Deployment Guide

Deploying an Enterprise-Class Teleworking Solution using Cisco Router and Security Device Manager

This deployment guide shows how the Cisco® Enterprise-Class Teleworker (ECT) solution can be deployed using Cisco Router and Security Device Manager (SDM) for commercial and small and medium-sized enterprises.

The Cisco® Enterprise Class Teleworker solution is a highly scalable Cisco IOS® Software-based solution that securely integrates the network infrastructure, management infrastructure, managed services, and applications across the entire enterprise, including LAN, WAN, branch, and teleworker locations.

The solution is an integral part of the Cisco Service-Oriented Network Architecture (SONA), a framework that enables enterprise customers to build integrated systems across a fully converged, intelligent network. Using the Cisco SONA framework, the enterprise network can evolve into an Intelligent Information Network-one that offers the kind of end-to-end functions and centralized, unified control that promote true business transparency and agility.

Cisco Systems® has successfully deployed the Enterprise Class Teleworker solution within its own organization, increasing productivity and improving efficiency while enabling "zero-touch" deployment, manageability, and low-to-negative total cost of ownership (TCO). Enterprises and service providers can use the Cisco ECT solution to offer the benefits of network services to their end users and customers, while maintaining an effective ROI.

For ECT/SONA Solution Overview, refer to: http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6660/prod_brochure0900aecd803fc7ec.html. For ECT/SONA solution, services and applications support, refer to the following Cisco.com link: http://cisco.com/go/ect/

Cisco SDM is a Web-style graphical user interface (GUI) tool that can be used to configure Cisco IOS® routers. It usually comes with a router's factory default configuration and can be invoked from any Java-enabled browser that has connectivity to the Cisco IOS router to be configured. The latest version of Cisco SDM is available at http://www.cisco.com/pcgi-bin/tablebuild.pl/sdm.

Please refer to http://www.cisco.com/go/sdm for coming up to speed with SDM. There you will find all the product documentation.

When Cisco ECT is deployed for a small number of VPN spokes, the network can be provisioned by configuring all hubs and spokes using Cisco SDM. This is the focus of this guide.

CISCO SDM USE FOR THE CISCO ECT SOLUTION

This guide covers the steps needed for the provisioning of a Cisco ECT solution using Cisco SDM. It explains how to configure DMVPN hubs and all necessary features needed for a spoke, including DMVPN, firewall, Network Address Translation (NAT), quality of service (QoS), and IP services.

Note: Only some selective screen shots are shown in this guide. You will find that some steps do not have a matching screen shot. We opted for selecting the most meaningful ones, to keep the guide shorter. The missing ones should not cause any confusion when following the detailed steps.

The configuration can be downloaded from Cisco SDM directly to the routers, or it can be saved to a file. In this last case, Secure Device Provisioning (SDP) can be used to remotely retrieve the configuration file, and to install a new certificate in a new spoke router. However, SDP is not covered in this guide.

Cisco SDM can be used to manage devices that are online, as it allows to the user to remotely access a router using Secure Sockets Layer (SSL) and change the configuration.

Cisco SDM is a good choice for deploying a Cisco ECT solution for a small number of routers. In this scenario, the VPN routers are usually provisioned locally at the central office and then shipped or hand-delivered to the end user, or sent to a small office.

Below is one possible list of features that can be enabled by Cisco SDM for a Cisco ECT remote spoke router, used for a small or medium-sized VPN deployment. Other features might be enabled for each particular case.

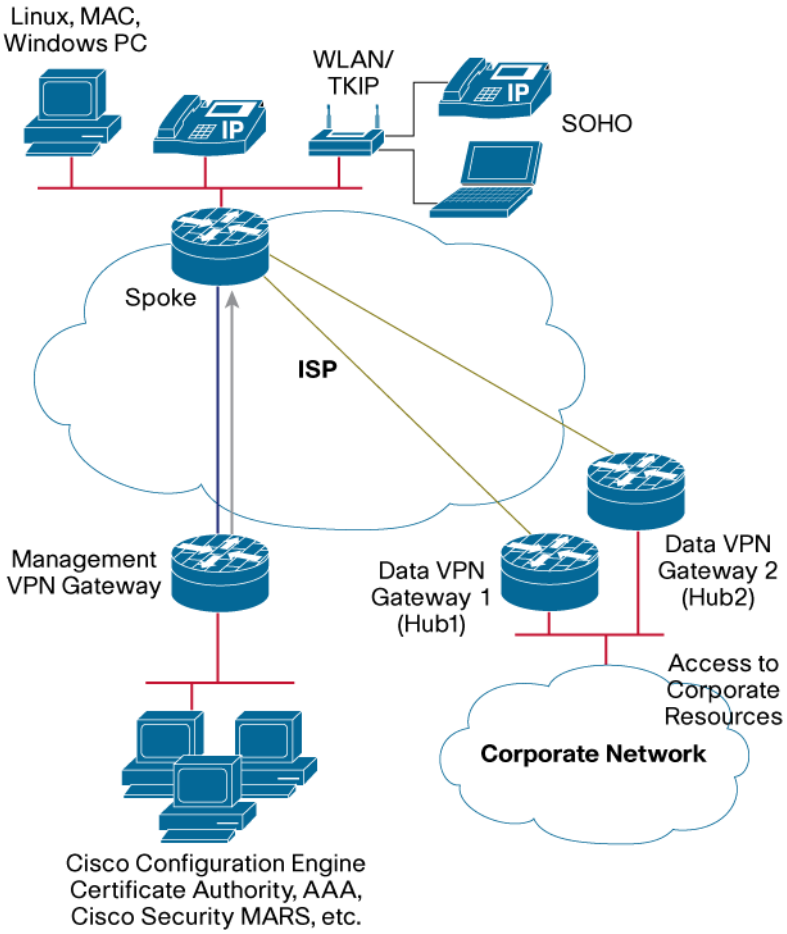
- Internet connectivity, DSL, cable, etc.
- Two VLANs; one for corporate traffic and one to be used as a guest VLAN
- DMVPN as the underlying VPN backbone
- Routing for DMVPN
- IP Security (IPsec) and Public Key Infrastructure (PKI) for VPN access
- Cisco IOS Firewall and access control lists (ACLs)
- Network/Port Address Translation (NAT/PAT)
- Intrusion prevention system (IPS)
- Quality of service (QoS)
- Network Admission Control (NAC)
- Baseline IP services: Dynamic Host Control Protocol (DHCP), DNS, Network Time Protocol (NTP), VTY access, etc.
- Wireless configuration (for a Cisco 871 router example)

Before deploying spokes, the primary and secondary DMVPN hubs need to be configured. This will be the first step.

Note: Cisco ECT is primarily deployed using PKI. This is highly recommended, although the solution could also be deployed using pre-shared keys. This guide assumes that the PKI infrastructure is already provisioned. For an explanation on how to provision the Cisco IOS PKI certificate server please read:
http://www.cisco.com/en/US/products/ps6350/products_configuration_guide_chapter09186a00804450cf.html

NETWORK ARCHITECTURE

Figure 1. Cisco ECT Architecture



The picture above (Figure 1) shows a typical ECT architecture. It shows how a remote router acting as a DMVPN spoke connects back to the corporate site. It also contains a separate management network, which allows for a central management of the remote routers and gives an opportunity to change the data security policies without breaking the remote connection to the distant router.

Platforms and Images

For a small deployment, use any Cisco 3800 Series router for hubs. For spokes, use a Cisco 870 Series router for home or small offices, a Cisco 1800 Series router for small to medium-sized offices, or any larger Cisco IOS router for large offices.

Cisco IOS Software Releases 12.4(6)T3 and 12.4(8) or above are recommended for hubs and spoke routers, or the latest available. An advance enterprise image is needed to enable all Cisco ECT features.

In this guide, Cisco SDM 2.3 is used for all security configurations. It was executed from a PC installation, but for a given version, the software is the same, only the location is different. For Internet access, Cisco SDM Express was used. Cisco SDM Express is only started from the router installation.

When a new router is ordered, Cisco SDM can usually be factory-installed in the router's flash memory. This Cisco SDM version may be outdated when it comes time to configure the router for Cisco ECT. When deploying the Cisco ECT solution, the latest Cisco SDM version should be installed for ease of use; otherwise, it is necessary to install the latest version on all Cisco ECT routers.

Start by installing the latest Cisco SDM version, which you can download from Cisco.com at http://www.cisco.com/cgi-bin/tablebuild.pl/sdm.

Note: In order to be able to download this software, an account with Cisco.com is required.

CONFIGURING DMVPN HUBS

Cisco SDM delivers commands to the active running configuration only. To save the configuration to NVRAM, go to "File > Write to Startup Config…" menu option.

Cisco SDM can also be used to configure DMVPN hubs used for Cisco ECT deployments. In the most common architecture, two DMVPN hubs are provisioned; one acts as primary and the second, a backup hub.

To configure a router as a primary DMVPN hub perform the following steps:

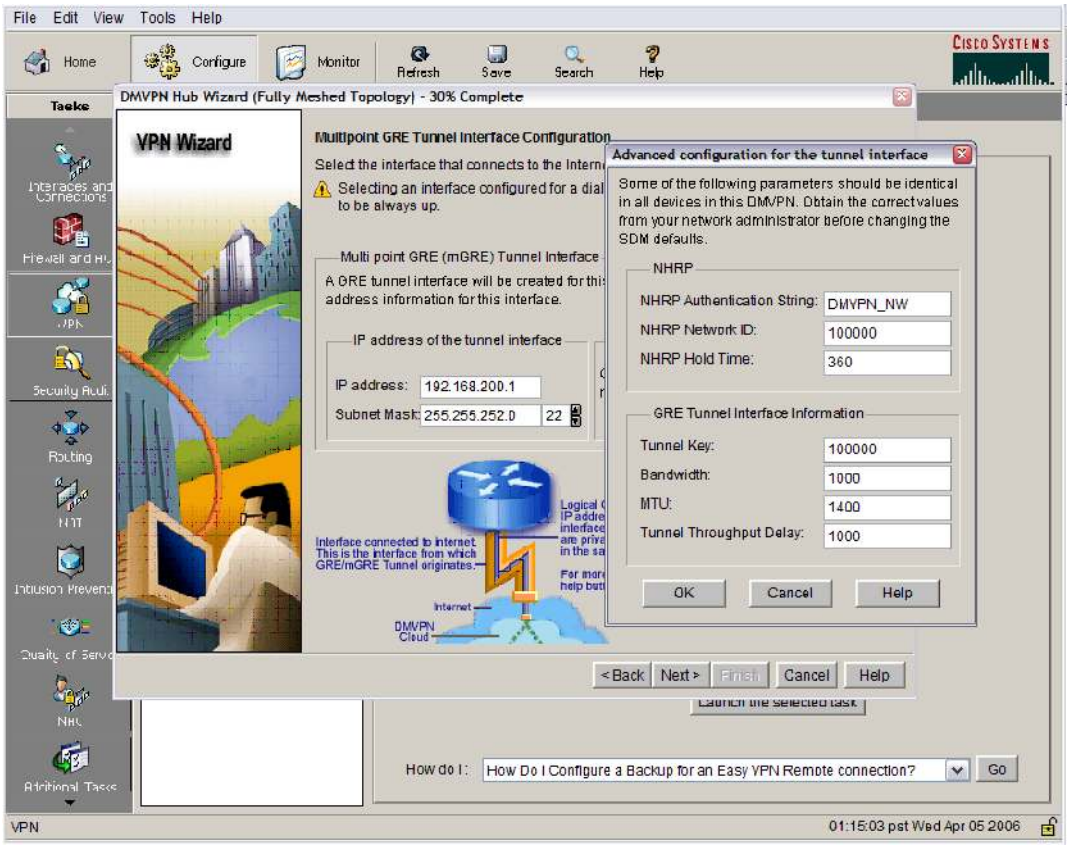
Step 1. Start Cisco SDM and connect to the router that will be configured as the hub.

Step 2. Navigate to Configure > VPN > Dynamic Multipoint VPN. Select "Create a hub" option and click on "launch the selected task" button.

Step 3. In the next screen, select **Full Mesh** if you want to allow direct spoke-to-spoke connections.

Step 4. Click **Next** and then select the primary hub to start.

Figure 2. Configure the DMVPN Hubs



In the Multipoint GRE Tunnel Interface Configuration screen specify the IP Address of the multipoint GRE tunnel interface. *IP Addresses of multipoint GRE tunnel interfaces on all routers in a DMVPN network must belong to the same subnet. Typically this is a private subnet.*

Make sure the “Tunnel Key” and “NHRP Network ID” are the same for all hubs and spokes, so that they share the same DMVPN area. (Figure 2)

Regarding the multipoint generic routing encapsulation (mGRE) tunnel interface, the same subnet must be used by all VPN routers that are part of the same DMVPN area. This is an internal subnet, only visible to the DMVPN routers.

Step 5. Select **Digital Certificates** in the Authentication screen that follows.

Note: If a digital certificate is not configured on this router, configure one. All the routers in a DMVPN cloud must be issued a digital certificate by the same CA server.

(Please refer to “Step 3—VPN configuration” in this guide for the steps required to install a PKI certificate in this router).

Step 6. Even though all three routing protocols (Enhanced Interior Gateway Routing Protocol [EIGRP], Open Shortest Path First [OSPF], and Routing Information Protocol [RIP]) will work, Cisco recommends EIGRP or OSPF.

Step 7. Select the appropriate AS number and the internal network networks that other VPN nodes should have access to.

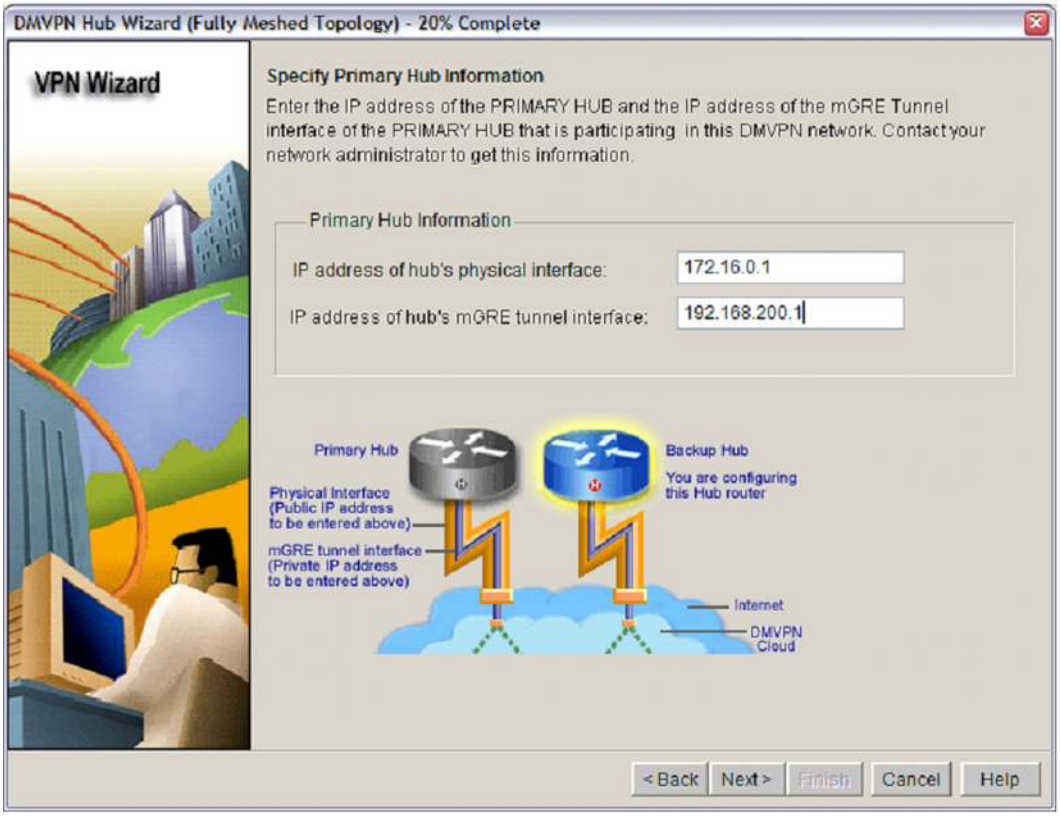
Step 8. Click **Finish** to generate and deliver the configuration to the router.

This is a sample configuration:


```
crypto isakmp policy 10
 encr 3des
!
crypto ipsec transform-set ESP-3DES-SHA1 esp-3des esp-sha-hmac
 mode transport
!
crypto ipsec profile SDM_Profile1
 set transform-set ESP-3DES-SHA1
!
interface Tunnel0
 bandwidth 1000
 ip address 192.168.200.1 255.255.252.0
 no ip redirects
 ip mtu 1400
 no ip next-hop-self eigrp 33
 ip nhrp authentication DMVPN_NW
 ip nhrp map multicast dynamic
 ip nhrp network-id 100000
 ip nhrp holdtime 360
 ip tcp adjust-mss 1360
 no ip split-horizon eigrp 33
 delay 1000
 tunnel source GigaEthentet0/0
 tunnel mode gre multipoint
 tunnel key 100000
 tunnel protection ipsec profile SDM_Profile1
!
!
router eigrp 33
 network 10.20.0.0 0.0.255.255
 network 192.168.200.0 0.0.3.255
 no auto-summary
!
```

Now perform the same steps, but select the “Backup” DMVPN hub. There is an additional screen to select the primary hub IP addresses (Figure 3).

