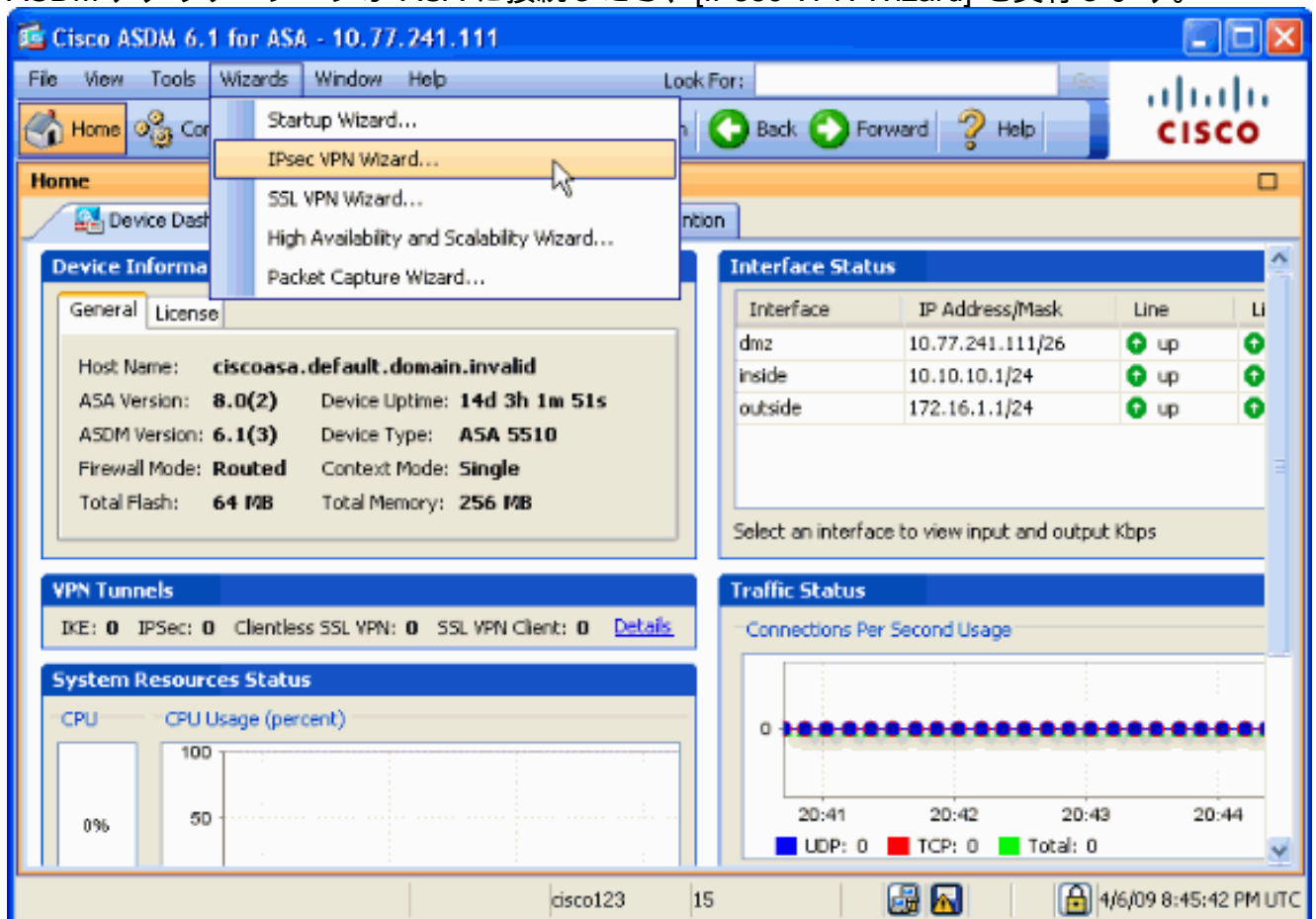
Run ASDM **Run Startup Wizard**

2. [Download ASDM Launcher and Start ASDM] をクリックして、ASDM アプリケーションのインストーラをダウンロードします。
3. ASDM Launcher がダウンロードされたら、プロンプトに従って一連のステップを実行し、該当ソフトウェアをインストールした後、Cisco ASDM Launcher を起動します。

4. http - コマンドで設定したインターフェイスの IP アドレスとユーザ名とパスワード (指定した場合) を入力します。次の例では、ユーザ名として `cisco123`、パスワードとして `cisco123` を使用しています。



5. ASDM アプリケーションが ASA に接続したら、[IPsec VPN Wizard] を実行します。



6. IPsec VPN トンネル タイプとして [Site-to-Site] を選択し、次のように [Next] をクリックします。



7. リモートピアの外部 IP アドレスを指定します。使用する認証情報（今の場合は事前共有鍵）を入力します。次の例では、**cisco123** という事前共有鍵を使用しています。[Tunnel Group Name] は、L2L VPN を設定する場合、デフォルトでは外部 IP アドレスになります。[Next] をクリックします。

The screenshot shows the 'VPN Wizard' window at 'Step 2 of 6: Remote Site Peer'. The left sidebar contains a network diagram with 'Branch', 'ISP', 'Home', and 'Corporate Network' components. The main area contains the following configuration fields:

- Peer IP Address: 172.17.1.1
- Authentication Method:
 - Pre-shared key
 - Pre-Shared Key: cisco123
 - Certificate
 - Certificate Signing Algorithm: rsa-sig
 - Certificate Name: [dropdown menu]
 - Challenge/response authentication (CRACK)
- Tunnel Group:
 - For site-to-site connections with pre-shared key authentication, the tunnel group name must be the same as either the peer IP address or the peer hostname, whichever is used as the peer's identity.
 - Tunnel Group Name: 172.17.1.1

At the bottom right, there are navigation buttons: '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'. The 'Next >' button is highlighted with a mouse cursor.

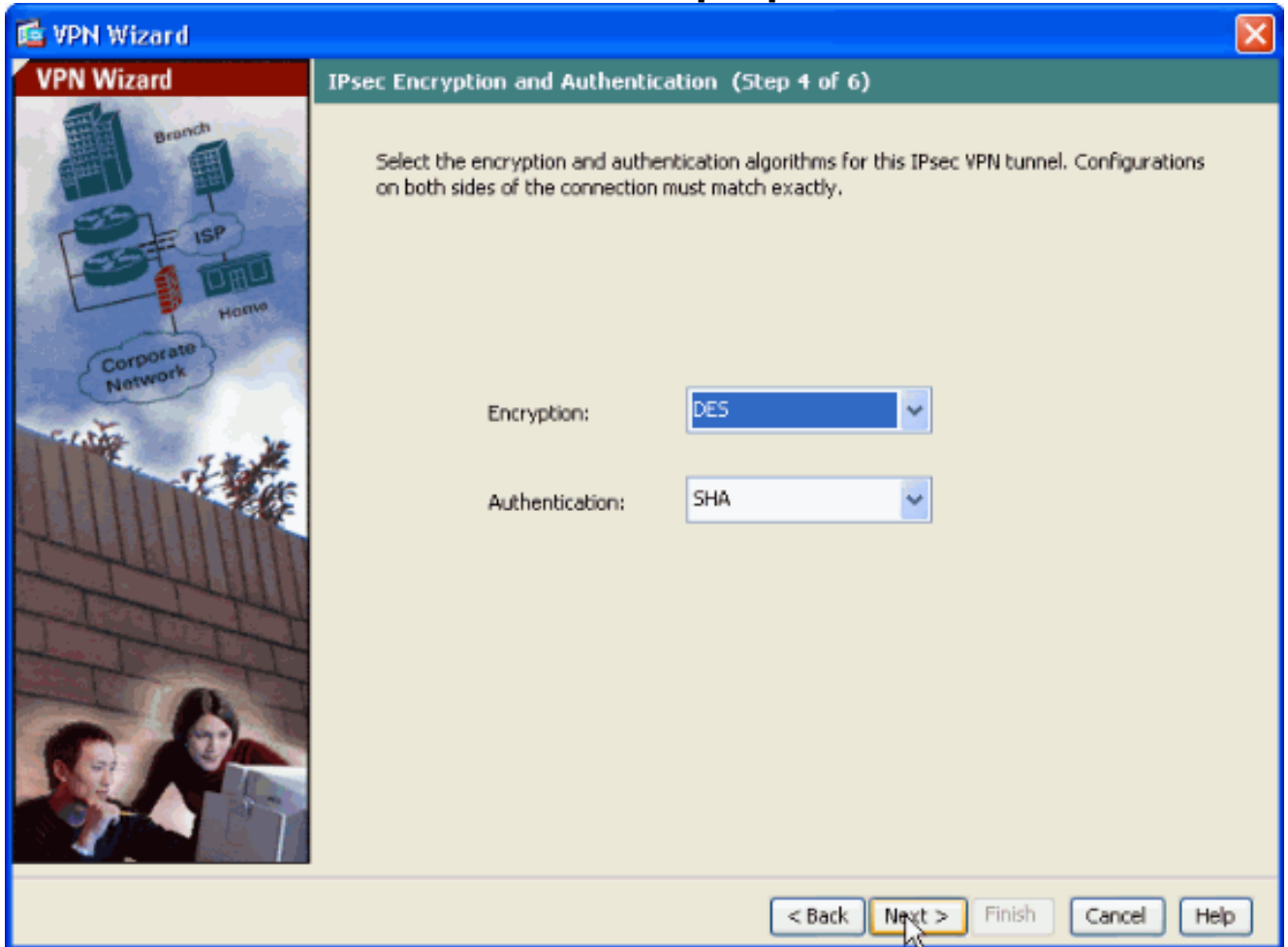
8. IKE（フェーズ 1ともいう）で使用する属性を指定します。それらの属性は、ASA および IOS ルータの両方で同じでなければなりません。[Next] をクリックします。

The screenshot shows the 'VPN Wizard' window at 'Step 3 of 6: IKE Policy'. The left sidebar is identical to the previous step. The main area contains the following configuration fields:

