Cisco RV Routers VPN Overview and Best Practices

Objective

The objective of this document is to give an overview of Virtual Private Network (VPN) best practices to anyone new to Cisco RV series routers.

Table of Contents

- Benefits of using a VPN Connection
- Risks of using a VPN Connection
- Types of VPN
  - Secure Sockets Layer (SSL)
  - IPsec Profile
  - Point-to-Point Tunneling Protocol (PPTP)
  - Generic Routing Encapsulation
  - Layer 2 Tunneling Protocol
- VPNs that are Compatible with Cisco RV Series VPN Routers
- Certificates
- Site-to-Site VPN on a Router
- Client-to-Site VPN on a Router
  - Create a Client-to-Site Profile
  - User Groups
  - User Accounts
- Client-to-Site at Client Location
- Setup Wizard
- Tips to Use When Configuring a VPN

Introduction

It seems so long ago that the only place you could work was at the office. You may remember, back in the day, having to head into the office on the weekend to get a work matter settled. There was no other way to obtain data from company resources unless you were physically in your office. Those days are over. In todayâ€™s times, you are able to be on the go; conducting business from home, another office, a coffee shop, or even another country. The downside is that hackers are always looking to grab your sensitive data. Just using the public Internet is not safe. What can you do to get flexibility as well as security? Set up a VPN!

A VPN connection allows users to access, send, and receive data to and from a private network by means of going through a public or shared network such as the Internet but still ensuring a secure connection to an underlying network infrastructure to protect the private network and its resources.

A VPN tunnel establishes a private network that can send data securely using encryption to encode the data, and authentication to ensure the identity of the client. Corporate offices often use a VPN connection since it is both useful and necessary to allow their employees to have access to their private network even if they are outside the office.

Normally, site-to-site VPNs connect entire networks to each other. They extend a network and allow computer resources from one location to be available at other locations. Through the use of a VPN capable router, a company can connect multiple fixed sites over a public network such as the Internet.

The client-to-site set up for a VPN allows a remote host, or client, to act as if they were located on the same local network. A VPN connection can be set up between the router and an endpoint after the router has been configured for Internet connection. The VPN client is dependent on the settings of the VPN router in addition to the requirement of matched settings in order to establish a connection. Also, some of the VPN client applications are platform specific, they are dependent on the Operating system (OS) version as well. The settings must be exactly the same or they cannot communicate.

A VPN can be set up with any of the following:

- Secure Socket Layer (SSL)
- Internet Protocol Security (IPSec)
- Point to Point Tunneling Protocol (PPTP)- not as secure as SSL or IPSec
- Generic Routing Encapsulation (GRE)
- Layer 2 Tunneling Protocol (L2TP)

If you have never set up a VPN before, you will receive a lot of new information throughout this article. This is not a step-by-step guide, but more of an overview for reference. Therefore, it would be beneficial to read this article in its entirety before moving on and attempting to set up a VPN on your network. Links for specific steps are provided throughout this article.

Third-party, non-Cisco products, including TheGreenBow, OpenVPN, Shrew Soft, and EZ VPN are not supported by Cisco. They are included strictly for guidance purposes. If you need support on these beyond the article, you should contact the third-party for support.

Benefits of using a VPN Connection

- Using a VPN connection helps protect confidential network data and resources.
- It provides convenience and accessibility for remote workers or corporate employees since they will be able to easily access the main office resources without having to be physically present and yet, maintain the security of the private network and its resources.
- Communication using a VPN connection provides a higher level of security compared to other methods of remote communication. An advanced encryption algorithm makes this possible, protecting the private network from unauthorized access.
- The actual geographic locations of the users are protected and not exposed to the public or shared networks like the Internet.
- A VPN allows new users or a group of users to be added without the need for additional components or a complicated configuration.

Risks of using a VPN Connection

- There can be security risks due to misconfiguration. Since the design and implementation of a VPN can be complicated, it is necessary to entrust the task of configuring the connection to a knowledgeable and experienced professional in order to make sure that the security of the private network would not be compromised.
- It may be less reliable. Since a VPN connection requires an Internet connection, it is important to have a provider with a proven and tested reputation to provide excellent Internet service and guarantee minimal to no downtime.
- If a situation occurs where there is a need to add new infrastructure or a new set of configurations, technical issues may arise due to incompatibility especially if it involves different products or vendors

other than the ones you are already using.
- Slow connection speeds can occur. If you are using an ISP connection that provides free VPN service, it may be expected that your connection would also be slow since these providers do not prioritize connection speeds. It is important to note that VPN throughput depends on the hardware capabilities of the router.