Figure 3. DMVPN Backup Hub



Following is a sample configuration. It is almost the same as the primary DMVPN hub, but here the we use the bandwidth command to lower the routing metric, or preference, for this tunnel interface, making this DMVPN hub second best from a spoke routing perspective. Everything else remains the same, except for the mGRE IP address, of course.

Note: The bandwidth for this mGRE interface is smaller than that of the primary one.

```
crypto isakmp policy 10
 encr 3des
!
crypto ipsec transform-set ESP-3DES-SHA1 esp-3des esp-sha-hmac
 mode transport
!
crypto ipsec profile SDM_Profile1
 set transform-set ESP-3DES-SHA1
!
interface Tunnel0
bandwidth 900
 ip address 192.168.200.2 255.255.252.0
 no ip redirects
 ip mtu 1400
 no ip next-hop-self eigrp 33
 ip nhrp authentication DMVPN_NW
```



```
 ip nhrp map multicast dynamic
 ip nhrp map multicast 172.16.0.1
 ip nhrp map 192.168.200.1 172.16.0.1
 ip nhrp network-id 100000
 ip nhrp holdtime 360
 ip nhrp nhs 192.168.200.1
 ip tcp adjust-mss 1360
 no ip split-horizon eigrp 33
 delay 1000
 tunnel source GigaEthentet0/0
 tunnel mode gre multipoint
 tunnel key 100000
 tunnel protection ipsec profile SDM_Profile1
!
router eigrp 33
 network 10.20.0.0 0.0.255.255
 network 192.168.200.0 0.0.3.255
 no auto-summary!
```

At this point, you must save the configuration to NVRAM by going to "File > Save to Startup Config…". Otherwise, the configuration will be lost when the router is power-cycled. It is also recommended that you save a copy of the configuration in your PC for future reference. This can be achieved by clicking on "File > Save Running Config to PC…".

ADDING A NEW CISCO ECT-ENABLED SITE

Note: Cisco SDM delivers commands to the active running configuration. To save the configuration to NVRAM you need to go to "File > Write to Startup Config…".

Step 1—Internet Connectivity

This example uses a new Cisco 871 router with just the factory default configuration.

Appendix A includes a sample factory configuration for a Cisco 871 router.

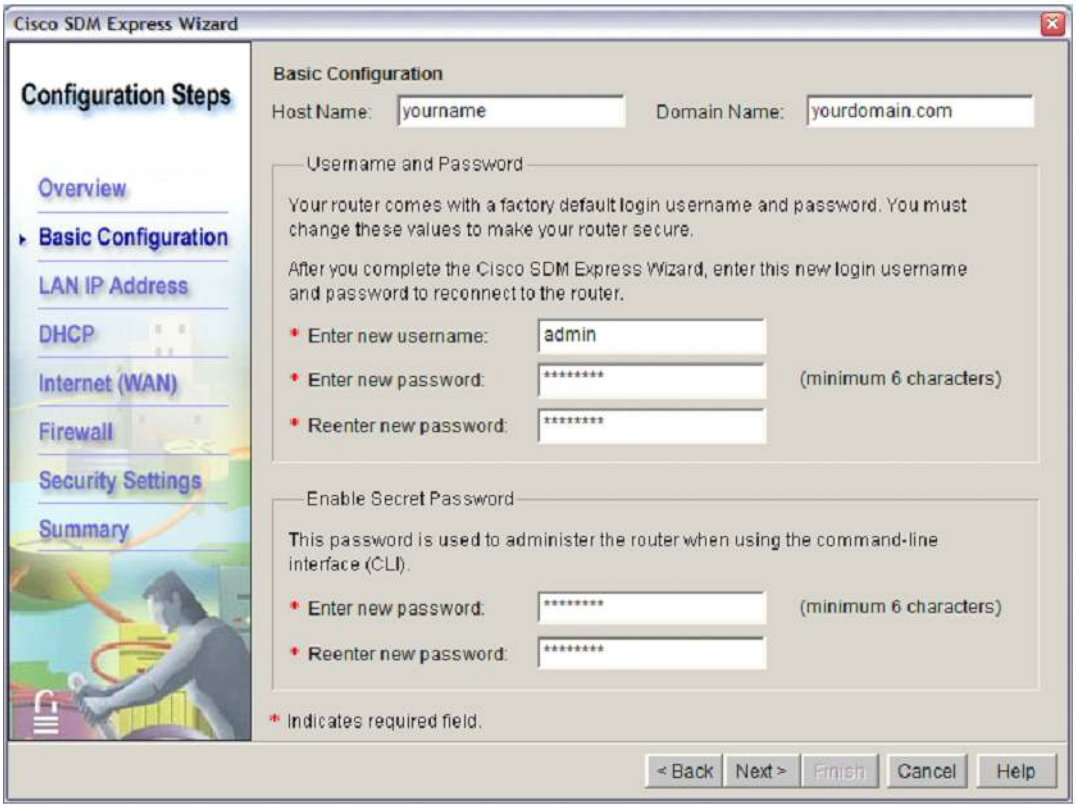
Note: In this example, the router uses DHCP to connect to the outside network, but can be configured with the addressing scheme used by the ISP at the final destination in mind. Then, the configuration can be saved to NVRAM.

The first step to provision this router is to carry out the Internet access configuration. If connecting from a DHCP-accessible site, such as a cable modem, these steps are needed:

1. Connect the WAN interface to the Internet (modem, NAT router). On a Cisco 871 router, this interface is "FastEthernet4".
2. Connect a PC to the Cisco 871 router (LAN side); to the FastEthernet0 of a Cisco 871 router, for example.
3. Type http://10.10.10.1 to access the Cisco SDM Express that comes in flash. Cisco SDM Express consists of a step-by-step wizard that you can use to set up login credentials, ISP network information, and basis firewall. If Cisco SDM Express is not there, run the setup of the downloaded Cisco SDM software and install it in the router.
4. Enter the default username/password cisco/cisco to gain access to the router.

5. In the first screen of the wizard, enter the hostname and login credentials for console/SSH and future Cisco SDM access (Figure 4).

Figure 4. Define Hostname and Login Credentials



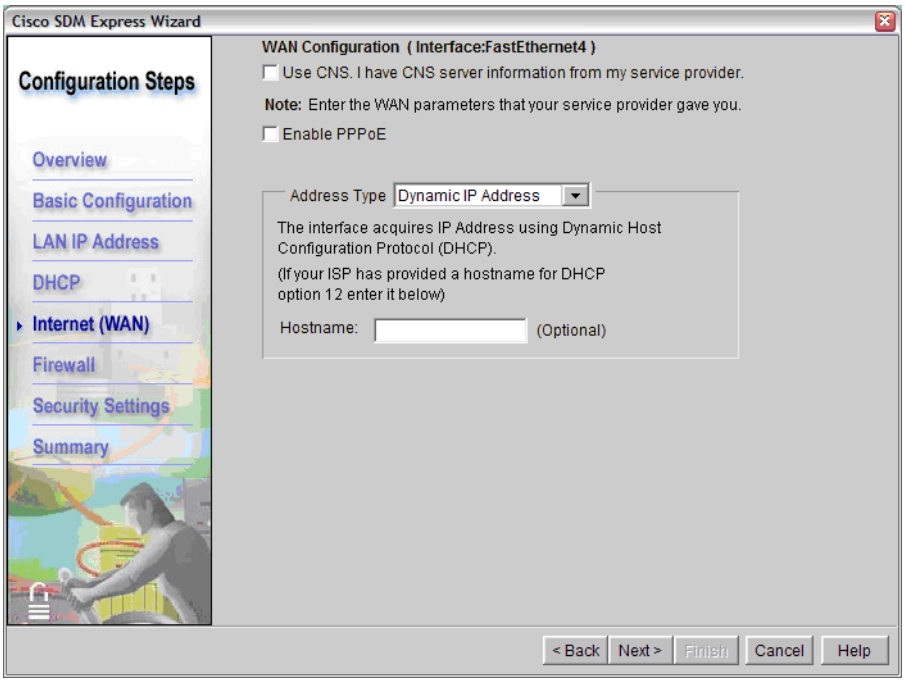
For the admin username (this will be the router login username/password): (Figure 4)

- For username, type: admin
- For password, type: cisco123
- For enable, enter: cisco123
- There is no need to configure the “Wireless Interface Configuration” at this point (in case you are using a wireless-enabled router)

6. Keep the default “LAN Interface Configuration” settings
7. Keep the default “DHCP Server Configuration” settings

8. For the “WAN configuration” select your ISP connection type: static, DHCP, or Point to Point Protocol over Ethernet (PPPoE). Configure the necessary parameters, if static or PPPoE is used. (Figure 5)

Figure 5. ISP Network Access



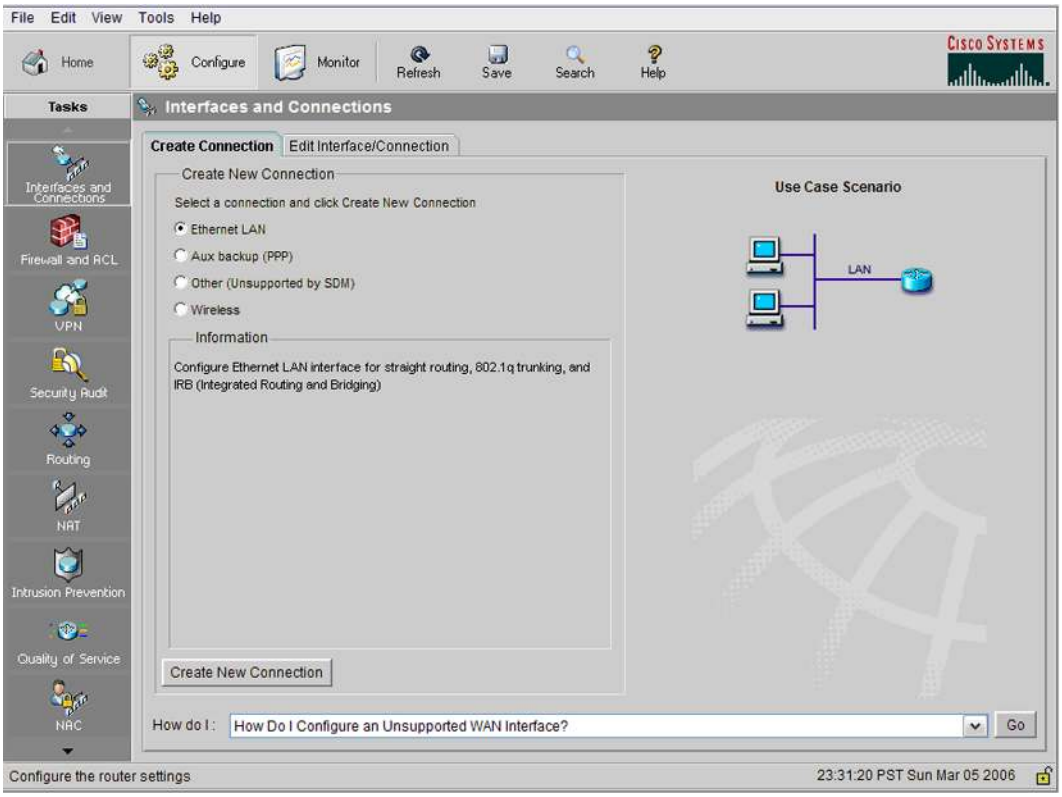
9. Keep the default “Interface WAN (advance options)” for NAT settings.
10. Keep the default “Firewall Configuration” settings.
11. Keep the default “Security Configuration” settings.
12. Click “Finish”. You can optionally save the configuration. Click “Yes” when prompted to “Permit DHCP traffic through the firewall”.
13. Close the wizard.

Once ISP access has been set up, the next logical step is to configure the LAN side. Cisco SDM will close the Express wizard at this point. You now need to start the full Cisco SDM software to begin with the LAN side configuration.

1. Start by restarting Cisco SDM. In the PC, click **Cisco SDM** and enter the **10.10.10.1** IP address. Cisco SDM will force you to remove the default **cisco/cisco** login credentials, as it is too obvious.

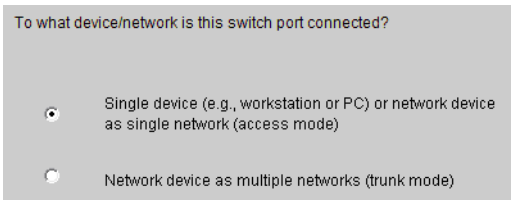
2. Now click the **Configure** top tab and then on **Interfaces and Connection** (Figure 6).

Figure 6. Create New LAN Connection



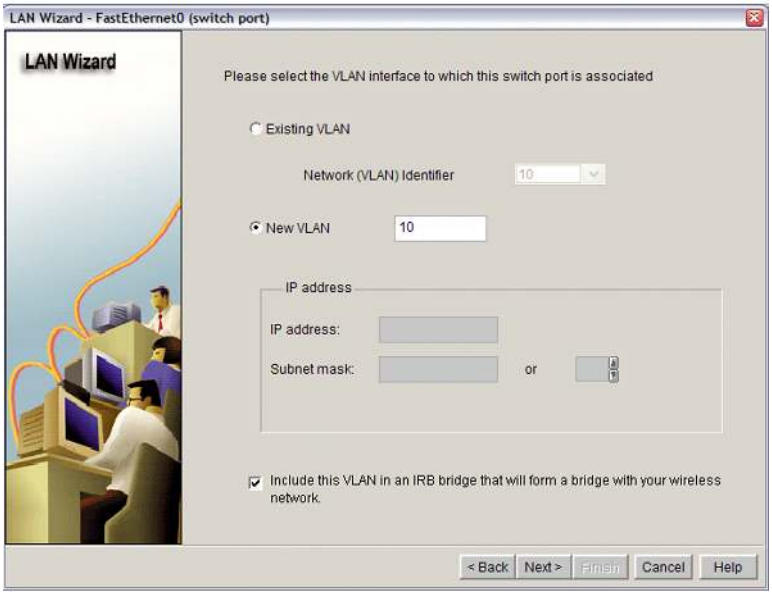
3. The wizard will prompt you to select the LAN interface to configure. Select one of the LAN interfaces that you want to use for corporate traffic.
4. Follow the wizard instructions. For Small Office/Home Office (SOHO), the switch port should be on “access mode” as shown in Figure 7.

Figure 7. Switch Mode for a Router with Switch Ports



5. Again, for a router with switch ports, create a VLAN for your corporate network (VLAN 10, for example). Select the option to "include the VLAN in an IRB bridge", so that you can later configure your wireless interface to share the same VLAN (Figure 8).
6. Click **Next**.

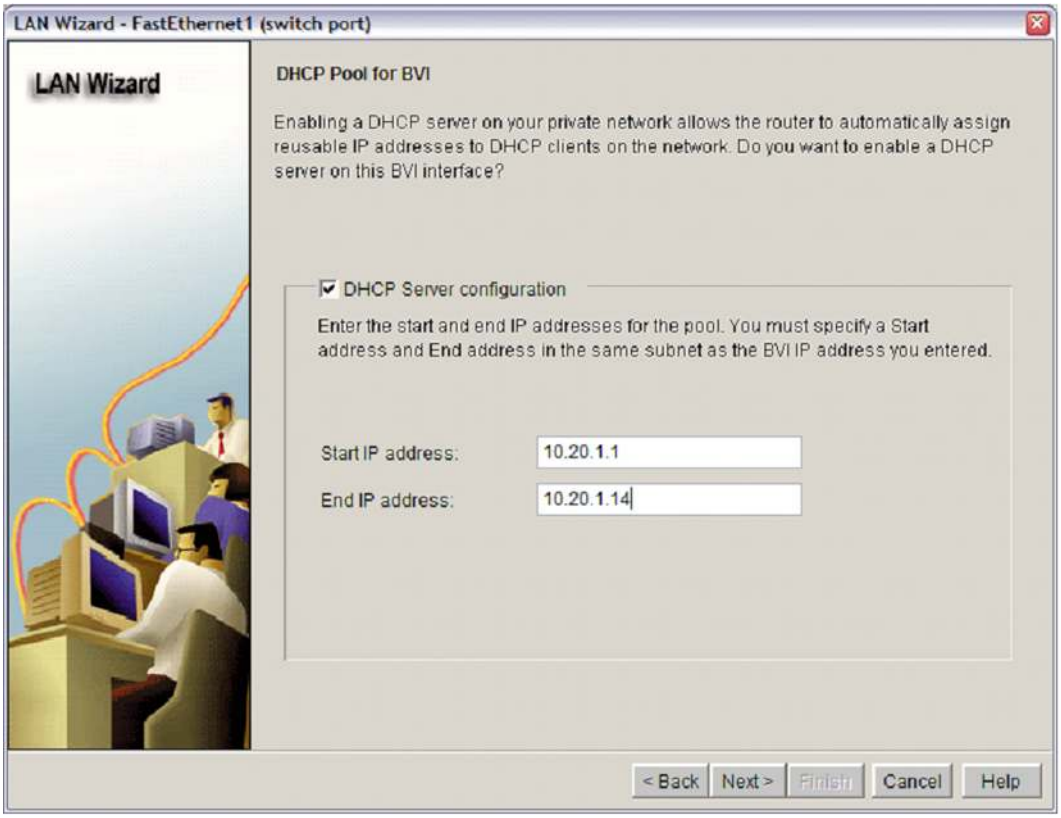
Figure 8. Create VLAN



7. Create a new bridge group, and give it number **1**. Then click **Next**.
8. In the following screen, give bridge group 1 an IP address (it needs to be unique for each spoke and routable thought the corporate network). For example: 10.1.1.1/28.

