# Working with VPN Service

# 6

## This chapter describes how to set up and manage VPN service in Mac OS X Server.

By configuring a Virtual Private Network (VPN) on your server you can give users a more secure way of remotely communicating with computers on your network.

This chapter describes the VPN authentication method and transport protocols and explains how to configure, manage, and monitor VPN service. It does not include information for configuring VPN clients to use your VPN server.

A VPN consists of two or more computers or networks (nodes) connected by a private link of encrypted data. This link simulates a local connection, as if the remote computer were attached to the local area network (LAN).

VPNs securely connect users working away from the office (for example, at home) to the LAN through a connection such as the Internet. From the user's perspective, the VPN connection appears as a dedicated private link.

VPN technology can also connect an organization to branch offices over the Internet while maintaining secure communications. The VPN connection across the Internet acts as a wide area network (WAN) link between the sites.

VPNs have several advantages for organizations whose computer resources are physically separated. For example, each remote user or node uses the network resources of its Internet Service Provider (ISP) rather than having a direct, wired link to the main location.

VPNs can permit verified mobile users to access private computer resources (file servers and so on) using any connection to the Internet. VPNs can also link multiple LANs together over great distances using the existing Internet infrastructure.

## VPN and Security

VPNs stress security by requiring strong authentication of identity and encrypted data transport between the nodes for data privacy and dependability. The following section contains information about each supported transport and authentication method.

### Transport Protocols

There are two encrypted transport protocols:  Layer Two Tunneling Protocol, Secure Internet Protocol (L2TP/IPSec) and Point–to–Point Tunneling Protocol (PPTP). You can enable either or both of these protocols. Each has its own strengths and requirements.

**L2TP/IPSec**

L2TP/IPSec uses strong IPSec encryption to tunnel data to and from network nodes. It is based on Cisco's L2F protocol.

IPSec requires security certificates (either self-signed or signed by a certificate authority such as Verisign) or a predefined shared secret between connecting nodes.

The shared secret must be entered on the server and the client.

The shared secret is not a password for authentication, nor does it generate encryption keys to establish secure tunnels between nodes. It is a token that the key management systems use to trust each other.

L2TP is Mac OS X Server's preferred VPN protocol because it has superior transport encryption and can be authenticated using Kerberos.

**PPTP**

PPTP is a commonly used Windows standard VPN protocol. PPTP offers good encryption (if strong passwords are used) and supports a number of authentication schemes. It uses the user-provided password to produce an encryption key.

By default, PPTP supports 128-bit (strong) encryption. PPTP also supports the 40-bit (weak) security encryption.

PPTP is necessary if you have Windows clients with versions earlier than Windows XP or if you have Mac OS X v10.2.x clients or earlier.

### Authentication Method

Mac OS X Server L2TP VPN uses Kerberos v5 or Microsoft's Challenge Handshake Authentication Protocol version 2 (MS-CHAPv2) for authentication. Mac OS X Server PPTP VPN exclusively uses MS-CHAPv2 for authentication.

Kerberos is a secure authentication protocol that uses a Kerberos Key Distribution Server as a trusted third party to authenticate a client to a server.

MS-CHAPv2 authentication encodes passwords when they're sent over the network, and stores them in a scrambled form on the server. This method offers good security during network transmission. It is also the standard Windows authentication scheme for VPN.

Mac OS X Server PPTP VPN can also use other authentication methods. Each method has its own strengths and requirements. These other authentication methods for PPTP are not available in Server Admin.

If you want to use an alternative authentication scheme (for example, to use RSA Security's SecurID authentication), you must edit the VPN configuration file manually. The configuration file is located at /Library/Preferences/SystemConfiguration/com.apple.RemoteAccessServers.plist

For more information, see "Offering SecurID Authentication with VPN Server" on page 138.

### Using VPN Service with Users in a Third-Party LDAP Domain

To use VPN service for users in a third-party LDAP domain (an Active Directory or Linux OpenLDAP domain), you must be able to use Kerberos authentication. If you need to use MSCHAPv2 to authenticate users, you can't offer VPN service for users in a third-party LDAP domain.

## Before You Set Up VPN Service

Before setting up VPN service, determine which transport protocol you're going to use. The table below shows which protocols are supported by different platforms.

| If you have | You can use L2TP/IPSec | You can use PPTP |
|---|---|---|
| Mac OS X v10.5 and v10.4.x clients | X | X |
| Mac OS X v10.3.x clients | X | X |
| Mac OS X v10.2.x clients | | X |
| Windows clients | X (if Windows XP) | X |
| Linux or Unix clients | X | X |

If you're using L2TP, you must have a Security Certificate (from a certificate authority or self-signed), or a predefined shared secret between connecting nodes. If you use a shared secret, it must also be secure (at least 8 alphanumeric characters, including punctuation and without spaces; preferably 12 or more) and kept secret by users.