For more information on how VPNs work, click here.

Tips to Use When Configuring a VPN

1. Use a different LAN IP subnet at both ends while configuring VPN between different sites. For example, if the site you connect to uses a 192.168.x.x addressing scheme, you would want to use a 10.x.x.x or 172.16.x.x - 172.31.x.x subnet. Another option would be to have different subnet masks. When you change your router IP address, the devices on Dynamic Host Configuration Protocol (DHCP) would automatically pick up an IP address in that subnet.
2. Use the static public IP on the WAN interface of the router for stable VPN connectivity.
3. Be sure the Encryption and Authentication level selected is the same as the router you wish to establish a VPN tunnel to for the VPN.
4. Be sure the PSK and Key Lifetime entered are the same as the remote router. A PSK can be whatever you want it to be, it just has to match at the site and with the client when they set up as a Client on their computer. Depending on the device, there may be forbidden symbols that you cannot use. Key Lifetime is how often the system changes the key. A Certificate is preferred since it is considered more secure.
5. For most VPNs, clients don't need a Certificate to use a VPN, it is just for verification through the router. For example, OpenVPN requires both client and site certificates.
6. Set your SA Lifetime in Phase I longer than your Phase II SA Lifetime. If you make your Phase I shorter than Phase II, then you will be having to renegotiate the tunnel back and forth frequently as opposed to the data tunnel. A data tunnel needs more security, so it is better to have the lifetime in Phase II to be shorter than Phase I.
7. Change all passwords to something more complex.

Types of VPN

Secure Sockets Layer (SSL)

Cisco RV34x series routers supports an SSL VPN, using AnyConnect. The RV160 and RV260 have the option to use OpenVPN, which is another SSL VPN. The SSL VPN server allows remote users to establish a secure VPN tunnel using a web browser. This feature allows easy access to a wide range of web resources and web-enabled applications using native Hypertext Transfer Protocol (HTTP) over SSL Hypertext Transfer Protocol Secure (HTTPS) browser support.

The SSL VPN allows users to remotely access restricted networks, using a secure and authenticated pathway by encrypting the network traffic.

There are two options to set up access in SSL:

1. Self-Signed Certificate: A Certificate that is signed by its own creator. This is not recommended and should only be used in a test environment.
2. CA Signed Certificate: This is much more secure and highly recommended. For a fee, a third-party validates that the network is legitimate and creates a CA Certificate which is then attached to the site. For more information on CA Certificates, check out the Certificates section of this article.

There are links to articles on AnyConnect within this document. For an overview of AnyConnect, click here.

IPsec Profile

Easy VPN (EZVPN), TheGreenBow, and Shrew Soft are Internet Protocol Security (IPSec) VPNs. IPSec VPNs provide secure tunnels between two peers or from a client-to-site. Packets that are considered sensitive should be sent through these secure tunnels. Parameters including hash algorithm, encryption algorithm, key lifetime, and mode must be used to protect these sensitive packets should be defined by specifying the characteristics of these tunnels. Then, when the IPsec peer sees such a sensitive packet, it sets up the appropriate secure tunnel and sends the packet through this tunnel to the remote peer.

When IPsec is implemented in a firewall or a router, it provides strong security that can be applied to all traffic crossing the perimeter. Traffic within a company or workgroup does not incur the overhead of security-related processing.

In order for the two ends of a VPN tunnel to be successfully encrypted and established, they both need to agree on the methods of encryption, decryption, and authentication. IPsec profile is the central configuration in IPsec that defines the algorithms such as encryption, authentication, and Diffie-Hellman (DH) group for Phase I and II negotiation in auto mode as well as manual keying mode.

Important components of IPsec include Internet Key Exchange (IKE) Phase 1 and Phase 2.

