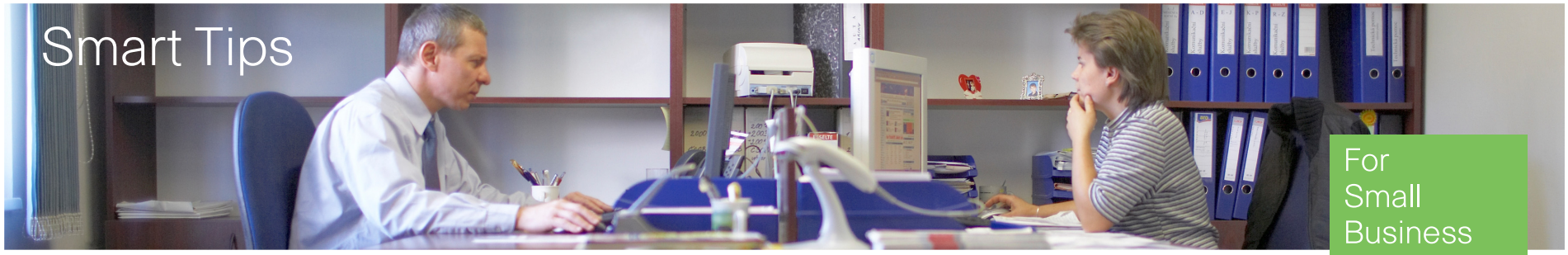


Configuring Site-to-Site VPN

Overview

VPN security solutions are becoming more important for small business companies. A VPN is a private communications network often used within a company to communicate securely over a public network infrastructure (the Internet) between geographically separate office locations. VPNs increase security for a distributed organization, making it easier for staff to work from different sites without compromising the network.

Two virtual private network (VPN) technologies are currently popular: site-to-site VPNs and remote access VPNs. This smart tip covers site-to-site VPN, which provides an Internet-based WAN infrastructure to extend network resources to remote offices, home offices, and business partner sites. All traffic between sites is encrypted using the IP Security (IPsec) protocol, and network features such as routing, quality of service (QoS), and multicast support are integrated.

Cisco small business routers deliver robust and easily managed VPN solutions to cost-conscious small business companies. This Smart Tip describes how a cost-effective VPN solution can be implemented to secure business operations and communications between sites. It describes the design tips for building a site-to-site IPsec VPN and provides configuration examples.

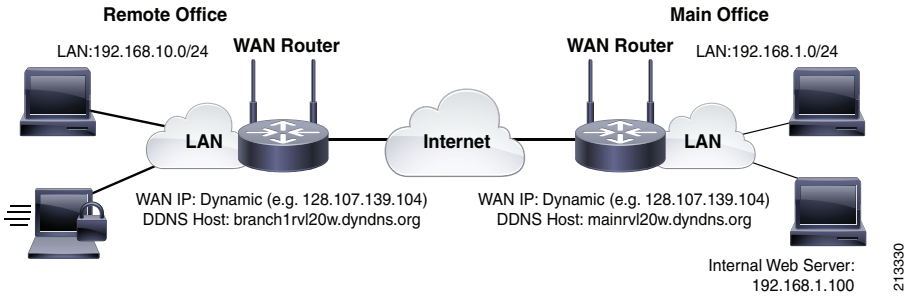
Featured Products

- Cisco RV120W Wireless-N VPN Firewall Router (GUI configuration screens of this router are shown in this document as an example)
- Cisco RV 220W Wireless-N Network Security Firewall
- Cisco RV042, RV042G, RV082, RV016, RVL200, WRVS4400N, and WRV210 small business routers
- Cisco RV180/180W Wireless-N Multifunction VPN Firewall

Network Diagram

Figure 1 illustrates a sample implementation of a site-to-site VPN tunnel using a Cisco small business router.

Figure 1 Site-to-Site VPN Topology



The WAN routers at the main office and remote office receive their IP addresses dynamically and have both firewalling and NAT enabled by default. The WAN routers can be accessed by their Dynamic DNS (DDNS) name (*mainrv120w.dyndns.org* and *branch1rv120w.dyndns.org*). A site-to-site VPN tunnel is configured and established between the two WAN routers.

