Application Note

Cisco Router and Security Device Manager **Dynamic Multipoint VPN**

Introduction

This document gives an example of how to deploy a dynamic multipoint VPN (DMVPN) hub-and-spoke network using multipoint generic routing encapsulation (GRE) and Next Hop Resolution Protocol (NHRP) with IP Security (IPSec) VPN[1] using Cisco Security Device Manager.

Technology

DMVPN

DMVPN is a Cisco IOS® Software feature that allows users to better scale large and small IPSec VPNs by combining generic routing encapsulation (GRE) tunnels, IPSec encryption, and NHRP.

IPSec

IPSec is a framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers. IPSec provides these security services at the IP layer; it uses Internet Key Exchange (IKE) to handle negotiation of protocols and algorithms based on local policy, and to generate the encryption and authentication keys to be used by IPSec.

NHRP

NHRP is a client-and-server protocol where the hub is the server and the spokes are the clients. The hub maintains an NHRP database of the public interface addresses of each spoke. Each spoke registers its real address when it boots and queries the NHRP database for real addresses of the destination spokes in order to build direct tunnels.

Multipoint GRE

Multipoint GRE allows a single GRE interface to support multiple IPSec tunnels and simplifies the size and complexity of the configuration.

Dynamic Routing Protocols

Dynamic routing protocols are used to advertise private networks behind a router to other routers in the DMVPN topology.

Deployment Scenario

Easy provisioning is an advantage to using DMVPN. When new spoke routers are added, they are dynamically configured and do not need to be manually added to the existing hub-router configuration.

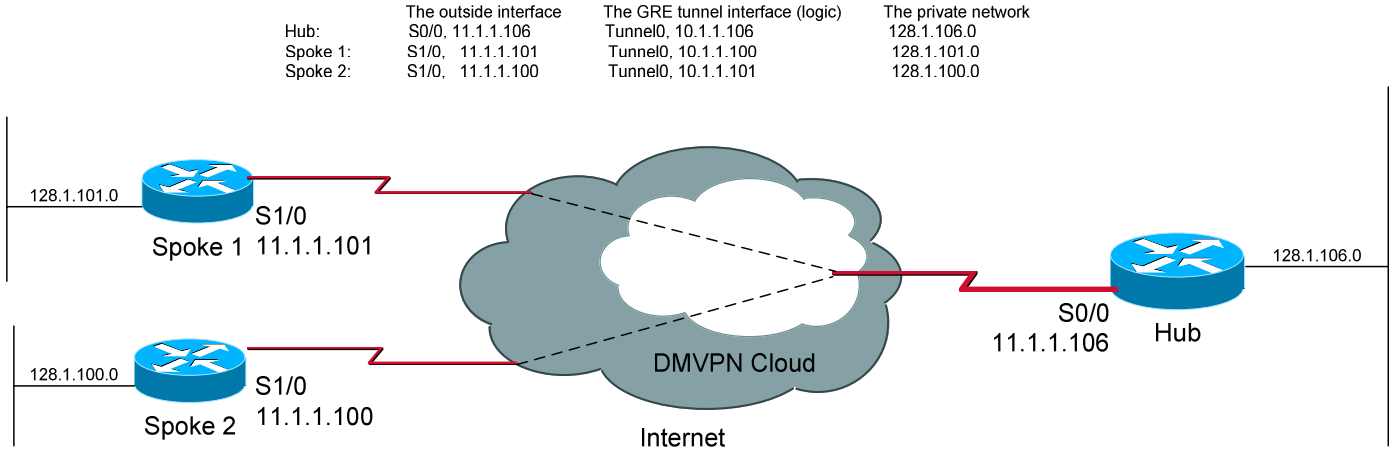
DMVPN can be used in many different solution scenarios. This document discusses a hub-and-spoke network with no redundancy running Cisco IOS Software Release 12.2(13)T or later.

[1] Cisco® Security Device Manager 1.1 does not support hub-and-spoke in a full-mesh topology; it only supports hub-and-spoke in a single DMVPM topology.

In hub-and-spoke network configurations, the spoke routers use IPSec tunnels to connect to the hub router to establish connectivity to the network. The hub router supports an IPSec tunnel for each spoke router. In addition, the hub acts as the distribution point for all routing information and connectivity to and from spoke routers. Hub-redundancy configuration is recommended for resiliency and load distribution.

Figure 1 shows a topology with all DMVPN traffic routed through the hub. A point-to-point GRE interface will be configured on the spoke, and the spoke will use it to create a tunnel to the hub which will remain up. Spokes do not create GRE tunnels to other spokes in this topology.

Figure 1 DMVPN Hub-and-Spoke Network Topology



This topology has the following characteristics:

- Each spoke has a permanent IPSec tunnel to the hub. Each spoke registers as a client of the NHRP server (the hub).
- IPSec performance is aggregated at the hub; the traffic destined from hosts behind Spoke 1 to hosts behind Spoke 2 will always be routed via the hub router.
- When a spoke needs to send a packet to a destination (private) subnet on another spoke, it queries the NHRP server for the real (outside) address of the destination (target) spoke. All spoke-to-spoke packets are decrypted and reencrypted at the hub.
- The IPSec encryption tunnel must be initiated by the spoke routers.

Sample Configuration

Without DMVPN, each spoke router requires a separate block of configuration lines on the hub router that define the crypto map characteristics, the crypto access list, and the GRE tunnel interface. On average, there are at least 13 lines of configuration per spoke router on the hub configuration. If there are 300 spoke routers, the hub needs at least an extra 3900 lines.

With DMVPN, users configure a single multipoint GRE tunnel interface, a single IPSec profile, and no crypto access lists on the hub router to manage all spoke routers. Thus, the size of the configuration on the hub router remains constant even if spoke routers are added to the network. DMVPN would reduce the configuration lines on the hub from 3900 to 16 lines.

The following is an example of the Cisco IOS Software commands necessary to configure a hub in a DMVPN hub-and-spoke network for this deployment scenario.