The basic purpose of IKE phase one is to authenticate the IPSec peers and to set up a secure channel between the peers to enable IKE exchanges. IKE phase one performs the following functions:

- Authenticates and protects the identities of the IPSec peers
- Negotiates a matching IKE Security Associations (SA) policy between peers to protect the IKE exchange
- Performs an authenticated Diffie-Hellman exchange with the end result of having matching shared secret keys
- Sets up a secure tunnel to negotiate IKE phase two parameters
- Occurs in two modes, main mode and aggressive mode

The purpose of IKE phase two is to negotiate IPSec SAs to set up the IPSec tunnel. IKE phase two performs the following functions:

- Negotiates IPSec SA parameters protected by an existing IKE SA
- Establishes IPSec security associations
- Periodically renegotiates IPSec SAs to ensure security
- Optionally performs an additional Diffie-Hellman exchange
- Only one mode used, quick mode

If Perfect Forward Secrecy (PFS) is specified in the IPSec policy, a new DH exchange is performed with each quick mode, providing keying material that has greater entropy (key material life) and thereby greater resistance to cryptographic attacks. Each DH exchange requires large exponentiations, thereby increasing CPU use and exacting a performance cost.

- Configuration of Internet Protocol Security (IPSec) Profile on an RV34x Series Router
- Configuring IPSec Profiles (Auto Keying Mode) on the RV160 and RV260
- Configuring IPsec Profile Manual Keying Mode on RV160 and RV260 Routers

Point-to-Point Tunneling Protocol (PPTP)

PPTP is a network protocol used to create VPN tunnels between public networks. PPTP servers are also known as Virtual Private Dialup Network (VPDN) servers. PPTP is sometimes used over other protocols because it is faster and has ability to work on mobile devices. However, it is important to note that it is not

as secure as other types of VPNs. There are multiple methods to connect with PPTP type accounts. Click the links to learn more:

- Configure a Point-to-Point Tunneling Protocol (PPTP) Server on the Rv34x Series Router
- Configure Point to Point Tunneling Protocol (PPTP) Server on RV320 and RV325 VPN Router Series on Windows

Generic Routing Encapsulation

Generic Routing Encapsulation (GRE) is a tunneling protocol that provides a simple generic approach to transport packets of one protocol over another protocol by means of encapsulation.

GRE encapsulates a payload, that is, an inner packet that needs to be delivered to a destination network inside an outer IP packet. The GRE tunnel behaves as virtual point-to-point link that has two endpoints identified by the tunnel source and tunnel destination address.

The tunnel endpoints send payloads through GRE tunnels by routing encapsulated packets through intervening IP networks. Other IP routers along the way do not parse the payload (the inner packet); they only parse the outer IP packet as they forward it towards the GRE tunnel endpoint. Upon reaching the tunnel endpoint, GRE encapsulation is removed, and the payload is forwarded to the packet's ultimate destination.

Encapsulation of datagrams in a network is done for multiple reasons, such as when a source server wants to influence the route that a packet takes to reach the destination host. The source server is also known as the encapsulation server.

IP-in-IP encapsulation involves the insertion of an outer IP header over the existing IP header. The source and destination address in the outer IP header point to the end points of the IP-in-IP tunnel. The stack of IP headers is used to direct the packet over a predetermined path to the destination, provided the network administrator knows the loopback addresses of the routers transporting the packet.

This tunneling mechanism can be used for determining availability and latency for most network architectures. It is to be noted that the entire path from source to the destination does not have to be included in the headers, but a segment of the network can be chosen for directing the packets.

Layer 2 Tunneling Protocol

L2TP does not provide encryption mechanisms for the traffic it tunnels. Instead it relies on other security protocols, such as IPSec, to encrypt the data.

A L2TP tunnel is established between the L2TP Access Concentrator (LAC) and the L2TP Network Server (LNS). An IPSec tunnel is also established between these devices and all L2TP tunnel traffic is encrypted using IPSec.

Some key terms with L2TP:

- **CHAP -** Challenge Handshake Authentication Protocol. A Point to Point authentication Protocol (PPP).
- **L2TP Access Concentrator (LAC) -** A LAC can be a Cisco network access server connected to the public switched telephone network (PSTN). The LAC need only implement media for operation over L2TP. An LAC can connect to the LNS using a local-area network or wide-area network such as public or private Frame Relay. The LAC is the initiator of incoming calls and the receiver of outgoing calls.
- **L2TP Network Server (LNS) -** Almost any Cisco router connected to a local-area network or wide-area network, such as public or private Frame Relay, can act as an LNS. It is the server side of the

L2TP protocol and must operate on any platform that terminates PPP sessions. The LNS is the initiator of outgoing calls and the receiver of incoming calls. Figure 1 depicts the call routine between the LAC and LNS.

