Connecting Remote Offices by Setting Up VPN Tunnels

Cisco RV0xx Series Routers

Overview

As your business expands to additional sites, you need to ensure that all employees have access to the network resources that they need to be productive. Yet you also want to ensure that your network is protected from outside threats. You can connect your sites and ensure security by creating a site-to-site Virtual Private Network (VPN), also called a gateway-to-gateway VPN.

A VPN creates a secure tunnel between two sites via the Internet. For example, users at your branch offices can access file servers at the main office. All data is encapsulated so that your confidential information is protected as your users send and receive data.

This application note explains how to set up a VPN between two RV0xx Series routers. You can then repeat the procedures to add tunnels to your other sites. A Cisco RV0xx Series router supports up to 100 VPN tunnels.

NOTE Even if you have an RV0xx Series router on one end of the tunnel, and a different model on the other end, you can use this information to set up your RV0xx Series router. Note the shared settings that you need to configure on your other router. Both devices must use a common key or certificate and must have the same security policies set up.

Contents

Topology Options

Before you configure the VPN settings on your routers, consider the topology options. A VPN topology specifies the peers and the networks that are part of the VPN and how they connect to one another. Depending on the number of sites and the nature of traffic, you can choose a hub-and-spoke topology or a mesh topology.

VPN Hub and Spoke Topology

In a VPN hub-and-spoke topology, multiple VPN routers (spokes) communicate securely with a central VPN router (hub). A separate, secured tunnel extends between each individual spoke and the hub.

In the following example, two branch offices (spokes) have site-to-site VPN tunnels to the main office (hub). The traffic typically is between a remote site and the main office. Inter-site traffic must pass through the hub first and then out to a spoke.

Figure 1   Hub and Spoke

284286
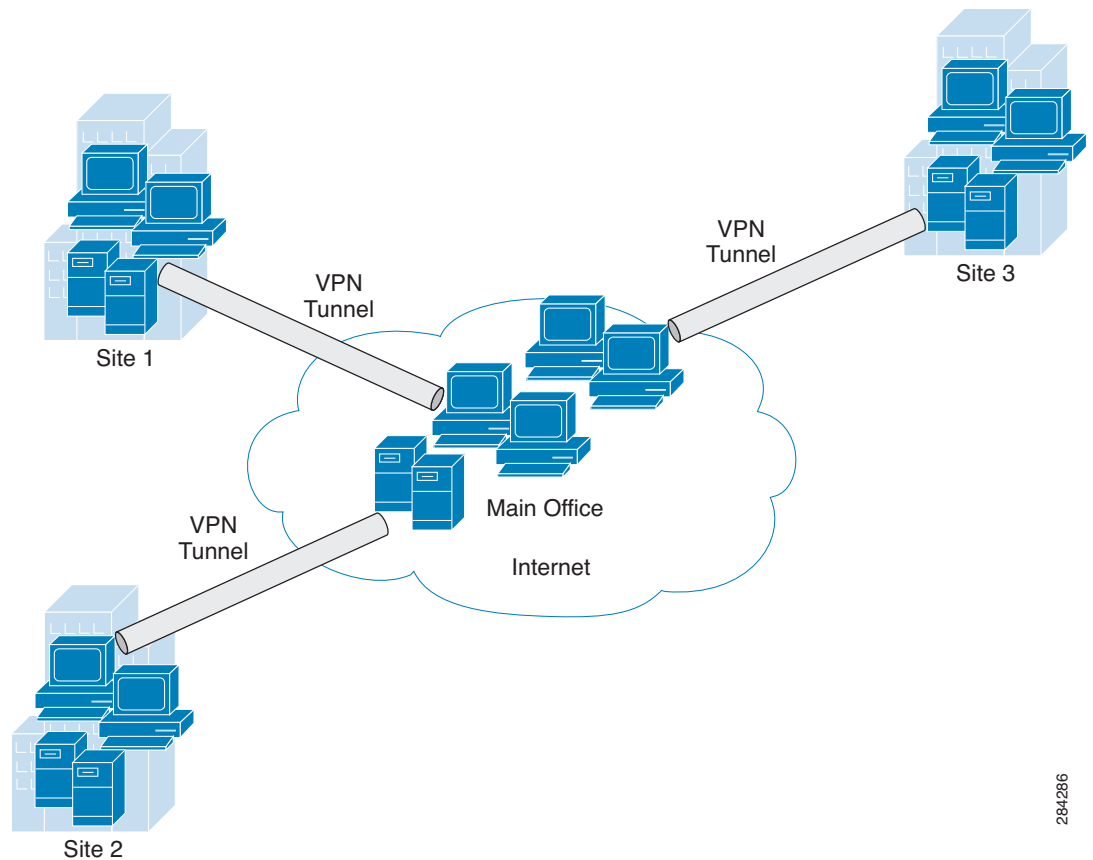
This topology is a simple way to allow all branch employees to access the main network. It works well if most traffic is from the remote sites to the main network and there is little traffic among the sites. Too much inter-site traffic may create bottlenecks at the hub.