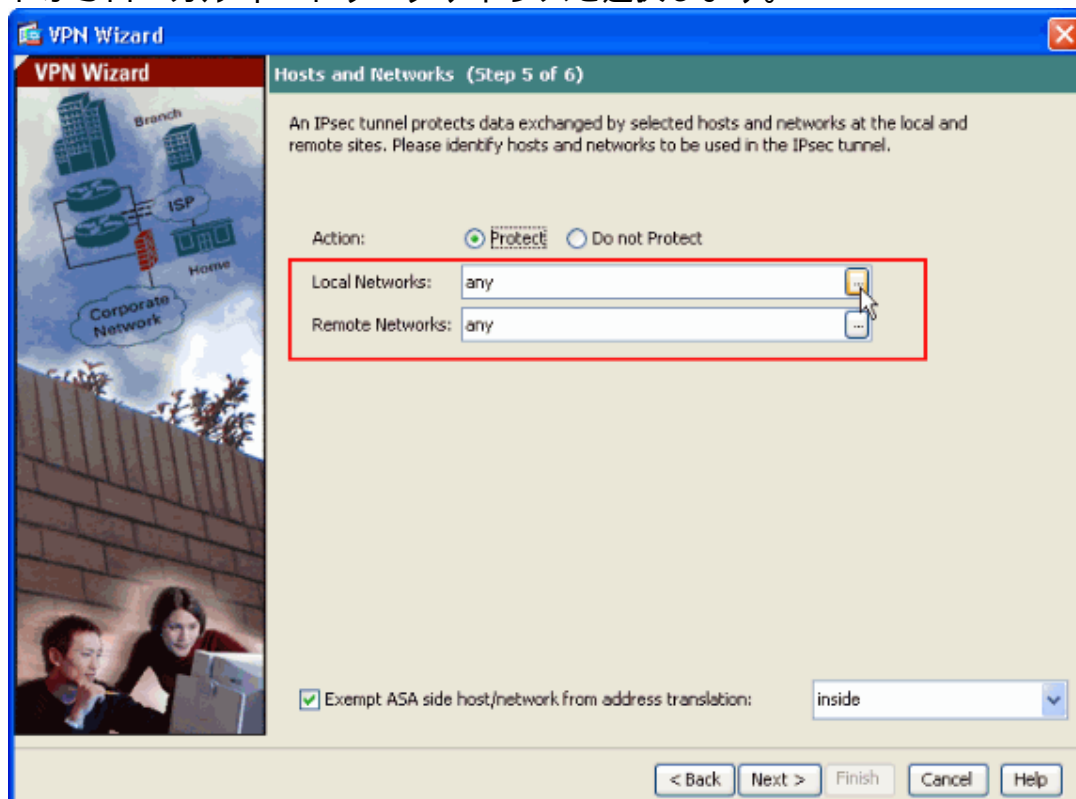
- Encryption: DES [dropdown menu]
- Authentication: SHA [dropdown menu]
- DH Group: [dropdown menu]

At the bottom right, there are navigation buttons: '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'. The 'Next >' button is highlighted with a mouse cursor.

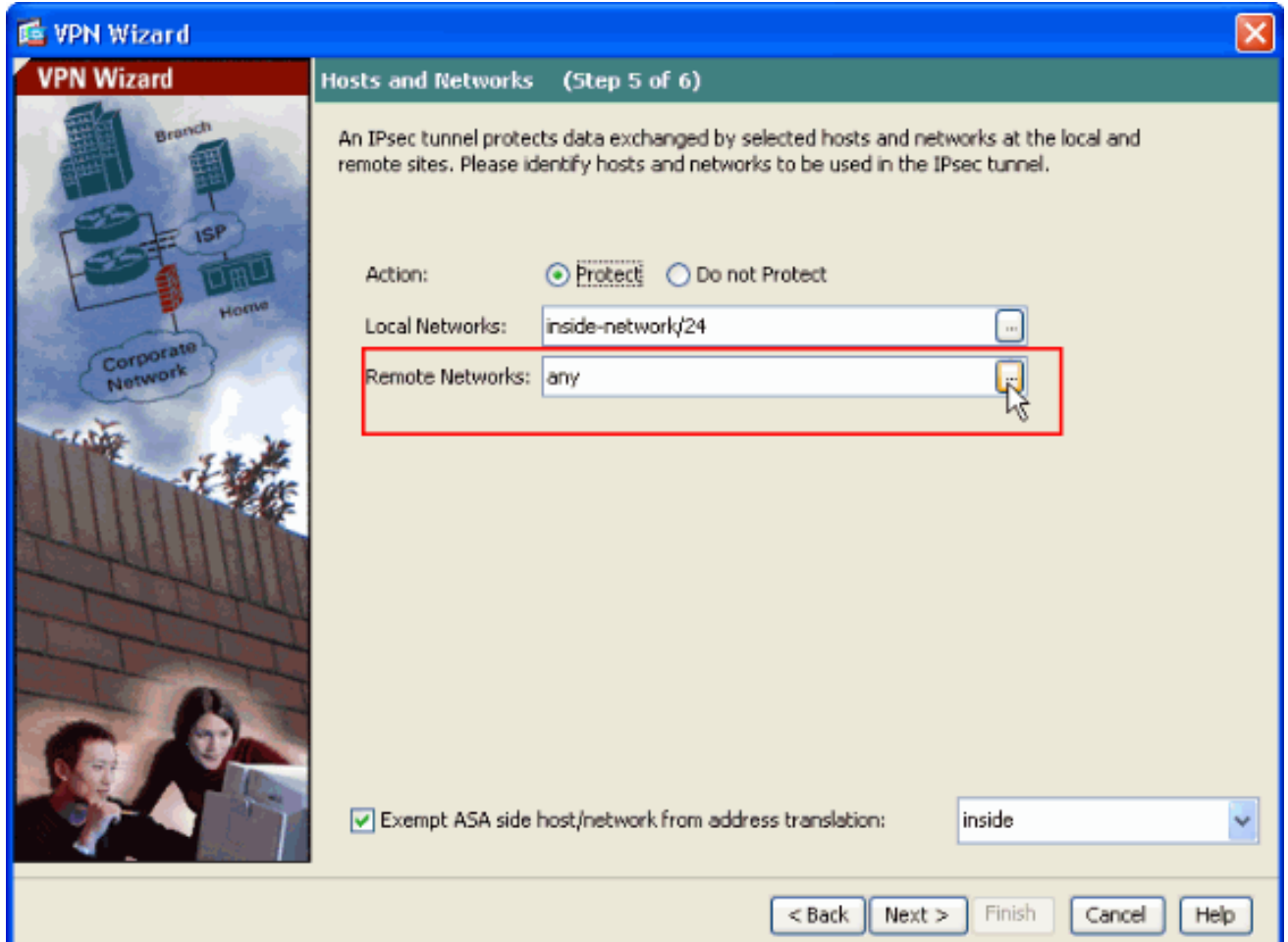
9. IPsec (フェーズ 2 ともいう) で使用する属性を指定します。それらの属性は、ASA および IOS ルータの両方で同じでなければなりません。[Next] をクリックします。



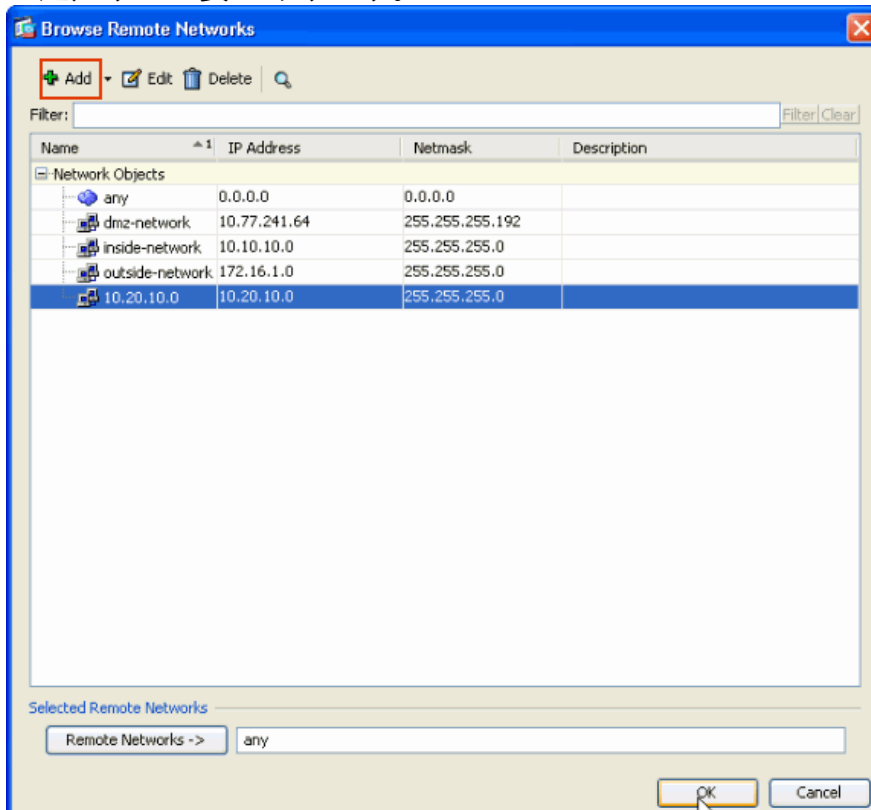
10. VPN トンネルを通過できるようなトラフィックのホストを指定します。このステップでは、VPN トンネルに対して [Local Networks] および [Remote Networks] を指定します。[Local Networks] の横にあるボタンを次の図のようにクリックして、ドロップダウンリストからローカル ネットワーク アドレスを選択します。