- **Virtual Private Dial Network (VPDN) -** A type of access VPN that uses PPP to deliver the service.

If you would like more information on L2TP click on the following links:

- Configure L2TP WAN Settings on the RV34x Router
- Wide-Area Networking Configuration Guide: Layer 2 Services, Cisco IOS XE Release 3S

VPNs that are Compatible with Cisco RV Series VPN Routers

	RV34X	RV32X	RV160X/RV260X
IPSec (IKEv1)			
ShrewSoft	Yes	Yes	Yes
Greenbow	Yes	Yes	Yes
Mac built-in client	Yes	Yes	No
iPhone/iPad	Yes	Yes	No
Android	Yes	Yes	Yes
L2TP/IPSec	Yes (PAP)	No	No
PPTP	Yes (PAP)	Yes*	Yes (PAP)
Other			
AnyConnect	Yes	No	No
Openvpn	No	Yes	Yes
IKEv2			
Windows	Yes*	No	Yes*
Mac	Yes	No	Yes
iPhone	Yes	No	Yes
Android	Yes	No	Yes

VPN Technology	Devices Supported	Clients Supported*	Details & Caveats
IPSec (IKEv1)	RV34X, RV32X, RV160X/RV260X	Native: Mac, iPhone, iPad, Android Other: EasyVPN (Cisco VPN Client), ShrewSoft, Greenbow	Easiest to setup, troubleshoot and support. It is available on all routers, is simple to setup (for the most part), has the best logging to troubleshoot. And includes the most devices. This is why we typically recommend ShrewSoft (free and works) and Greenbow (not free, but works). For Windows, we have ShrewSoft and Greenbow clients as options, since Windows doesnâ€™t have a pure IPSec native VPN client. For ShrewSoft and Greenbow, itâ€™s a little more involved, but not difficult. Once setup the first time, client profiles can be exported and then imported on other clients.

			For RV160X/RV260X routers, since we donâ€™t have the Easy VPN option, we have to use the 3rd Party Client option, which doesnâ€™t work with Mac, iPhone, or iPad. We can setup ShrewSoft, Greeenbow, and Android clients to connect, though. For Mac, iPhone, and iPad clients, I recommend IKEv2 (see below).
AnyConnect	RV34X	Windows, Mac, iPhone, iPad, Android	Some customers request a full Cisco solution and this is it. It is simple to setup, has logging, but can be challenging to understand the logs. Requires client licensing requirement incuring cost. Itâ€™s a full Cisco solution and is updated. Troubleshooting isnâ€™t as easy as IPSec, but better than the other VPN options.
L2TP/IPSec	RV34X	Native: Windows	This is what I will recommend for customers that need to use the built-in VPN client in Windows. Two caveats with this are: 1. We only support PAP authentication when using Local Authentication. We have to go into each client and select optional or no encryption, disable MS-CHAP options, and enable PAP. This means the username/password are sent in the clear. Itâ€™s not a huge deal since everything is encrypted with IPSec, and have to setup on each client. On Windows, this is configurable, but not on Mac, iPhone, iPad, or Android devices, so really can only be used by Windows clients unless they have an external authentication server like Radius or LDAP. 2. If the router is behind a NAT device, the connection will fail on Windows machines. The workaround is to create a registry key on each client to allow NAT on both the client and router.
IPSec (IKEv2)	RV34X, RV160X/RV260X	Native: Windows, Mac, iPhone, iPad, Android	Windows native client for IKEv2 requires certificate authentication, which requires a PKI infrastructure since both the router and all the clients need to have certificates from the same CA (or another trusted CA). For those that want to use IKEv2, we set that up for their Mac, iPhone,iPad, and Android devices and we usually setup IKEv1 for their Windows machines (ShrewSoft, Greenbow, or L2TP/IPSec).
Open VPN	RV32X, RV160X/RV260X	Open VPN is the client	Harder to setup, difficult to troubleshoot and support. Supported on RV160X/RV260X and RV320. Setting

	up is more complex than IPSec or AnyConnect, especially if they use certificates, which most do. Troubleshooting is harder since we donâ€™t have any useful logs on the router and rely on the client logs. Also, OpenVPN client version updates have without warning changed which certificates they accepted. Also, we found this doesnâ€™t work on Chromebooks and had to go to an IPSec solution.