9. After that, enable a “DHCP server”. Enter the start and end IP address of the spoke subnet in the following screen (Figure 9). Click **Next**.

Figure 9. Add DHCP Server for Trusted Pool



10. Enter the DNS server (required if you use static IP address) WINs and domain name.
11. Click **Finish**. Cisco SDM will deliver the generated configuration to the new Cisco ECT-enabled router.

This is the resulting configuration:

```
ip dhcp pool sdm-pool1
   network 10.20.1.0 255.255.255.240
   domain-name cisco.com
   dns-server 172.16.226.120 171.70.168.183
   default-router 10.20.1.1
!
bridge irb
!
bridge 1 protocol ieee
bridge 1 route ip
!
!
interface FastEthernet0
 switchport access vlan 10
!
```



```
interface Vlan10
 no ip address
 bridge-group 1
!
interface BVI1
 ip address 10.20.1.1 255.255.255.240
!
```

Also, a vlan.dat file is created and saved in the router's flash, with VLAN database information.

At this point, the Cisco 871 router would be able to access the Internet, if it were already connect to the ISP modem at the final destination.

Note: These steps only created a pool for corporate (trusted) access. If your deployment requires a pool for guest (non-trusted) access, which is usually the case when the Cisco ECT-enabled router is used for telecommuting and others need to share the same Internet access, there are additional steps. To create a "guest VLAN", follow the steps described above a second time. Create a second VLAN (VLAN 20, for example) and another bridge interface. For the guest pool, assign any private pool (10.1.1.0/24, for example).

All switch port interfaces need to be assigned to a VLAN to be able to connect to your corporate network or just to the Internet. You can assign interfaces to VLANs by clicking the **Edit Interface/Connection** tab and editing each of the interface properties. You can, for example, put two ports in the corporate VLAN and two on the guest VLAN.

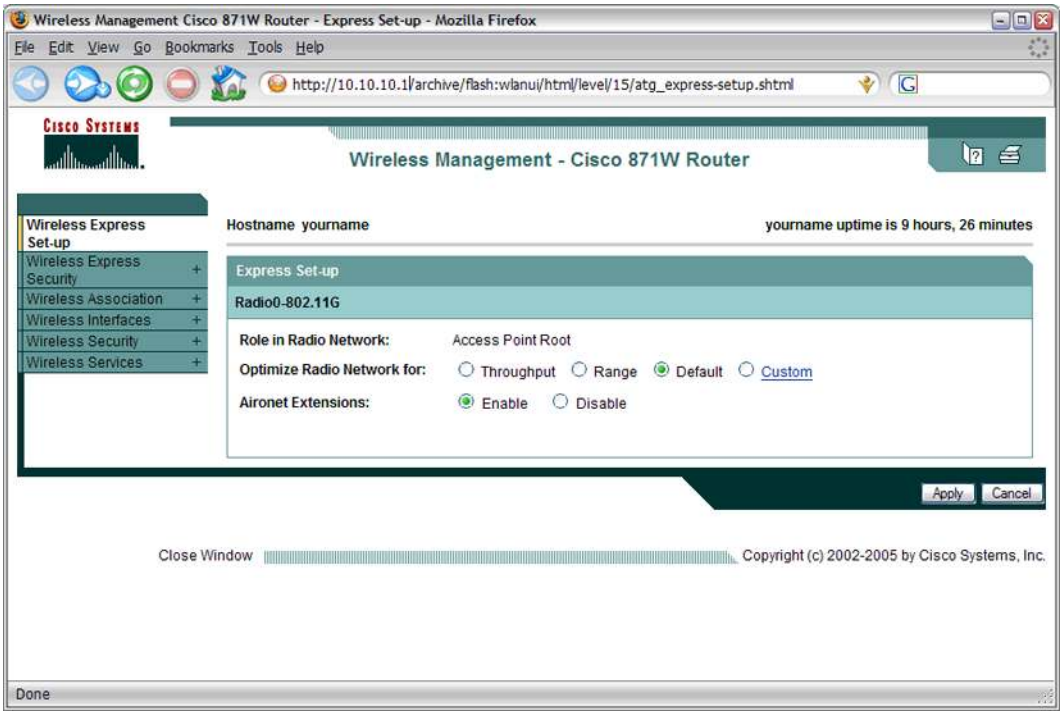
Step 2—Wireless Configuration (Cisco 871 or 1811 Router)

In this example, the Web-based user interface that comes with the Cisco 871 router is used to configure the wireless interface. For Cisco ECT, we recommend Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) for authentication, with Wi-Fi Protected Access (WPA) association mode and Temporal Key Integrity Protocol (TKIP) as the encryption method.

You can start it by typing http://10.10.10.1/archive/flash:wlanui/html/level/15/atg_express-setup.shtml (or use the newly assigned pool IP address if changed), or going to:

1. Cisco SDM **Interfaces and Connections**
2. Select **Wireless**
3. Click **Launch Wireless application**; this opens a browser window (Figure 10)

Figure 10. Wireless User Interface

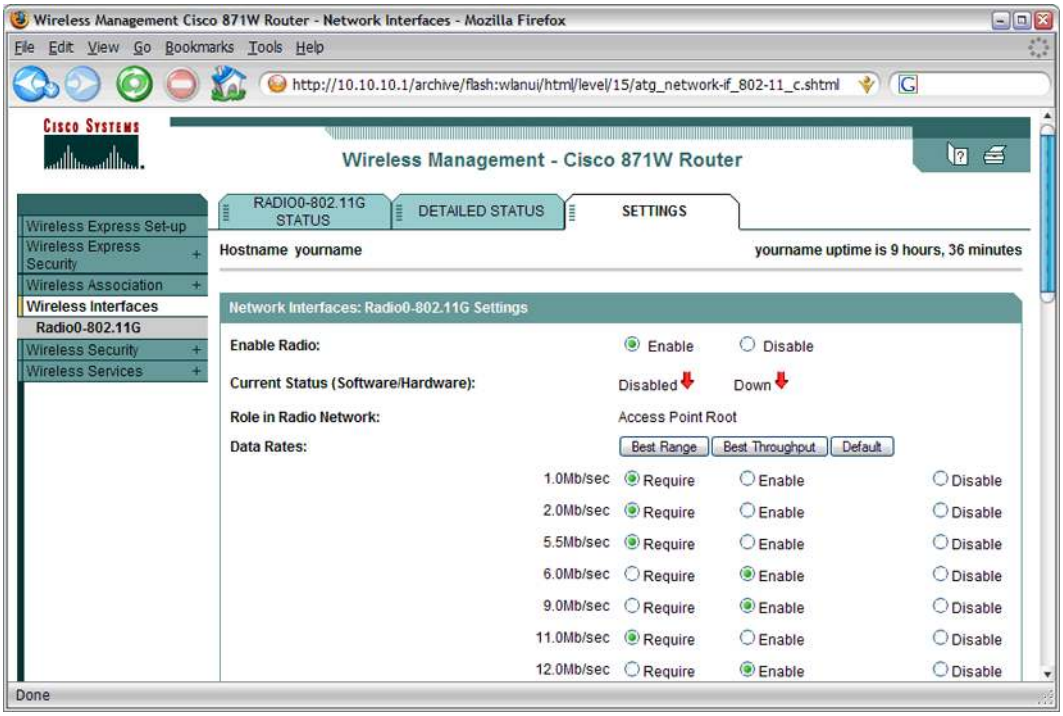


Now let us enable the wireless interface (Figure 11).

4. Select **Wireless Interfaces**
5. Select the **Radio0-802.11G** interface link (in the Cisco 871 router example)
6. Click **Settings** on the upper tab
7. Click the **Enable** radio button and then click **Apply**.

Note: There are multiple speed choices. You can keep the default ones, or select your own by scrolling down and selecting the required ones. We recommend keeping the defaults here.

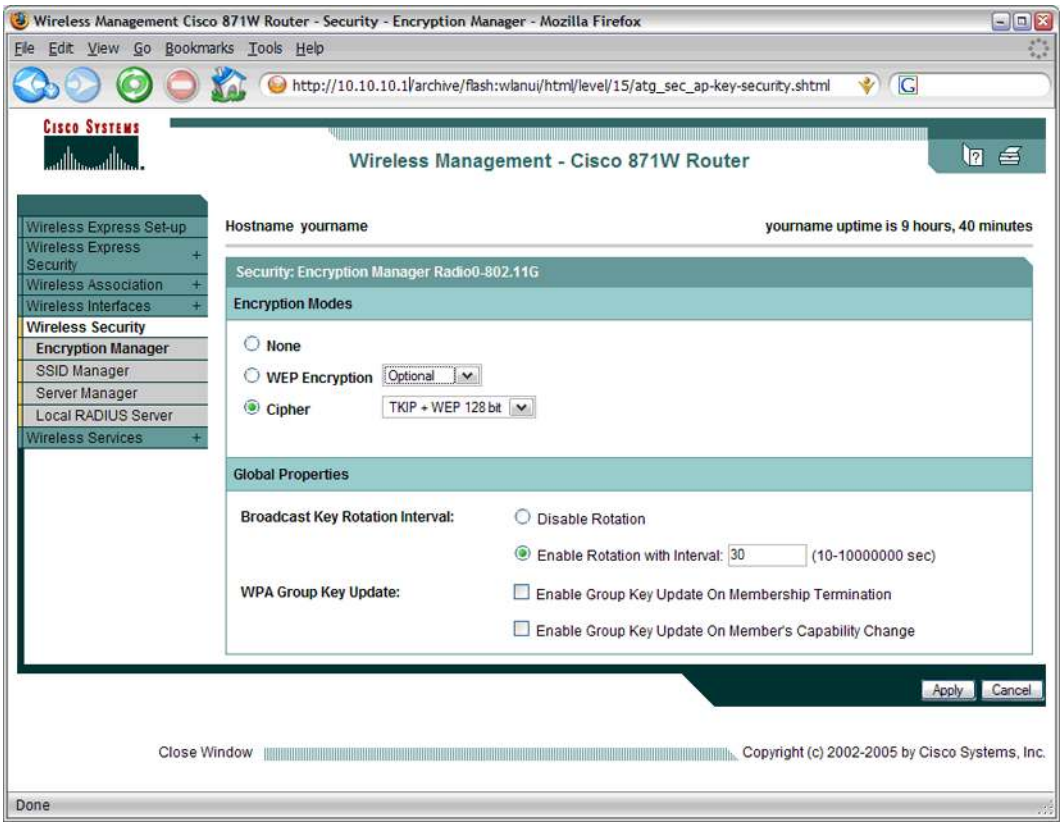
Figure 11. Enable the Wireless Interface



8. Select **Wireless Security** from the menu at left.

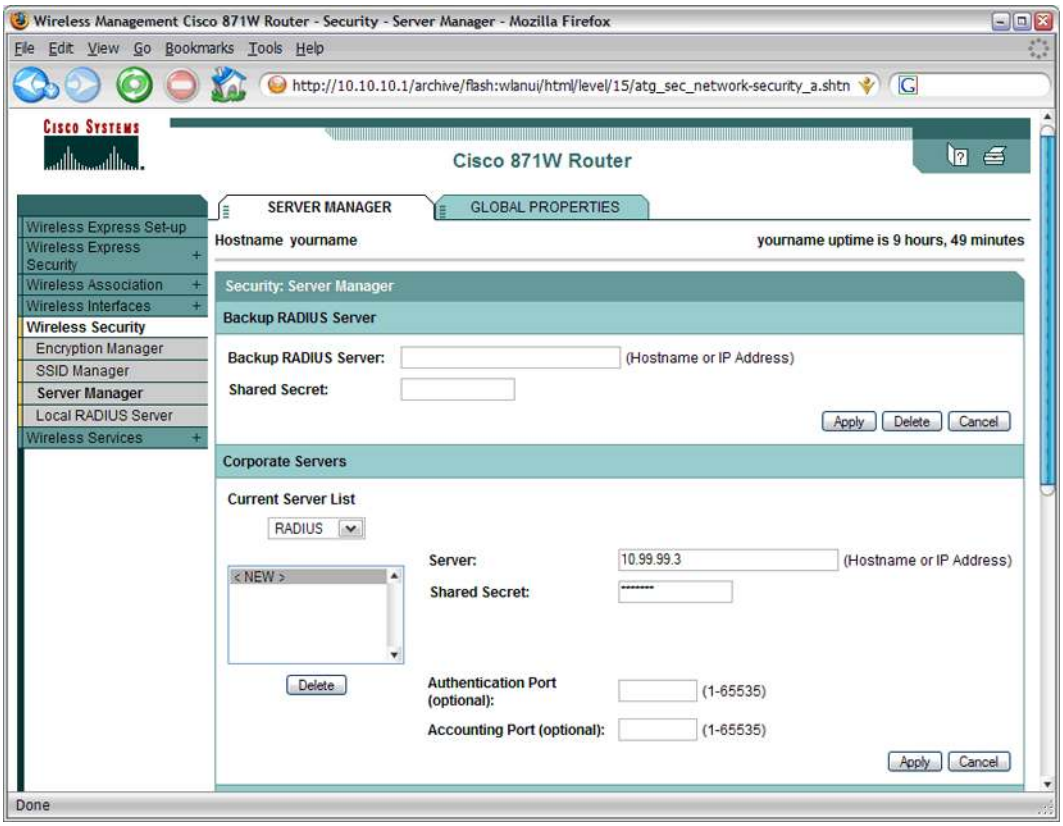
9. Click the **Cipher** radio button (Figure 12).
10. Select **TKIP + WEP 128 bit** from the drop-down list.
11. Under "Broadcast key rotation interval," click the **Enable Rotation** radio button and set the interval rotation to **30** seconds. (Figure 12).
12. Click **Apply**.

Figure 12. Wireless Encryption



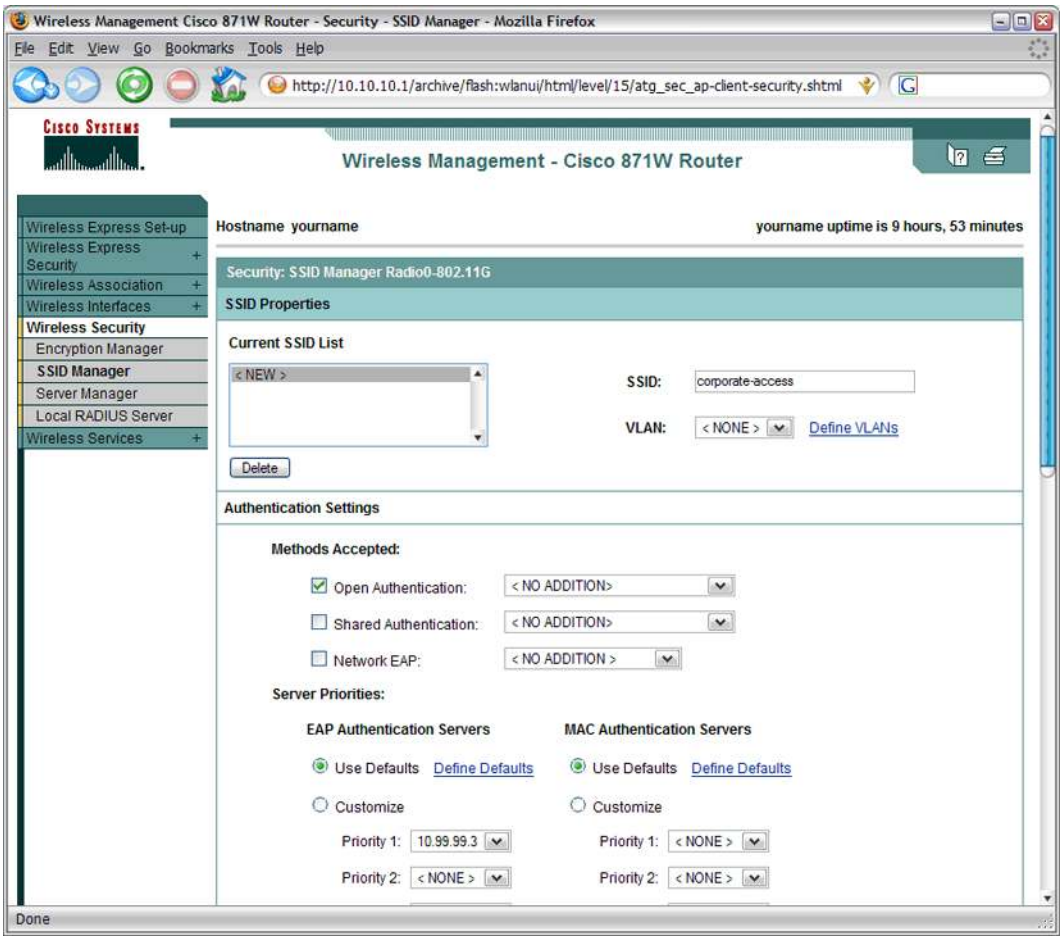
13. Now, create the EAP “Server Manager” – the authentication server that will be used. It can be global for all devices in the VPN, or local per device. You can keep the default “Global Properties” and also the “Default Server Properties” as shown in Figure 13. You just need the corporate AAA server ip address and shared key.