With this configuration, a host with the IP address 192.168.1.x/24 in the main office LAN and a host with IP address 192.168.10.x/24 in the remote office LAN can communicate with each other securely.

Key Features

Internet Key Exchange (IKE)

Internet Key Exchange (IKE) is the protocol used to set up a security association (SA) in the IPsec protocol suite. IKE builds on the Oakley protocol and Internet Security Association and Key Management Protocol (ISAKMP), and uses a Diffie–Hellman key exchange to set up a shared session secret, from which cryptographic keys are derived.

IP Security Protocol (IPsec)

IPsec is a protocol suite for securing IP communications by authenticating and encrypting each IP packet of a data stream. IPsec also includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session. IPsec can be used to protect data flows between a pair of hosts, gateways, or networks.

Design Tips

- VPN topology—With a site-to-site VPN, a secured IPsec tunnel is configured between every site and every other site. A multi-site topology is usually implemented as a full mesh of site-to-site VPN tunnels (that is, every site has established tunnels to every other site). If no communication is needed between remote offices, a hub-spoke VPN topology is used to reduce the number of VPN tunnels (that is, each site establishes a VPN tunnel only to the main office).
- WAN IP addressing and DDNS—The VPN tunnel needs to be established between two public IP addresses. If the WAN routers receive static IP addresses from the Internet Service Provider (ISP), the VPN tunnel can be implemented directly using static public IP addresses. However, most small businesses use cost-effective broadband Internet services such as DSL or cable modem, and receive dynamic IP addresses from their ISPs. In such cases, DDNS can be used to map the dynamic IP address to a fully qualified domain name (FQDN). In this Smart Tip, the WAN IP address is registered with *dyndns.org*, and the WAN routers automatically update the DDNS entries with their current WAN IP address.
- LAN IP addressing—The private LAN IP network address of each site should have no overlaps. The default LAN IP network address at each remote site should always be changed.
- VPN authentication—The IKE protocol is used to authenticate VPN peers when establishing a VPN tunnel. Various IKE authentication methods exist, and pre-shared key is the most convenient method. Cisco recommends applying a strong pre-shared key.
- VPN encryption—To ensure confidentiality of data transported over the VPN, encryption algorithms are used to encrypt the payload of IP packets. DES, 3DES, and AES are three common encryption standards. AES is considered the most secure when compared to DES and 3DES. Cisco highly recommends applying AES-128 bits or higher encryption (for example, AES-192 and AES-256). However, the stronger the encryption algorithm is, the more processing resource the router requires.
- VPN policy parameters—Table 1 shows the recommended VPN parameters, which include parameters for both IKE policy and IPsec policy. It is best to select the same VPN policy parameters for all tunnels, and to use a different pre-shared key on each pair of routers.

Table 1 Summary of Recommended VPN Parameters

Function	IKE Parameters	IPsec Parameters
Encryption algorithm	AES with 128-bit or higher	AES with 128-bit or higher
Hash algorithm	SHA-1	SHA-1
Authentication method	Pre-shared keys (strong)	N/A
Diffie-Hellman (DH) group	DH group 2 (1024 bit) or higher	DH group 2 (for PFS key group)
SA lifetime	8 hours (28800 seconds)	1 hour (3600 seconds)

Configuration Tips

Preconfiguration Checklist

1. Connect the Ethernet cable between the WAN port on the Cisco RV router and the Ethernet port on the DSL or cable modem.
2. Turn on the Cisco RV router and then connect internal PCs, servers, and other IP devices to the LAN switch or the switch ports on the RV router.
3. Make sure the LAN IP network addresses are configured at each site and are in different subnets. In this example, the main office LAN is using 192.168.1.0/24, and the remote site LAN is using 192.168.10.0/24.
4. Make sure local PCs and servers are able to communicate with each other and with the router.
5. Set up an internal web server with an IP address of 192.168.1.100 at the main office site.

Configuring WAN and DDNS Settings

The default WAN setting of the RV router is set to get its IP address dynamically from the ISP. Firewalling and NAT are also enabled by default. Go to **Status > System Summary**, and in the WAN information (IPv4) section, verify that the router receives its IP address, subnet mask, gateway, and DNS information from the ISP; and that NAT is enabled.