* We test as many combinations as we can, if there's a specific hardware/software combination please reach out here. Otherwise, see the related configuration guide by device for most recent version tested.

Certificates

Have you ever visited a website and were given a warning that it isnâ€™t secure? It doesnâ€™t fill you with confidence that your private information is secure, and it isnâ€™t! If a site is secure you will see a closed lock icon before the name of the site. This is a symbol that the site has been verified safe. You want to be sure to see that lock icon closed. The same is true for your VPN.

When you set up a VPN, you should obtain a Certificate from a Certificate Authority (CA). Certificates are purchased from third-party sites and used for authentication. It is an official way to prove that your site is secure. Essentially, the CA is a trusted source that verifies that you are a legitimate business and can be trusted. For a VPN you only need a lower level Certificate at a minimal cost. You get checked out by the CA, and once they verify your information, they will issue the Certificate to you. This Certificate can be downloaded as a file on your computer. You can then go into your router (or VPN server) and upload it there.

CA uses Public Key Infrastructure (PKI) when issuing digital certificates, which uses public key or private key encryption to ensure security. CAs are responsible for managing certificate requests and issuing digital certificates. A few third-party CAs include IdenTrust, Comodo, GoDaddy, GlobalSign, GeoTrust, and Verisign.

It is important that all gateways in a VPN use the same algorithm, otherwise they wonâ€™t be able to communicate. To keep things simple, it is recommended that all Certificates are purchased from the same trusted third-party. This keeps multiple Certificates easier to manage as they have to be manually renewed.

Note: Clients usually donâ€™t need a Certificate to use a VPN; it is just for verification through the router. An exception to this is OpenVPN, which requires a client Certificate.

Some small businesses choose to use a password or a pre-shared key in place of a Certificate for simplicity. This is less secure but can be set up at no cost.

More information on Certificates can be found in the links below:

- Certificate (Import/Export/Generate CSR) on the RV160 and RV260 Series Router
- Replace the Default Self-Signed Certificate with a 3rd Party SSL Certificate on the RV34x Series Router

Site-to-Site VPN on a Router

For the local and remote router, it is important to make sure the pre-shared key (PSK)/password/Certificate used for the VPN connection, and the security settings all match. If one or more routers use Network

Address Translation (NAT), which most of the Cisco RV series routers use, you will need to do firewall exemptions for the VPN connection on the local and remote router.

Check out these site-to-site articles for more information:

- Configuring Site-to-Site VPN on the RV34x
- Configure a Site-to-Site VPN on an RV340 or RV345 Router
- Cisco Tech Talk: Configuring Site-to-Site VPN on RV340 Series Routers (video)
- Configuring Site-to-Site VPN on an RV160 and RV260 Router (Basic Settings)
- Site-to-Site VPN on the RV160 and RV260 Router (Advanced Settings and Failover)

Client-to-Site VPN on a Router

Before a VPN can be set up on the client side, an administrator needs to configure it on the router.

Click to view these router configuration articles:

- Configuring VPN Setup Wizard on the RV160 and RV260 Routers
- Configuring Shrew Soft VPN Client with the RV160 and RV260
- Cisco Tech Talk: Configuring Shrew Soft VPN on RV160 and RV260 (video)
- Set Up and Use TheGreenBow IPsec VPN Client to Connect with RV160 and RV260 Routers

Create a Client-to-Site Profile

In a Client-to-Site VPN connection, clients from the Internet can connect to the server to access the corporate network or LAN behind the server but still maintain the security of the network and its resources. This feature is very useful since it creates a new VPN tunnel that would allow teleworkers and business travelers to access your network by using a VPN client software without compromising privacy and security. The following articles are specific to the RV34x series routers:

- Configure Client-to-Site Virtual Private Network (VPN) Connection on the RV34x Series Router
- Configure AnyConnect Virtual Private Network (VPN) Connectivity on the RV34x Series Router

The client-to-site VPN will not work if Port Forwarding is set for source *All Traffic* and destination *All Traffic*.

