VYATTA, INC. | Vyatta System

VPN

REFERENCE GUIDE

Introduction to VPN
IPsec Site-to-Site VPN
Remote Access VPN
OpenVPN

Vyatta
Suite 200
1301 Shoreway Road
Belmont, CA 94002
vyatta.com
650 413 7200
1 888 VYATTA 1 (US and Canada)

COPYRIGHT

PROPRIETARY NOTICES

RELEASE DATE: July 2011

DOCUMENT REVISION. R6.3 v01

RELEASED WITH: R6.3.0

PART NO. A0-0222-10-0011

Table of Contents

Quick Reference to Commands

Use this section to help you quickly locate a command.

Quick List of Examples

Use this list to help you locate examples you'd like to try or look at.

Preface

This document describes the various deployment, installation, and upgrade options for Vyatta software.

This preface provides information about using this guide. The following topics are presented:

Intended Audience

This guide is intended for experienced system and network administrators. Depending on the functionality to be used, readers should have specific knowledge in the following areas:

- Networking and data communications
- TCP/IP protocols
- General router configuration
- Routing protocols
- Network administration
- Network security
- IP services

Organization of This Guide

This guide has the following aid to help you find the information you are looking for:

- Quick Reference to Commands

  Use this list to help you quickly locate commands.

- Quick List of Examples

  Use this list to help you locate examples you'd like to try or look at.

This guide has the following chapters:

Document Conventions

This guide uses the following advisory paragraphs, as follows.

WARNING *Warnings alert you to situations that may pose a threat to personal safety.*

CAUTION *Cautions alert you to situations that might cause harm to your system or damage to equipment, or that may affect service.*

NOTE *Notes provide information you might need to avoid problems or configuration errors.*

This document uses the following typographic conventions.

`Monospace`	Examples, command-line output, and representations of configuration nodes.
`bold Monospace`	Your input: something you type at a command line.
bold	Commands, keywords, and file names, when mentioned inline. Objects in the user interface, such as tabs, buttons, screens, and panes.
italics	An argument or variable where you supply a value.
<key>	A key on your keyboard, such as <Enter>. Combinations of keys are joined by plus signs ("+"), as in <Ctrl>+c.
[key1 | key2]	Enumerated options for completing a syntax. An example is [enable | disable].
num1–numN	A inclusive range of numbers. An example is 1–65535, which means 1 through 65535, inclusive.
arg1..argN	A range of enumerated values. An example is eth0..eth3, which means eth0, eth1, eth2, or eth3.
arg[*arg*...] *arg*[,*arg*...]	A value that can optionally represent a list of elements (a space-separated list and a comma-separated list, respectively).

Vyatta Publications

Full product documentation is provided in the Vyatta technical library. To see what documentation is available for your release, see the *Guide to Vyatta Documentation*. This guide is posted with every release of Vyatta software and provides a great starting point for finding the information you need.

Additional information is available on www.vyatta.com and www.vyatta.org.

Chapter 1: Introduction to VPN

This chapter provides a brief background to different types of virtual private network (VPN).

This chapter presents the following topics:

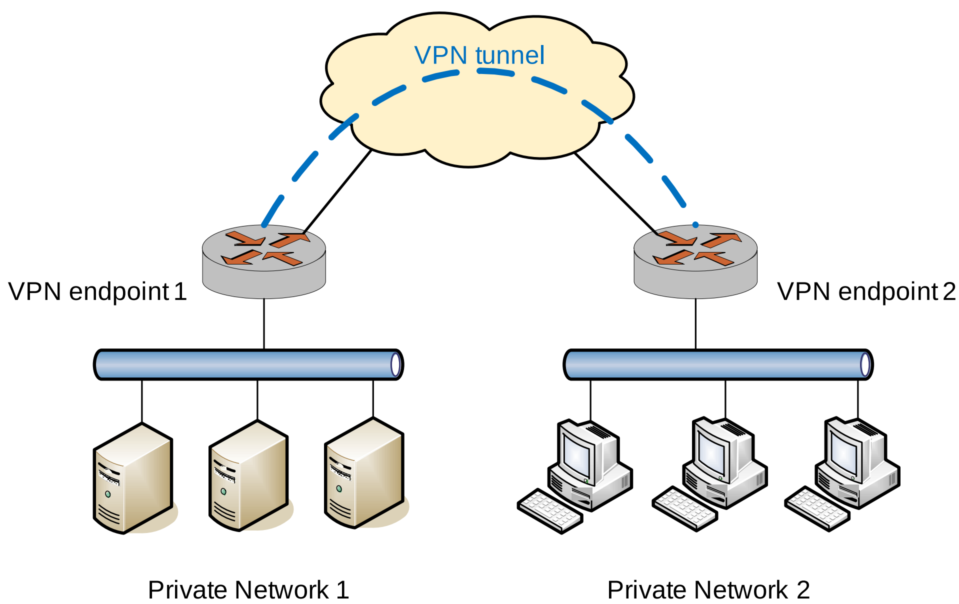
- Types of VPNs
- Supported Solutions
- Comparing VPN Solutions
- VPNs and NAT

Types of VPNs

The Vyatta system supports two different types of VPN solutions:

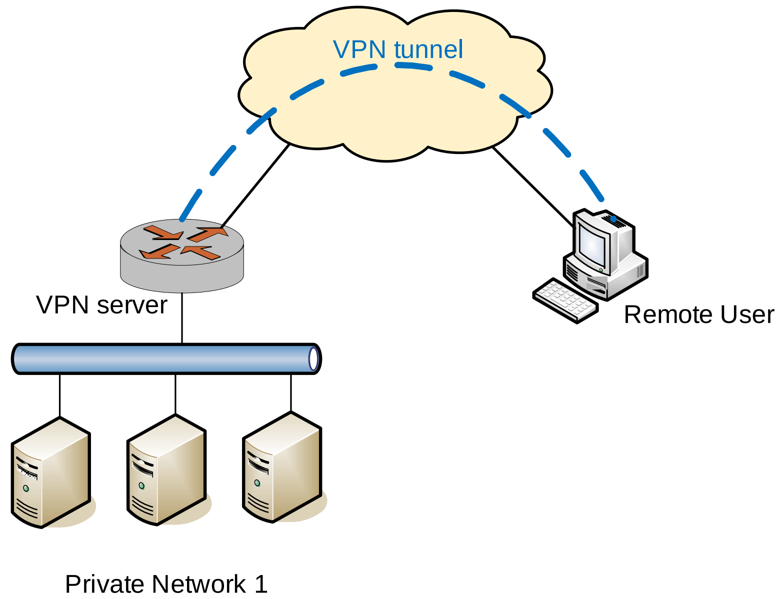
- "Site-to-site" VPN allows you to connect two or more sites separated by a wide area network such that they appear to be on a single private network. The sites are connected by a "tunnel" as shown in Figure 1-1.

Figure 1-1 Site-to-site VPN



- "Remote access" VPN allows a VPN tunnel to be established between a remote user and a VPN server. This allows, for example, a remote user to access the company network from home. This scenario is shown in Figure 1-2.

Figure 1-2 Remote access VPN



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

Supported Solutions

The Vyatta solution supports all of the following solutions:

- Site-to-Site with IPsec
- Remote Access Using PPTP
- Remote Access Using L2TP and IPsec
- Site-to-Site and Remote Access Using OpenVPN

Site-to-Site with IPsec

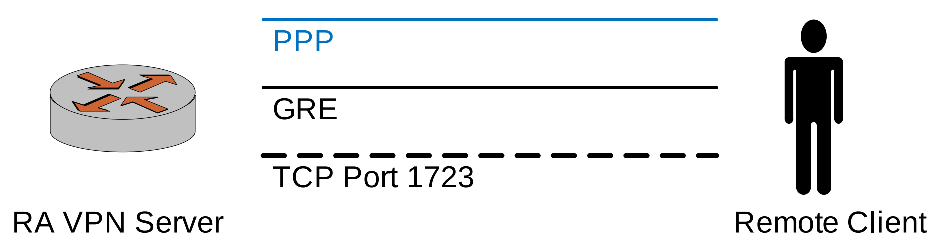
Figure 1-3 shows a site-to-site VPN functionality is implemented using IPsec.

Figure 1-3 Site-to-site - IPsec

Remote Access Using PPTP

Figure 1-4 shows a remote access VPN using Point-to-Point Tunneling Protocol (PPTP).

Figure 1-4 Remote-access - PPTP



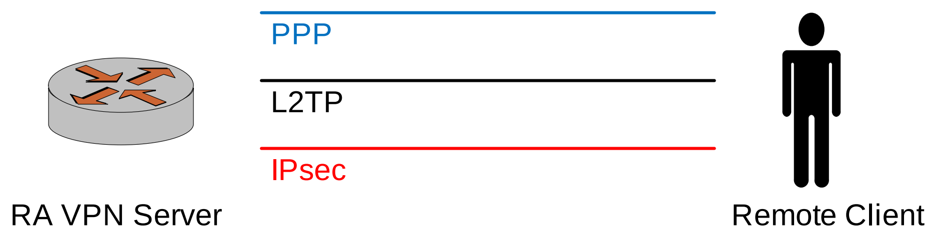
In this kind of solution:

1. The PPTP client establishes a TCP connection to server port 1723.
2. Through the connection above, the PPTP client and server establish a Generic Routing Encapsulation (GRE) tunnel.
3. A Point-to-Point Protocol (PPP) session is then established on top of the GRE tunnel; that is, the PPP packets are encapsulated and sent/received inside the GRE tunnel.

Remote Access Using L2TP and IPsec

Figure 1-5 shows a remote access VPN using Layer 2 Tunneling Protocol (L2TP) and IPsec.

Figure 1-5 Remote-access - L2TP/IPsec



In this kind of solution:

1 The remote host first establishes an IPsec tunnel with the VPN server.

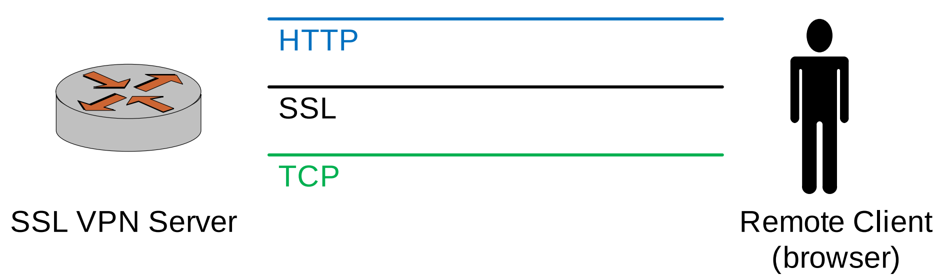
2 The L2TP client and server then establish an L2TP tunnel on top of the IPsec tunnel.

3 Finally, a PPP session is established on top of the L2TP tunnel; that is, the PPP packets are encapsulated and sent/received inside the L2TP tunnel.

Site-to-Site and Remote Access Using OpenVPN

OpenVPN is an open-source VPN solution that supports both site-to-site and remote access modes of operation. Although OpenVPN is sometimes referred to as a Secure Sockets Layer protocol (SSL) VPN solution, it should not be confused with "SSL VPN" as it is commonly understood, as a browser-based VPN product. At a high level, browser-based SSL VPN works as shown in Figure 1-6.

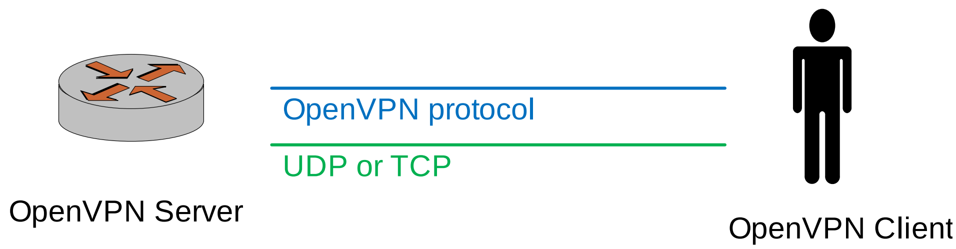
Figure 1-6 Browser-based SSL



In essence, 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 a bank's secure web site.

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 client's host. 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.

Figure 1-7 OpenVPN



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.

The reason that OpenVPN is sometimes called "SSL VPN" is that the SSL protocol is used (on top of the OpenVPN protocol) in one mode of operation and because OpenVPN uses the open-source OpenSSL library. As can be seen, an OpenVPN solution is quite different from the market definition of "SSL VPN," and there is no interoperability between them. In an OpenVPN solution, OpenVPN must be used on both tunnel endpoints.

Comparing VPN Solutions

Each solution has advantages and disadvantages. For example, PPTP sometimes raises concerns about security, while IPsec-based solutions have various issues when NAT is involved; also IPsec is complex and can be hard to troubleshoot. This section presents some deployment issues for the different solutions:

- PPTP
- L2TP/IPsec
- Pre-shared keys (L2TP/IPsec)
- X.509 certificates (L2TP/IPsec)

PPTP

The security of a PPTP solution is significantly affected by the strength of the passwords that users employ. Therefore, in a production environment, you should make an effort to use strong passwords for your users.

At the same time, stronger passwords have difficulties of their own—for example, they may be harder to remember. This could result in a user configuring the password in their VPN password such that the client “remembers” the password, or making a note of the password somewhere. This behavior undermines the added security of strong passwords.

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.

One issue is that since the L2TP server is listening on port 1701, it will also accept incoming L2TP connections that are not tunneled in IPsec. This may be a 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 user's traffic will be “in the clear;” that is, not encrypted.

In a production environment, it is recommended that that you prevent L2TP-only connections (that is, 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 only allow 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. This 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 will still possess the IPsec PSK and can still establish an IPsec session, which may not be desirable. To prevent this, 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 above. However, it 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 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.
- Once the certificates are obtained, there remains the problem of securely distributing the user certificate to each of the remote VPN users. This may involve, for example, physically taking a USB flash drive to each user's machine 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 because of the problem of distributing the certificates, IT personnel may need to preconfigure users' machines for remote access.

VPNs and NAT

When using NAT and VPN on the same device, special care must be taken to achieve desired results. Please refer to the *Masquerade NAT and VPN* configuration section in the *Vyatta NAT Reference Guide* for details.

Chapter 2: IPsec Site-to-Site VPN

This chapter explains how to set up IPsec site-to-site VPN connections on the Vyatta System.

This chapter presents the following topics:

- IPsec Site-to-Site VPN Configuration
- Monitoring IPsec Site-to-Site VPN
- IPsec Site-to-Site VPN Commands

IPsec Site-to-Site VPN Configuration

This section describes how to configure IPsec site-to-site Virtual Private Network (VPN) connections on the Vyatta System.

This section presents the following topics:

IPsec Site-to-Site VPN Overview

This section presents the following topics:

An IPsec Virtual Private Network (VPN) is a virtual network that operates across the public network, but remains “private” by establishing encrypted tunnels between two or more end points. VPNs provide:

- **Data integrity.** Data integrity ensures that no one has tampered with or modified data while it traverses the network. Data integrity is maintained with hash algorithms.
- **Authentication.** Authentication guarantees that data you receive is authentic; that is, that it originates from where it is supposed to, and not from someone masquerading as the source. Authentication is also ensured with hash algorithms.
- **Confidentiality.** Confidentiality ensures data is protected from being examined or copied while transiting the network. Confidentiality is accomplished using encryption.

An IP Security (IPsec) VPN secures communications and access to network resources for site-to-site access using encryption, authentication, and key management protocols. On a properly configured VPN, communications are secure, and the information that is passed is protected from attackers.

The Vyatta system currently supports site-to-site IPsec VPN connectivity. Site-to-site VPN connections are normally established between two (or more) VPN gateways and provide connectivity for user hosts, servers, and other devices at each location. Connectivity is normally based on IP source and destination network pairs, allowing multiple hosts to share the same tunnel between locations.

Site-to-site VPNs enable enterprises to create low-cost connectivity between offices. These site-to-site VPNs frequently replace more expensive WAN technologies such as private lines or Frame Relay.

IPsec Architecture

IPsec is a suite of protocols designed to provide end-to-end security at the network layer (Layer 3), using encryption and authentication techniques. From the point of view of IP networking equipment, encrypted packets can be routed just like any other ordinary IP packets. The only devices that require an IPsec implementation are the IPsec endpoints.

There are three main components of the IPsec architecture. These are:

- The Authentication Header (AH) protocol.
- The Encapsulating Security Payload (ESP) protocol
- The Internet Key Exchange (IKE) protocol, formerly referred to as ISAKMP/Oakley

Of these, the Vyatta system currently supports ESP, which encrypts the packet payload and prevents it from being monitored, and IKE, which provides a secure method of exchanging cryptographic keys and negotiating authentication and encryption methods.

The set of IPsec parameters describing a connection is called a *security policy*. The security policy describes how both endpoints will use security services, such as encryption, hash algorithms, and Diffie-Hellman groups, to communicate securely.

The IPsec peers negotiate a set of security parameters, which must match on both sides. Then they create a *security association* (SA). An IPsec SA describes the connection in one direction. For packets to travel in both directions in a connection, both an inbound and an outbound SA are required.

IPsec Phase 1 and Phase 2

The establishment of an IPsec connection takes place in two phases, called IKE phases:

- In IKE Phase 1, the two endpoints authenticate one another and negotiate keying material. This results in an encrypted tunnel used by Phase 2 for negotiating the ESP security associations.
- In IKE Phase 2, the two endpoints use the secure tunnel created in Phase 1 to negotiate ESP SAs. The ESP SAs are what are used to encrypt the actual user data that is passed between the two endpoints.

IKE Phase 1 establishes an ISAKMP SA (typically called an IKE SA). The IKE protocol is used to dynamically negotiate and authenticate keying material and other security parameters required to provide secure communications. IKE itself uses a combination of four protocols (including ISAKMP and Oakley) to dynamically manage keys in the context of IPsec.

If the IKE Phase 1 negotiation is successful, then the ISAKMP SA is established. The ISAKMP SA essentially contains the information from the "winning proposal" of the negotiation, recording the security encryption and keying material that was successfully negotiated. This creates a secure "control channel" where keys and other information for protecting Phase 2 negotiation are maintained. The ISAKMP SA encrypts only Phase 2 ESP security association negotiations, plus any IKE messages between the two endpoints.

An ISAKMP SA is maintained for a pre-determined lifetime. This lifetime is configured, not negotiated or passed between peers. The configured lifetime may be different between peers. When the configured lifetime expires, a new ISAKMP SA is negotiated.

IKE Phase 2 negotiations are also managed by the IKE protocol. Using the encryption provided by the security association, the security policy is used to try and negotiate a Phase 2 SA. The security policy includes information about the communicating hosts and subnets, as well as the ESP information for providing security services for the connection, such as encryption cipher and hash algorithm. If the IKE Phase 2 negotiation process is successful, a pair of ESP SAs (typically called IPsec SAs) is established—one inbound and one outbound—between the two endpoints. This is the encrypted VPN "tunnel" between the two endpoints. At this point, the user data can be exchanged through the encrypted tunnel.

Between any two IPsec VPN peers, there can be just one control channel for exchanging Phase 2 keying material. This means that between any two peers there will be just one ISAKMP SA on each peer.

However, between two VPN peers, any number of security policies can be defined. For example, you can define a security policy that creates a tunnel between two hosts, and a different security policy that creates a tunnel between a host and a subnet, or between two subnets. Since multiple tunnels can exist between two peers, this means that multiple IPsec SAs can be active at any time between two peers.

IKE Key Exchange

To be able to create an ISAKMP SA, the two devices must agree on all of the following:

- The encryption algorithm
- The bit-strength of the encryption key (Diffie-Hellman group)
- The authentication method
- The hash algorithm
- The authentication material (pre-shared secret)

All of this information is contained in an *IKE Phase 1 proposal*. A VPN gateway can be configured multiple Phase 1 proposals. Note that the SA lifetime is not negotiated.

During an IKE key exchange, one device (the *initiator*) sends the first packet in the exchange. This first packet consist of all the Phase 1 proposals configured for this VPN peer, in a sequence. This set of proposals informs the other gateway of what security and authentication policies it supports. The second device (the *responder*) inspects the set of proposals and returns the policy representing strongest security policy that both devices can agree on. If this process is successful, both devices agree on the parameter and the ISAKMP SA is established.

Once the ISAKMP SA has been established, the two devices can use this SA to encrypt the Phase 2 traffic where the two endpoints try to negotiate an IPsec SA for each matching security policy that has been configured between the two endpoints. Only after the IPsec SAs have been established can IPsec traffic be passed.

Different devices initiate IKE negotiation differently. Many VPN devices bring up VPN tunnels only on demand. These devices monitor traffic to see if it is “interesting”—that is, to see if it matches a configured security policy. Once the device receives traffic matching a specific security policy, the device will attempt to negotiate an IPsec SA that will be used to encrypt that traffic.

Other devices, including the Vyatta System, will attempt to initiate Phase 2 negotiations as soon as a correct policy configuration is entered. If both endpoints behave in this way, a race condition can occur, where duplicate IPsec SAs are created.

Encryption Ciphers

Ciphers are used to encrypt data, so that it cannot be read or monitored during transit. The Vyatta system supports the following encryption ciphers:

Table 2-1 Supported encryption ciphers

Cipher	Description
AES	The Advanced Encryption Standard (AES) is a U.S. government standard that was developed to take the place of DES, which has become easier to break using the more powerful computers available today. AES can run very quickly for a block cipher and can be implemented in a relatively small space. It has a block length which can vary between 192 and 256 bits, and a key length that can range between 128 and 256 bits in increments of 32 bits. The Vyatta system supports AES with a 128-bit key and with a 256-bit key.
3DES	Triple-DES is a variant of the Data Encryption Standard (DES). DES was formerly the most commonly used cipher, but in recent years has been compromised, and is no longer recommended as a first choice. The Vyatta system only supports Triple-DES. Triple-DES is an iterative block cipher, where DES is used in three consecutive iterations on the same block of text, where either two or three keys are used. The resulting ciphertext is much harder to break than DES. Using two keys yields 112 bits key strength; using 3 keys yields 168 bits key strength.

Hash Algorithms

A hash function is a cryptographic algorithm used for message authentication. A hash function takes a message of arbitrary length and produces an output of fixed length, called a message digest or fingerprint. Hash functions are used to verify that messages have not been tampered with.

The Vyatta system supports the following hash functions:

Table 2-2 Supported hash functions

Cipher	Description
MD5	MD5 is the most recent version of message digest algorithm. MD5 takes a message of arbitrary length and produces a 128-bit condensed digital representation, called a message digest. It is often used when a large file must be compressed and encrypted, then signed with a digital signature. Message digest is quite fast and efficient compared with SHA-1, because it uses primitive operations and produces a shorter message. However, it is not as secure as SHA-1, and has reportedly been compromised in some ways, though not yet in ways that make it insecure.
SHA-1	SHA stands for Secure Hash Algorithm, also known as the Secure Hash Standard. The SHA hash functions are five one-way cryptographic algorithms for computing a message digest. SHA-1 is an extension of the original SHA, and is the standard hash algorithm supported by the U.S. government. SHA-1 takes a message of arbitrary string length (the message must be smaller than 2^64 bits) and produces a 160-bit message digest. SHA-1 is slower than MD5, but it is more secure, because the additional bits in the message digest provide more protection from brute-force attacks.

Pre-Shared Keys

A pre-shared secret, or pre-shared key (PSK), is a method of authentication. The secret, or key, is a string agreed upon beforehand by both parties as key for authenticating the session. It is used to generate a hash such that each VPN endpoint can authenticate the other.

Note that the pre-shared secret, although an ordinary string, is not a “password.” It is actually used to generate a hashed key to form a “fingerprint” proving the identity of each endpoint. This means that long complex strings are more secure than short strings. Choose complex pre-shared secrets and avoid short ones, which can be more easily compromised by an attack.

The preshared secret is not passed during IKE negotiation. It is configured on both sides, and must match on both sides.

A pre-shared secret is an example of *symmetric cryptography:* the key is the same on both sides. Symmetric encryption algorithms are less computationally intensive than asymmetric algorithms, and are therefore faster. However, in symmetric cryptography, the two communicating parties must exchange keys in advance. Doing this securely can be a problem.

Pre-shared secret and digital signatures are the most common methods of IKE authentication. Pre-shared secret is an easy and effective way to quickly set up authentication with little administrative overhead. However, it has several drawbacks.

- If a pre-shared key is captured and no one is aware of it, the attacker has access to your network as long as that key is in use.
- Pre-shared secrets are manually configured, so they should be regularly changed. However, this task is often falls off the list of busy network administrators. Using pre-shared key values with remote users is equivalent to giviing them a password to your network.

NOTE *You should restrict the use of pre-shared keys to smaller, low-risk environments.*

Digital Signatures

Along with pre-shared key, RSA digital signatures are the most common means of IKE authentication.

An RSA digital signature is based on a cryptographic key that has two parts: a public part and a private part. One part (the public key) is widely shared, and may even be publicly distributed. The other part (the private key) remains secret. These keys are mathematically related but are independent, so that neither key is derivable from the other.

The key is used as input to a hash function; together, the key and the hash function form a signing function that, when applied to a document, creates a digital signature.

An RSA key can be used either to encrypt or authenticate, and this is based on two facts:

- Data encrypted with the agent's public key can only be decrypted by the agent, using the private key. This means that any peer can send information securely by encrypting it with the public key and forwarding it to the agent.
- Data processed with a hash function can be encrypted with the signer's private key—such data is said to be *digitally signed*. Since anyone with the public key can verify the digital signature, this communication can be accepted as authentically coming from the agent.

The algorithms that encrypt using RSA keys are very secure but extremely slow—so slow that it would be impracticable to encrypt an entire set of data using them. Instead, the agent produces a digital signature for the data, as follows:

1 A hash function is applied to the data to generate a message digest. The message digest is much shorter than the original data, and any peer possessing the same hash function can produce the identical message digest.

2 The private key is used to encrypt the message digest. This encrypted message digest is the digital signature.

3 The original message and the digital signature are all sent to the peer in an encrypted packet. (The encryption of the packet is independent of the digital signature.)

4 When the peer receives the packet, it decrypts the packet. Then it uses the sending agent's public key to decrypt the digital signature. This recovers the message digest.

5 The peer applies the hash function to the original message (which was also sent in the packet) and compares the resulting message digest to the message digest recovered from the digital signature.

    - If the message digests match, the peer can accept the communication as authentic.
    - If the message digests do not match, the peer must consider the communication to have been tampered with, or corrupted in some other way, and reject it.

When the system generates an RSA digital signature, it stores it in a file. The file containing the digital signature contains both the public key part and the private key part of the digital signature. When you view the RSA key, by looking at VPN configuration or by using the **show vpn ike rsa-keys** command, only the public key displays (along with any public keys configured for VPN peers). It is the public key that you should share with the other VPN peer.

By default, the RSA digital signature file for the local host is stored in the file **/etc/ipsec.d/rsa-keys/localhost.key**. When the key is required to authenticate the VPN peer, this is where the system looks for it. You can change the location and name of the file through configuration.

You can only have one RSA digital signature configured for the local host. If you generate a new key, it overwrites the previous key.

Diffie-Hellman Groups

Diffie-Hellman key exchange is a cryptographic protocol for securely exchanging encryption keys over an insecure communications channel, such as the Internet. Diffie-Hellman key exchange was developed in 1976 by Whitfield Diffie and Martin Hellman. It is based on two facts:

- Asymmetric encryption algorithms are much more secure than symmetric algorithms, which require that two parties exchange secret keys in advance. However,

- Asymmetric algorithms are much slower and much more computationally expensive than symmetric algorithms.

In a Diffie-Hellman key exchange, asymmetric cryptography is used at the outset of the communication (IKE Phase 1) to establish a shared key. Once the key has been exchanged, it can then be used symmetrically to encrypt subsequent communications (IKE Phase 2).

Diffie-Hellman key exchange uses a group of standardized global unique prime numbers and generators to provide secure asymmetric key exchange. The original specification of IKE defined four of these groups, called Diffie-Hellman groups or Oakley groups. Since then, a fifth has been defined.

The Vyatta system supports the following Diffie-Hellman groups:

Table 2-3 Supported Diffie-Hellman groups

Diffie-Hellman Group	Description
2	Diffie-Hellman group 2 is a modular exponentiation group (MODP). This group has a 1024-bit modulus.
5	Diffie-Hellman group 5 is a 1536-bit modular exponentiation (MODP) group. This group has a 1536-bit modulus.

IPsec Modes

IPsec, in general, supports two modes of operation: *aggressive mode*, and *main mode*.

Aggressive Mode

Aggressive mode was created to reduce latency during Phase 1 negotiation but it is vulnerable to attack. For this reason, the Vyatta system does not support aggressive mode.

Main Mode

Under ordinary conditions, establishing the ISAKMP SA requires several packets to be sent and received:

- The first two messages determine communications policy.
- The next two messages exchange Diffie-Hellman public data.
- The last two messages authenticate the Diffie-Hellman exchange.

This is the normal method of establishing a successful Phase 1 connection, and it is called *main mode*. This method provides the most security and privacy, because authentication information is not exchanged until a full Diffie-Hellman exchange has been negotiated and encryption has been enabled. The Vyatta system supports main mode.

Perfect Forward Secrecy

In Perfect Forward Secrecy (PFS), the private key is used to generate a temporary key (the session key) that is used for a short time and then discarded. Subsequent keys are independent of any previously created keys. This way, if a key is compromised, it does not affect any further keys, or compromise the security of data protected by other keys.

PFS provides a way to optimize both efficiently and security. Reasonably-sized keys are much more computationally efficient than large keys, but are also less secure. In PFS, you can use reasonably-sized keys and refresh them frequently.

Committing VPN Configuration Changes

An IPsec VPN connection includes multiple components, some of which are interdependent. For example, a VPN connection configuration requires a valid IKE group configuration, a valid ESP group configuration, and a valid tunnel configuration. In addition, the interface specified in the connection must be enabled for IPsec VPN. When you commit a VPN configuration, the Vyatta system performs a full verification on the configuration. If any required component is missing or incorrectly specified, the commit will fail.

For an IPsec VPN site-to-site connection configuration to successfully commit, all the following must be correctly configured:

- The interface and IP address must already be configured.
- The interface must be enabled for IPsec VPN.
- The peer must be configured.
- The IKE group specified in the peer configuration must be defined.
- The tunnel must be configured.
- The ESP group specified in the tunnel must be defined.
- The local IP address specified for the peer must be configured on the VPN-enabled interface.

In addition, please note that modifying global parameters (such as **ipsec-interface, auto-update,** or **nat-traversal**) requires an IPsec restart, and therefore restarts all tunnels.

Adding, modifying, or deleting a tunnel restarts only the modified tunnel. Modifying an existing IKE group or ESP group restarts any tunnel using the group. Changing authentication information (pre-shared key or RSA signature) does not result in a tunnel restart.

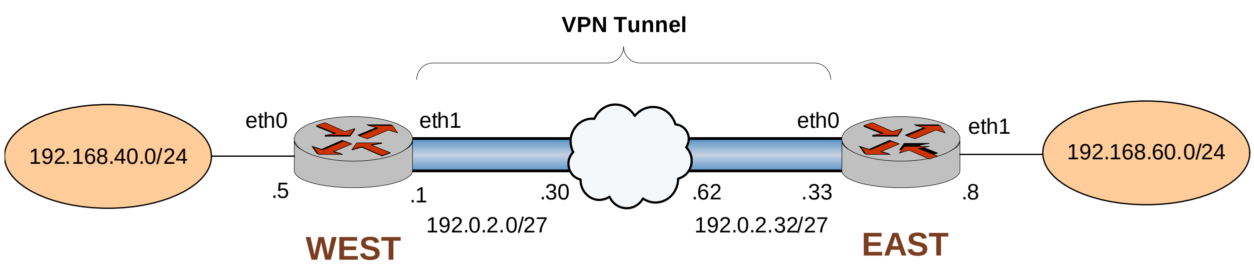
Configuring a Basic Site-to-Site Connection

This section presents the following topics:

- Configure WEST
- Configure EAST

This section presents a sample configuration for a basic IPsec tunnel between Vyatta Systems WEST and EAST. First WEST is configured, and then EAST. When you have finished, these peers will be configured as shown in Figure 2-1.

Figure 2-1 Basic site-to-site IPsec VPN connection



Before you begin:

- In this set of examples, we assume that you have two Vyatta systems, with host names configured WEST and EAST. (The example systems are configured with the host name in upper case.)
- Any Ethernet interface to be used for IPsec VPN must already be configured. In this example, you will need eth1 on WEST and eth0 on EAST, plus internal subnet information.
- The interface must be configured with the IP address you want to use as the source IP for packets sent to the peer VPN gateway. In this example, IP address 192.0.2.1 is defined on eth1 of WEST, and 192.0.2.33 is defined on eth0 of EAST. In examples where the interface is configured as a DHCP client, the interface address is set to **dhcp**.

***Tip:** Where public IP addresses would normally be used, the example uses RFC 3330 "TEST-NET" IP addresses (192.0.2.0/24)*

NOTE *The sending and receiving of ICMP redirects is disabled when IPsec VPN is configured.*

Configure WEST

This section presents the following topics:

- Enable VPN on WEST
- Configuring an IKE Group on WEST
- Configuring an ESP Group on WEST
- Creating the Connection to EAST

This section presents the following examples:

- Example 2-1 Enabling IPsec VPN on WEST
- Example 2-2 Configuring an IKE group on WEST
- Example 2-3 Configuring an ESP group on Vyatta system WEST
- Example 2-4 Creating a site-to-site connection from WEST to EAST

Enable VPN on WEST

In this section, you enable IPsec VPN on the interfaces that will be used in VPN connections. The VPN tunnel in the example configuration extends from eth1 on WEST through the wide area network to eth0 on EAST. This means that eth1 on WEST must have VPN enabled. The other interfaces on WEST need not.

To create an IPsec connection with another VPN gateway, you must specify the local IP address to be used as the source IP in packets sent to the destination gateway. This IP address:

- Must be one that is defined on a local Ethernet interface, and
- The interface must have IPsec VPN enabled on it

Example 2-1 enables IPsec VPN on eth1 on WEST. To do this, perform the following steps on WEST in configuration mode:

Example 2-1 Enabling IPsec VPN on WEST

Step	Command
Enable VPN on eth1 on WEST.	`vyatta@WEST#` **`set vpn ipsec ipsec-interfaces interface eth1`**
View IPsec interface configuration. Don’t commit yet.	`vyatta@WEST# show vpn ipsec ipsec-interfaces` `>  interface eth1`

Configuring an IKE Group on WEST

The IKE group allows you to pre-define a set of one or more proposals to be used in IKE Phase 1 negotiation, after which the ISAKMP security association (SA) can be set up. For each proposal in the group, the following information is defined:

- The cipher to be used to encrypt packets during IKE Phase 1
- The hash function to be used to authenticate packets during IKE Phase 1

The IKE group also has a configured lifetime, which is the duration of the ISAKMP SA. When the lifetime of the ISAKMP SA expires, a new Phase 1 negotiation takes place, and new encryption, hash, and keying information is established in a new pair of ISAKMP SAs.

The lifetime is an attribute of the IKE group as a whole. If the IKE group contains multiple proposals, the lifetime applies regardless of which proposal in the group is accepted.

Example 2-2 creates IKE group IKE-1W on WEST. This IKE group contains two proposals:

- Proposal 1 uses AES-256 as the encryption cipher and SHA-1 as the hash algorithm
- Proposal 2 uses AES-128 as the encryption cipher and SHA-1 as the hash algorithm

The lifetime of a proposal from this IKE group is set to 3600 seconds.

To create this IKE group, perform the following steps on WEST in configuration mode:

Example 2-2 Configuring an IKE group on WEST

Step	**Command**
Create the configuration node for proposal 1 of IKE group IKE-1W.	`vyatta@WEST#` **`set vpn ipsec ike-group IKE-1W proposal 1`**
Set the encryption cipher for proposal 1.	`vyatta@WEST#` **`set vpn ipsec ike-group IKE-1W proposal 1 encryption aes256`**
Set the hash algorithm for proposal 1.	`vyatta@WEST#` **`set vpn ipsec ike-group IKE-1W proposal 1 hash sha1`**
Set the encryption cipher for proposal 2. This also creates the configuration node for proposal 2 of IKE group IKE-1W.	`vyatta@WEST#` **`set vpn ipsec ike-group IKE-1W proposal 2 encryption aes128`**
Set the hash algorithm for proposal 2.	`vyatta@WEST#` **`set vpn ipsec ike-group IKE-1W proposal 2 hash sha1`**

Example 2-2 Configuring an IKE group on WEST

Set the lifetime for the whole IKE group.	`vyatta@WEST# set vpn ipsec ike-group IKE-1W lifetime 3600`

View the configuration for the IKE group. Don't commit yet.	`vyatta@WEST# show vpn ipsec ike-group IKE-1W`
	`> proposal 1 {`
	`>     encryption aes256`
	`>     hash sha1`
	`> }`
	`> proposal 2 {`
	`>     encryption aes128`
	`>     hash sha1`
	`> }`
	`> lifetime 3600`

Configuring an ESP Group on WEST

Encapsulated Security Payload (ESP) is an authentication protocol that provides authentication for IP packets, and it also encrypts them.

The ESP protocol negotiates a unique number for the session connection, called the Security Parameter Index (SPI). It also starts a numbering sequence for the packets and negotiates the hashing algorithm that will be used to authenticate packets.

The Vyatta system allows you to pre-define multiple ESP configurations. Each one is known as an "ESP group." ESP group includes the Phase 2 proposals, which contain the parameters needed to negotiate an IPsec security association:

- The cipher to be used to encrypt user data across the IPsec tunnel
- The hashing function to be used to authenticate packets in the IPsec tunnel
- The lifetime of the IPsec security association

Example 2-3 creates ESP group ESP-1W on Vyatta system WEST. This ESP group contains two proposals:

- Proposal 1 uses AES-256 as the encryption cipher and SHA-1 as the hash algorithm
- Proposal 2 uses Triple-DES as the encryption cipher and MD5 as the hash algorithm

The lifetime of a proposal from this ESP group is set to 1800 seconds.

To create this ESP group, perform the following steps on WEST in configuration mode:

Example 2-3 Configuring an ESP group on Vyatta system WEST

Step	Command
Create the configuration node for proposal 1 of ESP group ESP-1W.	vyatta@WEST# **set vpn ipsec esp-group ESP-1W proposal 1**
Set the encryption cipher for proposal 1.	vyatta@WEST# **set vpn ipsec esp-group ESP-1W proposal 1 encryption aes256**
Set the hash algorithm for proposal 1.	vyatta@WEST# **set vpn ipsec esp-group ESP-1W proposal 1 hash sha1**
Set the encryption cipher for proposal 2. This also creates the configuration node for proposal 2 of ESP group ESP-1W.	vyatta@WEST# **set vpn ipsec esp-group ESP-1W proposal 2 encryption 3des**
Set the hash algorithm for proposal 2.	vyatta@WEST# **set vpn ipsec esp-group ESP-1W proposal 2 hash md5**
Set the lifetime for the whole ESP group.	vyatta@WEST# **set vpn ipsec esp-group ESP-1W lifetime 1800**

View the configuration for the ESP group. Don't commit yet.	vyatta@WEST# show vpn ipsec esp-group ESP-1W
	> proposal 1 {
	> encryption aes256
	> hash sha1
	> }
	> proposal 2 {
	> encryption 3des
	> hash md5
	> }
	> lifetime 1800

Creating the Connection to EAST

In defining a site-to-site connection, you specify IPsec policy information (most of which is pre-configured as an IKE and ESP group) and the routing information for the two endpoints of the IPsec tunnel.

The local endpoint is the Vyatta system. The remote endpoint is the peer VPN gateway—this can be another Vyatta system, or it can be another IPsec-compliant router, an IPsec-capable firewall, or a VPN concentrator. For each end of the tunnel, you define the IP address and subnet mask of the local and remote subnets or hosts.

In all, you must specify:

- The IP address of the remote peer.
- The authentication mode that the peers will use to authenticate one another. The Vyatta system supports peer authentication by pre-shared secret (pre-shared key, or PSK), so you must also supply the string that will be used to generate the hashed key. Digital signatures and X.509 certificates are also supported.
- The IKE group to be used in the connection.
- The ESP group to be used in the connection.
- The IP address on this Vyatta system to use for the tunnel. This IP address must be pre-configured on the interface enabled for VPN.
- The communicating subnet or host for each end of the tunnel. You can define multiple tunnels for each VPN peer, and each tunnel can use a different security policy.

When supplying a preshared secret, keep the following in mind:

A pre-shared secret, or pre-shared key (PSK), is a method of authentication. The secret, or key, is a string agreed upon beforehand by both parties as key for authenticating the session. It is used to generate a hash such that each VPN endpoint can authenticate the other.

Note that the pre-shared secret, although an ordinary string, is not a "password." It is actually used to generate a hashed key to form a "fingerprint" proving the identity of each endpoint. This means that long complex strings are more secure than short strings. Choose complex pre-shared secrets and avoid short ones, which can be more easily compromised by an attack.

The preshared secret is not passed during IKE negotiation. It is configured on both sides, and must match on both sides.

A pre-shared secret is an example of *symmetric cryptography:* the key is the same on both sides. Symmetric encryption algorithms are less computationally intensive than asymmetric algorithms, and are therefore faster. However, in symmetric cryptography, the two communicating parties must exchange keys in advance. Doing this securely can be a problem.

Pre-shared secret and digital signatures are the most common methods of IKE authentication. Pre-shared secret is an easy and effective way to quickly set up authentication with little administrative overhead. However, it has several drawbacks.

- If a pre-shared key is captured and no one is aware of it, the attacker has access to your network as long as that key is in use.
- Pre-shared secrets are manually configured, so they should be regularly changed. However, this task is often falls off the list of busy network administrators. Using pre-shared key values with remote users is equivalent to giviing them a password to your network.

NOTE *You should restrict the use of pre-shared keys to smaller, low-risk environments.*

Example 2-4 defines a site-to-site connection to EAST.

- This connection is configured with a single tunnel:
  - — Tunnel 1 communicates between 192.168.40.0/24 on WEST and 192.168.60.0/24 on EAST, using ESP group ESP-1W.
- WEST uses IP address 192.0.2.1 on eth1.
- EAST uses IP address 192.0.2.33 on eth0.
- The IKE group is IKE-1W
- The authentication mode is pre-shared secret. The pre-shared secret is "test_key_1".

To configure this connection, perform the following steps on Vyatta system WEST in configuration mode:

Example 2-4 Creating a site-to-site connection from WEST to EAST

Step	Command
Create the node for EAST and set the authentication mode.	vyatta@WEST# **set vpn ipsec site-to-site peer 192.0.2.33 authentication mode pre-shared-secret**
Navigate to the node for the peer for easier editing.	vyatta@WEST# **edit vpn ipsec site-to-site peer 192.0.2.33** [edit vpn ipsec site-to-site peer 192.0.2.33]
Provide the string that will be used to generate encryption keys.	vyatta@WEST# **set authentication pre-shared-secret test_key_1** [edit vpn ipsec site-to-site peer 192.0.2.33]
Specify the default ESP group for all tunnels.	vyatta@WEST# **set default-esp-group ESP-1W** [edit vpn ipsec site-to-site peer 192.0.2.33]
Specify the IKE group.	vyatta@WEST# **set ike-group IKE-1W** [edit vpn ipsec site-to-site peer 192.0.2.33]
Identify the IP address on this Vyatta system to be used for this connection.	vyatta@WEST# **set local-ip 192.0.2.1** [edit vpn ipsec site-to-site peer 192.0.2.33]
Create a tunnel configuration, and provide the local subnet for this tunnel.	vyatta@WEST# **set tunnel 1 local subnet 192.168.40.0/24** [edit vpn ipsec site-to-site peer 192.0.2.33]
Provide the remote subnet for the tunnel.	vyatta@WEST# **set tunnel 1 remote subnet 192.168.60.0/24** [edit vpn ipsec site-to-site peer 192.0.2.33]
Return to the top of the configuration tree.	vyatta@WEST# **top**
Now commit the configuration.	vyatta@WEST# **commit**

Example 2-4 Creating a site-to-site connection from WEST to EAST

View the configuration for the site-to-site connection.	`vyatta@WEST# show vpn ipsec site-to-site peer 192.0.2.33`
	`authentication`
	`mode pre-shared-secret`
	`pre-shared-secret test_key_1`
	`}`
	`default-esp-group ESP-1W`
	`ike-group IKE-1W`
	`local-ip 192.0.2.1`
	`tunnel 1 {`
	`local {`
	`subnet 192.168.40.0/24`
	`}`
	`remote {`
	`subnet 192.168.60.0/24`
	`}`
	`}`

View IPsec interface configuration.	`vyatta@WEST# show vpn ipsec ipsec-interfaces` `interface eth1`
View Ethernet interface eth1 address configuration. **local-ip** is set to this address.	`vyatta@WEST# show interfaces ethernet eth1 address` `address 192.0.2.1/27`

Configure EAST

This section presents the following topics:

- Enabling VPN on EAST
- Configuring an IKE Group on EAST
- Configuring an ESP Group on EAST
- Creating the Connection to WEST

This section presents the following examples:

- Example 2-5 Enabling IPsec VPN on EAST
- Example 2-6 Configuring an IKE group on EAST
- Example 2-7 Configuring an ESP group on EAST
- Example 2-8 Creating a site-to-site connection from EAST to WEST

Enabling VPN on EAST

In this section, you enable IPsec VPN on the interfaces that will be used in VPN connections on Vyatta system EAST. The VPN tunnel in the example configuration extends from eth1 on WEST through the wide area network to eth0 on EAST. This means that eth0 on EAST must have VPN enabled. The other interfaces on EAST need not.

Example 2-5 enables IPsec VPN on eth0 on EAST. To do this, perform the following steps on EAST in configuration mode:

Example 2-5 Enabling IPsec VPN on EAST

Step	Command
Enable VPN on eth0 on EAST.	`vyatta@EAST#` **`set vpn ipsec ipsec-interfaces interface eth0`**
View IPsec interface configuration. Don't commit yet.	`vyatta@EAST# show vpn ipsec ipsec-interfaces` `>   interface eth0`

Configuring an IKE Group on EAST

Example 2-6 creates IKE group IKE-1E on EAST. This IKE group contains two proposals:

- Proposal 1 uses AES-256 as the encryption cipher and SHA-1 as the hash algorithm
- Proposal 2 uses AES-128 as the encryption cipher and SHA-1 as the hash algorithm

The lifetime of a proposal from this IKE group is set to 3600.

Note that these parameters correspond to those set in IKE-1W on WEST. You must ensure, in defining proposals, that the encryption ciphers and hash algorithms are such that the two peers will be able to agree on at least one combination.

To create this IKE group, perform the following steps on EAST in configuration mode:

Example 2-6 Configuring an IKE group on EAST

Step	Command
Create the configuration node for proposal 1 of IKE group IKE-1E.	`vyatta@EAST#` **`set vpn ipsec ike-group IKE-1E proposal 1`**
Set the encryption cipher for proposal 1.	`vyatta@EAST#` **`set vpn ipsec ike-group IKE-1E proposal 1 encryption aes256`**
Set the hash algorithm for proposal 1.	`vyatta@EAST#` **`set vpn ipsec ike-group IKE-1E proposal 1 hash sha1`**

Example 2-6 Configuring an IKE group on EAST

Set the encryption cipher for proposal 2. This also creates the configuration node for proposal 2 of IKE group IKE-1E.	vyatta@EAST# **set vpn ipsec ike-group IKE-1E proposal 2 encryption aes128**
Set the hash algorithm for proposal 2.	vyatta@EAST# **set vpn ipsec ike-group IKE-1E proposal 2 hash sha1**
Set the lifetime for the whole IKE group.	vyatta@EAST# **set vpn ipsec ike-group IKE-1E lifetime 3600**

View the configuration for the IKE group. Don't commit yet.	vyatta@EAST# show vpn ipsec ike-group IKE-1E
	> proposal 1 {
	> encryption aes256
	> hash sha1
	> }
	> proposal 2 {
	> encryption aes128
	> hash sha1
	> }
	> lifetime 3600

Configuring an ESP Group on EAST

Example 2-7 creates ESP group ESP-1E on EAST. This ESP group contains two proposals:

- Proposal 1 uses AES-256 as the encryption cipher and SHA-1 as the hash algorithm
- Proposal 2 uses Triple-DES as the encryption cipher and MD5 as the hash algorithm

The lifetime of a proposal from this ESP group is set to 1800 seconds.

To create this ESP group, perform the following steps on EAST in configuration mode:

Example 2-7 Configuring an ESP group on EAST

Step	Command
Create the configuration node for proposal 1 of ESP group ESP-1E.	vyatta@EAST# **set vpn ipsec esp-group ESP-1E proposal 1**
Set the encryption cipher for proposal 1.	vyatta@EAST# **set vpn ipsec esp-group ESP-1E proposal 1 encryption aes256**

Example 2-7 Configuring an ESP group on EAST

Set the hash algorithm for proposal 1.	`vyatta@EAST# set vpn ipsec esp-group ESP-1E proposal 1 hash sha1`
Set the encryption cipher for proposal 2. This also creates the configuration node for proposal 2 of ESP group ESP-1E.	`vyatta@EAST# set vpn ipsec esp-group ESP-1E proposal 2 encryption 3des`
Set the hash algorithm for proposal 2.	`vyatta@EAST# set vpn ipsec esp-group ESP-1E proposal 2 hash md5`
Set the lifetime for the whole ESP group.	`vyatta@EAST# set vpn ipsec esp-group ESP-1E lifetime 1800`

View the configuration for the ESP group. Don't commit yet.	`vyatta@EAST# show vpn ipsec esp-group ESP-1E`
	`> proposal 1 {`
	`>     encryption aes256`
	`>     hash sha1`
	`> }`
	`> proposal 2 {`
	`>     encryption 3des`
	`>     hash md5`
	`> }`
	`> lifetime 1800`

Creating the Connection to WEST

Example 2-8 defines a site-to-site connection to WEST. In this example:

- This connection is configured with a single tunnel:
  - — Tunnel 1 communicates between 192.168.60.0/24 on EAST and 192.168.40.0/24 on WEST, using ESP group ESP-1E.
- EAST uses IP address 192.0.2.33 on eth0.
- WEST uses IP address 192.0.2.1 on eth1.
- The IKE group is IKE-1E.
- The authentication mode is pre-shared secret. The pre-shared secret is "test_key_1".

To configure this connection, perform the following steps on EAST in configuration mode:

Example 2-8 Creating a site-to-site connection from EAST to WEST

Step	Command
Create the node for WEST and set the authentication mode	vyatta@EAST# **set vpn ipsec site-to-site peer 192.0.2.1 authentication mode pre-shared-secret**
Navigate to the node for the peer for easier editing	vyatta@EAST# **edit vpn ipsec site-to-site peer 192.0.2.1** [edit vpn ipsec site-to-site peer 192.0.2.1]
Provide the string that will be used to generate encryption keys.	vyatta@EAST# **set authentication pre-shared-secret test_key_1** [edit vpn ipsec site-to-site peer 192.0.2.1]
Specify the default ESP group for all tunnels.	vyatta@EAST# **set default-esp-group ESP-1E** [edit vpn ipsec site-to-site peer 192.0.2.1]
Specify the IKE group.	vyatta@EAST# **set ike-group IKE-1E** [edit vpn ipsec site-to-site peer 192.0.2.1]
Identify the IP address on this Vyatta system to be used for this connection.	vyatta@EAST# **set local-ip 192.0.2.33** [edit vpn ipsec site-to-site peer 192.0.2.1]
Create a tunnel configuration, and provide the local subnet for this tunnel.	vyatta@EAST# **set tunnel 1 local subnet 192.168.60.0/24** [edit vpn ipsec site-to-site peer 192.0.2.1]
Provide the remote subnet for the tunnel.	vyatta@EAST# **set tunnel 1 remote subnet 192.168.40.0/24** [edit vpn ipsec site-to-site peer 192.0.2.1]
Return to the top of the configuration tree.	vyatta@EAST# **top**
Now commit the configuration.	vyatta@EAST# **commit**

Example 2-8 Creating a site-to-site connection from EAST to WEST

View the configuration for the site-to-site connection.	<pre>vyatta@EAST# **show vpn ipsec site-to-site peer 192.0.2.1**
	   authentication
	      mode pre-shared-secret
	      pre-shared-secret test_key_1
	   }
	   default-esp-group ESP-1E
	   ike-group IKE-1E
	   local-ip 192.0.2.33
	   tunnel 1 {
	      local {
	         subnet 192.168.60.0/24
	      }
	      remote {
	         subnet 192.168.40.0/24
	      }
	   }</pre>

View IPsec interface configuration.	vyatta@EAST# **show vpn ipsec ipsec-interfaces** interface eth0
View Ethernet interface eth0 address configuration. **local-ip** is set to this address.	vyatta@EAST# **show interfaces ethernet eth0 address** address 192.0.2.33/27

Authenticating with RSA Digital Signatures

This section presents the following topics:

- Generate a Digital Signature on WEST
- Generate a Digital Signature on EAST
- Record EAST's Public Key on WEST
- Modify WEST's Connection to EAST
- Record WEST's Public Key on EAST
- Modify EAST's Connection to WEST

In this set of examples, you modify the VPN connection configured in the previous set of examples between WEST and EAST ("Configuring a Basic Site-to-Site Connection" on page 20). The site-to-site connection created in that set of examples used pre-shared keys for authentication. This set of examples modifies the connection to use RSA digital signatures for authentication.

Generate a Digital Signature on WEST

In this example, you generate WEST's digital signature. This signature will have two parts: a public part (the public key) and a private part (the private key). The public key will be shared with EAST; the private key will remain secret.

To generate an RSA digital signature for system WEST, perform the following steps in operational mode.

Example 2-9 Generating a digital signature on WEST

Step	Command
Generate the key.	`vyatta@WEST>` **`generate vpn rsa-key`**
The system warns you that the existing RSA key file will be overwritten. You have the opportunity to exit the key generation process by pressing <Ctrl>+c.	`A local RSA key file already exists and will be overwritten` `<CTRL>C to exit: 8`
The system indicates the location of the file where the key will be written.	`Generating rsa-key to /config/ipsec.d/rsa-keys/localhost.key`

The system displays the public portion of the generated key.
By default, this key (including the private portion of the key) is stored in /config/ipsec.d/rsa-keys/ localhost.key
	`Your new local RSA key has been generated`
	`The public portion of the key is:`
	
	`0sAQPEOQvukvkv1ofuO8gEKp7IFFZz4lQqMZyVMInoQKUU/T0iKSK/0NSH9L`
	`drr8yQUFayzKag6wM7ASXWXKyt0LS1Gn8tJVsjKGaOkFgLREtVJD3pRzoc7D`
	`SUOBViCD6f/TloTkPepRUtW1bmYev2H7tajSO0K0`
	`rqu+7nlocZI0ppMAyF6CS+Wd5W1JBpVGL+EkKfyEl9RagKxRW82XJbgY4LG7`
	`7K2YDN90Wd2GgMY3kf+YJLIzFEt/xRbh2/380FMpdaUYcbY31o/5PedUutJC`
	`K5RMwl+IJGaxrKf1OmCQfzXlkM09ijZx8kzPIlBk`
	`5hulZrbUWjzBJdFcwFAyPM3yCuv3+ndFX00t3ZLfKu+/wX595J`
	
	`vyatta@WEST>`

Generate a Digital Signature on EAST

In this example, you generate EAST's digital signature. This signature will have two parts: a public part (the public key) and a private part (the private key). The public key will be shared with WEST; the private key will remain secret.

To generate an RSA digital signature for system EAST, perform the following steps in operational mode.

Example 2-10 Generating a digital signature on EAST

Step	Command
Generate the key.	`vyatta@EAST>` **`generate vpn rsa-key`**
The system warns you that the existing RSA key file will be overwritten. You have the opportunity to exit the key generation process by pressing <Ctrl>+c.	`A local RSA key file already exists and will be overwritten` `<CTRL>C to exit: 5`
The system indicates the location of the file where the key will be written.	`Generating rsa-key to /config/ipsec.d/rsa-keys/localhost.key`

The system displays the public portion of the generated key.
By default, this key (including the private portion of the key) is stored in /config/ipsec.d/rsa-keys/ localhost.key
	`Your new local RSA key has been generated`
	`The public portion of the key is:`
	
	`0sAQOVBIJL+rIkpTuwh8FPeceAF0bhgLr++W51bOAIjFbRDbR8gX3Vlz6wiU`
	`bMgGwQxWlYQiqsCeacicsfZx/amlEn9PkSE4e7tqK/JQo40L5C7gcNM24mup`
	`1d+0WmN3zLb9Qhmq5q3pNJxEwnVbPPQeIdZMJxnb1+lA8DPC3SIxJM/3at1/`
	`KrwqCAhX3QNFY/zNmOtFogELCeyl4+d54wQljA+3dwFAQ4bboJ7YIDs+rqOR`
	`xWd3l3I7IajT/pLrwr5eZ8OA9NtAedbMiCwxyuyUbznxXZ8Z/MAi3xjL1pjY`
	`yWjNNiOij82QJfMOrjoXVCfcPn96ZN+Jqk+KknoVeNDwzpoahFOseJREeXzk`
	`w3/lkMN9N1`
	
	`vyatta@EAST>`

Record EAST's Public Key on WEST

In this example, you record the public key you have obtained from EAST. The key is then saved under a name that you can refer to in site-to-site configuration.

A digital signature can be typed in manually, but digital signatures are lengthy and difficult to type. It is generally easier to copy the digital signature into the clipboard of your system and then paste it into the configuration. You do this in a number of ways; for example:

- Receive the public key from the operator of the VPN peer in an e-mail—perhaps an e-mail protected by a PGP signature. Copy the key text into your clipboard.
- From an X.509 certificate, provided by a Certificate Agency.
- Connect to the VPN peer directly through a Telnet or SSH control session. View view the public portion of the key using a **show** command, select the text, and copy the key text into your clipboard.

Example 2-11 pastes EAST's public key into RSA configuration. The name "EAST-key" is used as the identifier of the key.

Before you begin, copy EAST's public key into your clipboard.

