BROCADE

CONFIGURATION GUIDE

Brocade Vyatta Network OS VPN Support Configuration Guide, 5.2R1

Supporting Brocade vRouter, VNF Platform, and Distributed Services Platform Deployments

53-1004719-01
24 October 2016

Contents

Preface

Document conventions

The document conventions describe text formatting conventions, command syntax conventions, and important notice formats used in Brocade technical documentation.

Notes, cautions, and warnings

Notes, cautions, and warning statements may be used in this document. They are listed in the order of increasing severity of potential hazards.

NOTE

A Note provides a tip, guidance, or advice, emphasizes important information, or provides a reference to related information.

ATTENTION

An Attention statement indicates a stronger note, for example, to alert you when traffic might be interrupted or the device might reboot.

CAUTION

A Caution statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.

DANGER

A Danger statement indicates conditions or situations that can be potentially lethal or extremely hazardous to you. Safety labels are also attached directly to products to warn of these conditions or situations.

Text formatting conventions

Text formatting conventions such as boldface, italic, or Courier font may be used to highlight specific words or phrases.

Format	Description
bold text	Identifies command names.
	Identifies keywords and operands.
	Identifies the names of GUI elements.
	Identifies text to enter in the GUI.
italic text	Identifies emphasis.
	Identifies variables.
	Identifies document titles.
`Courier font`	Identifies CLI output.
	Identifies command syntax examples.

Command syntax conventions

Bold and italic text identify command syntax components. Delimiters and operators define groupings of parameters and their logical relationships.

Convention	Description
bold text	Identifies command names, keywords, and command options.
italic text	Identifies a variable.
value	In Fibre Channel products, a fixed value provided as input to a command option is printed in plain text, for example, **--show** WWN.
[ ]	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.
{ **x** | **y** | **z** }	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options. In Fibre Channel products, square brackets may be used instead for this purpose.
x | **y**	A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, for example, passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, *member*[*member*...].
\	Indicates a "soft" line break in command examples. If a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

Brocade resources

Visit the Brocade website to locate related documentation for your product and additional Brocade resources.

White papers, data sheets, and the most recent versions of Brocade software and hardware manuals are available at www.brocade.com. Product documentation for all supported releases is available to registered users at MyBrocade.
Click the **Support** tab and select **Document Library** to access documentation on MyBrocade or www.brocade.com You can locate documentation by product or by operating system.

Release notes are bundled with software downloads on MyBrocade. Links to software downloads are available on the MyBrocade landing page and in the Document Library.

Document feedback

Quality is our first concern at Brocade, and we have made every effort to ensure the accuracy and completeness of this document. However, if you find an error or an omission, or you think that a topic needs further development, we want to hear from you. You can provide feedback in two ways:

- Through the online feedback form in the HTML documents posted on www.brocade.com
- By sending your feedback to documentation@brocade.com

Provide the publication title, part number, and as much detail as possible, including the topic heading and page number if applicable, as well as your suggestions for improvement.

Contacting Brocade Technical Support

As a Brocade customer, you can contact Brocade Technical Support 24x7 online, by telephone, or by e-mail. Brocade OEM customers should contact their OEM/solution provider.

Brocade customers

For product support information and the latest information on contacting the Technical Assistance Center, go to www.brocade.com and select **Support**.

If you have purchased Brocade product support directly from Brocade, use one of the following methods to contact the Brocade Technical Assistance Center 24x7.

Online	Telephone	E-mail
Preferred method of contact for non-urgent issues: • Case management through the MyBrocade portal. • Quick Access links to Knowledge Base, Community, Document Library, Software Downloads and Licensing tools	Required for Sev 1-Critical and Sev 2-High issues: • Continental US: 1-800-752-8061 • Europe, Middle East, Africa, and Asia Pacific: +800-AT FIBREE (+800 28 34 27 33) • Toll-free numbers are available in many countries. • For areas unable to access a toll-free number: +1-408-333-6061	support@brocade.com Please include: • Problem summary • Serial number • Installation details • Environment description

Brocade OEM customers

If you have purchased Brocade product support from a Brocade OEM/solution provider, contact your OEM/solution provider for all of your product support needs.