The Hub Configuration

```
!
! The IPSec peer address and the 'match' clause for the IPSec proxy are automatically
! derived from the NHRP mapping for the GRE tunnel.
crypto ipsec transform-set SDM_TRANSFORMSET_1 esp-sha-hmac esp-3des
 mode tunnel
 exit
crypto ipsec profile SDM_Profile1       ! This command is for tunnel interface
                                        ! to define the parameters for IPsec
                                        ! encryption between spoke and hub routers.
 set transform-set SDM_TRANSFORMSET_1   ! The only parameters required is the transform set
 exit
interface Tunnel0
 bandwidth 1000
 delay 1000
 ip nhrp holdtime 360
 ip nhrp network-id 100000          ! enables NHRP on an interface
 ip nhrp authentication DMVPN_NW    !Configure the authentication string for an interface
                                    ! using NHRP
 ip ospf network point-to-multipoint
 ip mtu 1400
 no shutdown
 ip address 10.1.1.106 255.255.255.0 ! Sets a primary address for the tunnel interface
 ip nhrp map multicast dynamic      ! Allows NHRP to automatically add spoke routers to the
                                    ! multicast NHRP mappings
 tunnel source Serial0/0            ! set source address for a tunnel interface
 tunnel mode gre multipoint         ! set the encapsulation mode to mGRE for the tunnel
                                    ! interface for data using dynamic spoke-to-spoke traffic
 tunnel protection ipsec profile SDM_Profile1  ! Associate the GRE tunnel interface with an
                                               ! IPSec profile
 tunnel key 100000                  ! enable an ID key for a tunnel interface
 exit
```

```
router ospf 100
 network 128.1.106.0 0.0.0.225 area 1
 network 10.1.1.106 0.0.0.255 area 1
 exit
crypto isakmp key ******** address 0.0.0.0 0.0.0.0 ! enable the negotiation with a peer
                                                   ! without a preconfigured IP address
```

The Spoke Configuration

```
!
!
crypto ipsec transform-set SDM_TRANSFORMSET_1 esp-sha-hmac esp-3des
 mode tunnel
 exit
crypto ipsec profile SDM_Profile1
 set transform-set SDM_TRANSFORMSET_1
 exit
interface Tunnel0
 bandwidth 1000
 delay 1000
 ip nhrp holdtime 360
 ip nhrp network-id 100000
 ip nhrp authentication DMVPN_NW
 ip ospf network point-to-multipoint
 ip mtu 1400
 no shutdown
 ip address 10.1.1.101 255.255.255.0
 ip nhrp nhs 10.1.1.106                ! configure the hub router as the NHRP next-hop server
                                       ! for NHRP registration
 ip nhrp map 10.1.1.106 11.1.1.106     ! statically configure the address mapping of IP
                                       ! destinations hub-tunnle-ip-addr/hub-physical-ip-addr
 tunnel source Serial1/0
 tunnel destination 11.1.1.106         ! specify the destination for a tunnel interface
```

```
                                        ! for data traffic using hub-and-spoke tunnels.

 tunnel protection ipsec profile SDM_Profile1
 tunnel key 100000
 exit
router ospf 100
 network 128.1.101.0 0.0.0.255 area 1
 network 10.1.1.101 0.0.0.255 area 1
 exit
crypto isakmp policy 1
 authentication pre-share
 encr 3des
 hash sha
 group 2
 lifetime 86400
 exit
crypto isakmp key ******** address 11.1.1.106
!
```

Cisco Security Device Manager DMVPN support

Although the DMVPN feature dramatically reduces the hub-router configuration, it still requires users to fully understand how to configure an IPSec Profile, the DMVPN hub, and the DMVPN spoke.

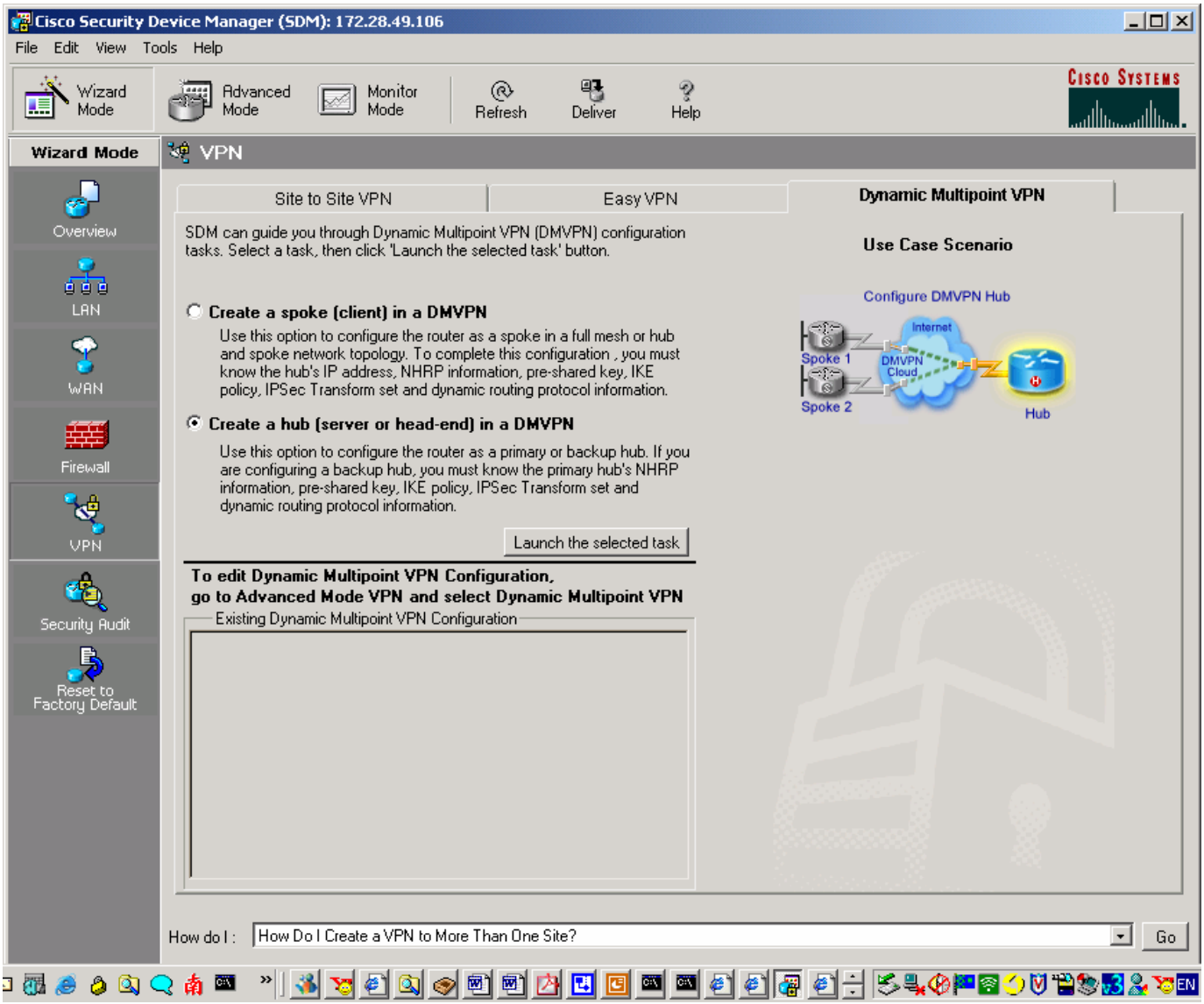
Cisco Router and Security Device Manager (SDM) allows users to easily configure the DMVPN feature with limited knowledge and minimal information (usually provided by the system administrator). The following steps are used to configure the same deployment scenario, this time using Cisco SDM as opposed to the Cisco IOS Software command-line interface (CLI).