If you are in operational mode on WEST, enter configuration mode now and perform the following steps:

Example 2-11 Record EAST's public key on WEST

Step	Command
Specify a name for EAST's public key and paste EAST's public key into the configuration.	`vyatta@WEST#` **`set vpn rsa-keys rsa-key-name EAST-key rsa-key`** `0sAQOVBIJL+rIkpTuwh8FPeceAF0bhgLr++W51bOAIjFb RDbR8gX3Vlz6wiUbMgGwQxWlYQiqsCeacicsfZx/amlEn9PkSE4e7tqK/JQo40L5C7gcNM24mup1d+0WmN3zLb9Qhmq5q3pNJxEwnVbPPQeIdZMJxnb1+lA8DPC3SIxJM/3at1/KrwqCAhX3QNFY/zNmOtFogELCeyl4+d54wQljA+3dwFAQ4bboJ7YIDs+rqORxWd3l3I7IajT/pLrwr5eZ8OA9NtAedbMiCwxyuyUbznxXZ8Z/MAi3xjL1pjYyWjNNiOij82QJfMOrjoXVCfcPn96ZN+Jqk+KknoVeNDwzpoahFOseJREeXzkw3/lkMN9N1`
Commit the configuration.	`vyatta@WEST#` **`commit`**
View the configuration for RSA keys. Since you have not changed the configuration for the local host's key, it does not display.	`vyatta@WEST#` **`show vpn rsa-keys`** `rsa-key-name EAST-key {` `rsa-key 0sAQOVBIJL+rIkpTuwh8FPeceAF0bhgLr++ W51bOAIjFbRDbR8gX3Vlz6wiUbMgGwQxWlYQiqsCeacicsfZx/amlEn9PkSE4e7tqK/JQo40L5C7gcNM24mup1d+0WmN3zLb9Qhmq5q3pNJxEwnVbPPQeIdZMJxnb1+lA8DPC3SIxJM/3at1/KrwqCAhX3QNFY/zNmOtFogELCeyl4+d54wQljA+3dwFAQ4bboJ7YIDs+rqORxWd3l3I7IajT/pLrwr5eZ8OA9NtAedbMiCwxyuyUbznxXZ8Z/MAi3xjL1pjYyWjNNiOij82QJfMOrjoXVCfcPn96ZN+Jqk+KknoVeNDwzpoahFOseJREeXzkw3/lkMN9N1` `}`  `vyatta@WEST#`

Modify WEST's Connection to EAST

Example 2-12 modifies the connection from WEST to EAST to use RSA digital signatures for authentication. In this example:

- The authentication mode is changed from pre-shared secret to RSA digital signatures.
- EAST's public key is specified as the remote key, under the identifier configured in the previous step (see "Record EAST's Public Key on WEST" on page 34).

To modify the site-to-site connection to use RSA configuration, perform the following steps:

Example 2-12 Configure WEST for RSA authentication

Step	Command
Remove the pre-shared key.	`vyatta@WEST#` **`delete vpn ipsec site-to-site peer 192.0.2.33 authentication pre-shared-secret`**
Change the authentication mode	`vyatta@WEST#` **`set vpn ipsec site-to-site peer 192.0.2.33 authentication mode rsa`**
Provide the identifier for EAST's digital signature.	`vyatta@WEST#` **`set vpn ipsec site-to-site peer 192.0.2.33 authentication rsa-key-name EAST-key`**
Commit the configuration.	`vyatta@WEST#` **`commit`**

View the modified configuration for the site-to-site connection.	`vyatta@WEST#` **`show vpn ipsec site-to-site peer 192.0.2.33`**
	`authentication {`
	`mode rsa`
	`rsa-key-name EAST-key`
	`}`
	`default-esp-group ESP-1W`
	`ike-group IKE-1W`
	`local-ip 192.0.2.1`
	`tunnel 1 {`
	`local {`
	`subnet 192.168.40.0/24`
	`}`
	`remote {`
	`subnet 192.168.60.0/24`
	`}`
	`}`

View IPsec interface configuration.	`vyatta@WEST#` **`show vpn ipsec ipsec-interfaces`** `interface eth1`
View Ethernet interface eth1 address configuration. **local-ip** is set to this address.	`vyatta@WEST#` **`show interfaces ethernet eth1 address`** `address 192.0.2.1/27`

Record WEST's Public Key on EAST

Example 2-13 pastes WEST's public key into RSA configuration. The name "WEST-key" is used as the identifier of the key.

Before you begin, copy WEST's public key into your clipboard.

If you are in operational mode on EAST, enter configuration mode now and perform the following steps:

Example 2-13 Record WEST's public key on EAST

Step	Command
Specify a name for WEST's public key and paste WEST's public key into the configuration.	vyatta@EAST# **set vpn rsa-keys rsa-key-name WEST-key rsa-key** 0sAQPEOQvukvkv1ofuO8gEKp7IFFZz4lQqMZyVMIno QKUU/T0iKSK/0NSH9Ldrr8yQUFayzKag6wM7ASXWXKyt0LS1Gn8tJVsjKGaO kFgLREtVJD3pRzoc7DSUOBViCD6f/TloTkPepRUtW1bmYev2H7tajSO0K0 rqu+7nlocZI0ppMAyF6CS+Wd5W1JBpVGL+EkKfyEl9RagKxRW82XJbgY4LG7 7K2YDN90Wd2GgMY3kf+YJLIzFEt/xRbh2/380FMpdaUYcbY31o/5PedUutJC K5RMwl+IJGaxrKf1OmCQfzXlkM09ijZx8kzPIlBk 5hulZrbUWjzBJdFcwFAyPM3yCuv3+ndFX00t3ZLfKu+/wX595J
Commit the configuration.	vyatta@EAST# **commit**

View the configuration for RSA keys.
Since you have not changed the configuration for the local host's key, it does not display.
	vyatta@EAST# **show vpn rsa-keys**
	
	rsa-key-name WEST-key {
	        rsa-key 0sAQPEOQvukvkv1ofuO8gEKp7IFFZz4lQqMZy
	VMInoQKUU/T0iKSK/0NSH9Ldrr8yQUFayzKag6wM7ASXWXKyt0LS1Gn8tJVs
	jKGaOkFgLREtVJD3pRzoc7DSUOBViCD6f/TloTkPepRUtW1bmYev2H7tajSO
	0K0
	rqu+7nlocZI0ppMAyF6CS+Wd5W1JBpVGL+EkKfyEl9RagKxRW82XJbgY4LG7
	7K2YDN90Wd2GgMY3kf+YJLIzFEt/xRbh2/380FMpdaUYcbY31o/5PedUutJC
	K5RMwl+IJGaxrKf1OmCQfzXlkM09ijZx8kzPIlBk
	5hulZrbUWjzBJdFcwFAyPM3yCuv3+ndFX00t3ZLfKu+/wX595J
	    }
	
	vyatta@EAST#

Modify EAST's Connection to WEST

Example 2-14 modifies the connection from EAST to WEST to use RSA digital signatures for authentication.

In this example:

- The authentication mode is changed from pre-shared secret to RSA digital signatures.
- WEST's public key is specified as the remote key, under the identifier configured in the previous step (see "Record WEST's Public Key on EAST" on page 36).

To modify the site-to-site connection to use RSA configuration, perform the following steps:

Example 2-14 Configure EAST for RSA authentication

Step	Command
Remove the pre-shared key.	`vyatta@EAST#` **`delete vpn ipsec site-to-site peer 192.0.2.1 authentication pre-shared-secret`**
Change the authentication mode	`vyatta@EAST#` **`set vpn ipsec site-to-site peer 192.0.2.1 authentication mode rsa`**
Provide the identifier for WEST's digital signature.	`vyatta@EAST#` **`set vpn ipsec site-to-site peer 192.0.2.1 authentication rsa-key-name WEST-key`**
Commit the configuration.	`vyatta@EAST#` **`commit`**

View the modified configuration for the site-to-site connection.	`vyatta@EAST#` **`show vpn ipsec site-to-site peer 192.0.2.1`**
	`authentication {`
	`mode rsa`
	`rsa-key WEST-key`
	`}`
	`default-esp-group ESP-1E`
	`ike-group IKE-1E`
	`local-ip 192.0.2.33`
	`tunnel 1 {`
	`local {`
	`subnet 192.168.60.0/24`
	`}`
	`remote {`
	`subnet 192.168.40.0/24`
	`}`
	`}`

View IPsec interface configuration.	`vyatta@EAST#` **`show vpn ipsec ipsec-interfaces`** `interface eth0`
View Ethernet interface eth0 address configuration. **local-ip** is set to this address.	`vyatta@EAST#` **`show interfaces ethernet eth0 address`** `address 192.0.2.33/27`

Authenticating with X.509 Certificates

This section presents the following topics:

- Modify WEST's Connection to EAST
- Modify EAST's Connection to WEST

In this set of examples, you modify the VPN connection configured in the basic set of examples between WEST and EAST ("Configuring a Basic Site-to-Site Connection" on page 20). The site-to-site connection created in that set of examples used pre-shared keys for authentication. This set of examples modifies the configuration to use X.509 certificates for authentication.

In general, the procedure for obtaining the files required to authenticate using X.509 certificates is as follows:

1. Generate the private key and a certificate signing request (CSR) (based on the public key). This can be accomplished using generate vpn x509 key-pair <name> (for example, **generate vpn x509 key-pair west**, where **west.key** is the private key and **west.csr** is the certificate signing request file—both created in **/config/auth**).
2. Send the CSR file (for example, **west.csr**) to the certificate authority (CA) and receive back a server certificate (for example, **west.crt**), the CA certificate (for example, **ca.crt**), and potentially, a certificate revocation list (CRL) file. This procedure varies according to the CA being used.

At this point the configuration can be modified to use these files.

Modify WEST's Connection to EAST

Example 2-15 modifies the connection from WEST to EAST to use X.509 certificates for authentication. In this example:

- The authentication mode is changed from pre-shared secret to X.509 certificates.
- The certificate for the peer is identified using its Distinguished Name information. This is the information prompted for when creating the certificate signing request (CSR) file on the peer.
- The locations of the CA certificate, the server certificate, and the private key file for the server are specified.

To modify the site-to-site connection to use X.509 certificate authentication, perform the following steps:

Example 2-15 Configure WEST for X.509 certificate authentication

Step	Command
Remove the pre-shared key.	`vyatta@WEST# delete vpn ipsec site-to-site peer 192.0.2.33 authentication pre-shared-secret`
Change the authentication mode.	`vyatta@WEST# set vpn ipsec site-to-site peer 192.0.2.33 authentication mode x509`
Specify the 'distinguished name' of the certificate for the peer.	`vyatta@WEST# set vpn ipsec site-to-site peer 192.0.2.33 authentication remote-id "C=US, ST=CA, O=ABC Company, CN=east, E=root@abcco.com"`

Example 2-15 Configure WEST for X.509 certificate authentication

Specify the location of the CA certificate.	`vyatta@WEST#` **`set vpn ipsec site-to-site peer 192.0.2.33 authentication x509 ca-cert-file /config/auth/ca.crt`**
Specify the location of the server certificate.	`vyatta@WEST#` **`set vpn ipsec site-to-site peer 192.0.2.33 authentication x509 cert-file /config/auth/west.crt`**
Specify the location of the server key file.	`vyatta@WEST#` **`set vpn ipsec site-to-site peer 192.0.2.33 authentication x509 key file /config/auth/west.key`**
Specify the password for the server key file.	`vyatta@WEST#` **`set vpn ipsec site-to-site peer 192.0.2.33 authentication x509 key password testpwd-west`**
Commit the configuration.	`vyatta@WEST#` **`commit`**
View the modified configuration for the site-to-site connection.	see below
View IPsec interface configuration.	`vyatta@WEST#` **`show vpn ipsec ipsec-interfaces`** `interface eth1`
View Ethernet interface eth1 address configuration. **local-ip** is set to this address.	`vyatta@WEST#` **`show interfaces ethernet eth1 address`** `address 192.0.2.1/27`

View the modified configuration for the site-to-site connection:

```
vyatta@WEST# show vpn ipsec site-to-site peer 192.0.2.33
   authentication {
      mode x509
      remote-id “C=US, ST=CA, O=ABC Company, CN=east,
                 E=root@abcco.com”
      x509 {
         ca-cert-file /config/auth/ca.crt
         cert-file /config/auth/west.crt
         key {
            file /config/auth/west.key
            password testpwd-west
         }
      }
   }
   default-esp-group ESP-1W
   ike-group IKE-1W
   local-ip 192.0.2.1
   tunnel 1 {
      local {
         subnet 192.168.40.0/24
      }
      remote {
         subnet 192.168.60.0/24
      }
   }
```

Modify EAST's Connection to WEST

Example 2-16 modifies the connection from EAST to WEST to use X.509 certificates for authentication.

In this example:

- The authentication mode is changed from pre-shared secret to X.509 certificates.
- The certificate for the peer is identified using its 'distinguished name' information. This is the information prompted for when creating the certificate signing request (CSR) file.
- The locations of the CA certificate, the server certificate, and the private key file for the server are specified.

To modify the site-to-site connection to use X.509 certificate authentication, perform the following steps:

Example 2-16 Configure EAST for X.509 certificate authentication

Step	Command
Remove the pre-shared key.	vyatta@EAST# **delete vpn ipsec site-to-site peer 192.0.2.1 authentication pre-shared-secret**
Change the authentication mode	vyatta@EAST# **set vpn ipsec site-to-site peer 192.0.2.1 authentication mode x509**
Specify the 'distinguished name' of the certificate for the peer.	vyatta@EAST# **set vpn ipsec site-to-site peer 192.0.2.1 authentication remote-id "C=US, ST=CA, O=ABC Company, CN=west, E=root@abcco.com"**
Specify the location of the CA certificate.	vyatta@EAST# **set vpn ipsec site-to-site peer 192.0.2.1 authentication x509 ca-cert-file /config/auth/ca.crt**
Specify the location of the server certificate.	vyatta@EAST# **set vpn ipsec site-to-site peer 192.0.2.1 authentication x509 cert-file /config/auth/east.crt**
Specify the location of the server key file.	vyatta@EAST# **set vpn ipsec site-to-site peer 192.0.2.1 authentication x509 key file /config/auth/east.key**
Specify the password for the server key file.	vyatta@EAST# **set vpn ipsec site-to-site peer 192.0.2.1 authentication x509 key password testpwd-east**
Commit the configuration.	vyatta@EAST# **commit**

Example 2-16 Configure EAST for X.509 certificate authentication

View the modified configuration for the site-to-site connection.	`vyatta@EAST# show vpn ipsec site-to-site peer 192.0.2.1`
	`  authentication {`
	`    mode x509`
	`    remote-id "C=US, ST=CA, O=ABC Company, CN=west,`
	`          E=root@abcco.com"`
	`    x509 {`
	`      ca-cert-file /config/auth/ca.crt`
	`      cert-file /config/auth/east.crt`
	`      key {`
	`        file /config/auth/east.key`
	`        password testpwd-east`
	`      }`
	`    }`
	`  }`
	`  default-esp-group ESP-1E`
	`  ike-group IKE-1E`
	`  local-ip 192.0.2.33`
	`  tunnel 1 {`
	`    local {`
	`      subnet 192.168.60.0/24`
	`    }`
	`    remote {`
	`      subnet 192.168.40.0/24`
	`    }`
	`  }`

View IPsec interface configuration.	`vyatta@EAST# show vpn ipsec ipsec-interfaces` ` interface eth0`
View Ethernet interface eth0 address configuration. **local-ip** is set to this address.	`vyatta@EAST# show interfaces ethernet eth0 address` ` address 192.0.2.33/27`

Defining a VPN Connection to a Peer with a Dynamic IP Address

This section presents the following topics:

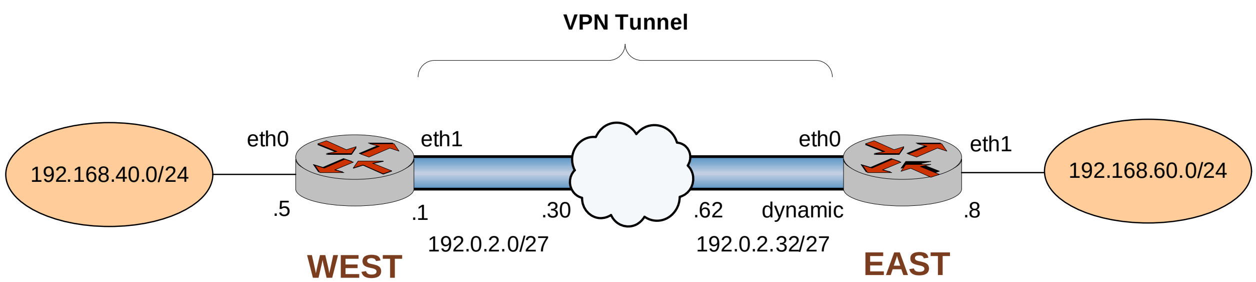
- Configure WEST
- Configure EAST

This section presents a sample configuration for a connection between WEST and EAST, where EAST has a dynamic IP address (it is configured as a DHCP client). In this example:

- EAST has a dynamic IP address from WEST's point of view.
- WEST retains its fixed IP address.

When you have finished, these systems will be configured as shown in Figure 2-2.

Figure 2-2 IPsec VPN connection with dynamic IP address



Before you begin:

- This example assumes that you have already configured a basic site-to-site connection using a preshared key between WEST and EAST, as explained in the section "Configuring a Basic Site-to-Site Connection" on page 20". Only the relevant changes to that configuration are presented here.

Configure WEST

Example 2-17 defines configuration changes for a new site-to-site connection to EAST.

- The main change is the IP address specification of the peer. This is set to 0.0.0.0 to represent "any" IP address. Because the IP address of the peer is unknown, WEST will not initiate connections to the peer. It will only receive connections from the peer.

To configure this connection, perform the following steps on WEST in configuration mode:

Example 2-17 Creating a site-to-site connection to a peer with a dynamic IP address

Step	Command
Delete the previous configuration.	`vyatta@WEST#` **`delete vpn ipsec site-to-site peer 192.0.2.33`**
Create the node for EAST and set the authentication mode.	`vyatta@WEST#` **`set vpn ipsec site-to-site peer 0.0.0.0 authentication mode pre-shared-secret`**
Navigate to the node for the peer for easier editing.	`vyatta@WEST#` **`edit vpn ipsec site-to-site peer 0.0.0.0`** `[edit vpn ipsec site-to-site peer 0.0.0.0]`

Example 2-17 Creating a site-to-site connection to a peer with a dynamic IP address

Provide the string that will be used to generate encryption keys.	`vyatta@WEST#` **`set authentication pre-shared-secret test_key_1`** `[edit vpn ipsec site-to-site peer 0.0.0.0]`
Specify thedefault ESP group for all tunnels.	`vyatta@WEST#` **`set default-esp-group ESP-1W`** `[edit vpn ipsec site-to-site peer 0.0.0.0]`
Specify the IKE group.	`vyatta@WEST#` **`set ike-group IKE-1W`** `[edit vpn ipsec site-to-site peer 0.0.0.0]`
Identify the IP address on this Vyatta system to be used for this connection.	`vyatta@WEST#` **`set local-ip 192.0.2.1`** `[edit vpn ipsec site-to-site peer 0.0.0.0]`
Create a tunnel configuration, and provide the local subnet for this tunnel.	`vyatta@WEST#` **`set tunnel 1 local subnet 192.168.40.0/24`** `[edit vpn ipsec site-to-site peer 0.0.0.0]`
Provide the remote subnet for the tunnel.	`vyatta@WEST#` **`set tunnel 1 remote subnet 192.168.60.0/24`** `[edit vpn ipsec site-to-site peer 0.0.0.0]`
Return to the top of the configuration tree.	`vyatta@WEST#` **`top`**
Commit the configuration.	`vyatta@WEST#` **`commit`**

View the configuration for the site-to-site connection.	`vyatta@WEST#` **`show vpn ipsec site-to-site peer 0.0.0.0`**
	`  authentication`
	`    mode pre-shared-secret`
	`    pre-shared-secret test_key_1`
	`  }`
	`  default-esp-group ESP-1W`
	`  ike-group IKE-1W`
	`  local-ip 192.0.2.1`
	`  tunnel 1 {`
	`    local {`
	`      subnet 192.168.40.0/24`
	`    }`
	`    remote {`
	`      subnet 192.168.60.0/24`
	`    }`
	`  }`

View IPsec interface configuration.	`vyatta@WEST#` **`show vpn ipsec ipsec-interfaces`** ` interface eth1`
View Ethernet interface eth1 address configuration. **local-ip** is set to this address.	`vyatta@WEST#` **`show interfaces ethernet eth1 address`** ` address 192.0.2.1/27`

Configure EAST

The connection from EAST to WEST only requires a minor change from that configured in the section “Configuring a Basic Site-to-Site Connection” on page 20.

- WEST retains its fixed IP, so no modification is required to the remote peer IP address.
- EAST has a dynamic local IP, so that must change. The **dhcp-interface** option specifies the DHCP client interface.

To configure this connection, perform the following steps on EAST in configuration mode:

Example 2-18 Specify that the local IP is dynamic.

<table>
<tr><th>Step</th><th>Command</th></tr>
<tr><td>Remove the existing local-ip configuration so that doesn’t conflict with the dhcp-interface configuration that will be set.</td><td><pre>vyatta@EAST# delete vpn ipsec site-to-site peer 192.0.2.1 local-ip
[edit]</pre></td></tr>
<tr><td>Specify the DHCP client interface to use for the connection.</td><td><pre>vyatta@EAST# set vpn ipsec site-to-site peer 192.0.2.1 dhcp-interface eth0
[edit]</pre></td></tr>
<tr><td>Commit the configuration.</td><td><pre>vyatta@EAST# commit</pre></td></tr>
<tr><td>View the configuration for the site-to-site connection.</td><td><pre>vyatta@EAST# show vpn ipsec site-to-site peer 192.0.2.1
   authentication
      mode pre-shared-secret
      pre-shared-secret test_key_1
   }
   default-esp-group ESP-1E
   dhcp-interface eth0
   ike-group IKE-1E
   tunnel 1 {
      local {
         subnet 192.168.60.0/24
      }
      remote {
         subnet 192.168.40.0/24
      }
   }</pre></td></tr>
<tr><td>View IPsec interface configuration.</td><td><pre>vyatta@EAST# show vpn ipsec ipsec-interfaces
 interface eth0</pre></td></tr>
</table>

Example 2-18 Specify that the local IP is dynamic.

View Ethernet interface eth0 address configuration. It is set to **dhcp** which configures it as a DHCP client. This is the setting required by **dhcp-interface**.	`vyatta@EAST# show interfaces ethernet eth0` ` address dhcp`

Defining a VPN Connection to a Peer Using Dynamic DNS

This section presents the following topics:

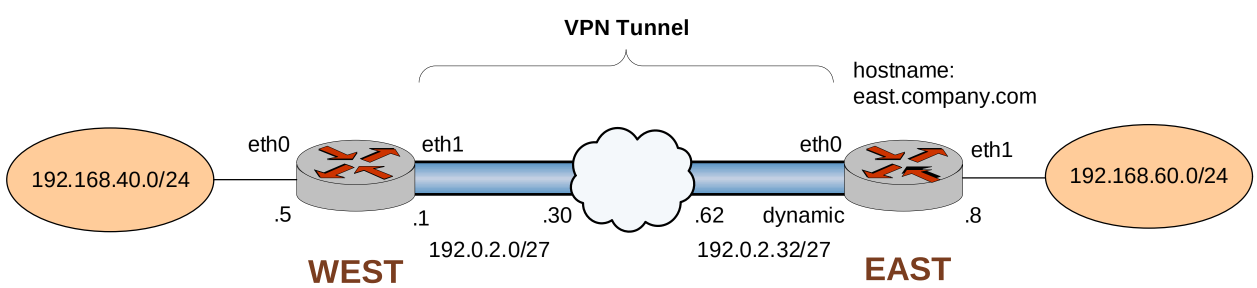
- Configure WEST
- Configure EAST

This section presents a sample configuration for a connection between WEST and EAST, where EAST has a dynamic IP address (it is configured as a DHCP client) and is configured for dynamic DNS. In this example:

- EAST has a dynamic IP address from WEST's point of view but WEST can initiate connections to EAST because EAST's hostname remains constant even though its IP address may change.
- WEST retains its fixed IP address.

When you have finished, these systems will be configured as shown in Figure 2-3.

Figure 2-3 IPsec VPN connection with dynamic IP address and dynamic DNS



Before you begin:

- This example assumes that you have already configured a basic site-to-site connection using a preshared key between WEST and EAST, as explained in the section "Configuring a Basic Site-to-Site Connection" on page 20". Only the relevant changes to that configuration are presented here.

Configure WEST

Example 2-19 defines configuration changes for a new site-to-site connection to EAST.

- The main change is the IP address specification of the peer. This is set to the hostname for EAST: "east.company.com". This is the hostname that is configured on EAST with the dynamic DNS provider. Because the IP address for EAST can be resolved, WEST can either initiate IPsec connections to, or receive IPsec connections from EAST.
- The other important change is to configure **auto-update** so that if EAST's IP address changes, the IPsec connection to EAST will be restarted automatically.

To configure this connection, perform the following steps on WEST in configuration mode:

Example 2-19 Creating a site-to-site connection to a peer with a dynamic IP address and using dynamic DNS

Step	Command
Delete the previous configuration.	`vyatta@WEST# delete vpn ipsec site-to-site peer 192.0.2.33`
Create the node for EAST and set the authentication mode.	`vyatta@WEST# set vpn ipsec site-to-site peer east.company.com authentication mode pre-shared-secret`
Navigate to the node for the peer for easier editing.	`vyatta@WEST# edit vpn ipsec site-to-site peer east.company.com` `[edit vpn ipsec site-to-site peer east.company.com]`
Provide the string that will be used to generate encryption keys.	`vyatta@WEST# set authentication pre-shared-secret test_key_1` `[edit vpn ipsec site-to-site peer east.company.com]`
Specify the default ESP group for all tunnels.	`vyatta@WEST# set default-esp-group ESP-1W` `[edit vpn ipsec site-to-site peer east.company.com]`
Specify the IKE group.	`vyatta@WEST# set ike-group IKE-1W` `[edit vpn ipsec site-to-site peer east.company.com]`
Identify the IP address on this Vyatta system to be used for this connection.	`vyatta@WEST# set local-ip 192.0.2.1` `[edit vpn ipsec site-to-site peer east.company.com]`
Create a tunnel configuration, and provide the local subnet for this tunnel.	`vyatta@WEST# set tunnel 1 local subnet 192.168.40.0/24` `[edit vpn ipsec site-to-site peer east.company.com]`
Provide the remote subnet for the tunnel.	`vyatta@WEST# set tunnel 1 remote subnet 192.168.60.0/24` `[edit vpn ipsec site-to-site peer east.company.com]`

Example 2-19 Creating a site-to-site connection to a peer with a dynamic IP address and using dynamic DNS

Return to the top of the configuration tree.	`vyatta@WEST#` **`top`**
Commit the configuration.	`vyatta@WEST#` **`commit`**

View the configuration for the site-to-site connection.	`vyatta@WEST#` **`show vpn ipsec site-to-site peer east.company.com`**
	`authentication`
	`mode pre-shared-secret`
	`pre-shared-secret test_key_1`
	`}`
	`default-esp-group ESP-1W`
	`ike-group IKE-1W`
	`local-ip 192.0.2.1`
	`tunnel 1 {`
	`local {`
	`subnet 192.168.40.0/24`
	`}`
	`remote {`
	`subnet 192.168.60.0/24`
	`}`
	`}`

View IPsec interface configuration.	`vyatta@WEST#` **`show vpn ipsec ipsec-interfaces`** `interface eth1`
View Ethernet interface eth1 address configuration. **local-ip** is set to this address.	`vyatta@WEST#` **`show interfaces ethernet eth1 address`** `address 192.0.2.1/27`
Specify that the IPsec connection should be refreshed every 60 seconds - in case the peer's IP address changes. If this happens the new IP address will be resolved via the dynamic DNS service provider.	`vyatta@WEST#` **`set vpn ipsec auto-update 60`** `[edit]`
Commit the configuration.	`vyatta@WEST#` **`commit`**
View the configuration.	`vyatta@WEST#` **`show vpn ipsec auto-update`** `auto-update 60`

Configure EAST

The connection from EAST to WEST only requires a minor change from that configured in the section "Configuring a Basic Site-to-Site Connection" on page 20.

- WEST retains its fixed IP, so no modification is required to the remote peer IP address.
- EAST has a dynamic local IP, so that must change. The **dhcp-interface** option specifies the DHCP client interface.
- EAST is also configured for dynamic DNS, in this case with service provider DynDNS. See the "Configuring Dynamic DNS" section in the *Vyatta Services Reference Guide* for details on configuring a system for dynamic DNS.

To configure this connection, perform the following steps on EAST in configuration mode:

Example 2-20 Specify that the local IP is dynamic.

Step	Command
Remove the existing **local-ip** configuration so that doesn't conflict with the **dhcp-interface** configuration that will be set.	`vyatta@EAST#` **`delete vpn ipsec site-to-site peer 192.0.2.1 local-ip`** `[edit]`
Specify the DHCP client interface to use for the connection.	`vyatta@EAST#` **`set vpn ipsec site-to-site peer 192.0.2.1 dhcp-interface eth0`** `[edit]`
Commit the configuration.	`vyatta@EAST#` **`commit`**

View the configuration for the site-to-site connection.	`vyatta@EAST#` **`show vpn ipsec site-to-site peer 192.0.2.1`**
	`authentication`
	`mode pre-shared-secret`
	`pre-shared-secret test_key_1`
	`}`
	`default-esp-group ESP-1E`
	`dhcp-interface eth0`
	`ike-group IKE-1E`
	`tunnel 1 {`
	`local {`
	`subnet 192.168.60.0/24`
	`}`
	`remote {`
	`subnet 192.168.40.0/24`
	`}`
	`}`

Example 2-20 Specify that the local IP is dynamic.

View IPsec interface configuration.	`vyatta@EAST# show vpn ipsec ipsec-interfaces` ` interface eth0`
View Ethernet interface eth0 address configuration. It is set to **dhcp** which configures it as a DHCP client. This is the setting required by **dhcp-interface**.	`vyatta@EAST# show interfaces ethernet eth0` ` address dhcp`

Display the dynamic DNS configuration on EAST:

Example 2-21 Display the dynamic DNS configuration.

Step	Command

View the dynamic DNS configuration.	`vyatta@EAST# show service dns dynamic`
	` interface eth0 {`
	`   service dyndns {`
	`     host-name east.company.com`
	`     login test`
	`     password testpassword`
	`   }`
	` }`

Defining a VPN Connection with NAT

This section presents the following topics:

- Configure WEST
- Configure EAST

Native IPsec packets are encapsulated using Encapsulated Security Payload (ESP). In these packets, the IP addresses are embedded within the encapsulated packet. This causes problems when IPsec packets must traverse a NAT gateway.

When performing Network Address Translation (NAT), the NAT gateway substitutes its own source IP address (and sometimes a port number), for the original source IP and port on outgoing packets. The NAT device listens for a reply, and when a response packet is received, the NAT device reverses the translation so that the incoming packet can arrive at the correct destination. This allows IP addresses within a private network to be "hidden" from external networks.

NAT does not work well with IPsec, because the IP addresses are embedded within the payload of the encapsulated packet. For a number of reasons, this means that the IPsec peer cannot be located behind the NAT device.

The IPsec NAT Traversal protocol (NAT-T, RFCs 3947 and 3948) allows each IPsec packet to be re-encapsulated within a UDP packet, which can be handled correctly by the NAT device. NAT-T runs on top of IPsec. To support NAT-T, the firewall must be set to allow all of the following:

- IKE through UDP port 500
- IPsec NAT-T through UDP port 4500
- ESP

Some gateway devices pre-allow all of these in a feature called "IPsec Passthrough." However, IPsec Passthrough is incompatible with NAT traversal. IPsec Passthrough devices recognize the IPsec-in-UDP packets and incorrectly attempt passthrough-type operations on the packets. This corrupts the packets in such a way that NAT-T no longer works.

NOTE *If you enable NAT traversal support, make sure you DISABLE IPsec Passthrough on the NAT device.*

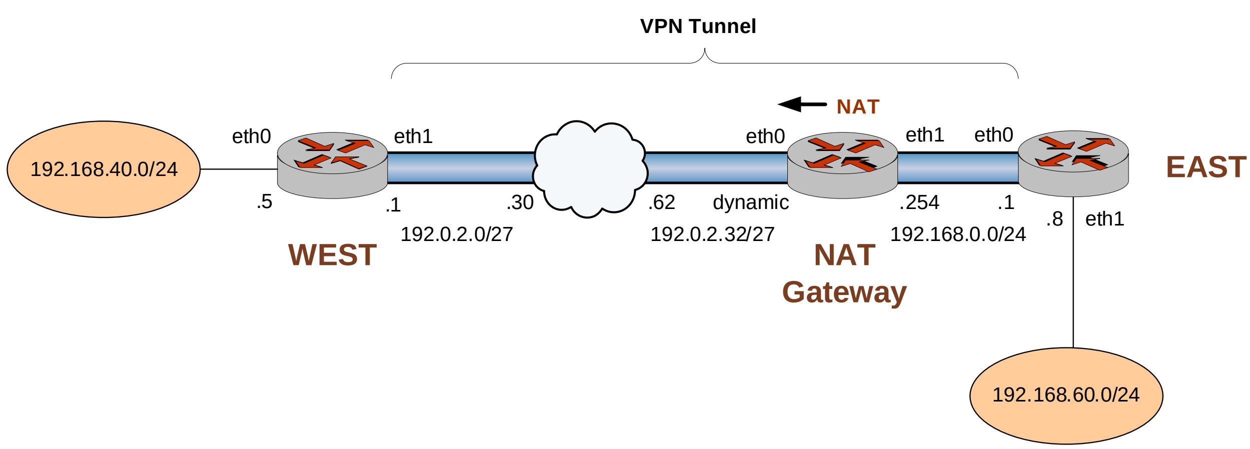
This section presents a sample configuration for a NATted connection between WEST and EAST. It is similar to the previous example except that in this case EAST resides behind a NAT device. In this example:

- EAST resides behind a NAT device, and has a dynamic IP address from WEST's point of view.
- WEST retains its fixed IP address.

This configuration is similar to something you might see for an IPsec endpoint that is behind a DSL connection, where the DSL peer's public IP address is dynamic and the DSL peer is performing NAT.

When you have finished, these systems will be configured as shown in Figure 2-4.

Figure 2-4 IPsec VPN connection with dynamic IP address and NAT



Before you begin:

- This example assumes that you have already configured a basic site-to-site connection using a preshared key between WEST and EAST, as explained in the section "Configuring a Basic Site-to-Site Connection" on page 20. Only the relevant changes to that configuration are presented here.
- This example also assumes that a Masquerade NAT rule is configured on a Vyatta device called "NAT Gateway" in front of EAST as follows:

Example 2-22 NAT configuration on the NAT Gateway

Step	Command

Show the configuration.	`vyatta@NATGwy# **show service nat rule 10**`
	`outbound-interface eth0`
	`source {`
	`address 192.168.0.0/24`
	`}`
	`type masquerade`

Configure WEST

To allow for EAST's dynamic IP address via NAT, WEST must specify that the VPN will be traversing NAT, that addresses from certain private networks are allowed, that addresses from the same subnet as the local private subnet are not allowed, and that a new site-to-site connection is required to a peer that has a dynamic IP address.

Example 2-23 defines configuration changes for a new site-to-site connection to EAST via NAT.

- One important change is to add the NAT traversal related commands.
- Another important change is the IP address of the peer. This is set to 0.0.0.0 to represent "any" IP address. Because the IP address of the peer is unknown, WEST will not initiate connections to the peer. It will only receive connections from the peer.
- All other information is set to be the same as the connection created for the basic site-to-site tunnel.

To configure this connection, perform the following steps on WEST in configuration mode:

Example 2-23 Creating a site-to-site connection to a peer with a dynamic IP address via NAT

Step	Command
Enable NAT traversal	vyatta@WEST# **set vpn ipsec nat-traversal enable** [edit]
Allow private network 10.0.0.0/8.	vyatta@WEST# **set vpn ipsec nat-networks allowed-network 10.0.0.0/8** [edit]
Allow private network 172.16.0.0/12.	vyatta@WEST# **set vpn ipsec nat-networks allowed-network 172.16.0.0/12** [edit]
Allow private network 192.168.0.0/16, but exclude the local subnet (192.168.40.0/24).	vyatta@WEST# **set vpn ipsec nat-networks allowed-network 192.168.0.0/16 exclude 192.168.40.0/24** [edit]
Commit the configuration.	vyatta@WEST# **commit**

View the newly added configuration (only the relevant parts of the configuration are shown).	vyatta@WEST# **show vpn ipsec**
	
	(...)
	nat-networks {
	allowed-network 10.0.0.0/8 {
	}
	allowed-network 172.16.0.0/12 {
	}
	allowed-network 192.168.0.0/16 {
	exclude-network 192.168.40.0/24
	}
	}
	nat-traversal enable
	(...)

Delete the previous configuration.	vyatta@WEST# **delete vpn ipsec site-to-site peer 192.0.2.33**
Create the node for EAST, setting the IP address to “any”, and set the authentication mode.	vyatta@WEST# **set vpn ipsec site-to-site peer 0.0.0.0 authentication mode pre-shared-secret**
Navigate to the node for the peer for easier editing.	vyatta@WEST# **edit vpn ipsec site-to-site peer 0.0.0.0** [edit vpn ipsec site-to-site peer 0.0.0.0]

Example 2-23 Creating a site-to-site connection to a peer with a dynamic IP address via NAT

Provide the string that will be used to generate encryption keys.	`vyatta@WEST# set authentication pre-shared-secret test_key_1` `[edit vpn ipsec site-to-site peer 0.0.0.0]`
Specify the default ESP group for all tunnels.	`vyatta@WEST# set default-esp-group ESP-1W` `[edit vpn ipsec site-to-site peer 0.0.0.0]`
Specify the IKE group.	`vyatta@WEST# set ike-group IKE-1W` `[edit vpn ipsec site-to-site peer 0.0.0.0]`
Identify the IP address on this Vyatta system to be used for this connection.	`vyatta@WEST# set local-ip 192.0.2.1` `[edit vpn ipsec site-to-site peer 0.0.0.0]`
Create a tunnel configuration, and provide the local subnet for this tunnel.	`vyatta@WEST# set tunnel 1 local subnet 192.168.40.0/24` `[edit vpn ipsec site-to-site peer 0.0.0.0]`
Provide the remote subnet for the tunnel.	`vyatta@WEST# set tunnel 1 remote subnet 192.168.60.0/24` `[edit vpn ipsec site-to-site peer 0.0.0.0]`
Return to the top of the configuration tree.	`vyatta@WEST# top`
Commit the configuration.	`vyatta@WEST# commit`

View the configuration for the site-to-site connection.	`vyatta@WEST# show vpn ipsec site-to-site peer 0.0.0.0`
	`authentication`
	`mode pre-shared-secret`
	`pre-shared-secret test_key_1`
	`}`
	`default-esp-group ESP-1W`
	`ike-group IKE-1W`
	`local-ip 192.0.2.1`
	`tunnel 1 {`
	`local {`
	`subnet 192.168.40.0/24`
	`}`
	`remote {`
	`subnet 192.168.60.0/24`
	`}`
	`}`

View IPsec interface configuration.	`vyatta@WEST# show vpn ipsec ipsec-interfaces` `interface eth1`
View Ethernet interface eth1 address configuration. **local-ip** is set to this address.	`vyatta@WEST# show interfaces ethernet eth1 address` `address 192.0.2.1/27`

Configure EAST

Similar to the WEST configuration, EAST must be configured for NAT traversal, but the connection from EAST to WEST requires only a minor change (**local-ip**) from that configured in the section “Configuring a Basic Site-to-Site Connection” on page 20.

- The NAT device keeps track of EAST’s fixed IP and correctly routes incoming packets to EAST, making any necessary changes to outgoing packets
- WEST retains its fixed IP, so no modification is required to the remote peer IP address.

To configure this connection, perform the following steps on EAST in configuration mode:

Example 2-24 Specify a new **local-ip** and that NAT must be traversed

Step	Command
Enable NAT traversal	vyatta@EAST# **set vpn ipsec nat-traversal enable** [edit]
Allow private network 10.0.0.0/8.	vyatta@EAST# **set vpn ipsec nat-networks allowed-network 10.0.0.0/8** [edit]
Allow private network 172.16.0.0/12.	vyatta@EAST# **set vpn ipsec nat-networks allowed-network 172.16.0.0/12** [edit]
Allow private network 192.168.0.0/16 but exclude the local subnet (192.168.60.0/24).	vyatta@EAST# **set vpn ipsec nat-networks allowed-network 192.168.0.0/16 exclude 192.168.60.0/24** [edit]
Commit the configuration.	vyatta@EAST# **commit**

Example 2-24 Specify a new **local-ip** and that NAT must be traversed

View the newly added configuration (only the relevant parts of the configuration are shown).	vyatta@EAST# **show vpn ipsec**
	
	(...)
	    nat-networks {
	        allowed-network 10.0.0.0/8 {
	        }
	        allowed-network 172.16.0.0/12 {
	        }
	        allowed-network 192.168.0.0/16 {
	            exclude-network 192.168.60.0/24
	        }
	    }
	    nat-traversal enable
	(...)

Identify the IP address on this Vyatta system to be used for this connection.	vyatta@EAST# **set vpn ipsec site-to-site peer 192.0.2.1 local-ip 192.168.0.1** [edit]
Commit the configuration.	vyatta@EAST# **commit**

View the modified configuration for the site-to-site connection.	vyatta@EAST# **show vpn ipsec site-to-site peer 192.0.2.1**
	    authentication
	        mode pre-shared-secret
	        pre-shared-secret test_key_1
	    }
	    default-esp-group ESP-1E
	    ike-group IKE-1E
	    local-ip 192.168.0.1
	    tunnel 1 {
	        local {
	            subnet 192.168.60.0/24
	        }
	        remote {
	            subnet 192.168.40.0/24
	        }
	    }

View IPsec interface configuration.	vyatta@EAST# **show vpn ipsec ipsec-interfaces** interface eth0
View Ethernet interface eth0 address configuration. **local-ip** is set to this address.	vyatta@EAST# **show interfaces ethernet eth0 address** address 192.168.0.1/24

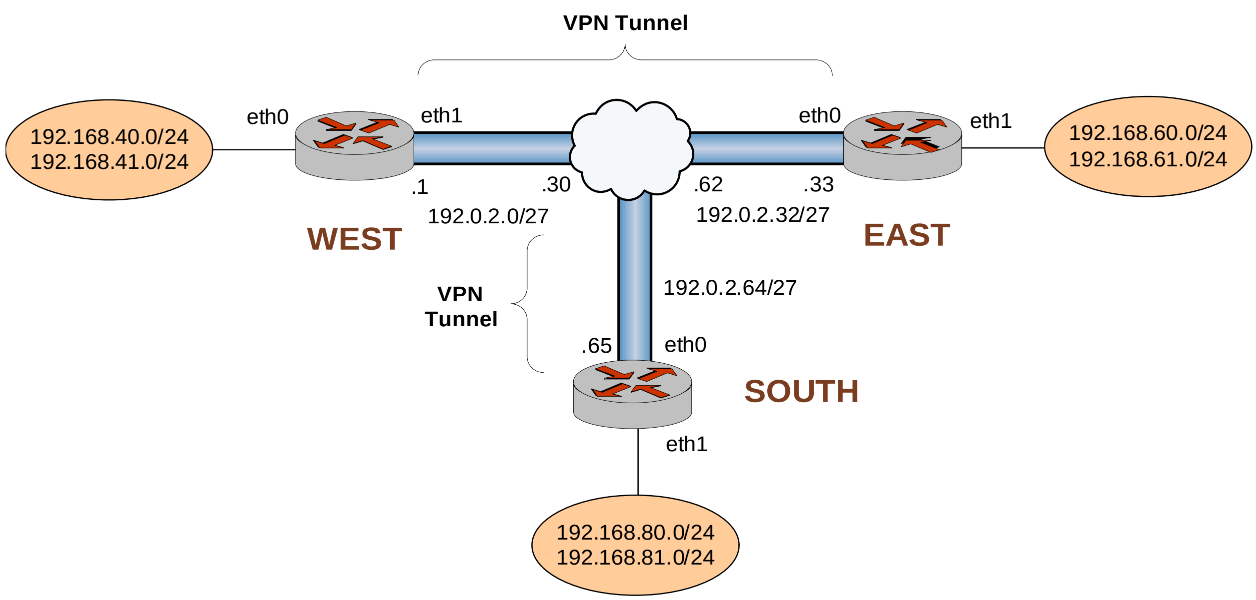
Configuring IPsec Tunnels between Three Gateways

This section presents the following topics:

- Configure WEST
- Configure EAST
- Configure SOUTH

This section presents a sample configuration for multiple site-to-site tunnels between three gateways: WEST, EAST, and SOUTH. When you have finished, these peers will be configured as shown in Figure 2-5.

Figure 2-5 Multiple site-to-site tunnels between three gateways



Configure WEST

This section presents the following topics:

- Configuring the Second ESP Group on WEST
- Adding Tunnels to the Connection to EAST
- Creating the Connection to SOUTH

This example assumes that WEST has already been configured for a basic connection to EAST, as described in “Configuring a Basic Site-to-Site Connection” on page 157. The additional configuration for WEST for this scenario consists of the following:

- An additional ESP group

- Three new tunnel configurations for the site-to-site connection to EAST
- A new site-to-site connection to SOUTH

This section presents the following examples:

- Example 2-25 Configuring a second ESP group on WEST
- Example 2-26 Adding tunnels to the connection to EAST
- Example 2-27 Creating a site-to-site connection from WEST to SOUTH

Configuring the Second ESP Group on WEST

Example 2-25 creates a second ESP group ESP-2W on WEST. This ESP group contains just one proposal:

- Proposal 1 uses AES-256 as the encryption cipher and SHA-1 as the hash algorithm
- The lifetime of a proposal from this ESP group is set to 600 seconds.

To create this ESP group, perform the following steps on WEST in configuration mode:

Example 2-25 Configuring a second ESP group on WEST

Step	Command
Create the configuration node for proposal 1 of ESP group ESP-2W.	`vyatta@WEST# set vpn ipsec esp-group ESP-2W proposal 1`
Set the encryption cipher for proposal 1.	`vyatta@WEST# set vpn ipsec esp-group ESP-2W proposal 1 encryption aes256`
Set the hash algorithm for proposal 1 of ESP-2W.	`vyatta@WEST# set vpn ipsec esp-group ESP-2W proposal 1 hash sha1`
Set the lifetime for ESP-2W.	`vyatta@WEST# set vpn ipsec esp-group ESP-2W lifetime 600`

View the configuration for the ESP group. Don't commit yet.	`vyatta@WEST# show vpn ipsec esp-group ESP-2W`
	`>   proposal 1 {`
	`>       encryption aes256`
	`>       hash sha1`
	`>   }`
	`>   lifetime 600`

Adding Tunnels to the Connection to EAST

Example 2-26 adds three tunnels to the site-to-site connection from WEST to EAST.

- Tunnel 2 communicates between 192.168.40.0/24 on WEST and 192.168.61.0/24 on EAST, and uses the default ESP group ESP-1W.
- Tunnel 3 communicates between 192.168.41.0/24 on WEST and 192.168.60.0/24 on EAST, and uses ESP group ESP-2W.
- Tunnel 4 communicates between 192.168.41.0/24 on WEST and 192.168.61.0/24 on EAST, and uses ESP group ESP-2W.

To configure this connection, perform the following steps on WEST in configuration mode:

Example 2-26 Adding tunnels to the connection to EAST

Step	Command
Navigate to the configuration node for EAST for easier editing	`vyatta@WEST#` **`edit vpn ipsec site-to-site peer 192.0.2.33`** `[edit vpn ipsec site-to-site peer 192.0.2.33]`
Create the configuration node for tunnel 2, and provide the local subnet for this tunnel.	`vyatta@WEST#` **`set tunnel 2 local subnet 192.168.40.0/24`** `[edit vpn ipsec site-to-site peer 192.0.2.33]`
Provide the remote subnet for tunnel 2.	`vyatta@WEST#` **`set tunnel 2 remote subnet 192.168.61.0/24`** `[edit vpn ipsec site-to-site peer 192.0.2.33]`
Create the configuration node for tunnel 3, and provide the local subnet for this tunnel.	`vyatta@WEST#` **`set tunnel 3 local subnet 192.168.41.0/24`** `[edit vpn ipsec site-to-site peer 192.0.2.33]`
Provide the remote subnet for tunnel 3.	`vyatta@WEST#` **`set tunnel 3 remote subnet 192.168.60.0/24`** `[edit vpn ipsec site-to-site peer 192.0.2.33]`
Specify the ESP group for tunnel 3.	`vyatta@WEST#` **`set tunnel 3 esp-group ESP-2W`** `[edit vpn ipsec site-to-site peer 192.0.2.33]`
Create the configuration node for tunnel 4, and provide the local subnet for this tunnel.	`vyatta@WEST#` **`set tunnel 4 local subnet 192.168.41.0/24`** `[edit vpn ipsec site-to-site peer 192.0.2.33]`
Provide the remote subnet for tunnel 4.	`vyatta@WEST#` **`set tunnel 4 remote subnet 192.168.61.0/24`** `[edit vpn ipsec site-to-site peer 192.0.2.33]`
Specify the ESP group for tunnel 4.	`vyatta@WEST#` **`set tunnel 4 esp-group ESP-2W`** `[edit vpn ipsec site-to-site peer 192.0.2.33]`
Return to the top of the configuration tree.	`vyatta@WEST#` **`top`**
Commit the configuration.	`vyatta@WEST#` **`commit`**

Example 2-26 Adding tunnels to the connection to EAST

View the configuration for the site-to-site connection.	`vyatta@WEST# show vpn ipsec site-to-site peer 192.0.2.33`
	`  authentication`
	`    mode pre-shared-secret`
	`    pre-shared-secret test_key_1`
	`  }`
	`  default-esp-group ESP-1W`
	`  ike-group IKE-1W`
	`  local-ip 192.0.2.1`
	`  tunnel 1 {`
	`    local {`
	`      subnet 192.168.40.0/24`
	`    }`
	`    remote {`
	`      subnet 192.168.60.0/24`
	`    }`
	`  }`
	`  tunnel 2 {`
	`    local {`
	`      subnet 192.168.40.0/24`
	`    }`
	`    remote {`
	`      subnet 192.168.61.0/24`
	`    }`
	`  }`
	`  tunnel 3 {`
	`    esp-group ESP-2W`
	`    local {`
	`      subnet 192.168.41.0/24`
	`    }`
	`    remote {`
	`      subnet 192.168.60.0/24`
	`    }`
	`  }`
	`  tunnel 4 {`
	`    esp-group ESP-2W`
	`    local {`
	`      subnet 192.168.41.0/24`
	`    }`
	`    remote {`
	`      subnet 192.168.61.0/24`
	`    }`
	`  }`

View IPsec interface configuration.	`vyatta@WEST# show vpn ipsec ipsec-interfaces` ` interface eth1`

Example 2-26 Adding tunnels to the connection to EAST

View Ethernet interface eth1 address configuration. **local-ip** is set to this address.	`vyatta@WEST#` **`show interfaces ethernet eth1 address`** `address 192.0.2.1/27`

Creating the Connection to SOUTH

Example 2-27 defines a site-to-site connection from WEST to SOUTH.

- The connection has four tunnels:
  - Tunnel 1 communicates between 192.168.40.0/24 on WEST and 192.168.80.0/24 on SOUTH, and uses the default ESP group ESP-1W.
  - Tunnel 2 communicates between 192.168.40.0/24 on WEST and 192.168.81.0/24 on SOUTH, and uses the default ESP group ESP-1W.
  - Tunnel 3 communicates between 192.168.41.0/24 on WEST and 192.168.80.0/24 on SOUTH, and uses the default ESP group ESP-1W.
  - Tunnel 4 communicates between 192.168.41.0/24 on WEST and 192.168.81.0/24 on SOUTH, and uses the default ESP group ESP-1W.
- WEST uses IP address 192.0.2.1 on eth1.
- SOUTH uses IP address 192.0.2.65 on eth0.
- The IKE group is IKE-1W
- The preshared secret is “test_key_2”.

To configure this connection, perform the following steps on WEST in configuration mode:

Example 2-27 Creating a site-to-site connection from WEST to SOUTH

Step	Command
Create the node for SOUTH and set the authentication mode	`vyatta@WEST#` **`set vpn ipsec site-to-site peer 192.0.2.65 authentication mode pre-shared-secret`**
Navigate to the node for the peer for easier editing	`vyatta@WEST#` **`edit vpn ipsec site-to-site peer 192.0.2.65`** `[edit vpn ipsec site-to-site peer 192.0.2.65]`
Provide the string that will be used to generate encryption keys.	`vyatta@WEST#` **`set authentication pre-shared-secret test_key_2`** `[edit vpn ipsec site-to-site peer 192.0.2.65]`
Specify the default ESP group for all tunnels.	`vyatta@WEST#` **`set default-esp-group ESP-1W`** `[edit vpn ipsec site-to-site peer 192.0.2.65]`
Specify the IKE group.	`vyatta@WEST#` **`set ike-group IKE-1W`** `[edit vpn ipsec site-to-site peer 192.0.2.65]`

Example 2-27 Creating a site-to-site connection from WEST to SOUTH

Identify the IP address on this Vyatta system to be used for this connection.	`vyatta@WEST#` **`set local-ip 192.0.2.1`** `[edit vpn ipsec site-to-site peer 192.0.2.65]`
Create the configuration node for tunnel 1, and provide the local subnet for this tunnel.	`vyatta@WEST#` **`set tunnel 1 local subnet 192.168.40.0/24`** `[edit vpn ipsec site-to-site peer 192.0.2.65]`
Provide the remote subnet for tunnel 1.	`vyatta@WEST#` **`set tunnel 1 remote subnet 192.168.80.0/24`** `[edit vpn ipsec site-to-site peer 192.0.2.65]`
Create the configuration node for tunnel 2, and provide the local subnet for this tunnel.	`vyatta@WEST#` **`set tunnel 2 local subnet 192.168.40.0/24`** `[edit vpn ipsec site-to-site peer 192.0.2.65]`
Provide the remote subnet for tunnel 2.	`vyatta@WEST#` **`set tunnel 2 remote subnet 192.168.81.0/24`** `[edit vpn ipsec site-to-site peer 192.0.2.65]`
Create the configuration node for tunnel 3, and provide the local subnet for this tunnel.	`vyatta@WEST#` **`set tunnel 3 local subnet 192.168.41.0/24`** `[edit vpn ipsec site-to-site peer 192.0.2.65]`
Provide the remote subnet for tunnel 3.	`vyatta@WEST#` **`set tunnel 3 remote subnet 192.168.80.0/24`** `[edit vpn ipsec site-to-site peer 192.0.2.65]`
Create the configuration node for tunnel 4, and provide the local subnet for this tunnel.	`vyatta@WEST#` **`set tunnel 4 local subnet 192.168.41.0/24`** `[edit vpn ipsec site-to-site peer 192.0.2.65]`
Provide the remote subnet for tunnel 4.	`vyatta@WEST#` **`set tunnel 4 remote subnet 192.168.81.0/24`** `[edit vpn ipsec site-to-site peer 192.0.2.65]`
Return to the top of the configuration tree.	`vyatta@WEST#` **`top`**
Commit the configuration.	`vyatta@WEST#` **`commit`**

Example 2-27 Creating a site-to-site connection from WEST to SOUTH

View the configuration for the site-to-site connection.	`vyatta@WEST# show vpn ipsec site-to-site peer 192.0.2.65`

```
vyatta@WEST# show vpn ipsec site-to-site peer 192.0.2.65
    authentication
        mode pre-shared-secret
        pre-shared-secret test_key_2
    }
    default-esp-group ESP-1W
    ike-group IKE-1W
    local-ip 192.0.2.1
    tunnel 1 {
        local {
            subnet 192.168.40.0/24
        }
        remote {
            subnet 192.168.80.0/24
        }
    }
    tunnel 2 {
        local {
            subnet 192.168.40.0/24
        }
        remote {
            subnet 192.168.81.0/24
        }
    }
    tunnel 3 {
        local {
            subnet 192.168.41.0/24
        }
        remote {
            subnet 192.168.80.0/24
        }
    }
    tunnel 4 {
        local {
            subnet 192.168.41.0/24
        }
        remote {
            subnet 192.168.81.0/24
        }
    }
```

Configure EAST

This section presents the following topics:

- Configuring the Second ESP Group on EAST
- Adding Tunnels to the Connection to WEST
- Creating the Connection to SOUTH

This example assumes that EAST has already been configured for a basic connection to WEST, as described in ""Configuring a Basic Site-to-Site Connection" on page 20. The additional configuration for EAST for this scenario consists of the following:

- An additional ESP group
- Three new tunnel configurations for the site-to-site connection to WEST
- A new site-to-site connection to SOUTH

This section presents the following examples:

- Example 2-28 Configuring a second ESP group on EAST
- Example 2-29 Adding tunnels to the connection to WEST
- Example 2-30 Creating a site-to-site connection from EAST to SOUTH

Configuring the Second ESP Group on EAST

Example 2-28 creates a second ESP group ESP-2W on EAST. This ESP group contains just one proposal:

- Proposal 1 uses AES-256 as the encryption cipher and SHA-1 as the hash algorithm

The lifetime of a proposal from this ESP group is set to 600 seconds.

To create this ESP group, perform the following steps on EAST in configuration mode:

Example 2-28 Configuring a second ESP group on EAST

Step	Command
Create the configuration node for proposal 1 of ESP group ESP-2E.	vyatta@EAST# **set vpn ipsec esp-group ESP-2E proposal 1**
Set the encryption cipher for proposal 1.	vyatta@EAST# **set vpn ipsec esp-group ESP-2E proposal 1 encryption aes256**
Set the hash algorithm for proposal 1 of ESP-2E.	vyatta@EAST# **set vpn ipsec esp-group ESP-2E proposal 1 hash sha1**
Set the lifetime for ESP-2E.	vyatta@EAST# **set vpn ipsec esp-group ESP-2E lifetime 600**

Example 2-28 Configuring a second ESP group on EAST

View the configuration for the ESP group. Don’t commit yet.	vyatta@EAST# **show vpn ipsec esp-group ESP-2E** > proposal 1 { > encryption aes256 > hash sha1 > } > lifetime 600

Adding Tunnels to the Connection to WEST

Example 2-29 adds three tunnels to the site-to-site connection from EAST to WEST.