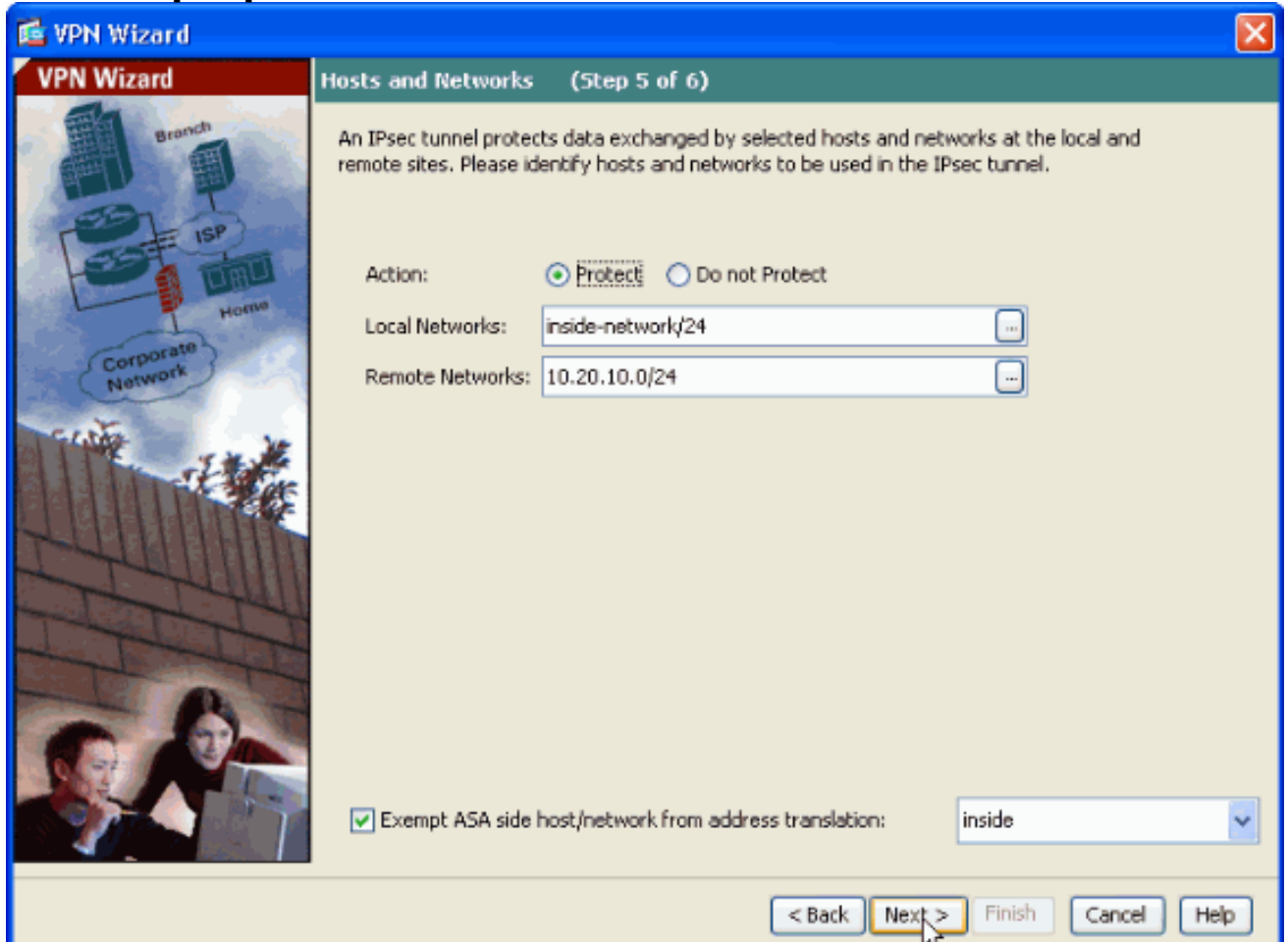
- ローカル ネットワーク アドレスを選択し、図のように [OK] をクリックします。
- [Remote Networks] の横にあるボタンを次の図のようにクリックして、ドロップダウン リストからリモート ネットワーク アドレスを選択します。



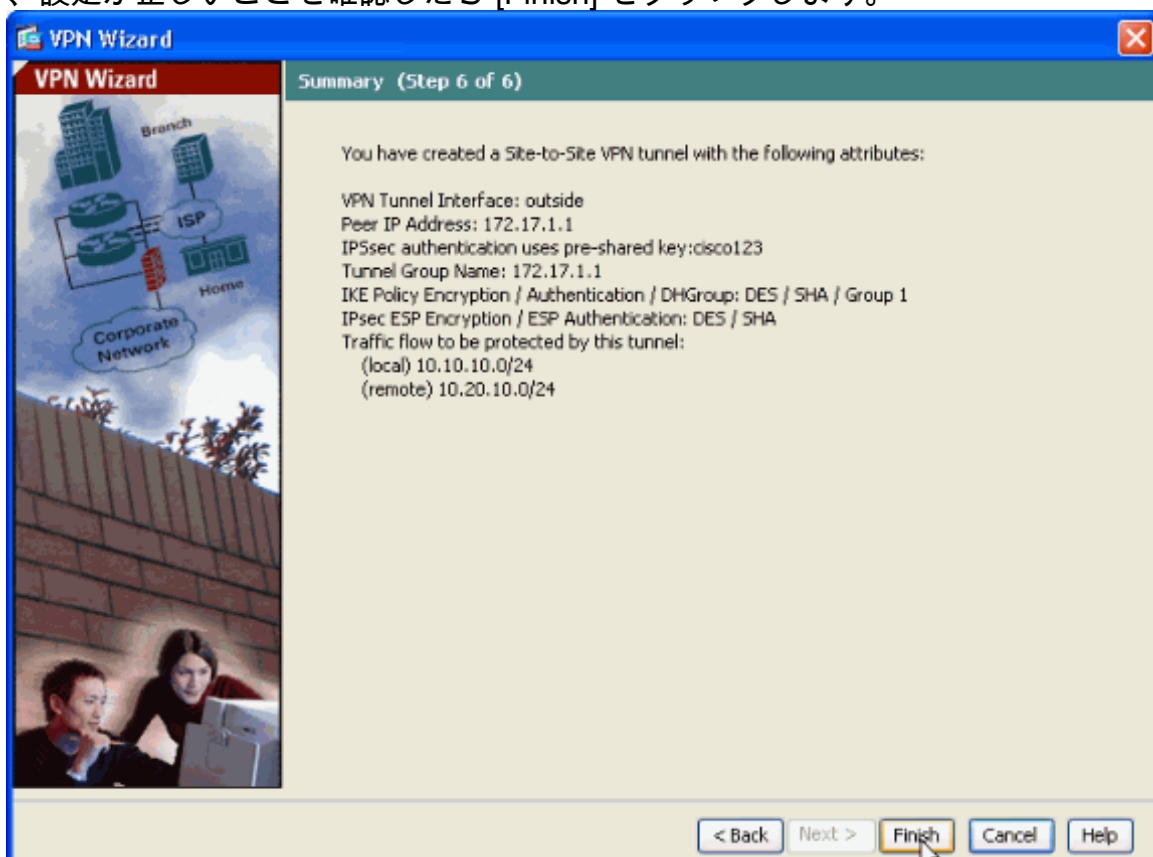
- リモート ネットワーク アドレスを選択し、図のように [OK] をクリックします。注リスト内にリモート ネットワークがない場合は、[Add] をクリックして、ネットワークをリストに追加する必要があります。



14. [Exempt ASA side host/network from address translation] チェックボックスにチェックマークを入れ、トンネルのトラフィックが **Network Address Translation** を受けないようにします。次に、[Next] をクリックします。



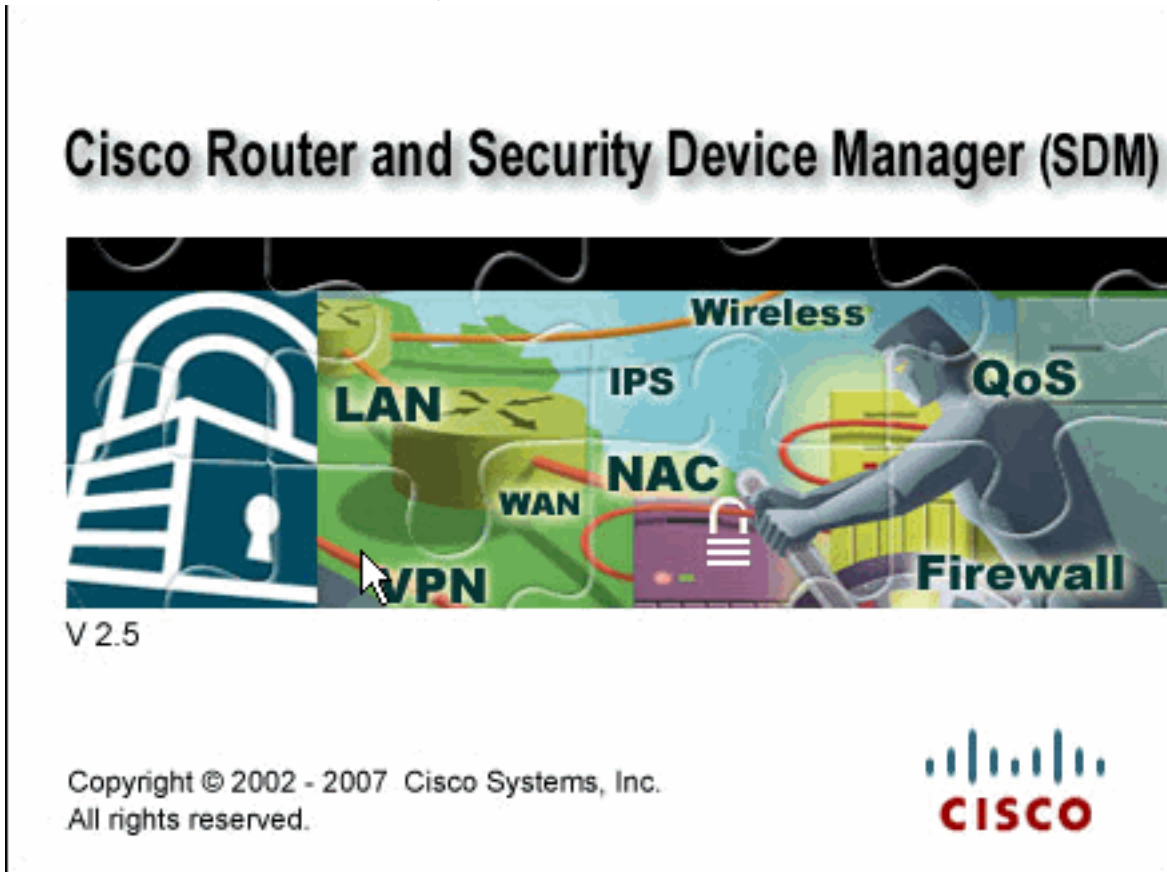
15. VPN Wizardによって定義された属性が、次の要約画面に表示されます。設定を再確認し、設定が正しいことを確認したら [Finish] をクリックします。