Figure 13. Create an Authentication Server Manager



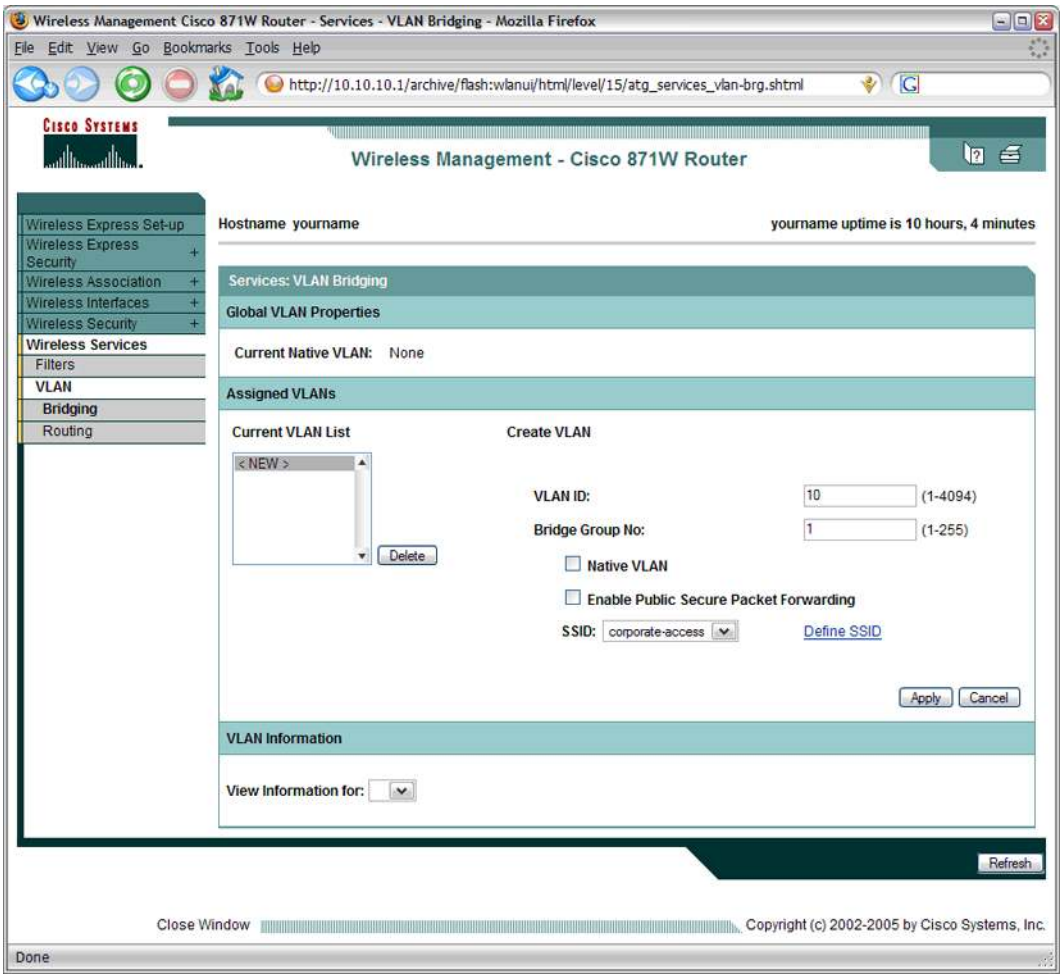
14. Next, create the SSID by first select the “SSID Manager” menu option on the left and select the EAP Server Manager that you just created before (Figure 14). You also need to give it a name, like “corporate-access”.

Figure 14. Create an SSID and Associate with EAP Server



15. Finally, associate the SSID with the corporate VLAN and the respective bridge interface. In this example, the corporate VLAN is **VLAN10** and the bridge interface is **BVI1**. Go to "Wireless Services > VLAN > Bridging". (Figure 15)
16. Select the SSID created previously (we called it "corporate-access")
17. For the VLAN ID, enter **10**; for Bridge Group No., enter **1** (Figure 15).

Figure 15. Associate SSID with VLAN and Bridge Interface



This is the resulting configuration:

```
!
aaa new-model
!
!
aaa group server radius rad_eap
!
aaa group server radius rad_mac
!
aaa group server radius rad_acct
!
```



```
aaa group server radius rad_admin
!
aaa group server tacacs+ tac_admin
!
aaa group server radius rad_pmip
!
aaa group server radius dummy
!
aaa group server radius rad_eap1
 server 10.99.99.3 auth-port 1645 acct-port 1646
!
aaa authentication login eap_methods group rad_eap
aaa authentication login mac_methods local
aaa authentication login eap_methods1 group rad_eap1
aaa authorization ipmobile default group rad_pmip
aaa accounting network acct_methods start-stop group rad_acct
!
…
!
interface Dot11Radio0
 no ip address
 !
 broadcast-key change 30
 !
 !
 encryption mode ciphers tkip wep128
 !
 ssid corporate-access
    vlan 10
    authentication open eap eap_methods1
 !
 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 Dot11Radio0.10
 encapsulation dot1Q 10
 no snmp trap link-status
 no cdp enable
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 spanning-disabled
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
!
```


Step 3—VPN Configuration

It might seem logical to next configure the firewall and ACLs, but it is better to do this last. Cisco SDM will automatically generate rules for VPN, DHCP, NTP, and other protocols if they are already configured.

For Cisco ECT, it is recommended to use one tunnel just dedicated for management, which should be completely separated from the corporate data access tunnels. The main objective is to always have a secure link to the remote device to provide for policy update, image management, and device and user authentication. The management VPN tunnel can be achieved with plain IPsec tunnel, or using Cisco Easy VPN. Please refer to the Cisco ECT deployment guide for more information about configuring the management gateway.

The use of PKI is recommended for Cisco ECT deployments; PKI is more secure than pre-shared keys, and it scales better.

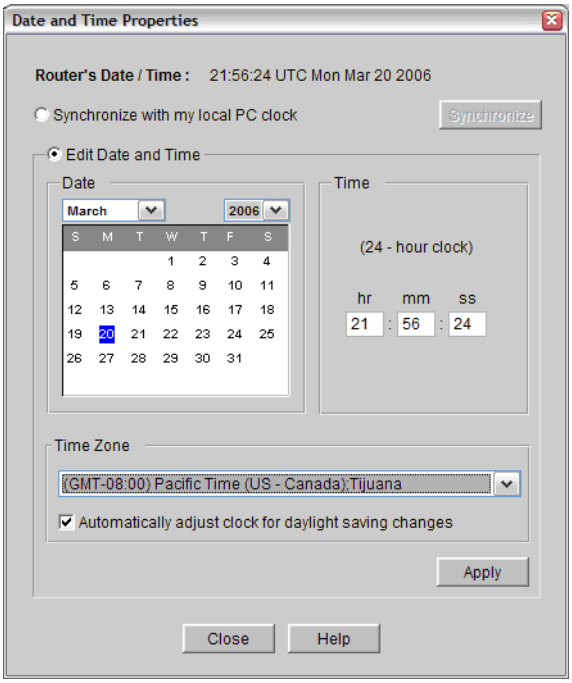
These are the steps for management and actual tunnel configuration:

- Add NTP servers for PKI
- Create a PKI certificate trust point
- Create an IKE policy
- Create an IPsec transform set

Use these policies for configuring a regular IPsec tunnel for management and DMVPN tunnels for data traffic.

Before starting, make sure that the time zone is set. Go to “Additional Tasks > Router Properties > Date/Time” to select your time zone (Figure 16).

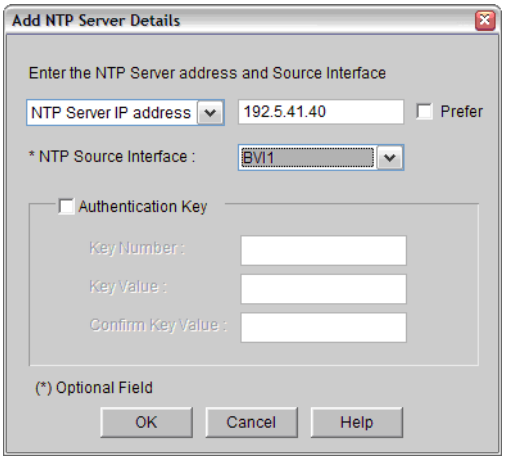
Figure 16. Set the Time Zone



Network Time Protocol

For PKI, the remote VPN router must be synchronized to a global clock to check for certificate validation. A public domain NTP server is recommended. Go to the “Additional Tasks” main tab. To add an NTP server, select **NTP** from the “Router Properties”. In Figure 17 we add the 192.5.41.40.

Figure 17. Adding an NTP Server



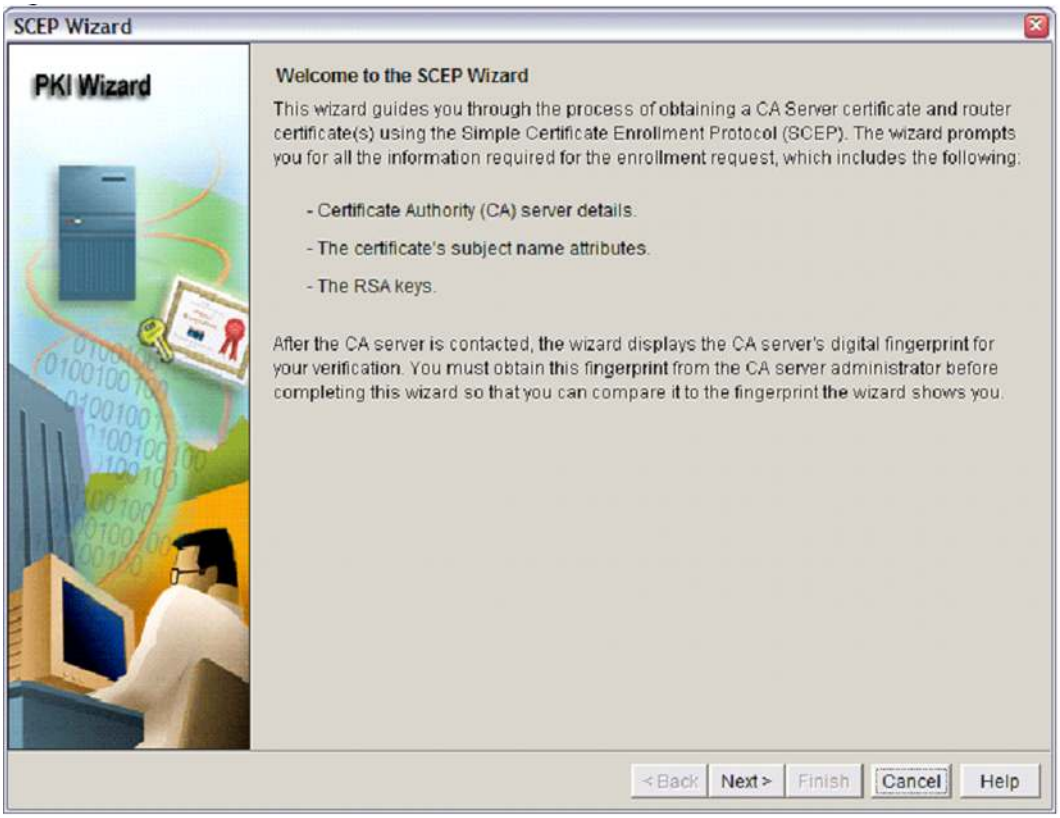
At this step, also add the clock adjustment settings. Select **Date/Time** from the “Router Properties” list, and set your clock to your local area. Make sure all your VPN routers are in the same time zone.

Crypto Policies

1. Click on **VPN**.
2. Click on **VPN Components**, followed by **Public Key Infrastructure**, and then **Certificate Wizards**.

3. Launch the SCEP Wizard (Figure 18)

Figure 18. Launch the Certificate Wizard



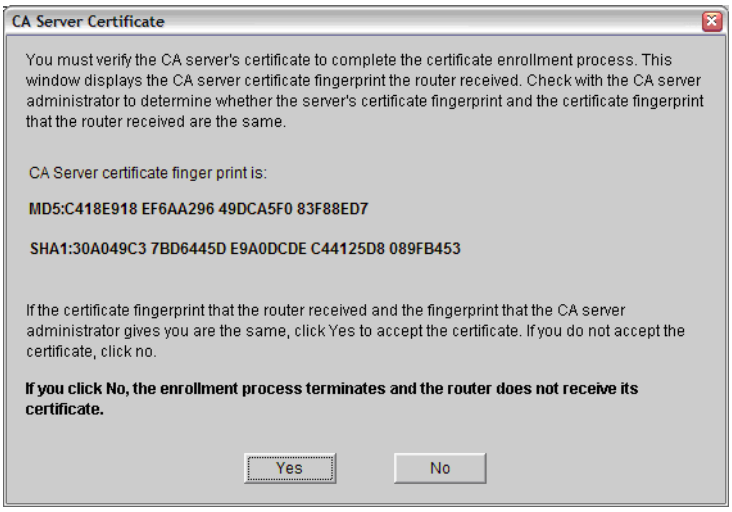
4. Enter the trust point name and the enrollment URL (for example: http://my-pki-server:80 Figure 19). The certificate server must have been already configured. More information is available in the Cisco ECT deployment guide.

Figure 19. Enter PKI Certificate Server Name

5. In the next screen, include the FQDN and serial number, but not the IP address; this will likely change due to DHCP reassignment.
6. On the next page, select **Generate new key pairs**.

7. Click **Next**. Cisco SDM will deliver the configuration to the Cisco 871 router, generate RSA keys, and enroll with the PKI certificate server. You will be prompted to accept the fingerprint, as shown in Figure 20. Click **Yes**.

Figure 20. Accept the PKI Certificate Enrollment



8. Next, the enrollment status screen pops up (Figure 21).
9. Click **Finish**.

Figure 21. Certificate Enrollment Request Sent to PKI Server

At this point, you can check in the router's console that the certificate was received from the PKI server. Here is an example:

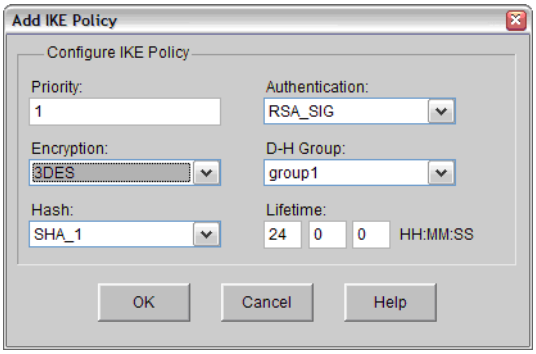
```
%SYS-5-CONFIG_I: Configured from console by admin on vty0 (10.10.10.2)
%CRYPTO-6-AUTOGEN: Generated new 512 bit key pair
CRYPTO_PKI:  Certificate Request Fingerprint MD5: AD9B9E47 0EB69623 380BE2BB 06DA2273
CRYPTO_PKI:  Certificate Request Fingerprint SHA1: EFAB5ABE FD1B2AC9 247F927F 5F9ED0FA
E1776578
%SYS-5-CONFIG_I: Configured from console by admin on vty0 (10.10.10.2)
%PKI-6-CERTRET: Certificate received from Certificate Authority
```

On Cisco SDM you can also click on **Router Certificates**, select the trust point that was just created, and click **Refresh** to see the result.

Now, we can proceed to configuring an IKE policy (Figure 22).

1. Click on **IKE Policies** and then **Add**.
2. Select the **3DES** (or **AES 256**) for encryption, **SHA** for hash, and **RSA-SIG** for authentication.
3. Click **OK**.

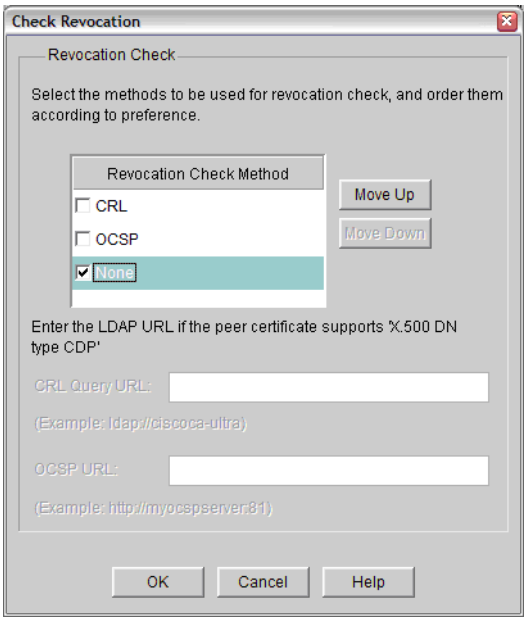
Figure 22. Add IKE policy



After you are done, it is necessary to set the certificate revocation list (CRL) check for "none"; a remote router will not be able to retrieve the CRL unless the tunnel is up. PKI certificate servers are usually behind a firewall and cannot be accessed from the Internet. You can optionally publish the CRL in a Lightweight Directory Access Protocol (LDAP) public access server.

To set the revocation check, go to **VPN-VPN Components-Router Certificates**. Select the PKI trust point just created. Click on **Revocation Check** and set it to **None** (Figure 23).

Figure 23. Revocation Check



Now we can create a new site-to-site VPN for the management gateway tunnel:

1. Select the site-to-site VPN and click **Add**.
2. Select **Launch the Selected Task**.
3. Select the **Site-to-Site VPN Wizard**.
4. In the next screen, select the WAN interface for this tunnel. For the Cisco 871 router, this is FastEthetnet4. It can also be a dialer interface if that is used.
5. Select your peer's (Secure Management Gateway) IP address. This is the public head-end IP address.
6. Select **Digital Certificates**.
7. In the next screen, and for the IKE policy, select the one you just created before.
8. In the next screen, select the default IPsec transform set.