- Tunnel 2 communicates between 192.168.60.0/24 on EAST and 192.168.41.0/24 on WEST, and uses the default ESP group ESP-1E.
- Tunnel 3 communicates between 192.168.61.0/24 on EAST and 192.168.40.0/24 on WEST, and uses ESP group ESP-2E.
- Tunnel 4 communicates between 192.168.61.0/24 on EAST and 192.168.41.0/24 on WEST, and uses ESP group ESP-2E.

To configure this connection, perform the following steps on EAST in configuration mode:

Example 2-29 Adding tunnels to the connection to WEST

Step	Command
Navigate to the configuration node for WEST for easier editing	vyatta@EAST# **edit vpn ipsec site-to-site peer 192.0.2.1** [edit vpn ipsec site-to-site peer 192.0.2.1]
Create the configuration node for tunnel 2, and provide the local subnet for this tunnel.	vyatta@EAST# **set tunnel 2 local subnet 192.168.60.0/24** [edit vpn ipsec site-to-site peer 192.0.2.1]
Provide the remote subnet for tunnel 2.	vyatta@EAST# **set tunnel 2 remote subnet 192.168.41.0/24** [edit vpn ipsec site-to-site peer 192.0.2.1]
Create the configuration node for tunnel 3, and provide the local subnet for this tunnel.	vyatta@EAST# **set tunnel 3 local subnet 192.168.61.0/24** [edit vpn ipsec site-to-site peer 192.0.2.1]
Provide the remote subnet for tunnel 3.	vyatta@EAST# **set tunnel 3 remote subnet 192.168.40.0/24** [edit vpn ipsec site-to-site peer 192.0.2.1]
Specify the ESP group for tunnel 3.	vyatta@EAST# **set tunnel 3 esp-group ESP-2E** [edit vpn ipsec site-to-site peer 192.0.2.1]

Example 2-29 Adding tunnels to the connection to WEST

Create the configuration node for tunnel 4, and provide the local subnet for this tunnel.	`vyatta@EAST#` **`set tunnel 4 local subnet 192.168.61.0/24`** `[edit vpn ipsec site-to-site peer 192.0.2.1]`
Provide the remote subnet for tunnel 4.	`vyatta@EAST#` **`set tunnel 4 remote subnet 192.168.41.0/24`** `[edit vpn ipsec site-to-site peer 192.0.2.1]`
Specify the ESP group for tunnel 4.	`vyatta@EAST#` **`set tunnel 4 esp-group ESP-2E`** `[edit vpn ipsec site-to-site peer 192.0.2.1]`
Return to the top of the configuration tree.	`vyatta@EAST#` **`top`**
Commit the configuration.	`vyatta@EAST#` **`commit`**

Example 2-29 Adding tunnels to the connection to WEST

View the configuration for the site-to-site connection.	`vyatta@EAST# show vpn ipsec site-to-site peer 192.0.2.1`
	`  authentication`
	`    mode pre-shared-secret`
	`    pre-shared-secret test_key_1`
	`  }`
	`  default-esp-group ESP-1E`
	`  ike-group IKE-1E`
	`  local-ip 192.0.2.33`
	`  tunnel 1 {`
	`    local {`
	`      subnet 192.168.60.0/24`
	`    }`
	`    remote {`
	`      subnet 192.168.40.0/24`
	`    }`
	`  }`
	`  tunnel 2 {`
	`    local {`
	`      subnet 192.168.60.0/24`
	`    }`
	`    remote {`
	`      subnet 192.168.41.0/24`
	`    }`
	`  }`
	`  tunnel 3 {`
	`    esp-group ESP-2E`
	`    local {`
	`      subnet 192.168.61.0/24`
	`    }`
	`    remote {`
	`      subnet 192.168.40.0/24`
	`    }`
	`  }`
	`  tunnel 4 {`
	`    esp-group ESP-2E`
	`    local {`
	`      subnet 192.168.61.0/24`
	`    }`
	`    remote {`
	`      subnet 192.168.41.0/24`
	`    }`
	`  }`

View IPsec interface configuration.	`vyatta@EAST# show vpn ipsec ipsec-interfaces` ` interface eth0`

Example 2-29 Adding tunnels to the connection to WEST

View Ethernet interface eth0 address configuration. **local-ip** is set to this address.	`vyatta@EAST#` **`show interfaces ethernet eth0 address`** `address 192.0.2.33/27`

Creating the Connection to SOUTH

Example 2-30 defines a site-to-site connection from EAST to SOUTH.

- The connection has four tunnels:
  - — Tunnel 1 communicates between 192.168.60.0/24 on EAST and 192.168.80.0/24 on SOUTH, and uses the default ESP group ESP-1E.
  - — Tunnel 2 communicates between 192.168.60.0/24 on EAST and 192.168.81.0/24 on SOUTH, and uses the default ESP group ESP-1E.
  - — Tunnel 3 communicates between 192.168.61.0/24 on EAST and 192.168.80.0/24 on SOUTH, and uses the default ESP group ESP-1E.
  - — Tunnel 4 communicates between 192.168.61.0/24 on EAST and 192.168.81.0/24 on SOUTH, and uses the default ESP group ESP-1E.
- EAST uses IP address 192.0.2.33 on eth1.
- SOUTH uses IP address 192.0.2.65 on eth0.
- The IKE group is IKE-1E
- The preshared secret is “test_key_2”.

To configure this connection, perform the following steps on EAST in configuration mode:

Example 2-30 Creating a site-to-site connection from EAST to SOUTH

Step	Command
Create the node for SOUTH and set the authentication mode	`vyatta@EAST#` **`set vpn ipsec site-to-site peer 192.0.2.65 authentication mode pre-shared-secret`**
Navigate to the node for the peer for easier editing	`vyatta@EAST#` **`edit vpn ipsec site-to-site peer 192.0.2.65`** `[edit vpn ipsec site-to-site peer 192.0.2.65]`
Provide the string that will be used to generate encryption keys.	`vyatta@EAST#` **`set authentication pre-shared-secret test_key_2`** `[edit vpn ipsec site-to-site peer 192.0.2.65]`
Specify the default ESP group.	`vyatta@EAST#` **`set default-esp-group ESP-1E`** `[edit vpn ipsec site-to-site peer 192.0.2.65]`
Specify the IKE group.	`vyatta@EAST#` **`set ike-group IKE-1E`** `[edit vpn ipsec site-to-site peer 192.0.2.65]`

Example 2-30 Creating a site-to-site connection from EAST to SOUTH

Identify the IP address on this Vyatta system to be used for this connection.	vyatta@EAST# **set local-ip 192.0.2.33** [edit vpn ipsec site-to-site peer 192.0.2.65]
Create the configuration node for tunnel 1, and provide the local subnet for this tunnel.	vyatta@EAST# **set tunnel 1 local subnet 192.168.60.0/24** [edit vpn ipsec site-to-site peer 192.0.2.65]
Provide the remote subnet for tunnel 1.	vyatta@EAST# **set tunnel 1 remote subnet 192.168.80.0/24** [edit vpn ipsec site-to-site peer 192.0.2.65]
Create the configuration node for tunnel 2, and provide the local subnet for this tunnel.	vyatta@EAST# **set tunnel 2 local subnet 192.168.60.0/24** [edit vpn ipsec site-to-site peer 192.0.2.65]
Provide the remote subnet for tunnel 2.	vyatta@EAST# **set tunnel 2 remote subnet 192.168.81.0/24** [edit vpn ipsec site-to-site peer 192.0.2.65]
Create the configuration node for tunnel 3, and provide the local subnet for this tunnel.	vyatta@EAST# **set tunnel 3 local subnet 192.168.61.0/24** [edit vpn ipsec site-to-site peer 192.0.2.65]
Provide the remote subnet for tunnel 3.	vyatta@EAST# **set tunnel 3 remote subnet 192.168.80.0/24** [edit vpn ipsec site-to-site peer 192.0.2.65]
Create the configuration node for tunnel 4, and provide the local subnet for this tunnel.	vyatta@EAST# **set tunnel 4 local subnet 192.168.61.0/24** [edit vpn ipsec site-to-site peer 192.0.2.65]
Provide the remote subnet for tunnel 4.	vyatta@EAST# **set tunnel 4 remote subnet 192.168.81.0/24** [edit vpn ipsec site-to-site peer 192.0.2.65]
Return to the top of the configuration tree.	vyatta@EAST# **top**
Commit the configuration.	vyatta@EAST# **commit**

Example 2-30 Creating a site-to-site connection from EAST to SOUTH

View the configuration for the site-to-site connection.	vyatta@EAST# **show vpn ipsec site-to-site peer 192.0.2.65**

```
vyatta@EAST# show vpn ipsec site-to-site peer 192.0.2.65
    authentication
        mode pre-shared-secret
        pre-shared-secret test_key_2
    }
    default-esp-group ESP-1E
    ike-group IKE-1E
    local-ip 192.0.2.33
    tunnel 1 {
        local {
            subnet 192.168.60.0/24
        }
        remote {
            subnet 192.168.80.0/24
        }
    }
    tunnel 2 {
        local {
            subnet 192.168.60.0/24
        }
        remote {
            subnet 192.168.81.0/24
        }
    }
    tunnel 3 {
        local {
            subnet 192.168.61.0/24
        }
        remote {
            subnet 192.168.80.0/24
        }
    }
    tunnel 4 {
        local {
            subnet 192.168.61.0/24
        }
        remote {
            subnet 192.168.81.0/24
        }
    }
```

Configure SOUTH

This section presents the following topics:

- Enabling VPN on SOUTH
- Configuring an IKE Group on SOUTH
- Configuring an ESP Group on SOUTH
- Creating the Connection to WEST
- Creating the Connection to EAST

This section presents the following examples:

- Example 2-31 Enabling IPsec VPN on SOUTH
- Example 2-32 Configuring an IKE group on SOUTH
- Example 2-33 Configuring an ESP group on SOUTH
- Example 2-34 Creating a site-to-site connection from SOUTH to WEST
- Example 2-35 Creating a site-to-site connection from SOUTH to EAST

Enabling VPN on SOUTH

In this section, you enable IPsec VPN on the interfaces that will be used in VPN connections on SOUTH. The VPN tunnels in the example configuration extend through the wide-area network to eth0 on SOUTH. This means that eth0 on SOUTH must have VPN enabled. The other interfaces on SOUTH need not.

Example 2-31 enables IPsec VPN on eth0 on SOUTH. To do this, perform the following steps on SOUTH in configuration mode:

Example 2-31 Enabling IPsec VPN on SOUTH

Step	Command
Enable VPN on eth0 on SOUTH.	`vyatta@SOUTH#` **`set vpn ipsec ipsec-interfaces interface eth0`**
View IPsec interface configuration. Don't commit yet.	`vyatta@SOUTH#` **`show vpn ipsec ipsec-interfaces`** `>  interface eth0`

Configuring an IKE Group on SOUTH

Example 2-32 creates IKE group IKE-1S on SOUTH. This IKE group contains two proposals:

- Proposal 1 uses AES-256 as the encryption cipher and SHA-1 as the hash algorithm
- Proposal 2 uses AES-128 as the encryption cipher and SHA-1 as the hash algorithm

The lifetime of a proposal from this IKE group is set to 3600.

Note that these parameters correspond to those set in IKE-1W on WEST and IKE-1E on EAST. You must ensure, in defining proposals, that the encryption ciphers and hash algorithms are such that the two peers will be able to agree on a combination.

To create this IKE group, perform the following steps on SOUTH in configuration mode:

Example 2-32 Configuring an IKE group on SOUTH

Step	Command
Creates the configuration node for proposal 1 of IKE group IKE-1S.	vyatta@SOUTH# **set vpn ipsec ike-group IKE-1S proposal 1**
Set the encryption cipher for proposal 1.	vyatta@SOUTH# **set vpn ipsec ike-group IKE-1S proposal 1 encryption aes256**
Set the hash algorithm for proposal 1.	vyatta@SOUTH# **set vpn ipsec ike-group IKE-1S proposal 1 hash sha1**
Set the encryption cipher for proposal 2. This also creates the configuration node for proposal 2 of IKE group IKE-1S.	vyatta@SOUTH# **set vpn ipsec ike-group IKE-1S proposal 2 encryption aes128**
Set the hash algorithm for proposal 2.	vyatta@SOUTH# **set vpn ipsec ike-group IKE-1S proposal 2 hash sha1**
Set the lifetime for the whole IKE group.	vyatta@SOUTH# **set vpn ipsec ike-group IKE-1S lifetime 3600**

View the configuration for the IKE group. Don’t commit yet.	vyatta@SOUTH# **show vpn ipsec ike-group IKE-1S**
	> proposal 1 {
	> encryption aes256
	> hash sha1
	> }
	> proposal 2 {
	> encryption aes128
	> hash sha1
	> }
	> lifetime 3600

Configuring an ESP Group on SOUTH

Example 2-33 creates ESP group ESP-1S on SOUTH. This ESP group contains two proposals:

- Proposal 1 uses AES-256 as the encryption cipher and SHA-1 as the hash algorithm
- Proposal 2 uses Triple-DES as the encryption cipher and MD5 as the hash algorithm

The lifetime of a proposal from this ESP group is set to 1800 seconds.

To create this ESP group, perform the following steps on SOUTH in configuration mode:

Example 2-33 Configuring an ESP group on SOUTH

Step	Command
Create the configuration node for proposal 1 of ESP group ESP-1S.	vyatta@SOUTH# **set vpn ipsec esp-group ESP-1S proposal 1**
Set the encryption cipher for proposal 1.	vyatta@SOUTH# **set vpn ipsec esp-group ESP-1S proposal 1 encryption aes256**
Set the hash algorithm for proposal 1.	vyatta@SOUTH# **set vpn ipsec esp-group ESP-1S proposal 1 hash sha1**
Set the encryption cipher for proposal 2. This also creates the configuration node for proposal 2 of ESP group ESP-1S.	vyatta@SOUTH# **set vpn ipsec esp-group ESP-1S proposal 2 encryption 3des**
Set the hash algorithm for proposal 2.	vyatta@SOUTH# **set vpn ipsec esp-group ESP-1S proposal 2 hash md5**
Set the lifetime for the whole ESP group.	vyatta@SOUTH# **set vpn ipsec esp-group ESP-1S lifetime 1800**

View the configuration for the ESP group. Don’t commit yet.	vyatta@SOUTH# **show vpn ipsec esp-group ESP-1S**
	`>   proposal 1 {`
	`>       encryption aes256`
	`>       hash sha1`
	`>   }`
	`>   proposal 2 {`
	`>       encryption 3de`
	`>       hash md5`
	`>   }`
	`>   lifetime 1800`

Creating the Connection to WEST

Example 2-34 defines a site-to-site connection to WEST.

- This connection is configured with four tunnels:
  - Tunnel 1 communicates between 192.168.80.0/24 on SOUTH and 192.168.40.0/24 on WEST, and uses the default ESP group ESP-1S.
  - Tunnel 2 communicates between 192.168.80.0/24 on SOUTH and 192.168.41.0/24 on WEST, and uses the default ESP group ESP-1S.
  - Tunnel 3 communicates between 192.168.81.0/24 on SOUTH and 192.168.40.0/24 on WEST, and uses the default ESP group ESP-1S.
  - Tunnel 4 communicates between 192.168.81.0/24 on SOUTH and 192.168.41.0/24 on WEST, and uses the default ESP group ESP-1S.
- SOUTH uses IP address 192.0.2.65 on eth0.
- WEST uses IP address 192.0.2.1 on eth1.
- The IKE group is IKE-1S.
- The preshared secret is “test_key_2”.

To configure this connection, perform the following steps on SOUTH in configuration mode:

Example 2-34 Creating a site-to-site connection from SOUTH to WEST

Step	Command
Create the node for WEST and set the authentication mode	`vyatta@SOUTH#` **`set vpn ipsec site-to-site peer 192.0.2.1 authentication mode pre-shared-secret`**
Navigate to the node for the peer for easier editing	`vyatta@SOUTH#` **`edit vpn ipsec site-to-site peer 192.0.2.1`** `[edit vpn ipsec site-to-site peer 192.0.2.1]`
Provide the string that will be used to generate encryption keys.	`vyatta@SOUTH#` **`set authentication pre-shared-secret test_key_2`** `[edit vpn ipsec site-to-site peer 192.0.2.1]`
Specify the default ESP group.	`vyatta@SOUTH#` **`set default-esp-group ESP-1S`** `[edit vpn ipsec site-to-site peer 192.0.2.1]`
Specify the IKE group.	`vyatta@SOUTH#` **`set ike-group IKE-1S`** `[edit vpn ipsec site-to-site peer 192.0.2.1]`
Identify the IP address on this Vyatta system to be used for this connection.	`vyatta@SOUTH#` **`set local-ip 192.0.2.65`** `[edit vpn ipsec site-to-site peer 192.0.2.1]`
Create the configuration node for tunnel 1, and provide the local subnet for this tunnel.	`vyatta@SOUTH#` **`set tunnel 1 local subnet 192.168.80.0/24`** `[edit vpn ipsec site-to-site peer 192.0.2.1]`

Example 2-34 Creating a site-to-site connection from SOUTH to WEST

Provide the remote subnet for tunnel 1.	`vyatta@SOUTH# set tunnel 1 remote subnet 192.168.40.0/24` `[edit vpn ipsec site-to-site peer 192.0.2.1]`
Create the configuration node for tunnel 2, and provide the local subnet for this tunnel.	`vyatta@SOUTH# set tunnel 2 local subnet 192.168.80.0/24` `[edit vpn ipsec site-to-site peer 192.0.2.1]`
Provide the remote subnet for tunnel 2.	`vyatta@SOUTH# set tunnel 2 remote subnet 192.168.41.0/24` `[edit vpn ipsec site-to-site peer 192.0.2.1]`
Create the configuration node for tunnel 3, and provide the local subnet for this tunnel.	`vyatta@SOUTH# set tunnel 3 local subnet 192.168.81.0/24` `[edit vpn ipsec site-to-site peer 192.0.2.1]`
Provide the remote subnet for tunnel 3.	`vyatta@SOUTH# set tunnel 3 remote subnet 192.168.40.0/24` `[edit vpn ipsec site-to-site peer 192.0.2.1]`
Create the configuration node for tunnel 4, and provide the local subnet for this tunnel.	`vyatta@SOUTH# set tunnel 4 local subnet 192.168.81.0/24` `[edit vpn ipsec site-to-site peer 192.0.2.1]`
Provide the remote subnet for tunnel 4.	`vyatta@SOUTH# set tunnel 4 remote subnet 192.168.41.0/24` `[edit vpn ipsec site-to-site peer 192.0.2.1]`
Return to the top of the configuration tree.	`vyatta@SOUTH# top`
Now commit the configuration.	`vyatta@SOUTH# commit`

Example 2-34 Creating a site-to-site connection from SOUTH to WEST

View the configuration for the site-to-site connection.	`vyatta@SOUTH# **show vpn ipsec site-to-site peer 192.0.2.1**`
View IPsec interface configuration.	`vyatta@SOUTH# **show vpn ipsec ipsec-interfaces**`

```
vyatta@SOUTH# show vpn ipsec site-to-site peer 192.0.2.1
    authentication
        mode pre-shared-secret
        pre-shared-secret test_key_2
    }
    default-esp-group ESP-1S
    ike-group IKE-1S
    local-ip 192.0.2.65
    tunnel 1 {
        local {
            subnet 192.168.80.0/24
        }
        remote {
            subnet 192.168.40.0/24
        }
    }
    tunnel 2 {
        local {
            subnet 192.168.80.0/24
        }
        remote {
            subnet 192.168.41.0/24
        }
    }
    tunnel 3 {
        local {
            subnet 192.168.81.0/24
        }
        remote {
            subnet 192.168.40.0/24
        }
    }
    tunnel 4 {
        local {
            subnet 192.168.81.0/24
        }
        remote {
            subnet 192.168.41.0/24
        }
    }
```

```
vyatta@SOUTH# show vpn ipsec ipsec-interfaces
 interface eth0
```

Example 2-34 Creating a site-to-site connection from SOUTH to WEST

View Ethernet interface eth0 address configuration. **local-ip** is set to this address.	`vyatta@SOUTH#` **`show interfaces ethernet eth0 address`** ` address 192.0.2.65/27`

Creating the Connection to EAST

Example 2-35 defines a site-to-site connection to EAST.

- This connection is configured with four tunnels:
  - Tunnel 1 communicates between 192.168.80.0/24 on SOUTH and 192.168.60.0/24 on EAST, and uses the default ESP group ESP-1S.
  - Tunnel 2 communicates between 192.168.80.0/24 on SOUTH and 192.168.61.0/24 on EAST, and uses the default ESP group ESP-1S.
  - Tunnel 3 communicates between 192.168.81.0/24 on SOUTH and 192.168.60.0/24 on EAST, and uses the default ESP group ESP-1S.
  - Tunnel 4 communicates between 192.168.81.0/24 on SOUTH and 192.168.61.0/24 on EAST, and uses the default ESP group ESP-1S.
- SOUTH uses IP address 192.0.2.65 on eth0.
- EAST uses IP address 192.0.2.33 on eth1.
- The IKE group is IKE-1S.
- The preshared secret is “test_key_2”.

To configure this connection, perform the following steps on SOUTH in configuration mode:

Example 2-35 Creating a site-to-site connection from SOUTH to EAST

Step	Command
Create the node for EAST and set the authentication mode	`vyatta@SOUTH#` **`set vpn ipsec site-to-site peer 192.0.2.33`**
Navigate to the node for the peer for easier editing	`vyatta@SOUTH#` **`edit vpn ipsec site-to-site peer 192.0.2.33`** `[edit vpn ipsec site-to-site peer 192.0.2.33]`
Provide the string that will be used to generate encryption keys.	`vyatta@SOUTH#` **`set authentication pre-shared-secret test_key_2`** `[edit vpn ipsec site-to-site peer 192.0.2.33]`
Specify the default ESP group.	`vyatta@SOUTH#` **`set default-esp-group ESP-1S`** `[edit vpn ipsec site-to-site peer 192.0.2.33]`
Specify the IKE group.	`vyatta@SOUTH#` **`set ike-group IKE-1S`** `[edit vpn ipsec site-to-site peer 192.0.2.33]`

Example 2-35 Creating a site-to-site connection from SOUTH to EAST

Identify the IP address on this Vyatta system to be used for this connection.	`vyatta@SOUTH#` **`set local-ip 192.0.2.65`** `[edit vpn ipsec site-to-site peer 192.0.2.33]`
Create the configuration node for tunnel 1, and provide the local subnet for this tunnel.	`vyatta@SOUTH#` **`set tunnel 1 local subnet 192.168.80.0/24`** `[edit vpn ipsec site-to-site peer 192.0.2.33]`
Provide the remote subnet for tunnel 1.	`vyatta@SOUTH#` **`set tunnel 1 remote subnet 192.168.60.0/24`** `[edit vpn ipsec site-to-site peer 192.0.2.33]`
Create the configuration node for tunnel 2, and provide the local subnet for this tunnel.	`vyatta@SOUTH#` **`set tunnel 2 local subnet 192.168.80.0/24`** `[edit vpn ipsec site-to-site peer 192.0.2.33]`
Provide the remote subnet for tunnel 2.	`vyatta@SOUTH#` **`set tunnel 2 remote subnet 192.168.61.0/24`** `[edit vpn ipsec site-to-site peer 192.0.2.33]`
Create the configuration node for tunnel 3, and provide the local subnet for this tunnel.	`vyatta@SOUTH#` **`set tunnel 3 local subnet 192.168.81.0/24`** `[edit vpn ipsec site-to-site peer 192.0.2.33]`
Provide the remote subnet for tunnel 3.	`vyatta@SOUTH#` **`set tunnel 3 remote subnet 192.168.60.0/24`** `[edit vpn ipsec site-to-site peer 192.0.2.33]`
Create the configuration node for tunnel 4, and provide the local subnet for this tunnel.	`vyatta@SOUTH#` **`set tunnel 4 local subnet 192.168.81.0/24`** `[edit vpn ipsec site-to-site peer 192.0.2.33]`
Provide the remote subnet for tunnel 4.	`vyatta@SOUTH#` **`set tunnel 4 remote subnet 192.168.61.0/24`** `[edit vpn ipsec site-to-site peer 192.0.2.33]`
Return to the top of the configuration tree.	`vyatta@SOUTH#` **`top`**
Now commit the configuration.	`vyatta@SOUTH#` **`commit`**

Example 2-35 Creating a site-to-site connection from SOUTH to EAST

View the configuration for the site-to-site connection.	see code below

```
vyatta@SOUTH# show vpn ipsec site-to-site peer 192.0.2.33
    authentication
        mode pre-shared-secret
        pre-shared-secret test_key_2
    }
    default-esp-group ESP-1S
    ike-group IKE-1S
    local-ip 192.0.2.65
    tunnel 1 {
        local {
            subnet 192.168.80.0/24
        }
        remote {
            subnet 192.168.60.0/24
        }
    }
    tunnel 2 {
        local {
            subnet 192.168.80.0/24
        }
        remote {
            subnet 192.168.61.0/24
        }
    }
    tunnel 3 {
        local {
            subnet 192.168.81.0/24
        }
        remote {
            subnet 192.168.60.0/24
        }
    }
    tunnel 4 {
        local {
            subnet 192.168.81.0/24
        }
        remote {
            subnet 192.168.61.0/24
        }
    }
```

Protecting a GRE Tunnel with IPsec

GRE, IP-in-IP, and SIT tunnels are not encrypted, and provide no security outside of a simple password-like key that is exchanged in clear text in each packet. This means that GRE, IP-in-IP, and SIT tunnels, on their own, do not provide adequate security for production environments.

At the same time, IPsec policy-based tunnels cannot directly route non-IP or multicast protocols, and IPsec also has limitations from an operations point of view. Using tunnel interfaces in conjunction with IPsec VPN provides secure, routable tunnel connections between gateways, that have some advantages over traditional IPsec policy-based tunnel mode connections:

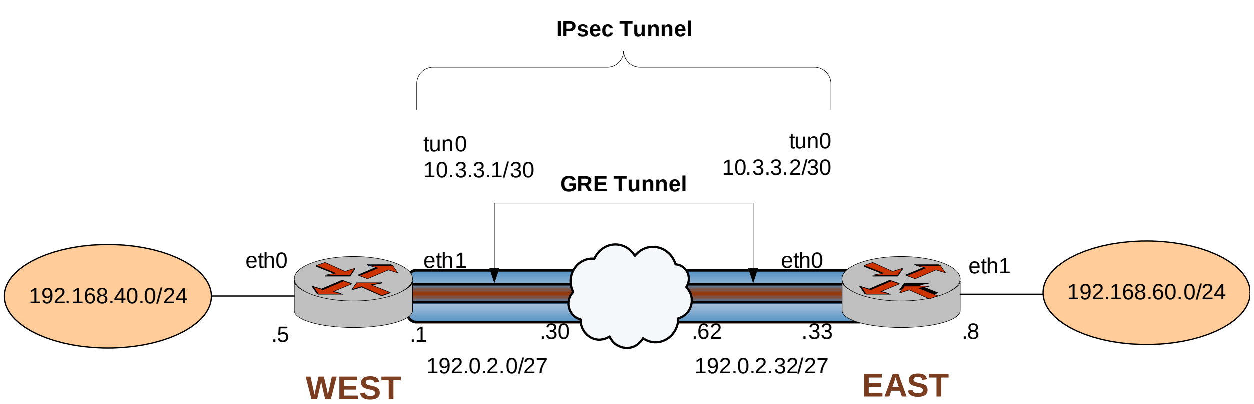
- Support for standard operational commands such as **show interfaces** and **show route**
- Support for operational tools such as **traceroute** and SNMP
- Dynamic tunnel failover using routing protocols
- Simplified IPsec policies and troubleshooting

For secure routable tunnels, GRE, IP-in-IP, and SIT tunnel interfaces should be used in conjunction with an IPsec connection, so that the IP tunnel can be protected by the IPsec tunnel.

This set of examples configures a GRE tunnel between EAST to WEST and protects it within an IPsec tunnel between the same endpoints.

When you have finished, WEST and EAST will be configured as shown in Figure 2-6.

Figure 2-6 GRE tunnel protected by an IPsec tunnel



Configure WEST

This section presents the following examples:

- Example 2-36 Defining the GRE tunnel from WEST to EAST
- Example 2-37 Defining the IPsec tunnel from WEST to EAST
- Example 2-38 Defining a static route on WEST

Define the GRE Tunnel on "WEST"

GRE tunnels are explained in detail in the *Vyatta Tunnels Reference Guide*. Please see that guide for further details.

Example 2-1 defines WEST's end of the GRE tunnel. In this example:

- The tunnel interface tun0 on router WEST is assigned the IP address 10.3.3.1/30.
- The encapsulation type is set to GRE.
- The IP address on the local side of the GRE tunnel (**local-ip**) is set to that of the local Ethernet interface (192.0.2.1).
- The IP address of the other end of the GRE tunnel (**remote-ip**) is set to the address of the remote system (192.0.2.33).
- Multicast is enabled in order to allow routing protocols to be carried on the GRE tunnel.

To create the tunnel interface and the tunnel endpoint on WEST, perform the following steps in configuration mode:

Example 2-36 Defining the GRE tunnel from WEST to EAST

Step	Command
Create the GRE tunnel interface, and specify the IP address to be associated with it.	vyatta@WEST# **set interfaces tunnel tun0 address 10.3.3.1/30**
Assign a brief description for the GRE tunnel interface.	vyatta@WEST# **set interfaces tunnel tun0 description "GRE tunnel to router EAST"**
Specify the encapsulation mode for the tunnel.	vyatta@WEST# **set interfaces tunnel tun0 encapsulation gre**
Allow multicast protocols (e.g., routing protocols) to be carried over the tunnel.	vyatta@WEST# **set interfaces tunnel tun0 multicast enable**
Specify the local IP address for the GRE tunnel.	vyatta@WEST# **set interfaces tunnel tun0 local-ip 192.0.2.1**
Specify the remote IP address for the GRE tunnel.	vyatta@WEST# **set interfaces tunnel tun0 remote-ip 192.0.2.33**
Commit the configuration.	vyatta@WEST# **commit**

Example 2-36 Defining the GRE tunnel from WEST to EAST

View the modified configuration.	`vyatta@WEST#` **`show interfaces tunnel tun0`**
	`address 10.3.3.1/30`
	`description “GRE tunnel to router EAST”`
	`encapsulation gre`
	`local-ip 192.0.2.1`
	`multicast enable`
	`remote-ip 192.0.2.33`

Define the IPsec Tunnel on “WEST”

Example 2-1 creates the IPsec tunnel from WEST to EAST.

- WEST uses IP address 192.0.2.1 on eth1.
- EAST uses IP address 192.0.2.33 on eth0.
- The IKE group is IKE-1W
- The preshared secret is “test_key_1”.
- All GRE traffic will be passed through the tunnel.

This examples assumes that you have already configured the following:

- IKE group IKE-1W (see page 22)
- ESP group ESP-1W (see page 23)

To create the IPsec tunnel from WEST to EAST, perform the following steps on WEST in configuration mode:

Example 2-37 Defining the IPsec tunnel from WEST to EAST

Step	Command
Enable VPN on eth1.	`vyatta@WEST#` **`set vpn ipsec ipsec-interfaces interface eth1`**
Define the site-to-site connection to EAST. Set the authentication mode.	`vyatta@WEST#` **`set vpn ipsec site-to-site peer 192.0.2.33 authentication mode pre-shared-secret`**
Navigate to the node for the peer for easier editing.	`vyatta@WEST#` **`edit vpn ipsec site-to-site peer 192.0.2.33`** `[edit vpn ipsec site-to-site peer 192.0.2.33]`
Provide the string that will be used to authenticate the peers.	`vyatta@WEST#` **`set authentication pre-shared-secret test_key_1`** `[edit vpn ipsec site-to-site peer 192.0.2.33]`
Specify the default ESP group for all tunnels.	`vyatta@WEST#` **`set default-esp-group ESP-1W`** `[edit vpn ipsec site-to-site peer 192.0.2.33]`

Example 2-37 Defining the IPsec tunnel from WEST to EAST

Specify the IKE group.	`vyatta@WEST# set ike-group IKE-1W` `[edit vpn ipsec site-to-site peer 192.0.2.33]`
Identify the IP address on this Vyatta system to be used for this connection.	`vyatta@WEST# set local-ip 192.0.2.1` `[edit vpn ipsec site-to-site peer 192.0.2.33]`
Specify that only GRE traffic will pass through the tunnel.	`vyatta@WEST# set tunnel 1 protocol gre` `[edit vpn ipsec site-to-site peer 192.0.2.33]`
Return to the top of the configuration hierarchy.	`vyatta@WEST# top`
Commit the configuration.	`vyatta@WEST# commit`

View the modified configuration.	`vyatta@WEST# show vpn ipsec site-to-site peer 192.0.2.33`
	`authentication`
	`mode pre-shared-secret`
	`pre-shared-secret test_key_1`
	`}`
	`default-esp-group ESP-1W`
	`ike-group IKE-1W`
	`local-ip 192.0.2.1`
	`tunnel 1 {`
	`protocol gre`
	`}`

View IPsec interface configuration.	`vyatta@WEST# show vpn ipsec ipsec-interfaces` `interface eth1`
View Ethernet interface eth1 address configuration. **local-ip** is set to this address.	`vyatta@WEST# show interfaces ethernet eth1 address` `address 192.0.2.1/27`

Define a static route on "WEST"

Example 2-38 creates the static route for traffic destined for the far end of the GRE tunnel.

NOTE *Routing protocols can be used to specify how to get to the remote network. This method simply provides the minimal requirement to achieve this.*

- Send traffic destined for 192.168.60.0/24 to the far end of the GRE tunnel at 10.3.3.2.

To create the static route, perform the following steps on WEST in configuration mode:

Example 2-38 Defining a static route on WEST

Step	Command
Create the static route.	`vyatta@WEST#` **`set protocols static route 192.168.60.0/24 next-hop 10.3.3.2`**
Commit the configuration.	`vyatta@WEST#` **`commit`**

View the modified configuration.	`vyatta@WEST#` **`show protocols static route`**
	`192.168.60.0/24 {`
	`next-hop 10.3.3.2`
	`}`

Configure EAST

This section presents the following examples:

- Example 2-39 Defining the GRE tunnel from EAST to WEST
- Example 2-40 Defining the IPsec tunnel from EAST to WEST
- Example 2-41 Defining a static route on EAST

Define the GRE Tunnel on "EAST"

GRE tunnels are explained in detail in *Vyatta Tunnels Reference Guide*. Please see that guide for more information.

Example 2-1 defines EAST's end of the GRE tunnel. In this example:

- The tunnel interface tun0 on router EAST is assigned the IP address 10.3.3.2/30.
- The encapsulation type is set to GRE.
- The IP address on the local side of the GRE tunnel (**local-ip**) is set to that of the local Ethernet interface (192.0.2.33).
- The IP address of the other end of the GRE tunnel (**remote-ip**) is set to the address of the remote system (192.0.2.1).

To create the tunnel interface and the tunnel endpoint on EAST, perform the following steps in configuration mode:

Example 2-39 Defining the GRE tunnel from EAST to WEST

Step	Command
Create the GRE tunnel interface, and specify the IP address to be associated with it.	`vyatta@EAST# set interfaces tunnel tun0 address 10.3.3.2/30`
Assign a brief description for the GRE tunnel interface.	`vyatta@EAST# set interfaces tunnel tun0 description “GRE tunnel to router WEST”`
Specify the encapsulation mode for the tunnel.	`vyatta@EAST# set interfaces tunnel tun0 encapsulation gre`
Allow multicast protocols (e.g., routing protocols) to be carried over the tunnel.	`vyatta@EAST# set interfaces tunnel tun0 multicast enable`
Specify the local IP address for the GRE tunnel.	`vyatta@EAST# set interfaces tunnel tun0 local-ip 192.0.2.33`
Specify the remote IP address for the GRE tunnel.	`vyatta@EAST# set interfaces tunnel tun0 remote-ip 192.0.2.1`
Commit the configuration.	`vyatta@EAST# commit`

View the modified configuration.	`vyatta@EAST# show interfaces tunnel tun0`
	`address 10.3.3.2/30`
	`description “GRE tunnel to router WEST”`
	`encapsulation gre`
	`local-ip 192.0.2.33`
	`multicast enable`
	`remote-ip 192.0.2.1`

Define the IPsec Tunnel on “EAST”

Example 2-1 creates the IPsec tunnel from EAST to WEST.

- EAST uses IP address 192.0.2.33 on eth0.
- WEST uses IP address 192.0.2.1 on eth1.
- The IKE group is IKE-1E
- The preshared secret is “test_key_1”.
- All GRE traffic will be passed through the tunnel.

This examples assumes that you have already configured the following:

- IKE group IKE-1E (see page 28)
- ESP group ESP-1E (see page 29)

To create the IPsec tunnel from EAST to WEST, perform the following steps on EAST in configuration mode:

Example 2-40 Defining the IPsec tunnel from EAST to WEST

Step	Command
Enable VPN on eth0.	`vyatta@EAST# set vpn ipsec ipsec-interfaces interface eth0`
Define the site-to-site connection to WEST. Set the authentication mode.	`vyatta@EAST# set vpn ipsec site-to-site peer 192.0.2.1 authentication mode pre-shared-secret`
Navigate to the node for the peer for easier editing.	`vyatta@EAST# edit vpn ipsec site-to-site peer 192.0.2.1` `[edit vpn ipsec site-to-site peer 192.0.2.1]`
Provide the string that will be used to authenticate the peers.	`vyatta@EAST# set authentication pre-shared-secret test_key_1` `[edit vpn ipsec site-to-site peer 192.0.2.1]`
Specify the default ESP group for all tunnels.	`vyatta@EAST# set default-esp-group ESP-1E` `[edit vpn ipsec site-to-site peer 192.0.2.1]`
Specify the IKE group.	`vyatta@EAST# set ike-group IKE-1E` `[edit vpn ipsec site-to-site peer 192.0.2.1]`
Identify the IP address on this Vyatta system to be used for this connection.	`vyatta@EAST# set local-ip 192.0.2.33` `[edit vpn ipsec site-to-site peer 192.0.2.1]`
Specify that only GRE traffic will pass through the tunnel.	`vyatta@EAST# set tunnel 1 protocol gre` `[edit vpn ipsec site-to-site peer 192.0.2.1]`
Return to the top of the configuration hierarchy.	`vyatta@EAST# top`
Commit the configuration.	`vyatta@EAST# commit`

View the modified configuration.	`vyatta@EAST# show vpn ipsec site-to-site peer 192.0.2.1`
	` authentication`
	`   mode pre-shared-secret`
	`   pre-shared-secret test_key_1`
	` }`
	` default-esp-group ESP-1E`
	` ike-group IKE-1E`
	` local-ip 192.0.2.33`
	` tunnel 1 {`
	`   protocol gre`
	` }`

Example 2-40 Defining the IPsec tunnel from EAST to WEST

View IPsec interface configuration.	vyatta@EAST# **show vpn ipsec ipsec-interfaces** interface eth0
View Ethernet interface eth0 address configuration. **local-ip** is set to this address.	vyatta@EAST# **show interfaces ethernet eth0 address** address 192.0.2.33/27

DEFINE A STATIC ROUTE ON "EAST"

Example 2-41 creates the static route for traffic destined for the far end of the GRE tunnel.

NOTE *Routing protocols can be used to specify how to get to the remote network. This method simply provides the minimal requirement to achieve this.*

- Send traffic destined for 192.168.40.0/24 to the far end of the GRE tunnel at 10.3.3.1.

To create the static route, perform the following steps on EAST in configuration mode:

Example 2-41 Defining a static route on EAST

Step	Command
Create the static route.	vyatta@EAST# **set protocols static route 192.168.40.0/24 next-hop 10.3.3.1**
Commit the configuration.	vyatta@EAST# **commit**

View the modified configuration.	vyatta@EAST# **show protocols static route**
	 192.168.40.0/24 {
	   next-hop 10.3.3.1
	 }

Bridging

IPsec protected GRE Tunnels can be used to bridge LAN segments across a WAN. For further details see the Bridging chapter in the *Vyatta LAN Interfaces Reference Guide*.

Monitoring IPsec Site-to-Site VPN

This section presents the following topics:

- Showing IKE Information
- Showing IPsec Information
- Viewing IPsec VPN Debug Information
- Sending IPSec VPN Messages to Syslog

This section includes the following examples:

- Example 2-42 Viewing IKE security associations
- Example 2-43 Viewing IKE status information
- Example 2-44 Viewing IPsec security associations
- Example 2-45 Viewing IPsec statistics
- Example 2-46 Viewing IPsec status information
- Example 2-47 Viewing IPsec VPN debug information

NOTE *The sample output in these examples may show information unrelated to the sample configurations.*

Showing IKE Information

To see IKE security associations, you can use the **show vpn ike sa** command, as shown in Example 2-42.

Example 2-42 Viewing IKE security associations

```
vyatta@WEST> show vpn ike sa

Peer ID / IP                            Local ID / IP
------------                            -------------
192.168.1.1                             192.168.1.2

    Description: site-to-site x509 tunnel

    State  Encrypt  Hash  D-H Grp  NAT-T  A-Time  L-Time
    -----  -------  ----  -------  -----  ------  ------
    up     aes128   sha1  5        no     2162    28800

vyatta@WEST>
```

To see the status of the IKE process, you can use the **show vpn ike status** command, as shown in Example 2-43.

Example 2-43 Viewing IKE status information

```
vyatta@west> show vpn ike status
IKE Process Running

PID: 5832

vyatta@west>
```

Showing IPsec Information

To see IPsec security associations, you can use the **show vpn ipsec sa** command, as shown in Example 2-44.

Example 2-44 Viewing IPsec security associations

```
vyatta@WEST> show vpn ipsec sa
Peer ID / IP                            Local ID / IP
------------                            -------------
1.1.1.2                                 192.168.1.2

    Tunnel  State  Bytes Out/In   Encrypt  Hash  NAT-T  A-Time  L-Time  Proto
    ------  -----  ------------   -------  ----  -----  ------  ------  -----
    1       up     0.0/0.0        aes128   sha1  yes    3415    3600    GRE
    2       down   n/a            n/a      n/a   yes    0       3600    all


Peer ID / IP                            Local ID / IP
------------                            -------------
192.168.2.2                             192.168.1.2

    Tunnel  State  Bytes Out/In   Encrypt  Hash  NAT-T  A-Time  L-Time  Proto
    ------  -----  ------------   -------  ----  -----  ------  ------  -----
    1       down   n/a            n/a      n/a   no     0       3600    GRE
vyatta@WEST>
```

To see IPsec statistics, you can use the **show vpn ipsec statistics** command, as shown in Example 2-45.

Example 2-45 Viewing IPsec statistics

```
vyatta@WEST> show vpn ipsec sa statistics

Peer ID / IP                            Local ID / IP
------------                            -------------
1.1.1.2                                 192.168.1.2


  Tun# Dir Source Network               Destination Network          Bytes
  ---- --- --------------               -------------------          -----
  1    in  192.168.2.2/32               192.168.1.2/32               0.0
  1    out 192.168.1.2/32               192.168.2.2/32               0.0
  2    in  n/a                          n/a                          0.0
  2    out n/a                          n/a                          0.0


Peer ID / IP                            Local ID / IP
------------                            -------------
192.168.2.2                             192.168.1.2

  Tun# Dir Source Network               Destination Network          Bytes
  ---- --- --------------               -------------------          -----
  1    in  n/a                          n/a                          0.0
  1    out n/a                          n/a                          0.0

vyatta@WEST>
```

To see the status of the IPsec process, you can use the **show vpn ipsec status** command, as shown in Example 2-46.

Example 2-46 Viewing IPsec status information

```
vyatta@WEST> show vpn ipsec status
IPSec Process Running  PID: 5832

4 Active IPsec Tunnels

IPsec Interfaces:
  eth1    (10.6.0.55)


vyatta@WEST>
```

Viewing IPsec VPN Debug Information

To see more detailed information when you are troubleshooting, you can use the **show vpn debug** command, with or without the **detail** option. Example 2-47 shows the command without the **detail** option.

Example 2-47 Viewing IPsec VPN debug information

```
vyatta@WEST> show vpn debug
000 Status of IKEv1 pluto daemon (strongSwan 4.3.2):
000 interface lo/lo ::1:500
000 interface lo/lo 127.0.0.1:500
000 interface eth0/eth0 172.16.117.128:500
000 interface eth2/eth2 172.16.139.128:500
000 %myid = (none)
000 loaded plugins: curl ldap random pubkey openssl hmac gmp
000 debug options: none
000
000 "peer-172.16.139.160-tunnel-1": 172.16.139.128...172.16.139.160; erouted; eroute 
owner: #5
000 "peer-172.16.139.160-tunnel-1":  ike_life: 28800s; ipsec_life: 3600s; rekey_margin: 
540s; rekey_fuzz: 100%; keyingtries: 3
000 "peer-172.16.139.160-tunnel-1":   policy: PSK+ENCRYPT+TUNNEL+PFS+UP; prio: 32,32; 
interface: eth2;
000 "peer-172.16.139.160-tunnel-1":   newest ISAKMP SA: #4; newest IPsec SA: #5;
000 "peer-172.16.139.160-tunnel-1":   IKE proposal: AES_CBC_128/HMAC_SHA1/MODP_1536
000 "peer-172.16.139.160-tunnel-1":   ESP proposal: AES_CBC_128/HMAC_SHA1/<Phase1>
000
000 #5: "peer-172.16.139.160-tunnel-1" STATE_QUICK_R2 (IPsec SA established); 
EVENT_SA_REPLACE in 3292s; newest IPSEC; eroute owner
000 #5: "peer-172.16.139.160-tunnel-1" esp.c75a2bd9@172.16.139.160 (0 bytes) 
esp.d1c08d06@172.16.139.128 (0 bytes); tunnel
000 #4: "peer-172.16.139.160-tunnel-1" STATE_MAIN_R3 (sent MR3, ISAKMP SA established); 
EVENT_SA_REPLACE in 28491s; newest ISAKMP
--More--
```

Sending IPSec VPN Messages to Syslog

This section presents the following examples:

- Example 2-48 Setting VPN log mode

The IPsec process generates log messages during operation. You can direct the system to send IPsec log messages to syslog. The result will depend on how the system syslog is configured.

Keep in mind that in the current implementation, the main syslog file reports only messages of severity **warning** and above, regardless of the severity level configured. If you want to configure a different level of severity for log messages (for example, if you want to see debug messages during troubleshooting), you must configure syslog to send messages into a different file, which you define within syslog.

Configuring log modes is optional. When a log mode is not configured, IPsec log messages consist mostly of IPsec startup and shutdown messages. The log modes allow you to direct the system to inspect the IPsec packets and report the results.

Note that some log modes (for example, **all** and **control**) generate several log messages per packet. Using any of these options may severely degrade system performance.

VPN IPsec log messages use standard syslog levels of severity.

The Vyatta system supports the following logging modes for IPsec VPN.

Table 2-4 IPsec VPN logging modes

Severity	Meaning
raw	Shows the raw bytes of messages.
crypt	Shows the encryption and decryption of messages.
parsing	Shows the structure of input messages.
emitting	Shows the structure of output messages.
control	Shows the decision-making process of the IKE daemon (Pluto).
private	Allows debugging output with private keys.
all	Enables all logging options.

Note that some logging modes (for example, "all") print several messages per packet. Verbose logging modes can cause severe performance degradation.

Example 2-48 configures logging for VPN messages on WEST. In this example:

- Two logging modes are applied:
  - — **raw**, which shows the raw bytes of messages
  - — **crypt**, which shows the encryption and decryption of messages.

To configure logging in this way, perform the following steps on WEST in configuration mode:

Example 2-48 Setting VPN log mode

Step	Command
Apply a log mode of raw.	vyatta@WEST# **set vpn ipsec logging log-modes raw**
Apply a second log mode of crypt.	vyatta@WEST# **set vpn ipsec logging log-modes crypt**
Commit the configuration.	vyatta@WEST# **commit**

View the configuration for logging.	vyatta@WEST# **exit**
	vyatta@WEST> **show vpn ipsec logging**
	    log-modes raw
	    log-modes crypt

IPsec Site-to-Site VPN Commands

This chapter contains the following commands.

Configuration Commands	
Global IPsec	
vpn ipsec	Enables IPsec VPN functionality on the system.
vpn ipsec auto-update <interval>	Specifies the interval to automatically refresh IPsec connections.
vpn ipsec ipsec-interfaces interface <if-name>	Enables IPsec VPN on an interface.
vpn ipsec logging	Specifies logging options for IPsec VPN.
vpn ipsec nat-networks allowed-network <ipv4net>	Specifies the private network addresses that remote hosts behind a NAT device may use.
vpn ipsec nat-traversal <state>	Specifies whether the local VPN gateway proposes NAT Traversal capability.
ESP Group	
vpn ipsec esp-group <name>	Defines a named ESP configuration for IKE Phase 2 negotiations.
vpn ipsec esp-group <name> compression <state>	Specifies whether this VPN gateway should propose the use of compression.
vpn ipsec esp-group <name> lifetime <lifetime>	Specifies how long an ESP encryption key can stay in effect.
vpn ipsec esp-group <name> mode <mode>	Specifies the IPsec connection mode to be used.
vpn ipsec esp-group <name> pfs <pfs>	Specifies whether or not PFS is used.
vpn ipsec esp-group <name> proposal <num>	Defines an ESP group proposal for IKE Phase 2 negotiation.
vpn ipsec esp-group <name> proposal <num> encryption <cipher>	Specifies the encryption cipher for an ESP proposal.
vpn ipsec esp-group <name> proposal <num> hash <hash>	Specifies the hash algorithm for an ESP proposal.
IKE Group	
vpn ipsec ike-group <name>	Defines a named IKE configuration for IKE Phase 1 negotiations.

vpn ipsec ike-group <name> dead-peer-detection	Defines the behavior if the VPN peer becomes unreachable.
vpn ipsec ike-group <name> lifetime <lifetime>	Specifies how long an IKE group key can stay in effect.
vpn ipsec ike-group <name> proposal <num>	Specifies the IKE group proposal number.
vpn ipsec ike-group <name> proposal <num> dh-group <group>	Specifies the Oakley group to be proposed for Diffie-Hellman key exchanges.
vpn ipsec ike-group <name> proposal <num> encryption <cipher>	Specifies the encryption cipher to be proposed in IKE Phase 1 negotiation.
vpn ipsec ike-group <name> proposal <num> hash <hash>	Specifies the hash algorithm to be proposed.
IPsec Peer	
vpn ipsec site-to-site peer <peer>	Defines a site-to-site connection between the Vyatta system and another VPN gateway.
vpn ipsec site-to-site peer <peer> authentication id <id>	Specifies local authentication credentials to send to the VPN peer.
vpn ipsec site-to-site peer <peer> authentication mode <mode>	Specifies the authentication method to be used for the connection with the VPN peer.
vpn ipsec site-to-site peer <peer> authentication pre-shared-secret <secret>	Specifies the pre-shared secret used to authenticate the VPN peer.
vpn ipsec site-to-site peer <peer> authentication remote-id <id>	Specifies the authentication credentials of the VPN peer.
vpn ipsec site-to-site peer <peer> authentication rsa-key-name <name>	Specifies the name of the digital signature used to authenticate the VPN peer.
vpn ipsec site-to-site peer <peer> authentication x509 ca-cert-file <file-name>	Specifies the name of an X.509 Certificate Authority (CA) certificate file for IPsec authentication of the VPN peer.
vpn ipsec site-to-site peer <peer> authentication x509 cert-file <file-name>	Specifies the name of the VPN server's certificate file for IPsec authentication of the VPN peer.
vpn ipsec site-to-site peer <peer> authentication x509 crl-file <file-name>	Specifies the name of an X.509 Certificate Revocation List (CRL) file for IPsec authentication of the VPN peer.
vpn ipsec site-to-site peer <peer> authentication x509 key file <file-name>	Specifies the name of VPN server's private key file for IPsec authentication of the VPN peer.
vpn ipsec site-to-site peer <peer> authentication x509 key password <password>	Specifies the password that protects the VPN server's private key.
vpn ipsec site-to-site peer <peer> connection-type	Specifies the type of peer connection.

vpn ipsec site-to-site peer <peer> default-esp-group <name>	Specifies a default ESP configuration to use for all tunnels to the peer.
vpn ipsec site-to-site peer <peer> dhcp-interface <interface>	Specifies a DHCP client interface to use for the connection.
vpn ipsec site-to-site peer <peer> ike-group <group>	Specifies the named IKE configuration to be used for a peer connection.
vpn ipsec site-to-site peer <peer> local-ip <ipv4>	Specifies the local IP address to be used as the source IP for packets destined for the remote peer.
vpn ipsec site-to-site peer <peer> tunnel <tunnel> allow-nat-networks <state>	Specifies whether or not a connection to a private network is allowed.
vpn ipsec site-to-site peer <peer> tunnel <tunnel> allow-public-networks <state>	Specifies whether or not a connection to a public network is allowed.
vpn ipsec site-to-site peer <peer> tunnel <tunnel> esp-group <name>	Specifies an ESP configuration to use for this tunnel.
vpn ipsec site-to-site peer <peer> tunnel <tunnel> local	Defines local configuration options for the IPsec tunnel.
vpn ipsec site-to-site peer <peer> tunnel <tunnel> protocol <protocol>	Specifies the protocol to match for traffic to enter the tunnel.
vpn ipsec site-to-site peer <peer> tunnel <tunnel> remote	Defines remote configuration options for the IPsec tunnel.
RSA Keys	
generate vpn rsa-key	Generates an RSA digital signature for the local host.
vpn rsa-keys	Records RSA keys for the local host.
Operational Commands	
clear vpn ipsec-peer <peer>	Restarts tunnels associated with the IPsec peer.
generate vpn rsa-key	Generates an RSA digital signature for the local host.
generate vpn x509 key-pair <name>	Generates an X.509 private key file and a certificate signing request file.
restart vpn	Restarts the IPsec process.
show vpn debug	Provides trace-level information about IPsec VPN.
show vpn ike rsa-keys	Displays RSA public keys recorded in the system.
show vpn ike sa	Provides information about all currently active IKE (ISAKMP) security associations.
show vpn ike secrets	Displays configured pre-shared secrets.

show vpn ike status	Displays summary information about the IKE process.
show vpn ipsec sa	Provides information about active IPsec security associations.
show vpn ipsec sa detail	Provides detailed information about active IPsec security associations.
show vpn ipsec sa nat-traversal	Provides information about all active IPsec security associations that are using NAT Traversal.
show vpn ipsec sa statistics	Display statistics information about active IPsec security associations.
show vpn ipsec status	Displays information about the status of IPsec processes.

clear vpn ipsec-peer <peer>

Restarts tunnels associated with the IPsec peer.

Syntax

clear vpn ipsec-peer *peer* [**tunnel** *tunnel*]

Command Mode

Operational mode.

Parameters

peer	The IP address of the VPN peer.
tunnel	The tunnel to be restarted.

Usage Guidelines

Use this command to restart IPsec tunnels associated with the specified peer. Restarting IPsec tunnels will cause the tunnels to be torn down and re-established.

If the **peer** is 0.0.0.0, “any”, or @id, then the tunnel is torn down and re-loaded but a new connection is not initiated because the remote end could be multiple end-points.

If no **tunnel** is specified then all tunnels associated with the peer will be restarted.

generate vpn rsa-key

Generates an RSA digital signature for the local host.

Syntax

generate vpn rsa-key [**bits** *16-4096* [**random** *random-device*]]

Command Mode

Operational mode.

Parameters

bits	Specifies the bit-length of the generated key, in 16-bit increments. The range is 16 to 4096. The default is 2192.
random *random-device*	Specifies the Linux kernel random number source device to use for generating random numbers. Supported values are as follows: **/dev/random**: Uses the **/dev/random** random device, which uses the system entropy to seed the random number generator. This is more secure than software generation, but can be extremely slow. See the "Usage Guidelines" for more information. **/dev/urandom**: Uses the **/dev/urandom** random device, which is a software random number generator. The default is **/dev/random**.

Usage Guidelines

Use this command to generate an RSA digital signature for the local host. This command is only available to users with administrative privileges.

RSA digital signatures are used to authenticate communications. To use RSA authentication, you must generate an RSA digital signature for the local host. This digital signature will have both a public key portion and a private key portion. The public key portion must be shared with the remote peer so that it can decrypt communications from this host.

The RSA digital signature for the local host can be generated using this command in operational mode. Once generated, the key is stored at the location specified by the **local-key rsa-key-name** option. By default, this is the **localhost.key** file in the **/config/ipsec.d/rsa-keys/** directory.

You can change the name and location where the key file is stored using the vpn rsa-keys command.

NOTE *If you save a configuration to floppy after changing the name and location of the localhost.keys file, then booting the system from LiveCD may generate a parse error because it will not be able to find the file.*

System entropy random number generation is more secure than software random number generation. However, in the Vyatta router's case, **/dev/random** may take a very long time to generate a key, because there may be limited system activity. In some cases, simply typing on the keyboard can generate sufficient entropy, but in others, the system may appear to hang for a long time—on the order of 45 minutes.

To avoid this, you can use a random device that does not rely on system entropy, such as /dev/urandom, which is a software random number generator; for example:

```
generate vpn rsa-key bits 2192 random /dev/urandom
```

Keep the following in mind:

If you are using **/dev/random** because security is a concern, keep in mind that you can increase the strength of the key simply by specifying a longer key length.

If you do use the **/dev/random** random device and key generation takes too long, remember that you can use <Ctrl>+c to interrupt the process.

generate vpn x509 key-pair <name>

Generates an X.509 private key file and a certificate signing request file.

Syntax

generate vpn x509 key-pair *name*

Command Mode

Operational mode.

Parameters

name	The name to be used for the X.509 private key file and certificate signing request file. The private key file will be called /config/auth/*name*.key and the certificate signing request file will be called /config/auth/*name*.csr.

Usage Guidelines

Use this command to generate an X.509 private key file and a certificate signing request file. The private key file is required for configuring a VPN for X.509 authentication (see vpn ipsec site-to-site peer <peer> authentication x509 key file <file-name>). The certificate signing request file must be sent to a certificate authority (CA). In return, the CA will provide a server certificate (e.g. *name*.crt), a CA certificate (e.g. ca.crt), and potentially, a certificate revocation list (.crl) file. This procedure varies according to the CA being used. The files returned are also used to configure a VPN for X.509 authentication (see vpn ipsec site-to-site peer <peer> authentication x509 cert-file <file-name> for specifying the server certificate, vpn ipsec site-to-site peer <peer> authentication x509 ca-cert-file <file-name> for specifying the CA certificate, and vpn ipsec site-to-site peer <peer> authentication x509 crl-file <file-name> for specifying the certificate revocation list).

restart vpn

Restarts the IPsec process.