VPN Mesh Topology

In a VPN mesh topology, each VPN router can communicate securely with all other VPN routers. Multiple secured tunnels extend from each site to all other sites.

In the following example, four sites are connected in a VPN mesh topology. Three VPN tunnels extend from each site, providing secure communications with all other sites. Data can travel directly between any two sites.

Figure 2   Mesh
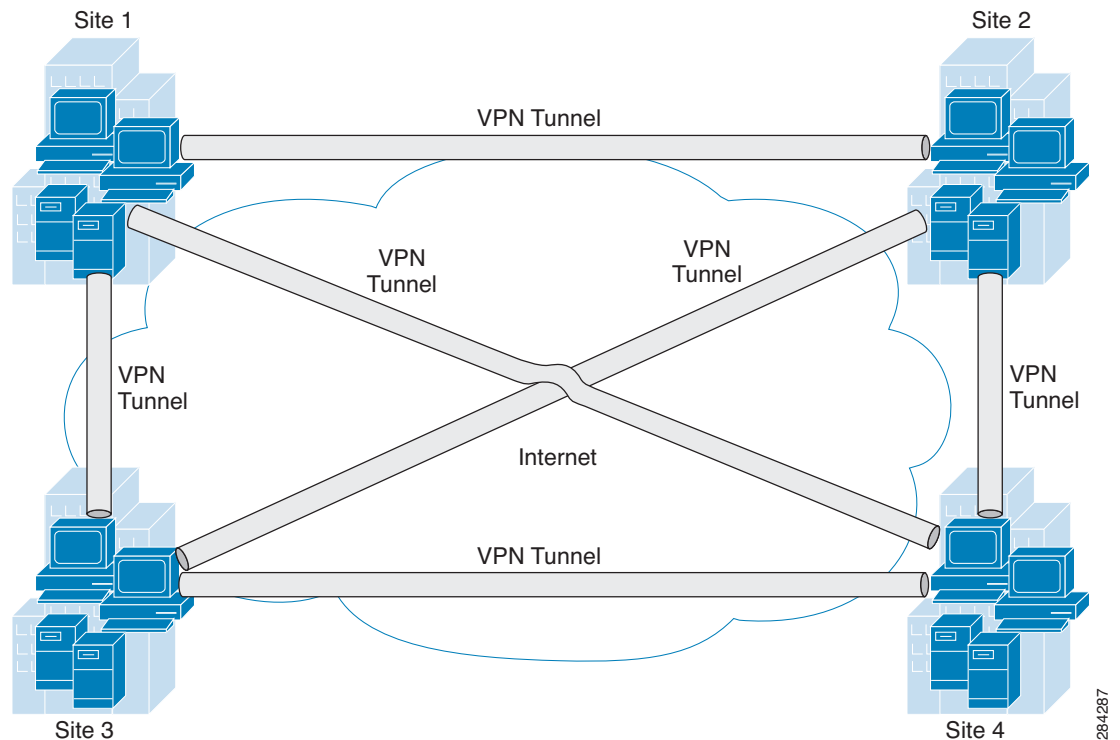
This topology requires much more configuration on each router. However, it works well in a complicated network with data traveling between multiple sites. Because all devices have direct peer relationships with one another, this design prevents the bottlenecks that can occur with a hub-and-spoke topology. This design also ensures that if one site is down, the other sites can continue to exchange data.

NOTE   When the number of nodes in a full mesh topology increases, scalability may become an issue—the limiting factor being the number of tunnels that the devices can support at a reasonable CPU utilization.

Other Design Considerations

Before you configure your VPN tunnels, consider the following points about your network setup.