User Groups

User groups are created on the router for a collection of users that share the same set of services. These user groups include options for the group, like a list of permissions on how they can access the VPN. Depending on the device, PPTP, site-to-site IPSec VPN, and client-to-site IPSec VPN can be allowed. For example, the RV260 has options that include OpenVPN but L2TP is not supported. The RV340 series is equipped with AnyConnect for an SSL VPN, as well as Captive Portal or EZ VPN.

These settings enable administrators to control and filter so that only authorized users can access the network. Shrew Soft and TheGreenBow are two of the most common VPN Clients available for download. They need to be configured based on the VPN settings of the router for them to be able to successfully establish a VPN tunnel. The following article specifically addresses the creation of a user group:

- Create a User Group for VPN Setup on the RV34x Router

When setting up User Groups for a VPN, be sure to leave the default admin account in the admin group and create a new user account and user group for VPN. If you move your admin account to a different group, you will prevent yourself from logging into the router. As a result, you would have to do a factory reset and configure for that router again, leaving the default admin account in the admin group alone.

User Accounts

User Accounts are created on the router in order to allow authentication of local users using the local database for various services like PPTP, VPN Client, web Graphical User Interface (GUI) login, and Secure Sockets Layer Virtual Private Network (SSLVPN). This enables the administrators to control and filter authorized users only to access the network. The following article specifically addresses the creation of a user account:

- Create a User Account for VPN Client Setup on the RV34x Router

Client-to-Site at Client Location

In a Client-to-Site VPN connection, clients from the Internet can connect to the server to access the corporate network or LAN behind the server but still maintains the security of the network and its resources. This feature is very useful since it creates a new VPN tunnel that allows teleworkers and business travelers to access your network by using a VPN client software without compromising privacy and security. The VPN is set up to encrypt and decrypt data as it is sent and received.

The AnyConnect application works with SSL VPN and is used with the RV34x routers specifically. It is not available with other RV series of routers. Starting with version 1.0.3.15, a router license is no longer necessary, but licenses need to be purchased for the client side of the VPN. For more information on Cisco AnyConnect Secure Mobility Client, click here. For directions on installation, select from the following articles:

- Install Cisco AnyConnect Secure Mobility Client on a Mac Computer
- Install Cisco AnyConnect Secure Mobility Client on a Windows Computer

There are some third-party applications that can be utilized for client-to-site VPN with all RV series routers. As stated previously, Cisco doesnâ€™t support these applications; this information is being provided for guidance purposes.

TheGreenBow VPN Client is a third-party VPN client application that makes it possible for a host device to configure a secure connection for client-to-site IPsec tunnel or SSL. This is a paid application that includes support.

- Set Up and Use TheGreenBow IPsec VPN Client to Connect with RV160 and RV260 Routers

OpenVPN is a free, open-source application that can be set up and used for an SSL VPN. It uses a client-server connection to provide secure communications between a server and a remote client location over the internet.

- OpenVPN on RV160 and RV260 Routers

Shrew Soft is a free, open-source application that can be set up and used for an IPsec VPN as well. It uses a client-server connection to provide secure communications between a server and a remote client location over the internet.

- Configuring Shrew Soft VPN Client with the RV160 and RV260

Easy VPN was commonly used on RV32x routers. Here is some information for reference:

- Configure Easy Client to Gateway Virtual Private Network (VPN) on RV320 and RV325 VPN Router Series
- Cisco Easy VPN Q&A

- Easy VPN on Cisco IOS Software-Based Routers

Setup Wizard

The latest Cisco RV series routers come with a VPN Setup Wizard that guides you through the steps for setup. The VPN Setup Wizard lets you configure basic LAN-to-LAN and remote access VPN connections and assign either pre-shared keys or digital certificates for authentication. Check out these articles for more information:

- Configuring VPN Setup Wizard on the RV160 and RV260
- Configure Virtual Private Network (VPN) Connection using the Setup Wizard on the RV34x Series Router

Conclusion

This article has led you to a better understanding of VPNs along with tips to get you on your way. Now you should be ready to configure your own! Take some time to view the links and decide the best way to set up a VPN on your Cisco RV series router.