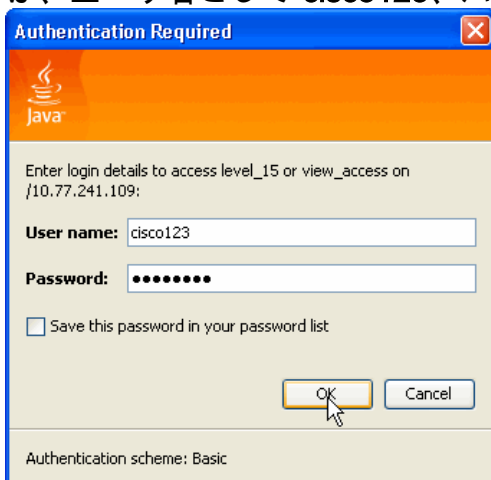
ルータ SDM の設定

Cisco IOS ルータ上でサイト間 VPN トンネルの設定を実行するには、次のステップを実行します。

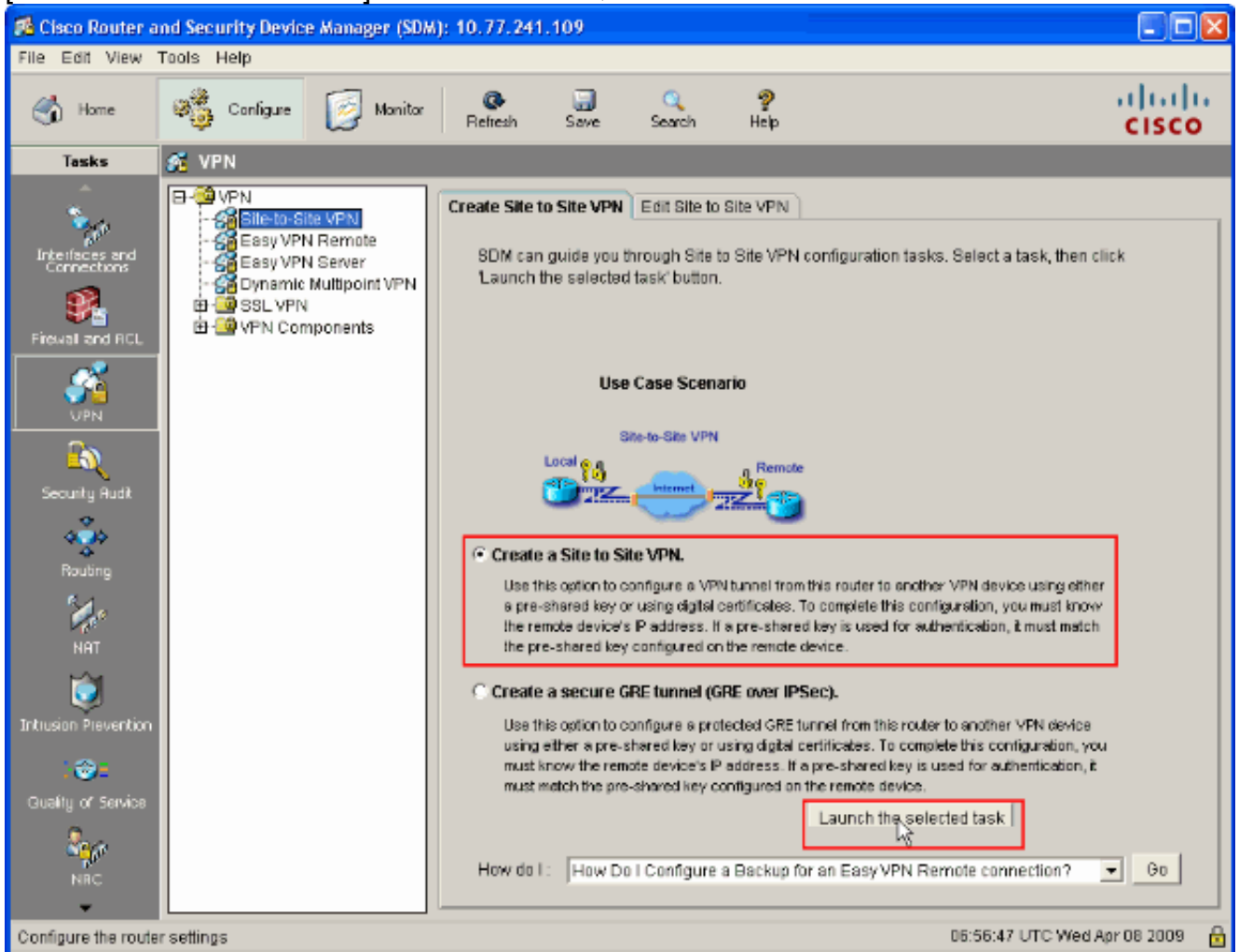
1. ブラウザを開き、<https://<SDMにアクセスするように設定されたルータのインターフェイスのIPアドレス>> と入力して、ルータ上の SDM にアクセスします。SSL 証明書の信頼性に関連してブラウザから出力されるすべての警告を承認します。デフォルトのユーザ名とパスワードは、両方とも空白です。ルータがこのウィンドウを表示するのは、SDM アプリケーションのダウンロードを許可するためです。次の例の場合、アプリケーションはローカルコンピュータにロードされ、Java アプレットでは動作しません。



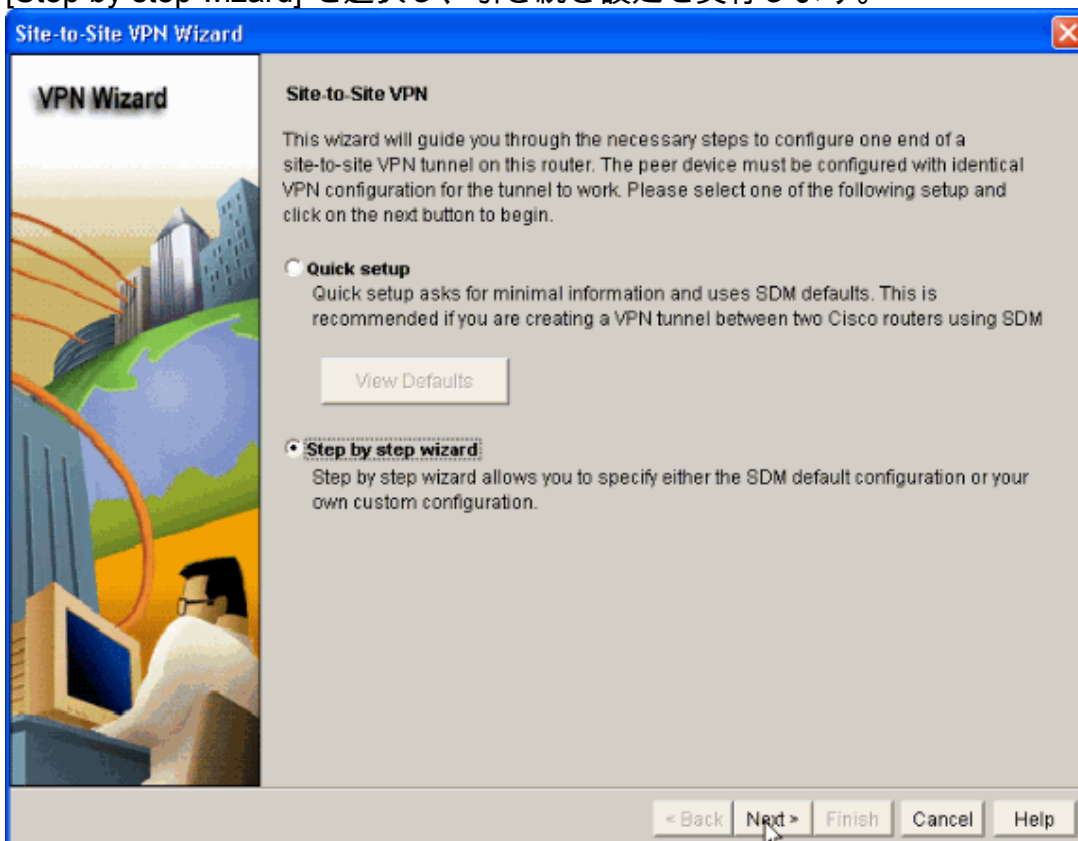
2. SDM のダウンロードが開始されます。SDM Launcher がダウンロードされたら、ソフトウェアをインストールし、Cisco SDM Launcher を実行するために、プロンプトに従って一連の手順を完了します。
3. ユーザ名とパスワードを、指定してある場合は入力し、[OK] をクリックします。次の例では、ユーザ名として **cisco123**、パスワードとして **cisco123** を使用しています。



4. [Configuration] -> [VPN] -> [Site-to-Site VPN] を選択した後、SDM ホーム ページ上で [Create a Site-to-Site VPN] の隣にあるラジオ ボタンをクリックします。次のように、[Launch The selected Task] をクリックします。



5. [Step by step wizard] を選択し、引き続き設定を実行します。



6. 次のウィンドウのそれぞれの部分で、VPN 接続情報を指定します。VPN トンネルのインターフェイスを、ドロップダウンリストから選択します。ここでは、[FastEthernet0] を選択しています。[Peer Identity] セクションでは、[Peer with static IP address] を選択し、リモートピアの IP アドレスを指定しています。[Authentication] セクションでは、[Pre-shared key] (事前共有鍵) (ここでは cisco123) を指定しています。次に、[Next] をクリックします。

Site-to-Site VPN Wizard

VPN Wizard

VPN Connection Information

Select the interface for this VPN connection: FastEthernet0 Details...