Create a Hub

To create a hub, take the following steps:

- Select the VPN Wizard (Figure 2) at the Wizard Mode and launch the DMVPN Wizard to create a hub.

Figure 2 DMVPN Wizards

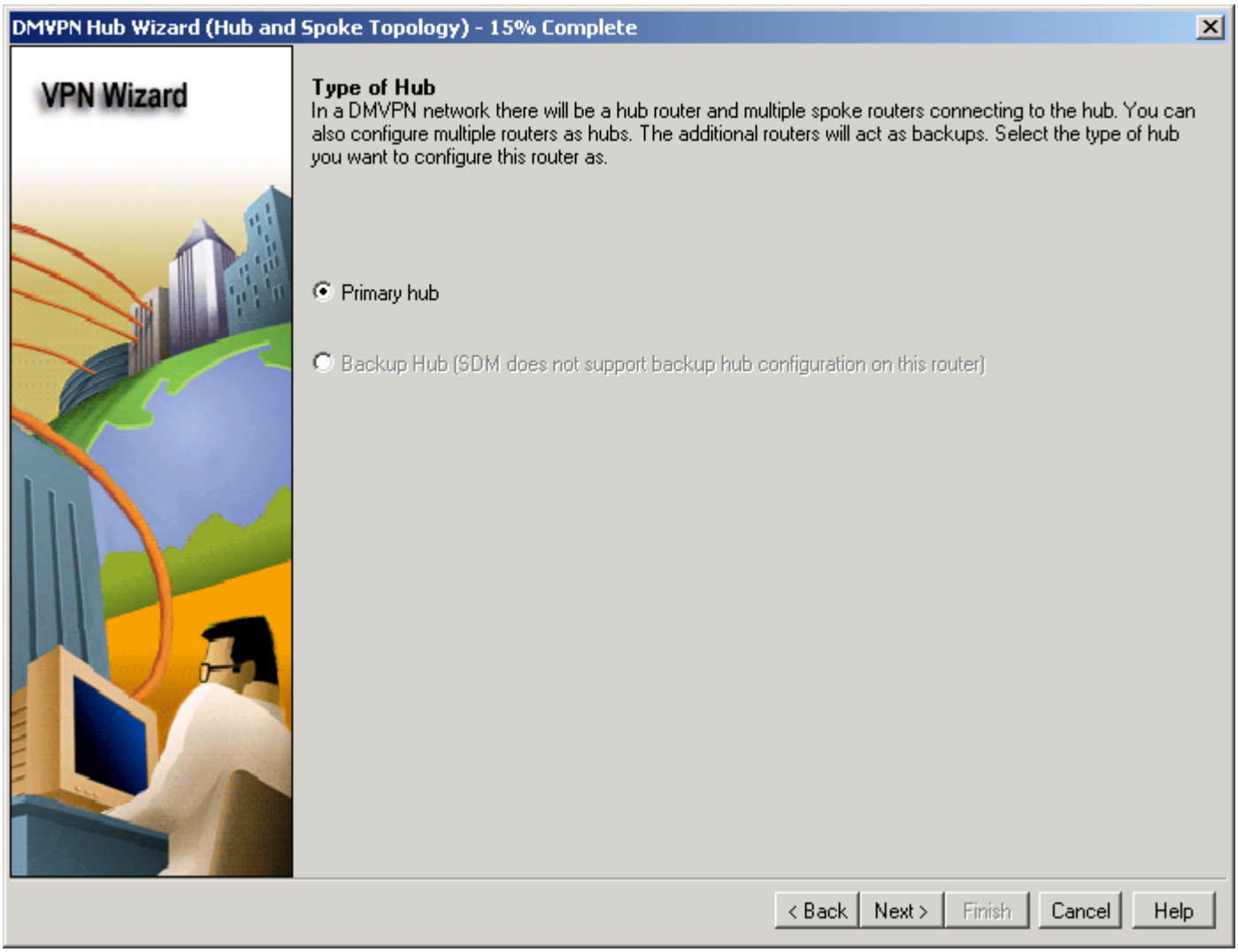


- Select **Hub and Spoke network** (Figure 3).

Figure 3 DMVPN Network Topology

- For “Type of Hub” select **Primary hub** (Figure 4).