- OEM/solution providers are trained and certified by Brocade to support Brocade® products.
- Brocade provides backline support for issues that cannot be resolved by the OEM/solution provider.
- Brocade Supplemental Support augments your existing OEM support contract, providing direct access to Brocade expertise. For more information, contact Brocade or your OEM.
- For questions regarding service levels and response times, contact your OEM/solution provider.

About This Guide

This guide describes all of the available documentation guides for Brocade Vyatta Network OS, plus the guides that apply specifically to Brocade 5600 vRouter, VNF Platform, and Distributed Services Platform.

VPN Support Overview

Supported VPN deployments

The following table shows the VPN deployment options that are supported by the Brocade vRouter.

TABLE 1 Site-to-site solutions

Solution Type	Ease of Configurability	Level of Security	Requires Public Key Infrastructure	Configurable/ Routable Interface	Bridgeable	Interoperability with Third-Party Solutions	Comments
IPsec (pre-shared keys)	Moderate	Good	No	No	No	Very common	
IPsec (RSA digital signatures)	Moderate	Good	No	No	No	Very common	
Elaborate	Very good	Yes	No	No	No	Common	Provides a very secure but more involved configuration.
VTI	Similar to underlying IPsec	Same as underlying IPsec	No	Yes	No	Common	Adds an interface that can be configured, routed, or both to an IPsec solution and operates with a variety of third-party equipment.
GRE over IPsec	Similar to underlying IPsec	Same as underlying IPsec	No	Yes	Yes	Common	Adds an interface that can be configured, routed, or both to an IPsec solution and operates with a variety of third-party equipment.
DMVPN	Adds some complexity to underlying IPsec	Same as underlying IPsec	No	Yes	No	Common	Provides the ability to easily scale a hub-and-spoke multipoint GRE over IPsec solution. This solution limits the number of subnets required, reduces the configuration complexity at the hub, and reduces traffic at the hub by providing dynamic spoke-to-spoke tunnels.

TABLE 1 Site-to-site solutions (continued)

Solution Type	Ease of Configurability	Level of Security	Requires Public Key Infrastructure	Configurable/ Routable Interface	Bridgeable	Interoperability with Third-Party Solutions	Comments
OpenVPN (pre-shared secret)	Easy	Good	No	Yes	Yes	Uncommon	Provides a highly flexible and resilient VPN protocol, which is recommended for Brocade vRouter to Brocade vRouter VPN connectivity.
OpenVPN (TLS)	Elaborate	Very good	Yes	Yes	Yes	Uncommon	