Peer Identity

Select the type of peer(s) used for this VPN connection: Peer with static IP address

Enter the IP address of the remote peer: 172.16.1.1

Authentication

Authentication ensures that each end of the VPN connection uses the same secret key.

Pre-shared Keys Digital Certificates

pre-shared key: *****

Re-enter Key: *****

< Back Next > Finish Cancel Help

7. [Add] をクリックして、暗号化アルゴリズム、認証アルゴリズム、および 鍵交換方法を指定する IKE プロポーザルを追加します。

Site-to-Site VPN Wizard

VPN Wizard

IKE Proposals

IKE proposals specify the encryption algorithm, authentication algorithm and key exchange method that is used by this router when negotiating a VPN connection with the remote device. For the VPN connection to be established with the remote device, the remote device should be configured with at least one of the policies listed below.

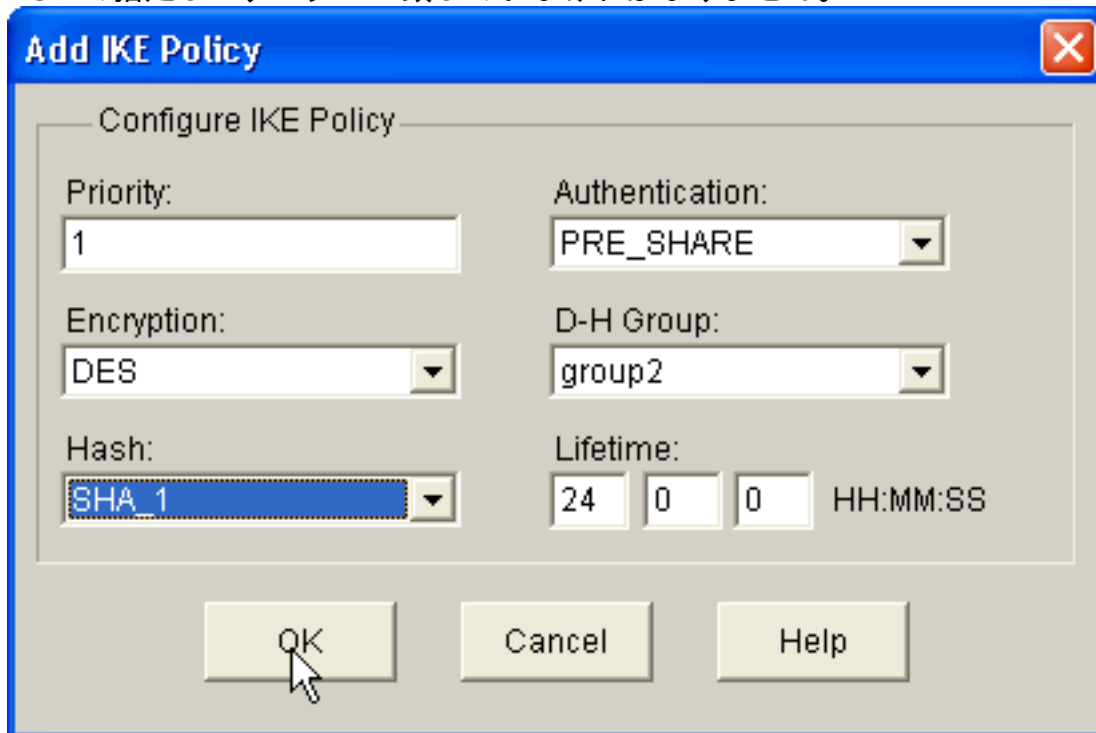
Click the Add... button to add more policies and the Edit... button to edit an existing policy.

Priority	Encryption	Hash	D-H Group	Authentication	Type
----------	------------	------	-----------	----------------	------

Add... Edit...

< Back Next > Finish Cancel Help

8. 暗号化アルゴリズム、認証アルゴリズム、および鍵交換方法を次のように指定し、[OK] をクリックします。暗号化アルゴリズム、認証アルゴリズム、および鍵交換方法の値は、ASA で指定したデータと一致していなければなりません。

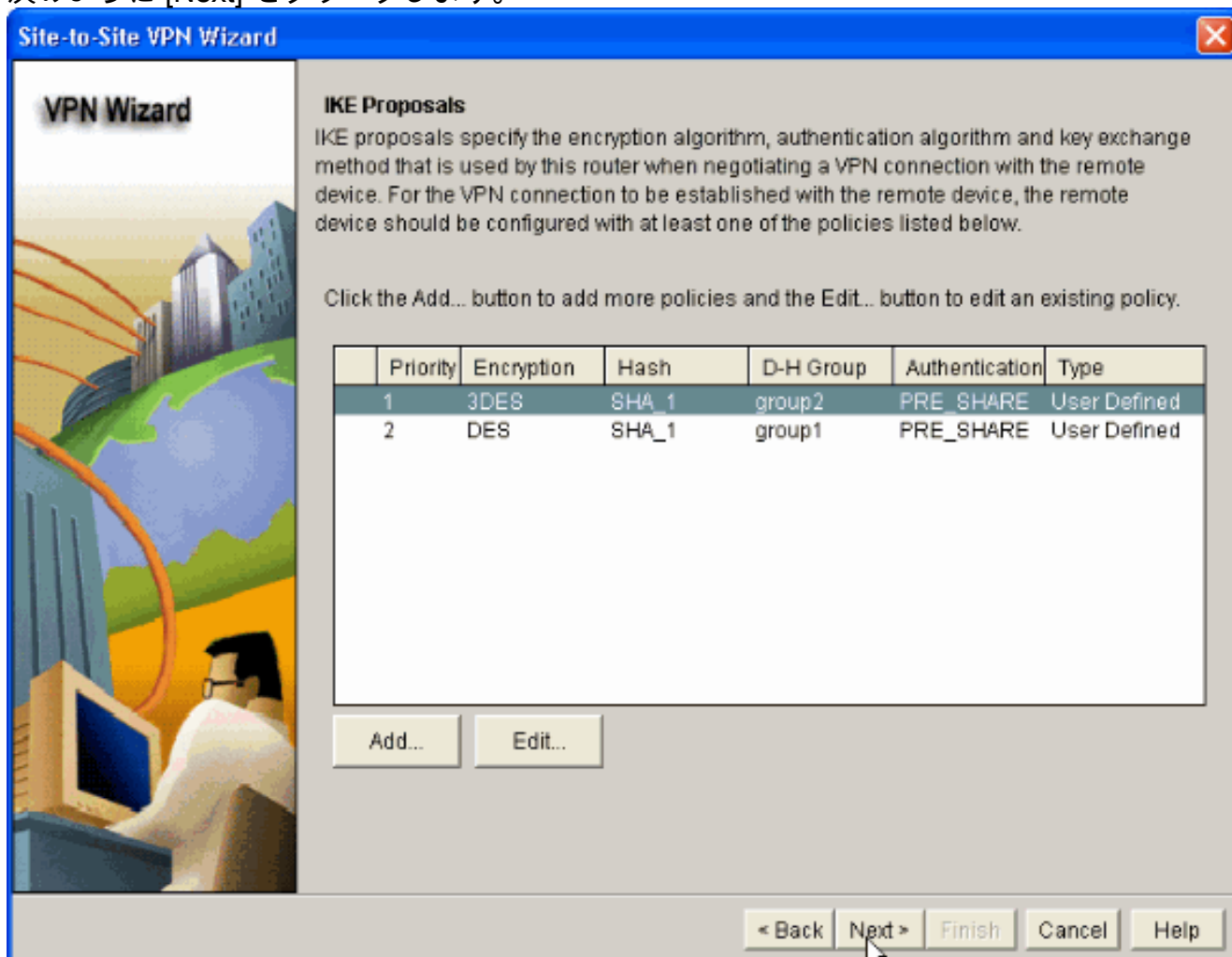


The dialog box titled "Add IKE Policy" contains the following configuration fields:

- Priority: 1
- Authentication: PRE_SHARE
- Encryption: DES
- D-H Group: group2
- Hash: SHA_1
- Lifetime: 24 0 0 HH:MM:SS

Buttons: OK, Cancel, Help

9. 次のように [Next] をクリックします。



The "Site-to-Site VPN Wizard" window shows the "IKE Proposals" section. It includes an illustration of a person at a computer on the left. The main area contains the following text:

IKE Proposals
IKE proposals specify the encryption algorithm, authentication algorithm and key exchange method that is used by this router when negotiating a VPN connection with the remote device. For the VPN connection to be established with the remote device, the remote device should be configured with at least one of the policies listed below.

Click the Add... button to add more policies and the Edit... button to edit an existing policy.