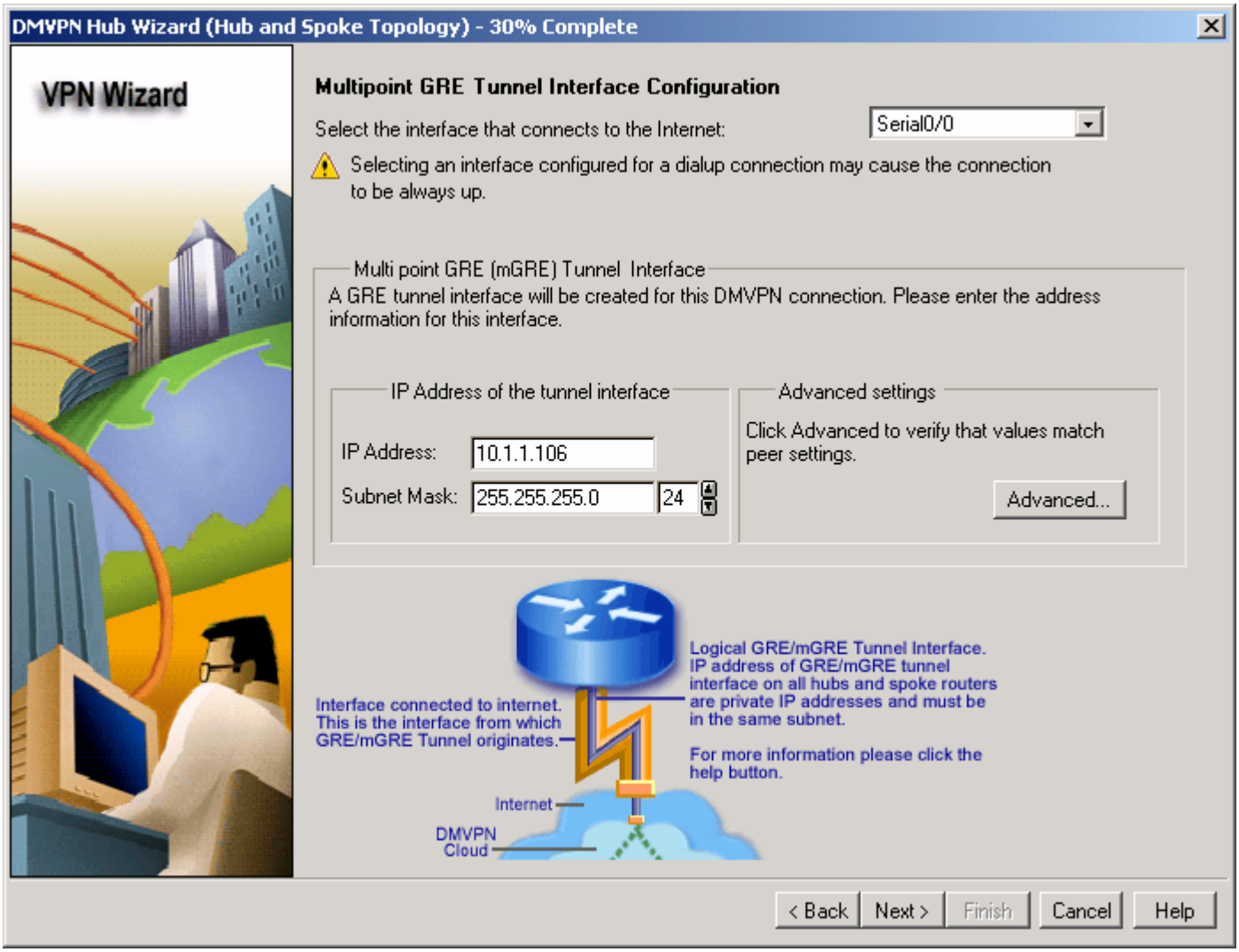
Figure 4 Type of Hub



To configure the mGRE tunnel interface (Figure 5), take the following steps:

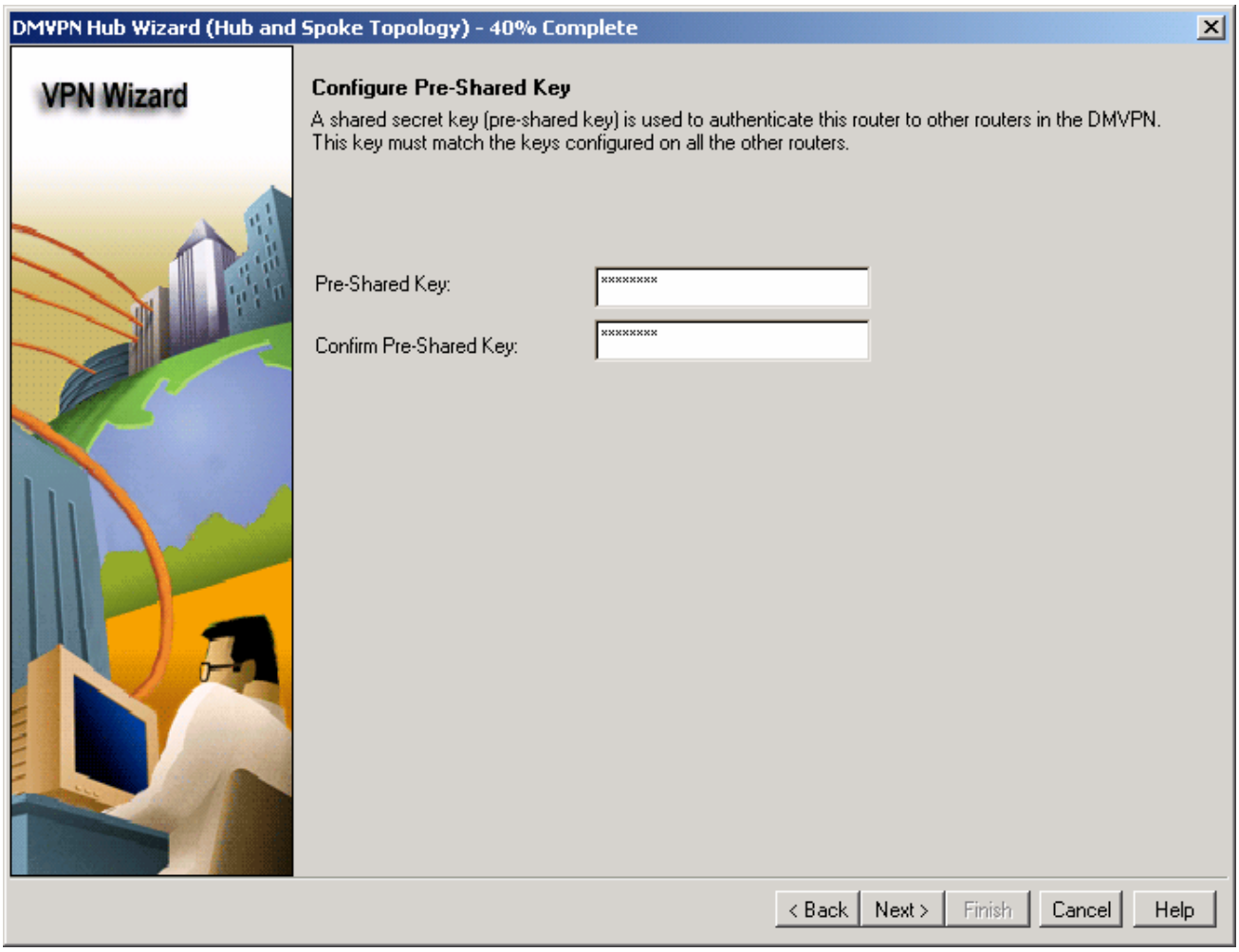
- Select the interface that connects to the Internet; in this scenario the hub uses **Serial0/0**
- The IP address of the tunnel is **10.1.1.106/24**
- Under Advanced settings, click **Advanced…**, and use the Cisco SDM default value
- Click **Next**