WAN Setup

The WAN setup pertains to the network that your router connects to outside your office. The first consideration is the type of IP addresses that you received for your Internet service at your two sites. As when constructing a physical tunnel or bridge, you need to know where the VPN tunnel is going.

- **If at least one site has a static IP address:** A VPN tunnel easily can be established if at least one of the sites has a static IP address for the WAN connection. A static IP address is a publicly routable Internet address that does not change. In this scenario, establishing a VPN tunnel can be compared to building a bridge between two docks (two sites with static IP addresses), or even setting a gangplank between a dock and an unanchored boat (one site with a static IP address and one with a dynamic IP address).

**Figure 3   Gateway To Gateway Tunnel with Static IP Addresses**
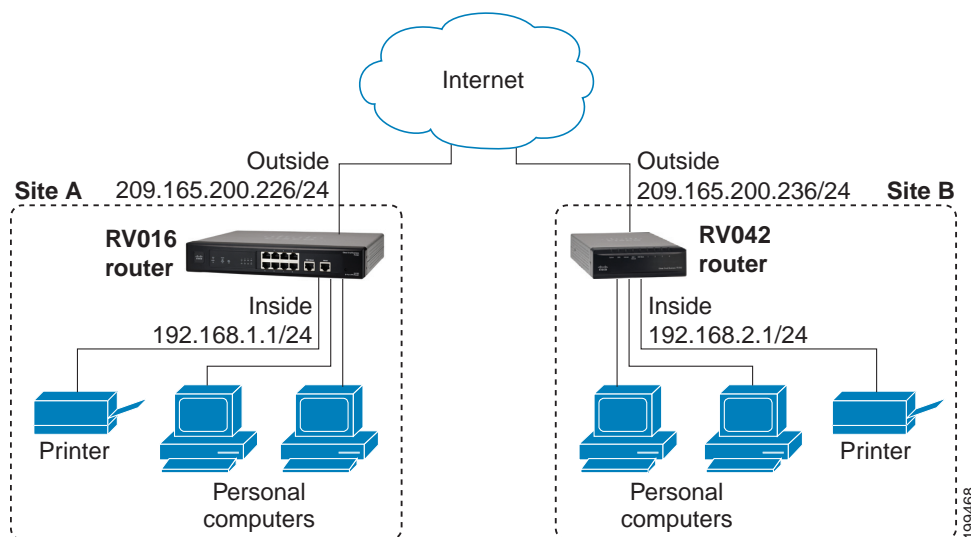
- **If both sites have dynamic IP addresses:** A dynamic IP address is a publicly routable IP address that is issued for your use when you connect to your service provider's network. Dynamic IP addresses may change without warning. In this scenario, establishing a VPN tunnel is like trying to build a bridge between two unanchored boats. However, you can "anchor"

one boat, so to speak, by obtaining a Fully Qualified Domain Name (FQDN) and registering at least one site with a Dynamic DNS service. This service associate tracks your dynamic IP address to ensure that your router is reachable even when the address changes.

As illustrated below, Dynamic DNS service ensures that traffic for the FQDN, MyBusiness.DynDNS.org, is routed to the dynamic IP address.

Figure 4   Gateway To Gateway Tunnel with a Dynamic IP Address
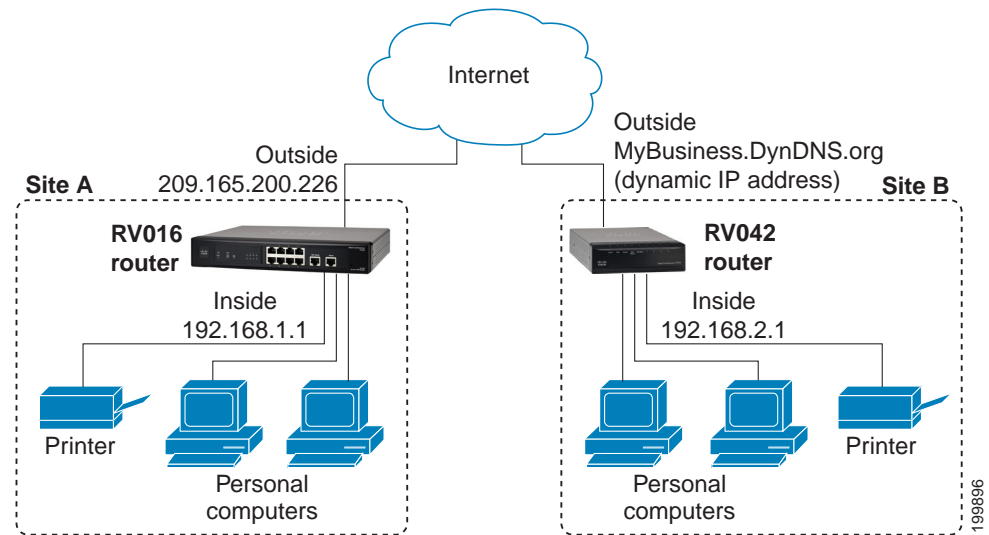
Free Dynamic DNS accounts are available through many providers. Examples are listed below.