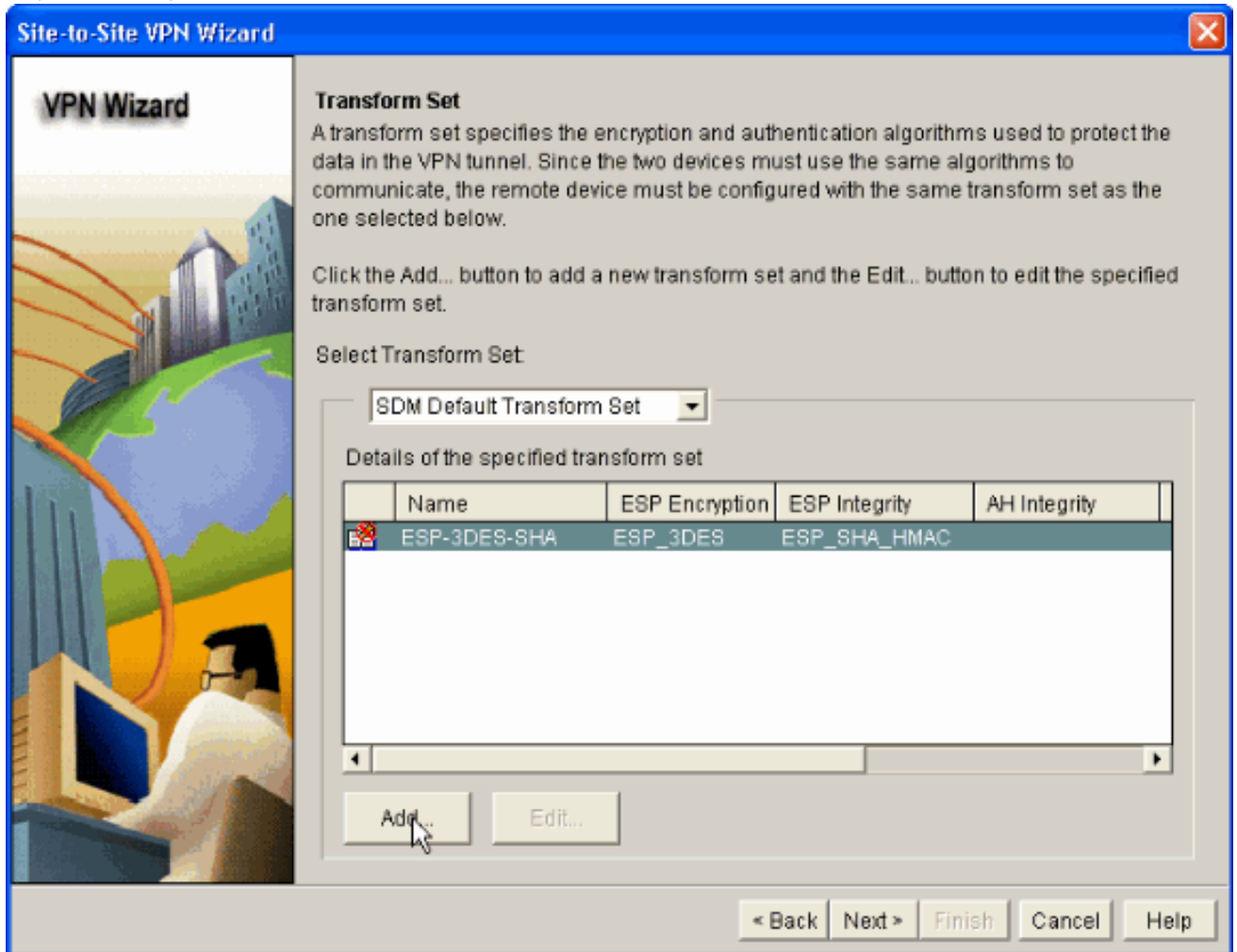
Priority	Encryption	Hash	D-H Group	Authentication	Type
1	3DES	SHA_1	group2	PRE_SHARE	User Defined
2	DES	SHA_1	group1	PRE_SHARE	User Defined

Buttons: Add..., Edit...

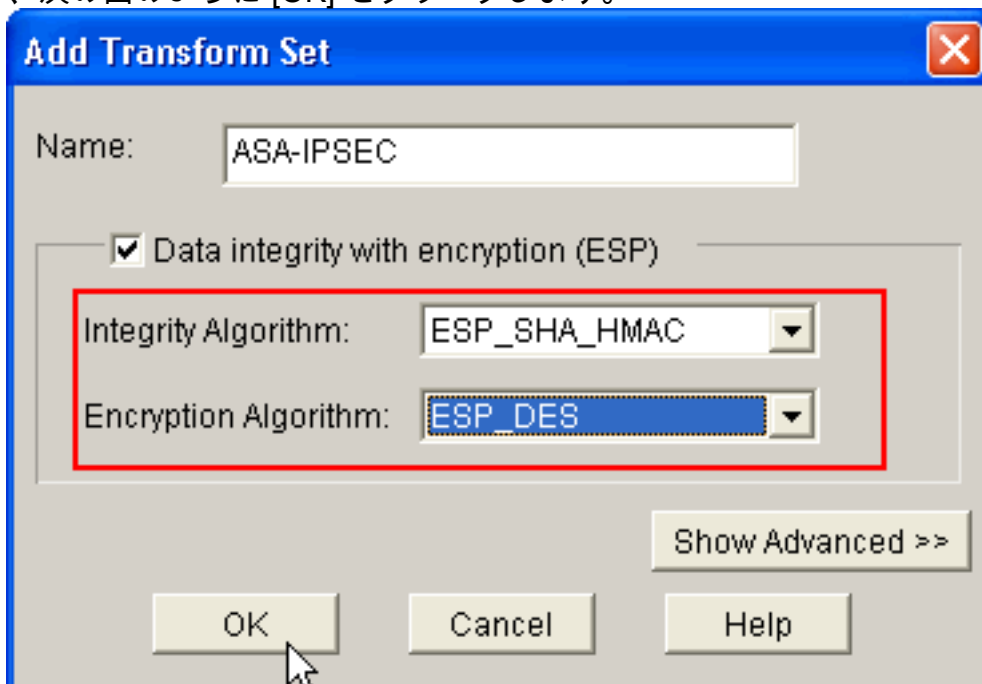
Navigation buttons at the bottom: < Back, Next >, Finish, Cancel, Help

10. 次の新しいウィンドウではトランスフォームセットを指定します。トランスフォームセットでは、VPN トンネルのデータを保護するのに使用する暗号化アルゴリズムと認証アル

ゴリズムを指定します。次に、[Add] をクリックして、詳細情報を設定します。[Add] をクリックし、詳細情報を指定すれば、トランスフォーム セットは必要に応じていくつでも追加できます。



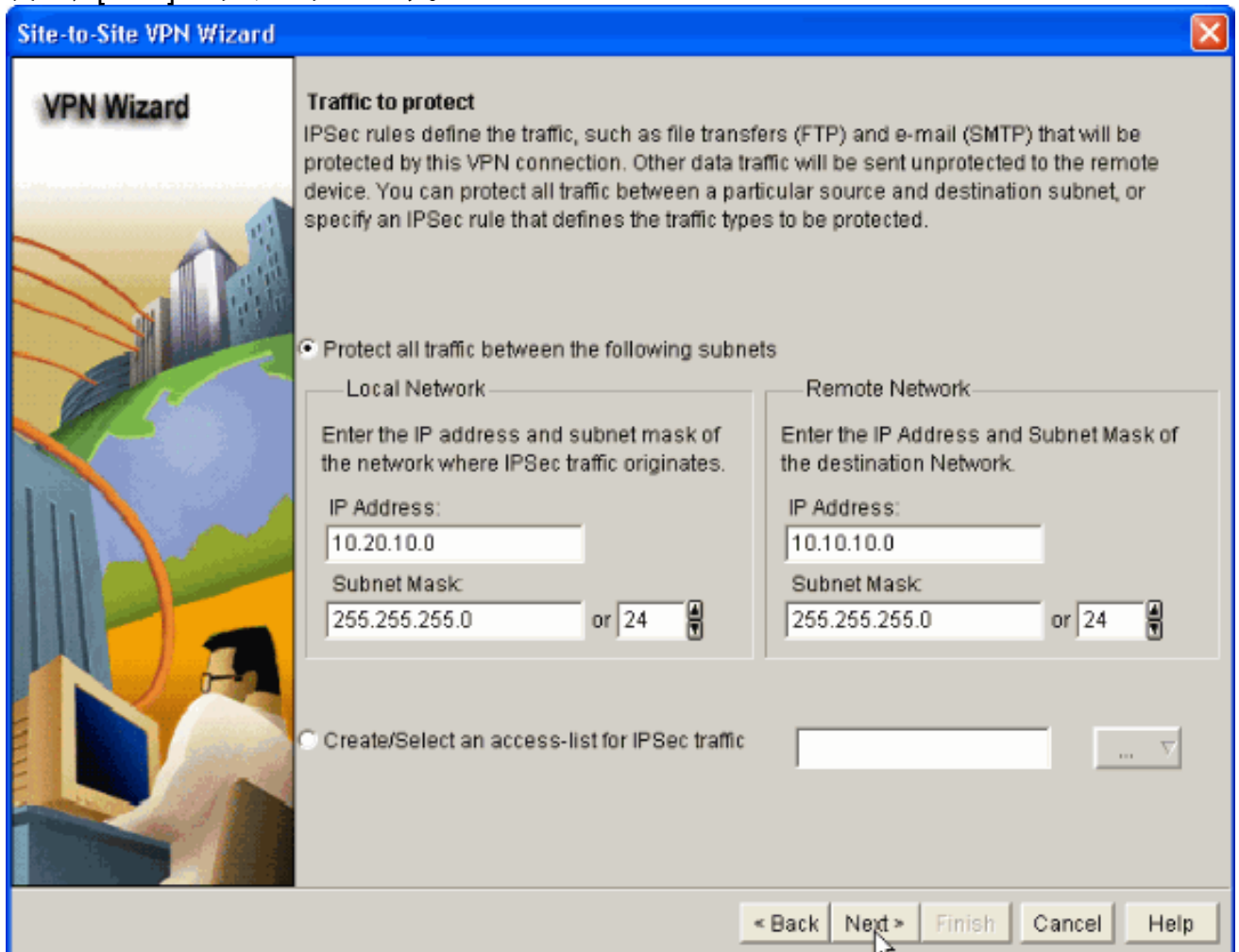
11. トランスフォーム セットの詳細情報 (暗号化アルゴリズムと認証アルゴリズム) を指定し、次の図のように [OK] をクリックします。



