Objective

Virtual Private Networks (VPNs) ensure business continuity and provide the ability to extend the corporate workplace to employees who need continual access to company resources. A VPN exists as a private network constructed within a public network infrastructure, such as the global Internet. A VPN extends a private network between geographically separate office locations. It enables a host computer to send and receive data across public networks as if they were a part of the private network. Security concerns may arise because of private data sent and received across public networks, but hosts encrypt all data using the IP Security (IPsec) protocol before sending through a VPN to allow staff to work from different sites without compromising the network.VPNs also integrate network features such as routing, Quality of Service (QoS), and multicast support.

Different VPN topologies exist including hub-and-spoke, point-to-point, and full mesh. This Smart Tip covers site-to-site (point-to-point) VPN, which provides an Internet-based infrastructure to extend network resources to remote offices, home offices, and business partner sites.

Cisco RV320 Gigabit Dual WAN VPN Routers deliver robust and easily managed VPN solutions to cost-conscious small business companies. Cisco 2900 Series Integrated Services Routers (ISRs) provide services to meet the demands of today’s medium-sized branches, support cloud-based services, and offer a wide array of common security features such as advanced application inspection and control, threat protection, and encryption architectures for enabling more scalable and manageable VPN networks with secure connectivity by Group Encrypted Transport VPN, Dynamic Multipoint VPN (DMVPN), or Enhanced Easy VPN.

This short guide provides an example design for building a site-to-site IPsec VPN tunnel between a Cisco RV320 Gigabit Dual WAN VPN Router and a Cisco 2900 Series ISR.

Applicable Devices

- Cisco RV320 Routers
- Cisco 1900/2900/3900 Series Integrated Services Routers (ISA2900)

Example Network Configuration

The following shows a sample implementation of site-to-site IPsec VPN tunnel using a Cisco RV320 Gigabit Dual WAN VPN Router and a Cisco 2900 Series ISR.

![Site-to-Site VPN Topology](image)

A site-to-site IPsec VPN tunnel is configured and established between the Cisco RV320 Gigabit Dual WAN VPN Router at the Remote Office and the Cisco 2900 Series ISR at the Main Office.
With this configuration, a host in Network B at the Remote Office and a host in Network A at the Main Office can communicate with each other securely over VPN.

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, 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. A secure policy for every peer must be manually maintained.

Internet Protocol Security (IPSec)

Internet Protocol Security (IPsec) uses cryptographic security services to protect communications over Internet Protocol (IP) networks. IPsec supports network-level peer authentication, data origin authentication, data integrity, data confidentiality (encryption), and replay protection. IPsec involves many component technologies and encryption methods. Yet, IPsec's operation can be broken down into five main steps:

Step 1. Interesting traffic initiates the IPsec process. Traffic is deemed interesting when the IPsec security policy configured in the IPsec peers starts the IKE process.
Step 2. IKE phase 1. IKE authenticates IPsec peers and negotiates IKE SAs during this phase, setting up a secure channel for negotiating IPsec SAs in IKE phase 2.
Step 3. IKE phase 2. IKE negotiates IPsec SA parameters and sets up matching IPsec SAs in the peers.
Step 4. Data transfer. Data is transferred between IPsec peers based on the IPsec parameters and keys stored in the SA database.
Step 5. IPsec tunnel termination. IPsec SAs terminate through deletion or by timing out.

Pre-Configuration

Step 1. Connect an Ethernet cable between the RV320 and its DSL or cable modem, and connect an Ethernet cable between the ISR2900 and its cable or DSL modem.
Step 2. Configure basic configurations on both the RV320 and the ISR2900.
Step 3. Make sure to configure the network IP addresses at each site on different subnets. In this example, the Remote Office LAN is using 20.0.0.0 and the Main Office LAN is using 10.0.0.0.
Step 4. Make sure local PCs are able connect to their respective routers, and with other PCs on the same LAN.

Configuring the Site-to-Site IPsec VPN Tunnel for RV320 at the Remote Office

Step 1. Go to VPN > Gateway-to-Gateway (see Figure 2)
   a.) Enter a Tunnel Name, such as RemoteOffice.
   b.) Select Interface as WAN1.
   c.) Select Keying Mode as IKE with Preshared Key.
   d.) Input Local IP Address and Remote IP Address.
   e.) Figure 2  RV320 Gigabit Dual WAN VPN Router Gateway-to-Gateway
Step 2. Set up IPSec Tunnel Settings (see Figure 3)
   a.) Select Encryption as 3DES.
   b.) Select Authentication as SHA1.
   c.) Check Perfect Forward Secrecy.
   d.) Set up the Presheared Key (needs to be the same on both routers).

Figure 3 IPSec Setup (Phase 1 and 2)
### Note:
Make sure the Preshared Key Strength Meter is to the maximum (green) to have a more secure connection.

**Step 3. Set up Advanced Settings (see Figure 3)**

- a.) Check and set AH Hash Algorithm as SHA1.
- b.) Check NetBIOS Broadcast.
- c.) Check and set Dead Peer Detection Interval (default is 10 seconds, with a maximum of 999 seconds).

**Figure 3 Advanced Settings**
Step 4. Click Save to complete the configuration.

Configuring the Site-to-Site IPsec VPN Tunnel for ISR2900 at the Main Office
Configuration Cisco 2900 Series (CLI)

```
router(config)#crypto isakmp policy 1
router(config)#crypto isakmp policy 1 authentication preshared
router(config)#crypto isakmp key <CISCO> address <IP address>
router(config)#access-list 100 permit ip <IP address main office><subnet mask><IP address remote office><subnet mask>
```

Note: In the case of multiple subnets, you will need to configure Access Lists to allow traffic to flow between the networks through the VPN tunnel.

Verify VPN Status on the ISR2900 at the Main Office

```
router(config)#show crypto ipsec sa

interface: <interface ID>
  Crypto map tag: MYMAP, local addr 192.168.1.4
  protected vrf: (none)
  local ident (addr/mask/prot/port): (10.0.0.0/255.0.0.0/0/0)
  remote ident (addr/mask/prot/port): (20.1.1.0/255.255.255.0/0/0)
  current peer 192.168.1.3 port 500
  PERMIT, flags=[origin_is_acl]
  #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
  #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
  #send errors 0, #recv errors 0
```

Note: Before verifying the VPN status, it helps to do a successful ping between the networks defined on the ACL, and then run this command to verify if the secure VPN connection was established.