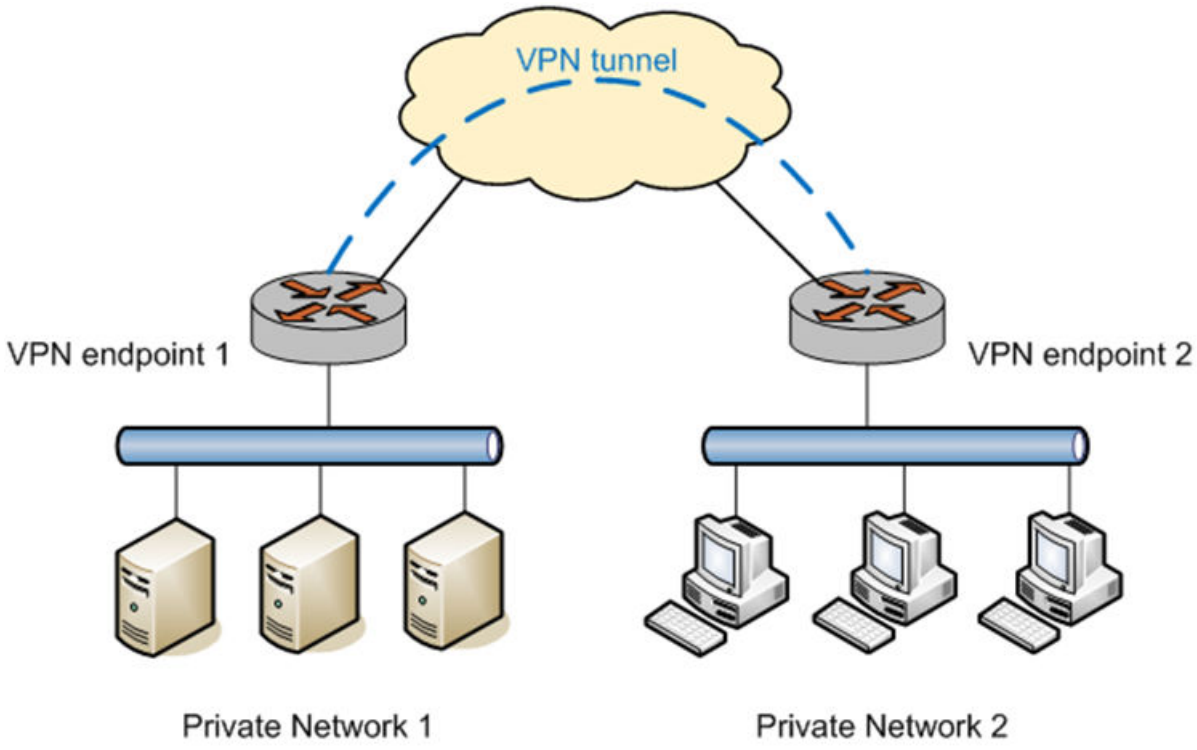
TABLE 2 Remote access solutions

Solution Type	Ease of Configurability	Level of Security	Requires Public Key Infrastructure	Configurable/ Routable Interface	Bridgeable	Interoperability with Third-Party Solutions	Comments
RA (L2TP / IPsec – pre-shared keys)	Easy	Good	No	N/A	No	Very common	Provides an easy way to configure Windows clients to connect remotely.
RA (L2TP / IPsec – X.509 certificates)	Elaborate	Very good	Yes	N/A	No	Common	Provides a more involved way to configure Windows clients to connect remotely.
OpenVPN (TLS)	Elaborate	Elaborate	Yes	N/A	No	Uncommon	Provides a more involved way to configure Windows clients to connect remotely.

Site-to-site IPsec VPN

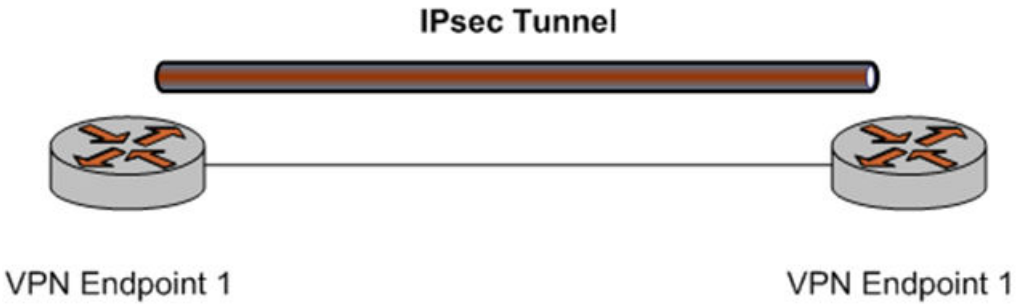
A site-to-site VPN that allows you to connect two or more sites separated by a wide area network (WAN) such that they appear to be on a single private network. The following figure shows a site connected by a tunnel.

FIGURE 1 Site-to-site IPsec VPN



The following figure shows how the Brocade vRouter supports IPsec-protected site-to-site tunnels.

FIGURE 2 IPsec tunnel



For site-to-site IPsec tunnels, the Brocade vRouter supports a special kind of interface—a virtual tunnel interface—that provides a routable interface at the endpoints of the tunnel.

For information about site-to-site VPN deployment and virtual tunnel interfaces, see *Brocade Vyatta Network OS IPsec Site-to-Site VPN Configuration Guide*.