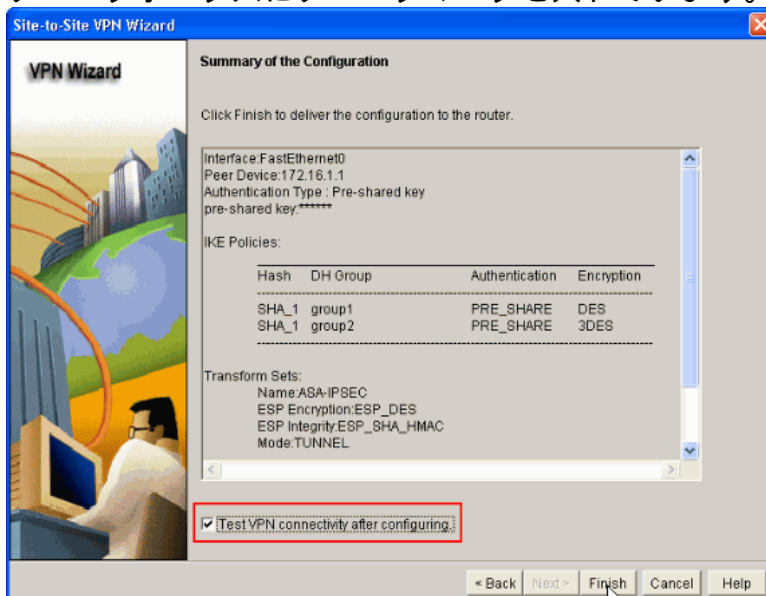
12. 次の図のように、使用する必要なトランスフォーム セットを、ドロップダウン リストから選択します。



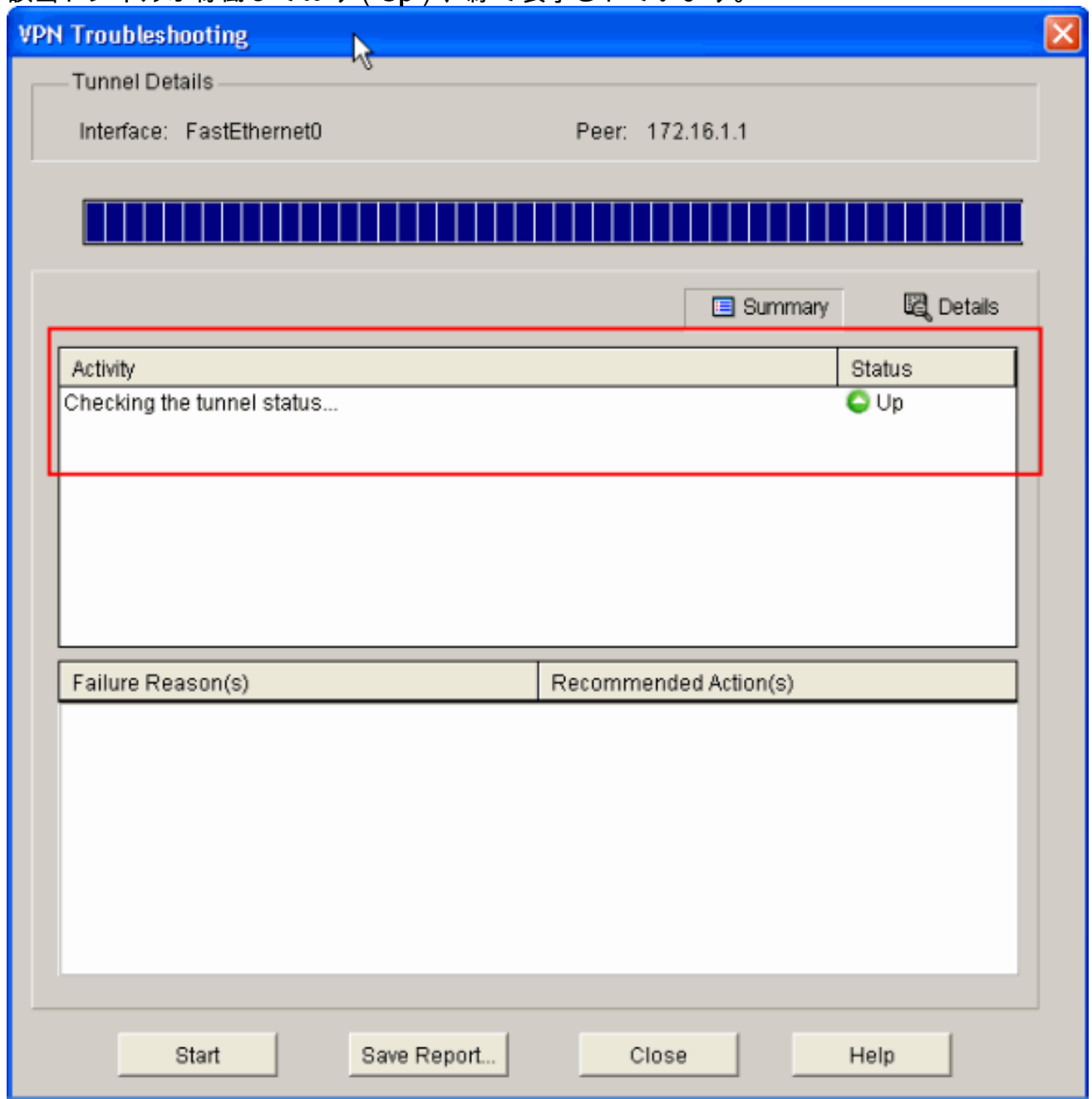
13. [Next] をクリックします。
14. 次のウィンドウで、VPNトンネルによって保護するトラフィックの詳細情報を指定します。保護するトラフィックの送信元ネットワークおよび宛先ネットワークを指定し、指定した送信元ネットワーク～宛先ネットワーク間のトラフィックが保護されるようにします。次の例の場合、送信元ネットワークは 10.20.10.0、宛先ネットワークは 10.10.10.0 です。次に、[Next] をクリックします。



15. 次のウィンドウは、実施したサイト間 VPN 設定の要約を示しています。VPN の接続をテストする場合は、[Test VPN Connectivity after configuring] チェックボックスにチェックマークを入れてください。今の場合、VPN の接続をチェックする必要があるため、該当するチェックボックスにチェックマークを入れています。次に、[Finish] をクリックします



16. 次の図のように、[Start] をクリックして、VPN の接続をチェックします。
17. 次のウィンドウに、VPN 接続テストの結果を示します。このウィンドウを見ると、該当トンネルが稼働している (Up) かしていない (Down) がわかります。この設定例では、該当トンネルが稼働しており (Up)、緑で表示されています。



Cisco IOS ルータの設定は、これで終わりです。

ASA CLI 設定

ASA

```
ASA#show run: SavedASA Version 8.0(2) !hostname
ASAenable password 8Ry2YjIyt7RRXU24 encryptednames!!---
Configure the outside interface. !interface Ethernet0/1
nameif outside security-level 0 ip address 172.16.1.1
255.255.255.0 !--- Configure the inside interface.
!interface Ethernet0/2 nameif inside security-level 100
ip address 10.10.10.1 255.255.255.0 !-- Output
suppressed !passwd 2KFQnbNIdI.2KYOU encryptedftp mode
passivedns server-group DefaultDNS domain-name
```

```

default.domain.invalidaccess-list 100 extended permit ip
any anyaccess-list inside_nat0_outbound extended permit
ip 10.10.10.0 255.255.255.0 10.20.10.0 255.255.255.0 !--
- This access list (inside_nat0_outbound) is used !---
with the nat zero command. This prevents traffic which
!--- matches the access list from undergoing network
address translation (NAT). !--- The traffic specified by
this ACL is traffic that is to be encrypted and !---
sent across the VPN tunnel. This ACL is intentionally !-
-- the same as (outside_1_cryptomap). !--- Two separate
access lists should always be used in this
configuration.access-list outside_1_cryptomap extended
permit ip 10.10.10.0 255.255.255.0 10.20.10.0
255.255.255.0!--- This access list (outside_cryptomap)
is used !--- with the crypto map outside_map !--- to
determine which traffic should be encrypted and sent !--
- across the tunnel. !--- This ACL is intentionally the
same as (inside_nat0_outbound). !--- Two separate access
lists should always be used in this configuration.pager
lines 24mtu inside 1500mtu outside 1500no failoverasdm
image disk0:/asdm-613.binasdm history enablearp timeout
14400global (outside) 1 interfacenat (inside) 1
10.10.10.0 255.255.255.0nat (inside) 0 access-list
inside_nat0_outbound!--- NAT 0 prevents NAT for networks
specified in !--- the ACL inside_nat0_outbound.access-
group 100 in interface outsidersroute outside 0.0.0.0
0.0.0.0 172.16.1.2 1timeout xlate 3:00:00timeout conn
1:00:00 half-closed 0:10:00 udp 0:02:00 icmp
0:00:02timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00
mgcp 0:05:00timeout mgcp-pat 0:05:00 sip 0:30:00
sip_media 0:02:00timeout uauth 0:05:00 absolutehttp
server enablehttp 0.0.0.0 0.0.0.0 dmzno snmp-server
locationno snmp-server contact!--- PHASE 2 CONFIGURATION
---! !--- The encryption types for Phase 2 are defined
here.crypto ipsec transform-set ESP-DES-SHA esp-des esp-
sha-hmac!--- Define the transform set for Phase 2.crypto
map outside_map 1 match address outside_1_cryptomap!---
Define which traffic should be sent to the IPsec
peer.crypto map outside_map 1 set peer 172.17.1.1!---
Sets the IPsec peercrypto map outside_map 1 set
transform-set ESP-DES-SHA!--- Sets the IPsec transform
set "ESP-AES-256-SHA" !--- to be used with the crypto
map entry "outside_map".crypto map outside_map interface
outside!--- Specifies the interface to be used with !---
the settings defined in this configuration.!--- PHASE 1
CONFIGURATION ---! !--- This configuration uses isakmp
policy 10. !--- The configuration commands here define
the Phase !--- 1 policy parameters that are used.crypto
isakmp enable outsidecrypto isakmp policy 10
authentication pre-share encryption des hash sha group 1
lifetime 86400telnet timeout 5ssh timeout 5console
timeout 0threat-detection basic-threatthreat-detection
statistics access-list! tunnel-group 172.17.1.1 type
ipsec-l2l!--- In order to create and manage the database
of connection-specific !--- records for ipsec-l2l?IPsec
(LAN-to-LAN) tunnels, use the command !--- tunnel-group
in global configuration mode. !--- For L2L connections
the name of the tunnel group MUST be the IP !--- address
of the IPsec peer.tunnel-group 172.17.1.1 ipsec-
attributes pre-shared-key *!--- Enter the pre-shared-key
in order to configure the !--- authentication
method.telnet timeout 5ssh timeout 5console timeout
0threat-detection basic-threatthreat-detection