Syntax

restart vpn

Command Mode

Operational mode.

Parameters

None.

Usage Guidelines

Use this command to restart the IPsec process.

Restarting IPsec will cause all tunnels to be torn down and re-established.

Examples

Example 2-49 shows the output resulting from the **restart vpn** command.

Example 2-49 “restart vpn” sample output

```
vyatta@WEST> restart vpn
Stopping Openswan IPsec…
Starting Openswan IPsec 2.4.6…

vyatta@WEST>
```

show vpn debug

Provides trace-level information about IPsec VPN.

Syntax

show vpn debug [**detail**]

Command Mode

Operational mode.

Parameters

detail	Provides extra verbose output at the trace level.

Usage Guidelines

Use this command to view trace-level messages for IPsec VPN.

This command is useful for troubleshooting and diagnostic situations.

Examples

Example 2-50 shows the output of the **show vpn debug** command.

Example 2-50 "show vpn debug" sample output

```
vyatta@WEST> show vpn debug
000 Status of IKEv1 pluto daemon (strongSwan 4.3.2):
000 interface lo/lo ::1:500
000 interface lo/lo 127.0.0.1:500
000 interface eth0/eth0 172.16.117.128:500
000 interface eth2/eth2 172.16.139.128:500
000 %myid = (none)
000 loaded plugins: curl ldap random pubkey openssl hmac gmp
000 debug options: none
000
000 "peer-172.16.139.160-tunnel-1": 172.16.139.128...172.16.139.160; erouted; eroute
owner: #5
000 "peer-172.16.139.160-tunnel-1":  ike_life: 28800s; ipsec_life: 3600s; rekey_margin:
540s; rekey_fuzz: 100%; keyingtries: 3
```

```
000 "peer-172.16.139.160-tunnel-1":   policy: PSK+ENCRYPT+TUNNEL+PFS+UP; prio: 32,32;
interface: eth2;
000 "peer-172.16.139.160-tunnel-1":   newest ISAKMP SA: #4; newest IPsec SA: #5;
000 "peer-172.16.139.160-tunnel-1":   IKE proposal: AES_CBC_128/HMAC_SHA1/MODP_1536
000 "peer-172.16.139.160-tunnel-1":   ESP proposal: AES_CBC_128/HMAC_SHA1/<Phase1>
000
000 #5: "peer-172.16.139.160-tunnel-1" STATE_QUICK_R2 (IPsec SA established);
EVENT_SA_REPLACE in 3292s; newest IPSEC; eroute owner
000 #5: "peer-172.16.139.160-tunnel-1" esp.c75a2bd9@172.16.139.160 (0 bytes)
esp.d1c08d06@172.16.139.128 (0 bytes); tunnel
000 #4: "peer-172.16.139.160-tunnel-1" STATE_MAIN_R3 (sent MR3, ISAKMP SA established);
EVENT_SA_REPLACE in 28491s; newest ISAKMP
--More--
```

Example 2-51 shows the output of the **show vpn debug detail** command.

Example 2-51 "show vpn debug detail" sample output

```
vyatta@WEST> show vpn debug detail
Unable to find IKEv2 messages. Strongswan might be running with IKEv2 turned off or
alternatively, your log files have been emptied (ie, logwatch)
vDUT-1
Wed Jan 20 23:22:27 GMT 2010
+ _________________________ version
+ ipsec --version
Linux strongSwan U4.3.2/K2.6.31-1-586-vyatta
Institute for Internet Technologies and Applications
University of Applied Sciences Rapperswil, Switzerland
See 'ipsec --copyright' for copyright information.
+ _________________________ /proc/net/pfkey
+ test -r /proc/net/pfkey
+ cat /proc/net/pfkey
sk       RefCnt Rmem   Wmem   User   Inode
+ _________________________ ip-xfrm-state
+ ip -s xfrm state
src 172.16.139.128 dst 172.16.139.160
   proto esp spi 0xc75a2bd9(3344575449) reqid 16385(0x00004001) mode tunnel
   replay-window 32 seq 0x00000000 flag  (0x00000000)
   auth hmac(sha1) 0x7cd0c727850b972ef14ad983e4067833ac9e9b74 (160 bits)
   enc cbc(aes) 0x492215c8e674a858e887d23b05ec8fb1 (128 bits)
   sel src 0.0.0.0/0 dst 0.0.0.0/0 uid 0
   lifetime config:
     limit: soft (INF)(bytes), hard (INF)(bytes)
     limit: soft (INF)(packets), hard (INF)(packets)
     expire add: soft 0(sec), hard 0(sec)
     expire use: soft 0(sec), hard 0(sec)
```

```
    lifetime current:
      0(bytes), 0(packets)
      add 2010-01-20 22:44:56 use -
    stats:
      replay-window 0 replay 0 failed 0
--More--
```

show vpn ike rsa-keys

Displays RSA public keys recorded in the system.

Syntax

show vpn ike rsa-keys

Command Mode

Operational mode.

Parameters

None.

Usage Guidelines

Use this command to display the public portion of all RSA digital signatures recorded on the system.

This will include the public portion of the RSA digital signature of the local host (the private portion will not be displayed), plus the public key configured for any VPN peer.

Examples

Example 2-52 shows output of the **show vpn ike rsa-keys** command, which displays the RSA digital signatures stored on router WEST. In this example:

- The public portion of the key for the local host is shown, but the private portion of the local key remains hidden in the RSA keys file.
- The RSA public key recorded for the VPN peer EAST is also shown.

Example 2-52 "show vpn ike rsa-keys" sample output

```
vyatta@WEST> show vpn ike rsa-keys

Local public key
0sAQNfpZicOXWl1rMvNWLIfFppq1uWtUvj8esyjBl/zBfrK4ecZbt7WzMdMLiLugYtVgo+zJ
QV5dmQnN+n3qkU9ZLM5QWBxG4iLFtYcwC5fCMx0hBJfnIEd68d11h7Ea6J4IAm3ZWXcBeOV4
S8mC4HV+mqZfv3xyh1ELjfmLM3fWkp8g5mX7ymgcTpneHiSYX1T9NU3i2CHjYfeKPFb4zJIo
pu2R654kODGOa+4r241Zx3cDIJgHBYSYOiSFYbcdQhKQS3cclFPGVMHYGXjjoiUSA7d2eMab
DtIU4FwnqH3qVN/kdedK34sEJiMUgieT6pJQ6W8y+5PgESvouykx8cyTiOobnx0G9oqFcxYL
knQ3GbrPej
```

```
==============================================================
Peer IP: 10.1.0.55  (EAST)

0sAQOVBIJL+rIkpTuwh8FPeceAF0bhgLr++W51bOAIjFbRDbR8gX3Vlz6wiUbMgGwQxWlYQi
qsCeacicsfZx/amlEn9PkSE4e7tqK/JQo40L5C7gcNM24mup1d+0WmN3zLb9Qhmq5q3pNJxE
wnVbPPQeIdZMJxnb1+lA8DPC3SIxJM/3at1/KrwqCAhX3QNFY/zNmOtFogELCeyl4+d54wQl
jA+3dwFAQ4bboJ7YIDs+rqORxWd3l3I7IajT/pLrwr5eZ8OA9NtAedbMiCwxyuyUbznxXZ8Z
/MAi3xjL1pjYyWjNNiOij82QJfMOrjoXVCfcPn96ZN+Jqk+KknoVeNDwzpoahFOseJREeXzk
w3/lkMN9N1
vyatta@WEST>
```

show vpn ike sa

Provides information about all currently active IKE (ISAKMP) security associations.

Syntax

show vpn ike sa [**nat-traversal** | **peer** *peer*]

Command Mode

Operational mode.

Parameters

nat-traversal	Displays all the IKE SAs that are using RFC 3947 NAT Traversal.
peer	Shows IKE SA information for the specified VPN peer. The format is the IP address of the peer. There will be at most one IKE SA per peer (except possibly during re-key negotiation).

Usage Guidelines

Use this command to display information about IKE security associations (SAs).

Examples

Example 2-53 shows the output of the **show vpn ike sa** command.

Example 2-53 "show vpn ike sa" sample output

```
vyatta@WEST> show vpn ike sa

Peer ID / IP                            Local ID / IP
------------                            -------------
192.168.1.1                             192.168.1.2

    Description: site-to-site x509 tunnel

    State  Encrypt  Hash  D-H Grp  NAT-T  A-Time  L-Time
    -----  -------  ----  -------  -----  ------  ------
```

```
    up      aes128    sha1   5         no      2162     28800

vyatta@WEST>
```

show vpn ike secrets

Displays configured pre-shared secrets.

Syntax

show vpn ike secrets

Command Mode

Operational mode.

Parameters

None.

Usage Guidelines

Use this command to display information about pre-shared secrets recorded in the system.

Examples

Example 2-54 shows the output of the **show vpn ike secrets** command.

Example 2-54 "show vpn ike secrets" sample output

```
vyatta@WEST> show vpn ike secrets

Local IP/ID                              Peer IP/ID
----------                               ----------
192.168.1.2                              1.1.1.2
N/A                                      192.168.2.2

    Secret: "secret"


Local IP/ID                              Peer IP/ID
-----------                              ----------
192.168.1.2                              192.168.2.2
N/A                                      192.168.2.2

    Secret: "secret"
```

show vpn ike status

Displays summary information about the IKE process.

Syntax

show vpn ike status

Command Mode

Operational mode.

Parameters

None

Usage Guidelines

Use this command to see the status of the IKE process.

Examples

Example 2-55 shows the output of the **show vpn ike status** command.

Example 2-55 “show vpn ike status” sample output

```
vyatta@west> show vpn ike status
IKE Process Running

PID: 5832

vyatta@west>
```

show vpn ipsec sa

Provides information about active IPsec security associations.

Syntax

show vpn ipsec sa [**peer** *peer* [**tunnel** *tunnel*]]

Command Mode

Operational mode.

Parameters

peer	The peer to display information about.
tunnel	The tunnel to display information about.

Usage Guidelines

Use this command to display information about remote VPN peers and IPsec security associations (SAs) currently in effect.

Examples

Example 2-56 shows the output of the **show vpn ipsec sa** command.

Example 2-56 "show vpn ipsec sa" sample output

```
vyatta@WEST> show vpn ipsec sa
Peer ID / IP                            Local ID / IP
------------                            -------------
1.1.1.2                                 192.168.1.2

    Tunnel  State  Bytes Out/In   Encrypt  Hash  NAT-T  A-Time  L-Time  Proto
    ------  -----  ------------   -------  ----  -----  ------  ------  -----
    1       up     0.0/0.0        aes128   sha1  yes    3415    3600    GRE
    2       down   n/a            n/a      n/a   yes    0       3600    all


Peer ID / IP                            Local ID / IP
------------                            -------------
192.168.2.2                             192.168.1.2
```

```
    Tunnel  State  Bytes Out/In   Encrypt  Hash  NAT-T  A-Time  L-Time  Proto
    ------  -----  ------------   -------  ----  -----  ------  ------  -----
    1       down   n/a            n/a      n/a   no     0       3600    GRE
vyatta@WEST>
```

Example 2-57 shows the output of the **show vpn ipsec sa peer** *peer* command.

Example 2-57 "show vpn ipsec sa peer *peer*" sample output

```
vyatta@WEST> show vpn ipsec sa peer 1.1.1.2

Peer ID / IP                            Local ID / IP
------------                            -------------
1.1.1.2                                 192.168.1.2

    Tunnel  State  Bytes Out/In   Encrypt  Hash  NAT-T  A-Time  L-Time  Proto
    ------  -----  ------------   -------  ----  -----  ------  ------  -----
    1       up     0.0/0.0        aes128   sha1  yes    3415    3600    GRE
    2       down   n/a            n/a      n/a   yes    0       3600    all

vyatta@WEST>
```

Example 2-58 shows the output of the **show vpn ipsec sa peer** *peer* **tunnel** *tunnel* command.

Example 2-58 "show vpn ipsec sa peer *peer* tunnel *tunnel*" sample output

```
vyatta@WEST> show vpn ipsec sa peer 1.1.1.2 tunnel 1

Peer ID / IP                            Local ID / IP
------------                            -------------
1.1.1.2                                 192.168.1.2

    Tunnel  State  Bytes Out/In   Encrypt  Hash  NAT-T  A-Time  L-Time  Proto
    ------  -----  ------------   -------  ----  -----  ------  ------  -----
    1       up     0.0/0.0        aes128   sha1  yes    3415    3600    GRE

vyatta@WEST>
```

show vpn ipsec sa detail

Provides detailed information about active IPsec security associations.

Syntax

show vpn ipsec sa detail [**peer** *peer* [**tunnel** *tunnel*]]

Command Mode

Operational mode.

Parameters

peer	The peer to display information about.
tunnel	The tunnel to display information about.

Usage Guidelines

Use this command to displaydetailed information about remote VPN peers and IPsec security associations (SAs) currently in effect.

Examples

Example 2-59 shows the output of the **show vpn ipsec sa detail** command.

Example 2-59 “show vpn ipsec sa detail” sample output

```
vyatta@WEST> show vpn ipsec sa detail
------------------------------------------------------------------
Peer IP:                192.168.1.1
Peer ID:                r2
Local IP:               192.168.1.2
Local ID:               r1
NAT Traversal:          no
NAT Source Port:        n/a
NAT Dest Port:          n/a

Description: site-to-site x509 tunnel

    Tunnel 1:
        State:                  up
```

```
        Inbound SPI:            714f7f33
        Outbound SPI:           8a84d58
        Encryption:             aes128
        Hash:                   sha1
        PFS Group:              5

        CA:
            C=US
            ST=CA
            L=BELMONT
            O=Organization
            CN=CertAuth
            E=test@example.com

        Local Net:              172.16.0.0/24
        Local Protocol:         all
        Local Port:             all

        Remote Net:             172.16.1.0/24
        Remote Protocol:        all
        Remote Port:            all

        Inbound Bytes:          0.0
        Outbound Bytes:         0.0
        Active Time (s):        1876
        Lifetime (s):           3600

vyatta@WEST>
```

Example 2-60 shows the output of the **show vpn ipsec sa detail peer** *peer* command for an x509 tunnel (note the "CA" information).

Example 2-60 "show vpn ipsec sa detail peer *peer*" sample output

```
vyatta@WEST> show vpn ipsec sa detail peer 192.168.1.1
------------------------------------------------------------------
Peer IP:                192.168.1.1
Peer ID:                r2
Local IP:               192.168.1.2
Local ID:               r1
NAT Traversal:          no
NAT Source Port:        n/a
NAT Dest Port:          n/a

Description: site-to-site x509 tunnel
```

```
    Tunnel 1:
        State:                  up
        Inbound SPI:            714f7f33
        Outbound SPI:           8a84d58
        Encryption:             aes128
        Hash:                   sha1
        PFS Group:              5

        CA:
            C=US
            ST=CA
            L=BELMONT
            O=Organization
            CN=CertAuth
            E=test@example.com

        Local Net:              172.16.0.0/24
        Local Protocol:         all
        Local Port:             all

        Remote Net:             172.16.1.0/24
        Remote Protocol:        all
        Remote Port:            all

        Inbound Bytes:          0.0
        Outbound Bytes:         0.0
        Active Time (s):        1876
        Lifetime (s):           3600

vyatta@WEST>
```

show vpn ipsec sa nat-traversal

Provides information about all active IPsec security associations that are using NAT Traversal.

Syntax

show vpn ipsec sa nat-traversal

Command Mode

Operational mode.

Parameters

None.

Usage Guidelines

Use this command to display information about all active IPsec security associations that are using RFC 3947 NAT Traversal.

show vpn ipsec sa statistics

Display statistics information about active IPsec security associations.

Syntax

show vpn ipsec sa statistics [peer *peer* **[tunnel** *tunnel*]]

Command Mode

Operational mode.

Parameters

peer	The peer to display information about.
tunnel	The tunnel to display information about.

Usage Guidelines

Use this command to see statistics for active IPsec security associations.

Examples

Example 2-61 shows the output of the **show vpn ipsec sa statistics** command.

Example 2-61 "show vpn ipsec sa statistics" sample output

```
vyatta@WEST> show vpn ipsec sa statistics

Peer ID / IP                            Local ID / IP
------------                            -------------
1.1.1.2                                 192.168.1.2


  Tun# Dir Source Network               Destination Network          Bytes
  ---- --- --------------               -------------------          -----
  1    in  192.168.2.2/32               192.168.1.2/32               0.0
  1    out 192.168.1.2/32               192.168.2.2/32               0.0
  2    in  n/a                          n/a                          0.0
  2    out n/a                          n/a                          0.0
```

```
Peer ID / IP                            Local ID / IP
------------                            -------------
192.168.2.2                             192.168.1.2

  Tun# Dir Source Network               Destination Network          Bytes
  ---- --- --------------               -------------------          -----
  1    in  n/a                          n/a                          0.0
  1    out n/a                          n/a                          0.0

vyatta@WEST>
```

show vpn ipsec status

Displays information about the status of IPsec processes.

Syntax

show vpn ipsec status

Command Mode

Operational mode.

Parameters

None

Usage Guidelines

Use this command to display information about the status about running IPsec processes.

The information shown includes:

- The process ID
- The number of active tunnels
- The interfaces configured for IPsec
- The IP addresses of interfaces configured for IPsec

Examples

Example 2-62 shows the output of the **show vpn ipsec status** command.

Example 2-62 "show vpn ipsec status" sample output

```
vyatta@WEST> show vpn ipsec status
IPSec Process Running  PID: 5832

4 Active IPsec Tunnels

IPsec Interfaces:
  eth1    (10.6.0.55)


vyatta@WEST>
```

vpn ipsec

Enables IPsec VPN functionality on the system.

Syntax

set vpn ipsec

delete vpn ipsec

show vpn ipsec

Command Mode

Configuration mode.

Configuration Statement

```
vpn {
    ipsec {
    }
}
```

Parameters

None.

Default

None.

Usage Guidelines

Use this command to enable IPsec VPN functionality on the Vyatta System.

To configure VPN connections, you must also enable IPsec VPN on each interface to be used for sending and receiving VPN traffic. To do this, use the vpn ipsec ipsec-interfaces interface <if-name> command.

NOTE *The sending and receiving of ICMP redirects is disabled when IPsec VPN is configured.*

Use the **set** form of this command to enable IPsec VPN.

Use the **delete** form of this command to remove all IPsec VPN configuration and disable IPsec VPN functionality.

Use the **show** form of this command to view the IPsec VPN configuration.

vpn ipsec auto-update <interval>

Specifies the interval to automatically refresh IPsec connections.

Syntax

set vpn ipsec auto-update *interval*

delete vpn ipsec auto-update

show vpn ipsec auto-update

Command Mode

Configuration mode.

Configuration Statement

```
vpn {
    ipsec {
        auto-update interval
    }
}
```

Parameters

interval	The interval (seconds) in which to review IPsec connections for changes (for example, the IP address of a dynamic DNS peer changes) and restart them if changes are found. The range is 30 to 65535.

Default

IPsec connections are not refreshed periodically.

Usage Guidelines

Use this command to specify the interval to automatically refresh IPsec connections. This is most useful for connections where the remote peer uses dynamic DNS to keep track of its address. Auto-update will review information pertaining to the connection at the specified interval and, if it is changed (for example, if the dynamic DNS peer's IP address has changed), will restart the connection.

Use the **set** form of this command to specify the interval at which to automatically refresh IPsec connections.

Use the **delete** form of this command to remove the configuration.

Use the **show** form of this command to view the configuration.

vpn ipsec esp-group <name>

Defines a named ESP configuration for IKE Phase 2 negotiations.

Syntax

set vpn ipsec esp-group *name*

delete vpn ipsec esp-group

show vpn ipsec esp-group

Command Mode

Configuration mode.

Configuration Statement

```
vpn {
    ipsec {
        esp-group name {
        }
    }
}
```

Parameters

name	Multi-node. The name to be used to refer to the ESP configuration. You can create multiple ESP configurations by creating multiple **esp-group** configuration nodes. At least one ESP configuration must be defined, for use in tunnel configuration.

Default

None.

Usage Guidelines

Use this command to define an ESP group.

An ESP group lets you set the Encapsulating Security Payload (ESP) parameters required for IKE Phase 2, and to set the lifetime of the resulting IPsec security association.

Use the **set** form of this command to create and modify an ESP group.

Use the **delete** form of this command to remove ESP group configuration.

Use the **show** form of this command to view ESP group configuration.

vpn ipsec esp-group <name> compression <state>

Specifies whether this VPN gateway should propose the use of compression.

Syntax

set vpn ipsec esp-group *name* **compression** *state*

delete vpn ipsec esp-group *name* **compression**

show vpn ipsec esp-group *name* **compression**

Command Mode

Configuration mode.

Configuration Statement

```
vpn {
    ipsec {
        esp-group name {
            compression state
        }
    }
}
```

Parameters

name	The name to be used to refer to the ESP configuration.
state	Enables or disables proposal of ESP compression. Supported values are as follows: **enable**: Enables proposal of ESP compression. **disable**: Disables proposal ESP compression.

Default

ESP compression is disabled.

Usage Guidelines

Use this command to specify whether or not to propose ESP compression during IKE Phase 2 negotiation.

NOTE *Regardless of this setting, if the other gateway proposes compression, this gateway will comply.*

Use the **set** form of this command to specify whether or not to enable ESP compression.

Use the **delete** form of this command to restore the default behavior.

Use the **show** form of this command to view ESP compression configuration.

vpn ipsec esp-group <name> lifetime <lifetime>

Specifies how long an ESP encryption key can stay in effect.

Syntax

set vpn ipsec esp-group *name* **lifetime** *lifetime*

delete vpn ipsec esp-group *name* **lifetime**

show vpn ipsec esp-group *name* **lifetime**

Command Mode

Configuration mode.

Configuration Statement

```
vpn {
    ipsec {
        esp-group name {
            lifetime lifetime
        }
    }
}
```

Parameters

name	The name to be used to refer to the ESP configuration.
lifetime	The time, in seconds, that any key created during IKE Phase 2 negotiation can persist before the next negotiation is triggered. The range is 30 to 86400 (that is, 24 hours). The default is 3600 (1 hour).

Default

Keys stay in effect for 3,600 seconds (1 hour).

Usage Guidelines

Use this command to specify the lifetime of a key.

Use the **set** form of this command to specify the lifetime of a key.

Use the **delete** form of this command to remove the lifetime configuration.

Use the **show** form of this command to view the lifetime configuration.

vpn ipsec esp-group <name> mode <mode>

Specifies the IPsec connection mode to be used.

Syntax

set vpn ipsec esp-group *name* **mode** *mode*

delete vpn ipsec esp-group *name* **mode**

show vpn ipsec esp-group *name* **mode**

Command Mode

Configuration mode.

Configuration Statement

```
vpn {
    ipsec {
        esp-group name {
            mode mode
        }
    }
}
```

Parameters

name	The name to be used to refer to the ESP configuration.
mode	The IPsec connection mode. Supported values are as follows: **tunnel**: Tunnel mode. **transport**: Transport mode.

Default

IPsec connections use tunnel mode.

Usage Guidelines

Use this command to specify the IPsec connection mode to be used.

Use the **set** form of this command to specify the IPsec connection mode to be used.

Use the **delete** form of this command to restore the default IPsec connection mode.

Use the **show** form of this command to view IPsec connection mode configuration.

vpn ipsec esp-group <name> pfs <pfs>

Specifies whether or not PFS is used.

Syntax

set vpn ipsec esp-group *name* **pfs** *pfs*

delete vpn ipsec esp-group *name* **pfs**

show vpn ipsec esp-group *name* **pfs**

Command Mode

Configuration mode.

Configuration Statement

```
vpn {
    ipsec {
        esp-group name {
            pfs pfs
        }
    }
}
```

Parameters

name	The name to be used to refer to the ESP configuration.
pfs	Enables or disables Perfect Forward Secrecy. Supported values are as follows: **enable:** Enables Perfect Forward Secrecy using Diffie-Hellman group defined in the ike-group. **dh-group2:** Enables Perfect Forward Secrecy using Diffie-Hellman group 2. **dh-group5:** Enables Perfect Forward Secrecy using Diffie-Hellman group 5. **disable:** Disables Perfect Forward Secrecy.

Default

Perfect Forward Secrecy is enabled and uses the Diffie-Hellman group defined in the ike-group.

Usage Guidelines

Use this command to specify whether or not Perfect Forward Secrecy (PFS) will be used and, if used, which Diffie-Hellman group is to be used.

NOTE *Regardless of the setting of this parameter, if the far-end VPN peer requests PFS, the Vyatta system will use PFS.*

Use the **set** form of this command to specify whether or not Perfect Forward Secrecy (PFS) will be used.

Use the **delete** form of this command to restore default PFS configuration.

Use the **show** form of this command to view PFS configuration.

vpn ipsec esp-group <name> proposal <num>

Defines an ESP group proposal for IKE Phase 2 negotation.

Syntax

set vpn ipsec esp-group *name* **proposal** *num*

delete vpn ipsec esp-group proposal

show vpn ipsec esp-group proposal

Command Mode

Configuration mode.

Configuration Statement

```
vpn {
    ipsec {
        esp-group name {
            proposal num {
            }
        }
    }
}
```

Parameters

name	The name to be used to refer to the ESP configuration.
num	Multi-node. An integer uniquely identifying a proposal to be used in IKE Phase 2 negotiation. You can define multiple proposals within a single ESP configuration by creating multiple **proposal** configuration nodes. Each must have a unique identifier.

Default

None.

Usage Guidelines

Use this command to define an ESP proposal for IKE Phase 2 negotiation.

Use the **set** form of this command to create an ESP proposal.

Use the **delete** form of this command to remove an ESP proposal and all its configuration.

Use the **show** form of this command to view ESP proposal configuration.

vpn ipsec esp-group <name> proposal <num> encryption <cipher>

Specifies the encryption cipher for an ESP proposal.

Syntax

set vpn ipsec esp-group *name* **proposal** *num* **encryption** *cipher*

delete vpn ipsec esp-group proposal *num* **encryption**

show vpn ipsec esp-group proposal *num* **encryption**

Command Mode

Configuration mode.

Configuration Statement

```
vpn {
    ipsec {
        esp-group name {
            proposal num {
                encryption cipher
            }
        }
    }
}
```

Parameters

name	The name to be used to refer to the ESP configuration.
proposal	An integer uniquely identifying a proposal to be used in IKE Phase 2 negotiation.
cipher	The encryption cipher to be proposed. Supported values are as follows: **aes128**: Advanced Encryption Standard with a 128-bit key. **aes256**: Advanced Encryption Standard with a 256-bit key. **3des**: Triple-DES (Data Encryption Standard).

Default

The default is **aes128**.

Usage Guidelines

Use this command to specify the encryption cipher to be proposed in an ESP proposal during IKE Phase 2 negotiation.

Use the **set** form of this command to specify the encryption cipher.

Use the **delete** form of this command to restore default encryption configuration.

Use the **show** form of this command to view ESP proposal encryption configuration.

vpn ipsec esp-group <name> proposal <num> hash <hash>

Specifies the hash algorithm for an ESP proposal.

Syntax

set vpn ipsec esp-group *name* **proposal** *num* **hash** *hash*

delete vpn ipsec esp-group proposal *num* **hash**

show vpn ipsec esp-group proposal *num* **hash**

Command Mode

Configuration mode.

Configuration Statement

```
vpn {
    ipsec {
        esp-group name {
            proposal num {
                hash hash
            }
        }
    }
}
```

Parameters

name	The name to be used to refer to the ESP configuration.
proposal	An integer uniquely identifying a proposal to be used in IKE Phase 2 negotiation.
hash	The hash algorithm to be used. Supported values are as follows: **sha1**: The SHA-1 variant of the Secure Hash Algorithm. **md5**: Version 5 of the message digest algorithm.

Default

The default is **sha1**.

Usage Guidelines

Use this command to specify the hash algorithm to be proposed in an ESP proposal.

Use the **set** form of this command to specify the hash algorithm to be proposed.

Use the **delete** form of this command to restore default hash algorithm configuration.

Use the **show** form of this command to view ESP proposal hash algorithm configuration.

vpn ipsec ike-group <name>

Defines a named IKE configuration for IKE Phase 1 negotiations.

Syntax

set vpn ipsec ike-group *name*

delete vpn ipsec ike-group

show vpn ipsec ike-group

Command Mode

Configuration mode.

Configuration Statement

```
vpn {
    ipsec {
        ike-group name {
        }
    }
}
```

Parameters

name	Mandatory. Multi-node. The name to be used to refer to this IKE configuration. You can create multiple IKE configurations by creating multiple **ike-group** configuration nodes.

Default

None.

Usage Guidelines

Use this command to configure a set of values for IKE configuration.

This configuration can be referred to as part of configuring a site-to-site configuration with a VPN peer, using vpn ipsec site-to-site peer <peer> command.

Use the **set** form of this command to create an IKE group.

Use the **delete** form of this command to remove an IKE group and all its configuration.

Use the **show** form of this command to view IKE group configuration.

vpn ipsec ike-group <name> dead-peer-detection

Defines the behavior if the VPN peer becomes unreachable.

Syntax

set vpn ipsec ike-group *name* **dead-peer-detection** [**action** *action* | **interval** *interval* | **timeout** *timeout*]

delete vpn ipsec ike-group *name* **dead-peer-detection**

show vpn ipsec ike-group *name* **dead-peer-detection**

Command Mode

Configuration mode.

Configuration Statement

```
vpn {
    ipsec {
        ike-group name {
            dead-peer-detection {
                action action
                interval interval
                timeout timeout
            }
        }
    }
}
```

Parameters

name	The name to be used to refer to this IKE configuration.
action	Specifies the action to be taken if the timeout interval expires. Supported values are as follows: **hold**: Queue packets until the tunnel comes back up. **clear**: Delete the connection information. **restart**: Attempt to restart the tunnel.
interval	The interval, in seconds, at which IKE keep-alive messages will be sent to VPN peers. The range is 15 to 86400. The default is 30.

timeout	The interval, in seconds, after which if the peer has not responded the defined action will be taken. The range is 30 to 86400. The default is 120.

Default

Dead peers are not detected.

Usage Guidelines

Use this command to specify how the system should detect dead IPsec VPN peers.

Use the **set** form of this command to configure dead peer detection.

Use the **delete** form of this command to remove dead peer detection configuration.

Use the **show** form of this command to view dead peer detection configuration.

vpn ipsec ike-group <name> lifetime <lifetime>

Specifies how long an IKE group key can stay in effect.

Syntax

set vpn ipsec ike-group *name* **lifetime** *lifetime*

delete vpn ipsec ike-group *name* **lifetime**

show vpn ipsec ike-group *name* **lifetime**

Command Mode

Configuration mode.

Configuration Statement

```
vpn {
    ipsec {
        ike-group name {
            lifetime lifetime
        }
    }
}
```

Parameters

name	The name to be used to refer to this IKE configuration.
lifetime	The time, in seconds, that any key created during IKE Phase 1 negotiation can persist before the next negotiation is triggered. The range is 30 to 86400 (that is, 24 hours). The default is 28800 (8 hours).

Default

An IKE key stays in effect for 8 hours.

Usage Guidelines

Use this command to specify the lifetime of an IKE key.

Use the **set** form of this command to specify key lifetime.

Use the **delete** form of this command to restore the default key lifetime.

Use the **show** form of this command to view key lifetime configuration.

vpn ipsec ike-group <name> proposal <num>

Specifies the IKE group proposal number.

Syntax

set vpn ipsec ike-group *name* **proposal** *num*

delete vpn ipsec ike-group proposal

show vpn ipsec ike-group proposal

Command Mode

Configuration mode.

Configuration Statement

```
vpn {
    ipsec {
        ike-group name {
            proposal num {
            }
        }
    }
}
```

Parameters

name	The name to be used to refer to the IKE configuration.
proposal	Multi-node. An integer uniquely identifying an IKE proposal . You can define up to 10 proposals within a single IKE configuration by creating multiple **proposal** configuration nodes. Each proposal must have a unique identifier.

Default

None.

Usage Guidelines

Use this command to create an IKE proposal. The proposal will be used in IKE Phase 1 negotiation.

Use the **set** form of this command to create an IKE proposal.

Use the **delete** form of this command to remove an IKE proposal and all its configuration.

Use the **show** form of this command to view IKE proposal configuration.

vpn ipsec ike-group <name> proposal <num> dh-group <group>

Specifies the Oakley group to be proposed for Diffie-Hellman key exchanges.

Syntax

set vpn ipsec ike-group *name* **proposal** *num* **dh-group** *group*

delete vpn ipsec ike-group proposal *num* **dh-group**

show vpn ipsec ike-group proposal *num* **dh-group**

Command Mode

Configuration mode.

Configuration Statement

```
vpn {
    ipsec {
        ike-group name {
            proposal num {
                dh-group group
            }
        }
    }
}
```

Parameters

name	The name to be used to refer to the IKE configuration.
proposal	An integer uniquely identifying an IKE proposal.
group	The Oakley group to be used in Diffie-Hellman key exchanges. Supported values are as follows: **2**: Oakley group 2. **5**: Oakley group 5.

Default

None.

Usage Guidelines

Use this command to specify the Oakley group to be proposed for Diffie-Hellman key exchanges.

Use the **set** form of this command to specify the Oakley group.

Use the **delete** form of this command to remove Oakley group configuration.

Use the **show** form of this command to view Oakley group configuration.

vpn ipsec ike-group <name> proposal <num> encryption <cipher>

Specifies the encryption cipher to be proposed in IKE Phase 1 negotiation.

Syntax

set vpn ipsec ike-group *name* **proposal** *num* **encryption** *cipher*

delete vpn ipsec ike-group proposal *num* **encryption**

show vpn ipsec ike-group proposal *num* **encryption**

Command Mode

Configuration mode.

Configuration Statement

```
vpn {
    ipsec {
        ike-group name {
            proposal num {
                encryption cipher
            }
        }
    }
}
```

Parameters

name	The name to be used to refer to the IKE configuration.
proposal	An integer uniquely identifying an IKE proposal.
cipher	The encryption cipher to be used in IKE Phase 1 negotiaton. Supported values are as follows: **aes128**: Advanced Encryption Standard with a 128-bit key. **aes256**: Advanced Encryption Standard with a 256-bit key. **3des**: Triple-DES (Data Encryption Standard).

Default

The default is **aes128**.

Usage Guidelines

Use this command to specify the encryption cipher to be proposed in IKE Phase 1 negotiation.

Use the **set** form of this command to set the encryption cipher.

Use the **delete** form of this command to restore the default encryption cipher.

Use the **show** form of this command to view encryption cipher configuration.

vpn ipsec ike-group <name> proposal <num> hash <hash>

Specifies the hash algorithm to be proposed.

Syntax

set vpn ipsec ike-group *name* **proposal** *num* **hash** *hash*

delete vpn ipsec ike-group proposal *num* **hash**

show vpn ipsec ike-group proposal *num* **hash**

Command Mode

Configuration mode.

Configuration Statement

```
vpn {
    ipsec {
        ike-group name {
            proposal num {
                hash hash
            }
        }
    }
}
```

Parameters

name	The name to be used to refer to the IKE configuration.
proposal	An integer uniquely identifying an IKE proposal.
hash	The hash algorithm to be used. Supported values are as follows: **sha1**: The SHA-1 variant of the Secure Hash Algorithm. **md5**: Version 5 of the message digest algorithm.

Default

The default is **sha1**.

Usage Guidelines

Use this command to specify the hash algorithm to be proposed in an IKE proposal.

Use the **set** form of this command to specify the hash algorithm to be proposed.

Use the **delete** form of this command to restore default hash algorithm configuration.

Use the **show** form of this command to view IKE proposal hash algorithm configuration.

vpn ipsec ipsec-interfaces interface <if-name>

Enables IPsec VPN on an interface.

Syntax

set vpn ipsec ipsec-interfaces interface *if-name*

delete vpn ipsec ipsec-interfaces interface *if-name*

show vpn ipsec ipsec-interfaces interface

Command Mode

Configuration mode.

Configuration Statement

```
vpn {
    ipsec {
        ipsec-interfaces {
            interface if-name
        }
    }
}
```

Parameters

if-name	Multi-node. The name of a network interface to be used for IPsec VPN. The network interface must already be created and configured. You can enable IPsec VPN on more than one interface by creating multiple **interface** configuration nodes.

Default

None.

Usage Guidelines

Use this command to configure IPsec on an interface.

Use the **set** form of this command to enable IPsec on an interface.

Use the **delete** form of this command to remove the IPsec interfaces configuration.

NOTE *If you delete an interface from IPsec configuration, IPsec connections referencing this tunnel will no longer operate. If you attempt to enable a connection referencing the IP address of a deleted interface, an error will result.*

Use the **show** form of this command to view IPsec interfaces configuration.

vpn ipsec logging

Specifies logging options for IPsec VPN.

Syntax

set vpn ipsec logging [log-modes *mode***]**

delete vpn ipsec logging [log-modes]

show vpn ipsec logging [log-modes]

Command Mode

Configuration mode.

Configuration Statement

```
vpn {
    ipsec {
        logging {
            log-modes mode
        }
    }
}
```

Parameters

log-modes *mode*	Mandatory. Multi-node. The log mode to be used for IPsec log messages. Supported values are as follows: **all**: Enables all logging options. **raw**: Shows the raw bytes of messages. **crypt**: Shows the encryption and decryption of messages. **parsing**: Shows the structure of input messages. **emitting**: Shows the structure of output messages. **control**: Shows the decision-making process of the IKE daemon (Pluto). **private**: Allows debugging output with private keys. You can configure multiple log modes, by creating more than one **log-mode** configuration node.

Default

None.

Usage Guidelines

Use this command to define logging options for IPsec VPN.

When this command is set, the system uses the Vyatta system's internal VPN logging daemon for IPsec log messages.

The IPsec process generates log messages during operation. You can direct the system to send IPsec log messages to syslog. The result will depend on how the system syslog is configured.

Keep in mind that in the current implementation, the main syslog file reports only messages of severity **warning** and above, regardless of the severity level configured. If you want to configure a different level of severity for log messages (for example, if you want to see debug messages during troubleshooting), you must configure syslog to send messages into a different file, which you define within syslog.

Configuring log modes is optional. When a log mode is not configured, IPsec log messages consist mostly of IPsec startup and shutdown messages. The log modes allow you to direct the system to inspect the IPsec packets and report the results.

Note that some log modes (for example, **all** and **control**) generate several log messages per packet. Using any of these options may severely degrade system performance.

VPN IPsec log messages use standard syslog levels of severity.

Use the **set** form of this command to specify logging modes for IPsec VPN.

Use the **delete** form of this command to remove the logging configuration.

Use the **show** form of this command to view the logging configuration.

vpn ipsec nat-networks allowed-network <ipv4net>

Specifies the private network addresses that remote hosts behind a NAT device may use.

Syntax

set vpn ipsec nat-networks allowed-network *ipv4net* [**exclude** *ipv4net-exclude*]

delete vpn ipsec nat-networks allowed-network *ipv4net* [**exclude** *ipv4net-exclude*]

show vpn ipsec nat-networks allowed-network [*ipv4net* [**exclude**]]

Command Mode

Configuration mode.

Configuration Statement

```
vpn {
    ipsec {
        nat-networks {
            allowed-network ipv4net {
                exclude ipv4net-exclude
            }
        }
    }
}
```

Parameters

ipv4net	Multi-node. An IPv4 network of private IP addresses that remote hosts behind a NAT device may use.
ipv4net-exclude	Multi-node. An IPv4 network to be excluded from the allowed network range. These are the RFC 1918 (“private”) IP addresses being used on the network internal to this VPN gateway.

Default

None.

Usage Guidelines

Use this command to specify RFC 1918 private IP addresses for remote networks that may reside behind a NAT device.

Unlike public IP addresses, private IP addresses may be re-used between sites. That means that private IP address ranges behind a NAT device at the far end of the VPN connection may overlap or be coextensive with private IP addresses on the internal network behind this VPN gateway, causing routing problems. For this reason, you must specify the allowed private network addresses that reside behind a NAT device, excluding internal network addresses.

Table 2-5 lists the three blocks of the IP address space that the Internet Assigned Numbers Authority (IANA) has reserved for private internets.

Table 2-5 IP addresses reserved for private networks

Network	Prefix
10.0.0.0–10.255.255.255	10.0.0.0/8
172.16.0.0–172.31.255.255	172.16.0.0/12
192.168.0.0–192.168.255.255	192.168.0.0/16

Use the **set** form of this command to specify the private network addresses that remote hosts behind a NAT device may use.

Use the **delete** form of this command to remove the configuration.

Use the **show** form of this command to view the configuration.

vpn ipsec nat-traversal <state>

Specifies whether the local VPN gateway proposes NAT Traversal capability.

Syntax

set vpn ipsec nat-traversal *state*

delete vpn ipsec nat-traversal

show vpn ipsec nat-traversal

Command Mode

Configuration mode.

Configuration Statement

```
vpn {
    ipsec {
        nat-traversal state
    }
}
```

Parameters

state	Enables or disables RFC 3947 NAT Traversal. Supported values are as follows: **enable**: Enables NAT Traversal. **disable**: Disables NAT Traversal.

Default

None.

Usage Guidelines

Use this command to direct the Vyatta system to propose RFC 3947 NAT Traversal support during IKE negotiation.

Regardless of the setting of this parameter, if the far-end VPN peer requests NAT Traversal, the Vyatta system will use NAT Traversal.

Use the **set** form of this command to specify whether the system proposes NAT Ttraversal capability.

Use the **delete** form of this command to remove the configuration.

Use the **show** form of this command to view the configuration.

vpn ipsec site-to-site peer <peer>

Defines a site-to-site connection between the Vyatta system and another VPN gateway.

Syntax

set vpn ipsec site-to-site peer *peer*

delete vpn ipsec site-to-site peer *peer*

show vpn ipsec site-to-site peer *peer*

Command Mode

Configuration mode.

Configuration Statement

```
vpn {
    ipsec {
        site-to-site {
            peer peer{
            }
        }
    }
}
```

Parameters

peer	Multi-node. The address of the far-end VPN gateway. The format is an IPv4 address, a hostname, an authentication ID, or **0.0.0.0**. You can define more than one VPN peer by creating multiple **peer** configuration nodes.

Default

None.

Usage Guidelines

Use this command to define a site-to-site connection with another VPN peer.

For peers that have a known IP address or hostname, specify the IPv4 address or hostname of the peer. For those that have a known authentication ID (prefixed with "@") specify the authentication ID of the peer. For peers where the IP address is unknown—for example, in the scenario where there are multiple "road warrior" peers—specify **0.0.0.0** as the peer, meaning there are multiple possible peers.

Use the **set** form of this command to define a site-to-site connection with another VPN peer.

Use the **delete** form of this command to remove the peer configuration.

Use the **show** form of this command to view the peer configuration.

vpn ipsec site-to-site peer <peer> authentication id <id>

Specifies local authentication credentials to send to the VPN peer.

Syntax

set vpn ipsec site-to-site peer *peer* **authentication id** *id*

delete vpn ipsec site-to-site peer *peer* **authentication id**

show vpn ipsec site-to-site peer *peer* **authentication id**

Command Mode

Configuration mode.

Configuration Statement

```
vpn {
    ipsec {
        site-to-site {
            peer peer {
                authentication {
                    id id
                }
            }
        }
    }
}
```

Parameters

peer	Mandatory. The address of the far-end VPN gateway. The format is an IPv4 address, a hostname, an authentication ID, or **0.0.0.0**.
id *id*	The local authentication credentials to send to the VPN peer. Can be specified if the **local-ip** address for the peer is set to **0.0.0.0** (which means the external address of the interface is dynamic); ignored otherwise. Use the format @*id* to specify the *id*.

Default

None.

Usage Guidelines

Use this command to specify the local authentication credentials to send to the VPN peer.

Use the **set** form of this command to specify the local authentication credentials to send to the VPN peer.

Use the **delete** form of this command to remove the local authentication credentials.

Use the **show** form of this command to view the local authentication credentials.

vpn ipsec site-to-site peer <peer> authentication mode <mode>

Specifies the authentication method to be used for the connection with the VPN peer.

Syntax

set vpn ipsec site-to-site peer *peer* **authentication mode** *mode*

delete vpn ipsec site-to-site peer *peer* **authentication mode**

show vpn ipsec site-to-site peer *peer* **authentication mode**

Command Mode

Configuration mode.

Configuration Statement

```
vpn {
    ipsec {
        site-to-site {
            peer peer {
                authentication {
                    mode mode
                }
            }
        }
    }
}
```

Parameters

peer	Mandatory. The address of the far-end VPN gateway. The format is an IPv4 address, a hostname, an authentication ID, or 0.0.0.0.

mode *mode*	Specifies the authentication method to be used for this connection. Supported values are as follows: **pre-shared-secret:** Uses a pre-shared secret for authentication. **rsa:** Uses an RSA digital signature for authentication. **x509:** Uses X.509 V.3 certificates for authentication.

Default

None.

Usage Guidelines

Use this command to specify the authentication method to be used for the connection to the VPN peer.

Use the **set** form of this command to specify the authentication method to be used for the connection to the VPN peer.

Use the **delete** form of this command to remove the authentication method configuration.

Use the **show** form of this command to view the authentication method configuration.

vpn ipsec site-to-site peer <peer> authentication pre-shared-secret <secret>

Specifies the pre-shared secret used to authenticate the VPN peer.

Syntax

set vpn ipsec site-to-site peer *peer* **authentication pre-shared-secret** *secret*

delete vpn ipsec site-to-site peer *peer* **authentication pre-shared-secret**

show vpn ipsec site-to-site peer *peer* **authentication pre-shared-secret**

Command Mode

Configuration mode.

Configuration Statement

```
vpn {
    ipsec {
        site-to-site {
            peer peer {
                authentication {
                    pre-shared-secret secret
                }
            }
        }
    }
}
```

Parameters

peer	Mandatory. The address of the far-end VPN gateway. The format is an IPv4 address, a hostname, an authentication ID, or **0.0.0.0**.
pre-shared-secret *secret*	Specifies the pre-shared secret to be used to authenticate the VPN peer.

Default

None.

Usage Guidelines

Use this command to specify the pre-shared secret used to authenticate the VPN peer. The **pre-shared-secret** set here is only valid if the **authentication mode** is set to **pre-shared-secret**.

Use the **set** form of this command to specify the pre-shared secret used to authenticate the VPN peer.

Use the **delete** form of this command to remove the pre-shared secret configuration.

Use the **show** form of this command to view the pre-shared secret configuration.

vpn ipsec site-to-site peer <peer> authentication remote-id <id>

Specifies the authentication credentials of the VPN peer.

Syntax

set vpn ipsec site-to-site peer *peer* **authentication remote-id** *id*

delete vpn ipsec site-to-site peer *peer* **authentication remote-id**

show vpn ipsec site-to-site peer *peer* **authentication remote-id**

Command Mode

Configuration mode.

Configuration Statement

```
vpn {
    ipsec {
        site-to-site {
            peer peer {
                authentication {
                    remote-id id
                }
            }
        }
    }
}
```

Parameters

peer	Mandatory. The address of the far-end VPN gateway. The format is an IPv4 address, a hostname, an authentication ID, or **0.0.0.0**.
remote-id *id*	The authentication credentials of the remote VPN peer. The id can be an IP address, a hostname, an authentication ID in the form @*id*, or, for X.509, a string specifying the “distinguished name” of the certificate for the remote end of the tunnel.

Default

None.

Usage Guidelines

Use this command to specify the authentication credentials of the VPN peer. The **remote-id** is an override to the default authentication - the peer IP address. The remote peer uses an authentication ID for authentication when it's IP address is dynamic or it identifies itself with a different IP address or hostname. An example of this is when the remote peer is behind a NAT device.

Another case where **remote-id** is required is for X.509 authentication. In this case, a string specifying the "distinguished name" of the certificate for the remote end of the tunnel is used. For example, the string "C=US, ST=CA, O=ABC Company, CN=test, E=root@abcco.com" specifies the information included in the X.509 certificate for the peer.

Use the **set** form of this command to specify the authentication credentials of the VPN peer.

Use the **delete** form of this command to remove the remote peer authentication credentials.

Use the **show** form of this command to view the remote peer authentication credentials.

vpn ipsec site-to-site peer <peer> authentication rsa-key-name <name>

Specifies the name of the digital signature used to authenticate the VPN peer.

Syntax

set vpn ipsec site-to-site peer *peer* **authentication rsa-key-name** *name*

delete vpn ipsec site-to-site peer *peer* **authentication rsa-key-name**

show vpn ipsec site-to-site peer *peer* **authentication rsa-key-name**

Command Mode

Configuration mode.

Configuration Statement

```
vpn {
    ipsec {
        site-to-site {
            peer peer {
                authentication {
                    rsa-key-name name
                }
            }
        }
    }
}
```

Parameters

peer	Mandatory. The address of the far-end VPN gateway. The format is an IPv4 address, a hostname, an authentication ID, or **0.0.0.0**.
rsa-key-name *name*	The name of the digital signature used to authenticate the VPN peer. To record an RSA digital signature for a VPN peer, use the **set** vpn rsa-keys command (see page 207).

Default

None.

Usage Guidelines

Use this command to specify the name of the digital signature to use to authenticate the VPN peer. The **rsa-key-name** set here is only valid if the **authentication mode** is set to **rsa.**

Use the **set** form of this command to specify the name of the digital signature to use to authenticate the VPN peer.

Use the **delete** form of this command to remove the name of the digital signature.

Use the **show** form of this command to view the name of the digital signature.

vpn ipsec site-to-site peer <peer> authentication x509 ca-cert-file <file-name>

Specifies the name of an X.509 Certificate Authority (CA) certificate file for IPsec authentication of the VPN peer.

Syntax

set vpn ipsec site-to-site peer *peer* **authentication x509 ca-cert-file** *file-name*

delete vpn ipsec site-to-site peer *peer* **authentication x509 ca-cert-file**

show vpn ipsec site-to-site peer *peer* **authentication x509 ca-cert-file**

Command Mode

Configuration mode.

Configuration Statement

```
vpn {
    ipsec {
        site-to-site {
            peer peer {
                authentication {
                    x509 {
                        ca-cert-file file-name
                    }
                }
            }
        }
    }
}
```

Parameters

file-name	The certificate file name. This parameter is mandatory if **authentication mode** is **x509**.

Default

None.

Usage Guidelines

Use this command to specify the name of an X.509 Certificate Authority (CA) certificate file. The X.509 CA certificate is used for IPsec authentication for the VPN peer.

Certificate and key files are assumed to be in /config/auth unless an absolute path is specified.

Use the **set** form of this command to specify the name of the CA certificate file.

Use the **delete** form of this command to remove the name of the CA certificate file.

Use the **show** form of this command to display CA certificate file configuration.

vpn ipsec site-to-site peer <peer> authentication x509 cert-file <file-name>

Specifies the name of the VPN server's certificate file for IPsec authentication of the VPN peer.

Syntax

set vpn ipsec site-to-site peer *peer* **authentication x509 cert-file** *file-name*

delete vpn ipsec site-to-site peer *peer* **authentication x509 cert-file**

show vpn ipsec site-to-site peer *peer* **authentication x509 cert-file**

Command Mode

Configuration mode.

Configuration Statement

```
vpn {
    ipsec {
        site-to-site {
            peer peer {
                authentication {
                    x509 {
                        cert-file file-name
                    }
                }
            }
        }
    }
}
```

Parameters

file-name	The name of the VPN server's certificate file. This parameter is mandatory if **authentication mode** is **x509**.

Default

None.

Usage Guidelines

Use this command to specify the name to the VPN server's certificate file. The VPN server's certificate certifies the identity of the VPN server.

Certificate and key files are assumed to be in /config/auth unless an absolute path is specified.

Use the **set** form of this command to specify the name of the VPN server's certificate file.

Use the **delete** form of this command to remove the name of the VPN server's certificate file.

Use the **show** form of this command to display VPN server certificate file configuration.

vpn ipsec site-to-site peer <peer> authentication x509 crl-file <file-name>

Specifies the name of an X.509 Certificate Revocation List (CRL) file for IPsec authentication of the VPN peer.

Syntax

set vpn ipsec site-to-site peer *peer* **authentication x509 crl-file** *file-name*

delete vpn ipsec site-to-site peer *peer* **authentication x509 crl-file**

show vpn ipsec site-to-site peer *peer* **authentication x509 crl-file**

Command Mode

Configuration mode.

Configuration Statement

```
vpn {
    ipsec {
        site-to-site {
            peer peer {
                authentication {
                    x509 {
                        crl-file file-name
                    }
                }
            }
        }
    }
}
```

Parameters

file-name	The name of the CRL file.

Default

None.

Usage Guidelines

Use this command to specify the name of a Certificate Revocation List (CRL) file.

A CRL is a time-stamped signed data structure issued by the Certificate Authority (CA) identifying revoked certificates. When the remote user attempts to log on to the system, the system checks both the remote user's certificate signature and also the CRL to make sure that the remote user's certificate serial number is not on the CRL. If it is, the login attempt will be refused.

The file is assumed to be in /config/auth unless an absolute path is specified.

Use the **set** form of this command to specify the name of the CRL file.

Use the **delete** form of this command to remove the name of the CRL file.

Use the **show** form of this command to display CRL file configuration.

vpn ipsec site-to-site peer <peer> authentication x509 key file <file-name>

Specifies the name of VPN server's private key file for IPsec authentication of the VPN peer.

Syntax

set vpn ipsec site-to-site peer *peer* **authentication x509 key file** *file-name*

delete vpn ipsec site-to-site peer *peer* **authentication x509 key file**

show vpn ipsec site-to-site peer *peer* **authentication x509 key file**

Command Mode

Configuration mode.

Configuration Statement

```
vpn {
    ipsec {
        site-to-site {
            peer peer {
                authentication {
                    x509 {
                        key {
                            file file-name
                        }
                    }
                }
            }
        }
    }
}
```

Parameters

file-name	The name of the VPN server's private key file. This parameter is mandatory if **authentication mode** is **x509**.

Default

None.

Usage Guidelines

Use this command to specify the name of the VPN server’s private key file. The VPN server’s private key certifies the identity of the VPN server.

The file is assumed to be in /config/auth unless an absolute path is specified.

Use the **set** form of this command to specify the location of the VPN server’s private key file.

Use the **delete** form of this command to remove the location of the VPN server’s private key file.

Use the **show** form of this command to display VPN server private key file configuration.

vpn ipsec site-to-site peer <peer> authentication x509 key password <password>

Specifies the password that protects the VPN server's private key.

Syntax

set vpn l2tp remote-access ipsec-settings authentication x509 key password *password*

delete vpn l2tp remote-access ipsec-settings authentication x509 key password

show vpn l2tp remote-access ipsec-settings authentication x509 key password

Command Mode

Configuration mode.

Configuration Statement

```
vpn {
    l2tp {
        remote-access {
            ipsec-settings {
                authentication {
                    x509 {
                        key {
                            password password
                        }
                    }
                }
            }
        }
    }
}
```

Parameters

password	The password protecting the VPN server's private key file.

Default

None.

Usage Guidelines

Use this command to specify a password that protects the VPN server's private key.

Use the **set** form of this command to specify the password for the VPN server's private key.

Use the **delete** form of this command to remove the password for the VPN server's private key.

Use the **show** form of this command to display VPN servers private key password configuration.

vpn ipsec site-to-site peer <peer> connection-type

Specifies the type of peer connection.

Syntax

set vpn ipsec site-to-site peer *peer* **connection-type {initiate | respond}**

delete vpn ipsec site-to-site peer *peer* **connection-type**

show vpn ipsec site-to-site peer *peer* **connection-type**

Command Mode

Configuration mode.

Configuration Statement

```
vpn {
    ipsec {
        site-to-site {
            peer peer{
                connection-type [initiate|respond]
            }
        }
    }
}
```

Parameters

peer	Mandatory. The address of the far-end VPN gateway. The format is an IPv4 address, a hostname, an authentication ID, or **0.0.0.0**.
initiate	Indicates that the connection to the remote peer will be initiated by the local peer unless the remote peer is set to **0.0.0.0**, **@id**, or **any**. This is the default behavior.
respond	Indicates that the local peer will not initiate a connection to the remote peer, but will respond to connections initiated by the remote peer.

Default

A connection to the remote peer is initiated by the local peer unless the remote peer is set to **0.0.0.0**, **@id**, or **any**.

Usage Guidelines

Use this command to specify the type of peer connection.

Use the **set** form of this command to specify the type of peer connection.

Use the **delete** form of this command to return the connection type to its default behavior.

Use the **show** form of this command to view connection type configuration.

vpn ipsec site-to-site peer <peer> default-esp-group <name>

Specifies a default ESP configuration to use for all tunnels to the peer.

Syntax

set vpn ipsec site-to-site peer *peer* **default-esp-group** *name*

delete vpn ipsec site-to-site peer *peer* **default-esp-group**

show vpn ipsec site-to-site peer *peer* **default-esp-group**

Command Mode

Configuration mode.

Configuration Statement

```
vpn {
    ipsec {
        site-to-site {
            peer peer{
                default-esp-group name
            }
        }
    }
}
```

Parameters

peer	Mandatory. The address of the far-end VPN gateway. The format is an IPv4 address, a hostname, an authentication ID, or **0.0.0.0**.
name	Specifies the named ESP configuration (ESP group) to be used by default for all connections. The ESP group must have already been defined, using the vpn ipsec esp-group <name> command.

Default

None.

Usage Guidelines

Use this command to specify a default ESP configuration to use for all tunnels to the peer. This setting can be overridden on a per-tunnel basis using the vpn ipsec site-to-site peer <peer> tunnel <tunnel> esp-group <name> command.

Use the **set** form of this command to specify an ESP configuration to use for all connections by default.

Use the **delete** form of this command to remove the configuration

Use the **show** form of this command to view the configuration.

vpn ipsec site-to-site peer <peer> dhcp-interface <interface>

Specifies a DHCP client interface to use for the connection.

Syntax

set vpn ipsec site-to-site peer *peer* **dhcp-interface** *interface*

delete vpn ipsec site-to-site peer *peer* **dhcp-interface**

show vpn ipsec site-to-site peer *peer* **dhcp-interface**

Command Mode

Configuration mode.

Configuration Statement

```
vpn {
    ipsec {
        site-to-site {
            peer peer{
                dhcp-interface interface
            }
        }
    }
}
```

Parameters

peer	Mandatory. The address of the far-end VPN gateway. The format is an IPv4 address, a hostname, an authentication ID, or **0.0.0.0**.
interface	The interface to use for the VPN connection (e.g. eth0). Please note that the interface must already have IPsec VPN enabled, using the vpn ipsec ipsec-interfaces interface <if-name> command, and must be configured as a DHCP client.