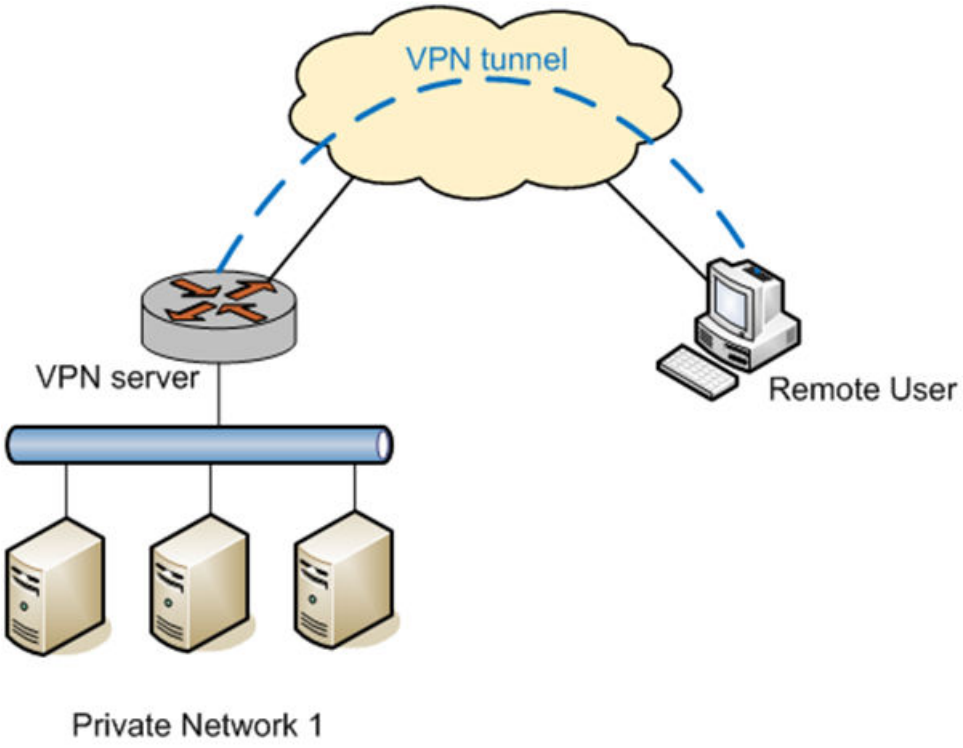
Remote access VPN

A remote access VPN allows a VPN tunnel to be established between a remote user and a VPN server. For example, a remote access VPN allows a remote user to access the company network from home.

Conceptually, site-to-site VPN and remote access VPN are similar in that they both use a tunnel to make the two endpoints appear to be on the same network. The solutions vary in the way that the tunnel is established.

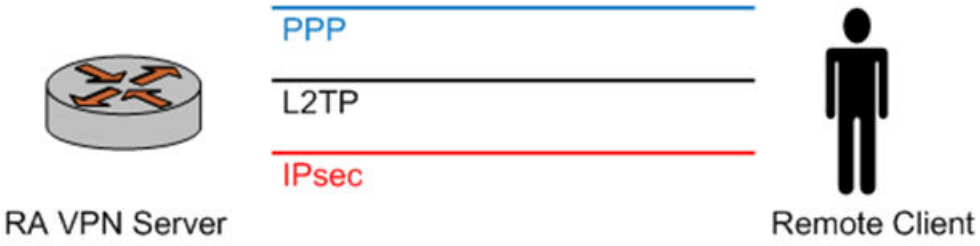
The following figure shows the general remote access scenario.

FIGURE 3 Remote access VPN



The following figure shows the one way option to implement a remote access VPN is by using Layer 2 Tunneling Protocol (L2TP) and IPsec.

FIGURE 4 Remote access VPN using L2TP and IPsec



In L2TP- and IPsec-based remote access VPN:

1. The remote host first establishes an IPsec tunnel with the VPN server.
2. The L2TP client and server then establish an L2TP tunnel on top of the IPsec tunnel.
3. Finally, a PPP session is established on top of the L2TP tunnel; that is, the PPP packets are encapsulated and sent and received inside the L2TP tunnel. The Brocade vRouter supports L2TP/IPsec-based remote access VPN. This deployment is described in Vyatta Remote Access VPN Reference Guide.

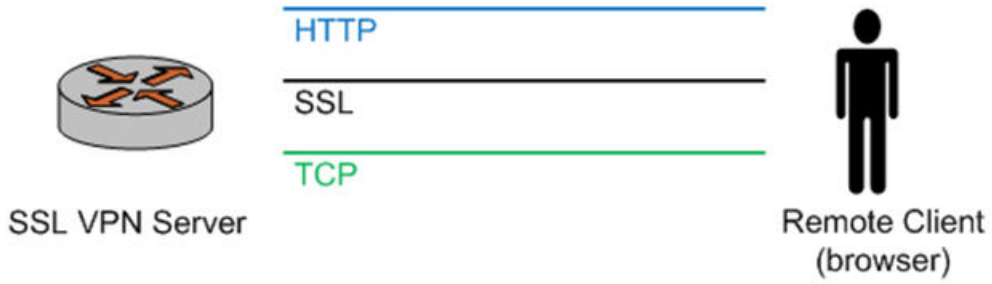
For more information about remote access VPN, refer to

OpenVPN

OpenVPN is an open-source VPN solution that employs the Secure Sockets Layer (SSL)protocol for security. OpenVPN supports both site-to-site and remote access modes of operation.