```



```
statistics access-list!class-map inspection_default
match default-inspection-traffic!! !-- Output
suppressed!username cisco123 password ffIRPGpDSOJh9YLq
encrypted privilege
15Cryptochecksum:be38dfaef777a339b9e1c89202572a7d: end
```

ルータ CLI 設定

ルータ

```
Building configuration...Current configuration : 2403
bytes!version 12.3service timestamps debug datetime
msecservice timestamps log datetime msecservice
password-encryption!hostname R3!boot-start-markerboot-
end-marker!no logging buffered!username cisco123
privilege 15 password 7 1511021F07257A767Bno aaa new-
modelip subnet-zero!!ip cef!!ip ips po max-events 100no
ftp-server write-enable!!-- Configuration for IKE
policies. !--- Enables the IKE policy configuration
(config-isakmp) !--- command mode, where you can specify
the parameters that !--- are used during an IKE
negotiation. Encryption and Policy details are hidden as
the default values are chosen.crypto isakmp policy 2
authentication pre-share!--- Specifies the pre-shared
key "cisco123" which should !--- be identical at both
peers. This is a global !--- configuration mode
command.crypto isakmp key cisco123 address
172.16.1.1!!!-- Configuration for IPsec policies. !---
Enables the crypto transform configuration mode, !---
where you can specify the transform sets that are used
!--- during an IPsec negotiation.crypto ipsec transform-
set ASA-IPSEC esp-des esp-sha-hmac !!-- !--- Indicates
that IKE is used to establish !--- the IPsec Security
Association for protecting the !--- traffic specified by
this crypto map entry.crypto map SDM_CMAP_1 1 ipsec-
isakmp description Tunnel to172.16.1.1 !--- !--- Sets
the IP address of the remote end. set peer 172.16.1.1 !-
-- !--- Configures IPsec to use the transform-set !---
"ASA-IPSEC" defined earlier in this configuration. set
transform-set ASA-IPSEC !--- !--- Specifies the
interesting traffic to be encrypted. match address
100!!!!-- Configures the interface to use the !---
crypto map "SDM_CMAP_1" for IPsec.interface
FastEthernet0 ip address 172.17.1.1 255.255.255.0 duplex
auto speed auto crypto map SDM_CMAP_1!interface
FastEthernet1 ip address 10.20.10.2 255.255.255.0 duplex
auto speed auto!interface FastEthernet2 no ip
address!interface Vlan1 ip address 10.77.241.109
255.255.255.192!ip classlessip route 10.10.10.0
255.255.255.0 172.17.1.2ip route 10.77.233.0
255.255.255.0 10.77.241.65ip route 172.16.1.0
255.255.255.0 172.17.1.2!!ip nat inside source route-map
nonat interface FastEthernet0 overload!ip http serverip
http authentication localip http secure-server!!--
Configure the access-lists and map them to the Crypto
map configured.access-list 100 remark SDM_ACL
Category=4access-list 100 remark IPsec Ruleaccess-list
100 permit ip 10.20.10.0 0.0.0.255 10.10.10.0
0.0.0.255!!!!-- This ACL 110 identifies the traffic
flows using route map access-list 110 deny ip 10.20.10.0
0.0.0.255 10.10.10.0 0.0.0.255access-list 110 permit ip
10.20.10.0 0.0.0.255 anyroute-map nonat permit 10 match
```

```
ip address 110!control-plane!!line con 0 login localline
aux 0line vty 0 4 privilege level 15 login local
transport input telnet ssh!end
```

確認

ここでは、設定が正常に動作していることを確認します。

[Output Interpreter Tool](#) (OIT) ([登録ユーザ専用](#)) では、特定の **show** コマンドがサポートされています。OIT を使用して、**show** コマンド出力の解析を表示できます。

- [PIX セキュリティ アプライアンス : show コマンド](#)
- [リモート IOS ルータ : show コマンド](#)

[ASA/PIX セキュリティ アプライアンス - show コマンド](#)

- **show crypto isakmp sa** か。ピアですべての電流 IKE SA を示します。ASA#**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: 11 IKE Peer: 172.17.1.1 Type : L2L Role : initiator Rekey : no State : MM_ACTIVE
- **show crypto ipsec sa** か。ピアですべての現在の IPsec SA を示します。ASA#**show crypto ipsec sa**
interface: outside Crypto map tag: outside_map, seq num: 1, local addr: 172.16.1.1 local ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0) remote ident (addr/mask/prot/port): (10.20.10.0/255.255.255.0/0/0) current_peer: 172.17.1.1 #pkts encaps: 9, #pkts encrypt: 9, #pkts digest: 9 #pkts decaps: 9, #pkts decrypt: 9, #pkts verify: 9 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 9, #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.: 172.16.1.1, remote crypto endpt.: 172.17.1.1 path mtu 1500, ipsec overhead 58, media mtu 1500 current outbound spi: 434C4A7F inbound esp sas: spi: 0xB7C1948E (3082917006) transform: esp-des esp-sha-hmac none in use settings={L2L, Tunnel, PFS Group 2, } slot: 0, conn_id: 12288, crypto-map: outside_map sa timing: remaining key lifetime (kB/sec): (4274999/3588) IV size: 8 bytes replay detection support: Y outbound esp sas: spi: 0x434C4A7F (1129073279) transform: esp-des esp-sha-hmac none in use settings={L2L, Tunnel, PFS Group 2, } slot: 0, conn_id: 12288, crypto-map: outside_map sa timing: remaining key lifetime (kB/sec): (4274999/3588) IV size: 8 bytes replay detection support: Y

[リモート IOS ルータ : show コマンド](#)

- **show crypto isakmp sa** か。ピアですべての電流 IKE SA を示します。Router#**show crypto isakmp sa**
dst src state conn-id slot status172.17.1.1 172.16.1.1 QM_IDLE 3 0 ACTIVE
- **show crypto ipsec sa** か。ピアですべての現在の IPsec SA を示します。Router#**show crypto ipsec sa**
interface: FastEthernet0 Crypto map tag: SDM_CMAP_1, local addr 172.17.1.1 protected vrf: (none) local ident (addr/mask/prot/port): (10.20.10.0/255.255.255.0/0/0) remote ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0) current_peer 172.16.1.1 port 500 PERMIT, flags={origin_is_acl,} #pkts encaps: 68, #pkts encrypt: 68, #pkts digest: 68 #pkts decaps: 68, #pkts decrypt: 68, #pkts verify: 68 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 0, #pkts compr. failed: 0 #pkts not decompressed: 0, #pkts decompress failed: 0 #send errors 0, #recv errors 0 local crypto endpt.: 172.17.1.1, remote crypto endpt.: 172.16.1.1 path mtu 1500, ip mtu 1500 current outbound spi: 0xB7C1948E(3082917006) inbound esp sas: spi: 0x434C4A7F(1129073279) transform: esp-des esp-sha-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): (4578719/3004)          IV size: 8 bytes          replay
detection support: Y          Status: ACTIVE          inbound ah sas:          inbound pcp sas:
outbound esp sas:          spi: 0xB7C1948E(3082917006)          transform: esp-des esp-sha-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): (4578719/3002)          IV size:
8 bytes          replay detection support: Y          Status: ACTIVE          outbound ah sas:
outbound pcp sas:

```

- **show crypto engine connections active** か。暗号化パケット および 復号化パケット (ルータ だけ) についての現在の接続および情報を示します。Router#**show crypto engine connections active**

active	ID	Interface	IP-Address	State	Algorithm	Encrypt	Decrypt
3	FastEthernet0	172.17.1.1	set	HM	MAC_SHA+DES_56_CB	0	02001
	FastEthernet0	172.17.1.1	set	DES	+SHA	0	592002
	FastEthernet0	172.17.1.1	set	DES	+SHA	59	0

トラブルシューティング

ここでは、設定のトラブルシューティングに役立つ情報について説明します。


[Output Interpreter Tool](#) (OIT) ([登録ユーザ専用](#)) では、特定の **show** コマンドがサポートされています。OIT を使用して、**show** コマンド出力の解析を表示できます。

注 **debug** コマンドを使用する前に、『[debug コマンドの重要な情報](#)』および『[IP Security のトラブルシューティング : debug コマンドの説明と使用](#)』を参照してください。

- **debug crypto ipsec 7?Displays** フェーズ2 の IPsec ネゴシエーション。 **debug crypto isakmp 7?Displays** フェーズ1 の ISAKMP ネゴシエーション。
- **debug crypto ipsec** か。フェーズ2 の IPsec ネゴシエーションを表示する。 **debug crypto isakmp** か。フェーズ1 の ISAKMP ネゴシエーションを表示する。

サイト間 VPN のトラブルシューティングの詳細は、『[一般的な L2L およびリモート アクセス IPsec VPN のトラブルシューティング方法について](#)』を参照してください。

関連情報

- [Cisco PIX Firewall ソフトウェア](#)
- [Cisco Adaptive Security Device Manager](#)
- [Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス](#)
- [Configuration Professional : ASA/PIX と IOS ルータ構成例間のサイト間の IPsec VPN](#)
- [Cisco Secure PIX ファイアウォール コマンド リファレンス](#)
- [Cisco Router and Security Device Manager](#)
- [Requests for Comments \(RFC \)](#) 
- [テクニカルサポートとドキュメント - Cisco Systems](#)