Figure 5 Multipoint GRE Tunnel Interface Configuration



In the Configure Pre-Shared Key screen (Figure 6), enter **ciscoSDM** (the key is displayed encrypted on screen), then click **Next.**

Figure 6 Configure Pre-Shared Key

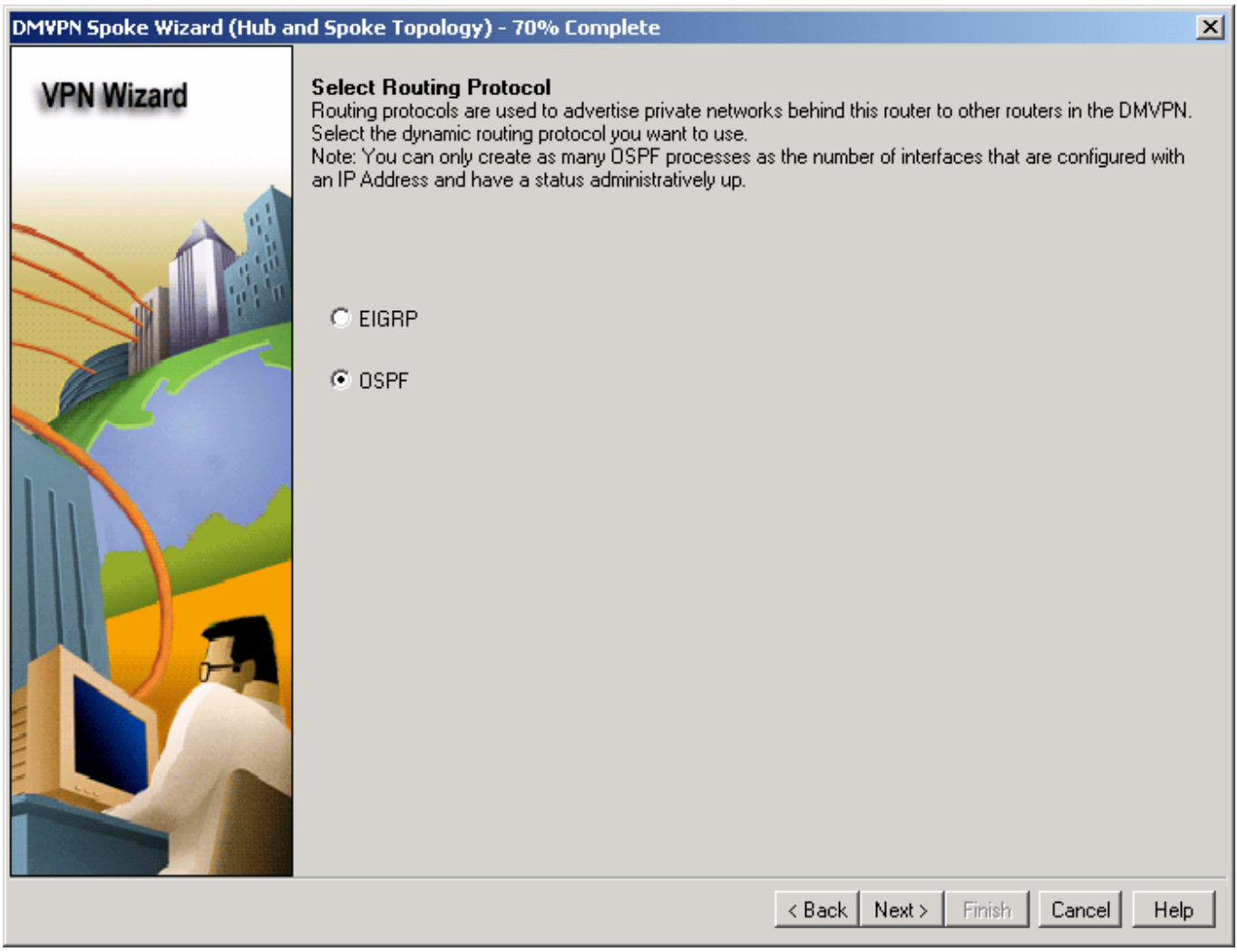


Then Cisco SDM prompts for the following:

- IKE policy: use Cisco SDM default, then click **Next**
- Transform Set: use Cisco SDM default, then click **Next**

In the Select Routing Protocol screen (Figure 7), **OSPF** is used for this example. Click **Next.**