Go to **Networking > Dynamic DNS** to configure the DDNS entries on each WAN router. For detailed steps, see the Cisco Smart Tips "Enabling WAN Public Access with DDNS and Port Forwarding" at the following URL: http://tools.cisco.com/s2slv2/ViewDocument?docName=EXT-AS-339923.

In this example, we create the DDNS entry *mainrv120w.dyndns.org* for the WAN router at the main office, and the DDNS entry *branch1rv120w.dyndns.org* for the WAN router at the remote office.

Configuring the VPN Tunnel on the WAN Router at the Main Office Site

In this section, you configure the endpoint on the main office WAN router side of a site-to-site VPN tunnel.

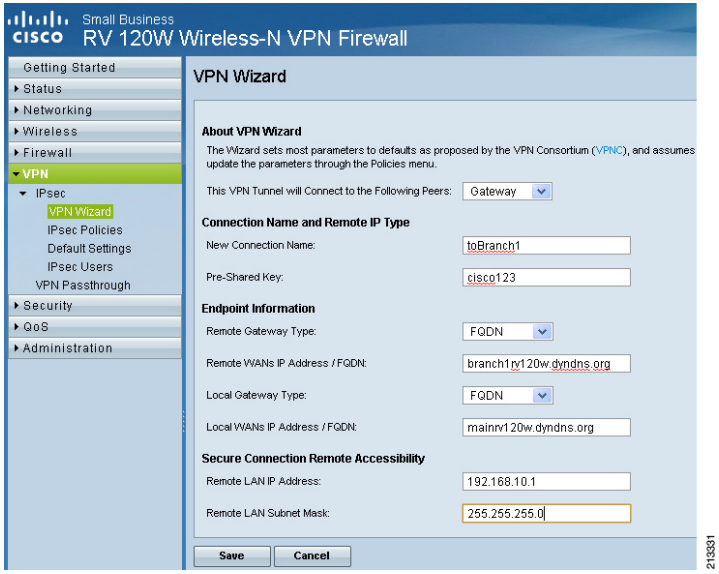
Step 1 Go to **VPN > IPsec > VPN Wizard** (See Figure 2.)

1. Select *Gateway* as the VPN type.
2. Enter a VPN connection name, such as *toBranch1*.
3. Input the pre-shared key. This key needs to match on both ends of the VPN tunnel.
4. Select *FQDN* for Remote Gateway Type and enter *brach1rv120w.dyndns.org* for the remote WAN's IP address/FQDN. This is the DDNS name of the WAN router at the remote office site.
5. Select *FQDN* for Local Gateway Type and enter *mainrv120w.dyndns.org* for local WANs IP address/FQDN. This is the DDNS name of the WAN router at the main office site. The local WAN's IP address/FQDN information is usually automatically filled by the system.

Note If the WAN router uses a static WAN IP address, select *IP address* for Gateway Type and enter the IP address in the WAN's IP Address/FQDN fields.

6. Input the remote LAN IP address and its subnet mask; for example, *192.168.10.1* and *255.255.255.0*.
7. Click **Save** to complete the wizard.

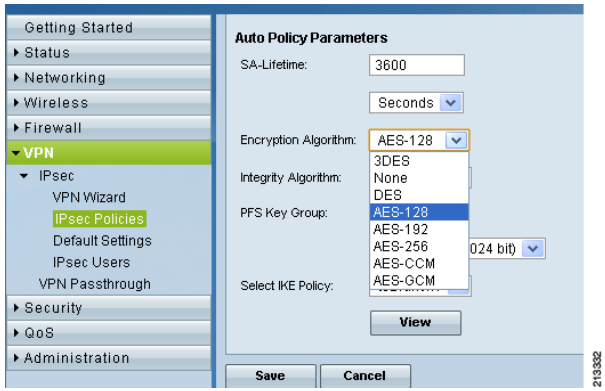
Figure 2 VPN Wizard



Step 2 Go to **VPN > IPsec > IPsec Policies**, select the policy named *toBranch1* in the **VPN Policies Table**, and click **Disable**.