- http://dyn.com/dyndns

- http://update.ods.org

- http://www.dhs.org

- http://www.3322.org

- http://www.no-ip.com

LAN Setup

The LAN setup pertains to the network that your router connects to inside your office. It should not be necessary to make any changes in your LAN setup, unless both sites have the same addressing. The two ends of the tunnel cannot be on the same subnet. For example, if the LAN IP address of the RV0xx router at Site A is 192.168.15.1, Site B must use a different subnet, such as 192.168.75.1.

Configuring a VPN Tunnel on a Cisco RV0xx Series Router

This procedure describes the basic tasks in configuring your router. Example entries are provided on .

NOTE

- For a hub-and-spoke topology, configure one tunnel between each remote site and the central site. For the scenario illustrated in **Figure 1**, configure three VPN tunnels on the router at the main site, and configure one VPN tunnel on the router at each remote site.

- For a mesh topology, configure multiple tunnels on each router to ensure connectivity between all sites. For the scenario illustrated in **Figure 2**, configure three VPN tunnels on each router.

STEP 1 Connect a computer to your Cisco RV0xx Series router (called Site A in the examples), and start the web-based configuration utility.

STEP 2 Click **VPN > Gateway to Gateway** in the navigation tree.

STEP 3 Enter the following information about the tunnel:

- **Tunnel Name**—Enter a name, for your reference. This name will be used on the *VPN > Summary* page.

- **Interface**—Select the appropriate Interface, **WAN1** or **WAN2**.

Note: The **Enable** check box is unavailable until after you save the configuration.

STEP 4 In the *Local Group Setup* section, enter the following information about this router (Site A):

- **Local Security Gateway Type**—Select **IP Only**. The WAN IP address of the router will be automatically detected and will appear in the *IP Address* field.

- **Local Security Group Type**—Select **Subnet**. Enter the LAN **IP Address** and the subnet mask.

STEP 5 In the *Remote Group Setup* section, enter the following information about the router at the other end of the tunnel (Site B):

- **Remote Security Gateway Type**—Depending on the type of IP address for the Internet connection, choose one of the following options:

  - *If the remote gateway (Site B) has a static WAN IP address:* Select **IP Only**. Enter the WAN **IP Address** of the Site B router.

- *If the remote gateway (Site B) has a dynamic IP address and a Dynamic DNS hostname:* Select **Dynamic IP + Domain Name (FQDN) Authentication**. Enter the registered **Domain Name** of the Site B router, such as MyBusiness.DynDNS.org.

- **Remote Security Group Type**—Select **Subnet**. Enter the LAN **IP Address** and **Subnet Mask** of the Site B router.

STEP 6 In the *IPSec Setup* section, keep the default settings (recommended) or enter other settings if desired. Ensure that you configure the Site B router with the same settings.

STEP 7 In the **Preshared Key** field, enter a string for this key, for example, 13572468. Ensure that you configure the other router with the same preshared key.

STEP 8 If you need more detailed settings, click **Advanced**. Otherwise, click **Save**.

Note: Advanced settings can be used to enable features such as dead peer detection, NAT traversal, split DNS, and NetBIOS broadcast messages.

STEP 9 At the remote site (Site B), set up the router with the corresponding settings (where Site B is the "local gateway" and Site A is the "remote gateway:).

STEP 10 Use the *VPN > Summary* page to verify that the tunnel is active.

STEP 11 Verify that a computer at Site A can ping a computer at Site B, and vice versa. (Refer to Windows Help for more information). If the ping test is successful, then the VPN tunnel is configured correctly.