If you're using PPTP, make sure all your clients support 128-bit PPTP connections for greatest transport security. Using only 40-bit transport security is a serious security risk.

## Configuring Other Network Services for VPN

Enabling VPN on Mac OS X Server requires detailed control of DHCP. DHCP is configured separately in Server Admin. The IP addresses given to VPN clients cannot overlap with addresses given to local DHCP clients. To learn more about DHCP, see Chapter 2, "Working with DHCP Service," on page 25.

Enabling VPN also requires Firewall services to be configured. The firewall settings must be able to pass network traffic from external IP addresses through the firewall to the LAN. The firewall settings can be as open or restricted as necessary.

For example, if your VPN clients use a large range of IP addresses (you have many users, each connecting from different ISPs) you might need to open the "any" firewall address group to VPN connections.

If you want to narrow access to a small range of IP addresses, including static ones, you can create an address group that reflects that smaller range, and only enable VPN traffic originating from that list. You must also open the relevant firewall ports for the VPN type you are using (L2TP or PPTP).

Further, a VPN using L2TP must permit traffic for VPN clients on UDP port 4500 (IKE NAT Traversal) if you are using a NAT gateway.

Your specific network configuration can also require other open ports.

## Setup Overview

Here is an overview of the steps for setting up print service:

**Step 1: Before you begin**
For information to keep in mind before you setup VPN service, read "Before You Set Up VPN Service" on page 127 and "Configuring Other Network Services for VPN" on page 128.

**Step 2: Turn VPN service on**
Before configuring VPN service, you must turn it on. See "Turning VPN Service On" on page 129.

**Step 3: Configure VPN L2TP settings**
Use Server Admin to enable L2TP over IPSec, set the IP address allocation range, and set the shared secret or security certificate. See "Configuring L2TP Settings" on page 129.

**Step 4: Configure VPN PPTP settings**
Use Server Admin to enable PPTP to specify, encryption key length, and to specify the IP address allocation range. See "Configuring PPTP Settings" on page 131.

**Step 5: Configure VPN Logging settings**
Use the Logging settings to enable VPN verbose logging. See "Configuring Logging Settings" on page 132.

**Step 6: Configure VPN Client Information settings**
Use Server Admin to configure network settings for VPN clients. See "Configuring Client Information Settings" on page 132.

## Turning VPN Service On

Before you can configure VPN service, you must turn the VPN service on in Server Admin.

**To turn VPN service on:**

1. Open Server Admin and connect to the server.
2. Click Settings, then click Services.
3. Click the VPN checkbox.
4. Click Save.

## Setting Up VPN Service

There are two groups of settings for VPN service in Server Admin:

- **Connections.** Shows you information about users who are connected using VPN.
- **Settings.** Configures and manages L2TP and PPTP VPN service connections.

The following sections describe how to configure these settings. A final section explains how to start VPN service after you set up VPN.

### Configuring L2TP Settings

Use Server Admin to designate L2TP as the transport protocol.

If you enable this protocol, you must also configure the connection settings. You must designate an IPSec shared secret (if you don't use a signed security certificate), the IP address allocation range to be given to your clients, and the group that will use the VPN service (if needed).

If both L2TP and PPTP are used, each protocol should have a separate, nonoverlapping address range.

When configuring VPN, make sure the firewall allows VPN traffic on needed ports with the following settings:

- For the "any" address group, enable GRE, ESP, VPN L2TP (port 1701), and VPN ISAKMP/IKE (port 500).
- For the "192.168-net" address group, choose to allow all traffic.

For more information, see "Configuring Services Settings" on page 88.

**To configure L2TP settings:**

1. Open Server Admin and connect to the server.
2. Click the triangle to the left of the server.

   The list of servers appears.
3. From the expanded Servers list, select VPN.
4. Click Settings, then click L2TP.
5. Select the "Enable L2TP over IPSec" checkbox.
6. In the "Starting IP address" field set the beginning IP address of the VPN allocation range.

   It can't overlap the DHCP allocation range, so enter 192.168.0.128.
7. In the "Ending IP address" field set the ending IP address of the VPN allocation range.

   It can't overlap the DHCP allocation range, so enter 192.168.0.255.
8. (Optional) You can load-balance VPN by selecting the Enable Load Balancing checkbox and entering an IP address in the Cluster IP address field.
9. Choose a PPP authentication type.

   If you choose Directory Service and your computer is bound to a Kerberos authentication server, from the Authentication pop-up menu select Kerberos. Otherwise, choose MS-CHAPv2.

   If you choose RADIUS, enter the following information:

   **Primary IP Address:** Enter the IP address of the primary RADIUS server.

   **Shared Secret:** Enter a shared secret for the primary RADIUS server.

   **Secondary IP Address:** Enter the IP address of the secondary RADIUS server.

   **Shared Secret:** Enter a shared secret for the secondary RADIUS server.
10. Enter the shared secret or select the certificate to use in the IPSec Authentication section.