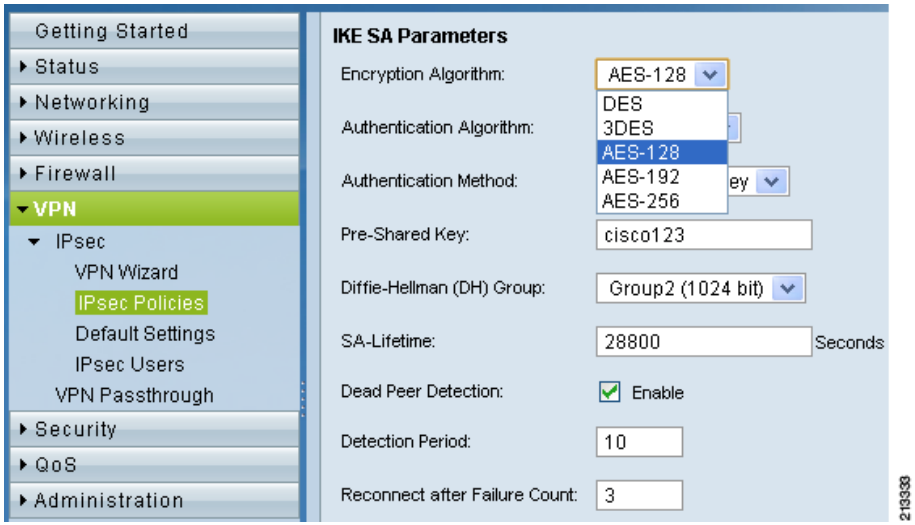
Step 3 Go to **VPN > IPsec > IPsec Policies**, select the policy named *toBranch1* in the **VPN Policies Table**, click **Edit**, go to the Auto Policy Parameters section to change the Encryption Algorithm from *3DES* to *AES-128*, and click **Save**. (See Figure 3.)

Figure 3 VPN Policy Parameters



Step 4 Select the policy named *toBranch1* in the **IKE Policies Table,** click **Edit,** go to the IKE SA Parameters section to change the Encryption Algorithm from *3DES* to *AES-128*, enable Dead Peer Detection, and click **Save**. (See Figure 4.)

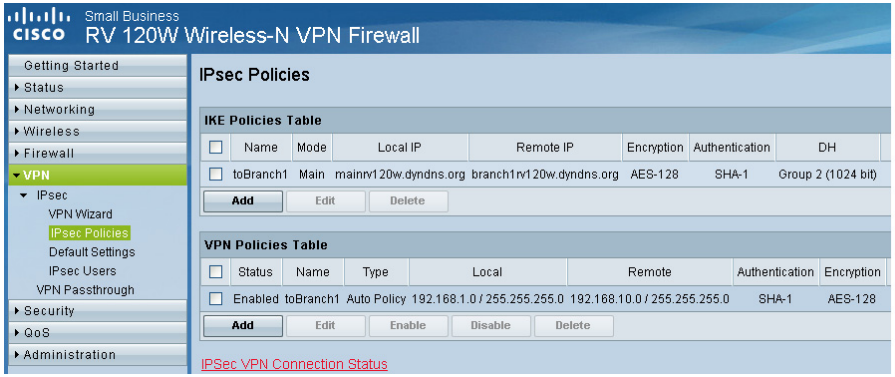
Figure 4 IKE Policy Parameters



Step 5 Go to **VPN > IPsec > IPsec Policies**, select the policy named *toBranch1* in the **VPN Policies Table**, and click **Enable**.

Step 6 To validate the VPN configuration, go to **VPN > IPsec > IPsec Policies**, and make sure the policy table displays following the IKE and VPN tables. (See Figure 5.)