STEP 12 Repeat this procedure to configure additional VPN tunnel.

Example: Sites with Static WAN IP Addresses

Settings on the Site A Router:

Field	Value
Local Group Setup	
Local Security Gateway Type	IP Only
IP Address	(Automatically detected) 203.165.200.226
Local Security Group Type	Subnet

Field	Value
IP Address	192.168.1.0
Subnet Mask	255.255.255.0
Remote Group Setup	
Remote Security Gateway Type	IP Only
IP Address	209.165.200.238
Remote Security Group Type	Subnet
IP Address	192.168.2.0
Subnet Mask	255.255.255.0
IPSec Setup	
Keying Mode	IKE with Preshared Key
Phase 1 Encryption	DES
Phase 1 Authentication	MD5
Phase 1 SA Life Time	28800
Perfect Forward Secrecy	Enabled
Phase 2 DH Group	Group 1 - 768 bit
Phase 2 Encryption	DES
Phase 2 Authentication	MD5
Phase 2 SA Life Time	3600
Preshared Key	13572468#123456789

Field	Value
Minimum Preshared Key Complexity	Enabled
Advanced	Default settings

Settings on the Site B Router:

Field	Values
Local Group Setup	
Local Security Gateway Type	IP Only
IP Address	(Automatically detected) 209.165.200.238
Local Security Group Type	Subnet
IP Address	192.168.2.0
Subnet Mask	255.255.255.0
Remote Group Setup	
Remote Security Gateway Type	IP Only
IP Address	203.165.200.226
Remote Security Group Type	Subnet
IP Address	192.168.1.0
Subnet Mask	255.255.255.0
IPSec Setup	
Keying Mode	IKE with Preshared Key
Phase 1 Encryption	DES

Field	Values
Phase 1 Authentication	MD5
Phase 1 SA Life Time	28800
Perfect Forward Secrecy	Enabled
Phase 2 DH Group	Group 1 - 768 bit
Phase 2 Encryption	DES
Phase 2 Authentication	MD5
Phase 2 SA Life Time	3600
Preshared Key	13572468#123456789
Minimum Preshared Key Complexity	Enabled
Advanced	Default settings

Example: Site with a Dynamic WAN IP Address

Settings on the Site A Router:

Field	Value
Local Group Setup	
Local Security Gateway Type	IP Only
IP Address	(Automatically detected) 203.165.200.226

Field	Value
Local Security Group Type	Subnet
IP Address	192.168.1.0
Subnet Mask	255.255.255.0
Remote Group Setup	
Remote Security Gateway Type	Dynamic IP + Domain Name (FQDN) Authentication
Domain Name	cisco.com
Remote Security Group Type	Subnet
IP Address	192.168.2.0
Subnet Mask	255.255.255.0
IPSec Setup	
Keying Mode	IKE with Preshared Key
Phase 1 Encryption	DES
Phase 1 Authentication	MD5
Phase 1 SA Life Time	28800
Perfect Forward Secrecy	Enabled
Phase 2 DH Group	Group 1 - 768 bit
Phase 2 Encryption	DES
Phase 2 Authentication	MD5

Field	Value
Phase 2 SA Life Time	3600
Preshared Key	13572468#123456789
Minimum Preshared Key Complexity	Enabled
Advanced	Default settings

Settings on the Site B Router:

Field	Values
Local Group Setup	
Local Security Gateway Type	Dynamic IP + Domain Name (FQDN) Authentication
Domain Name	cisco.com
Local Security Group Type	Subnet
IP Address	192.168.2.0
Subnet Mask	255.255.255.0
Remote Group Setup	
Remote Security Gateway Type	IP Only
IP Address	203.165.200.226
Remote Security Group Type	Subnet
IP Address	192.168.1.0
Subnet Mask	255.255.255.0

Field	Values
IPSec Setup	
Keying Mode	IKE with Preshared Key
Phase 1 Encryption	DES
Phase 1 Authentication	MD5
Phase 1 SA Life Time	28800
Perfect Forward Secrecy	Enabled
Phase 2 DH Group	Group 1 - 768 bit
Phase 2 Encryption	DES
Phase 2 Authentication	MD5
Phase 2 SA Life Time	3600
Preshared Key	13572468#123456789
Minimum Preshared Key Complexity	Enabled
Advanced	Default settings

OL-26286-01