Because OpenVPN employs SSL in one mode of operation, and because it makes use of the open-source OpenSSL library, OpenVPN is sometimes referred as an SSL VPN solution. However, it should not be confused with SSL VPN as commonly understood to be a browser-based VPN product. They are quite different, and there is no interoperability between them. The following figure shows, a high level, browser-based SSL VPN works.

FIGURE 5 Browser-based SSL VPN

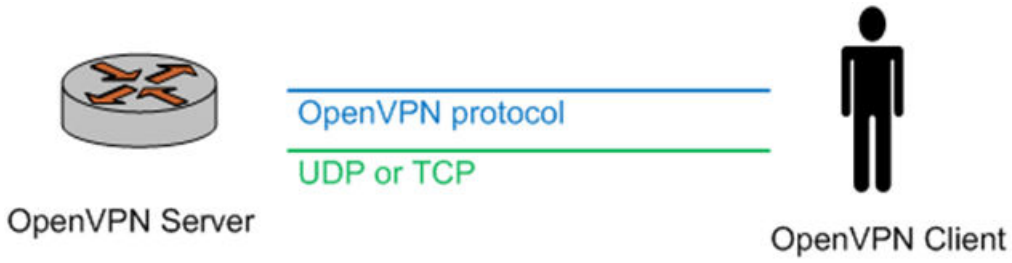


On the client side, the remote user points the web browser to a secure (HTTPS) web site. The browser establishes a TCP connection to the server, then an SSL protocol session within this connection, and finally an HTTP session on top of the SSL session. The SSL session provides a secure tunnel for authentication of the HTTP session, similar to logging into the secure web site of a bank.

In most such solutions, after the user has been authenticated, the browser dynamically downloads a fragment of code (for example, an ActiveX component) to be run on the host of the client. Such code can then, for example, create a virtual interface, so that VPN traffic can be routed through the tunnel. The application of the name SSL VPN to this solution refers to the fact that security is provided by the SSL protocol.

In contrast, OpenVPN implements its own communication protocol. This protocol is transported on top of UDP or TCP and provides a secure tunnel for VPN traffic. By default, UDP is used for better performance. In an OpenVPN solution, OpenVPN must be used on both tunnel endpoints. The following figure shows this scenario.

FIGURE 6 OpenVPN



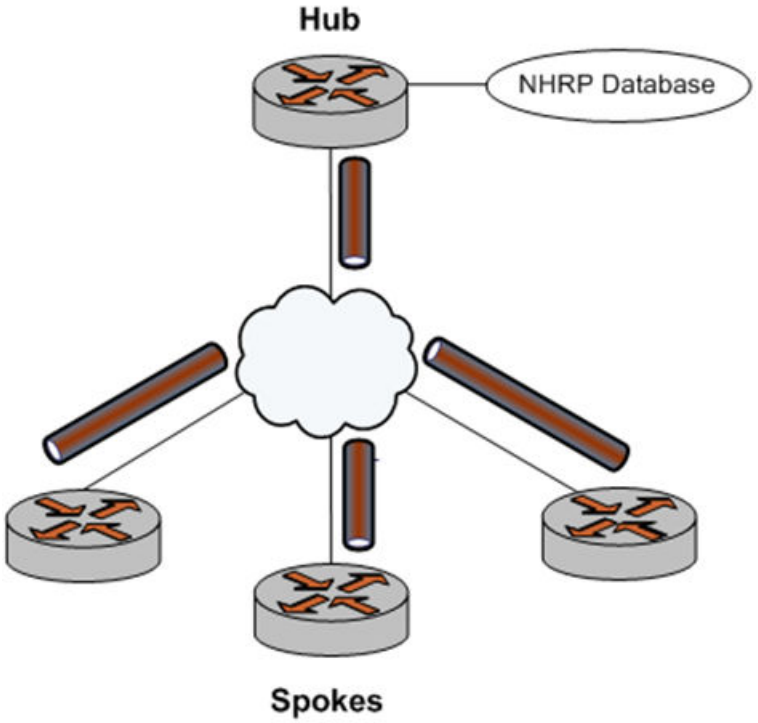
OpenVPN supports both site-to-site and remote access modes of operation. Support for OPENVPN on the Brocade vRouter is described in *Vyatta OpenVPN Reference Guide*.