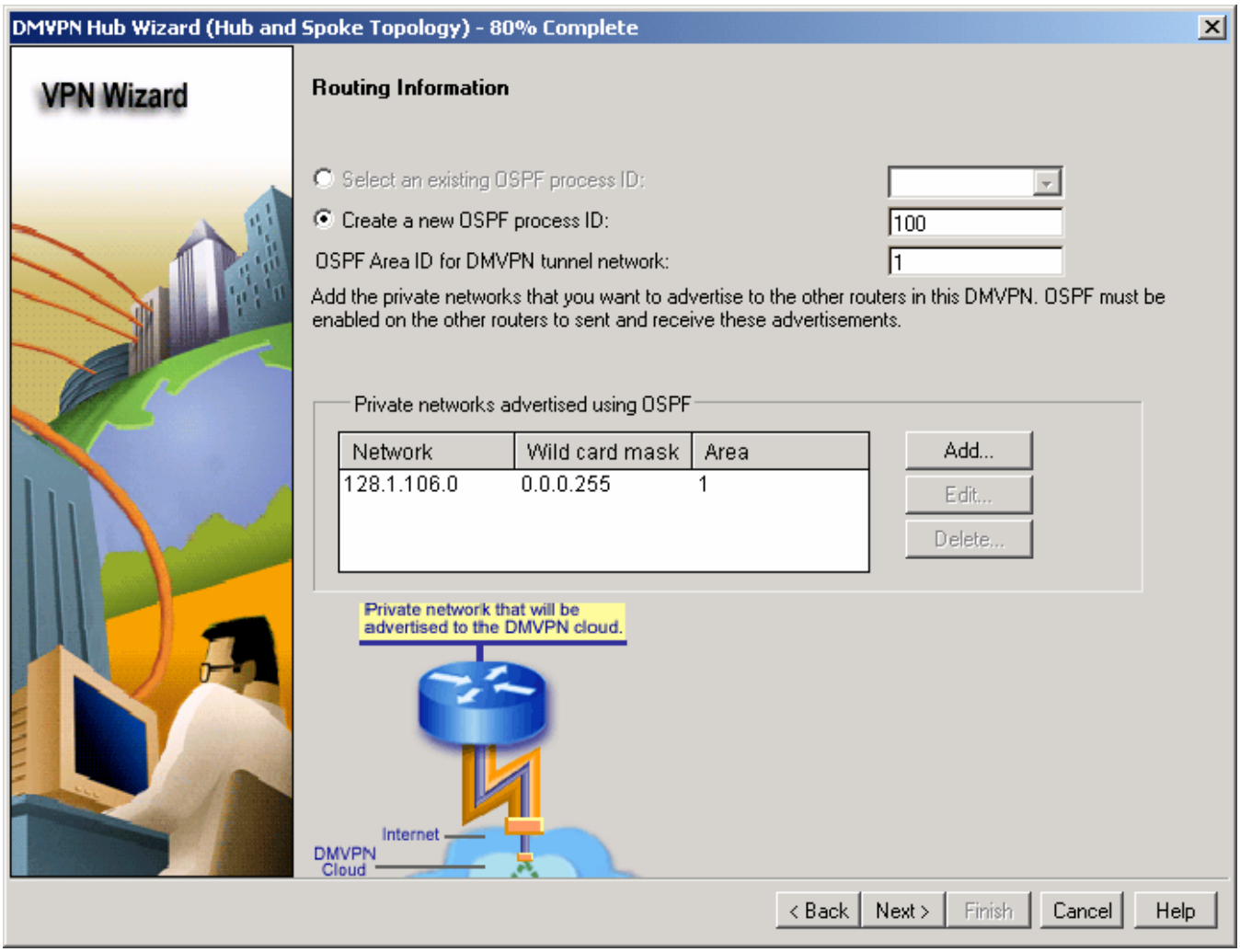
Figure 7 Selecting Routing Protocol



In the Routing Information screen (Figure 8), take the following steps:

- Create a new OSPF process ID: **100**
- OSPF Area ID for DMVPN tunnel network: **1**
- Private networks advertised using OSPF: click **Add…**
- Network: **128.1.106.0**
- **Wild card mask: 0.0.0.255**
- Area: **1**
- Click **Next**

Figure 8 Routing Information



Next, click **Spoke Configuration** to preview the configuration procedure Cisco SDM recommends for a spoke that will connect to this hub. Cisco SDM includes the necessary hub information in the procedure so that you do not have to record it yourself. Click **Save** to save the corresponding Spoke Configuration for reference when configuring the spoke router.

The following is the Cisco SDM spoke configuration procedure generated from the DMVPN hub that you just created.

```
!
!How to configure DMVPN spoke

Select Wizard mode from the tool bar and click on the VPN icon.
Select the DMVPN tab and then select Spoke and click on Launch Selected Task button. Then follow
the steps given below.

Welcome Screen:
   Click Next
Type of DMVPN network:
   If you want dynamic spoke to spoke tunnel initiation please select Fully Meshed network.
   Otherwise select Hub and Spoke network.
   Click Next
Specify Hub Information:
   Public IP Address:11.1.1.106
   IP Address of Hub's mGRE tunnel:10.1.1.106
   Click Next:
Configure GRE Tunnel:
   Interface that connects to the internet : Select the interface that connects to the internet
from the list.
   IP Address of tunnel Interface:-
      IP Address:Get an IP address from your network administrator.
      Subnet Mask:255.255.255.0
   Advanced:-
      Click on the advanced button.
      In the Advanced tunnel information dialog box verify that the fields have the following
values:
      NHRP Network ID : 100000
      NHRP Hold time : 360
```

Tunnel Key : 100000

Bandwidth : 1000

MTU : 1400

Tunnel Throughput Delay : 1000

Click Next Configure Pre-Shared Key:

Pre-Shared Key:********

Confirm Pre-Shared Key:********

Click Next

Key Exchange Policy:

Please verify if any one of the following IKE policies are listed in the list.

If not add any one of the following policies by clicking on the add button and choosing appropriate values in Add IKE policy dialog box.

IKE policies:

Hash	Encryption	DH Group	Authentication
SHA_1	DES	group2	PRE_SHARE

Transform Sets:

Select a transform set with the following parameters. If none available create a new one.

ESP Integrity:ESP_SHA_HMAC

ESP Encryption:ESP_3DES

Mode:TUNNEL

Select Routing Protocol:

Select : OSPF

Click Next

Routing Information:

For OSPF process ID enter : 100

For OSPF Area ID for DMVPN tunnel network enter: 1

Add private networks you wish to advertise to the DMVPN network.

!

!