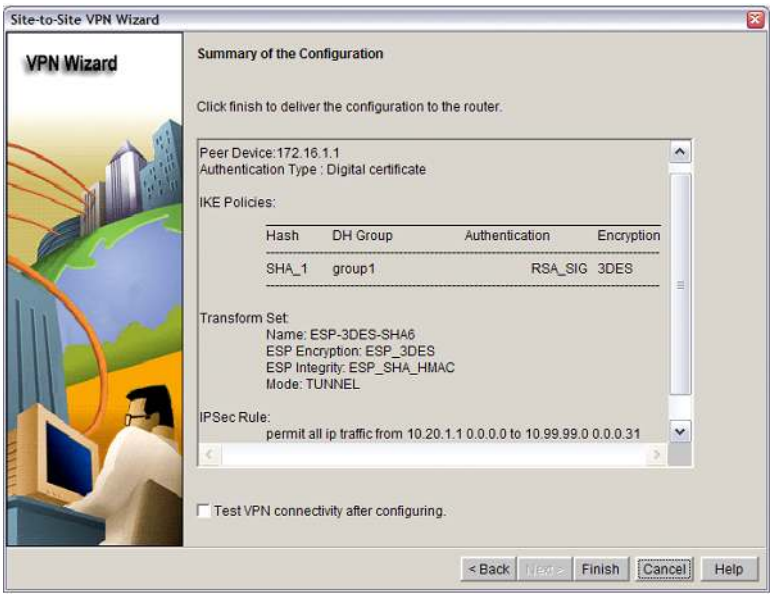
9. Next, Cisco SDM asks about the protected subnet. If, for example, the remote Cisco 871 VPN router will be assigned the 10.20.1.0/28 protected subnet, and the Cisco ECT-enabled management servers sit in the 10.99.99.0/27 subnet, then the selection would be as shown in Figure 24.

Note: Only the router IP address is used. End PCs or other hosts should not have access to the management servers. Only the router itself needs to be allowed (Figure 24).

Figure 24. Define Traffic for the Management Servers

10. In the following screen, Cisco SDM asks to confirm the values entered (Figure 25).
11. If all values are correct, click **Finish**.

Figure 25. Push the Management Tunnel Configuration to the Cisco 871 Router



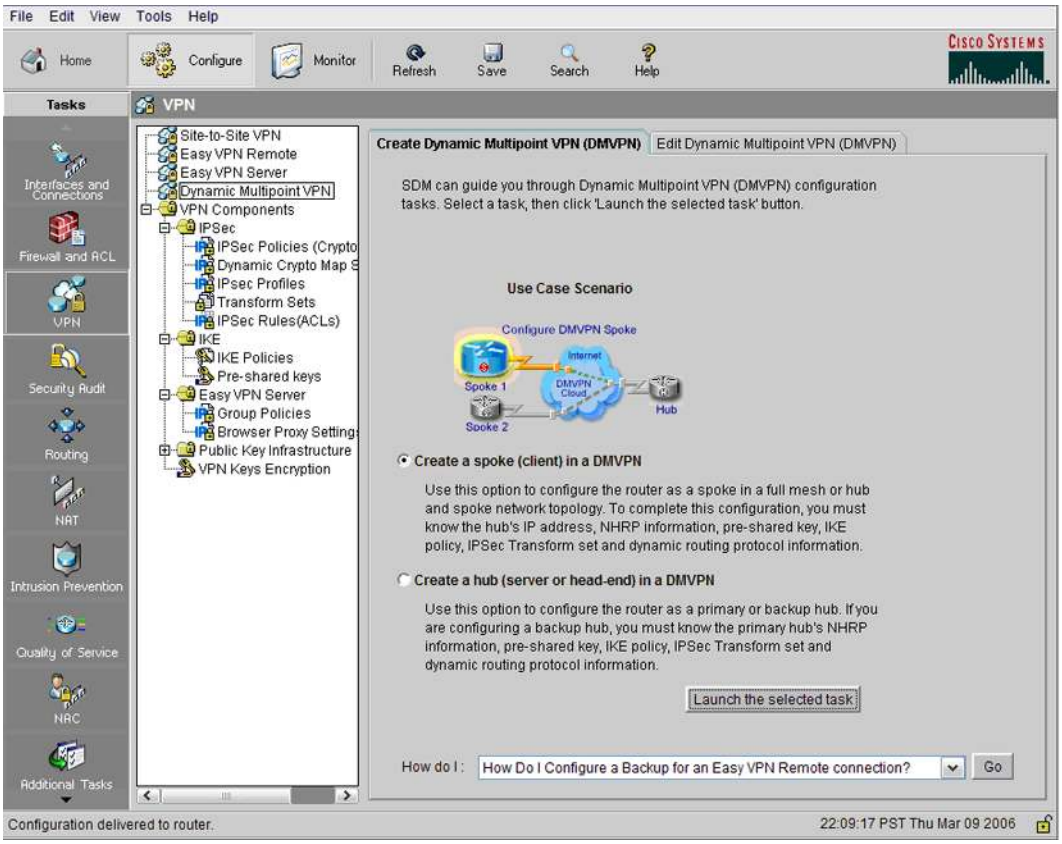
The above steps result in the following sample configuration:

```
crypto isakmp policy 10
 encr 3des
!
crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
!
crypto map SDM_MAP 1 ipsec-isakmp
 description Tunnel to172.16.1.1
 set peer 172.16.1.1
 set security-association lifetime kilobytes 4608000
 set security-association lifetime seconds 3600
 set transform-set ESP-3DES-SHA
 match address 100
 qos pre-classify
!
interface FastEthernet4
 ip nat outside
 crypto map SDM_MAP
!
ip nat inside source route-map SDM_RMAP_1 interface FastEthernet4 overload
!
ip access-list extended SDM_NAT
remark IPSec Rule
 deny   ip host 10.20.1.1 10.99.99.0 0.0.0.31
!
access-list 100 remark SDM_ACL Category=4
access-list 100 remark IPSec Rule
access-list 100 permit ip host 10.20.1.1 10.99.99.0 0.0.0.31
!
route-map SDM_RMAP_1 permit 1
 match ip address SDM_NAT
```


Now that a management tunnel is established, we can configure the DMVPN network that will be used for remote data access to the corporate servers.

1. Under the VPN tab, select **Dynamic Multipoint VPN** and click the **Create a spoke (client) in a DMVPN** radio button (Figure 26).
2. Click **Launch the selected task**.

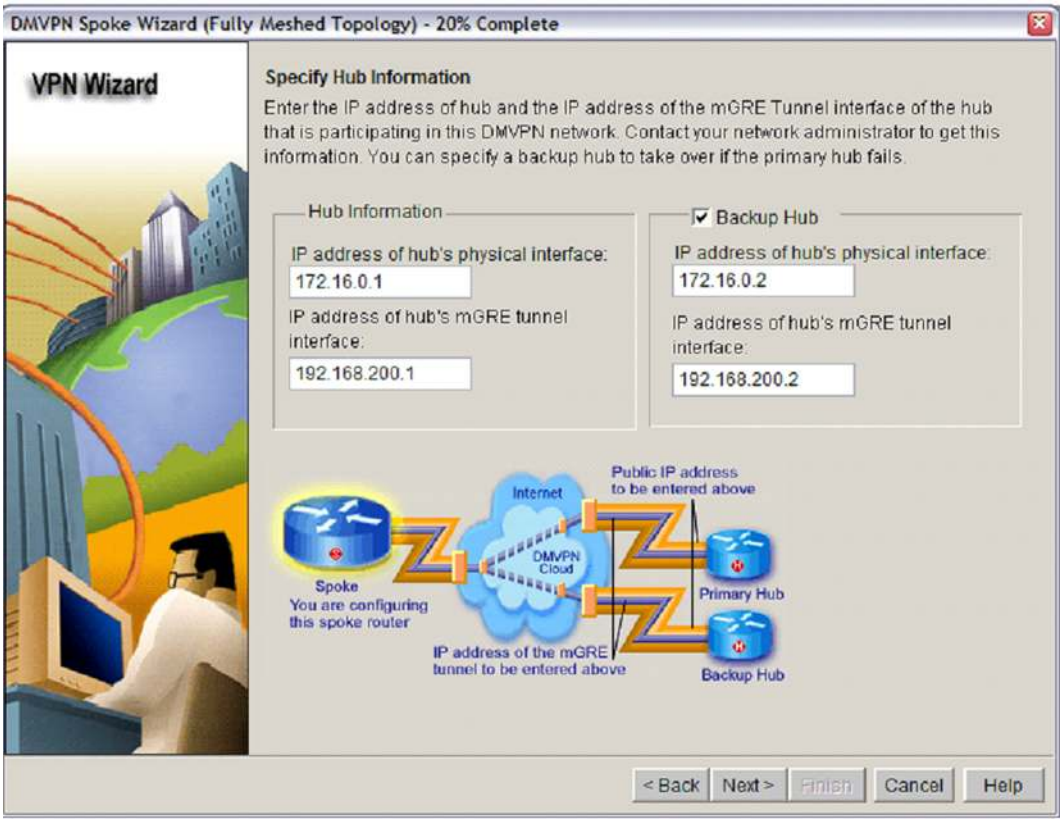
Figure 26. Start DMVPN Configuration



3. When prompted about the DMVPN topology, select the one that fits your deployment. Full mesh is recommended for direct spoke-to-spoke. Load in the hubs is reduced when it is foreseen that a significant percentage of direct spoke-to-spoke traffic will occur.

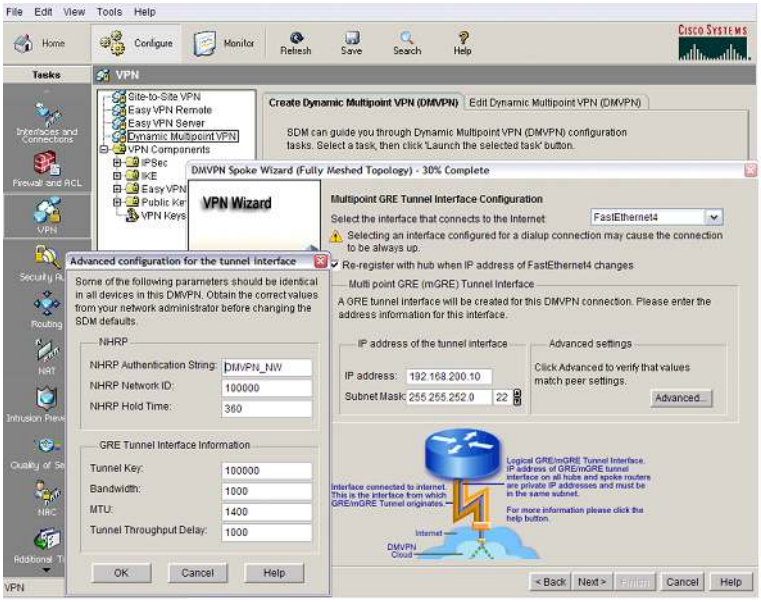
4. In the next screen (Figure 27), enter your DMVPN IP addresses (these are the internal multipoint GRE [mGRE] IP addresses). For Cisco ECT, it is recommended to use a backup hub that can take over all traffic when the main hub goes down for any reason.
5. Click **Next**.

Figure 27. DMVPN Hubs Where the Spoke Will Connect



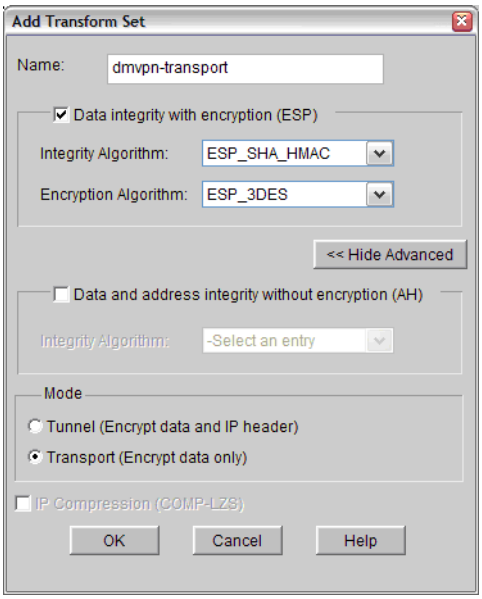
Next, select the next available mGRE tunnel IP address for the new spoke. It is necessary to set the common NHRP parameters for the entire DMVPN deployment in advance (Figure 28). The WAN interface also needs to be selected at this point, usually the FastEthernet4 for a Cisco 871 router, or the dialer interface if PPPoE is used to connect to the Internet.

Figure 28. NHRP and DMVPN Parameters



6. Next, select **Digital Certificates** and **Create a new IPsec transform set**.
7. In the "Add Transform Set" window (Figure 29), select **Transport Mode**. It is the supported method for DMVPN.

Figure 29. Create a Transport Mode IPsec Transform Set for DMVPN



8. In the next screen, select the routing protocol. EIGRP, OSPF, and RIP will work, but EIGRP or OSPF are recommended for a Cisco ECT deployment.

This results in the following sample configuration:

```
crypto ipsec transform-set dmvpn-transport esp-3des esp-sha-hmac
 mode transport
!
crypto ipsec profile SDM_Profile1
 set transform-set dmvpn-transport
!
interface Tunnel0
 bandwidth 1000
 ip address 192.168.200.10 255.255.240.0
 no ip redirects
 ip mtu 1400
 ip nhrp authentication secret12
 ip nhrp map 192.168.250.2 172.16.0.2
 ip nhrp map multicast 172.16.0.1
 ip nhrp map 192.168.250.1 172.16.0.1
 ip nhrp map multicast 172.16.0.2
 ip nhrp network-id 100000
 ip nhrp holdtime 360
 ip nhrp nhs 192.168.250.1
 ip nhrp nhs 192.168.250.2
 ip tcp adjust-mss 1360
 delay 1000
 tunnel source FastEthernet4
 tunnel mode gre multipoint
 tunnel key 100000
 tunnel protection ipsec profile SDM_Profile1
!
router eigrp 33
 network 192.168.0.16 0.0.0.15
 network 192.168.192.0 0.0.15.255
 no auto-summary
```


Step 4—NAT/PAT

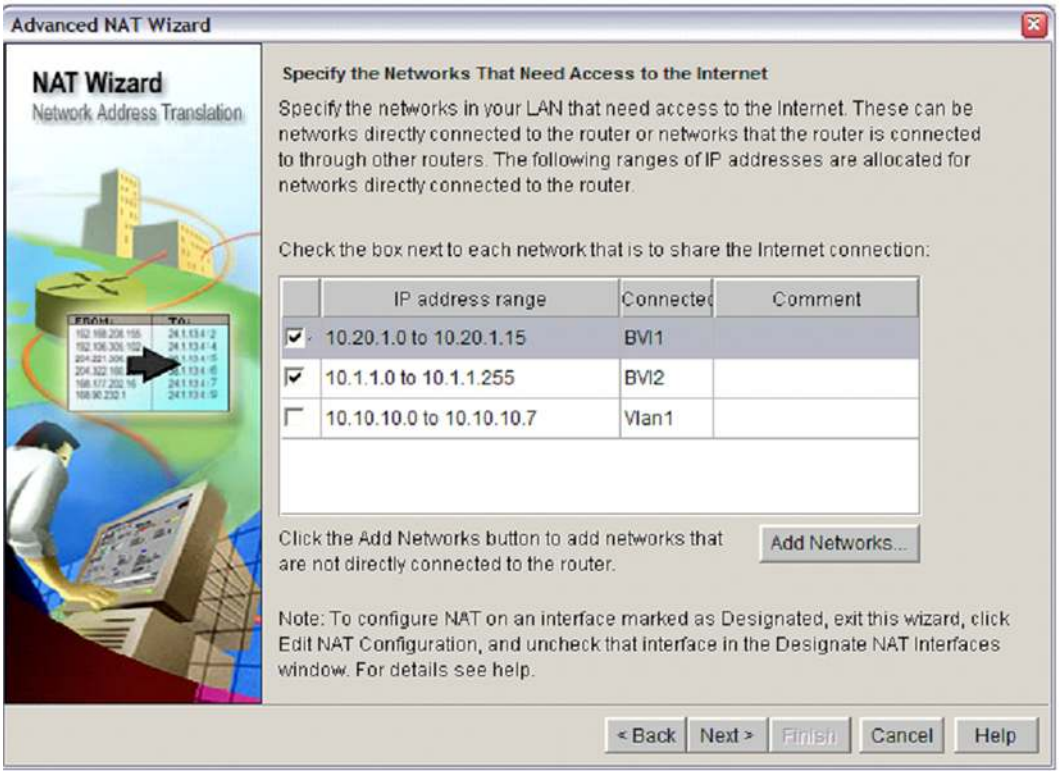
To have a guest VLAN, or to enable split tunneling to make sure that only your corporate traffic comes to your data gateways and all other traffic goes directly to the Internet, you will need to enable NAT/PAT in the remote device.

If all traffic is routed through your corporate gateways, there is no need to enable NAT. For a Cisco ECT deployment it is optional, but it is most common to allow a guest VLAN to directly access the Internet.

For a remote VPN router we advise the use of PAT. To add PAT:

1. Select the NAT/PAT menu from the list on the left.
2. Select **Basic NAT** and start the Advanced NAT Wizard (Figure 30).