Dynamic multipoint VPN

Dynamic multipoint VPN (DMVPN) is a VPN architecture that makes it easier to configure topologies in which many sites need to interconnect. Scaling an ordinary site-to-site IPsec VPN for such a network would be operationally complex: the tunnels between the sites would need to be fully meshed. In addition, each pair of endpoints requires its own network, which causes high IP address space consumption.

DMVPN uses multipoint Generic Routing Encapsulation (mGRE) tunnels with the Next Hop Reachability Protocol (NHRP) addressing service to allow a dynamic mesh of VPN tunnels that do not need to be statically configured. The following figure shows that the tunnels are protected using IPsec.

FIGURE 7 DMVPN



For more information about DMVPN, refer to *Brocade Vyatta Network OS DMVPN Configuration Guide*.

Comparing VPN Solutions

Each VPN solution has advantages and disadvantages. For example, IPsec-based solutions have various issues when NAT is involved; in addition, IPsec is complex and can be hard to troubleshoot. This section presents some deployment issues for the different solutions.

L2TP/IPsec

When an L2TP server is started, it listens on UDP port 1701 for incoming L2TP connections on the external interface of the VPN server. In the normal mode of operation, a VPN client establishes an IPsec session with the VPN server first, and then the L2TP connection is established within the IPsec tunnel.

Because the L2TP server is listening on port 1701, the server also accepts incoming L2TP connections that are not tunneled in IPsec. This acceptance may be an issue, for example, if a user establishes an L2TP VPN connection without the IPsec tunnel (note that the Windows VPN client does not allow this), in which case all the traffic from the user is in the clear; that is, not encrypted.

In a production environment, it is recommended that you prevent L2TP-only connections (L2TP connections not tunneled in IPsec). Depending on the setup, there are different ways to achieve this. For example:

- If the VPN server is deployed in a demilitarized zone (DMZ) and has a firewall in front of it, then the firewall can be configured to allow only IPsec traffic to the VPN server (in other words, UDP port 1701 is not allowed). This way, L2TP/IPsec connections can be established, but L2TP-only connections will be blocked.

If the VPN server is directly exposed, the firewall on the VPN server should be configured to disallow L2TP-only connections. For example, the following rule can be defined and applied to local on the external interface to allow L2TP/IPsec connections. (L2TP-only connections can be blocked by the default-drop rule.)

```
rule 10 {
                        action accept
                                destination {
                                        port 1701
                                }
                                ipsec {
                                        match-ipsec
                                }
                                protocol udp
            }
```

Pre-shared keys (L2TP/IPsec)

Pre-shared keys (PSKs) for L2TP/IPsec are easy to configure, both on the VPN server and on all the VPN clients. However, the same PSK must be used for all remote VPN users for the IPsec part of their VPN connections. The use of the same PSK can be a problem-for example when VPN access needs to be revoked for a particular user. Although access can be revoked at higher-level user authentication, the user still has the IPsec PSK and can still establish an IPsec session, which may not be desirable. To prevent the establishment of an IPSec session, a new PSK needs to be configured on the VPN server and all VPN clients.

X.509 certificates (L2TP/IPsec)

Using X.509 certificates with L2TP/IPsec avoids the issue with the PSK solution described in the preceding section. However, its usage presents its own challenges. Here are several examples.

- X.509 certificates must be generated using a Public Key Infrastructure (PKI) with a particular certificate authority (CA). This PKI can be either a commercial PKI (for example, VeriSign) or an in-house PKI established using either a commercial product (for example, a PKI appliance) or open-source software (for example, OpenSSL). Setting up an in-house PKI involves complex security issues.
- After the certificates are obtained, there remains the problem of securely distributing the user certificate to each of the remote VPN users. This distribution may involve, for example, physically taking a USB flash drive to the machine of each user and manually transferring the certificate.
- When using X.509 certificates with L2TP/IPsec, the configuration for the Windows VPN client becomes much more complicated than configuration using a pre-shared key. For this reason and the certificate-distribution problem, IT personnel may need to preconfigure user machines for remote access.