Default

None.

Usage Guidelines

Use this command to specify a DHCP client interface to use for the connection. The connection will be automatically restarted if the IP address changes.

NOTE *This option cannot be used if vpn ipsec site-to-site peer <peer> local-ip <ipv4> is also set.*

Use the **set** form of this command to specify a DHCP interface to use for the connection.

Use the **delete** form of this command to remove the configuration

Use the **show** form of this command to view the configuration.

vpn ipsec site-to-site peer <peer> ike-group <group>

Specifies the named IKE configuration to be used for a peer connection.

Syntax

set vpn ipsec site-to-site peer *peer* **ike-group** *group*

delete vpn ipsec site-to-site peer *peer* **ike-group**

show vpn ipsec site-to-site peer *peer* **ike-group**

Command Mode

Configuration mode.

Configuration Statement

```
vpn {
    ipsec {
        site-to-site {
            peer peer{
                ike-group group
            }
        }
    }
}
```

Parameters

peer	Mandatory. The address of the far-end VPN gateway. The format is an IPv4 address, a hostname, an authentication ID, or **0.0.0.0**.
group	Mandatory. The named IKE configuration to be used for this connection. The IKE configuration must have already been defined, using the vpn ipsec ike-group <name> command.

Default

None.

Usage Guidelines

Use this command to specify a named IKE configuration (an IKE group) to be used for an IPsec peer connection.

Use the **set** form of this command to specify the IKE group.

Use the **delete** form of this command to remove IKE group configuration.

Use the **show** form of this command to view IKE group configuration.

vpn ipsec site-to-site peer <peer> local-ip <ipv4>

Specifies the local IP address to be used as the source IP for packets destined for the remote peer.

Syntax

set vpn ipsec site-to-site peer *peer* **local-ip** *ipv4*

delete vpn ipsec site-to-site peer *peer* **local-ip**

show vpn ipsec site-to-site peer *peer* **local-ip**

Command Mode

Configuration mode.

Configuration Statement

```
vpn {
    ipsec {
        site-to-site {
            peer peer {
                local-ip ipv4
            }
        }
    }
}
```

Parameters

peer	Mandatory. The address of the far-end VPN gateway. The format is an IPv4 address, a hostname, an authentication ID, or 0.0.0.0.

ipv4	Mandatory. The local IP address to be used as the source IP for packets destined for the remote peer. Please note that the interface associated with this address must already have IPsec VPN enabled, using the vpn ipsec ipsec-interfaces interface <if-name> command. Note also the following: If the VPN tunnel is being clustered for high availability, the **local-ip** attribute must be the cluster IP address, not the IP address configured for the physical interface. Otherwise, the **local-ip** must be the address configured for the physical interface. If the physical interface has a dynamic IP address then the **local-ip** must be set to **0.0.0.0** and the authentication ID, though not required, can be set using the vpn ipsec site-to-site peer <peer> authentication rsa-key-name <name> command.

Default

None.

Usage Guidelines

Use this command to specify the local IP address to be used as the source IP for packets destined for the remote peer.

Use special address **0.0.0.0** in cases the local external IP address is dynamic or unknown; for example, because the address is supplied by a PPPoE connection or DHCP server. If you use an address of **0.0.0.0**, you must set the local authentication ID using the vpn ipsec site-to-site peer <peer> authentication rsa-key-name <name> command.

When the **local-ip** is set to **0.0.0.0** the default route is used and the connection will not be automatically updated if the IP address changes (a restart vpn is required when the IP address changes). A better alternative for use with DHCP client interfaces is the vpn ipsec site-to-site peer <peer> dhcp-interface <interface> command.

NOTE *The **local-ip** option cannot be used if vpn ipsec site-to-site peer <peer> dhcp-interface <interface> is also set.*

Use the **set** form of this command to specify the local IP address to be used as the source IP for packets destined for the remote peer.

Use the **delete** form of this command to remove local IP address configuration.

Use the **show** form of this command to view local IP address configuration.

vpn ipsec site-to-site peer <peer> tunnel <tunnel> allow-nat-networks <state>

Specifies whether or not a connection to a private network is allowed.

Syntax

set vpn ipsec site-to-site peer *peer* **tunnel** *tunnel* **allow-nat-networks** *state*

delete vpn ipsec site-to-site peer *peer* **tunnel** *tunnel* **allow-nat-networks**

show vpn ipsec site-to-site peer *peer* **tunnel** *tunnel* **allow-nat-networks**

Command Mode

Configuration mode.

Configuration Statement

```
vpn {
    ipsec {
        site-to-site {
            peer peer {
                tunnel tunnel {
                    allow-nat-networks state
                }
            }
        }
    }
}
```

Parameters

peer	Mandatory. The address of the far-end VPN gateway. The format is an IPv4 address, a hostname, an authentication ID, or **0.0.0.0**.

tunnel	Mandatory. Multi-node. An integer that uniquely identifies this tunnel configuration for this peer VPN gateway. Each tunnel corresponds to a distinct connection configuration. The range is 1 to 65535. A given VPN peer may have more than one tunnel configuration, but each peer must have at least one. To define more than one tunnel configuration for a peer, create multiple **tunnel** configuration nodes within the peer configuration.
state	Allows connection to a defined network of private IP addresses on a per-tunnel basis. Supported values are as follows: **enable**: Allow connection to the private network. **disable**: Do not allow connection to the private network. This option is mandatory if the **allow-public-networks** is enabled; optional otherwise. The allowed private network must be defined using the vpn ipsec nat-networks allowed-network <ipv4net> command. If this option is enabled, any value set for the **remote subnet** option is ignored.

Default

A connection to a private network is not allowed (disabled).

Usage Guidelines

Use this command to specify whether or not a connection to a private network is allowed.

Use the **set** form of this command to specify whether or not a connection to a private network is allowed.

Use the **delete** form of this command to remove the configuration and return it to the default behavior.

Use the **show** form of this command to view the configuration.

vpn ipsec site-to-site peer <peer> tunnel <tunnel> allow-public-networks <state>

Specifies whether or not a connection to a public network is allowed.

Syntax

set vpn ipsec site-to-site peer *peer* **tunnel** *tunnel* **allow-public-networks** *state*

delete vpn ipsec site-to-site peer *peer* **tunnel** *tunnel* **allow-public-networks**

show vpn ipsec site-to-site peer *peer* **tunnel** *tunnel* **allow-public-networks**

Command Mode

Configuration mode.

Configuration Statement

```
vpn {
    ipsec {
        site-to-site {
            peer peer {
                tunnel tunnel {
                    allow-public-networks state
                }
            }
        }
    }
}
```

Parameters

peer	Mandatory. The address of the far-end VPN gateway. The format is an IPv4 address, a hostname, an authentication ID, or **0.0.0.0**.

tunnel	Mandatory. Multi-node. An integer that uniquely identifies this tunnel configuration for this peer VPN gateway. Each tunnel corresponds to a distinct connection configuration. The range is 1 to 65535. A given VPN peer may have more than one tunnel configuration, but each peer must have at least one. To define more than one tunnel configuration for a peer, create multiple **tunnel** configuration nodes within the peer configuration.
state	Allows connections to public IP addresses on a per-tunnel basis. Supported values are as follows **enable**: Allow connections to public networks. **disable**: Do not allow connections to public networks. This option requires that the **allow-nat-networks** option be enabled, and that allowed NAT networks be specified using vpn ipsec nat-networks allowed-network <ipv4net> command.

Default

A connection to a public network is not allowed (disabled).

Usage Guidelines

Use this command to specify whether or not a connection to a public network is allowed.

Use the **set** form of this command to specify whether or not a connection to a public network is allowed.

Use the **delete** form of this command to remove the configuration and return it to the default behavior.

Use the **show** form of this command to view the configuration.

vpn ipsec site-to-site peer <peer> tunnel <tunnel> esp-group <name>

Specifies an ESP configuration to use for this tunnel.

Syntax

set vpn ipsec site-to-site peer *peer* **tunnel** *tunnel* **esp-group** *name*

delete vpn ipsec site-to-site peer *peer* **tunnel** *tunnel* **esp-group**

show vpn ipsec site-to-site peer *peer* **tunnel** *tunnel* **esp-group**

Command Mode

Configuration mode.

Configuration Statement

```
vpn {
    ipsec {
        site-to-site {
            peer peer {
                tunnel tunnel {
                    esp-group name
                }
            }
        }
    }
}
```

Parameters

peer	Mandatory. The address of the far-end VPN gateway. The format is an IPv4 address, a hostname, an authentication ID, or **0.0.0.0**.

tunnel	Mandatory. Multi-node. An integer that uniquely identifies this tunnel configuration for this peer VPN gateway. Each tunnel corresponds to a distinct connection configuration. The range is 1 to 65535. A given VPN peer may have more than one tunnel configuration, but each peer must have at least one. To define more than one tunnel configuration for a peer, create multiple **tunnel** configuration nodes within the peer configuration.
name	Specifies the named ESP configuration (ESP group) to be used for this connection. The ESP group must have already been defined, using the vpn ipsec esp-group <name> command.

Default

The ESP group specified by vpn ipsec site-to-site peer <peer> default-esp-group <name> will be used.

Usage Guidelines

Use this command to specify an ESP configuration to use for this connection. It will override the ESP group specified by vpn ipsec site-to-site peer <peer> default-esp-group <name> which will be used by default.

Use the **set** form of this command to specify an ESP configuration to use for this connection.

Use the **delete** form of this command to remove the configuration.

Use the **show** form of this command to view the configuration.

vpn ipsec site-to-site peer <peer> tunnel <tunnel> local

Defines local configuration options for the IPsec tunnel.

Syntax

set vpn ipsec site-to-site peer *peer* **tunnel** *tunnel* **local** [**port** *port* | **subnet** *ipv4net*]

delete vpn ipsec site-to-site peer *peer* **tunnel** *tunnel* **local** [**port** | **subnet**]

show vpn ipsec site-to-site peer *peer* **tunnel** *tunnel* **local** [**port** | **subnet**]

Command Mode

Configuration mode.

Configuration Statement

```
vpn {
    ipsec {
        site-to-site {
            peer peer {
                tunnel tunnel {
                    local {
                        port port
                        subnet ipv4net
                    }
                }
            }
        }
    }
}
```

Parameters

peer	Mandatory. The address of the far-end VPN gateway. The format is an IPv4 address, a hostname, an authentication ID, or **0.0.0.0**.

tunnel	Mandatory. Multi-node. An integer that uniquely identifies this tunnel configuration for this peer VPN gateway. Each tunnel corresponds to a distinct connection configuration. The range is 1 to 65535. A given VPN peer may have more than one tunnel configuration, but each peer must have at least one. To define more than one tunnel configuration for a peer, create multiple **tunnel** configuration nodes within the peer configuration.
port	Applicable only when the protocol is TCP or UDP. The local port to match. Only traffic from or to this port on the local subnet will travel through this tunnel. Supported formats are as follows: *port-name*: Matches the name of an IP service; for example, **http**. You can specify any service name in the file **/etc/services**. *port-num*: Matches a port number. The range is 1 to 65535. The default is **all**.
ipv4net	Mandatory. The local subnet to which the remote VPN gateway will have access. The format is an IPv4 network address, where network address **0.0.0.0/0** means any local subnet. The default is the subnet the **local-ip** is on.

Default

None.

Usage Guidelines

Use this command to define local configuration options for the IPsec tunnel.

Use the **set** form of this command to set the local tunnel characteristics.

Use the **delete** form of this command to remove local tunnel configuration.

Use the **show** form of this command to view local tunnel configuration.

vpn ipsec site-to-site peer <peer> tunnel <tunnel> protocol <protocol>

Specifies the protocol to match for traffic to enter the tunnel.

Syntax

set vpn ipsec site-to-site peer *peer* **tunnel** *tunnel* **protocol** *protocol*

delete vpn ipsec site-to-site peer *peer* **tunnel** *tunnel* **protocol**

show vpn ipsec site-to-site peer *peer* **tunnel** *tunnel* **protocol**

Command Mode

Configuration mode.

Configuration Statement

```
vpn {
    ipsec {
        site-to-site {
            peer peer {
                tunnel tunnel {
                    protocol protocol
                }
            }
        }
    }
}
```

Parameters

peer	Mandatory. The address of the far-end VPN gateway. The format is an IPv4 address, a hostname, an authentication ID, or **0.0.0.0**.

tunnel	Mandatory. Multi-node. An integer that uniquely identifies this tunnel configuration for this peer VPN gateway. Each tunnel corresponds to a distinct connection configuration. The range is 1 to 65535. A given VPN peer may have more than one tunnel configuration, but each peer must have at least one. To define more than one tunnel configuration for a peer, create multiple **tunnel** configuration nodes within the peer configuration.
protocol	Any protocol literals or numbers listed in the file **/etc/protocols** can be used. The keywords **tcp_udp** (for both TCP and UDP) and **all** (for all protocols) are also supported.

Default

The default is **all**.

Usage Guidelines

Use this command to specify the protocol to match for traffic to enter the tunnel.

Use the **set** form of this command to specify the protocol

Use the **delete** form of this command to remove protocol configuration.

Use the **show** form of this command to view protocol configuration.

vpn ipsec site-to-site peer <peer> tunnel <tunnel> remote

Defines remote configuration options for the IPsec tunnel.

Syntax

set vpn ipsec site-to-site peer *peer* **tunnel** *tunnel* **remote** [**port** *port* | **subnet** *ipv4net*]

delete vpn ipsec site-to-site peer *peer* **tunnel** *tunnel* **remote** [**port** | **subnet**]

show vpn ipsec site-to-site peer *peer* **tunnel** *tunnel* **remote** [**port** | **subnet**]

Command Mode

Configuration mode.

Configuration Statement

```
vpn {
    ipsec {
        site-to-site {
            peer peer {
                tunnel tunnel {
                    remote {
                        port port
                        subnet ipv4net
                    }
                }
            }
        }
    }
}
```

Parameters

peer	Mandatory. The address of the far-end VPN gateway. The format is an IPv4 address, a hostname, an authentication ID, or **0.0.0.0**.

tunnel	Mandatory. Multi-node. An integer that uniquely identifies this tunnel configuration for this peer VPN gateway. Each tunnel corresponds to a distinct connection configuration. The range is 1 to 65535. A given VPN peer may have more than one tunnel configuration, but each peer must have at least one. To define more than one tunnel configuration for a peer, create multiple **tunnel** configuration nodes within the peer configuration.
port	Applicable only when the protocol is TCP or UDP. The remote port to match. Only traffic from or to this port on the remote subnet will travel through this tunnel. Supported formats are as follows: *port-name*: Matches the name of an IP service; for example, **http**. You can specify any service name in the file **/etc/services**. *port-num*: Matches a port number. The range is 1 to 65535. The default is **all**.
ipv4net	Mandatory. The remote subnet behind the remote VPN gateway, to which the Vyatta system will have access. The format is an IPv4 network address, where network address **0.0.0.0/0** means any subnet behind the remote VPN gateway. This option is ignored if **allowed-nat-networks** is enabled. The default is the subnet of the peer.

Default

None.

Usage Guidelines

Use this command to define local configuration options for the IPsec tunnel.

Use the **set** form of this command to set the local tunnel characteristics.

Use the **delete** form of this command to remove local tunnel configuration.

Use the **show** form of this command to view local tunnel configuration.

vpn rsa-keys

Records RSA keys for the local host.

Syntax

set vpn rsa-keys [**local-key file** *file-name* | **rsa-key-name** *name* **rsa-key** *key*]

delete vpn rsa-keys local-key file [**local-key file** | **rsa-key-name** [*name* **rsa-key**]]

show vpn rsa-keys local-key file [**local-key file** | **rsa-key-name** [*name* **rsa-key**]]

Command Mode

Configuration mode.

Configuration Statement

```
vpn {
    rsa-keys {
        local-key {
            file file-name
        rsa-key-name name {
            rsa-key key
        }
    }
}
```

Parameters

local-key file *file-name*	Specifies the name and location of the file containing the RSA digital signature of the local host (both public key and private key). By default, the RSA digital signature for the local host is recorded in **/config/ipsec.d/rsa-keys/**.
rsa-key-name *name*	A mnemonic name for the remote key. This is the name you refer to when configuring RSA configuration in site-to-site connections.
rsa-key *key*	The RSA public key data for the remote peer.

Default

None.

Usage Guidelines

Use this command to view or change the location of the file containing RSA key information for the local host, or to record an RSA public key for a remote host.

The RSA digital signature for the local host can be generated using the generate vpn rsa-key command in operational mode. Once generated, the key is stored at the location specified by the **local-key rsa-key-name** option. By default, this is the **localhost.key** file in the **/config/ipsec.d/rsa-keys/** directory.

The main use of the **local-key** option is to save your RSA key to the floppy drive, so that you can load it on reboot if you are running the Vyatta system using LiveCD.

NOTE *If you save a configuration to floppy after changing the name and location of the localhost.keys file, then booting the system from LiveCD may generate a parse error because it will not be able to find the file.*

You must also enter the public key of the remote peer, as the **rsa-key-name** *name* **rsa-key** attribute. Digital signatures are lengthy, so to configure this value copy it as text into your clipboard and paste it into the configuration. Once recorded with a mnemonic name, you can refer to the RSA key by the name in site-to-site connection configurations.

Use the **set** form of this command to set RSA key configuration.

Use the **delete** form of this command to remove RSA key configuration.

Use the **show** form of this command to view RSA key configuration.

Chapter 3: Remote Access VPN

This chapter explains how to set up VPN access for remote users of the Vyatta System.

This chapter presents the following topics:

Remote Access VPN Configuration

This section describes how to configure remote Virtual Private Network (VPN) access on the Vyatta System.

This section presents the following topics:

- Remote Access VPN Overview
- Remote Access VPN Configuration Examples

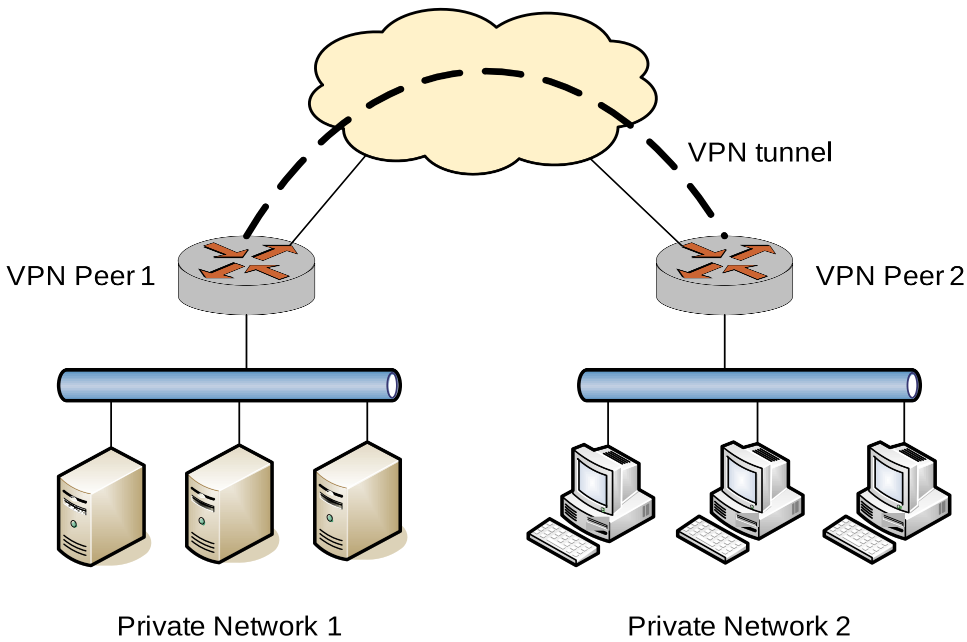
Remote Access VPN Overview

This section presents the following topics:

- Remote VPN Access using PPTP
- Remote VPN Access Using L2TP/IPsec with Pre-Shared Key
- Remote VPN Access Using L2TP/IPsec with X.509 Certificates
- Planning Considerations
- Connecting Remotely Using Site-to-Site IPSec
- Remote Access using OpenVPN
- Configuring with Zone-Based Firewall

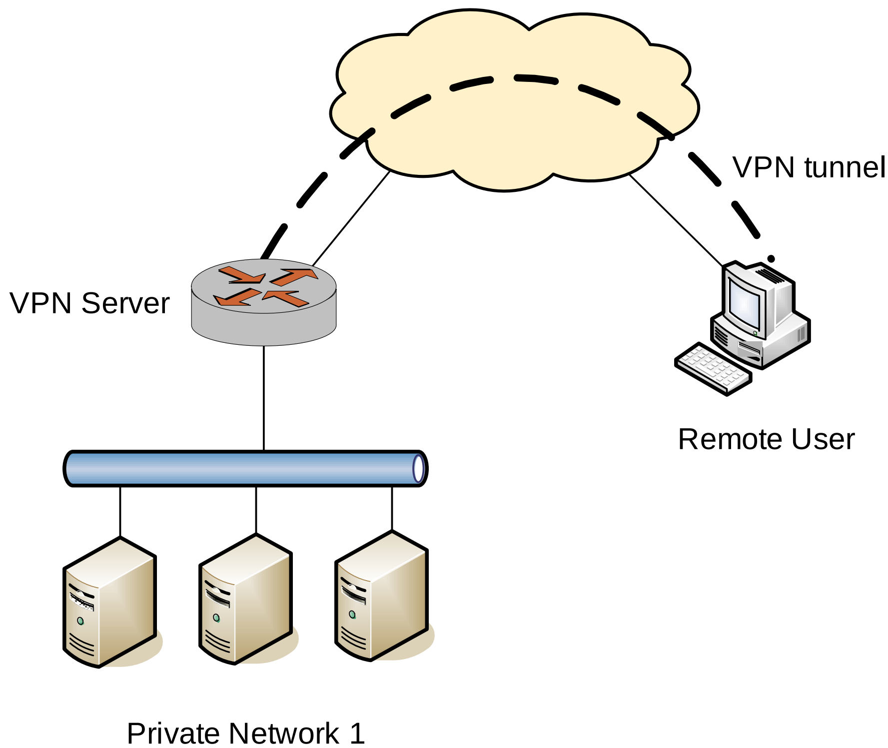
The Vyatta system currently supports two main VPN mechanisms: site-to-site IPsec VPN, and Remote Access VPN (RA VPN). A site-to-site IPsec VPN connection allows two or more remote private networks to be “merged” into a single network as shown in Figure 3-1.

Figure 3-1 Site-to-site IPsec VPN



With RA VPN, the Vyatta system acts as a VPN server to a remote user with a client PC. A typical use for this capability is a travelling employee accessing the corporate network over the Internet. In this scenario, the remote employee's computer appears as another host on the corporate private subnet and is able to access all resources within that subnet. This scenario is shown in Figure 3-2.

Figure 3-2 Remote Access VPN



The Vyatta RA VPN implementation supports the built-in Windows VPN clients: Point-to-Point Tunnelling Protocol (PPTP) VPN and Layer 2 Tunneling Protocol (L2TP)/IPsec VPN.

The Windows L2TP/IPsec client supports two IPsec authentication mechanisms:

- Pre-shared key (PSK), where the two IPsec peers can use a PSK to authenticate each other based on the assumption that only the other peer knows the key.
- X.509 certificates, which are based on public key cryptography—specifically, digital signatures.

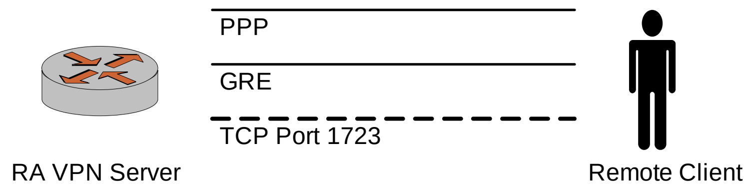
The Vyatta system supports both pre-shared key and X.509 certificate authentication for L2TP/IPsec client; consequently, the Vyatta system supports three different RA VPN deployments:

- PPTP
- L2TP/IPsec authenticated with pre-shared key
- L2TP/IPsec authenticated with X.509 certificates

Remote VPN Access using PPTP

In this scenario, the remote user establishes a PPTP VPN session with the VPN server as shown in Figure 3-3.

Figure 3-3 Remote Access VPN—PPTP



1 The remote client establishes a TCP connection to server port 1723.

2 Through the TCP connection, the PPTP client and server establish a Generic Routing Encapsulation (GRE) tunnel.

3 A Point-to-Point Protocol (PPP) session is then established on top of the GRE tunnel; that is, the PPP packets are encapsulated and sent/received inside the GRE tunnel.

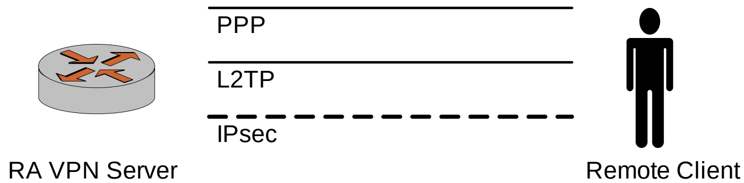
In this deployment, both user authentication and data encryption are done at the PPP level, using a user name/password combination with MS CHAPv2 for authentication and MPPE for encryption.

Note that the security of this solution is significantly affected by the "strength" of a user's passwords, since the password is used to derive the encryption authentication keys. As a result, studies have shown that PPTP deployments are relatively weak compared to other solutions.

Remote VPN Access Using L2TP/IPsec with Pre-Shared Key

Figure 3-4 shows establishment of an L2TP/IPsec VPN session.

Figure 3-4 Remote Access VPN—L2TP/IPsec with pre-shared key



1. The remote client 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, i.e., the PPP packets are encapsulated and sent/received inside the L2TP tunnel.

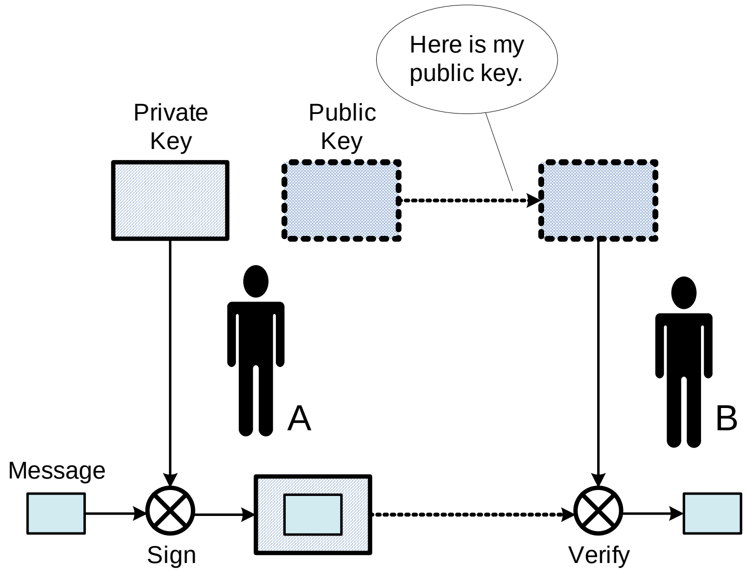
With this solution, only user authentication is done at the PPP level (with username/password). Data encryption is provided by the IPsec tunnel. Furthermore, in order to perform encryption, IPsec also requires authentication (studies have shown that IPsec encryption-only mode is not secure) at the host level.

When pre-shared key is used with L2TP/IPsec, all remote clients must be configured with the same PSK for IPsec authentication. This presents both a security challenge and an operations challenge, since when the key is changed, all remote clients must be re-configured. An alternative is to use L2TP/IPsec with X.509 certificates, as discussed in the next section.

Remote VPN Access Using L2TP/IPsec with X.509 Certificates

Figure 3-5 shows a conceptual diagram of how digital signatures work.

Figure 3-5 Digital signature



1 Peers A and B are communicating. A has a public key and a private key. A gives her public key to B.

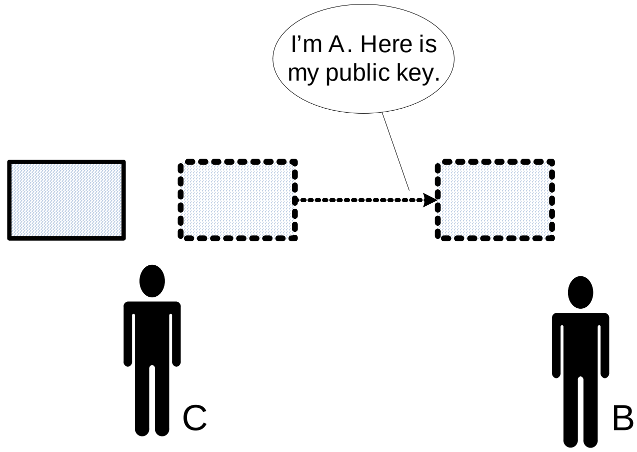
2 A “signs” (encrypts) a message using her private key and sends the signed (encrypted) message to B.

3 B can “verify” the signature by decrypting it using A's public key and checking the result against the original message.

Therefore, B can authenticate A by asking A to sign a message and then verifying the signature using A’s public key. Since A’s private key is only known to A, only A can create a signature that can be verified using A’s public key.

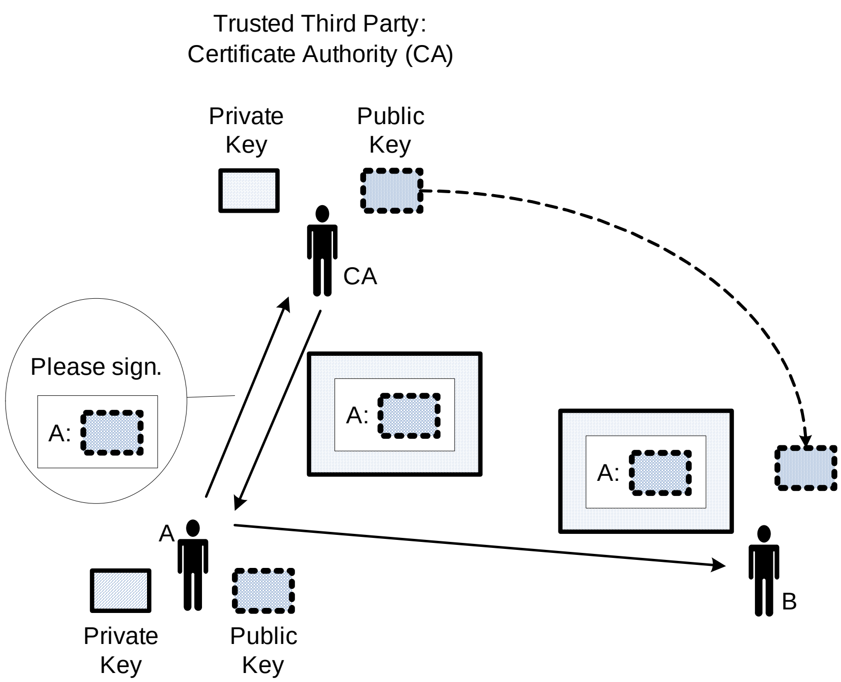
One problem with this authentication scheme is that B cannot know whether the public key he obtained is in fact A’s public key. For example, in Figure 3-6, a malicious attacker C pretends to be A and gives B a different public key.

Figure 3-6 Malicious attacker



In practice, this problem is solved by using a Public Key Infrastructure (PKI), which is based on a trusted third party, the Certificate Authority (CA). The CA can be either a commercial CA, such as Verisign, or a CA set up internal to the organization. Figure 3-7 illustrates conceptually how PKI works.

Figure 3-7 Trusted Third Party: Certificate Authority



1 Both A and B trust CA.
2 A asks the CA to sign a message verifying A's public key.
3 The CA signs the message using its private key, resulting in a "certificate."
4 A gives the certificate to B.
5 B can verify the certificate from A (and hence A's public key) using the CA's public key.

X.509 is a standard that defines public key certificate formats, revocation, and so on. Given the above scheme, L2TP/IPsec VPN with X.509 certificates works as follows.

1 The network admin obtains a certificate signed by a CA for each remote user (A in the example) and distributes it, along with public/private keys for the user, to the user through a secure channel.
2 The network admin configures the VPN server (B in the example) with the CA's public key, among other things.
3 When the remote client connects to the VPN server, it presents its certificate.
4 The VPN server verifies the certificate using the CA's public key. If the authentication is successful, the result tells the server the client's public key.
5 The server can then use the client's public key for authentication as described previously.
6 If authentication is successful, the IPsec tunnel is established between the client and server. Then the L2TP and PPP operations are identical to the PSK case described previously.

Planning Considerations

The following points should be taken into consideration when planning a Remote Access VPN configuration:

- **Dedicated subnet** - At least one dedicated subnet should be used for remote access VPN users. This subnet should not overlap with existing subnets on the private network.
- **Address pools must not overlap** - As it is possible to define multiple address pools, care must be take not to overlap the address ranges in these pools.
- **Routes to VPN clients are required** - In addition to configuring the remote access VPN server and clients, routers on the corporate network must be made aware of the VPN client subnet so that they know to forward traffic destined for clients through the VPN server. This can be done using static routes and route redistribution in local routing protocols.

- **Concurrent use of site-to-site and remote access VPN** - Do not configure both site-to-site and remote access VPN servers on the same Vyatta device if both connect to clients with dynamic IP addresses. This is a problem because it is unclear whether the incoming connection requests are from a site-to-site client or a remote access client.
- **Full Tunneling vs. Split Tunneling** - Full Tunneling means that all traffic from the remote access VPN client (that is, traffic destined for the corporate network and traffic destined for the Internet) flows across the VPN. Split Tunneling means that only traffic destined for the corporate network flows across the VPN. Internet traffic goes directly from the client to the Internet. The advantage of Full Tunneling is that Internet access can be controlled centrally. The disadvantage is that it consumes more corporate bandwidth and VPN server resources to service the additional traffic. The advantage of Split Tunneling is that it it makes better use of network resources. The disadvantage is that Internet access control must be provided and maintained on the client. In addition, the routing configuration on the client becomes complicated and must be performed manually each time the client connects if the default classful route added by the client software (that is, a route to 10.0.0.0/8, 172.16.0.0/12, or 192.168.0.0/16) is insufficient (for example, if you need to reach both 10.1.0.0/24 and 172.16.1.0/24). If this is the case, and Split Tunneling is desired, OpenVPN is a better solution as it provides better Split Tunnel support. For more information on OpenVPN, please see *Chapter 4: OpenVPN*.

  Full Tunneling is the default with Windows (PPTP and L2TP) clients. Split Tunneling is the default with OpenVPN clients.

Connecting Remotely Using Site-to-Site IPSec

The Vyatta system supports IPSec remote access using multiple site-to-site connections from dynamic IP addresses—so-called “road warrior” configuration. For this information, please see the section “Bridging” on page 87.

Remote Access using OpenVPN

The Vyatta system also supports remote access using OpenVPN. For more information on OpenVPN see *Chapter 4: OpenVPN*.

Configuring with Zone-Based Firewall

To configure the firewall to treat all Remote Access VPN users as a separate firewall zone see the “Zone-Based Firewall Configuration” section in the *Vyatta Firewall Reference Guide*.

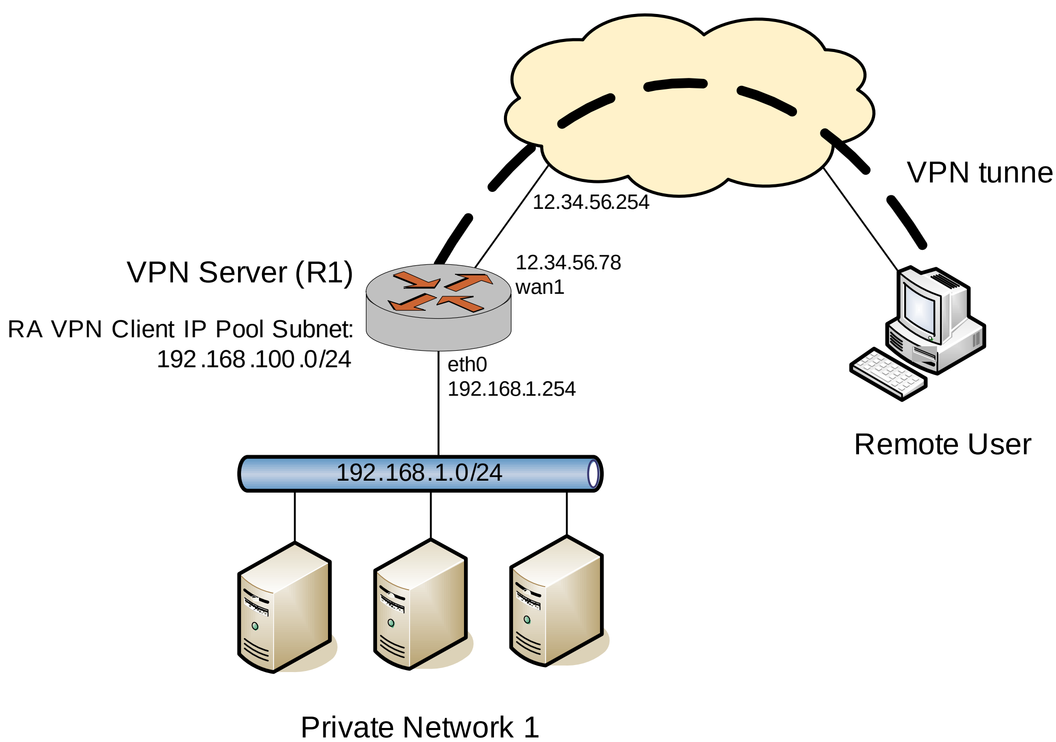
Remote Access VPN Configuration Examples

This section presents the following topics:

- PPTP VPN Example
- L2TP/IPsec with Pre-Shared Key VPN Example
- L2TP/IPsec with X.509 Certificates VPN Example
- PPTP VPN Example with a Dynamic IP Address and using Dynamic DNS
- Configuring Split Tunneling on a Windows Client

This section provides configuration examples for three of the RA VPN scenarios supported: PPTP, L2TP/IPsec with pre-shared key, and L2TP/IPsec with X.509 certificates. Each configuration example uses the diagram shown in Figure 3-8 as the deployment scenario:

Figure 3-8 Remote Access VPN Example



PPTP VPN Example

The first step in configuring a basic remote access VPN setup using PPTP between R1 and a Windows XP client is to configure R1 as a PPTP–based VPN server.

Example 3-1 Remote Access VPN - PPTP example)

Step	Command
Bind the PPTP server to the external address.	vyatta@R1# **set vpn pptp remote-access outside-address 12.34.56.78**
Set up the pool of IP addresses that remote VPN connections will assume. In this case we make 10 addresses available (from .101 to .110) on subnet 192.168.100.0/24. Note that we do not use the subnet on the LAN.	vyatta@R1# **set vpn pptp remote-access client-ip-pool start 192.168.100.101** vyatta@R1# **set vpn pptp remote-access client-ip-pool stop 192.168.100.110**
Set up the authentication mode - in this case "local".	vyatta@R1# **set vpn pptp remote-access authentication mode local**
Set up a user (testuser) and password (testpassword).	vyatta@R1# **set vpn pptp remote-access authentication local-users username testuser password testpassword**
Commit the change.	vyatta@R1# **commit**

Show the configuration.	vyatta@R1# **show vpn pptp remote-access**
	authentication {
	local-users {
	username testuser{
	password testpassword
	}
	}
	mode local
	}
	client-ip-pool {
	start 192.168.100.101
	stop 192.168.100.110
	}
	outside-address 12.34.56.78

The next step is to configure the PPTP VPN client on a Windows XP SP2 system (the remote user in the example). You can use the Windows "New Connection Wizard" as follows.

1 Select Start > Control Panel > Network Connections.

2 Click Create a new connection. The New Connection Wizard launches. Click Next.

3 Select Connect to the network at my workplace. Click Next.

4 Select Virtual Private Network connection. Click Next.

5 Enter a name for the connection; for example “Vyatta-PPTP.” Click Next.

6 Select Do not dial the initial connection. Click Next.

7 Type the VPN server address (12.34.56.78 in the example). Click Next.

8 Select Do not use my smart card. Click Next.

9 Click Finish.

To connect to the VPN server, double-click the VPN connection icon, enter your user name (“testuser” in the example) and password (“testpassword” in the example), and then click Connect. The “show interfaces” and “show vpn remote-access” operational commands will display the connected user on an interface named “pptpX” where “X” is an integer.

NOTE *You must make sure that, between the remote client and the VPN server, nothing is blocking packets with protocol GRE or TCP port 1723. (Check firewall settings, home gateway, DSL modem, ISP, and so on.)*

L2TP/IPsec with Pre-Shared Key VPN Example

The first step in configuring a basic remote access VPN setup using L2TP/IPsec with pre-shared key between R1 and a Windows XP client is to configure R1 as an L2TP/IPsec–based VPN server.

Example 3-2 Remote Access VPN - L2TP/IPsec example

Step	Command
Define the interface used for IPsec; in this case, wan1.	`vyatta@R1#` **`set vpn ipsec ipsec-interfaces interface wan1`**
Enable NAT traversal. This is mandatory.	`vyatta@R1#` **`set vpn ipsec nat-traversal enable`**
Set the allowed subnet.	`vyatta@R1#` **`set vpn ipsec nat-networks allowed-network 192.168.100.0/24`**
Commit the change.	`vyatta@R1#` **`commit`**

Show the ipsec configuration.	`vyatta@R1#` **`show vpn ipsec`**
	`ipsec-interfaces {`
	`    interface wan1`
	`}`
	`nat-networks {`
	`    allowed-network 192.168.100.0/24 {`
	`    }`
	`}`
	`nat-traversal enable`

Example 3-2 Remote Access VPN - L2TP/IPsec example

Bind the L2TP server to the external address.	vyatta@R1# **set vpn l2tp remote-access outside-address 12.34.56.78**
Set the nexthop address.	vyatta@R1# **set vpn l2tp remote-access outside-nexthop 12.34.56.254**
Set up the pool of IP addresses that remote VPN connections will assume. In this case we make 10 addresses available (from .101 to .110) on subnet 192.168.100.0/24. Note that we do not use the subnet on the LAN.	vyatta@R1# **set vpn l2tp remote-access client-ip-pool start 192.168.100.101** vyatta@R1# **set vpn l2tp remote-access client-ip-pool stop 192.168.100.110**
Set the IPsec authentication mode to pre-shared secret.	vyatta@R1# **set vpn l2tp remote-access ipsec-settings authentication mode pre-shared-secret**
Set the pre-shared secret.	vyatta@R1# **set vpn l2tp remote-access ipsec-settings authentication pre-shared-secret !secrettext!**
Set the L2TP remote access authentication mode to local.	vyatta@R1# **set vpn l2tp remote-access authentication mode local**
Set theL2TP remote access username and password.	vyatta@R1# **set vpn l2tp remote-access authentication local-users username testuser password testpassword**
Commit the change.	vyatta@R1# **commit**

Example 3-2 Remote Access VPN - L2TP/IPsec example

Show the l2tp remote access configuration.	`vyatta@R1# show vpn l2tp remote-access`
	`authentication {`
	`    local-users {`
	`        username testuser {`
	`            password testpassword`
	`        }`
	`    }`
	`    mode local`
	`}`
	`client-ip-pool {`
	`    start 192.168.100.101`
	`    stop 192.168.100.110`
	`}`
	`ipsec-settings {`
	`    authentication {`
	`        mode pre-shared-secret`
	`        pre-shared-secret !secrettext!`
	`    }`
	`}`
	`outside-address 12.34.56.78`
	`outside-nexthop 12.34.56.254`

The next step is to configure the L2TP/IPsec VPN client on a Windows XP SP2 system (the remote user in the example). You can use the Windows "New Connection Wizard" as follows.

1 Select Start > Control Panel > Network Connections.
2 Click "Create a new connection". The New Connection Wizard launches. Click Next.
3 Select "Connect to the network at my workplace". Click Next.
4 Select "Virtual Private Network connection". Click Next.
5 Enter a name for the connection; for example "Vyatta-L2TP." Click Next.
6 Select "Do not dial the initial connection". Click Next.
7 Type the VPN server address (12.34.56.78 in the example). Click Next.
8 If asked, select "Do not use my smart card". Click Next.
9 Click Finish.

By default, after the VPN configuration is created, a pre-shared key is not configured and must be added.

1 Go to "Network Connections" in the "Control Panel".

2 Right-click the “Vyatta-L2TP” (or whatever name you specified) icon. Select “Properties”.

3 Click the “Security” tab. Click “IPsec Settings...”.

4 Check the “Use pre-shared key for authentication” checkbox.

5 Type the pre-shared key (!secrettext! in our example) in the “Key” field.

6 Click “OK”. Click “OK”.

To connect to the VPN server, double-click the “Vyatta-L2TP” icon, type the user name (“testuser” in our example) and password (“testpassword” in our example), and then click “Connect”. The “show interfaces” and “show vpn remote-access” operational commands will display the connected user on an interface named “l2tpX” where “X” is an integer.

NOTE *You need to make sure that, between the remote client and the VPN server, nothing is blocking packets with protocol L2TP or UDP port 500. (Check firewall settings, home gateway, DSL modem, ISP, etc.)*

L2TP/IPsec with X.509 Certificates VPN Example

The first step in configuring a basic remote access VPN setup using L2TP/IPsec with X.509 certificates between R1 and a Windows XP client is to obtain the files necessary for authentication using X.509 certificates. In general, the procedure for doing this is as follows:

1 Generate the private key and a certificate signing request (CSR) (based on the public key). This can be accomplished using generate vpn x509 key-pair <name> (for example, **generate vpn x509 key-pair R1**, where **R1.key** is the private key and **R1.csr** is the certificate signing request file - both created in /config/auth).

2 Send the CSR file (for example, **R1.csr**) to the certificate autority (CA) and receive back a server certificate (for example, **R1.crt**), the CA certificate (for example, **ca.crt**), and potentially, a certificate revocation list (CRL) file. This procedure varies according to the CA being used.

3 The same procedure should be followed to obtain equivalent files for the Windows client machine (for example, **windows.crt** and **windows.key**). The same CA certificate (**ca.crt**) can be used on the Windows machine.

NOTE *If the CA can combine the **windows.crt** and **windows.key** files and export a PKCS #12 file (for example, **windows.p12)**, it will save a step later on.*

Once the X.509-related files have been generated or acquired, the next step is to configure R1 as an L2TP/IPsec–based VPN server.

Example 3-3 Remote Access VPN - L2TP/IPsec example

Step	Command
Define the interface used for IPsec; in this case, wan1.	`vyatta@R1#` **`set vpn ipsec ipsec-interfaces interface wan1`**
Enable NAT traversal. This is mandatory.	`vyatta@R1#` **`set vpn ipsec nat-traversal enable`**
Set the allowed subnet.	`vyatta@R1#` **`set vpn ipsec nat-networks allowed-network 192.168.100.0/24`**
Commit the change.	`vyatta@R1#` **`commit`**

Show the ipsec configuration.	`vyatta@R1#` **`show vpn ipsec`**
	`ipsec-interfaces {`
	`    interface wan1`
	`}`
	`nat-networks {`
	`    allowed-network 192.168.100.0/24 {`
	`    }`
	`}`
	`nat-traversal enable`

Bind the L2TP server to the external address.	`vyatta@R1#` **`set vpn l2tp remote-access outside-address 12.34.56.78`**
Set the nexthop address.	`vyatta@R1#` **`set vpn l2tp remote-access outside-nexthop 12.34.56.254`**
Set up the pool of IP addresses that remote VPN connections will assume. In this case we make 10 addresses available (from .101 to .110) on subnet 192.168.100.0/24. Note that we do not use the subnet on the LAN.	`vyatta@R1#` **`set vpn l2tp remote-access client-ip-pool start 192.168.100.101`** `vyatta@R1#` **`set vpn l2tp remote-access client-ip-pool stop 192.168.100.110`**
Set the IPsec authentication mode to x509.	`vyatta@R1#` **`set vpn l2tp remote-access ipsec-settings authentication mode x509`**
Specify the location of the CA certificate.	`vyatta@R1#` **`set vpn l2tp remote-access ipsec-settings authentication x509 ca-cert-file /config/auth/ca.crt`**
Specify the location of the server certificate.	`vyatta@R1#` **`set vpn l2tp remote-access ipsec-settings authentication x509 server-cert-file /config/auth/R1.crt`**
Specify the location of the server key file.	`vyatta@R1#` **`set vpn l2tp remote-access ipsec-settings authentication x509 server-key-file /config/auth/R1.key`**

Example 3-3 Remote Access VPN - L2TP/IPsec example

Specify the password for the server key file.	vyatta@R1# **set vpn l2tp remote-access ipsec-settings authentication x509 server-key-password testpwd-R1**
Set the L2TP remote access authentication mode to local.	vyatta@R1# **set vpn l2tp remote-access authentication mode local**
Set theL2TP remote access username and password.	vyatta@R1# **set vpn l2tp remote-access authentication local-users username testuser password testpassword**
Commit the change.	vyatta@R1# **commit**

Show the l2tp remote access configuration.	vyatta@R1# **show vpn l2tp remote-access**
	authentication {
	    local-users {
	        username testuser {
	            password testpassword
	        }
	    }
	    mode local
	}
	client-ip-pool {
	    start 192.168.100.101
	    stop 192.168.100.110
	}
	ipsec-settings {
	    authentication {
	        mode x509
	        x509 {
	            ca-cert-file /config/auth/ca.crt
	            server-cert-file /config/auth/R1.crt
	            server-key-file /config/auth/R1.key
	            server-key-password testpwd-R1
	        }
	    }
	}
	outside-address 12.34.56.78
	outside-nexthop 12.34.56.254

Once R1 is configured, the next step is to configure the L2TP/IPsec VPN client on a Windows XP SP2 system (the remote user in the example). The first part of this is to import the key and certificate files created by the CA onto the Windows machine. Windows expects the key and server certificates to be wrapped into a single file in a PKCS #12 format (a .p12 file).

***NOTE** If the CA does not provide this then you will need to use a tool (e.g. openssl) to combine the key file and the certificate file for the Windows machine into a .p12 file.*

1. Copy the **ca.crt** and **windows.p12** files to the Windows machine.
2. On the Windows machine: Select Start > Run... - the Run dialog opens.
3. Enter “mmc” at the “Open:” prompt. Click OK. The “Console1” MMC console opens.
4. Select File > Add/Remove Snap-in.... The Add/Remove Snap-in dialog opens.
5. Click Add.... The Add Standalone Snap-in dialog opens.
6. Select “Certificates” in the list of Available standalone snap-ins. Click Add. The Certificates snap-in dialog opens.
7. Select “Computer account”, Click Next. The Select Computer dialog appears.
8. Select “Local computer (the computer this console is running on)”. Click Finish. Click Close. Click OK. “Certificates (Local Computer)” appears beneath “Console Root” in the “Console1” MMC console.
9. Expand “Certificates (Local Computer)”.
10. Right click “Personal” and select All Tasks > Import.... The Certificate Import Wizard opens.
11. Click Next. Specify the location of the **windows.p12** file. Click Next.
12. Enter the password for the private key. Click Next. Click Finish.
13. Right click “Trusted Root Certification Authorities” and select All Tasks > Import.... The Certificate Import Wizard opens.
14. Click Next. Specify the location of the **ca.crt** file. Click Next.
15. Click Finish. Close the “Console1” MMC console.

At this point the necessary key and certificate files have been imported to the Windows machine. The next part of configuring the L2TP/IPsec VPN client on the Windows XP SP2 system is to specify the VPN connection. You can use the Windows “New Connection Wizard” as follows.

1. Select Start > Control Panel > Network Connections.
2. Click “Create a new connection”. The New Connection Wizard launches. Click Next.
3. Select “Connect to the network at my workplace”. Click Next.
4. Select “Virtual Private Network connection”. Click Next.
5. Enter a name for the connection; for example “Vyatta-X509.” Click Next.
6. Select “Do not dial the initial connection”. Click Next.
7. Type the VPN server address (12.34.56.78 in the example). Click Next.
8. If asked, select “Do not use my smart card”. Click Next.

9 Click Finish.

At this point, the configuration on the Windows machine is complete.

To connect to the VPN server, double-click the "Vyatta-X509" icon. Enter the User name and Password then click "Connect"to establish the connection.

The "show interfaces" and "show vpn remote-access" operational commands will display the connected user on an interface named "l2tpX" where "X" is an integer.

NOTE *You need to make sure that, between the remote client and the VPN server, nothing is blocking packets with protocol L2TP or UDP port 500. (Check firewall settings, home gateway, DSL modem, ISP, etc.)*

PPTP VPN Example with a Dynamic IP Address and using Dynamic DNS

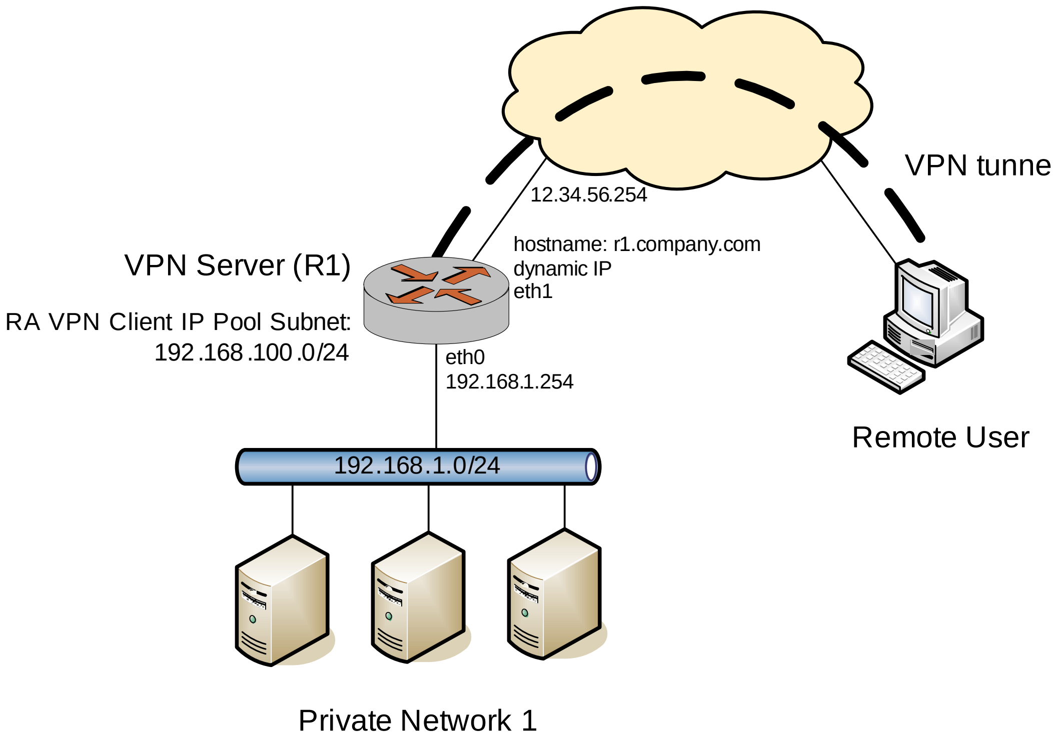
The following example shows how to configure RA VPN in the situation where the external interface on the RA VPN server has a dynamic IP address rather than a static IP address. The difference between these two scenarios is that instead of configuring an **outside-address**, you configure a **dhcp-interface**.

This example assumes that R1 is configured for dynamic DNS, in this case with service provider DynDNS. See the "Configuring Dynamic DNS" section in the *Vyatta Services Reference Guide* for details on configuring a system for dynamic DNS.

NOTE *In this example we use PPTP, but the same would apply if L2TP/IPsec was used.*

This configuration example uses the diagram shown in Figure 3-9 as the deployment scenario:

Figure 3-9 Remote Access VPN Example with a Dynamic IP Address



The first step in configuring a basic remote access VPN setup using PPTP between R1 and a Windows XP client is to configure R1 as a PPTP–based VPN server.

Example 3-4 Remote Access VPN with dynamic IP - PPTP example)

Step	Command
Bind the PPTP server to the external interface.	vyatta@R1# **set vpn pptp remote-access dhcp-interface eth1**
Set up the pool of IP addresses that remote VPN connections will assume. In this case we make 10 addresses available (from .101 to .110) on subnet 192.168.100.0/24. Note that we do not use the subnet on the LAN.	vyatta@R1# **set vpn pptp remote-access client-ip-pool start 192.168.100.101** vyatta@R1# **set vpn pptp remote-access client-ip-pool stop 192.168.100.110**
Set up the authentication mode - in this case “local”.	vyatta@R1# **set vpn pptp remote-access authentication mode local**
Set up a user (testuser) and password (testpassword).	vyatta@R1# **set vpn pptp remote-access authentication local-users username testuser password testpassword**

Example 3-4 Remote Access VPN with dynamic IP - PPTP example)

Commit the change.	`vyatta@R1# commit`

Show the configuration.	`vyatta@R1# show vpn pptp remote-access`
	`authentication {`
	`local-users {`
	`username testuser{`
	`password testpassword`
	`}`
	`}`
	`mode local`
	`}`
	`client-ip-pool {`
	`start 192.168.100.101`
	`stop 192.168.100.110`
	`}`
	`dhcp-interface eth1`

View ethernet interface eth1 address configuration. It is set to **dhcp** which configures it as a DHCP client. This is the setting required by **dhcp-interface**.	`vyatta@R1# show interfaces ethernet eth1` `address dhcp`

Display the dynamic DNS configuration on R1:

Example 3-5 Display the dynamic DNS configuration.

Step	Command

View the dynamic DNS configuration.	`vyatta@R1# show service dns dynamic`
	`interface eth1 {`
	`service dyndns {`
	`host-name r1.company.com`
	`login test`
	`password testpassword`
	`}`
	`}`

The next step is to configure the PPTP VPN client on a Windows XP SP2 system (the remote user in the example). The main change between this and the PPTP example that uses a static IP address at the RA VPN server (see "PPTP VPN Example" on page 219) is that instead of specifying the IP address of the RA VPN server, you must specify the hostname that has been configured with the dynamic DNS provider. In this case the hostname is “r1.company.com”. You can use the Windows “New Connection Wizard” as follows:

1 Select Start > Control Panel > Network Connections.
2 Click Create a new connection. The New Connection Wizard launches. Click Next.
3 Select Connect to the network at my workplace. Click Next.
4 Select Virtual Private Network connection. Click Next.
5 Enter a name for the connection; for example “Vyatta-PPTP.” Click Next.
6 Select Do not dial the initial connection. Click Next.
7 Type the VPN server hostname (r1.company.com in the example). Click Next.
8 Select Do not use my smart card. Click Next.
9 Click Finish.