Figure 30. PAT Configuration



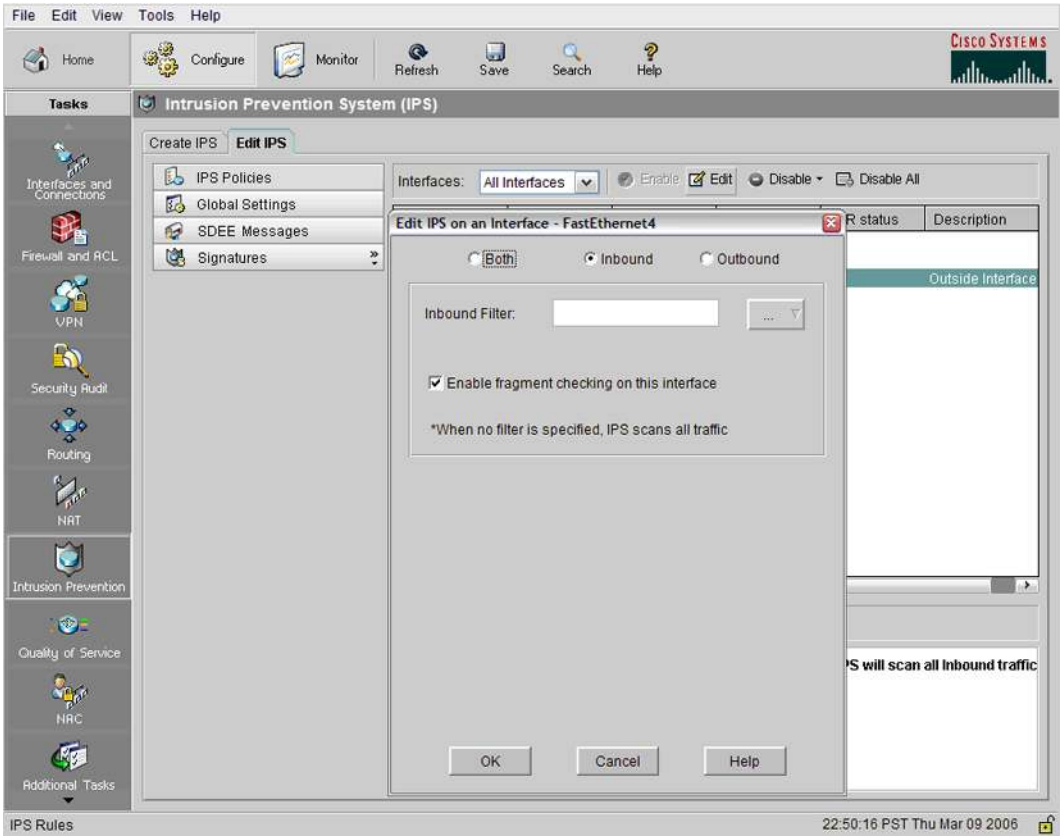
3. Select the outside (WAN) interface. This is usually the FastEthernet4 interface for an Cisco 871 router, or Dialer1 if PPPoE is used.
4. Select both the corporate and guest VLAN pools, BVI1 and 2 (if configured), to allow for Internet access for the Cisco 871 router.
5. Click **Finish**.

Step 5—Intrusion Prevention

This is a quick process.

1. Select the **Intrusion Prevention** tab option from the left menu (Figure 31).
2. Click the **Edit IPS** tab on top. For Cisco ECT deployments, it is recommended to always use IPS at least for the WAN interface.
3. When using a Cisco 871 router as a VPN router, select the **FastEthernet4** interface and click **Enable**. You have selected the respective interface and the click on **Edit** (Figure 31).
4. In the "Edit IPS on an Interface—FastEthernet4" window, select the **Inbound** traffic radio button. Click **OK**. The **Enable fragment checking on this interface** option should also be checked, to protect against IP fragment attacks.

Figure 31. Intrusion Prevention

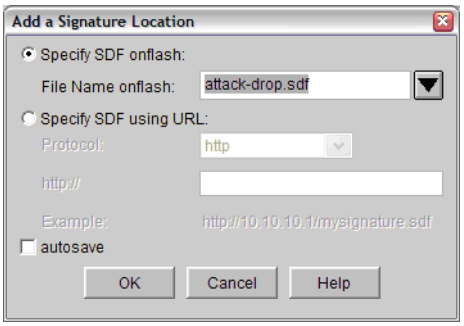


To select the signature definition file (SDF), go to the **Global Settings** menu and click **+ Add**. The "Add a Signature Location" window will appear (Figure 32). Select an SDF from the drop-down menu.

By default, new integrated service routers come with an attack-drop.sdf on flash. This file can also be kept updated by downloading it from http://www.cisco.com/cgi-bin/tablebuild.pl/ios-sigup where Cisco publishes it.

Note: In order to be able to download this software, an account with Cisco.com is required.

Figure 32. Select the Signature Definition File



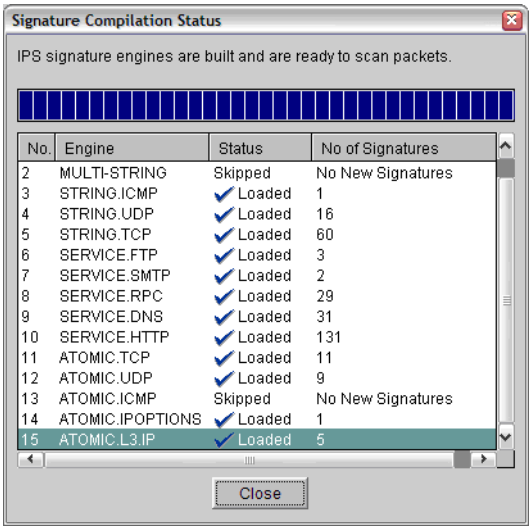
Note: If you wish to disable a particular signature, just click on the **Signatures** menu from Figure 31 to view and select it.

This is the resulting configuration:

```
ip ips sdf location flash://attack-drop.sdf
!
ip ips name ips-rule
!
interface FastEthernet4
  ip ips ips-rule in
```

The list of built-in signatures is shown in the Signature Compilation Status window (Figure 33).

Figure 33. Select IPS Signatures



Step 6—Quality of Service

For a Cisco ECT deployment, it is recommended that voice, ISAKMP, and routing traffic be prioritized so that voice quality is clear, the router does not lose tunnels during IKE renegotiation, and routing traffic can go though.

1. Select the **Quality of Service** tab to launch the QoS wizard.
2. Select the outside interface. For a Cisco 871 router, it is **FastEthernet4**.
3. On the following screen (Figure 34), Cisco SDM allows us to fine-tune some default values. There is no need to change them for a Cisco ECT deployment.

Figure 34. Default QoS Settings

This is the resulting sample configuration:

```
class-map match-any SDMVoice-FastEthernet4
 match protocol rtp audio
class-map match-any SDMTrans-FastEthernet4
 match protocol citrix
 match protocol finger
 match protocol notes
 match protocol novadigm
 match protocol pcanywhere
 match protocol secure-telnet
 match protocol sqlnet
 match protocol sqlserver
```



```
 match protocol ssh
 match protocol telnet
 match protocol xwindows
class-map match-any SDMScave-FastEthernet4
 match protocol napster
 match protocol fasttrack
 match protocol gnutella
class-map type access-control match-all http
 match field TCP dest-port eq 80
class-map type stack match-all ip_tcp
 match field IP protocol eq 6 next TCP
class-map type stack match-all ip_udp
 match field IP protocol eq 17 next UDP
class-map match-any SDMIVideo-FastEthernet4
 match protocol rtp video
class-map match-any SDMSVideo-FastEthernet4
 match protocol cuseeme
 match protocol netshow
 match protocol rtsp
 match protocol streamwork
 match protocol vdolive
class-map type access-control match-all ftp
 match field TCP dest-port eq 21
class-map match-any SDMBulk-FastEthernet4
 match protocol exchange
 match protocol ftp
 match protocol irc
 match protocol nntp
 match protocol pop3
 match protocol printer
 match protocol secure-ftp
 match protocol secure-irc
 match protocol secure-nntp
 match protocol secure-pop3
 match protocol smtp
 match protocol tftp
class-map match-any SDMSignal-FastEthernet4
 match protocol h323
 match protocol rtcp
class-map match-any SDMRout-FastEthernet4
 match protocol bgp
 match protocol eigrp
 match protocol ospf
 match protocol rip
 match protocol rsvp
class-map match-any SDMManage-FastEthernet4
```



```
 match protocol dhcp
 match protocol dns
 match protocol imap
 match protocol kerberos
 match protocol ldap
 match protocol secure-imap
 match protocol secure-ldap
 match protocol snmp
 match protocol socks
 match protocol syslog
class-map type access-control match-all codered
 match start l3-start offset 40 size 32 regex "GET /default.ida\x3FNNNNNNNNNNNNNN"
 match field TCP dest-port e
!
policy-map SDM-Pol-FastEthernet4
 class SDMTrans-FastEthernet4
  bandwidth remaining percent 33
  set dscp af21
 class SDMSignal-FastEthernet4
  bandwidth remaining percent 40
  set dscp cs3
 class SDMRout-FastEthernet4
  bandwidth remaining percent 3
  set dscp cs6
 class SDMVoice-FastEthernet4
  priority percent 70
  set dscp ef
 class SDMManage-FastEthernet4
  bandwidth remaining percent 3
  set dscp cs2
!
interface FastEthernet4
 ip nbar protocol-discovery
 service-policy output SDM-Pol-FastEthernet4
```

Note: Cisco SDM will activate Network-Based Application Recognition (NBAR) for matching traffic.

Not all of settings shown in the above sample configuration are necessary for an ECT spoke. We can see, for example, that for many routing protocols are used. For an ECT deployment, only one is actually deployed. But it is much easier to accept SDM default QoS settings, as this is a superset of an ECT spoke needs, and thus will still provide the minimum quality of service, plus extra settings.

Step 7—Network Admission Control

For a Cisco ECT deployment, you can optionally enable Network Admission Control (NAC).

1. Start by selecting the **NAC Components** tab.
2. Under the NAC Components menu, select **Exception Policies**.
3. If you use voice over your VPN, you will want to create an exception policy for IP phones. In the Add Exception Policy window, in the "Name" field, enter **ip-phones**. Click **Add** to create a new access rule and **permit ip any any** (Figure 35)

Figure 35. Create an Access List for Permitting IP Phone Traffic

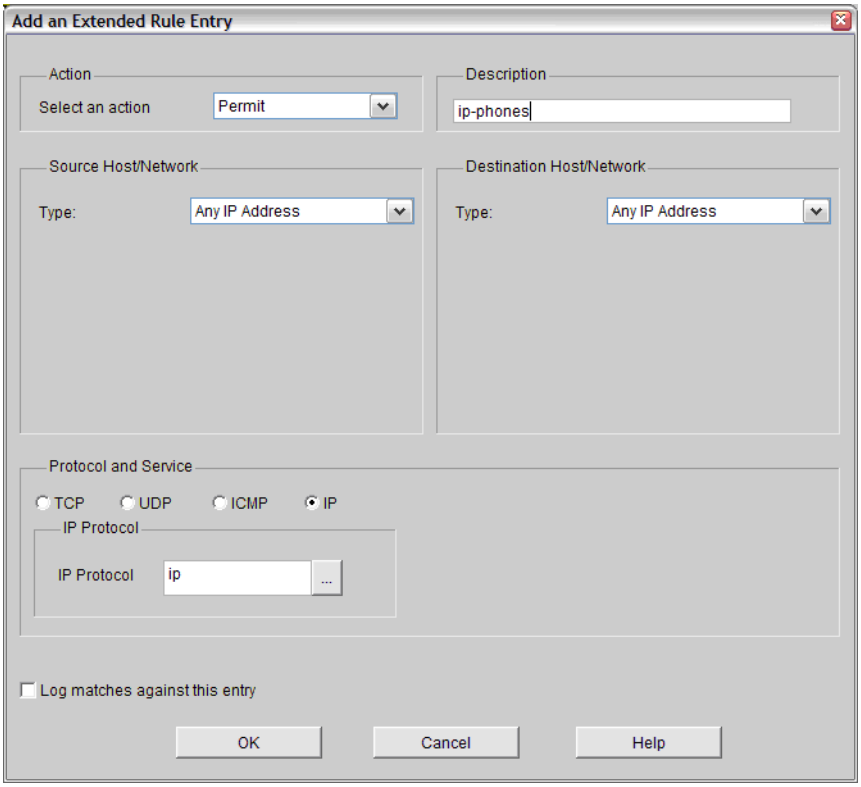
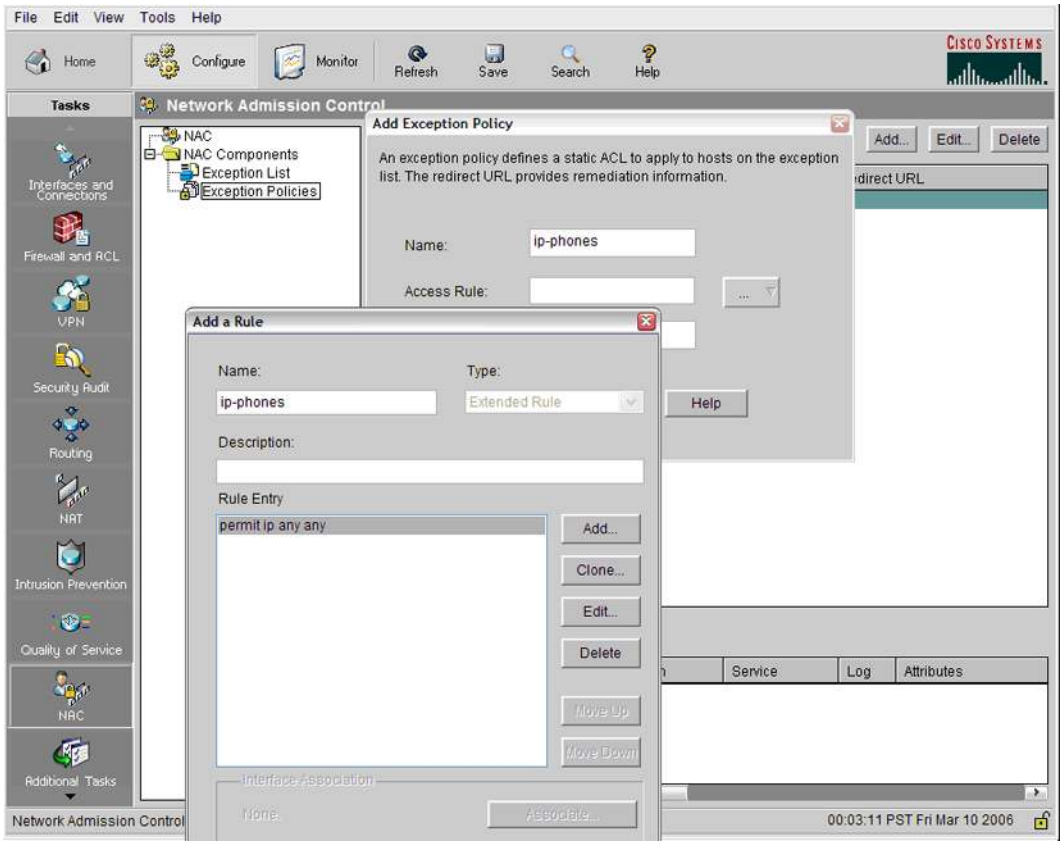


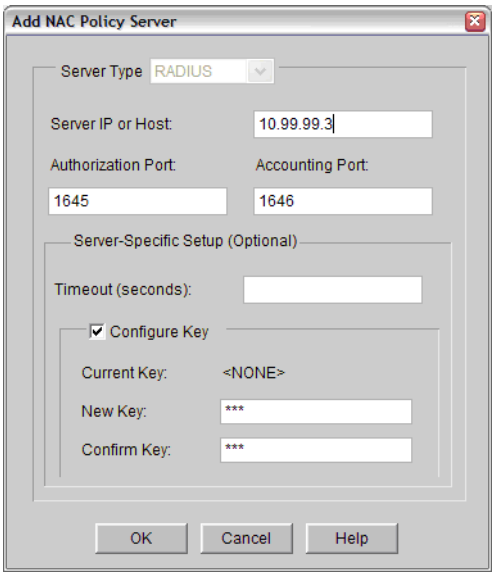
Figure 36. Add Exception for IP Phones



4. Next, create an exception list for IP phones. Just add on and select the policy you just created (Figure 36).
5. Return to the **NAC** menu and launch the **NAC** wizard on the top of the menu.
6. Select **BVI1** for the interface and **Strict Validation** for the default option.