Figure 5 Validating the VPN Configuration

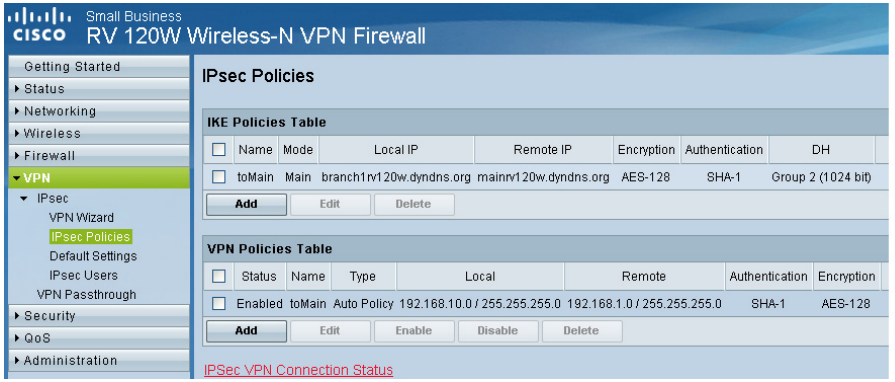


Configuring the VPN Tunnel on the WAN Router at the Remote Office Site

Follow the same steps in the preceding section to configure the other endpoint of the site-to-site VPN tunnel on the remote WAN router. In this example, make sure to use *branch1rv120w.dyndns.org* as the local gateway name, *mainrv120w.dyndns.org* as the remote gateway name, *192.168.1.0/24* as the remote LAN IP address, and use the same pre-shared key. Follow the same steps to create more VPN tunnels if there is more than one remote site.

After completing the configuration of the VPN wizard and changing the encryption from 3DES to AES-128, the final VPN policy table should appear as shown in Figure 6.

Figure 6 Final VPN Policy Table



Validating the VPN Tunnel

Step 1 From a client PC or laptop connected to the local LAN in the remote office site, ping the IP address of a PC in the main office; or browse to the internal web server such as 192.168.1.100. Perform the same validation from the PC in the main office site.

The ping should be successful and the web browser should display the contents of the internal web site.

Step 2 Go to **VPN > IPsec > IPsec Policies** and click the **IPsec VPN Connection Status link** on both WAN routers. (See Figure 7 for the main office router and Figure 8 for the remote office router.)

Figure 7 Verifying VPN Status on Main Office WAN Router

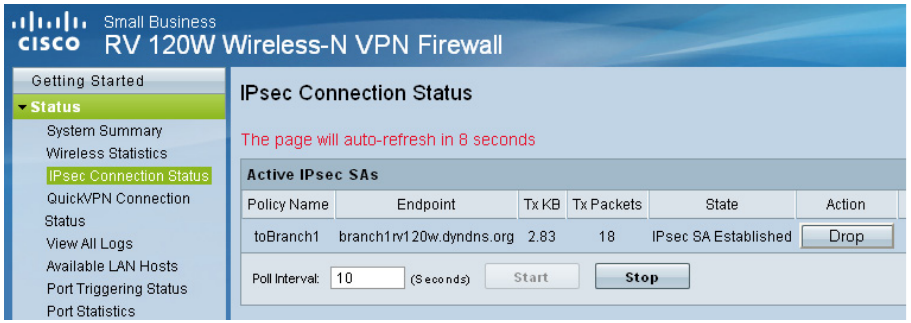
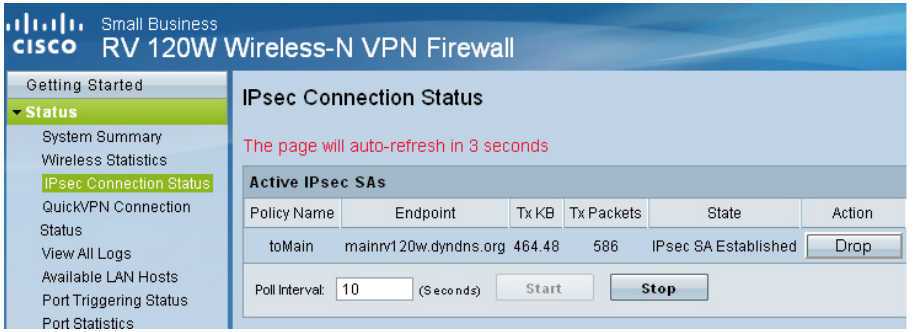


Figure 8 Verifying VPN Status on Remote Office WAN Router



The state for each IPsec tunnel should show *IPsec SA Established*.

Note You can also go to **Status > IPsec Connection Status** to view the same information. The **Drop** button in the action column can be used to terminate the established VPN tunnel, and the Connect button can be used to manually establish the tunnel.