To connect to the VPN server, double-click the VPN connection icon, enter your user name (“testuser” in the example) and password (“testpassword” in the example), and then click Connect. The “show interfaces” and “show vpn remote-access” operational commands will display the connected user on an interface named “pptpX” where “X” is an integer.

NOTE *You must make sure that, between the remote client and the VPN server, nothing is blocking packets with protocol GRE or TCP port 1723. (Check firewall settings, home gateway, DSL modem, ISP, and so on.)*

Configuring Split Tunneling on a Windows Client

On a Windows client, by default, after the VPN configuration is created, the client is configured for Full Tunneling (all traffic flows across the VPN). If you want to configure the client for Split Tunneling (where Internet traffic does not flow across the VPN), you can modify the client VPN configuration as follows:

1 Select Start > Control Panel > Network Connections.
2 Right-click the icon for the VPN connection (“Vyatta-PPTP” in the first example). Click Properties.
3 Click the Networking tab. Select “Internet Protocol (TCP/IP)”, then click Properties.
4 Click Advanced. Uncheck the “Use default gateway on remote network” checkbox.
5 Click OK three times.

Monitoring Remote Access VPN

This section presents the following topics:

- Showing Interface Information
- Showing Remote Access VPN Information

This section includes the following examples:

- Example 3-6 Viewing interface information
- Example 3-7 Viewing Remote Access VPN information

Showing Interface Information

To see high-level interface information, you can use the **show interfaces** operational mode command, as shown in Example 3-6. For Remote Access VPN connections, in addition to the local interface andthe IP address it is bound to, you will see the remote user's name and the IP address assigned to the remote user (see pptp0 and pptp4 in this example).

Example 3-6 Viewing interface information

```
vyatta@vyatta:~$ show interfaces

Interface     IP Address          State       Link   Description
eth0          192.168.55.11/24    up          up     mgmt
eth1          192.168.1.2/30      up          up
eth2          172.16.0.1/24       up          up
eth3          -                   up          up
gre0          -                   admin down  down
lo            127.0.0.1/8         up          up
lo            ::1/128             up          up
pptp0         10.255.254.0        up          up     User: bill (172.16.2.100)
pptp4         10.255.254.0        up          up     User: dave (172.16.2.101)

vyatta@vyatta:~$
```

Showing Remote Access VPN Information

To see Remote Access VPN information specifically, you can use the **show vpn remote-access** operational mode command, as shown in Example 3-7.

Example 3-7 Viewing Remote Access VPN information

```
vyatta@vyatta:~$ show vpn remote-access

Active remote access VPN sessions:

User       Time      Proto Iface Remote IP       TX pkt/byte   RX pkt/byte
---------- --------- ----- ----- --------------- ------ ------ ------ ------
bill       12h09m41s PPTP  pptp0 172.16.2.100       154  21.6K  10.2K 809.3K
dave       22h07m55s PPTP  pptp4 172.16.2.101    479.9K  47.8M 318.9K  16.6M

vyatta@vyatta:~$
```

Remote Access VPN Commands

This chapter contains the following commands.

Configuration Commands	
Global IPsec	
vpn ipsec	For these commands, see "Chapter 2: IPsec Site-to-Site VPN."
vpn ipsec auto-update <interval>	
vpn ipsec ipsec-interfaces interface <if-name>	
vpn ipsec logging	
vpn ipsec nat-networks allowed-network <ipv4net>	
vpn ipsec nat-traversal <state>	
L2TP	
vpn l2tp	Creates the top-most configuration node for L2TP VPN, enabling L2TP VPN functionality.
vpn l2tp remote-access authentication mode <mode>	Specifies user authentication mode for L2TP VPN remote access connections.
vpn l2tp remote-access authentication local-users user-name <user-name>	Specifies the login credentials for L2TP VPN remote users being authenticated locally.
vpn l2tp remote-access authentication radius-server <ipv4> key <key>	Defines a RADIUS server authenticating L2TP VPN remote users.
vpn l2tp remote-access client-ip-pool start <ipv4>	Specifies the beginning address of a pool of IP addresses for L2TP VPN remote clients.
vpn l2tp remote-access client-ip-pool stop <ipv4>	Specifies the ending address of a pool of IP addresses for L2TP VPN remote clients.
vpn l2tp remote-access dhcp-interface <interface>	Specifies a DHCP client interface to use for remote access L2TP VPN connections.
vpn l2tp remote-access dns-servers server-1 <ipv4>	Specifies the IP address for the primary DNS server for L2TP VPN remote clients.
vpn l2tp remote-access dns-servers server-2 <ipv4>	Specifies the IP address for the secondary DNS server for L2TP VPN remote clients.
vpn l2tp remote-access ipsec-settings authentication mode <mode>	Sets the IPsec authentication mode to be used for IPsec authentication on remote access L2TP VPN connections.

vpn l2tp remote-access ipsec-settings authentication pre-shared-secret <secret>	Sets a pre-shared key for IPsec authentication on remote access L2TP VPN connections.
vpn l2tp remote-access ipsec-settings authentication x509 ca-cert-file <file-name>	Specifies the name of an X.509 Certificate Authority (CA) certificate file for IPsec authentication on remote access L2TP VPN connections.
vpn l2tp remote-access ipsec-settings authentication x509 crl-file <file-name>	Specifies the name of an X.509 Certificate Revocation List (CRL) file for IPsec authentication on L2TP VPN remote access connections.
vpn l2tp remote-access ipsec-settings authentication x509 server-cert-file <file-name>	Specifies the name of VPN server's certificate file for IPsec authentication on L2TP VPN remote access connections.
vpn l2tp remote-access ipsec-settings authentication x509 server-key-file <file-name>	Specifies the name of VPN server's private key file for IPsec authentication on L2TP VPN remote access connections.
vpn l2tp remote-access ipsec-settings authentication x509 server-key-password <password>	Specifies the password that protects the L2TP VPN server's private key.
vpn l2tp remote-access ipsec-settings ike-lifetime <lifetime>	Specifies the IKE lifetime of an L2TP connection.
vpn l2tp remote-access mtu <mtu>	Specifies the MTU for an L2TP connection.
vpn l2tp remote-access outside-address <ipv4>	Sets the IP address to be bound to the L2TP server.
vpn l2tp remote-access outside-nexthop <ipv4>	Sets the IP address of the next hop on the external network.
vpn l2tp remote-access wins-servers server-1 <ipv4>	Specifies the IP address for the primary WINS server for L2TP VPN remote clients.
vpn l2tp remote-access wins-servers server-2 <ipv4>	Specifies the IP address for the secondary WINS server for L2TP VPN remote clients.
PPTP	
vpn pptp	Creates the top-most configuration node for PPTP VPN, enabling PPTP VPN functionality.
vpn pptp remote-access authentication mode <mode>	Specifies user authentication mode for PPTP VPN remote access connections.
vpn pptp remote-access authentication local-users user-name <user-name>	Specifies the login credentials for PPTP VPN remote users being authenticated locally.
vpn pptp remote-access authentication radius-server <ipv4> key <key>	Specifies the RADIUS server to use to authenticate PPTP VPN remote users.

vpn pptp remote-access client-ip-pool start <ipv4>	Specifies the beginning address of a pool of IP addresses for PPTP VPN remote clients.
vpn pptp remote-access client-ip-pool stop <ipv4>	Specifies the ending address of a pool of IP addresses for PPTP VPN remote clients.
vpn pptp remote-access dhcp-interface <interface>	Specifies a DHCP client interface to use for remote access PPTP VPN connections.
vpn pptp remote-access dns-servers server-1 <ipv4>	Specifies the IP address for the primary DNS server for PPTP VPN remote clients.
vpn pptp remote-access dns-servers server-2 <ipv4>	Specifies the IP address for the secondary DNS server for PPTP VPN remote clients.
vpn pptp remote-access mtu <mtu>	Specifies the MTU for a PPTP connection.
vpn pptp remote-access outside-address <ipv4>	Sets the IP address to be bound to the PPTP server.
vpn pptp remote-access wins-servers server-1 <ipv4>	Specifies the IP address for the primary WINS server for PPTP VPN remote clients.
vpn pptp remote-access wins-servers server-2 <ipv4>	Specifies the IP address for the secondary WINS server for PPTP VPN remote clients.
Operational Commands	
clear vpn remote-access interface <interface>	Terminates the specified active session.
clear vpn remote-access user <user-name>	Terminates the specified user’s active sessions.
generate vpn x509 key-pair <name>	Generates an X.509 private key file and a certificate signing request file. See “Chapter 2: IPsec Site-to-Site VPN.”
restart vpn	Restarts the IPsec process. See “Chapter 2: IPsec Site-to-Site VPN.”
show vpn debug	Provides trace-level information about IPsec VPN. See “Chapter 2: IPsec Site-to-Site VPN.”
show vpn ipsec sa	Provides information about active IPsec security associations. See “Chapter 2: IPsec Site-to-Site VPN.”
show vpn ipsec sa nat-traversal	Provides information about all active IPsec security associations that are using NAT Traversal. See “Chapter 2: IPsec Site-to-Site VPN.”
show vpn ipsec status	Displays information about the status of IPsec processes. See “Chapter 2: IPsec Site-to-Site VPN.”
show vpn remote-access	Shows information about currently active remote access VPN sessions.

clear vpn remote-access interface <interface>

Terminates the specified active session.

Syntax

clear vpn remote-access interface *interface*

Command Mode

Operational mode.

Configuration Statement

None.

Parameters

interface	The interface associated with the session to be terminated.

Default

None.

Usage Guidelines

Use this command to terminate a specific remote access VPN tunnel.

Examples

Example 3-8 terminates the active session on pptp0.

Example 3-8 "clear vpn remote-access interface": Terminating an active session

```
vyatta@vyatta# clear vpn remote-access interface pptp0
vyatta@vyatta#
```

clear vpn remote-access user <user-name>

Terminates the specified user's active sessions.

Syntax

clear vpn remote-access user *user-name*

Command Mode

Operational mode.

Configuration Statement

None.

Parameters

user-name	The user name associated with the sessions to be terminated.

Default

None.

Usage Guidelines

Use this command to terminate all remote access VPN tunnels for the specified user.

Examples

Example 3-9 terminates all active sessions for user robert.

Example 3-9 "clear vpn remote-access user": Terminating a user's active sessions

```
vyatta@vyatta# clear vpn remote-access user robert
vyatta@vyatta#
```

show vpn remote-access

Shows information about currently active remote access VPN sessions.

Syntax

show vpn remote-access

Command Mode

Operational mode.

Configuration Statement

None.

Parameters

None

Default

None.

Usage Guidelines

Use this command to see information about the currently active remote access VPN sessions.

Examples

Example 3-10 shows the output of the **show vpn remote-access** command.

Example 3-10 “show vpn remote-access”: Viewing remote VPN sessions

```
vyatta@vyatta# show vpn remote-access
Active remote access VPN sessions:

User       Time      Proto Iface Remote IP       TX pkt/byte   RX pkt/byte
---------- --------- ----- ----- --------------- ------ ------ ------ ------
stig       01d02h12m PPTP  pptp0 10.254.1.1       28.0K   7.7M  26.3K   2.0M
shemminger 00h12m15s PPTP  pptp1 10.254.1.2       85.2K 119.6M  46.6K   2.7M
ancheng    15h15m33s PPTP  pptp2 10.254.1.3       73.6K  28.5M  68.3K   4.3M
vpn:~#
```

```
vyatta@vyatta#
```

vpn l2tp

Creates the top-most configuration node for L2TP VPN, enabling L2TP VPN functionality.

Syntax

set vpn l2tp

delete vpn l2tp

show vpn l2tp

Command Mode

Configuration mode.

Configuration Statement

```
vpn {
    l2tp
}
```

Parameters

None.

Default

None.

Usage Guidelines

Use this command to create the configuration node for Layer 2 Tunneling Protocol (L2TP) Virtual Private Network (VPN) functionality.

Use the **set** form of this command to create the L2TP VPN configuration node.

Use the **delete** form of this command to remove all L2TP VPN configuration.

Use the **show** form of this command to display L2TP VPN configuration.

vpn l2tp remote-access authentication mode <mode>

Specifies user authentication mode for L2TP VPN remote access connections.

Syntax

set vpn l2tp remote-access authentication mode *mode*

delete vpn l2tp remote-access authentication mode

show vpn l2tp remote-access authentication mode

Command Mode

Configuration mode.

Configuration Statement

```
vpn {
    l2tp {
        remote-access {
            authentication {
                mode mode
            }
        }
    }
}
```

Parameters

mode	Mandatory. The mode to be used for authenticating remote users. Supported values are as follows: **local:** Authenticates users locally. **radius:** Authenticates using a RADIUS server.

Default

Users are authenticated using the system's local user database defined in the vpn l2tp configuration.

Usage Guidelines

Use this command to specify how L2TP VPN remote users are to be authenticated.

Users can be authenticated either locally, using login credentials specified using the vpn l2tp remote-access authentication local-users user-name <user-name> command, or using one or more servers running the Remote Access Dial In User Service (RADIUS) protocol.

If you specify RADIUS authentication, you must specify the location of the RADIUS servers, and record the RADIUS login password, by using the vpn l2tp remote-access authentication radius-server <ipv4> key <key> command.

Use the **set** form of this command to configure the authentication mode for users.

Use the **delete** form of this command to remove the user authentication mode.

Use the **show** form of this command to display the user authentication mode.

vpn l2tp remote-access authentication local-users user-name <user-name>

Specifies the login credentials for L2TP VPN remote users being authenticated locally.

Syntax

set vpn l2tp remote-access authentication local-users user-name *user-name* [**disable** | **password** *password* | **static-ip** *ipv4*]

delete vpn l2tp remote-access authentication local-users user-name *user-name* [**disable** | **password** | **static-ip**]

show vpn l2tp remote-access authentication local-users user-name *user-name* [**password** | **static-ip**]

Command Mode

Configuration mode.

Configuration Statement

```
vpn {
    l2tp {
        remote-access {
            authentication {
                local-users {
                    user-name user-name {
                        disable
                        password password
                        static-ip ipv4
                    }
                }
            }
        }
    }
}
```

Parameters

user-name	The user name. Mandatory if **authentication mode** is **local.**
disable	Disables remote access for the user.

password	The login password for the specified user. Mandatory if **authentication mode** is **local**.
ipv4	The IPv4 address to assign the user when they connect. This address does not have to be part of the **client-ip-pool**.

Default

None.

Usage Guidelines

Use this command to specify login credentials for L2TP VPN remote users and, optionally, to specify the IP address that will be assigned to a user when they connect.

Use the **set** form of this command to create the user name configuration node for the user.

Use the **delete** form of this command to remove a user's login credentials.

Use the **show** form of this command to display the user login authentication configuration.

vpn l2tp remote-access authentication radius-server <ipv4> key <key>

Defines a RADIUS server authenticating L2TP VPN remote users.

Syntax

set vpn l2tp remote-access authentication radius-server *ipv4* **key** *key*

delete vpn l2tp remote-access authentication radius-server *ipv4* [**key**]

show vpn l2tp remote-access authentication radius-server *ipv4* [**key**]

Command Mode

Configuration mode.

Configuration Statement

```
vpn {

    l2tp {
        remote-access {
            authentication {
                radius-server ipv4 {
                    key key
                }
            }
        }
    }

}
```

Parameters

ipv4	Multi-node. The IPv4 address of the RADIUS server. Mandatory if **authentication mode** is **radius**. You can define more than one RADIUS server by creating multiple **radius-server** configuration nodes.

key	The password for the RADIUS server. This must be the same as that recorded on the RADIUS server. Mandatory if **authentication mode** is **radius**. Supported characters are alphanumeric, space, and special characters. Strings containing spaces must be enclosed in double quotes.

Default

None.

Usage Guidelines

Use this command to define one or more RADIUS servers for authenticating remote L2TP VPN and the login credentials required to access it.

At least one RADIUS server must be defined if RADIUS is set as the user authentication mode.

RADIUS servers are queried in the order they were configured. If the query to the first RADIUS server times out, the next RADIUS server in the list is queried. If no query is successful, the login attempt fails.

The RADIUS secret is specified in plain text. RADIUS secrets are stored in plain text on the system, and used as part of a cryptographic operation for transferring authentication information securely over the network. When you view RADIUS secrets, they are displayed in plain text.

Use the **set** form of this command to define a RADIUS server. Note that you cannot use **set** to change the IP address of a defined server. To change the server's IP address, delete the server and create a new one.

Use the **delete** form of this command to remove the RADIUS server configuration node or the key. Note that the key is mandatory; if you delete the key, you must configure another one.

Use the **show** form of this command to display RADIUS server configuration.

vpn l2tp remote-access client-ip-pool start <ipv4>

Specifies the beginning address of a pool of IP addresses for L2TP VPN remote clients.

Syntax

set vpn l2tp remote-access client-ip-pool start *ipv4*

delete vpn l2tp remote-access client-ip-pool start

show vpn l2tp remote-access client-ip-pool start

Command Mode

Configuration mode.

Configuration Statement

```
vpn {
    l2tp {
        remote-access {
            client-ip-pool {
                start ipv4
            }
        }
    }
}
```

Parameters

ipv4	Mandatory. The IP address that designates the beginning of the address pool.

Default

None.

Usage Guidelines

Use this command to specify the start of an address pool for remote remote L2TP VPN clients.

Both the start address and the stop address must be specified. The stop address is specified using the vpn l2tp remote-access client-ip-pool stop <ipv4> command.

Use the **set** form of this command to define the start address.

Use the **delete** form of this command to remove the start address.

Use the **show** form of this command to display the start address.

vpn l2tp remote-access client-ip-pool stop <ipv4>

Specifies the ending address of a pool of IP addresses for L2TP VPN remote clients.

Syntax

set vpn l2tp remote-access client-ip-pool stop *ipv4*

delete vpn l2tp remote-access client-ip-pool stop

show vpn l2tp remote-access client-ip-pool stop

Command Mode

Configuration mode.

Configuration Statement

```
vpn {
    l2tp {
        remote-access {
            client-ip-pool {
                stop ipv4
            }
        }
    }
}
```

Parameters

ipv4	Mandatory. The IP address that designates the end of the address pool.

Default

None.

Usage Guidelines

Use this command to specify the end of the address pool for remote L2TP VPN clients.

Both the start address and the stop address must be specified. The start address is specified using the vpn l2tp remote-access client-ip-pool start <ipv4> command.

Use the **set** form of this command to define the stop address.

Use the **delete** form of this command to remove the stop address.

Use the **show** form of this command to display the stop address.

vpn l2tp remote-access dhcp-interface <interface>

Specifies a DHCP client interface to use for remote access L2TP VPN connections.

Syntax

set vpn l2tp remote-access dhcp-interface *interface*

delete vpn l2tp remote-access dhcp-interface

show vpn l2tp remote-access dhcp-interface

Command Mode

Configuration mode.

Configuration Statement

```
vpn {
    l2tp {
        remote-access {
            dhcp-interface interface
        }
    }
}
```

Parameters

interface	The interface to use for remote access L2TP VPN connections (e.g. eth0). Please note that the interface must already have IPsec VPN enabled, using the vpn ipsec ipsec-interfaces interface <if-name> command, and must be configured as a DHCP client.

Default

None.

Usage Guidelines

Use this command to specify a DHCP client interface to use for remote access L2TP VPN connections. Connections will be automatically restarted if the IP address changes.

The DHCP interface is the interface facing the external network. This is the interface to which the L2TP server binds, and only remote connections coming into this interface will be accepted.

NOTE *This option cannot be used if vpn l2tp remote-access outside-address <ipv4> is also set.*

Use the **set** form of this command to specify a DHCP interface to use for remote accss L2TP VPN connections.

Use the **delete** form of this command to remove the configuration

Use the **show** form of this command to view the configuration.

vpn l2tp remote-access dns-servers server-1 <ipv4>

Specifies the IP address for the primary DNS server for L2TP VPN remote clients.

Syntax

set vpn l2tp remote-access dns-servers server-1 *ipv4*

delete vpn l2tp remote-access dns-servers server-1

show vpn l2tp remote-access dns-servers server-1

Command Mode

Configuration mode.

Configuration Statement

```
vpn {
    l2tp {
        remote-access {
            dns-servers {
                server-1 ipv4
            }
        }
    }
}
```

Parameters

ipv4	The IP address of the primary DNS server for remote clients.

Default

None.

Usage Guidelines

Use this command to specify the primary DNS server to be associated with remote L2TP VPN clients.

Use the **set** form of this command to specify the primary DNS server IP address.

Use the **delete** form of this command to remove the primary DNS server IP address.

Use the **show** form of this command to display the primary DNS server IP address.

vpn l2tp remote-access dns-servers server-2 <ipv4>

Specifies the IP address for the secondary DNS server for L2TP VPN remote clients.

Syntax

set vpn l2tp remote-access dns-servers server-2 *ipv4*

delete vpn l2tp remote-access dns-servers server-2

show vpn l2tp remote-access dns-servers server-2

Command Mode

Configuration mode.

Configuration Statement

```
vpn {
    l2tp {
        remote-access {
            dns-servers {
                server-2 ipv4
            }
        }
    }
}
```

Parameters

ipv4	The IP address of the secondary DNS server for remote clients.

Default

None.

Usage Guidelines

Use this command to specify the secondary DNS server to be associated with remote L2TP VPN clients.

Use the **set** form of this command to specify the secondary DNS server IP address.

Use the **delete** form of this command to remove the secondary DNS server IP address.

Use the **show** form of this command to display the secondary DNS server IP address.

vpn l2tp remote-access ipsec-settings authentication mode <mode>

Sets the IPsec authentication mode to be used for IPsec authentication on remote access L2TP VPN connections.

Syntax

set vpn l2tp remote-access ipsec-settings authentication mode *mode*

delete vpn l2tp remote-access ipsec-settings authentication mode

show vpn l2tp remote-access ipsec-settings authentication mode

Command Mode

Configuration mode.

Configuration Statement

```
vpn {
    l2tp {
        remote-access {
            ipsec-settings {
                authentication {
                    mode mode
                }
            }
        }
    }
}
```

Parameters

mode	Mandatory. Specifies the authentication mode to be used for IPsec authentication on L2TP VPN remote access connections. Supported values are as follows: **pre-shared-secret**: Uses a pre-shared secret for authentication. **x509**: Uses X.509 V.3 certificates for authentication.

Default

Pre-shared secret.

Usage Guidelines

Use this command to set the authentication mode to be used for IPsec authentication on remote access L2TP VPN connections.

A pre-shared secret, or pre-shared key (PSK), is a method of authentication. The secret, or key, is a string agreed upon beforehand by both parties as key for authenticating the session. It is used to generate a hash such that each VPN endpoint can authenticate the other.

If the **authentication mode** is **pre-shared-secret**, you must configure the secret using the vpn l2tp remote-access ipsec-settings authentication pre-shared-secret <secret> command.

The pre-shared secret is not passed from side to side. It is configured on both sides, and must match on both sides. Pre-shared secrets are less secure than X.509 certificates.

NOTE *You should restrict the use of pre-shared keys to smaller, low-risk environments.*

X.509 v.3 certificates are certificates conforming to the ITU-T X.509 version 3 standard for public key infrastructure (PKI). The certificate is issued by a Certificate Authority (CA), and stored securely on the local Vyatta system.

If the mode is X.509 certificates, you must configure all X.509 certificate information.

Use the **set** form of this command to specify the authentication mode for remote access L2TP VPN.

Use the **delete** form of this command to remove authentication mode configuration.

Use the **show** form of this command to display authentication mode configuration.

vpn l2tp remote-access ipsec-settings authentication pre-shared-secret <secret>

Sets a pre-shared key for IPsec authentication on remote access L2TP VPN connections.

Syntax

set vpn l2tp remote-access ipsec-settings authentication pre-shared-secret *secret*

delete vpn l2tp remote-access ipsec-settings authentication pre-shared-secret

show vpn l2tp remote-access ipsec-settings authentication pre-shared-secret

Command Mode

Configuration mode.

Configuration Statement

```
vpn {
    l2tp {
        remote-access {
            ipsec-settings {
                authentication {
                    pre-shared-secret secret
                }
            }
        }
    }
}
```

Parameters

secret	The password, or secret, to be used to authenticate the remote access connection. This parameter is mandatory if **authentication mode** is **pre-shared-secret**. The secret must be the same on both sides of the connection.

Default

None.

Usage Guidelines

Use this command to set a pre-shared secret to be used to authenticate the IPsec part of remote access L2TP VPN connections.

Use the **set** form of this command to specify the pre-shared secret.

Use the **delete** form of this command to remove pre-shared secret configuration.

Use the **show** form of this command to display pre-shared secret configuration.

vpn l2tp remote-access ipsec-settings authentication x509 ca-cert-file <file-name>

Specifies the name of an X.509 Certificate Authority (CA) certificate file for IPsec authentication on remote access L2TP VPN connections.

Syntax

set vpn l2tp remote-access ipsec-settings authentication x509 ca-cert-file *file-name*

delete vpn l2tp remote-access ipsec-settings authentication x509 ca-cert-file

show vpn l2tp remote-access ipsec-settings authentication x509 ca-cert-file

Command Mode

Configuration mode.

Configuration Statement

```
vpn {
    l2tp {
        remote-access {
            ipsec-settings {
                authentication {
                    x509 {
                        ca-cert-file file-name
                    }
                }
            }
        }
    }
}
```

Parameters

file-name	The name of a certificate file. This parameter is mandatory if **authentication mode** is **x509**.

Default

None.

Usage Guidelines

Use this command to specify the name of an X.509 Certificate Authority (CA) certificate file. The X.509 CA certificate is used for IPsec authentication on remote access L2TP VPN connections.

The file is assumed to be in /config/auth unless an absolute path is specified.

Use the **set** form of this command to specify the name of the CA certificate file.

Use the **delete** form of this command to remove the name of the CA certificate file.

Use the **show** form of this command to display CA certificate file configuration.

vpn l2tp remote-access ipsec-settings authentication x509 crl-file <file-name>

Specifies the name of an X.509 Certificate Revocation List (CRL) file for IPsec authentication on L2TP VPN remote access connections.

Syntax

set vpn l2tp remote-access ipsec-settings authentication x509 crl-file *file-name*

delete vpn l2tp remote-access ipsec-settings authentication x509 crl-file

show vpn l2tp remote-access ipsec-settings authentication x509 crl-file

Command Mode

Configuration mode.

Configuration Statement

```
vpn {
    l2tp {
        remote-access {
            ipsec-settings {
                authentication {
                    x509 {
                        crl-file file-name
                    }
                }
            }
        }
    }
}
```

Parameters

file-name	The name of the CRL file.

Default

None.

Usage Guidelines

Use this command to specify the name of a Certificate Revocation List (CRL) file.

A CRL is a time-stamped signed data structure issued by the Certificate Authority (CA) identifying revoked certificates. When the remote user attempts to log on to the system, the system checks both the remote user's certificate signature and also the CRL to make sure that the remote user's certificate serial number is not on the CRL.

The file is assumed to be in /config/auth unless an absolute path is specified.

Use the **set** form of this command to specify the location of the CRL file.

Use the **delete** form of this command to remove the location of the CRL file.

Use the **show** form of this command to display CRL file configuration.

vpn l2tp remote-access ipsec-settings authentication x509 server-cert-file <file-name>

Specifies the name of VPN server's certificate file for IPsec authentication on L2TP VPN remote access connections.

Syntax

set vpn l2tp remote-access ipsec-settings authentication x509 server-cert-file *file-name*

delete vpn l2tp remote-access ipsec-settings authentication x509 server-cert-file

show vpn l2tp remote-access ipsec-settings authentication x509 server-cert-file

Command Mode

Configuration mode.

Configuration Statement

```
vpn {
    l2tp {
        remote-access {
            ipsec-settings {
                authentication {
                    x509 {
                        server-cert-file file-name
                    }
                }
            }
        }
    }
}
```

Parameters

file-name	The name of the VPN server's certificate file. This parameter is mandatory if **authentication mode** is **x509**.

Default

None.

Usage Guidelines

Use this command to specify the name of the VPN server's certificate file.

VPN server's certificate certifies the identity of the VPN server.

The file is assumed to be in /config/auth unless an absolute path is specified.

Use the **set** form of this command to specify the name of the VPN server's certificate file.

Use the **delete** form of this command to remove the name of the VPN server's certificate file.

Use the **show** form of this command to display VPN server certificate file configuration.

vpn l2tp remote-access ipsec-settings authentication x509 server-key-file <file-name>

Specifies the name of VPN server's private key file for IPsec authentication on L2TP VPN remote access connections.

Syntax

set vpn l2tp remote-access ipsec-settings authentication x509 server-key-file *file-name*

delete vpn l2tp remote-access ipsec-settings authentication x509 server-key-file

show vpn l2tp remote-access ipsec-settings authentication x509 server-key-file

Command Mode

Configuration mode.

Configuration Statement

```
vpn {

    l2tp {
        remote-access {
            ipsec-settings {
                authentication {
                    x509 {
                        server-key-file file-name
                    }
                }
            }
        }
    }

}
```

Parameters

file-name	The name of the VPN server's private key file. This parameter is mandatory if **authentication mode** is **x509**.

Default

None.

Usage Guidelines

Use this command to specify the name of the VPN server's private key file.

VPN server's private key certifies the identity of the VPN server.

The file is assumed to be in /config/auth unless an absolute path is specified.

Use the **set** form of this command to specify the name of the VPN server's private key file.

Use the **delete** form of this command to remove the name of the VPN server's private key file.

Use the **show** form of this command to display VPN server private key file configuration.

vpn l2tp remote-access ipsec-settings authentication x509 server-key-password <password>

Specifies the password that protects the L2TP VPN server's private key.

Syntax

set vpn l2tp remote-access ipsec-settings authentication x509 server-key-password *password*

delete vpn l2tp remote-access ipsec-settings authentication x509 server-key-password

show vpn l2tp remote-access ipsec-settings authentication x509 server-key-password

Command Mode

Configuration mode.

Configuration Statement

```
vpn {
    l2tp {
        remote-access {
            ipsec-settings {
                authentication {
                    x509 {
                        server-key-password password
                    }
                }
            }
        }
    }
}
```

Parameters

password	The password protecting the VPN server's private key file.

Default

None.

Usage Guidelines

Use this command to specify a password that protects the VPN server's private key.

Use the **set** form of this command to specify the password for the VPN server's private key.

Use the **delete** form of this command to remove the password for the VPN server's private key.

Use the **show** form of this command to display VPN servers private key password configuration.

vpn l2tp remote-access ipsec-settings ike-lifetime <lifetime>

Specifies the IKE lifetime of an L2TP connection.

Syntax

set vpn l2tp remote-access ipsec-settings ike-lifetime *lifetime*

delete vpn l2tp remote-access ipsec-settings ike-lifetime

show vpn l2tp remote-access ipsec-settings ike-lifetime

Command Mode

Configuration mode.

Configuration Statement

```
vpn {
    l2tp {
        remote-access {
            ipsec-settings {
                ike-lifetime lifetime
            }
        }
    }
}
```

Parameters

lifetime	The length of time (in seconds) the IKE connection will remain active after the last traffic from the remote end is received. The range is 30 to 86400 (that is, 24 hours). The default is 3600 (1 hour).

Default

The IKE lifetime is 3600 seconds (1 hour).

Usage Guidelines

Use this command to specify the IKE lifetime of an L2TP connection. The IKE lifetime is used to terminate a connection when the remote end has not been heard from for a period of time.

Use the **set** form of this command to specify the IKE lifetime of an L2TP connection.

Use the **delete** form of this command to return the IKE lifetime to its default.

Use the **show** form of this command to display IKE lifetime configuration.

vpn l2tp remote-access mtu <mtu>

Specifies the MTU for an L2TP connection.

Syntax

set vpn l2tp remote-access mtu *mtu*

delete vpn l2tp remote-access mtu

show vpn l2tp remote-access mtu

Command Mode

Configuration mode.

Configuration Statement

```
vpn {
    l2tp {
        remote-access {
            mtu mtu
        }
    }
}
```

Parameters

mtu	Sets the MTU, in octets, for the interface as a whole, including any logical interfaces configured for it. The range is 128 to 16384.

Default

If this value is not set, fragmentation is never performed.

Usage Guidelines

Use this command to set the maximum transmission unit (MTU) for an L2TP connection.

When forwarding, IPv4 packets larger than the MTU will be fragmented unless the DF bit is set. In that case, the packets will be dropped and an ICMP "Packet too big" message is returned to the sender.

Use the **set** form of this command to specify the MTU.

Use the **delete** form of this command to remove MTU value and disable fragmentation.

Use the **show** form of this command to view MTU configuration.

vpn l2tp remote-access outside-address <ipv4>

Sets the IP address to be bound to the L2TP server.

Syntax

set vpn l2tp remote-access outside-address *ipv4*

delete vpn l2tp remote-access

show vpn l2tp remote-access

Command Mode

Configuration mode.

Configuration Statement

```
vpn {
    l2tp {
        remote-access {
            outside-address ipv4
        }
    }
}
```

Parameters

ipv4	Mandatory. The IPv4 address to which the L2TP server should bind.

Default

None.

Usage Guidelines

Use this command to set the outside address for a remote access L2TP VPN connection.

The outside address is the address of the interface facing the external network. This is the address to which the L2TP server binds, and only remote connections coming into this address will be accepted.

NOTE *This option cannot be used if vpn l2tp remote-access dhcp-interface <interface> is also set.*

Use the **set** form of this command to set the L2TP VPN outside address.

Use the **delete** form of this command to remove the L2TP VPN outside address.

Use the **show** form of this command to display L2TP VPN outside address configuration.

vpn l2tp remote-access outside-nexthop <ipv4>

Sets the IP address of the next hop on the external network.

Syntax

set vpn l2tp remote-access outside-nexthop *ipv4*

delete vpn l2tp remote-access outside-nexthop *ipv4*

show vpn l2tp remote-access outside-nexthop

Command Mode

Configuration mode.

Configuration Statement

```
vpn {
    l2tp {
        remote-access {
            outside-nexthop ipv4
        }
    }
}
```

Parameters

ipv4	The IPv4 address of the next hop on the outside network.

Default

None.

Usage Guidelines

Use this command to set the next hop on the external network for a remote access L2TP VPN connection.

Use the **set** form of this command to set the L2TP VPN outside next hop.

Use the **delete** form of this command to remove the L2TP VPN outside next hop.

Use the **show** form of this command to display L2TP VPN outside next-hop configuration.

vpn l2tp remote-access wins-servers server-1 <ipv4>

Specifies the IP address for the primary WINS server for L2TP VPN remote clients.

Syntax

set vpn l2tp remote-access wins-servers server-1 *ipv4*

delete vpn l2tp remote-access wins-servers server-1

show vpn l2tp remote-access wins-servers server-1

Command Mode

Configuration mode.

Configuration Statement

```
vpn {
    l2tp {
        remote-access {
            wins-servers {
                server-1 ipv4
            }
        }
    }
}
```

Parameters

ipv4	The IP address of the primary WINS server for remote clients.

Default

None.

Usage Guidelines

Use this command to specify a primary WINS server to be associated with remote L2TP VPN clients.

The Windows Internet Net Service (WINS) is used to support environments in which users access resources that have NetBIOS names.

Use the **set** form of this command to specify the primary WINS server IP address.

Use the **delete** form of this command to remove the primary WINS server IP address.

Use the **show** form of this command to display the primary WINS server IP address.

vpn l2tp remote-access wins-servers server-2 <ipv4>

Specifies the IP address for the secondary WINS server for L2TP VPN remote clients.

Syntax

set vpn l2tp remote-access wins-servers server-2 *ipv4*

delete vpn l2tp remote-access wins-servers server-2

show vpn l2tp remote-access wins-servers server-2

Command Mode

Configuration mode.

Configuration Statement

```
vpn {
    l2tp {
        remote-access {
            wins-servers {
                server-2 ipv4
            }
        }
    }
}
```

Parameters

ipv4	The IP address of the secondary WINS server for remote clients.

Default

None.

Usage Guidelines

Use this command to specify the secondary WINS server to be associated with remote L2TP VPN clients.

The Windows Internet Net Service (WINS) is used to support environments in which users access resources that have NetBIOS names.

Use the **set** form of this command to specify the secondary WINS server IP address.

Use the **delete** form of this command to remove the secondary WINS server IP address.

Use the **show** form of this command to display the secondary WINS server IP address.

vpn pptp

Creates the top-most configuration node for PPTP VPN, enabling PPTP VPN functionality.

Syntax

set vpn pptp

delete vpn pptp

show vpn pptp

Command Mode

Configuration mode.

Configuration Statement

```
vpn {
    pptp
}
```

Parameters

None.

Default

None.

Usage Guidelines

Use this command to create the configuration node for Point-to-Point Tunneling Protocol (PPTP) Virtual Private Network (VPN) functionality.

Use the **set** form of this command to create the PPTP VPN configuration node.

Use the **delete** form of this command to remove all PPTP VPN configuration.

Use the **show** form of this command to display PPTP VPN configuration.

vpn pptp remote-access authentication mode <mode>

Specifies user authentication mode for PPTP VPN remote access connections.

Syntax

set vpn pptp remote-access authentication mode *mode*

delete vpn pptp remote-access authentication mode

show vpn pptp remote-access authentication mode

Command Mode

Configuration mode.

Configuration Statement

```
vpn {
    pptp {
        remote-access {
            authentication {
                mode mode
            }
        }
    }
}
```

Parameters

mode	Mandatory. The mode to be used for authenticating remote users. Supported values are as follows: **local**: Authenticates users locally. **radius**: Authenticates using a RADIUS server.

Default

Users are authenticated using the system's local user database defined in the vpn pptp configuration.

Usage Guidelines

Use this command to specify how PPTP VPN remote users are to be authenticated.

Users can be authenticated either locally, using login credentials specified using the vpn pptp remote-access authentication local-users user-name <user-name> command, or using one or more servers running the Remote Access Dial In User Service (RADIUS) protocol.

If you specify RADIUS authentication, you must specify the location of the RADIUS servers, and record the RADIUS login password, by using the vpn pptp remote-access authentication radius-server <ipv4> key <key> command.

Use the **set** form of this command to configure the authentication mode.

Use the **delete** form of this command to remove the authentication mode.

Use the **show** form of this command to display the authentication mode.

vpn pptp remote-access authentication local-users user-name <user-name>

Specifies the login credentials for PPTP VPN remote users being authenticated locally.

Syntax

set vpn pptp remote-access authentication local-users user-name *user-name* [**disable** | **password** *password* | **static-ip** *ipv4*]

delete vpn pptp remote-access authentication local-users user-name *user-name* [**disable** | **password** | **static-ip**]

show vpn pptp remote-access authentication local-users user-name *user-name* [**password** | **static-ip**]

Command Mode

Configuration mode.

Configuration Statement

```
vpn {

    pptp {
        remote-access {
            authentication {
                local-users {
                    user-name user-name {
                        disable
                        password password
                        static-ip ipv4
                    }
                }
            }
        }
    }

}
```

Parameters

user-name	The user name. This parameter is mandatory if **authentication mode** is **local**.

disable	Disables remote access for the user.
password	The password associated with the user name. This parameter is mandatory if **authentication mode** is **local**.
ipv4	The IPv4 address to assign the user when they connect. This address does not have to be part of the **client-ip-pool**.

Default

None.

Usage Guidelines

Use this command to specify user information for PPTP VPN remote access users that are to be authenticated locally.

Use the **set** form of this command to specify user information for PPTP VPN remote access users that are to be authenticated locally.

Use the **delete** form of this command to remove the configuration.

Use the **show** form of this command to display the configuration.

vpn pptp remote-access authentication radius-server <ipv4> key <key>

Specifies the RADIUS server to use to authenticate PPTP VPN remote users.

Syntax

set vpn pptp remote-access authentication radius-server *ipv4* **key** *key*

delete vpn pptp remote-access authentication radius-server *ipv4* [**key**]

show vpn pptp remote-access authentication radius-server *ipv4* [**key**]

Command Mode

Configuration mode.

Configuration Statement

```
vpn {
    pptp {
        remote-access {
            authentication {
                radius-server ipv4 {
                    key key
                }
            }
        }
    }
}
```

Parameters

radius-server	The IPv4 address of the RADIUS server to use to authenticate remote users. This parameter is mandatory if **authentication mode** is **radius**.
key	The key used to access the RADIUS server. This parameter is mandatory if **authentication mode** is **radius**.

Default

None.

Usage Guidelines

Use this command to define one or more RADIUS servers for authenticating remote PPTP VPN and the login credentials required to access it.

At least one RADIUS server must be defined if RADIUS is set as the user authentication mode.

RADIUS servers are queried in the order they were configured. If the query to the first RADIUS server times out, the next RADIUS server in the list is queried. If no query is successful, the login attempt fails.

The RADIUS secret is specified in plain text. RADIUS secrets are stored in plain text on the system, and used as part of a cryptographic operation for transferring authentication information securely over the network. When you view RADIUS secrets, they are displayed in plain text.

Use the **set** form of this command to define a RADIUS server. Note that you cannot use **set** to change the IP address of a defined server. To change the server's IP address, delete the server and create a new one.

Use the **delete** form of this command to remove the RADIUS server configuration node or the key. Note that the key is mandatory; if you delete the key, you must configure another one.

Use the **show** form of this command to display RADIUS server configuration.

vpn pptp remote-access client-ip-pool start <ipv4>

Specifies the beginning address of a pool of IP addresses for PPTP VPN remote clients.

Syntax

set vpn pptp remote-access client-ip-pool start *ipv4*

delete vpn pptp remote-access client-ip-pool start

show vpn pptp remote-access client-ip-pool start

Command Mode

Configuration mode.

Configuration Statement

```
vpn {
    pptp {
        remote-access {
            client-ip-pool {
                start ipv4
            }
        }
    }
}
```

Parameters

ipv4	Mandatory. The IP address that designates the beginning of the address pool.

Default

None.

Usage Guidelines

Use this command to specify the start of the address pool for remote PPTP VPN clients.

Both the start address and the stop address must be specified. The stop address is specified using the vpn pptp remote-access client-ip-pool stop <ipv4> command.

Use the **set** form of this command to define the start address.

Use the **delete** form of this command to remove the start address.

Use the **show** form of this command to display the start address.

vpn pptp remote-access client-ip-pool stop <ipv4>

Specifies the ending address of a pool of IP addresses for PPTP VPN remote clients.

Syntax

set vpn pptp remote-access client-ip-pool stop *ipv4*

delete vpn pptp remote-access client-ip-pool stop

show vpn pptp remote-access client-ip-pool stop

Command Mode

Configuration mode.

Configuration Statement

```
vpn {
    pptp {
        remote-access {
            client-ip-pool {
                stop ipv4
            }
        }
    }
}
```

Parameters

ipv4	Mandatory. The IP address that designates the end of the address pool.

Default

None.

Usage Guidelines

Use this command to specify the end of the address pool for remote PPTP VPN clients.

Both the start address and the stop address must be specified. The start address is specified using the vpn pptp remote-access client-ip-pool start <ipv4> command. Use the **set** form of this command to define the stop address.

Use the **delete** form of this command to remove the stop address.

Use the **show** form of this command to display the stop address.

vpn pptp remote-access dhcp-interface <interface>

Specifies a DHCP client interface to use for remote access PPTP VPN connections.

Syntax

set vpn pptp remote-access dhcp-interface *interface*

delete vpn pptp remote-access dhcp-interface

show vpn pptp remote-access dhcp-interface

Command Mode

Configuration mode.

Configuration Statement

```
vpn {
    pptp {
        remote-access {
            dhcp-interface interface
        }
    }
}
```

Parameters

interface	The interface to use for remote access PPTP VPN connections (e.g. eth0). Please note that the interface must be configured as a DHCP client.

Default

None.

Usage Guidelines

Use this command to specify a DHCP client interface to use for remote access PPTP VPN connections. Connections will be automatically restarted if the IP address changes.

The DHCP interface is the interface facing the external network. This is the interface to which the PPTP server binds, and only remote connections coming into this interface will be accepted.

NOTE *This option cannot be used if vpn pptp remote-access outside-address <ipv4> is also set.*

Use the **set** form of this command to specify a DHCP interface to use for remote accss PPTP VPN connections.

Use the **delete** form of this command to remove the configuration

Use the **show** form of this command to view the configuration.

vpn pptp remote-access dns-servers server-1 <ipv4>

Specifies the IP address for the primary DNS server for PPTP VPN remote clients.

Syntax

set vpn pptp remote-access dns-servers server-1 *ipv4*

delete vpn pptp remote-access dns-servers server-1

show vpn pptp remote-access dns-servers server-1

Command Mode

Configuration mode.

Configuration Statement

```
vpn {

    pptp {
        remote-access {
            dns-servers {
                server-1 ipv4
            }
        }
    }

}
```

Parameters

ipv4	The IP address of the primary DNS server for remote clients.

Default

None.

Usage Guidelines

Use this command to specify the primary DNS server to be associated with PPTP VPN remote clients.

Use the **set** form of this command to specify the primary DNS server IP address.

Use the **delete** form of this command to remove the primary DNS server IP address.

Use the **show** form of this command to display the primary DNS server IP address.

vpn pptp remote-access dns-servers server-2 <ipv4>

Specifies the IP address for the secondary DNS server for PPTP VPN remote clients.

Syntax

set vpn pptp remote-access dns-servers server-2 *ipv4*

delete vpn pptp remote-access dns-servers server-2

show vpn pptp remote-access dns-servers server-2

Command Mode

Configuration mode.

Configuration Statement

```
vpn {

    pptp {
        remote-access {
            dns-servers {
                server-2 ipv4
            }
        }
    }

}
```

Parameters

ipv4	The IP address of the secondary DNS server for remote clients.

Default

None.

Usage Guidelines

Use this command to specify the secondary DNS server to be associated with remote clients.

Use the **set** form of this command to specify the secondary DNS server IP address.

Use the **delete** form of this command to remove the secondary DNS server IP address.

Use the **show** form of this command to display the secondary DNS server IP address.

vpn pptp remote-access mtu <mtu>

Specifies the MTU for a PPTP connection.

Syntax

set vpn pptp remote-access mtu *mtu*

delete vpn pptp remote-access mtu

show vpn pptp remote-access mtu

Command Mode

Configuration mode.

Configuration Statement

```
vpn {
    pptp {
        remote-access {
            mtu mtu
        }
    }
}
```

Parameters

mtu	Sets the MTU, in octets, for the interface as a whole, including any logical interfaces configured for it. The range is 128 to 16384.

Default

If this value is not set, fragmentation is never performed.

Usage Guidelines

Use this command to set the maximum transmission unit (MTU) for an PPTP connection.

When forwarding, IPv4 packets larger than the MTU will be fragmented unless the DF bit is set. In that case, the packets will be dropped and an ICMP "Packet too big" message is returned to the sender.

Use the **set** form of this command to specify the MTU.

Use the **delete** form of this command to remove MTU value and disable fragmentation.

Use the **show** form of this command to view MTU configuration.

vpn pptp remote-access outside-address <ipv4>

Sets the IP address to be bound to the PPTP server.

Syntax

set vpn pptp remote-access outside-address *ipv4*

delete vpn pptp remote-access

show vpn pptp remote-access

Command Mode

Configuration mode.

Configuration Statement

```
vpn {
    pptp {
        remote-access {
            outside-address ipv4
        }
    }
}
```

Parameters

ipv4	Mandatory. The IPv4 address to which the PPTP server should bind.

Default

None.

Usage Guidelines

Use this command to set the outside address for a remote access PPTP VPN connection.

The outside address is the address of the interface facing the external network. This is the address to which the PPTP server binds, and only remote connections coming into the address will be accepted.

***NOTE** This option cannot be used if vpn pptp remote-access dhcp-interface <interface> is also set.*

Use the **set** form of this command to set the PPTP VPN outside address.

Use the **delete** form of this command to remove the PPTP VPN outside address.

Use the **show** form of this command to display PPTP VPN outside address configuration.

vpn pptp remote-access wins-servers server-1 <ipv4>

Specifies the IP address for the primary WINS server for PPTP VPN remote clients.

Syntax

set vpn pptp remote-access wins-servers server-1 *ipv4*

delete vpn pptp remote-access wins-servers server-1

show vpn pptp remote-access wins-servers server-1

Command Mode

Configuration mode.

Configuration Statement

```
vpn {
    pptp {
        remote-access {
            wins-servers {
                server-1 ipv4
            }
        }
    }
}
```

Parameters

ipv4	The IP address of the primary WINS server for remote clients.

Default

None.

Usage Guidelines

Use this command to specify the primary WINS server to be associated with remote PPTP VPN clients.

The Windows Internet Net Service (WINS) is used to support environments in which users access resources that have NetBIOS names.

Use the **set** form of this command to specify the primary WINS server IP address.

Use the **delete** form of this command to remove the primary WINS server IP address.

Use the **show** form of this command to display the primary WINS server IP address.

vpn pptp remote-access wins-servers server-2 <ipv4>

Specifies the IP address for the secondary WINS server for PPTP VPN remote clients.

Syntax

set vpn pptp remote-access wins-servers server-2 *ipv4*

delete vpn pptp remote-access wins-servers server-2

show vpn pptp remote-access wins-servers server-2

Command Mode

Configuration mode.

Configuration Statement

```
vpn {
    pptp {
        remote-access {
            wins-servers {
                server-2 ipv4
            }
        }
    }
}
```

Parameters

ipv4	The IP address of the secondary WINS server for remote clients.

Default

None.

Usage Guidelines

Use this command to specify the secondary WINS server to be associated with remote PPTP VPN clients.

The Windows Internet Net Service (WINS) is used to support environments in which users access resources that have NetBIOS names.

Use the **set** form of this command to specify the secondary WINS server IP address.

Use the **delete** form of this command to remove the secondary WINS server IP address.

Use the **show** form of this command to display the secondary WINS server IP address.

Chapter 4: OpenVPN

This chapter explains how to set up both site-to-site and remote access OpenVPN virtual private networks on the Vyatta System.

This chapter presents the following topics:

- OpenVPN Configuration
- OpenVPN Commands

OpenVPN Configuration

This section presents the following topics:

- OpenVPN Security Mechanisms
- OpenVPN Modes of Operation
- Configuration Examples for Basic Usage
- Configuration Examples for Advanced Options
- Unsupported OpenVPN Options
- Bridging

NOTE *Committing changes to the OpenVPN configuration will cause the OpenVPN process for the specified OpenVPN interface (e.g. vtun0) to restart. This will result in all existing OpenVPN tunnels on the OpenVPN interface being reset. The exceptions to this are commands under the* ***interfaces openvpn <vtunx> server client*** *configuration node and the* ***interfaces openvpn <vtunx> description*** *command.*

OpenVPN Security Mechanisms

This section provides a high-level overview of the security mechanisms and modes of operation for OpenVPN.

This section presents the following topics:

- Pre-Shared Secret
- TLS

The security requirements for a virtual private network include authentication, confidentiality, and integrity. OpenVPN provides a choice of two different security mechanisms: pre-shared secret and transport layer security (TLS).

NOTE *SSL is the predecessor of TLS, and most references to SSL nowadays are, in fact, references to TLS. Therefore, these terms are used interchangeably in this document.*

Pre-Shared Secret

When pre-shared secret is used for security, OpenVPN works as follows:

1. The administrator uses the Vyatta operational command **generate vpn openvpn-key** to generate a file containing a certain number of random data bytes; that is, the secret to be used to provide security.
2. The administrator transfers the secret file to each of the two tunnel endpoints using pre-established secure channels. For example, the file can be generated on one of the endpoints and then transferred to the other endpoint using a secure file transfer protocol, such as SCP.

3 When the two endpoints want to establish the VPN tunnel, the OpenVPN process on the one endpoint authenticates the other endpoint. Authentication is based on the assumption that the pre-shared secret is known only to the other endpoint; that is, authentication is based on the assumption that if any host knows the shared secret, that host must be the other endpoint.

4 Once the endpoints are authenticated, the OpenVPN process on each side derives a set of keys from the pre-shared secret. These keys are used for two purposes:

— Some are used in an encryption algorithm to encrypt the tunnel data. This provides data confidentiality.

— The others are used in a message authentication code (MAC) that uses a hash algorithm with the keys on the tunnel data. This provides data integrity.

TLS

Transport Layer Security (TLS) is a cryptographic protocol that uses public key cryptography and does not require the two endpoints to have a pre-shared secret. OpenVPN uses TLS with X.509 certificates, and requires public key infrastructure (PKI) to generate the certificates. (For a brief overview of X.509 certificates, please see "Remote VPN Access Using L2TP/IPsec with X.509 Certificates" on page 214.) When TLS is used, OpenVPN works as follows:

1 Using PKI, the adminstrator generates a certificate and the associated files for each endpoint. All certificates are "signed" by the certificate authority (CA) of the PKI. The certificate for an endpoint contains many pieces of information, one of which is the endpoint's name, which is stored in the Common Name field of the certificate.

2 The adminstrator transfers each certificate and the associated files to the corresponding endpoint using a pre-established, secure channel (for example, SCP).

3 When two endpoints want to establish the VPN tunnel, one takes a passive role while the other endpoint must take an active role and initiate the TLS session with the passive endpoint.

4 Once the active endpoint initiates the TLS session, the two sides authenticate one another using their public/private key pairs and the CA's public key, which is known to both endpoints.

5 After the two endpoints have authenticated each other, they establish a shared secret using public key cryptography. Each endpoint then derives a set of keys for the session. As for the pre-shared secret mechanism, these keys are then used for encryption and MAC on the tunnel data to provide data confidentiality and integrity. However, unlike the pre-shared secret mechanism, these keys are only used for the one session, and for this reason they are called "session keys."

Certificate generation and distribution using PKI involves numerous complex security issues, which are outside the scope of this document.

OpenVPN Modes of Operation

OpenVPN supports both site-to-site and remote access operation. In addition, client-side remote access support is available for accessing configuration information from an OpenVPN Access Server.

NOTE *If client-side access to an OpenVPN Access Server is configured, all openvpn configuration parameters other than those used to connect to the OpenVPN Access Server (i.e. those within **interfaces openvpn <vtunx> remote-configuration**) will be ignored.*

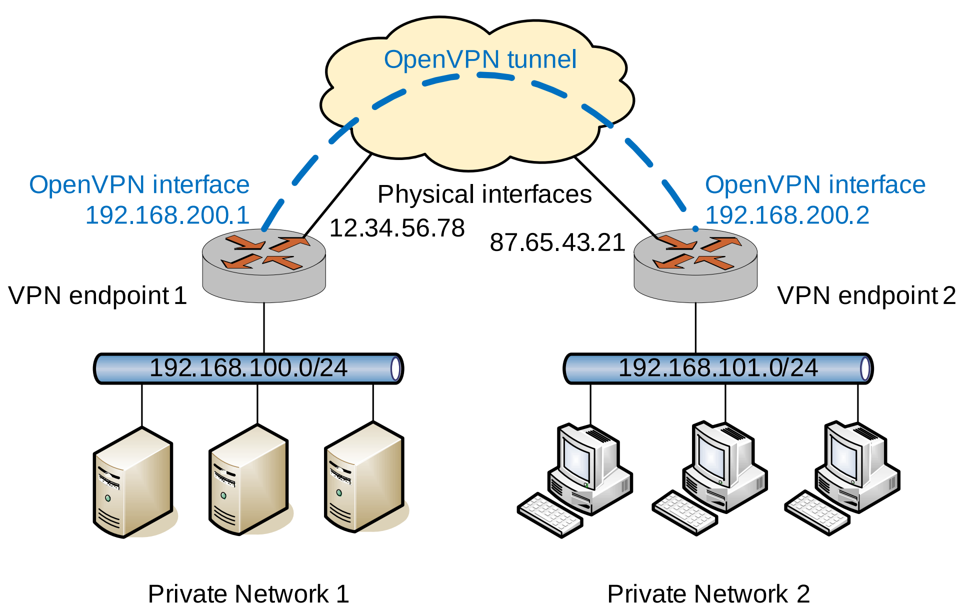
This section presents more details about these modes of operation, in the following topics:

- Site-to-Site Operation
- Remote Access Operation
- Client-Side Access to an OpenVPN Access Server

Site-to-Site Operation

Figure 4-1 illustrates a simple site-to-site VPN scenario. This scenario could represent, for example, a connection between a branch office and a data center.

Figure 4-1 Site-to-site operation



At each of the two VPN tunnel endpoints, the OpenVPN process creates a routable "tunnel interface" and establishes a secure tunnel with the other endpoint. Subsequently, the two interfaces appear to be on the same network, although packets flowing between these two interfaces are actually processed and sent through the secure tunnel by the OpenVPN process.

Note that there are two relevant IP addresses on each endpoint:

- The tunnel IP address: This address is the virtual IP address (VIP) on each end of the tunnel. The tunnel IP addresses at each end of the tunnel must be on the same subnet. In the example in Figure 4-1, the tunnel IP addresses of the two endpoints are 192.168.200.1 and 192.168.200.2.
- The physical IP address: This is the IP address configured for the physical network interface over which the VPN tunnel is established. In the example above, the physical IP addresses of the two endpoints are 12.34.56.78 and 87.65.43.21.

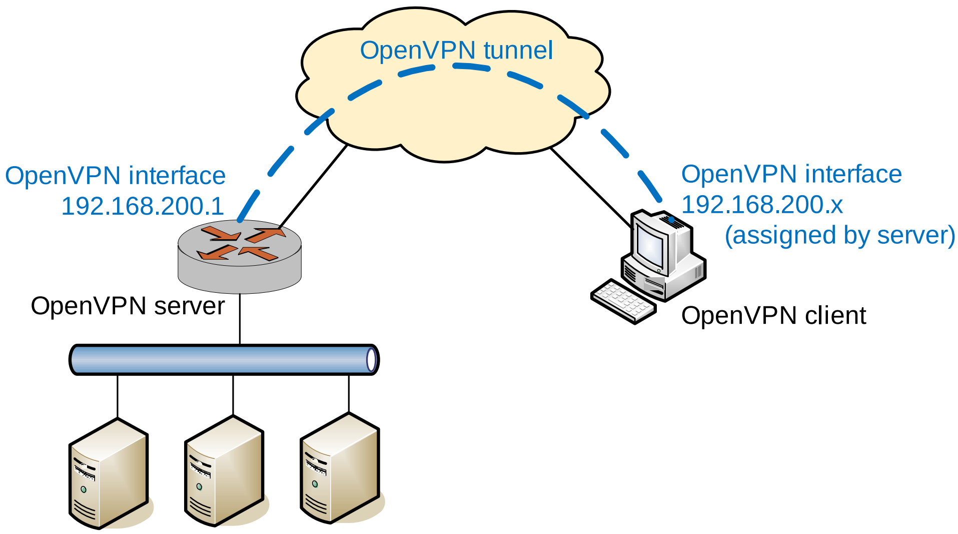
In most scenarios, the VPN tunnel is used to transport traffic from different private subnets across the wide area network (WAN). In the example above, the private subnets 192.168.100.0/24 and 192.168.101.0/24 are each "behind" a VPN tunnel endpoint. Therefore, on each endpoint, you must add a static route that directs traffic to and from the remote private subnet through the tunnel interface.