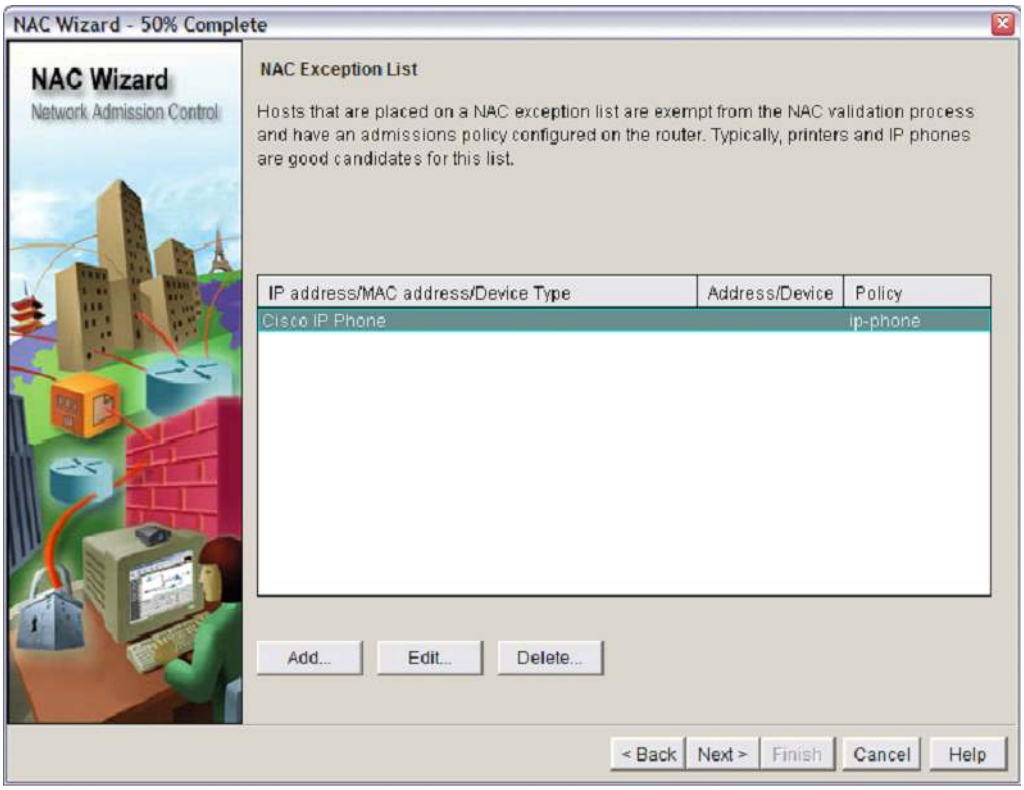
7. Next, add your NAC RADIUS server, which should be part of the management network (Figure 37), for example the 10.99.99.3 in this guide's example.

Figure 37. Add the NAC AAA Server



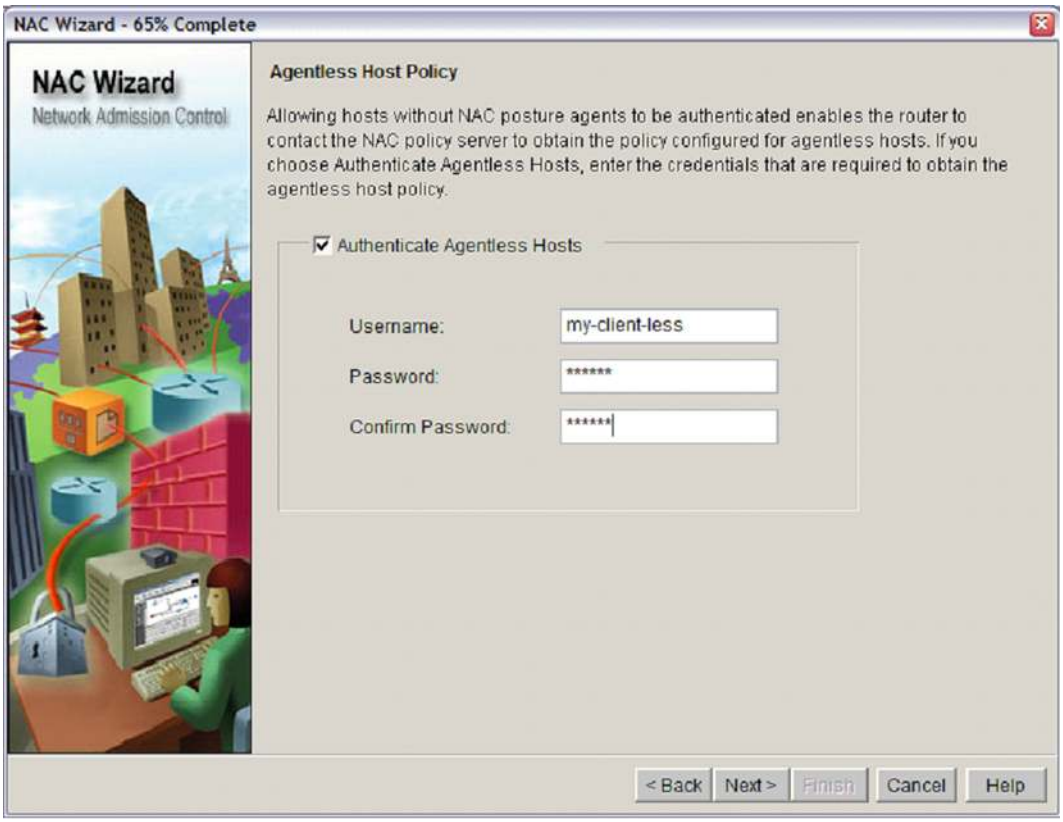
8. Select the **ip-phone** exception list you created before (Figure 38)

Figure 38. Attach the Correct Exception List



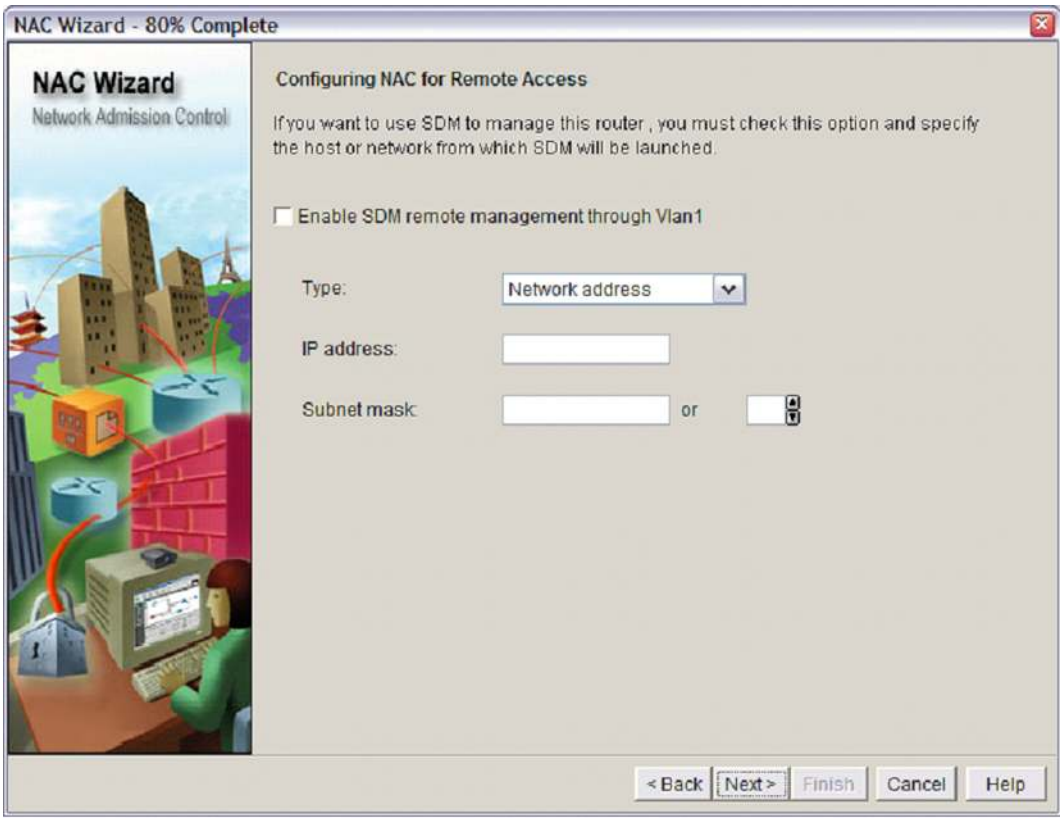
9. Next, you can optionally authenticate clientless hosts by entering a username/password for them (Figure 39). This is the case of Linux, or Apple hosts, for example.

Figure 39. Clientless NAC Hosts



10. Since we are applying NAC to the inside (LAN-facing) interface for the Cisco ECT deployment, there is no need to enable remote management. We will always be able to come through the management tunnel. Do not enable management (Figure 40).

Figure 40. Configure NAC for Remote Access



11. Click **Next** to push the configuration lines to the router.

Step 8—Additional Tasks

Besides the security aspects of the remote device, some more IP services need to be added to make the Cisco ECT spoke ready for use. These include:

- VTY/SSH setting for remote management

VTY Access

You will need to keep a privilege 15 user configured in the remote router for management (*privilege 15 means full access to the router's enable mode*). Removing the default **cisco/cisco** username and password is recommended; it is too obvious. The first step is to add a new user for administration. Select **Additional Tasks** on the left and then **Router Access—User Accounts/View**. The click **Add** to be able to create a new user (Figure 41).

Figure 41. Add New Username

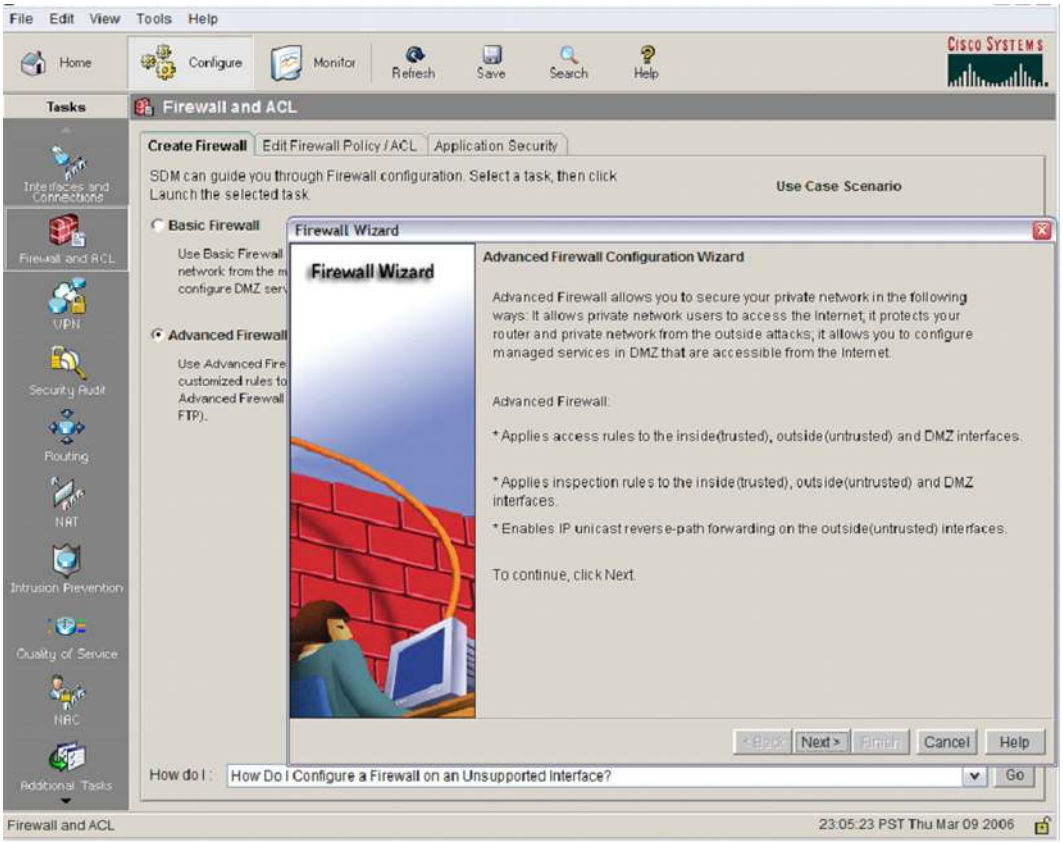
Still in the same menu option (**Router Access—User Accounts/View**) we can delete the default "cisco" user. First select the "cisco" user and then click on **Delete**. You can optionally add a management "back door" to the router, to be able to remotely SSH into the router. Make sure that you only allow incoming SSH sessions from a specific subnet; that should be part of your internal management network.

To add an optional management access to the router, click **Management Access** under the **Router Access** menu on the left and **Add**.

Step 9—Firewalls and ACLs

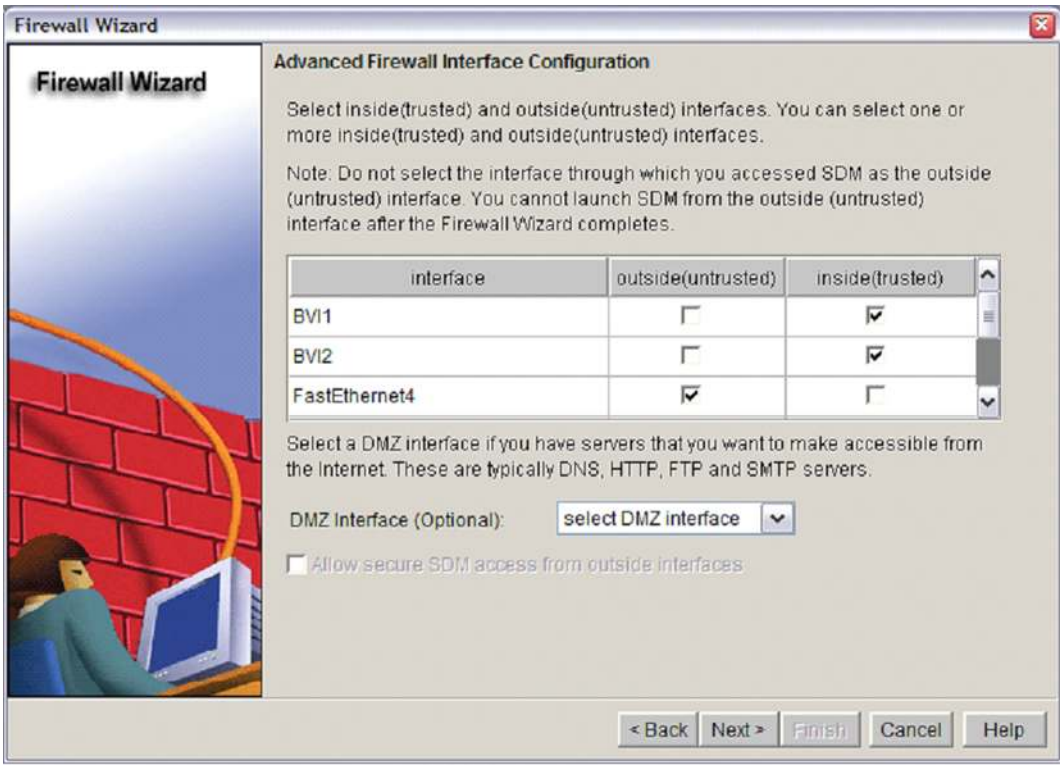
The “Firewall and ACL” task defines access policies and creates rules for deep inspection defined protocols. Start by selecting **Firewall and ACL** at left. Under the Create Firewall tab, select the **Advanced Firewall** radio button and click **Launch the selected task**. The Firewall Wizard will appear (Figure 42).

Figure 42. Start the Firewall Configuration



In the wizard there is no DMZ for an ECT spoke. The inside interfaces are the BVI1 (corporate VLAN) and BVI2 (guest VLAN) and the outside interface is FastEthernet4 (Figure 43).

Figure 43. Marking Interfaces for Firewall



In the next screen, the default “high security” can be kept (Figure 44).

Figure 44. Firewall Security Level

The other options, “medium” and “low”, provide less firewall features. The decision depends on the corporate policy rules. The “low security” option just applies the regular IOS Firewall. The other options will use Application Firewall to block access for peer-to-peer file haring applications and other applications.

Click **Finish** to push the configuration to the router.

The “low security” sample configuration is:

```
ip inspect log drop-pkt
ip inspect name SDM_LOW cuseeme
ip inspect name SDM_LOW dns
ip inspect name SDM_LOW ftp
ip inspect name SDM_LOW h323
ip inspect name SDM_LOW https
ip inspect name SDM_LOW icmp
ip inspect name SDM_LOW imap
ip inspect name SDM_LOW pop3
ip inspect name SDM_LOW netshow
ip inspect name SDM_LOW rcmd
ip inspect name SDM_LOW realaudio
ip inspect name SDM_LOW rtsp
ip inspect name SDM_LOW esmtp
ip inspect name SDM_LOW sqlnet
```

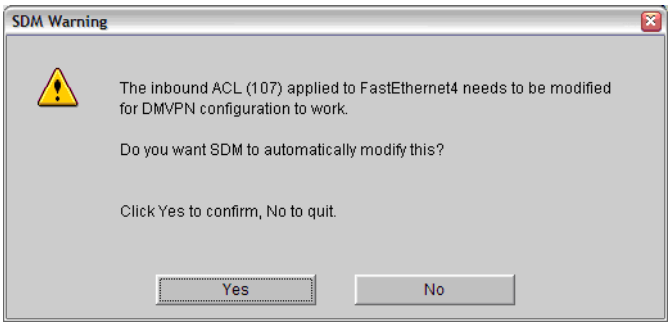


```
ip inspect name SDM_LOW streamworks
ip inspect name SDM_LOW tftp
ip inspect name SDM_LOW tcp
ip inspect name SDM_LOW udp
ip inspect name SDM_LOW vdolive
```

For the outside WAN interface, IPsec, ISAKMP, NTP, and BOOTPC traffic need to be allowed so that IKE/IPsec tunnels can be established, NTP is able to synchronize the clock, and the DHCP client is able to request an IP address from the ISP DHCP server.

Cisco SDM will automatically prompt you to accept auto-generated rules. Figure 45 shows an example. Make sure you accept them all.

Figure 45. Accept ACL Rules to Allow VPN-Related Traffic



Step 10—Extra Configuration Using Console Access

There are some configurations steps that are required for a Cisco ECT deployment that this version of Cisco SDM does not support. You can find information on how to configure them on http://www.cisco.com/go/ect under the "Layered and Perimeter Security Managed Services" section. Authentication proxy and 802.1x are missing, although all are optional.