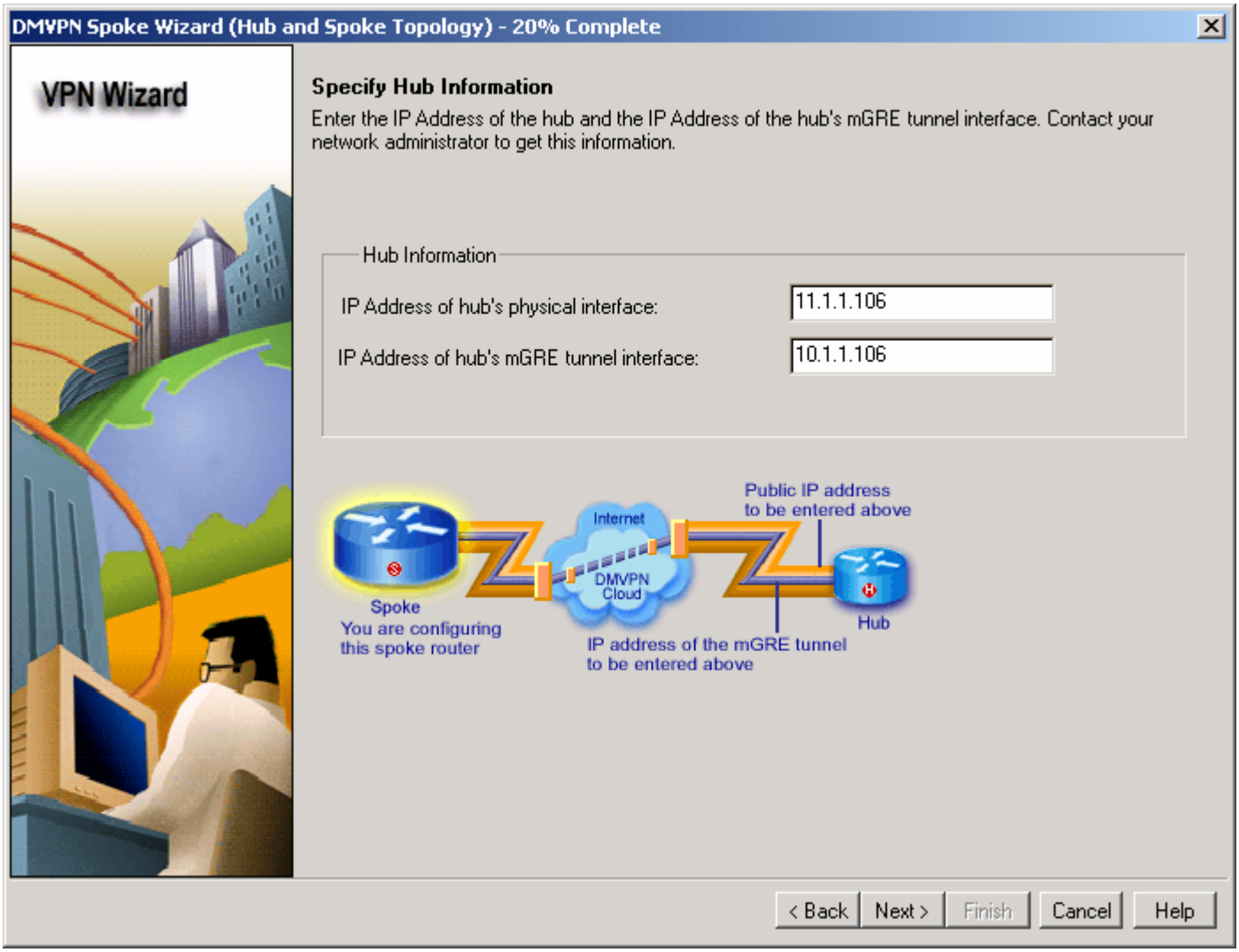
Click **Finish** to deliver the configuration.

Create a Spoke

The following are the steps necessary to configure Spoke 1 router with Cisco SDM. Users invoke the VPN Wizard at the Wizard mode and launch the DMVPN Wizard for creating a spoke (Figure 9).

- Select **Hub and Spoke network**, click **Next**
- Specify Hub Information
  - Public IP Address of hub's physical interface: **11.1.1.106**
  - IP Address of hub's multipoint GRE tunnel interface: **10.1.1.106**
- Click **Next**

Figure 9 Hub Information



For the Multipoint GRE Tunnel Interface Configuration, take the following steps:

- Select the interface that connects to the Internet. For this example Spoke 1 is **Serial1/0**.
- IP Address of the tunnel: **10.1.1.101/24**.
- Under Advanced settings, click **Advanced…**and verify that the values match those that are configured on the hub.
- Then click **Next**. Configure the same Pre-Shared key as used by the hub.

To configure a Key Exchange Policy, enter the following:

- Hash: **SHA_1**
- Encryption: **DES**
- DH Group: **group2**
- Authentication: **PRE_SHARE**
- Configure Transform Sets. In this example:

  – ESP Integrity: **ESP_SHA_HMAC**

  – ESP Encryption: **ESP_3DES**

  – Mode: **TUNNEL**
- Routing Protocol: **OSPF**.
- Create a new OSPF process ID: **100**.
- OSPF Area ID for DMVPN tunnel network: **1**.
- Private network advertised using OSPF: **128.1.101.0/0.0.0.255/1**.
- Click **Finish** and deliver the configuration.

Once the DMVPN is configured using the VPN Wizard, use the Advanced Mode/VPN/Dynamic Multipoint VPN to display and alter the configuration further if desired.

Verification

Users can go to **Monitor Mode**, then select **SDM Monitor/VPN Status** to view and verify the tunnel status. Figure 10 shows the IKE SAs, and Figure 11 shows the DMVPN Tunnels.