In site-to-site mode, a single host can establish multiple OpenVPN tunnels, each of which may be to distinct sites. Even if all tunnels originate from a single physical interface, each tunnel is represented by a different tunnel interface IP address and operates independently.

Remote Access Operation

OpenVPN also supports remote access VPN using a client-server mode. In this mode, one OpenVPN endpoint acts as the server and all remote endpoints operate as clients, which connect to the OpenVPN server to establish VPN tunnels, so that each client establishes has an independent tunnel to the server. A simple remote access VPN setup is shown in Figure 4-2.

Figure 4-2 Remote access operation



One major difference between site-to-site mode and client-server mode is that in client-server mode, all the VPN tunnels on the server side terminate at a single tunnel interface. Having a single termination point eliminates the need to set up separate tunnel interface IP addresses for each VPN tunnel. This is more convenient and operationally simpler for a remote access setup.

Another difference is that in client-server mode, the server-side OpenVPN process dynamically allocates all tunnel IP addresses from a configured subnet (192.168.200.0/24 in the example) instead of using fixed tunnel IP addresses for tunnel endpoints. Thus, when the OpenVPN process is started on the server, it creates the tunnel interface and assigns it an IP address from the subnet to the interface (for example, 192.168.200.1). Then, when a client establishes a VPN tunnel with the server, the server-side OpenVPN process also allocates the client an IP address from the same subnet (for example, 192.168.200.4) and the tunnel interface on the client adopts this address.

Client-Side Access to an OpenVPN Access Server

This feature is available only in the Vyatta Subscription Edition.

OpenVPN Access Server is a server that authenticates remote client access requests (either locally or via an authentication server) and provides OpenVPN tunnel configuration information to the requesting client. It can also provide OpenVPN client software if the client requires it, though this is not required for Vyatta clients. The configuration information allows the client to then establish an OpenVPN tunnel with an OpenVPN server with minimal configuration on the client side.

The sequence of events is as follows:

1 An administrator configures an OpenVPN Access Server for Vyatta client access and, potentially, configures a separate authentication server and OpenVPN server. The Vyatta client only requires configuration information from the server. It does not require client software.

NOTE *It is possible for the OpenVPN Access Server to act as the access server, the authentication server, and the OpenVPN server.*

NOTE *The OpenVPN Access Server product is not available from Vyatta. It is available from OpenVPN at* http://openvpn.net.

2 The Vyatta client accesses the OpenVPN Access Server and provides a username and password.

3 The OpenVPN Access Server authenticates the user, either acting as its own authentication server or using an external authentication server such as a RADIUS server.

4 After authentication, the OpenVPN Access Server sends the Vyatta client device the configuration information necessary to establish an OpenVPN tunnel with an OpenVPN server.

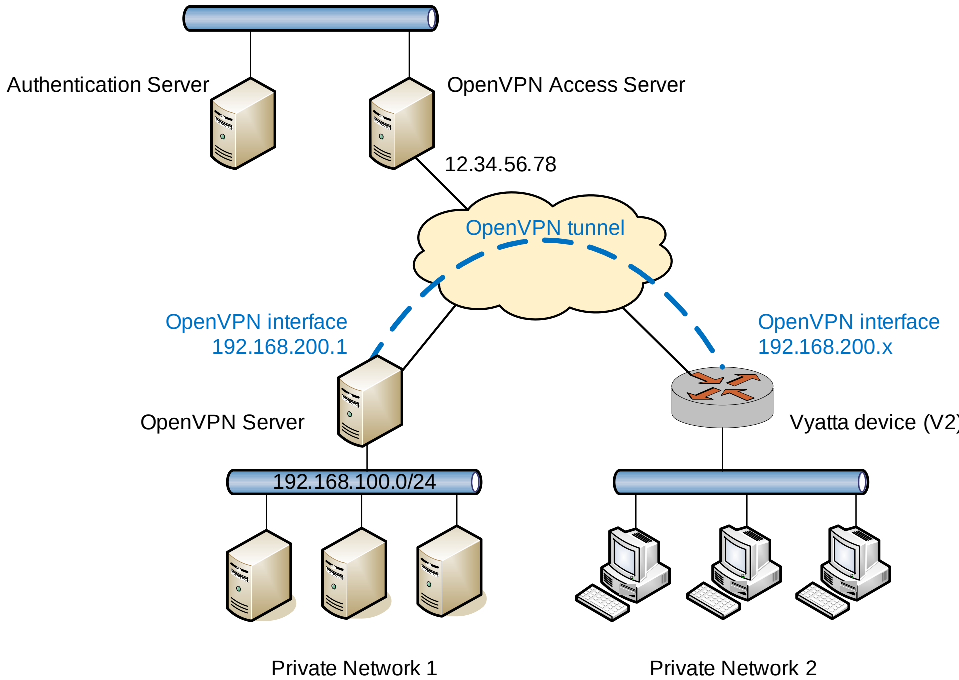
5 The Vyatta client then establishes an OpenVPN tunnel with the OpenVPN server specified in the downloaded configuration and is provided an IP address on the OpenVPN tunnel subnet.

NOTE *If the OpenVPN server is configured such that Autologin is enabled then a* ***tunnel-username*** *and* ***tunnel-password*** *are not required, otherwise they are required to establish the VPN tunnel.*

The Vyatta system has the OpenVPN client software preloaded and can use the OpenVPN Access Server to obtain the information necessary to establish an OpenVPN tunnel with an OpenVPN server. The only required configuration information is the OpenVPN Access Server's IP address or hostname, a username and password for the OpenVPN Access Server, and, potentially, the tunnel-username and tunnel-password for establishing the tunnel with the OpenVPN server.

An OpenVPN setup using an OpenVPN Access Server, an authentication server, and OpenVPN server is shown in Figure 4-3.

Figure 4-3 Client-side access to an OpenVPN Access Server



You can use the operational command **show interfaces** to show the assigned IP address on the client side of the OpenVPN tunnel.

Configuration Examples for Basic Usage

This section describes several basic scenarios of OpenVPN usage and explains how to configure them. This section presents the following topics:

- Site-to-Site Mode with Pre-Shared Secret
- Site-to-Site Mode with TLS
- Client-Server Mode
- Setting Up OpenVPN Clients on Windows Hosts
- Firewall Configuration
- Using an OpenVPN Access Server

Site-to-Site Mode with Pre-Shared Secret

Figure 4-4 shows the site-to-site scenario configured with pre-shared secret.

In this example:

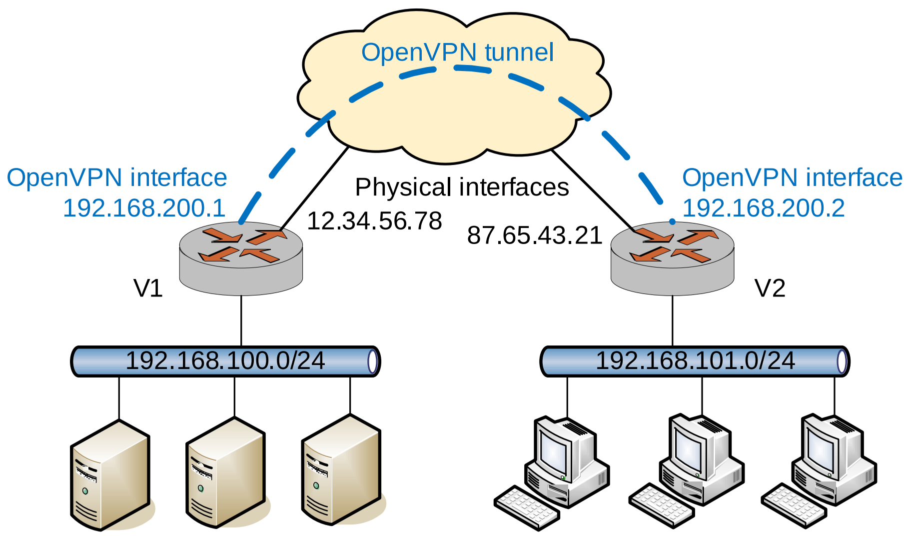
- The physical IP addresses for V1 and V2 are 12.34.56.78 and 87.65.43.21, respectively.

- The tunnel IP addresses for V1 and V2 are 192.168.200.1 and 192.168.200.2, respectively.
- The subnet to be accessed from V1 (via V2 over the VPN) is 192.168.100.0/24.
- The subnet we want to access on V2 (via V1over the VPN) is 192.168.101.0/24.

To configure an OpenVPN tunnel, you create an interface of type **openvpn**.The interface name is in the form of **vtun***num*; for example, **vtun0**, **vtun1**, and so on.

In addition, you must add a static interface route to direct traffic for the remote subnet through the tunnel interface **vtun0**. (For information on setting up static routes, see the *Vyatta Basic Routing Reference Guide*.)

Figure 4-4 Site-to-site VPN with pre-shared secret



This section presents the following examples:

- Example 4-1 Site-to-site OpenVPN with pre-shared secret: V1 endpoint
- Example 4-2 Site-to-site OpenVPN with pre-shared secret: V1 static route
- Example 4-3 Site-to-site OpenVPN with pre-shared secret: V2 endpoint
- Example 4-4 Site-to-site OpenVPN with pre-shared secret: V2 static route

To configure the V1 endpoint, perform the following steps in configuration mode.

Example 4-1 Site-to-site OpenVPN with pre-shared secret: V1 endpoint

Step	Command
Create the vtun0 configuration node.	`vyatta@V1# set interfaces openvpn vtun0`

Example 4-1 Site-to-site OpenVPN with pre-shared secret: V1 endpoint

Set the tunnel IP address for the local endpoint.	`vyatta@V1#` **`set interfaces openvpn vtun0 local-address 192.168.200.1`**
Set the OpenVPN mode to "site-to-site".	`vyatta@V1#` **`set interfaces openvpn vtun0 mode site-to-site`**
Set the tunnel IP address of the remote endpoint.	`vyatta@V1#` **`set interfaces openvpn vtun0 remote-address 192.168.200.2`**
Specify the physical IP address of the remote host.	`vyatta@V1#` **`set interfaces openvpn vtun0 remote-host 87.65.43.21`**
Specify the location of the file containing the pre-shared secret.	`vyatta@V1#` **`set interfaces openvpn vtun0 shared-secret-key-file /config/auth/secret`**
Commit the change.	`vyatta@V1# commit`

Show the OpenVPN configuration.	`vyatta@V1#` **`show interfaces openvpn vtun0`**
	` local-address 192.168.200.1`
	` mode site-to-site`
	` remote-address 192.168.200.2`
	` remote-host 87.65.43.21`
	` shared-secret-key-file /config/auth/secret`

To configure a static route to access the remote subnet via the OpenVPN tunnel, perform the following steps in configuration mode.

Example 4-2 Site-to-site OpenVPN with pre-shared secret: V1 static route

Step	Command
Create the static route to access the remote subnet via the OpenVPN tunnel.	`vyatta@V1#` **`set protocols static interface-route 192.168.101.0/24 next-hop-interface vtun0`**
Commit the change.	`vyatta@V1# commit`

Show the static routing configuration.	`vyatta@V1#` **`show protocols static`**
	` interface-route 192.168.101.0/24 {`
	`   next-hop-interface vtun0 {`
	`   }`
	` }`

The VPN endpoint V2 is identically to endpoint V1, except that local and remote tunnel IP addresses are reversed. To configure the V2 endpoint, perform the following steps in configuration mode.

Example 4-3 Site-to-site OpenVPN with pre-shared secret: V2 endpoint

Step	Command
Create the vtun0 configuration node.	vyatta@V2# **set interfaces openvpn vtun0**
Set the tunnel IP address for the local endpoint.	vyatta@V2# **set interfaces openvpn vtun0 local-address 192.168.200.2**
Set the OpenVPN mode to "site-to-site".	vyatta@V2# **set interfaces openvpn vtun0 mode site-to-site**
Set the tunnel IP address of the remote endpoint.	vyatta@V2# **set interfaces openvpn vtun0 remote-address 192.168.200.1**
Specify the physical IP address of the remote host.	vyatta@V2# **set interfaces openvpn vtun0 remote-host 12.34.56.78**
Specify the location of the file containing the pre-shared secret.	vyatta@V2# **set interfaces openvpn vtun0 shared-secret-key-file /config/auth/secret**
Commit the change.	vyatta@V2# commit
Show the OpenVPN configuration.	vyatta@V2# **show interfaces openvpn vtun0** local-address 192.168.200.2 mode site-to-site remote-address 192.168.200.1 remote-host 12.34.56.78 shared-secret-key-file /config/auth/secret

Again, the shared secret file (created using generate vpn openvpn-key <filename> on one system and copied to the other) must be the same on both endpoints (the path need not be the same, but the content must be). Note also that the **remote-host** option is only required on one of the endpoints; that is, the site-to-site tunnel can be established as long as even one endpoint has enough information to contact the other.

To configure a static route to access the remote subnet via the OpenVPN tunnel, perform the following steps in configuration mode.

Example 4-4 Site-to-site OpenVPN with pre-shared secret: V2 static route

Step	Command
Create the static route to access the remote subnet via the OpenVPN tunnel.	vyatta@V2# **set protocols static interface-route 192.168.100.0/24 next-hop-interface vtun0**

Example 4-4 Site-to-site OpenVPN with pre-shared secret: V2 static route

Commit the change.	`vyatta@V2# commit`

Show the static routing configuration.	`vyatta@V2# show protocols static`
	` interface-route 192.168.100.0/24 {`
	`    next-hop-interface vtun0 {`
	`    }`
	` }`

Site-to-Site Mode with TLS

When TLS is used in site-to-site mode, the Vyatta configuration is the same as the previous section, except that you must configure TLS-related options instead of the **shared-secret-key-file** option. As discussed above, one endpoint takes the passive role and the other takes the active role.

Each endpoint must also have the following files, which are required for the TLS protocol.

- **CA certificate file**: This file contains the certificate authority's certificate, which will be used to validate the other endpoint's certificate.
- **Host certificate file**: This file contains the endpoint's own certificate, which will be presented to the other endpoint during the TLS negotiation.
- **Host key file:** This file contains the endpoint's own private key, which is kept secret from anybody else.
- **Certificate revocation list (CRL) file**: (Optional) This file contains a list of certificates that have been revoked, which will prevent endpoints with these certificates from establishing a VPN tunnel.
- **DH parameters file**: (Only needed by the passive endpoint) This file contains Diffie Hellman parameters that are required only by the endpoint taking the passive role in the TLS negotiation.

More information about these files is available in the OpenVPN documentation.

The configuration that follows corresponds to the configuration for the example in the previous section. Assumed that the necessary files have been generated and distributed to each endpoint and that V1 and V2 are passive and active, respectively.

To configure V1 for a site-to-site VPN with TLS, perform the following steps in configuration mode.

Example 4-5 V1 OpenVPN configuration - site-to-site with TLS

Step	Command
Create the vtun0 configuration node.	vyatta@V1# **set interfaces openvpn vtun0**
Set the local IP address of the VPN tunnel.	vyatta@V1# **set interfaces openvpn vtun0 local-address 192.168.200.1**
Set the OpenVPN mode.	vyatta@V1# **set interfaces openvpn vtun0 mode site-to-site**
Set the remote IP address of the VPN tunnel.	vyatta@V1# **set interfaces openvpn vtun0 remote-address 192.168.200.2**
Specify the physical IP address of the remote host.	vyatta@V1# **set interfaces openvpn vtun0 remote-host 87.65.43.21**
Set the role of this endpoint.	vyatta@V1# **set interfaces openvpn vtun0 tls role passive**
Specify the location of the CA certificate file.	vyatta@V1# **set interfaces openvpn vtun0 tls ca-cert-file /config/auth/ca.crt**
Specify the location of the host certificate file.	vyatta@V1# **set interfaces openvpn vtun0 tls cert-file /config/auth/V1.crt**
Specify the location of the CRL parameters file.	vyatta@V1# **set interfaces openvpn vtun0 tls crl-file /config/auth/crl.pem**
Specify the location of the DH file.	vyatta@V1# **set interfaces openvpn vtun0 tls dh-file /config/auth/dh1024.pem**
Specify the location of the host key file.	vyatta@V1# **set interfaces openvpn vtun0 tls key-file /config/auth/V1.key**
Commit the change.	vyatta@V1# commit

Show the OpenVPN configuration.	vyatta@V1# **show interfaces openvpn vtun0**
	local-address 192.168.200.1
	mode site-to-site
	remote-address 192.168.200.2
	remote-host 87.65.43.21
	tls {
	role passive
	ca-cert-file /config/auth/ca.crt
	cert-file /config/auth/V1.crt
	crl-file /config/auth/cr1.pem
	dh-file /config/auth/dh1024.pem
	key-file /config/auth/V1.key
	}

Note that the configuration is the same as the previous section except that the **shared-secret-key-file** option has been replaced by **tls** options. That endpoint V1 takes the passive role means the **dh-file** option is required. The optional **crl-file** is also specified in this example.

To configure V2 for a site-to-site VPN with TLS, perform the following steps in configuration mode.

Example 4-6 V2 OpenVPN configuration - site-to-site with TLS

Step	Command
Create the vtun0 configuration node.	`vyatta@V2# set interfaces openvpn vtun0`
Set the local IP address of the VPN tunnel.	vyatta@V2# **set interfaces openvpn vtun0 local-address 192.168.200.2**
Set the OpenVPN mode.	vyatta@V2# **set interfaces openvpn vtun0 mode site-to-site**
Set the remote IP address of the VPN tunnel.	vyatta@V2# **set interfaces openvpn vtun0 remote-address 192.168.200.1**
Specify the physical IP address of the remote host.	vyatta@V2# **set interfaces openvpn vtun0 remote-host 12.34.56.78**
Set the role of this endpoint.	vyatta@V2# **set interfaces openvpn vtun0 tls role active**
Specify the location of the CA certificate file.	vyatta@V2# **set interfaces openvpn vtun0 tls ca-cert-file /config/auth/ca.crt**
Specify the location of the host certificate file.	vyatta@V2# **set interfaces openvpn vtun0 tls cert-file /config/auth/V2.crt**
Specify the location of the host key file.	vyatta@V2# **set interfaces openvpn vtun0 tls key-file /config/auth/V2.key**
Commit the change.	`vyatta@V2# commit`

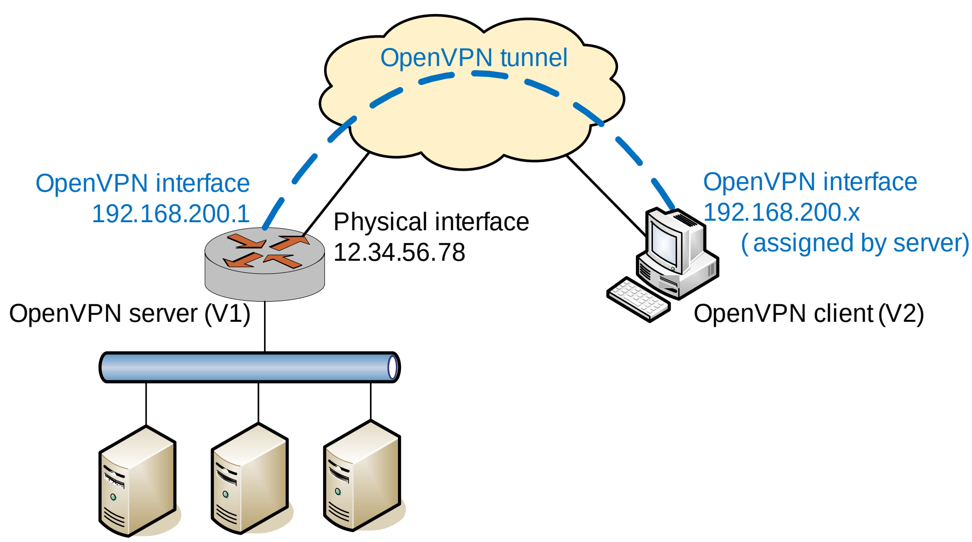
Show the OpenVPN configuration.	vyatta@V2# **show interfaces openvpn vtun0**
	`local-address 192.168.200.2`
	`mode site-to-site`
	`remote-address 192.168.200.1`
	`remote-host 12.34.56.78`
	`tls {`
	`  role active`
	`  ca-cert-file /config/auth/ca.crt`
	`  cert-file /config/auth/V2.crt`
	`  key-file /config/auth/V2.key`
	`}`

The configuration is the same as in the previous example, except for that the **tls** option is specified, the optional **crl-file** option is not specified, and the fact that endpoint V2 takes the active role means **dh-file** is not needed.

Client-Server Mode

In a typical remote access VPN setup there is one OpenVPN endpoint that acts as the server. Remote users will run OpenVPN as clients to connect to the server and establish VPN tunnels. This is illustrated in Figure 4-5.

Figure 4-5 Client-server mode



One thing to note is that OpenVPN requires TLS in client-server mode, and the server takes the passive role while the clients are active. Therefore, it is not necessary to specify the **tls role** option when operating in this mode. In the above example, assuming that V1 is the server and V2 is a client, the configuration for V1 is shown below.

To configure V1 for client-server with TLS, perform the following steps in configuration mode. In this example:

- The **mode** option specifies that this endpoint will operate in server mode.
- The **server subnet** option indicates that the client's tunnel IP address is allocated from the 192.168.200.0/24 subnet and that the server's tunnel IP address (that is, the address of **vtun0** on the server) is 192.168.200.1.
- The **remote-host** option is not set since the clients will be actively contacting the server.

Example 4-7 V1 OpenVPN configuration - client-server with TLS (server)

<table>
<tr><th>Step</th><th>Command</th></tr>
<tr><td>Create the vtun0 configuration node.</td><td><code>vyatta@V1# set interfaces openvpn vtun0</code></td></tr>
<tr><td>Set the OpenVPN mode.</td><td><code>vyatta@V1# set interfaces openvpn vtun0 mode server</code></td></tr>
<tr><td>Set the subnet for the OpenVPN tunnel.</td><td><code>vyatta@V1# set interfaces openvpn vtun0 server subnet 192.168.200.0/24</code></td></tr>
<tr><td>Specify the location of the CA certificate file.</td><td><code>vyatta@V1# set interfaces openvpn vtun0 tls ca-cert-file /config/auth/ca.crt</code></td></tr>
<tr><td>Specify the location of the host certificate file.</td><td><code>vyatta@V1# set interfaces openvpn vtun0 tls cert-file /config/auth/V1.crt</code></td></tr>
<tr><td>Specify the location of the CRL parameters file.</td><td><code>vyatta@V1# set interfaces openvpn vtun0 tls crl-file /config/auth/crl.pem</code></td></tr>
<tr><td>Specify the location of the DH file.</td><td><code>vyatta@V1# set interfaces openvpn vtun0 tls dh-file /config/auth/dh1024.pem</code></td></tr>
<tr><td>Specify the location of the host key file.</td><td><code>vyatta@V1# set interfaces openvpn vtun0 tls key-file /config/auth/V1.key</code></td></tr>
<tr><td>Commit the change.</td><td><code>vyatta@V1# commit</code></td></tr>
<tr><td>Show the OpenVPN configuration.</td><td><pre>vyatta@V1# show interfaces openvpn vtun0
 mode server
 server {
   subnet 192.168.200.0/24
 }
 tls {
   ca-cert-file /config/auth/ca.crt
   cert-file /config/auth/V1.crt
   crl-file /config/auth/cr1.pem
   dh-file /config/auth/dh1024.pem
   key-file /config/auth/V1.key
 }</pre></td></tr>
</table>

To configure V2 for client-server with TLS, perform the following steps in configuration mode. In this example:

- V2 is in client mode and so it needs to actively contact the server; therefore the **remote-host** option is needed to indicate where the server is.
- When the tunnel is established, V2's tunnel IP address (that is, the address of **vtun0** on V2) will be assigned by V1 from the 192.168.200.0/24 subnet.

Example 4-8 V2 OpenVPN configuration - client-server with TLS (client)

Step	Command
Create the vtun0 configuration node.	`vyatta@V2# set interfaces openvpn vtun0`
Set the OpenVPN mode.	vyatta@V2# **set interfaces openvpn vtun0 mode client**
Specify the physical IP address of the remote host.	vyatta@V2# **set interfaces openvpn vtun0 remote-host 12.34.56.78**
Specify the location of the CA certificate file.	vyatta@V2# **set interfaces openvpn vtun0 tls ca-cert-file /config/auth/ca.crt**
Specify the location of the host certificate file.	vyatta@V2# **set interfaces openvpn vtun0 tls cert-file /config/auth/V2.crt**
Specify the location of the host key file.	vyatta@V2# **set interfaces openvpn vtun0 tls key-file /config/auth/V2.key**
Commit the change.	`vyatta@V2# commit`

Show the OpenVPN configuration.	vyatta@V2# **show interfaces openvpn vtun0**
	mode client
	remote-host 12.34.56.78
	tls {
	ca-cert-file /config/auth/ca.crt
	cert-file /config/auth/V2.crt
	key-file /config/auth/V2.key
	}

Setting Up OpenVPN Clients on Windows Hosts

As mentioned earlier, OpenVPN is different from and cannot interoperate with the “SSL VPN” solutions on the market, and therefore OpenVPN must be installed on all VPN hosts. In a remote access VPN setup, many remote users will need to connect to the OpenVPN server from hosts that run Windows. To set up the OpenVPN client on a Windows machine, download and install the OpenVPN Windows Installer package from the OpenVPN Web site (http://openvpn.net/index.php/downloads.html).

After installation, the OpenVPN client can be either run from the Windows command line or controlled by the OpenVPN GUI. Using the setup from the previous section as example, if the client V2 is a Windows host, the OpenVPN client can be run from the command line by issuing the command shown in Example 4-9, using the addressing, certificate, and key information for your site.

Example 4-9 Running OpenVPN from the command line

```
openvpn --dev tun --client --remote ip-address --ca ca-cert-filename
--cert endpoint-cert-filename --key endpoint-key-filename
```

This command establishes a VPN tunnel with the OpenVPN server V1 in Example 4-8. Note that the referenced files must be in the same directory from which this command is issued. Otherwise, full paths should be used for the files.

Alternatively, to control the OpenVPN client using the OpenVPN GUI,you must create a control file. The file must be named with extension **.ovpn**; for example, **vyatta.ovpn**. A configuration file that corresponds to the preceding command line contains would look as shown in Example 4-10 (with corresponding changes for your site information).

Example 4-10 OpenVPN configuration file

```
dev tun
client
remote 12.34.56.78
ca ca.crt
cert V2.crt
key V2.key
```

Put the configuration file and the referenced files (certificates, etc.) into the OpenVPN configuration directory. This is usually **C:\Program files\OpenVPN\config**.

Start the OpenVPN GUI, which will show an icon in the notification area of the Windows taskbar. To establish the OpenVPN tunnel, right-click the icon and select **Connect** from the drop-down menu. If there are multiple **ovpn** configuration files, the actions for each configuration appear in each file's own drop-down menu.

Firewall Configuration

The firewall configuration for an OpenVPN tunnel interface is the same as the configuration for other types of interfaces. Here is an example.

To configure firewall on V1, perform the following steps in configuration mode.

Example 4-11 V1 OpenVPN firewall configuration

Step	Command
Create the vtun0 configuration node.	vyatta@V1# **set interfaces openvpn vtun0**
Additional configuration commands.	...
Set the firewall rule for inbound traffic on the vtun0 interface.	vyatta@V1# **set interfaces openvpn vtun0 firewall in name rules-in**
Additional configuration commands.	...
Commit the change.	vyatta@V1# commit

Show the OpenVPN configuration.	vyatta@V1# **show interfaces openvpn vtun0**
	 ...
	 firewall {
	    in {
	        name rules-in
	    }
	 }
	 ...

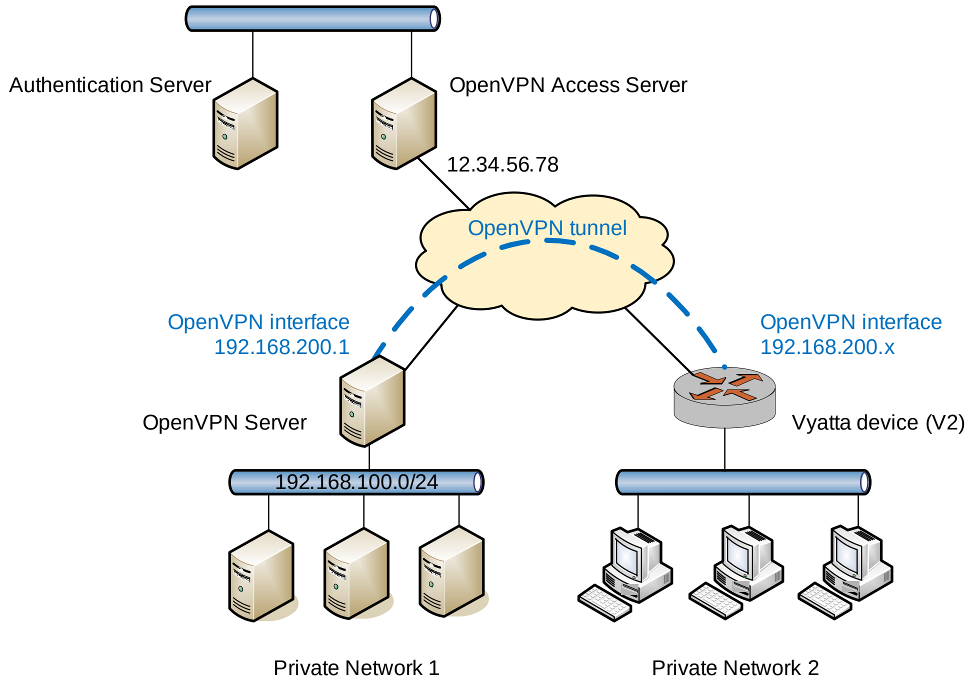
For more information on configuring firewall for interfaces, see the firewall chapter in the *Vyatta Firewall Reference Guide*.

Using an OpenVPN Access Server

This feature is available only in the Vyatta Subscription Edition.

Another OpenVPN scenario involves connecting to an OpenVPN Access Server and using the configuration information it provides to establish an OpenVPN tunnel to an OpenVPN server. The configuration for this is very simple, as the OpenVPN Access Server provides all the necessary VPN configuration information to the connecting host (the Vyatta system in this case) . A configuration scenario using an OpenVPN Access Server is shown in Figure 4-6.

Figure 4-6 Using an OpenVPN Access Server to establish an OpenVPN tunnel



To configure V2 to establish an OpenVPN tunnel to an OpenVPN server using an OpenVPN Access Server as shown in Figure 4-6, perform the following steps in configuration mode.

Example 4-12 V2 - Client-Side Connection to OpenVPN Access Server (Autologin enabled)

Step	**Command**
Create the vtun0 configuration node.	`vyatta@V2# **set interfaces openvpn vtun0**`
Specify the OpenVPN Access Server IP address.	`vyatta@V2# **set interfaces openvpn vtun0 remote-configuration server 12.34.56.78**`
Specify the user name to be authenticated at the OpenVPN Access Server.	`vyatta@V2# **set interfaces openvpn vtun0 remote-configuration username abcd**`
Specify the password to be authenticated at the OpenVPN Access Server.	`vyatta@V2# **set interfaces openvpn vtun0 remote-configuration password efgh**`
Commit the change.	`vyatta@V2# **commit**`

Example 4-12 V2 - Client-Side Connection to OpenVPN Access Server (Autologin enabled)

Show the configuration.	`vyatta@V2# show interfaces openvpn vtun0`
	` remote-configuration {`
	`   password efgh`
	`   server 12.34.56.78`
	`   username abcd`
	` }`

This example is valid for a scenario where Autologin is enabled on the OpenVPN server for tunnel establishment. If Autologin is disabled, the interfaces openvpn <vtunx> remote-configuration tunnel-username <username> and interfaces openvpn <vtunx> remote-configuration tunnel-password <password> commands must also be used to establish the tunnel.

To configure V2 to establish an OpenVPN tunnel to an OpenVPN server (with Autologin disabled) using an OpenVPN Access Server as shown in Figure 4-6, perform the following steps in configuration mode.

Example 4-13 V2 - Client-Side Connection to OpenVPN Access Server (Autologin disabled)

Step	Command
Create the vtun0 configuration node.	`vyatta@V2# set interfaces openvpn vtun0`
Specify the OpenVPN Access Server IP address.	`vyatta@V2# set interfaces openvpn vtun0 remote-configuration server 12.34.56.78`
Specify the user name to be authenticated at the OpenVPN Access Server.	`vyatta@V2# set interfaces openvpn vtun0 remote-configuration username abcd`
Specify the password to be authenticated at the OpenVPN Access Server.	`vyatta@V2# set interfaces openvpn vtun0 remote-configuration password efgh`
Specify the user name required to establish the tunnel with the OpenVPN server.	`vyatta@V2# set interfaces openvpn vtun0 remote-configuration tunnel-username tun-un3`
Specify the password required to establish the tunnel with the OpenVPN server.	`vyatta@V2# set interfaces openvpn vtun0 remote-configuration tunnel-password tun-pwdxyz`
Commit the change.	`vyatta@V2# commit`

Example 4-13 V2 - Client-Side Connection to OpenVPN Access Server (Autologin disabled)

Show the configuration.	`vyatta@V2#` **`show interfaces openvpn vtun0`**
	`remote-configuation {`
	`password efgh`
	`server 12.34.56.78`
	`tunnel-password tun-un3`
	`tunnel-username tun-pwdxyz`
	`username abcd`
	`}`

Configuration Examples for Advanced Options

The previous section presented some basic OpenVPN scenarios and provided configuration steps for the Vyatta system. This section presents a number of more advanced concepts and configuration options that may be useful to administrators of more complex environments.

This section presents the following topics:

- Transport Protocol (Site-to-Site, Client, Server)
- Cryptographic Algorithms (Site-to-Site, Client, Server)
- Split Tunnelling (Site-to-Site, Client, Server)
- Broadcast Network (Site-to-Site, Client, Server)
- Multiple Remote Endpoints (Client Only)
- Client-Server Topology (Server Only)
- Client-Specific Settings (Server Only)

Transport Protocol (Site-to-Site, Client, Server)

By default, OpenVPN uses UDP as the underlying transport protocol. Since UDP is connectionless, either side can initiate the VPN tunnel by sending packets to UDP port 1194 (default) on the other endpoint. Alternatively, OpenVPN can also use TCP as the transport. However, if TCP is used, one endpoint must take a *passive* role (that is, it listens to incoming TCP connections), and the other endpoint must take an *active* role (that is, it initiates the TCP connection to the TCP port on the passive endpoint).

Each protocol has different advantages in this context. For example, using TCP is much less prone to firewall or NAT problems in networks between the two endpoints. However, when packet losses occur, the TCP retransmissions at the tunnel level may interfere with retransmissions done by the individual TCP flows inside the VPN tunnel; therefore, using UDP can result in better performance.

The related configuration options are shown in Example 4-14 and are described following the example.

Example 4-14 Configuration options related to protocol type

```
interfaces {
    openvpn <if_name> {
        protocol <protocol>
        local-host <local_host_ip>
        local-port <local_port>
        remote-port <remote_port>
    }
}
```

- **protocol**: Valid values for this option are **udp**, **tcp-active**, and **tcp-passive**. If **protocol** is not specified or if it is specified as **udp**, then UDP is used. On the other hand, if TCP is used, note the following requirements:
  - — As discussed above, when TCP is used, one endpoint must be active and the other one passive.
  - — On the **tcp-active** endpoint, the **remote-host** option must be set so that it can initiate the TCP connection.
  - — On the **tcp-passive** endpoint, if the **remote-host** option is set, then only the specified host can initiate the TCP connection to this endpoint.
  - — If TCP is used in client-server mode, naturally the client must be **tcp-active** and the server must be **tcp-passive**.
  - — When TCP is used in combination with TLS, the active/passive roles for TCP and TLS should match. In other words, the **tcp-active** endpoint should also be active for TLS (similarly for "passive"). (Note that this is not an OpenVPN restriction, but it is enforced to avoid confusion.)
- **local-host**: This value can be an IP address on any of network interfaces on this endpoint. If **local-host** is set, the OpenVPN process will only accept sessions coming in on the particular IP address. This applies to both UDP and TCP. If **local-host** is not set, OpenVPN accepts incoming sessions on any interfaces. This option can be used for any of the following:
  - — The server endpoint in client-server mode
  - — Either endpoint when UDP is used in site-to-site mode
  - — The **tcp-passive** endpoint when TCP is used in site-to-site mode
- **local-port:** This value specifies the UDP or TCP port number on which OpenVPN will accept incoming sessions. If not set, OpenVPN accepts incoming sessions on the default port 1194. This option can be used for any of the following:

— The server endpoint in client-server mode

— Either endpoint when UDP is used in site-to-site mode

— The **tcp-passive** endpoint when TCP is used in site-to-site mode

- **remote-port**: This option specifies the UDP or TCP port number on the other endpoint to which OpenVPN will initiate sessions. In other words, the other endpoint is accepting sessions on this port. If not set, OpenVPN will initiate the session to the default port 1194 on the remote endpoint. Note that, if set, the **remote-port** setting on one endpoint must match the **local-port** setting on the other, and vice versa. This option can be used for any of the following:

— The client endpoint in client-server mode

— Either endpoint when UDP is used in site-to-site mode

— The **tcp-active** endpoint when TCP is used in site-to-site mode

Cryptographic Algorithms (Site-to-Site, Client, Server)

As discussed earlier, whichever security mechanism is used (pre-shared secret or TLS), after the VPN tunnel is established, the two endpoints will apply an encryption algorithm and a hash algorithm on the tunneled VPN data to provide confidentiality and integrity. By default, the encryption and hash algorithms used by OpenVPN are Blowfish (with 128-bit keys) and SHA-1, respectively. This configuration should be reasonable in typical environments: the Blowfish algorithm performs well in software and has no known weakness, and SHA-1 is widely used and is part of the NIST Secure Hash Standard.

When a particular encryption or hash algorithm is required in an environment, the two configuration options shown in Example 4-15 can be used to specify the algorithm.

Example 4-15 Configuration options related to security

```
interfaces {
    openvpn <if_name> {
        encryption <algorithm>
        hash <algorithm>
    }
}
```

- **encryption**: This option specifies the encryption algorithm to use, and the following values are allowed.

— **des**: DES algorithm

- — **3des**: DES algorithm with triple encryption
- — **bf128**: Blowfish algorithm with 128-bit key
- — **bf256**: Blowfish algorithm with 256-bit key
- — **aes128**: AES algorithm with 128-bit key
- — **aes192**: AES algorithm with 192-bit key
- — **aes256**: AES algorithm with 256-bit key

- **hash**: This option specifies the hash algorithm to use, and the following values are allowed.
  - — **md5**: MD5 algorithm
  - — **sha1**: SHA-1 algorithm
  - — **sha256**: SHA-256 algorithm
  - — **sha512**: SHA-512 algorithm

Split Tunnelling (Site-to-Site, Client, Server)

When the OpenVPN tunnel is established between the two endpoints, by default only the VPN traffic is routed through the tunnel. Other traffic, such as packets going to other places on the Internet, is still routed using the normal default route, not through the VPN tunnel. This is called split tunnelling, because there are considered to be two "tunnels": the normal traffic route and the VPN tunnel.

On the one hand, split tunnelling is very efficient, since non-VPN traffic (for example, Internet traffic) travels through the normal route. In a remote access VPN setup, for example, this means that the remote user's Internet traffic travels to and from their ISP directly without going to the VPN server, company network, firewall, and so on. On the other hand, bypassing these functions can be considered a security issue, since in such cases the Internet traffic is not filtered or protected according to a company policy.

To disable split tunnelling, use the configuration shown in Example 4-16.

Example 4-16 Configuration options related to split tunnelling

```
interfaces {
    openvpn if_name {
        replace-default-route {
            local
        }
    }
}
```

- **replace-default-route**: This option tells OpenVPN that the default route should be replaced by a route through the VPN tunnel, i.e., split tunnelling should be disabled. Note that, when set, this option has different effects depending on the OpenVPN mode in which the endpoint operates.
  - — If the endpoint is in site-to-site mode or client mode, setting **replace-default-route** will replace the default route on *this* endpoint with a route through VPN tunnel. In other words, it disables split tunnelling on *this* endpoint.
  - — If the endpoint is in server mode, setting **replace-default-route** will cause the *clients* connecting to this server to replace their default route. In other words, it disables split tunnelling on the *clients*.
- **local**: The local option under **replace-default-route** must be set **if and only if** the two tunnel endpoints are directly connected, i.e., on the same subnet.

Of course, since the OpenVPN tunnel interface is routable, static routes can be added, with or without split tunnelling, to override the default behavior.

Broadcast Network (Site-to-Site, Client, Server)

By default, an OpenVPN interfce is configured as a 'tun' device. A 'tun' device is a virtual network interface that operates on Layer 3 (network layer) traffic such as IP packets. There are cases where the virtual interface needs to operate on Layer 2 (link layer) traffic, such as Ethernet frames. One example of this is where subnets on each end of a tunnel must reside on the same subnet. In this case, the two subnets must be bridged across the tunnel. Bridging occurs on Layer 2. Another example is where a DHCP Relay resides on one side of a tunnel and the DHCP Server or DHCP clients are on the other side. Clients must broadcast DHCP discovery messages and require a broadcast network in order to do this. Because of this, DHCP Relay requires that all interfaces that it binds to be broadcast interfaces.

A 'tap' device is a virtual network interface that operates on Layer 2 (link layer) traffic and provides a broadcast network. A 'tap' device is automatically configured by the system if the OpenVPN tunnel is to be used to bridge two subnets. If an OpenVPN tunnel is added to a bridge group then a 'tap' device is implied and does not need to be configured explicitly. For cases that don't involve bridging, a 'tap' device must be configured explicitly using the interfaces openvpn <vtunx> device-type tap command.

Client and Server Configuration

To configure an OpenVPN Client or Server as a 'tap' device, use the configuration shown in Example 4-17.

Example 4-17 Configuration options related to 'tap' devices for Client and Server interfaces

```
interfaces {
    openvpn if_name {
        device-type
            tap
    }
}
```

- **device-type tap:** This option tells OpenVPN that the tunnel is to be used as a ‘tap’ device and operate on Layer 2 traffic. This configuration is required on both ends of the OpenVPN tunnel.

Site-to-site Configuration

For Site-to-site instances, in addition to configuring the interface as ‘tap’ device, you must also specify the subnet mask for the local address specified. To configure an OpenVPN Site-to-site interface as a ‘tap’ device, use the configuration shown in Example 4-18.

Example 4-18 Configuration options related to ‘tap’ devices for Site-to-site interfaces

```
interfaces {
    openvpn if_name {
        device-type
            tap
        local-address ipv4 {
            subnet-mask mask
        }
    }
}
```

- **device-type tap:** This option tells OpenVPN that the tunnel is to be used as a ‘tap’ device and operate on Layer 2 traffic. This configuration is required on both ends of the OpenVPN tunnel.
- **local-address:** This is the IP address at the local end of the OpenVPN tunnel.
- **subnet-mask:** This is the subnet mask for the **local-address** (for example, 255.255.255.0).

Multiple Remote Endpoints (Client Only)

In client-server mode, the **remote-host** option must be specified on the client endpoints so the clients can initiate the VPN sessions. In some environments, the administrator may want the clients to have a list of servers to provide some redundancy— if one of the servers fails, a client can try the next one. In the Vyatta system, this server list can be configured by specifying multiple **remote-host** entries.

To configure multiple endpoints on V2, perform the following steps in configuration mode.

Example 4-19 V2 OpenVPN multiple endpoints configuration

Step	Command
Create the vtun0 configuration node.	`vyatta@V2# set interfaces openvpn vtun0`
Additional configuration commands.	`...`
Specify the physical IP address of the first remote host.	`vyatta@V2# set interfaces openvpn vtun0 remote-host 12.34.56.78`
Specify the physical IP address of the second remote host.	`vyatta@V2# set interfaces openvpn vtun0 remote-host 12.34.56.79`
Specify the physical IP address of the third remote host.	`vyatta@V2# set interfaces openvpn vtun0 remote-host 12.34.56.80`
Set the firewall rule for inbound traffic on the vtun0 interface.	`vyatta@V2# set interfaces openvpn vtun0 firewall in name rules-in`
Additional configuration commands.	`...`
Commit the change.	`vyatta@V2# commit`

Show the OpenVPN configuration.	`vyatta@V2# show interfaces openvpn vtun0`
	`...`
	`remote-host 12.34.56.78`
	`remote-host 12.34.56.79`
	`remote-host 12.34.56.80`
	`...`

When multiple entries are specified, a client will start from the beginning of the list and attempt to establish a VPN tunnel with the first **remote-host**. If the first one does not work, the client will try the second one, and so on.

Note that multiple **remote-host** entries can also be specified in site-to-site mode. However, since the two endpoints are most likely fixed in this mode, such usage probably does not make sense in most cases.

Client-Server Topology (Server Only)

In client-server mode, two different client-server topologies can be configured using the topology option. The two different topologies are **subnet** and **point-to-point**, as shown in Example 4-20.

Example 4-20 Configuration options related to topology

```
interfaces {
    openvpn if_name {
        server {
            topology [subnet|point-to-point]
        }
    }
}
```

The **topology** option primarily specifies how the tunnel interface is configured, how the addresses are allocated, and so on. At a high level, the key implications of these topologies are the following.

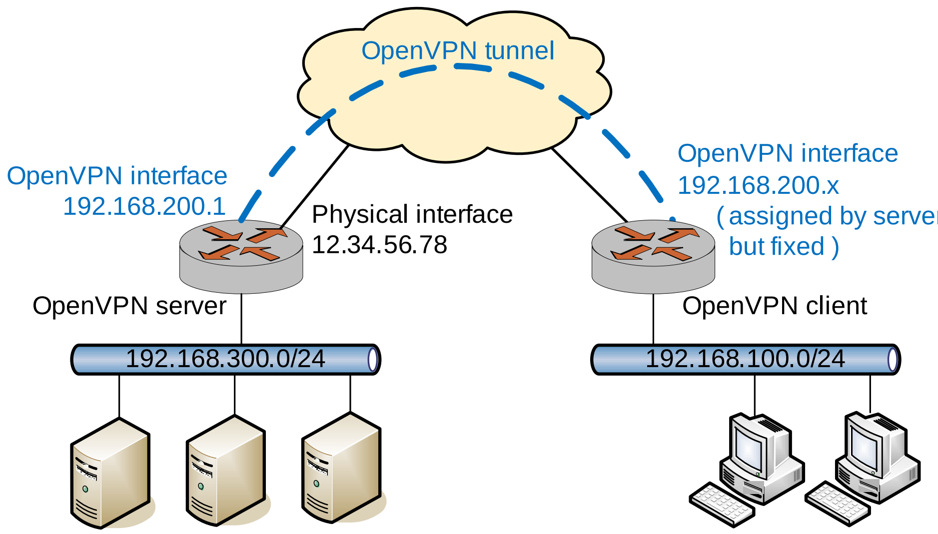
- **subnet**: This topology is compatible with OpenVPN clients on Windows hosts and is the default if **topology** is not set. Routing protocols that are configured to use a broadcast-style network are suited to this topology. However, this topology does not provide client isolation; that is, clients can reach one another.
- **point-to-point**: This topology is *not* compatible with Windows clients, and routing protocols using a broadcast-style network would not work with this. On the other hand, this topology provides client isolation.

Client-Specific Settings (Server Only)

In a typical remote access VPN setup, the “clients” are remote users—for example, users trying to access the company private network from home. Therefore, when a client establishes a VPN tunnel with the VPN server, it only needs to ensure that the client host itself can access the private network; so, it can use any tunnel IP address assigned by the server.

However, in some environments, the client-server mode is used to implement site-to-site functionality; that is, each client is in fact a “site” that establishes, in effect, a “site-to-site” tunnel with the server. This is illustrated in Example 4-7.

Figure 4-7 Client-server mode



In such an environment, it may be useful to give a fixed IP address to each OpenVPN client. Furthermore, in such cases there may be a private network behind a client as well, and the OpenVPN server needs to know that traffic destined to this private network should be routed to the particular client. Similarly, there may be networks behind the OpenVPN server that the client needs to access. In other words, these are client-specific settings that are tied to a particular client, and they can be configured using the options shown in Example 4-21 and explained following the example.

Example 4-21 Configuration options related to client-server

```
interfaces {
    openvpn <if_name> {
        server {
            client <client_name> {
                ip <client_ip>
                push-route <ipv4net>
                subnet <client_subnet>
            }
        }
    }
}
```

- **client**: This specifies a name for the client; this name corresponds to the common name specified in the client's certificate. When a client initiates the VPN session, the server uses the name in the certificate to look up and apply client-specific settings (if any).

- **ip**: This specifies the fixed IP address that will be assigned to the particular client.
- **push-route**: This specifies the network address of a network behind the OpenVPN server that the client can route traffic to. Multiple networks can be specified with multiple **push-route** configuration statements.
- **subnet**: This specifies the private subnet behind the particular client, and the OpenVPN process routes traffic destined to this subnet to the client. Multiple networks can be specified with multiple **subnet** configuration statements.

  Note that this setting only informs the OpenVPN server to which client the traffic for this subnet should be routed. However, before the OpenVPN server is in a position to make this decision, the traffic must be routed to the tunnel interface, so that it is processed by the OpenVPN server. For this reason, a static interface route must be added separately to direct traffic for this subnet to the tunnel interface.

In the above example, the server V1 can be configured with the client settings specific to the client V2 as follows (note that a static interface route is also needed for the client V2's subnet).

To configure this scenario, perform the following steps in configuration mode.

Example 4-22 V1 OpenVPN configuration - site-to-site with pre-shared secret

Step	Command
Create the vtun0 configuration node.	`vyatta@V1#` **`set interfaces openvpn vtun0`**
Additional configuration commands.	`...`
Create the server configuration node.	`vyatta@V1#` **`set interfaces openvpn vtun0 server`**
Additional configuration commands.	`...`
Create the client V2 configuration node.	`vyatta@V1#` **`set interfaces openvpn vtun0 server client V2`**
Specify the IP address of the client.	`vyatta@V1#` **`set interfaces openvpn vtun0 server client V2 ip 192.168.200.100`**
Specify the subnet at the server that the client can access.	`vyatta@V1#` **`set interfaces openvpn vtun0 server client V2 push-route 192.168.300.0/24`**
Set the subnet at the client.	`vyatta@V1#` **`set interfaces openvpn vtun0 server client V2 subnet 192.168.100.0/24`**
Additional configuration commands.	`...`

Example 4-22 V1 OpenVPN configuration - site-to-site with pre-shared secret

Commit the change.	`vyatta@V1# commit`

Show the OpenVPN configuration.	`vyatta@V1# show interfaces openvpn vtun0`
	`...`
	`server {`
	`   ...`
	`   client V2 {`
	`       ip 192.168.200.100`
	`       push-route 192.168.300.0/24`
	`       subnet 192.168.100.0/24`
	`   }`
	`   ...`
	`}`
	`...`

To configure the static interface route to access the remote subnet via the OpenVPN tunnel, perform the following steps in configuration mode.

Example 4-23 V1 static interface route configuration

Step	Command
Create the static interface route to access the remote subnet via the OpenVPN tunnel.	`vyatta@V1# set protocols static interface-route 192.168.100.0/24 next-hop-interface vtun0`
Commit the change.	`vyatta@V1# commit`

Show the static routing configuration.	`vyatta@V1# show protocols static`
	`interface-route 192.168.100.0/24 {`
	`   next-hop-interface vtun0 {`
	`   }`
	`}`

Unsupported OpenVPN Options

OpenVPN has over two hundred options, not all of which are feasible to support in the Vyatta configuration. At the same time, the administrator of a particular environment might require OpenVPN options not supported by the Vyatta configuration. For these cases, the Vyatta system provides the **openvpn-option** configuration attribute; this attribute allows any OpenVPN option to be specified, as shown in Example 4-24.

Example 4-24 The “openvpn-option” configuration attibute

```
interfaces {
    openvpn <if_name> {
        openvpn-option <options>
    }
}
```

The text of the **openvpn-option** attribute value is passed directly (without any validation) to OpenVPN when OpenVPN is invoked, as if the text had been typed on the OpenVPN command line by the user. Therefore, multiple options can be entered together as shown below.

To configure this example, perform the following steps in configuration mode.

Example 4-25 Entering multiple OpenVPN options using “openvpn-option”

Step	**Command**
Create the vtun0 configuration node.	`vyatta@V1#` **`set interfaces openvpn vtun0`**
Additional configuration commands.	`...`
Set the desired OpenVPN options.	`vyatta@V1#` **`set interfaces openvpn vtun0 openvpn-option "--verb 5 --secret /config/auth/secret 1"`**
Additional configuration commands.	`...`
Commit the change.	`vyatta@V1# commit`

Show the OpenVPN configuration.	`vyatta@V1#` **`show interfaces openvpn vtun0`**
	`...`
	`openvpn-option "--verb 5 --secret /config/auth/secret 1"`
	`...`

It is also possible to enter the commands separately as shown below.

To configure this example, perform the following steps in configuration mode.

Example 4-26 Entering multiple OpenVPN options via multiple commands using “openvpn-option”

Step	Command
Create the vtun0 configuration node.	vyatta@V1# **set interfaces openvpn vtun0**
Additional configuration commands.	...
Set another desired OpenVPN option.	vyatta@V1# **set interfaces openvpn vtun0 openvpn-option "--secret /config/auth/secret 1"**
Set a desired OpenVPN option.	vyatta@V1# **set interfaces openvpn vtun0 openvpn-option "--verb 5"**
Additional configuration commands.	...
Commit the change.	vyatta@V1# commit
Show the OpenVPN configuration.	vyatta@V1# **show interfaces openvpn vtun0** ... openvpn-option "--secret /config/auth/secret 1" openvpn-option "--verb 5" ...

No validation is done on this setting; therefore, when using it, you should make sure that the specified OpenVPN options and their values (if any) are valid. Furthermore, since many OpenVPN options conflict with one another, you should also ensure that the specified options do not conflict with one another or with any other OpenVPN options configured through the Vyatta configuration. Finally, some OpenVPN options require coordination between the two endpoints (for example, the value must be 0 on one side and 1 on the other), and you must ensure such constraints are met.

Bridging

OpenVPN can be used to bridge LAN segments across a WAN. For further details see the Bridging chapter in the *Vyatta LAN Interfaces Reference Guide*.

OpenVPN Commands

This chapter contains the following commands.

Configuration Commands	
Global OpenVPN Commands	
interfaces openvpn <vtunx>	Defines an OpenVPN interface.
interfaces openvpn <vtunx> description <desc>	Specifies a description for an OpenVPN interface.
interfaces openvpn <vtunx> device-type tap	Configures an OpenVPN interface as a ‘tap’ device.
interfaces openvpn <vtunx> disable	Disables an OpenVPN interface without discarding configuration.
interfaces openvpn <vtunx> encryption <algorithm>	Specifies the encryption algorithm to be used for the OpenVPN tunnel.
interfaces openvpn <vtunx> hash <algorithm>	Specifies the hash algorithm to be used for the OpenVPN tunnel.
interfaces openvpn <vtunx> local-address <ipv4>	Sets the IP address for the tunnel interface of the local OpenVPN endpoint.
interfaces openvpn <vtunx> local-host <ipv4>	Specifies the IP address of the local physical interface.
interfaces openvpn <vtunx> local-port <port>	Specifies the port number to be used for OpenVPN traffic on the local tunnel interface.
interfaces openvpn <vtunx> mode <mode>	Specifies the mode the OpenVPN interface will operate in.
interfaces openvpn <vtunx> openvpn-option <options>	Specifies additional OpenVPN options.
interfaces openvpn <vtunx> protocol <protocol>	Specifies the OpenVPN communications protocol.
interfaces openvpn <vtunx> remote-address <ipv4>	Specifies the IP address for the tunnel interface of the remote OpenVPN endpoint.
interfaces openvpn <vtunx> remote-host <hostname>	Specifies the remote IP address or hostname to which connections are made.
interfaces openvpn <vtunx> remote-port <port>	Specifies the port number on which outgoing sessions are sent.
interfaces openvpn <vtunx> replace-default-route	Specifies that the default route should be through the OpenVPN tunnel.
interfaces openvpn <vtunx> shared-secret-key-file <filename>	Specifies the file containing a secret key shared with the remote end of the tunnel.

OpenVPN Server	
interfaces openvpn <vtunx> server	Defines an OpenVPN server mode endpoint.
interfaces openvpn <vtunx> server client <client-name>	Defines a client site on the server in a client-server environment.
interfaces openvpn <vtunx> server client <client-name> disable	Specifies a client that will be disallowed from connecting to the OpenVPN server.
interfaces openvpn <vtunx> server client <client-name> ip <ipv4>	Specifies the IP address of a client in a client-server environment.
interfaces openvpn <vtunx> server client <client-name> push-route <ipv4net>	Specifies a route to be pushed to a client in a client-server environment.
interfaces openvpn <vtunx> server client <client-name> subnet <ipv4net>	Specifies a subnet at a client site in a client-server environment.
interfaces openvpn <vtunx> server domain-name <domain-name>	Provides the domain name for OpenVPN clients.
interfaces openvpn <vtunx> server max-connections <num>	Specifies the maximum number of clients that can connect to the server in a client-server environment.
interfaces openvpn <vtunx> server name-server <ipv4>	Specifies a name server address to be pushed to clients in a client-server environment.
interfaces openvpn <vtunx> server push-route <ipv4net>	Specifies a route to be pushed to all clients in a client-server environment.
interfaces openvpn <vtunx> server subnet <ipv4net>	Specifies the subnet from which client IP addresses are allocated.
interfaces openvpn <vtunx> server topology <topology>	Specifies the topology to use in a client-server environment.
OpenVPN Access Server Client Access	
interfaces openvpn <vtunx> remote-configuration password <password>	Specifies the password for client authentication by an OpenVPN Access Server.
interfaces openvpn <vtunx> remote-configuration server <address>	Specifies an OpenVPN Access Server for a client to connect to.
interfaces openvpn <vtunx> remote-configuration tunnel-password <password>	Specifies the password for tunnel establishment to an OpenVPN server.
interfaces openvpn <vtunx> remote-configuration tunnel-username <username>	Specifies a username for tunnel establishment to an OpenVPN server.
interfaces openvpn <vtunx> remote-configuration username <username>	Specifies a username for client authentication by an OpenVPN Access Server.