Also, for the PKI trust point it is recommended to have "source interface <inside>"; BVI1 in the case of the Cisco 871 router. This will make sure that auto-enroll will use the tunnel-protected network to request a new certificate, and thus it will encrypt the traffic.

One more missing command is the static routing of hub IP addresses to the outside interface. Usually, DMVPN hubs will have public IP addresses that are part of the corporate set of subnet pools. These subnets will be routed out to spokes, once the GRE tunnel comes up. To avoid a routing loop, it is recommended that DMVPN hubs' host IP addresses are routed to the Internet.

For example, if DHCP is used to connect to the Internet and the DMVPN hubs would have IP addresses in the 172.16.1.0/29 network, we would need to set these, as well as the management server's host and network.

Here is a sample configuration:

```
! Management Gateway
ip route 172.16.0.0 255.255.255.255 dhcp
! DMVPN hubs
ip route 172.16.1.0 255.255.255.248 dhcp
! Management subnet
ip route 10.99.99.0 255.255.255.224 dhcp
!
```


After all the Cisco ECT-needed features have been configured, you must save the configuration to NVRAM by going to "File > Save to Startup Config…". Otherwise all will be lost when the router is power-cycled. You should also save a copy of the configuration in your PC for future reference. This can be achieved by clicking on "File > Save Running Config to PC…".

REFERENCES

Step 1. ECT solution guides and information: http://www.cisco.com/go/ect

Step 2. Deploying PKI with Cisco IOS® Software: http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps5207/products_feature_guide09186a00801d1cb0.html

APPENDIX A

Cisco 871 Spoke Router Example Running Cisco IOS Software Release 12.4(6)T

Please note the following hosts/networks for this example:

Spoke-protected subnet	10.20.1.0/28
Guest VLAN	10.1.1.0/24
Management VPN gateway	172.16.1.1
DMVPN primary	172.16.0.1 mGRE- 192.168.200.1
DMVPN secondary	172.16.0.2 mGRE- 192.168.200.2
871-Spoke-mGRE	192.168.200.10
Management "DMZ" network	10.99.99.0/24
PKI certificate server	10.99.99.5
AAA server	10.99.99.3

Cisco 871 Spoke Router Full Configuration Example

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname ect-spoke1
!
boot-start-marker
boot-end-marker
!
logging buffered 51200 warnings
!
aaa new-model
!
!
aaa group server radius rad_eap
!
aaa group server radius rad_mac
!
aaa group server radius rad_acct
!
```



```
aaa group server radius rad_admin
!
aaa group server tacacs+ tac_admin
!
aaa group server radius rad_pmip
!
aaa group server radius dummy
!
aaa group server radius rad_eap1
 server 10.99.99.3 auth-port 1645 acct-port 1646
!
aaa authentication login eap_methods group rad_eap
aaa authentication login mac_methods local
aaa authentication login eap_methods1 group rad_eap1
aaa authorization ipmobile default group rad_pmip
aaa accounting network acct_methods start-stop group rad_acct
!
aaa session-id common
!
resource policy
!
clock timezone pst -8
clock summer-time pdt recurring
ip cef
!
!
no ip dhcp use vrf connected
ip dhcp excluded-address 10.10.10.1
ip dhcp excluded-address 10.20.1.1
ip dhcp excluded-address 10.1.1.1
!
ip dhcp pool sdm-pool
   import all
   network 10.10.10.0 255.255.255.248
   default-router 10.10.10.1
   lease 0 2
!
ip dhcp pool sdm-pool1
   network 10.20.1.0 255.255.255.248
   domain-name cisco.com
   dns-server 172.16.226.120 171.70.168.183
   default-router 10.20.1.1
!
ip dhcp pool sdm-pool2
   network 10.1.1.0 255.255.255.0
   default-router 10.1.1.1
```



```
!
!
no ip domain lookup
ip domain name cisco.com
ip inspect name SDM_LOW cuseeme
ip inspect name SDM_LOW dns
ip inspect name SDM_LOW ftp
ip inspect name SDM_LOW h323
ip inspect name SDM_LOW https
ip inspect name SDM_LOW icmp
ip inspect name SDM_LOW imap
ip inspect name SDM_LOW pop3
ip inspect name SDM_LOW netshow
ip inspect name SDM_LOW rcmd
ip inspect name SDM_LOW realaudio
ip inspect name SDM_LOW rtsp
ip inspect name SDM_LOW esmtp
ip inspect name SDM_LOW sqlnet
ip inspect name SDM_LOW streamworks
ip inspect name SDM_LOW tftp
ip inspect name SDM_LOW tcp
ip inspect name SDM_LOW udp
ip inspect name SDM_LOW vdolive
ip admission name nac-test eapoudp inactivity-time 60
ip ips sdf location flash://attack-drop.sdf
ip ips notify SDEE
ip ips name sdm_ips_rule
!
!
crypto pki trustpoint TP-self-signed-3740638028
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-3740638028
 revocation-check none
 rsakeypair TP-self-signed-3740638028
!
crypto pki trustpoint cert-server1
 enrollment url http://10.99.99.5:80
 serial-number
 revocation-check none
 source interface BVI1
 auto-enroll
!
!
crypto pki certificate chain TP-self-signed-3740638028
crypto pki certificate chain cert-server1
 certificate 2ED4EAFF000000000C24
```



```
 certificate ca 7E68D38270C9E1B14A3251FAEE65D498
identity policy ip-phones
 access-group ip-phones
eou allow clientless
username ect-admin privilege 15 secret 5 $1$Wgrl$aw6HshmzbkBTTheWw/Wvb0
!
!
class-map match-any SDMVoice-FastEthernet4
 match protocol rtp audio
class-map match-any SDMTrans-FastEthernet4
 match protocol citrix
 match protocol finger
 match protocol notes
 match protocol novadigm
 match protocol pcanywhere
 match protocol secure-telnet
 match protocol sqlnet
 match protocol sqlserver
 match protocol ssh
 match protocol telnet
 match protocol xwindows
class-map match-any SDMScave-FastEthernet4
 match protocol napster
 match protocol fasttrack
 match protocol gnutella
class-map match-any SDMIVideo-FastEthernet4
 match protocol rtp video
class-map match-any SDMSVideo-FastEthernet4
 match protocol cuseeme
 match protocol netshow
 match protocol rtsp
 match protocol streamwork
 match protocol vdolive
class-map match-any SDMBulk-FastEthernet4
 match protocol exchange
 match protocol ftp
 match protocol irc
 match protocol nntp
 match protocol pop3
 match protocol printer
 match protocol secure-ftp
 match protocol secure-irc
 match protocol secure-nntp
 match protocol secure-pop3
 match protocol smtp
 match protocol tftp
```



```
class-map match-any SDMSignal-FastEthernet4
 match protocol h323
 match protocol rtcp
class-map match-any SDMRout-FastEthernet4
 match protocol bgp
 match protocol eigrp
 match protocol ospf
 match protocol rip
 match protocol rsvp
class-map match-any SDMManage-FastEthernet4
 match protocol dhcp
 match protocol dns
 match protocol imap
 match protocol kerberos
 match protocol ldap
 match protocol secure-imap
 match protocol secure-ldap
 match protocol snmp
 match protocol socks
 match protocol syslog
!
!
policy-map SDM-Pol-FastEthernet4
 class SDMTrans-FastEthernet4
  bandwidth remaining percent 33
  set dscp af21
 class SDMSignal-FastEthernet4
  bandwidth remaining percent 40
  set dscp cs3
 class SDMRout-FastEthernet4
  bandwidth remaining percent 3
  set dscp cs6
 class SDMVoice-FastEthernet4
  priority percent 70
  set dscp ef
 class SDMManage-FastEthernet4
  bandwidth remaining percent 3
  set dscp cs2
!
!
!
crypto isakmp policy 1
 encr 3des
!
!
crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
```



```
crypto ipsec transform-set transport esp-3des esp-sha-hmac
 mode transport
!
crypto ipsec profile SDM_Profile1
 set transform-set transport
!
!
crypto map SDM_CMAP_1 1 ipsec-isakmp
 description Tunnel to172.16.1.1
 set peer 172.16.1.1
 set transform-set ESP-3DES-SHA
 match address 102
 qos pre-classify
!
bridge irb
!
!
!
interface Tunnel0
 bandwidth 1000
 ip address 192.168.200.10 255.255.252.0
 no ip redirects
 ip mtu 1400
 ip nhrp authentication DMVPN_NW
 ip nhrp map 192.168.200.1 172.16.0.1
 ip nhrp map multicast 172.16.0.1
 ip nhrp map multicast 172.16.0.2
 ip nhrp map 192.168.200.2 172.16.0.2
 ip nhrp network-id 100000
 ip nhrp holdtime 360
 ip nhrp nhs 192.168.200.1
 ip nhrp nhs 192.168.200.2
 ip nhrp registration no-unique
 ip virtual-reassembly
 ip tcp adjust-mss 1360
 delay 1000
 tunnel source FastEthernet4
 tunnel mode gre multipoint
 tunnel key 100000
 tunnel protection ipsec profile SDM_Profile1
!
interface FastEthernet0
 switchport access vlan 10
!
interface FastEthernet1
 switchport access vlan 10
```



```
!
interface FastEthernet2
 switchport access vlan 10
!
interface FastEthernet3
 switchport access vlan 20
!
interface FastEthernet4
 description $FW_OUTSIDE$
 no ip dhcp client request tftp-server-address
 ip address dhcp client-id FastEthernet4
 ip access-group 101 in
 ip nbar protocol-discovery
 ip nat outside
 ip inspect SDM_LOW out
 ip ips sdm_ips_rule in
 ip virtual-reassembly
 duplex auto
 speed auto
 crypto map SDM_CMAP_1
 service-policy output SDM-Pol-FastEthernet4
!
interface Dot11Radio0
 no ip address
 !
 broadcast-key change 30
 !
 !
 encryption mode ciphers tkip wep128
 !
 ssid corporate-access
    vlan 10
    authentication open eap eap_methods1
 !
 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 Dot11Radio0.10
 encapsulation dot1Q 10
 no snmp trap link-status
 no cdp enable
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 spanning-disabled
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
```



```
 no bridge-group 1 unicast-flooding
!
interface Vlan1
 description $ETH-SW-LAUNCH$$INTF-INFO-HWIC 4ESW$
 no ip dhcp client request tftp-server-address
 ip address 10.10.10.1 255.255.255.248
 ip virtual-reassembly
!
interface Vlan10
 no ip address
 bridge-group 1
!
interface Vlan20
 no ip address
 bridge-group 2
!
interface BVI1
 description $FW_INSIDE$
 ip address 10.20.1.1 255.255.255.240
 ip access-group 100 in
 ip nat inside
 ip admission nac-test
 ip virtual-reassembly
!
interface BVI2
 ip address 10.1.1.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
!
router eigrp 33
 network 192.168.200.0 0.0.3.255
 network 10.20.1.0 0.0.0.15
 no auto-summary
!
ip route 172.16.0.0 255.255.255.248 dhcp
ip route 172.16.1.0 255.255.255.248 dhcp
ip route 10.99.99.0 255.255.255.224 dhcp
!
!
ip http server
ip http authentication local
ip http secure-server
ip http timeout-policy idle 600 life 86400 requests 10000
ip nat inside source route-map SDM_RMAP_1 interface FastEthernet4 overload
!
ip access-list extended ip-phones
```



```
 remark permit any
 remark SDM_ACL Category=64
 permit ip any any
!
access-list 100 remark auto generated by SDM firewall configuration
access-list 100 remark SDM_ACL Category=1
access-list 100 deny   ip host 255.255.255.255 any
access-list 100 deny   ip 127.0.0.0 0.255.255.255 any
access-list 100 permit ip any any
access-list 101 remark auto generated by SDM firewall configuration
access-list 101 remark SDM_ACL Category=1
access-list 101 permit tcp host 10.99.99.5 eq www any gt 1024
access-list 101 permit udp any any eq non500-isakmp
access-list 101 permit udp any any eq isakmp
access-list 101 permit esp any any
access-list 101 permit ahp any any
access-list 101 permit gre any any
access-list 101 remark Auto generated by SDM for NTP (123) 192.5.41.40
access-list 101 permit udp host 192.5.41.40 eq ntp any eq ntp
access-list 101 permit ahp host 171.16.1.1 any
access-list 101 permit esp host 171.16.1.1 any
access-list 101 permit udp host 171.16.1.1 any eq isakmp
access-list 101 permit udp host 171.16.1.1 any eq non500-isakmp
access-list 101 remark IPSec Rule
access-list 101 permit ip 10.99.99.0 0.0.0.31 host 10.20.1.1
access-list 101 deny   ip 10.1.1.0 0.0.0.255 any
access-list 101 deny   ip 10.20.1.0 0.0.0.15 any
access-list 101 permit udp any eq bootps any eq bootpc
access-list 101 permit icmp any any echo-reply
access-list 101 permit icmp any any time-exceeded
access-list 101 permit icmp any any unreachable
access-list 101 deny   ip 10.0.0.0 0.255.255.255 any
access-list 101 deny   ip 172.16.0.0 0.15.255.255 any
access-list 101 deny   ip 192.168.0.0 0.0.255.255 any
access-list 101 deny   ip 127.0.0.0 0.255.255.255 any
access-list 101 deny   ip host 255.255.255.255 any
access-list 101 deny   ip any any log
access-list 102 remark SDM_ACL Category=4
access-list 102 remark IPSec Rule
access-list 102 permit ip host 10.20.1.1 10.99.99.0 0.0.0.31
access-list 103 remark SDM_ACL Category=2
access-list 103 remark IPSec Rule
access-list 103 deny   ip host 10.20.1.1 10.99.99.0 0.0.0.31
access-list 103 permit ip 10.1.1.0 0.0.0.255 any
access-list 103 permit ip 10.20.1.0 0.0.0.7 any
no cdp run
```



```
!
!
!
route-map SDM_RMAP_1 permit 1
 match ip address 103
!
radius-server attribute 32 include-in-access-req format %h
radius-server host 10.99.99.3 auth-port 1645 acct-port 1646 key stealth
radius-server vsa send accounting
!
control-plane
!
bridge 1 protocol ieee
bridge 1 route ip
bridge 2 protocol ieee
bridge 2 route ip
banner login ^C
------------------------------------------------------------------------
Cisco Router and Security Device Manager (SDM) is installed on this device. This feature
requires the one-time use of the username "cisco"
with the password "cisco".


Please change these publicly known initial credentials using Cisco SDM or the Cisco IOS
CLI. Here are the Cisco IOS commands.


username <myuser>  privilege 15 secret 0 <mypassword>
no username cisco


Replace <myuser> and <mypassword> with the username and password you want to use.


For more information about Cisco SDM please follow the instructions in the QUICK START
GUIDE for your router or go to http://www.cisco.com/go/sdm
------------------------------------------------------------------------
^C
!
line con 0
 no modem enable
line aux 0
line vty 0 4
 privilege level 15
 transport input telnet ssh
 transport output telnet ssh
line vty 5 15
 privilege level 15
 transport input telnet ssh
!
scheduler max-task-time 5000
```



```
ntp clock-period 17175050
ntp server 192.5.41.40 source BVI1
!
webvpn context Default_context
 ssl authenticate verify all
 !
 no inservice
!
end
```

Cisco 871 Router Factory Default Configuration Example

```
!  This is the default startup configuration file for Cisco Router and Security
!  Device Manager (SDM)
!  DO NOT modify this file; it is required by Cisco SDM as is for factory
!  defaults Version 1.0
!
hostname yourname
!
logging buffered 51200 warnings
!
username cisco privilege 15 secret 0 cisco
!
ip dhcp excluded-address 10.10.10.1
!
ip dhcp pool sdm-pool
   import all
   network 10.10.10.0 255.255.255.248
   default-router 10.10.10.1
   lease 0 2
!
no ip domain lookup
ip domain-name yourdomain.com
!
interface FastEthernet0
 no ip address
 no shutdown
!
interface FastEthernet1
 no ip address
 no shutdown
!
interface FastEthernet2
 no ip address
 no shutdown
!
interface FastEthernet3
```



```
 no ip address
 no shutdown
!
!
interface Vlan1
 description $ETH-SW-LAUNCH$$INTF-INFO-HWIC 4ESW$
 ip address 10.10.10.1 255.255.255.248
 ip tcp adjust-mss 1452
!
ip http server
ip http secure-server
ip http authentication local
ip http timeout-policy idle 600 life 86400 requests 10000
!
banner login ^
----------------------------------------------------------------------
Cisco Router and Security Device Manager (SDM) is installed on this device. This feature
requires the one-time use of the username "cisco"
with the password "cisco".


Please change these publicly known initial credentials using Cisco SDM or the Cisco IOS
CLI. Here are the Cisco IOS commands.


username <myuser>  privilege 15 secret 0 <mypassword>
no username cisco


Replace <myuser> and <mypassword> with the username and password you want to use.


For more information about Cisco SDM, please follow the instructions in the QUICK START
GUIDE for your router or go to http://www.cisco.com/go/sdm
----------------------------------------------------------------------
^
!
no cdp run
!
!
line con 0
 login local
line vty 0 4
 privilege level 15
 login local
 transport input telnet
 transport input telnet ssh
line vty 5 15
 privilege level 15
 login local
 transport input telnet
```



```
 transport input telnet ssh
!
!  End of Cisco SDM default config file
End
```


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.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 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.com Website at www.cisco.com/go/offices.

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus • 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 USA C07-359528-00 07/06