Figure 10 IKE SAs

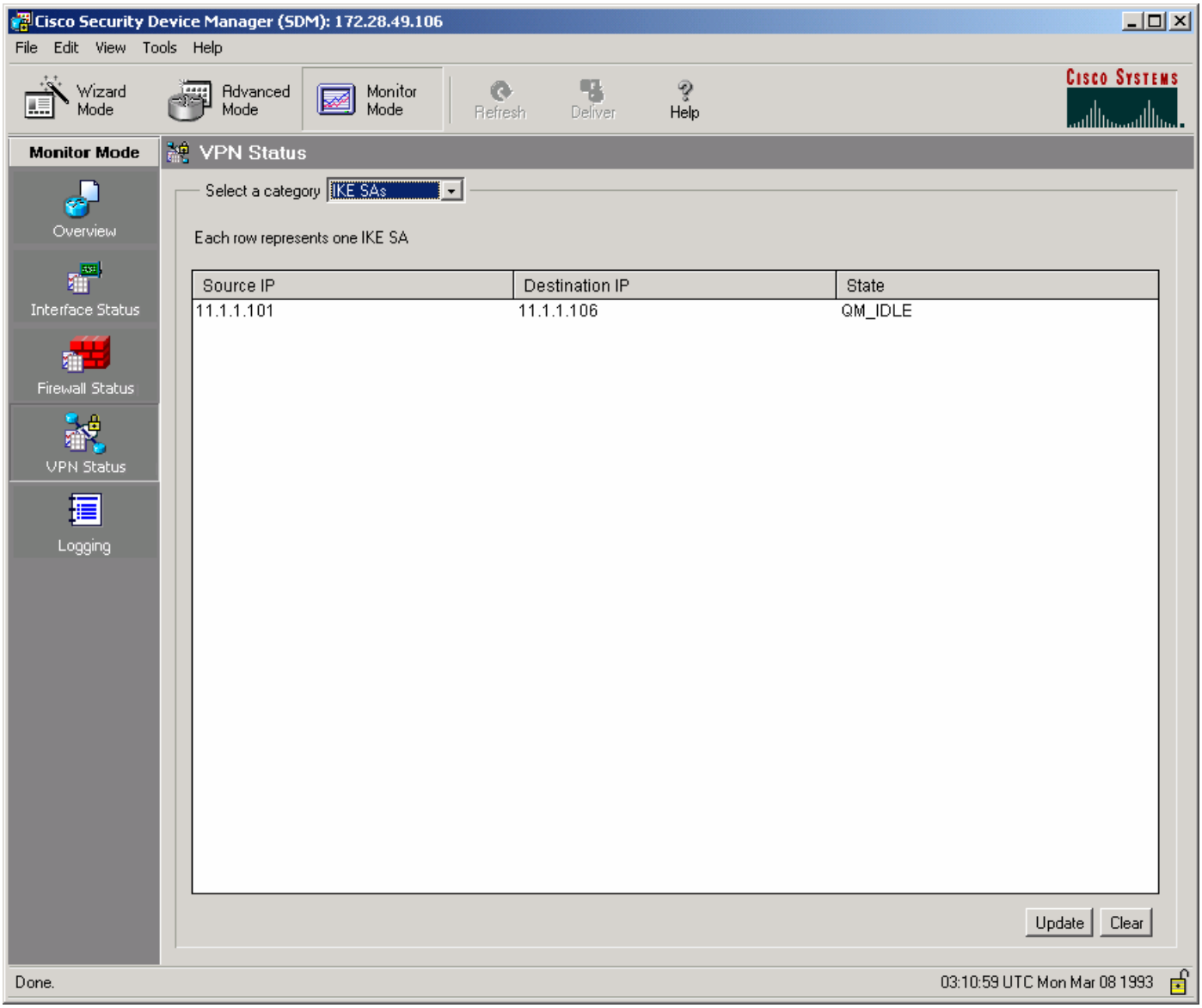
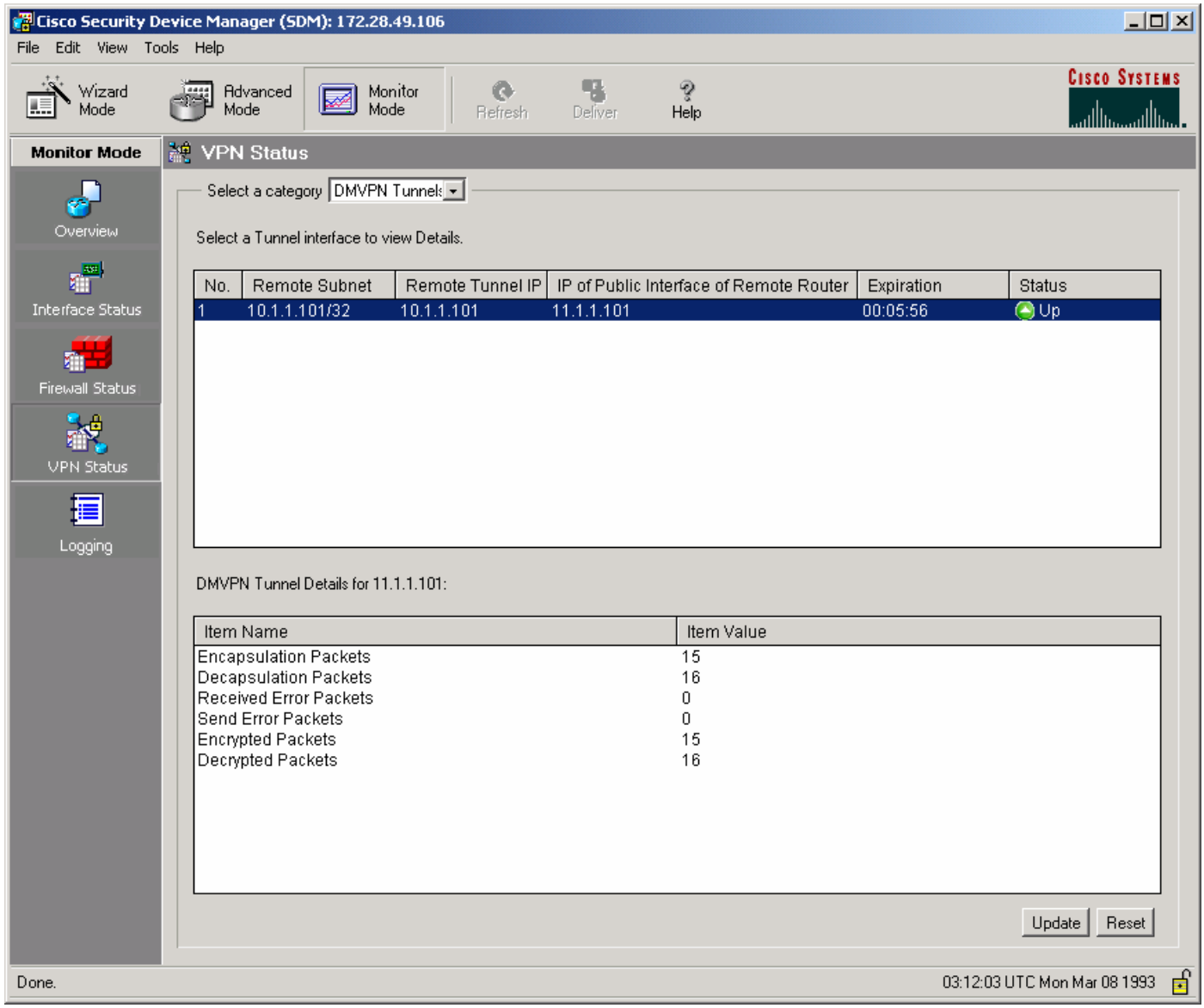


Figure 11 DMVPN Tunnels



In summary, by using the Cisco Security Device Manager DMVPN Wizard, users can generate the same complex DMVPN configuration for both hub and spoke routers easily and quickly with minimum knowledge of Cisco IOS Software commands and DMVPN.

References

Dynamic Multipoint VPN (DMVPN):

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftgreips.pdf

Deploying IPSec Virtual Private Network (Solutions Guide):

http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/depip_wp.pdf

DMPVN Homepage:

http://www.cisco.com/warp/customer/105/dmvpn.html

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International
BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 317 7777
Fax: +65 317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on **the Cisco Web site at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico• The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Printed in the USA