TLS	
interfaces openvpn <vtunx> tls	Defines a Transport Layer Security (TLS) configuration.
interfaces openvpn <vtunx> tls ca-cert-file <filename>	Specifies the file containing the certificate authority's certificate.
interfaces openvpn <vtunx> tls cert-file <filename>	Specifies the file containing the endpoint's own certificate.
interfaces openvpn <vtunx> tls crl-file <filename>	Specifies the file containing a certificate revocation list.
interfaces openvpn <vtunx> tls dh-file <filename>	Specifies the file containing Diffie Hellman parameters.
interfaces openvpn <vtunx> tls key-file <filename>	Specifies the file containing the endpoint's own private key.
interfaces openvpn <vtunx> tls role <role>	Specifies the TLS role the endpoint will take.
Operational Commands	
generate vpn openvpn-key <filename>	Generates a shared secret file.
reset openvpn client <client-name>	Resets a client connection.
reset openvpn interface <vtunx>	Resets all tunnel connections on an OpenVPN interface.
show interfaces openvpn	Displays a status summary of all OpenVPN interfaces.
show interfaces openvpn <interface>	Displays the detailed status of an OpenVPN interface.
show interfaces openvpn <interface> brief	Displays the status summary of an OpenVPN interface.
show interfaces openvpn <interface> capture	Captures data passing through the OpenVPN interface.
show interfaces openvpn detail	Displays the detailed status of all OpenVPN interfaces on the system.
show openvpn status client	Displays information on OpenVPN connections in client mode.
show openvpn status server	Displays information on connected clients in server mode.
show openvpn status site-to-site	Displays information on OpenVPN connections in site-to-site mode.

Commands for using other system features with OpenVPN interfaces can be found in the following locations

Related Commands Documented Elsewhere	
Firewall	Commands for configuring firewall on OpenVPN interfaces are described in the *Vyatta Firewall Reference Guide*.

generate vpn openvpn-key <filename>

Generates a shared secret file.

Syntax

generate vpn openvpn-key *filename*

Command Mode

Operational mode.

Parameters

filename	The name of the shared secret file that is generated.

Default

None.

Usage Guidelines

Use this command to generate a shared secret file that is required when the OpenVPN pre-shared secret mechanism is used. This command is only available to users with administrative privileges.

interfaces openvpn <vtunx>

Defines an OpenVPN interface.

Syntax

set interfaces openvpn *vtunx*

delete interfaces openvpn *vtunx*

show interfaces openvpn *vtunx*

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {
    openvpn vtunx {
    }
}
```

Parameters

vtunx	Mandatory. Multi-node. The identifier for the OpenVPN interface you are defining. This may be **vtun0** to **vtun***x*, where *x* is a non-negative integer. You can define more than one OpenVPN interface by creating multiple **interfaces openvpn** configuration nodes.

Default

None.

Usage Guidelines

Use this command to configure an OpenVPN interface.

Use the **set** form of this command to create an OpenVPN interface.

Use the **delete** form of this command to remove all configuration for an OpenVPN interface.

Use the **show** form of this command to view OpenVPN interface configuration.

interfaces openvpn <vtunx> description <desc>

Specifies a description for an OpenVPN interface.

Syntax

set interfaces openvpn *vtunx* **description** *desc*

delete interfaces openvpn *vtunx* **description**

show interfaces openvpn *vtunx* **description**

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {
    openvpn vtunx {
        description desc
    }
}
```

Parameters

vtunx	The identifier for the OpenVPN interface. This may be **vtun0** to **vtun***x*, where *x* is a non-negative integer.
desc	A brief description for the interface. If the description contains space characters, it must be enclosed in double quotes.

Default

None.

Usage Guidelines

Use this command to specify a description for the OpenVPN interface.

NOTE *Committing configuration changes to this configuration node does not result in the OpenVPN process being restarted.*

Use the **set** form of this command to specify the description for the interface.

Use the **delete** form of this command to remove the description for the interface.

Use the **show** form of this command to view the description for the interface.

interfaces openvpn <vtunx> device-type tap

Configures an OpenVPN interface as a ‘tap’ device.

Syntax

set interfaces openvpn *vtunx* **device-type tap**

delete interfaces openvpn *vtunx* **device-type tap**

show interfaces openvpn *vtunx* **device-type**

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {
    openvpn vtunx {
        device-type {
            tap
        }
    }
}
```

Parameters

vtunx	The identifier for the OpenVPN interface. This may be **vtun0** to **vtun***x*, where *x* is a non-negative integer.

Default

The OpenVPN interface is configured as a ‘tun’ device.

Usage Guidelines

Use this command to specify that the OpenVPN interface is to be configuread as a ‘tap’ device.

By default, an OpenVPN interfce is configured as a ‘tun’ device. A ‘tun’ device is a virtual network interface that operates on Layer 3 (network layer) traffic such as IP packets. A ‘tap’ device is also a virtual network interface but it operates on Layer 2 (link layer) traffic such as Ethernet frames. It is used in instances where two ends of an OpenVPN tunnel must be bridged or require a broadcast interface. An example of this is DHCP Relay.

NOTE *Each end of an OpenVPN tunnel must have the same* ***device-type*** *configuration.*

Use the **set** form of this command to specify that the interface is to be configured as a ‘tap’ device.

Use the **delete** form of this command to return the interface to its default behavior.

Use the **show** form of this command to view the **device-type** configuration.

interfaces openvpn <vtunx> disable

Disables an OpenVPN interface without discarding configuration.

Syntax

set interfaces openvpn *vtunx* **disable**

delete interfaces openvpn *vtunx* **disable**

show interfaces openvpn *vtunx*

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {
    openvpn vtunx {
        disable
    }
}
```

Parameters

vtunx	The identifier for the OpenVPN interface. This may be **vtun0** to **vtun***x*, where *x* is a non-negative integer.

Default

The OpenVPN interface configuration is enabled.

Usage Guidelines

Use this command to disable the OpenVPN interface without discarding configuration. The interface can then be re-enabled at a later time without the need to redefine the configuration.

Use the **set** form of this command to disable the interface.

Use the **delete** form of this command to enable the interface.

Use the **show** form of this command to view the OpenVPN interface configuration.

interfaces openvpn <vtunx> encryption <algorithm>

Specifies the encryption algorithm to be used for the OpenVPN tunnel.

Syntax

set interfaces openvpn *vtunx* **encryption** *algorithm*

delete interfaces openvpn *vtunx* **encryption**

show interfaces openvpn *vtunx* **encryption**

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {
    openvpn vtunx {
        encryption algorithm
    }
}
```

Parameters

vtunx	The identifier for the OpenVPN interface. This may be **vtun0** to **vtun***x*, where *x* is a non-negative integer.
algorithm	The encryption algorithm that will be used within the OpenVPN tunnel. Supported values are as follows: **3des**: DES algorithm with triple encryption **aes128**: AES algorithm with 128-bit key **aes192**: AES algorithm with 192-bit key **aes256**: AES algorithm with 256-bit key **bf128**: Blowfish algorithm with 128-bit key **bf256**: Blowfish algorithm with 256-bit key **des**: DES algorithm The default is **bf128**.

Default

Blowfish algorithm with 128-bit key is used as the encryption algorithm.

Usage Guidelines

Use this command to configure the encryption algorithm that will be used within the OpenVPN tunnel.

Use the **set** form of this command to define the encryption algorithm that will be used within the OpenVPN tunnel.

Use the **delete** form of this command to remove the encryption algorithm that will be used within the OpenVPN tunnel and return to the default.

Use the **show** form of this command to view the encryption algorithm that will be used within the OpenVPN tunnel.

interfaces openvpn <vtunx> hash <algorithm>

Specifies the hash algorithm to be used for the OpenVPN tunnel.

Syntax

set interfaces openvpn *vtunx* **hash** *algorithm*

delete interfaces openvpn *vtunx* **hash**

show interfaces openvpn *vtunx* **hash**

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {
    openvpn vtunx {
        hash algorithm
    }
}
```

Parameters

vtunx	The identifier for the OpenVPN interface. This may be **vtun0** to **vtun***x*, where *x* is a non-negative integer.
algorithm	The hash algorithm that will be used within the OpenVPN tunnel. Supported values are as follows: **md5**: MD5 algorithm **sha1**: SHA-1 algorithm **sha256**: SHA-256 algorithm **sha512**: SHA-512 algorithm The default is **sha1**.

Default

SHA-1 is used as the hash algorithm.

Usage Guidelines

Use this command to configure the hash algorithm that will be used within the OpenVPN tunnel.

Use the **set** form of this command to define the hash algorithm that will be used within the OpenVPN tunnel.

Use the **delete** form of this command to remove the hash algorithm that will be used within the OpenVPN tunnel and return to the default.

Use the **show** form of this command to view the hash algorithm that will be used within the OpenVPN tunnel.

interfaces openvpn <vtunx> local-address <ipv4>

Sets the IP address for the tunnel interface of the local OpenVPN endpoint.

Syntax

set interfaces openvpn *vtunx* **local-address** *ipv4* [**subnet-mask** *mask*]

delete interfaces openvpn *vtunx* **local-address** [**subnet-mask**]

show interfaces openvpn *vtunx* **local-address** [**subnet-mask**]

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {
    openvpn vtunx {
        local-address ipv4 {
            subnet-mask mask
        }
    }
}
```

Parameters

vtunx	The identifier for the OpenVPN interface. This may be **vtun0** to **vtun***x*, where *x* is a non-negative integer.
ipv4	Mandatory. An IPv4 address.
mask	A subnet mask for the network associated with the **local-address**. This is only required when interfaces openvpn <vtunx> device-type tap is set.

Default

None.

Usage Guidelines

Use this command to configure the tunnel IP address on the local end of the OpenVPN tunnel. Only a single address can be specified. This is required for site-to-site mode OpenVPN tunnels but not for client-server mode tunnels. The **subnet-mask** is only required when the interface is configured as a broadcast interface using interfaces openvpn <vtunx> device-type tap.

Use the **set** form of this command to define the tunnel IP address on the local end of the OpenVPN tunnel.

Use the **delete** form of this command to remove the tunnel IP address on the local end of the OpenVPN tunnel.

Use the **show** form of this command to view the tunnel IP address on the local end of the OpenVPN tunnel.

interfaces openvpn <vtunx> local-host <ipv4>

Specifies the IP address of the local physical interface.

Syntax

set interfaces openvpn *vtunx* **local-host** *ipv4*

delete interfaces openvpn *vtunx* **local-host**

show interfaces openvpn *vtunx* **local-host**

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {
    openvpn vtunx {
        local-host ipv4
    }
}
```

Parameters

vtunx	The identifier for the OpenVPN interface. This may be **vtun0** to **vtun***x*, where *x* is a non-negative integer.
ipv4	Optional. The IP address of the local physical interface. This is the IP address on which connections are accepted. If not specified then all connections are accepted.

Default

None.

Usage Guidelines

Use this command to configure the local IP address to which connections are accepted. This can be used for a server endpoint in a client-server mode tunnel or the tcp-passive endpoint when TCP is used in site-to-site mode. The value can be an IP address on any of network interfaces on this endpoint. If this is set, the OpenVPN process will only accept sessions coming in on the particular IP address, and this applies to both UDP and TCP. If not set, OpenVPN accepts incoming sessions on any interface.

Use the **set** form of this command to specify the local IP address to which connections are accepted.

Use the **delete** form of this command to remove the local IP address to which connections are accepted.

Use the **show** form of this command to view the local IP address to which connections are accepted.

interfaces openvpn <vtunx> local-port <port>

Specifies the port number to be used for OpenVPN traffic on the local tunnel interface.

Syntax

set interfaces openvpn *vtunx* **local-port** *port*

delete interfaces openvpn *vtunx* **local-port**

show interfaces openvpn *vtunx* **local-port**

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {
   openvpn vtunx {
      local-port port
   }
}
```

Parameters

vtunx	The identifier for the OpenVPN interface. This may be **vtun0** to **vtun***x*, where *x* is a non-negative integer.
port	Optional. The port number on which incoming sessions are accepted. The default is port **1194**.

Default

The default is port **1194**.

Usage Guidelines

Use this command to configure the local UDP or TCP port on which incoming sessions are accepted. This can be used for a server endpoint in a client-server mode tunnel or the tcp-passive endpoint when TCP is used in site-to-site mode.

Use the **set** form of this command to specify the local port to which incoming sessions are accepted.

Use the **delete** form of this command to remove the local port to which incoming sessions are accepted.

Use the **show** form of this command to view the local port to which incoming sessions are accepted.

interfaces openvpn <vtunx> mode <mode>

Specifies the mode the OpenVPN interface will operate in.

Syntax

set interfaces openvpn *vtunx* **mode** *mode*

delete interfaces openvpn *vtunx* **mode**

show interfaces openvpn *vtunx* **mode**

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {
    openvpn vtunx {
        mode mode
    }
}
```

Parameters

vtunx	The identifier for the OpenVPN interface. This may be **vtun0** to **vtun***x*, where *x* is a non-negative integer.
mode	Mandatory. The mode the OpenVPN interface will operate in. Supported values are as follows: **client**: The endpoint is the client in a client-server OpenVPN tunnel. **server**: The endpoint is the server in a client-server OpenVPN tunnel. **site-to-site**: The endpoint is one end of a site-to-site OpenVPN tunnel.

Default

None.

Usage Guidelines

Use this command to specify the mode the OpenVPN interface will operate in.

Use the **set** form of this command to specify the mode the OpenVPN interface will operate in.

Use the **delete** form of this command to remove the mode the OpenVPN interface will operate in.

Use the **show** form of this command to view the mode the OpenVPN interface will operate in.

interfaces openvpn <vtunx> openvpn-option <options>

Specifies additional OpenVPN options.

Syntax

set interfaces openvpn *vtunx* **openvpn-option** *options*

delete interfaces openvpn *vtunx* **openvpn-option**

show interfaces openvpn *vtunx* **openvpn-option**

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {
    openvpn vtunx {
        openvpn-option options
    }
}
```

Parameters

vtunx	The identifier for the OpenVPN interface. This may be **vtun0** to **vtun***x*, where *x* is a non-negative integer.
options	Multi-node. The string of options to pass to the OpenVPN process. You can define multiple openvpn option lists by creating multiple **openvpn-option** configuration nodes. Each must have a unique configuration.

Default

None.

Usage Guidelines

Use this command to specify additional OpenVPN options that are not available within Vyatta OpenVPN commands. As the OpenVPN process has over two hundred commands only a base set is available through Vyatta commands. This command provides access to all options available in OpenVPN. Further information regarding OpenVPN can be found at http://openvpn.net/.

Use the **set** form of this command to specify additional OpenVPN options.

Use the **delete** form of this command to remove additional OpenVPN options.

Use the **show** form of this command to view additional OpenVPN options.

interfaces openvpn <vtunx> protocol <protocol>

Specifies the OpenVPN communications protocol.

Syntax

set interfaces openvpn *vtunx* **protocol** *protocol*

delete interfaces openvpn *vtunx* **protocol**

show interfaces openvpn *vtunx* **protocol**

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {
    openvpn vtunx {
        protocol protocol
    }
}
```

Parameters

vtunx	The identifier for the OpenVPN interface. This may be **vtun0** to **vtun***x*, where *x* is a non-negative integer.
protocol	The OpenVPN communications protocol. Supported values are as follows: **tcp-active**: TCP transport protocol - active role. **tcp-passive**: TCP transport protocol - passive role. **udp**: UDP transport protocol. This is the default.

Default

The default is **udp**.

Usage Guidelines

Use this command to specify the OpenVPN communications protocol.

Use the **set** form of this command to specify the OpenVPN communications protocol.

Use the **delete** form of this command to remove the OpenVPN communications protocol.

Use the **show** form of this command to view the OpenVPN communications protocol.

interfaces openvpn <vtunx> remote-address <ipv4>

Specifies the IP address for the tunnel interface of the remote OpenVPN endpoint.

Syntax

set interfaces openvpn *vtunx* **remote-address** *ipv4*

delete interfaces openvpn *vtunx* **remote-address**

show interfaces openvpn *vtunx* **remote-address**

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {
    openvpn vtunx {
        remote-address ipv4
    }
}
```

Parameters

vtunx	The identifier for the OpenVPN interface. This may be **vtun0** to **vtun***x*, where *x* is a non-negative integer.
ipv4	Mandatory. The tunnel IP address on the remote end of the OpenVPN tunnel.

Default

None.

Usage Guidelines

Use this command to configure the tunnel IP address on the remote end of the OpenVPN tunnel. Only a single address can be specified. This is required for site-to-site mode OpenVPN tunnels but not for client-server mode tunnels.

Use the **set** form of this command to define the tunnel IP address on the remote end of the OpenVPN tunnel.

Use the **delete** form of this command to remove the tunnel IP address on the remote end of the OpenVPN tunnel.

Use the **show** form of this command to view the tunnel IP address on the remote end of the OpenVPN tunnel.

interfaces openvpn <vtunx> remote-configuration password <password>

Specifies the password for client authentication by an OpenVPN Access Server.

Availability

Vyatta Subscription Edition

Syntax

set interfaces openvpn *vtunx* **remote-configuration password** *password*

delete interfaces openvpn *vtunx* **remote-configuration password**

show interfaces openvpn *vtunx* **remote-configuration password**

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {
    openvpn vtunx {
        remote-configuration {
            password password
    }
}
```

Parameters

vtunx	The identifier for the OpenVPN interface. This may be **vtun0** to **vtun***x*, where *x* is a non-negative integer.
password	The password to be used in conjuction with a username for authentication by the OpenVPN Access Server.

Default

None.

Usage Guidelines

Use this command to specify a password the OpenVPN Access Server can use to authenticate a client. This password is used when the client initiates a connection with the OpenVPN Access Server.

Use the **set** form of this command to specify the password.

Use the **delete** form of this command to remove the password .

Use the **show** form of this command to view password configuration.

interfaces openvpn <vtunx> remote-configuration server <address>

Specifies an OpenVPN Access Server for a client to connect to.

Availability

Vyatta Subscription Edition

Syntax

set interfaces openvpn *vtunx* **remote-configuration server** *address*

delete interfaces openvpn *vtunx* **remote-configuration server**

show interfaces openvpn *vtunx* **remote-configuration server**

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {
    openvpn vtunx {
        remote-configuration {
            server address
    }
}
```

Parameters

vtunx	The identifier for the OpenVPN interface. This may be **vtun0** to **vtun***x*, where *x* is a non-negative integer.
address	The IP address (or hostname) of an OpenVPN Access Server.

Default

None.

Usage Guidelines

Use this command to specify the IP address or hostname of an OpenVPN Access Server a client can use when establishing an OpenVPN tunnel.

Use the **set** form of this command to specify the IP address or hostname.

Use the **delete** form of this command to remove the IP address or hostname.

Use the **show** form of this command to view IP address or hostname configuration.

interfaces openvpn <vtunx> remote-configuration tunnel-password <password>

Specifies the password for tunnel establishment to an OpenVPN server.

Availability

Vyatta Subscription Edition

Syntax

set interfaces openvpn *vtunx* **remote-configuration tunnel-password** *password*

delete interfaces openvpn *vtunx* **remote-configuration tunnel-password**

show interfaces openvpn *vtunx* **remote-configuration tunnel-password**

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {
    openvpn vtunx {
        remote-configuration {
            tunnel-password password
    }
}
```

Parameters

vtunx	The identifier for the OpenVPN interface. This may be **vtun0** to **vtun***x*, where *x* is a non-negative integer.
password	The password to be used in conjuction with a username for tunnel establishment to an OpenVPN server.

Default

None.

Usage Guidelines

Use this command to specify a password used to establish an OpenVPN tunnel with an OpenVPN server. The password is only required if the OpenVPN server has Autologin disabled and you are using an OpenVPN Access Server to provide OpenVPN tunnel configuration information.

Use the **set** form of this command to specify the password.

Use the **delete** form of this command to remove the password.

Use the **show** form of this command to view password configuration.

interfaces openvpn <vtunx> remote-configuration tunnel-username <username>

Specifies a username for tunnel establishment to an OpenVPN server.

Availability

Vyatta Subscription Edition

Syntax

set interfaces openvpn *vtunx* **remote-configuration tunnel-username** *username*

delete interfaces openvpn *vtunx* **remote-configuration tunnel-username**

show interfaces openvpn *vtunx* **remote-configuration tunnel-username**

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {
    openvpn vtunx {
        remote-configuration {
            tunnel-username username
    }
}
```

Parameters

vtunx	The identifier for the OpenVPN interface. This may be **vtun0** to **vtun***x*, where *x* is a non-negative integer.
username	The username to be used in conjuction with a password for tunnel establishment to an OpenVPN server.

Default

None.

Usage Guidelines

Use this command to specify a username used to establish an OpenVPN tunnel with an OpenVPN server. The username is only required if the OpenVPN server has Autologin disabled and you are using an OpenVPN Access Server to provide OpenVPN tunnel configuration information.

Use the **set** form of this command to configure the username.

Use the **delete** form of this command to remove the username.

Use the **show** form of this command to view username configuration.

interfaces openvpn <vtunx> remote-configuration username <username>

Specifies a username for client authentication by an OpenVPN Access Server.

Availability

Vyatta Subscription Edition

Syntax

set interfaces openvpn *vtunx* **remote-configuration username** *username*

delete interfaces openvpn *vtunx* **remote-configuration username**

show interfaces openvpn *vtunx* **remote-configuration username**

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {
    openvpn vtunx {
        remote-configuration {
            username username
    }
}
```

Parameters

vtunx	The identifier for the OpenVPN interface. This may be **vtun0** to **vtun***x*, where *x* is a non-negative integer.
username	The username to be used in conjuction with a password for authentication by the OpenVPN Access Server.

Default

None.

Usage Guidelines

Use this command to specify a username the OpenVPN Access Server can use to authenticate a client. This username is used when the client initiates a connection with the OpenVPN Access Server.

Use the **set** form of this command to configure the username.

Use the **delete** form of this command to remove the username.

Use the **show** form of this command to view username configuration.

interfaces openvpn <vtunx> remote-host <hostname>

Specifies the remote IP address or hostname to which connections are made.

Syntax

set interfaces openvpn *vtunx* **remote-host** *hostname*

delete interfaces openvpn *vtunx* **remote-host**

show interfaces openvpn *vtunx* **remote-host**

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {
    openvpn vtunx {
        remote-host hostname
    }
}
```

Parameters

vtunx	The identifier for the OpenVPN interface. This may be **vtun0** to **vtun***x*, where *x* is a non-negative integer.
hostname	The remote IP address or hostname to which connections are made.

Default

None.

Usage Guidelines

Use this command to configure the remote IP address or hostname to which connections are made. This is required by a client to specify a server endpoint in a client-server mode tunnel. It is also required by both sides in site-to-site mode.

Use the **set** form of this command to specify the remote IP address or hostname to which connections are made.

Use the **delete** form of this command to remove the remote IP address or hostname to which connections are made.

Use the **show** form of this command to view the remote IP address or hostname to which connections are made.

interfaces openvpn <vtunx> remote-port <port>

Specifies the port number on which outgoing sessions are sent.

Syntax

set interfaces openvpn *vtunx* **remote-port** *port*

delete interfaces openvpn *vtunx* **remote-port**

show interfaces openvpn *vtunx* **remote-port**

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {
    openvpn vtunx {
        remote-port port
    }
}
```

Parameters

vtunx	The identifier for the OpenVPN interface. This may be **vtun0** to **vtun***x*, where *x* is a non-negative integer.
port	Optional. The port number on which outgoing sessions are sent. The default is port **1194**.

Default

The default is port **1194**.

Usage Guidelines

Use this command to configure the remote UDP or TCP port on which outgoing sessions are sent. This can be used for a client endpoint in a client-server mode tunnel, either endpoint when UDP is used in site-to-site mode, or the tcp-active endpoint when TCP is used in site-to-site mode. Note that, if set, the remote-port setting on one endpoint must match the local-port setting on the other, and vice versa.

Use the **set** form of this command to specify the remote UDP or TCP port on which outgoing sessions are sent.

Use the **delete** form of this command to remove the remote UDP or TCP port on which outgoing sessions are sent.

Use the **show** form of this command to view the remote UDP or TCP port on which outgoing sessions are sent.

interfaces openvpn <vtunx> replace-default-route

Specifies that the default route should be through the OpenVPN tunnel.

Syntax

set interfaces openvpn *vtunx* **replace-default-route** [**local**]

delete interfaces openvpn *vtunx* **replace-default-route**

show interfaces openvpn *vtunx* **replace-default-route**

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {
    openvpn vtunx {
        replace-default-route {
            local
        }
    }
}
```

Parameters

vtunx	The identifier for the OpenVPN interface. This may be **vtun0** to **vtun***x*, where *x* is a non-negative integer.
local	Optional. This option must be set **if and only if** the two tunnel endpoints are directly connected, i.e., on the same subnet.

Default

None.

Usage Guidelines

Use this command to tell OpenVPN that the default route should be replaced by a route through the VPN tunnel, i.e., split tunnelling should be disabled. Note that, when set, this option has different effects depending on the OpenVPN mode in which the endpoint operates.

If the endpoint is in site-to-site mode or client mode, setting **replace-default-route** will replace the default route on this endpoint with a route through VPN tunnel. In other words, it disables split tunnelling on this endpoint.

If the endpoint is in server mode, setting **replace-default-route** will cause the clients connecting to this server to replace their default route. In other words, it disables split tunnelling on the clients.

Use the **set** form of this command to specify that the default route should be through the OpenVPN tunnel.

Use the **delete** form of this command to remove the configuration.

Use the **show** form of this command to view the configuration.

interfaces openvpn <vtunx> server

Defines an OpenVPN server mode endpoint.

Syntax

set interfaces openvpn *vtunx* **server**

delete interfaces openvpn *vtunx* **server**

show interfaces openvpn *vtunx* **server**

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {
    openvpn vtunx {
        server {
        }
    }
}
```

Parameters

vtunx	The identifier for the OpenVPN interface. This may be **vtun0** to **vtun***x*, where *x* is a non-negative integer.

Default

None.

Usage Guidelines

Use this command to define an OpenVPN server mode endpoint.

Use the **set** form of this command to create the server mode configuration node.

Use the **delete** form of this command to remove the server mode configuration node.

Use the **show** form of this command to view the configuration.

interfaces openvpn <vtunx> server client <client-name>

Defines a client site on the server in a client-server environment.

Syntax

set interfaces openvpn *vtunx* **server client** *client-name*

delete interfaces openvpn *vtunx* **server client** [*client-name*]

show interfaces openvpn *vtunx* **server client** [*client-name*]

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {
    openvpn vtunx {
        server {
            client client-name {
            }
        }
    }
}
```

Parameters

vtunx	The identifier for the OpenVPN interface. This may be **vtun0** to **vtun***x*, where *x* is a non-negative integer.
client-name	Mandatory. The "name" of the client. It corresponds to the "common name" contained in the client's certificate. When a client initiates the VPN session, the server uses the name in the certificate to look up and apply client-specific settings (if any).

Default

None.

Usage Guidelines

Use this command to define a client site on the server in a client-server environment.

NOTE *Committing configuration changes to this configuration node does not result in the OpenVPN process being restarted. The configuration change will take effect the next time the client connects to the server.*

Use the **set** form of this command to create the client configuration node.

Use the **delete** form of this command to remove the client configuration node.

Use the **show** form of this command to view the configuration.

interfaces openvpn <vtunx> server client <client-name> disable

Specifies a client that will be disallowed from connecting to the OpenVPN server.

Syntax

set interfaces openvpn *vtunx* **server client** *client-name* **disable**

delete interfaces openvpn *vtunx* **server client** *client-name* **disable**

show interfaces openvpn *vtunx* **server client** *client-name*

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {
    openvpn vtunx {
        server {
            client client-name {
                disable
            }
        }
    }
}
```

Parameters

vtunx	The identifier for the OpenVPN interface. This may be **vtun0** to **vtun***x*, where *x* is a non-negative integer.
client-name	Mandatory. The "name" of the client. It corresponds to the "common name" contained in the client's certificate.

Default

Clients are allowed to connect to the OpenVPN server.

Usage Guidelines

Use this command to specify a client that will be disallowed from connecting to the OpenVPN server the next time it tries to connect (and any subsequent attempts). This will not affect the client's current connection. The current connection can be reset using the reset openvpn client <client-name> command.

NOTE *If an OpenVPN client tries to connect to an OpenVPN server and is refused by the server, the client process will exit.*

Use the **set** form of this command to specify a client that will be disallowed from connecting to the OpenVPN server on any subsequent attempts.

Use the **delete** form of this command to allow the client to connect to the OpenVPN server.

NOTE *A OpenVPN client needs to be restarted before it will initiate a new connection to the OpenVPN server.*

Use the **show** form of this command to view the configuration.

interfaces openvpn <vtunx> server client <client-name> ip <ipv4>

Specifies the IP address of a client in a client-server environment.

Syntax

set interfaces openvpn *vtunx* **server client** *client-name* **ip** *ipv4*

delete interfaces openvpn *vtunx* **server client** *client-name* **ip**

show interfaces openvpn *vtunx* **server client** *client-name* **ip**

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {
    openvpn vtunx {
        server {
            client client-name {
                ip ipv4
            }
        }
    }
}
```

Parameters

vtunx	The identifier for the OpenVPN interface. This may be **vtun0** to **vtun***x*, where *x* is a non-negative integer.
client-name	Mandatory. The "name" of the client. It corresponds to the "common name" contained in the client's certificate. When a client initiates the VPN session, the server uses the name in the certificate to look up and apply client-specific settings (if any).
ipv4	The IP address to be assigned to the client.

Default

None.

Usage Guidelines

Use this command to specify the IP address to assign to the client in a client-server environment.

NOTE *Committing configuration changes to this configuration node does not result in the OpenVPN process being restarted. The configuration change will take effect the next time the client connects to the server.*

Use the **set** form of this command to specify the IP address to assign to the client in a client-server environment.

Use the **delete** form of this command to remove the IP address.

Use the **show** form of this command to view the IP address.

interfaces openvpn <vtunx> server client <client-name> push-route <ipv4net>

Specifies a route to be pushed to a client in a client-server environment.

Syntax

set interfaces openvpn *vtunx* **server client** *client-name* **push-route** *ipv4net*

delete interfaces openvpn *vtunx* **server client** *client-name* **push-route** *ipv4net*

show interfaces openvpn *vtunx* **server client** *client-name* **push-route**

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {
    openvpn vtunx {
        server {
            client client-name {
                push-route ipv4net
            }
        }
    }
}
```

Parameters

vtunx	The identifier for the OpenVPN interface. This may be **vtun0** to **vtun***x*, where *x* is a non-negative integer.
client-name	Mandatory. The "name" of the client. It corresponds to the "common name" contained in the client's certificate. When a client initiates the VPN session, the server uses the name in the certificate to look up and apply client-specific settings (if any).
ipv4net	Multi-node. The subnet to be made accessible to the OpenVPN client via the OpenVPN server. You can define multiple subnets to push to clients by creating multiple **push-route** configuration nodes. Each must have a unique IPv4net address.

Default

None.

Usage Guidelines

Use this command to specify a subnet that the client can access by routing packets through the server.

NOTE *Committing configuration changes to this configuration node does not result in the OpenVPN process being restarted. The configuration change will take effect the next time the client connects to the server. Use the reset openvpn interface <vtunx> command on the client to reset the connection.*

Use the **set** form of this command to specify a route to be pushed to all clients .

Use the **delete** form of this command to remove the route configuration.

Use the **show** form of this command to view the route configuration.

interfaces openvpn <vtunx> server client <client-name> subnet <ipv4net>

Specifies a subnet at a client site in a client-server environment.

Syntax

set interfaces openvpn *vtunx* **server client** *client-name* **subnet** *ipv4net*

delete interfaces openvpn *vtunx* **server client** *client-name* **subnet** *ipv4net*

show interfaces openvpn *vtunx* **server client** *client-name* **subnet**

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {
    openvpn vtunx {
        server {
            client client-name {
                subnet ipv4net
            }
        }
    }
}
```

Parameters

vtunx	The identifier for the OpenVPN interface. This may be **vtun0** to **vtun***x*, where *x* is a non-negative integer.
client-name	Mandatory. The "name" of the client. It corresponds to the "common name" contained in the client's certificate. When a client initiates the VPN session, the server uses the name in the certificate to look up and apply client-specific settings (if any).
ipv4net	Multi-node. A subnet at the client site. You can define multiple subnet addresses by creating multiple **subnet** configuration nodes. Each must have a unique IPv4 network address.

Default

None.

Usage Guidelines

Use this command to identify a subnet at a client site in a client-server environment.

NOTE *Committing configuration changes to this configuration node does not result in the OpenVPN process being restarted. The configuration change will take effect the next time the client connects to the server.*

Use the **set** form of this command to specify the subnet.

Use the **delete** form of this command to remove the subnet configuration.

Use the **show** form of this command to view the subnet configuration.

interfaces openvpn <vtunx> server domain-name <domain-name>

Provides the domain name for OpenVPN clients.

Syntax

set interfaces openvpn *vtunx* **server domain-name** *domain-name*

delete interfaces openvpn *vtunx* **server domain-name**

show interfaces openvpn *vtunx* **server domain-name**

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {
    openvpn vtunx {
        server {
            domain-name domain-name
        }
    }
}
```

Parameters

vtunx	The identifier for the OpenVPN interface. This may be **vtun0** to **vtun***x*, where *x* is a non-negative integer.
domain-name	The domain name to be given to OpenVPN clients connected to this OpenVPN server. A domain name can include letters, numbers, hyphens ("-"), and one period ("."). For example, "vyatta.com".

Default

None.

Usage Guidelines

Use this command to specify the domain name to be given to OpenVPN clients connected to this OpenVPN server.

NOTE *Certain applications on Windows clients (for example, "ipconfig"), refer to the domain name as the "Connection-specific DNS Suffix".*

Use the **set** form of this command to specify the domain name to be given to OpenVPN clients connected to this OpenVPN server.

Use the **delete** form of this command to remove the domain name configuration.

Use the **show** form of this command to view the domain name configuration.

interfaces openvpn <vtunx> server max-connections <num>

Specifies the maximum number of clients that can connect to the server in a client-server environment.

Syntax

set interfaces openvpn *vtunx* **server max-connections** *num*

delete interfaces openvpn *vtunx* **server max-connections**

show interfaces openvpn *vtunx* **server max-connections**

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {
    openvpn vtunx {
        server {
            max-connections num
        }
    }
}
```

Parameters

vtunx	The identifier for the OpenVPN interface. This may be **vtun0** to **vtun***x*, where *x* is a non-negative integer.
num	The maximum number of client connections that the server will accept. The range of supported values is 1 to 1024. The default is 1024.

Default

The number of clients that can connect is either 1024 or the limit of system resources.

Usage Guidelines

Use this command to specify the maximum number of client connections that the server will accept. Once the limit is reached, any additional clients that attempt to connect to the server will be refused.

Use the **set** form of this command to specify the maximum number of clients that can connect to the server.

Use the **delete** form of this command to return to the default configuration.

Use the **show** form of this command to view the maximum number of client connections configured.

interfaces openvpn <vtunx> server name-server <ipv4>

Specifies a name server address to be pushed to clients in a client-server environment.

Syntax

set interfaces openvpn *vtunx* **server name-server** *ipv4*

delete interfaces openvpn *vtunx* **server name-server** *ipv4*

show interfaces openvpn *vtunx* **server name-server**

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {
    openvpn vtunx {
        server {
            name-server ipv4
        }
    }
}
```

Parameters

vtunx	The identifier for the OpenVPN interface. This may be **vtun0** to **vtun***x*, where *x* is a non-negative integer.
ipv4	Multi-node. The IPv4 address of the name server to push to clients. You can define multiple name server addresses to push to clients by creating multiple **name-server** configuration nodes. Each must have a unique IPv4 address.

Default

None.

Usage Guidelines

Use this command to specify an IPv4 address of a name server to be pushed to clients in an OpenVPN client-server environment. This is supported by Windows clients. Other client types may not support this.

Use the **set** form of this command to specify a IPv4 address of a name server to be pushed to clients.

Use the **delete** form of this command to remove the name server configuration.

Use the **show** form of this command to view the name server configuration.

interfaces openvpn <vtunx> server push-route <ipv4net>

Specifies a route to be pushed to all clients in a client-server environment.

Syntax

set interfaces openvpn *vtunx* **server push-route** *ipv4net*

delete interfaces openvpn *vtunx* **server push-route** *ipv4net*

show interfaces openvpn *vtunx* **server push-route**

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {
    openvpn vtunx {
        server {
            push-route ipv4net
        }
    }
}
```

Parameters

vtunx	The identifier for the OpenVPN interface. This may be **vtun0** to **vtun***x*, where *x* is a non-negative integer.
ipv4net	Multi-node. The subnet to be made accessible to the OpenVPN clients via the OpenVPN server. You can define multiple subnets to push to clients by creating multiple **push-route** configuration nodes. Each must have a unique IPv4net address.

Default

None.

Usage Guidelines

Use this command to specify a subnet that all clients can access by routing packets through the server. This route is pushed to all clients and the OpenVPN process is restarted.

Use the **set** form of this command to specify a route to be pushed to all clients .

Use the **delete** form of this command to remove the route configuration.

Use the **show** form of this command to view the route configuration.

interfaces openvpn <vtunx> server subnet <ipv4net>

Specifies the subnet from which client IP addresses are allocated.

Syntax

set interfaces openvpn *vtunx* **server subnet** *ipv4net*

delete interfaces openvpn *vtunx* **server subnet**

show interfaces openvpn *vtunx* **server subnet**

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {
    openvpn vtunx {
        server {
            subnet ipv4net
        }
    }
}
```

Parameters

vtunx	The identifier for the OpenVPN interface. This may be **vtun0** to **vtun***x*, where *x* is a non-negative integer.
ipv4net	The subnet from which client IP addresses are allocated. The prefix for the subnet must be /29 or smaller.

Default

None.

Usage Guidelines

This command is used on the server side of a client-server OpenVPN connection and specifies the subnet on which the remote clients will receive IP addresses.

Use this command to specify the subnet from which client IP addresses are allocated.

Use the **set** form of this command to specify the subnet.

Use the **delete** form of this command to remove the subnet configuration.

Use the **show** form of this command to view the subnet configuration.

interfaces openvpn <vtunx> server topology <topology>

Specifies the topology to use in a client-server environment.

Syntax

set interfaces openvpn *vtunx* **server topology** *topology*

delete interfaces openvpn *vtunx* **server topology**

show interfaces openvpn *vtunx* **server topology**

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {
    openvpn vtunx {
        server {
            topology topology
        }
    }
}
```

Parameters

vtunx	The identifier for the OpenVPN interface. This may be **vtun0** to **vtun***x*, where *x* is a non-negative integer.
topology	The topology used in client-server mode. Supported values are as follows: **point-to-point**: This topology provides "client isolation" (i.e. the clients can not reach each other) but is *not* compatible with Windows clients, and routing protocols using a broadcast-style network would not work with this. **subnet**: This topology is compatible with OpenVPN clients on Windows hosts and is the default if topology is not set. Routing protocols that are configured to use a broadcast-style network should work with this topology. However, this topology does not provide "client isolation" (i.e. the clients can reach each other).

Default

The default is **subnet**.

Usage Guidelines

Use this command to specify the topology to use in a client-server environment.

Use the **set** form of this command to specify the topology.

Use the **delete** form of this command to remove the topology configuration.

Use the **show** form of this command to view the topology configuration.

interfaces openvpn <vtunx> shared-secret-key-file <filename>

Specifies the file containing a secret key shared with the remote end of the tunnel.

Syntax

set interfaces openvpn *vtunx* **shared-secret-key-file** *filename*

delete interfaces openvpn *vtunx* **shared-secret-key-file**

show interfaces openvpn *vtunx* **shared-secret-key-file**

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {
    openvpn vtunx {
        shared-secret-key-file filename
    }
}
```

Parameters

vtunx	The identifier for the OpenVPN interface. This may be **vtun0** to **vtun***x*, where *x* is a non-negative integer.
filename	The the shared secret file. The file can be generated using the **generate vpn openvpn-key** operational command, and the other endpoint must have the same file for the pre-shared secret mechanism to work.

Default

None.

Usage Guidelines

Use this command to specify the file containing a secret key shared with the remote end of the tunnel.

Certificate and key files are assumed to be in /config/auth unless an absolute path is specified.

Use the **set** form of this command to specify the file containing a secret key shared with the remote end of the tunnel.

Use the **delete** form of this command to remove the shared secret key file configuration.

Use the **show** form of this command to view the shared secret key file configuration.

interfaces openvpn <vtunx> tls

Defines a Transport Layer Security (TLS) configuration.

Syntax

set interfaces openvpn *vtunx* tls

delete interfaces openvpn *vtunx* tls

show interfaces openvpn *vtunx* tls

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {
    openvpn vtunx {
        tls {
        }
    }
}
```

Parameters

vtunx	The identifier for the OpenVPN interface. This may be **vtun0** to **vtun*x***, where *x* is a non-negative integer.

Default

None.

Usage Guidelines

Use this command to define a Transport Layer Security (TLS) configuration.

Use the **set** form of this command to create the TLS configuration node.

Use the **delete** form of this command to remove the TLS configuration node.

Use the **show** form of this command to view the TLS configuration.

interfaces openvpn <vtunx> tls ca-cert-file <filename>

Specifies the file containing the certificate authority’s certificate.

Syntax

set interfaces openvpn *vtunx* **tls ca-cert-file** *filename*

delete interfaces openvpn *vtunx* **tls ca-cert-file**

show interfaces openvpn *vtunx* **tls ca-cert-file**

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {
    openvpn vtunx {
        tls {
            ca-cert-file filename
        }
    }
}
```

Parameters

vtunx	The identifier for the OpenVPN interface. This may be **vtun0** to **vtun***x*, where *x* is a non-negative integer.
filename	The file containing the certificate authority's certificate, which will be used to validate the other endpoint's certificate.

Default

None.

Usage Guidelines

Use this command to specify the file containing the certificate authority’s certificate.

Certificate and key files are assumed to be in /config/auth unless an absolute path is specified.

Use the **set** form of this command to specify the file containing the certificate authority's certificate.

Use the **delete** form of this command to remove the pointer to the file containing the certificate authority's certificate.

Use the **show** form of this command to view the configuration.

interfaces openvpn <vtunx> tls cert-file <filename>

Specifies the file containing the endpoint’s own certificate.

Syntax

set interfaces openvpn *vtunx* **tls cert-file** *filename*

delete interfaces openvpn *vtunx* **tls cert-file**

show interfaces openvpn *vtunx* **tls cert-file**

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {
    openvpn vtunx {
        tls {
            cert-file filename
        }
    }
}
```

Parameters

vtunx	The identifier for the OpenVPN interface. This may be **vtun0** to **vtun***x*, where *x* is a non-negative integer.
filename	The file containing the endpoint's own certificate, which will be presented to the other endpoint during the TLS negotiation.

Default

None.

Usage Guidelines

Use this command to specify the file containing the endpoint’s own certificate.

Certificate and key files are assumed to be in /config/auth unless an absolute path is specified.

Use the **set** form of this command to specify the file containing the endpoint's certificate.

Use the **delete** form of this command to remove the pointer to the file containing the endpoint's certificate.

Use the **show** form of this command to view the configuration.

interfaces openvpn <vtunx> tls crl-file <filename>

Specifies the file containing a certificate revocation list.

Syntax

set interfaces openvpn *vtunx* **tls crl-file** *filename*

delete interfaces openvpn *vtunx* **tls crl-file**

show interfaces openvpn *vtunx* **tls crl-file**

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {
    openvpn vtunx {
        tls {
            crl-file filename
        }
    }
}
```

Parameters

vtunx	The identifier for the OpenVPN interface. This may be **vtun0** to **vtun***x*, where *x* is a non-negative integer.
filename	A file containing a list of certificates that have been revoked, which will prevent endpoints with these certificates from establishing a VPN tunnel. Specifying this file in the TLS configuration is optional.

Default

None.

Usage Guidelines

Use this command to specify the file containing a certificate revocation list.

The file is assumed to be located in /config/auth unless an absolute path is specified.

Use the **set** form of this command to specify the file containing a certificate revocation list.

Use the **delete** form of this command to remove the pointer to the file containing a certificate revocation list.

Use the **show** form of this command to view the configuration.

interfaces openvpn <vtunx> tls dh-file <filename>

Specifies the file containing Diffie Hellman parameters.

Syntax

set interfaces openvpn *vtunx* **tls dh-file** *filename*

delete interfaces openvpn *vtunx* **tls dh-file**

show interfaces openvpn *vtunx* **tls dh-file**

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {
    openvpn vtunx {
        tls {
            dh-file filename
        }
    }
}
```

Parameters

vtunx	The identifier for the OpenVPN interface. This may be **vtun0** to **vtun***x*, where *x* is a non-negative integer.
filename	A file containing Diffie Hellman parameters that are required **only** by the endpoint taking the passive role in the TLS negotiation.

Default

None.

Usage Guidelines

Use this command to specify the file containing Diffie Hellman parameters.

The file is assumed to be in /config/auth unless an absolute path is specified.

Use the **set** form of this command to specify the file containing Diffie Hellman parameters.

Use the **delete** form of this command to remove the pointer to the file containing Diffie Hellman parameters.

Use the **show** form of this command to view the configuration.

interfaces openvpn <vtunx> tls key-file <filename>

Specifies the file containing the endpoint's own private key.

Syntax

set interfaces openvpn *vtunx* **tls key-file** *filename*

delete interfaces openvpn *vtunx* **tls key-file**

show interfaces openvpn *vtunx* **tls key-file**

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {
    openvpn vtunx {
        tls {
            key-file filename
        }
    }
}
```

Parameters

vtunx	The identifier for the OpenVPN interface. This may be **vtun0** to **vtun***x*, where *x* is a non-negative integer.
filename	A file containing the endpoint's own private key, which is kept secret from everyone.

Default

None.

Usage Guidelines

Use this command to specify the file containing the endpoint's own private key.

The file is assumed to be in /config/auth unless an absolute path is specified.

Use the **set** form of this command to specify the file containing the endpoint's own private key.

Use the **delete** form of this command to remove the pointer to the file containing the endpoint's own private key.

Use the **show** form of this command to view the configuration.

interfaces openvpn <vtunx> tls role <role>

Specifies the TLS role the endpoint will take.

Syntax

set interfaces openvpn *vtunx* **tls role** *role*

delete interfaces openvpn *vtunx* **tls role**

show interfaces openvpn *vtunx* **tls role**

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {
    openvpn vtunx {
        tls {
            role role
        }
    }
}
```

Parameters

vtunx	The identifier for the OpenVPN interface. This may be **vtun0** to **vtun***x*, where *x* is a non-negative integer.
role	The TLS role that the endpoint will take. Supported values are as follows: **active**: The endpoint takes the active role. **passive**: The endpoint takes the passive role.

Default

None.

Usage Guidelines

Use this command to specify the TLS role the endpoint will take.

Use the **set** form of this command to specify the TLS role the endpoint will take.

Use the **delete** form of this command to remove the TLS role.

Use the **show** form of this command to view the configuration.

reset openvpn client <client-name>

Resets a client connection.

Syntax

reset openvpn client *client-name*

Command Mode

Operational mode.

Parameters

client-name	The "name" of the client. It corresponds to the "common name" contained in the client's certificate. When a client initiates the VPN session, the server uses the name in the certificate to look up and apply client-specific settings (if any). This can be determined using the show openvpn status server command.

Default

None.

Usage Guidelines

Use this command to reset the connection to a specific client. The connection to the client will be disconnected and the server will wait for the client to re-establish the connection.

NOTE *The OpenVPN process does not get restarted by this command.*

reset openvpn interface <vtunx>

Resets all tunnel connections on an OpenVPN interface.

Syntax

reset openvpn interface *vtunx*

Command Mode

Operational mode.

Parameters

vtunx	The identifier for the OpenVPN interface. This may be **vtun0** to **vtun***x*, where *x* is a non-negative integer.

Default

None.

Usage Guidelines

Use this command to to reset all tunnel connections on an OpenVPN interface. In a site-to-site environment, the connection will be re-established after it is reset. This is also the case on the client side in a client-server environment. On the server side in a client-server environment all connections are dropped. The server will then wait for the clients to re-establish the connections.

NOTE *The OpenVPN process does not get restarted by this command, though all tunnel connections are reset.*

show interfaces openvpn

Displays a status summary of all OpenVPN interfaces.

Syntax

show interfaces openvpn

Command Mode

Operational mode.

Parameters

None.

Default

None.

Usage Guidelines

Use this command to display the high level status of all OpenVPN interfaces on the system.

Examples

Example 4-27 shows the output of the **show interfaces openvpn** command.

Example 4-27 "show interfaces openvpn": Viewing OpenVPN interface status

```
vyatta@vyatta# show interfaces openvpn
Interface     IP Address          State       Link    Description
vtun0         192.168.200.1/32     up           up
vyatta@vyatta#
```

show interfaces openvpn <interface>

Displays the detailed status of an OpenVPN interface.

Syntax

show interfaces openvpn *interface*

Command Mode

Operational mode.

Parameters

interface	The OpenVPN interface name.

Default

None.

Usage Guidelines

Use this command to display detailed status of an OpenVPN interface.

Examples

Example 4-28 shows the output of the **show interfaces openvpn <interface>** command.

Example 4-28 “show interfaces openvpn vtun0”: Viewing OpenVPN interface status

```
vyatta@vyatta# show interfaces openvpn vtun0
vtun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state
UNKNOWN qlen 100
    link/[65534]
    inet 192.168.200.1 peer 192.168.200.2/32 scope global vtun0

    RX:  bytes    packets     errors     dropped     overrun       mcast
          1216         16          0           0           0           0
    TX:  bytes    packets     errors     dropped     carrier collisions
             0          0          0           0           0           0
vyatta@vyatta#
```

show interfaces openvpn <interface> brief

Displays the status summary of an OpenVPN interface.

Syntax

show interfaces openvpn *interface* **brief**

Command Mode

Operational mode.

Parameters

interface	The OpenVPN interface name.

Default

None.

Usage Guidelines

Use this command to display a status summary of an OpenVPN interface.

Examples

Example 4-29 shows the output of the **show interfaces openvpn <interface> brief** command.

Example 4-29 “show interfaces openvpn vtun0 brief”: Viewing OpenVPN interface status

```
vyatta@vyatta# show interfaces openvpn vtun0 brief
Interface     IP Address          State       Link   Description
vtun0         192.168.200.1/32     up          up
vyatta@vyatta#
```

show interfaces openvpn <interface> capture

Captures data passing through the OpenVPN interface.

Syntax

show interfaces openvpn *interface* **capture**

Command Mode

Operational mode.

Parameters

interface	The OpenVPN interface name.

Default

None.

Usage Guidelines

Use this command to capture data passing through an OpenVPN interface.

Examples

Example 4-30 shows the output of the **show interfaces openvpn <interface> capture** command.

Example 4-30 “show interfaces openvpn vtun0 capture”: Capturing OpenVPN interface traffic

```
vyatta@vyatta# show interfaces openvpn vtun0 capture
Capturing traffic on vtun0 ...
```

show interfaces openvpn detail

Displays the detailed status of all OpenVPN interfaces on the system.

Syntax

show interfaces openvpn detail

Command Mode

Operational mode.

Parameters

None.

Default

None.

Usage Guidelines

Use this command to display detailed status of all OpenVPN interfaces on the system.

Examples

Example 4-31 shows the output of the **show interfaces openvpn detail** command.

Example 4-31 “show interfaces openvpn detail”: Viewing OpenVPN interface status

```
vyatta@vyatta# show interfaces openvpn detail
vtun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state
UNKNOWN qlen 100
    link/[65534]
    inet 192.168.200.1 peer 192.168.200.2/32 scope global vtun0

    RX:  bytes    packets     errors     dropped     overrun      mcast
          1216         16          0           0           0          0
    TX:  bytes    packets     errors     dropped     carrier collisions
             0          0          0           0           0          0
vyatta@vyatta#
```

show openvpn status client

Displays information on OpenVPN connections in client mode.

Syntax

show openvpn status client

Command Mode

Operational mode.

Parameters

None.

Default

None.

Usage Guidelines

Use this command to display information on all OpenVPN client mode connections. This command is only available on a client-mode endpoint.

Examples

Example 4-32 shows the output of the **show openvpn status client** command.

Example 4-32 “show openvpn status client”: Viewing OpenVPN client status

```
vyatta@vyatta:~$ show openvpn status client
OpenVPN client status on vtun2 [openvpn client]

Server CN       Remote IP       Tunnel IP       TX byte RX byte Connected Since
--------------- --------------- --------------- ------- ------- ----------------------
N/A             172.16.117.128  N/A                6.8K    8.1K N/A

vyatta@vyatta:~$
```

show openvpn status server

Displays information on connected clients in server mode.

Syntax

show openvpn status server

Command Mode

Operational mode.

Parameters

None.

Default

None.

Usage Guidelines

Use this command to display information on all connected clients. This command is only available on a server-mode endpoint. Also, note that the command output is not updated in real time. The time it was last updated is displayed.

Examples

Example 4-33 shows the output of the **show openvpn status server** command.

Example 4-33 "show openvpn status server": Viewing OpenVPN server status

```
vyatta@vyatta:~$ show openvpn status server
OpenVPN server status on vtun0 (last updated on Wed Oct 29 22:34:18 2008)

Client          Remote IP       Tunnel IP       TX byte RX byte Connected Since
--------------- --------------- --------------- ------- ------- ----------------
vclient1        192.168.252.3   192.168.200.4   16.0K   16.5K   Wed Oct 29 21:59:50 2008
vyatta@vyatta:~$
```

show openvpn status site-to-site

Displays information on OpenVPN connections in site-to-site mode.

Syntax

show openvpn status site-to-site

Command Mode

Operational mode.

Parameters

None.

Default

None.

Usage Guidelines

Use this command to display information on all connected sites. This command is only available on a site-to-site-mode endpoint.

Examples

Example 4-34 shows the output of the **show openvpn status site-to-site** command.

Example 4-34 "show openvpn status site-to-site": Viewing OpenVPN site-to-site status

```
vyatta@vyatta:~$ show openvpn status site-to-site
OpenVPN client status on vtun1 [openvpn with psk]

Remote CN       Remote IP       Tunnel IP       TX byte RX byte Connected Since
--------------- --------------- --------------- ------- ------- ----------------------
None (PSK)      192.168.74.160  192.168.2.2        8.9K    8.8K N/A

OpenVPN client status on vtun0 [openvpn with tls]

Remote CN       Remote IP       Tunnel IP       TX byte RX byte Connected Since
--------------- --------------- --------------- ------- ------- ----------------------
N/A             192.168.74.160  192.168.1.2       17.5K   15.1K N/A
```

```
vyatta@vyatta:~$
```

Glossary of Acronyms

ACL	access control list
ADSL	Asymmetric Digital Subscriber Line
API	Application Programming Interface
AS	autonomous system
ARP	Address Resolution Protocol
BGP	Border Gateway Protocol
BIOS	Basic Input Output System
BPDU	Bridge Protocol Data Unit
CA	certificate authority
CCMP	AES in counter mode with CBC-MAC
CHAP	Challenge Handshake Authentication Protocol
CLI	command-line interface
DDNS	dynamic DNS
DHCP	Dynamic Host Configuration Protocol
DHCPv6	Dynamic Host Configuration Protocol version 6
DLCI	data-link connection identifier
DMI	desktop management interface

DMZ	demilitarized zone
DN	distinguished name
DNS	Domain Name System
DSCP	Differentiated Services Code Point
DSL	Digital Subscriber Line
eBGP	external BGP
EGP	Exterior Gateway Protocol
ECMP	equal-cost multipath
ESP	Encapsulating Security Payload
FIB	Forwarding Information Base
FTP	File Transfer Protocol
GRE	Generic Routing Encapsulation
HDLC	High-Level Data Link Control
I/O	Input/Ouput
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IGP	Interior Gateway Protocol
IPS	Intrusion Protection System
IKE	Internet Key Exchange
IP	Internet Protocol
IPOA	IP over ATM
IPsec	IP security
IPv4	IP Version 4
IPv6	IP Version 6
ISP	Internet Service Provider

L2TP	Layer 2 Tunneling Protocol
LACP	Link Aggregation Control Protocol
LAN	local area network
LDAP	Lightweight Directory Access Protocol
LLDP	Link Layer Discovery Protocol
MAC	medium access control
MIB	Management Information Base
MLPPP	multilink PPP
MRRU	maximum received reconstructed unit
MTU	maximum transmission unit
NAT	Network Address Translation
ND	Neighbor Discovery
NIC	network interface card
NTP	Network Time Protocol
OSPF	Open Shortest Path First
OSPFv2	OSPF Version 2
OSPFv3	OSPF Version 3
PAM	Pluggable Authentication Module
PAP	Password Authentication Protocol
PAT	Port Address Translation
PCI	peripheral component interconnect
PKI	Public Key Infrastructure
PPP	Point-to-Point Protocol
PPPoA	PPP over ATM
PPPoE	PPP over Ethernet
PPTP	Point-to-Point Tunneling Protocol

PVC	permanent virtual circuit
QoS	quality of service
RADIUS	Remote Authentication Dial-In User Service
RIB	Routing Information Base
RIP	Routing Information Protocol
RIPng	RIP next generation
Rx	receive
SLAAC	Stateless Address Auto-Configuration
SNMP	Simple Network Management Protocol
SMTP	Simple Mail Transfer Protocol
SONET	Synchronous Optical Network
SSH	Secure Shell
SSID	Service Set Identifier
STP	Spanning Tree Protocol
TACACS+	Terminal Access Controller Access Control System Plus
TCP	Transmission Control Protocol
TKIP	Temporal Key Integrity Protocol
ToS	Type of Service
Tx	transmit
UDP	User Datagram Protocol
vif	virtual interface
VLAN	virtual LAN
VPN	Virtual Private Network
VRRP	Virtual Router Redundancy Protocol
WAN	wide area network
WAP	wireless access point

WPA	Wired Protected Access