    The shared secret is a common password that authenticates members of the cluster. IPSec uses the shared secret as a preshared key to establish secure tunnels between the cluster nodes.
11. Click Save.

## Configuring PPTP Settings

Use Server Admin to designate PPTP as the transport protocol.

If you enable this protocol, you must also configure connection settings. You should designate an encryption key length (40-bit or 128-bit), the IP address allocation range to be given to your clients, and the group that will use the VPN service (if needed).

If you use L2TP and PPTP, each protocol should have a separate, nonoverlapping address range.

When configuring VPN, make sure the firewall allows VPN traffic on needed ports with the following settings:

- For the "any" address group, enable GRE, ESP, VPN L2TP (port 1701), and IKE (port 500).
- For the "192.168-net" address group, choose to allow all traffic.

For more information, see "Configuring Services Settings" on page 88.

**To configure PPTP settings:**

1. Open Server Admin and connect to the server.
2. Click the triangle to the left of the server.

   The list of servers appears.
3. From the expanded Servers list, select VPN.
4. Click Settings, then click PPTP.
5. Select "Enable PPTP."
6. If needed, select "Allow 40-bit encryption keys in addition to 128-bit" to permit both 40-bit and 128-bit key encryption access to VPN.

   > *WARNING:* 40-bit encryption keys are much less secure but can be necessary for some VPN client applications.

7. In the "Starting IP address" field set the beginning IP address of the VPN allocation range.

   It can't overlap the DHCP allocation range, so enter 192.168.0.128.
8. In the "Ending IP address" field set the ending IP address of the VPN allocation range.

   It can't overlap the DHCP allocation range, so enter 192.168.0.255.
9. Choose a PPP authentication type.

   If you choose Directory Service and your computer is bound to a Kerberos authentication server, from the Authentication pop-up menu select Kerberos. Otherwise, choose MS-CHAPv2.

If you choose RADIUS, enter the following information:

**Primary IP Address:** Enter the IP address of the primary RADIUS server.

**Shared Secret:** Enter a shared secret for the primary RADIUS server.

**Secondary IP Address:** Enter the IP address of the secondary RADIUS server.

**Shared Secret:** Enter a shared secret for the secondary RADIUS server.

10 Click Save.

## Configuring Client Information Settings

When a user connects to your server through VPN, that user is given an IP address from your allocated range. This range is not served by a DHCP server, so you must configure the network mask, DNS address, and search domains.

**To configure Client Information settings:**

1 Open Server Admin and connect to the server.

2 Click the triangle to the left of the server.

The list of servers appears.

3 From the expanded Servers list, select VPN.

4 Click Settings, then click Client Information.

5 Enter the IP address of the DNS server.

Add the gateway computer's internal IP address (usually something like 192.168.x.1).

6 Enter search domains as needed.

7 Click Save.

## Configuring Logging Settings

You can choose from two levels of detail for VPN service logs.

- **Nonverbose logs:** Describe conditions where you must take immediate action (for example, if the VPN service can't start up).
- **Verbose logs:** Record all activity by the VPN service, including routine functions.

By default, nonverbose logging is enabled.

**To change logging settings to verbose:**

1 Open Server Admin and connect to the server.

2 Click the triangle to the left of the server.

The list of servers appears.

3 From the expanded Servers list, select VPN.

4 Click Settings, then click Logging.

5 Select "Verbose logging" to enable verbose logging.

6 Click Save.

## Starting VPN Service

You use Server Admin to start VPN service.

**To start VPN service:**

1 Open Server Admin and connect to the server.

2 Click the triangle to the left of the server.

The list of servers appears.

3 From the expanded Servers list, select VPN.

4 Click the Start VPN button below the Servers list.

Click Settings, then click L2TP or PPTP and verify that the "Enable L2TP over IPsec" or "Enable PPTP" checkbox is selected.

## Managing VPN Service

This section describes tasks associated with managing VPN service. It includes starting, stopping, and configuring the service.

### Stopping VPN Service

You use Server Admin to stop VPN service.

**To stop VPN service:**

1 Open Server Admin and connect to the server.

2 Click the triangle to the left of the server.

The list of servers appears.

3 From the expanded Servers list, select VPN.

4 Click the Stop VPN button below the Servers list.

### Configuring VPN Network Routing Definitions

By using network routing definitions, you can choose whether to route data from VPN clients to an address group through the VPN tunnel (referred to as *private*) or over the VPN user's ISP connection (referred to as *public*).

For example, you can have all VPN client traffic that goes to the LAN IP address range go through the secure tunnel to the LAN, but make all traffic to other addresses be routed through the user's normal, unsecured Internet connection.

This helps you have greater control over what goes through the VPN tunnel.

### Important Notes About VPN Routing Definitions

- If no routing definitions are added, traffic is routed through the VPN connection by default.
- If routing definitions are added, the VPN connection is no longer set as the default route, and traffic destined for addresses not specifically declared as a private route will not go over the VPN connection.
- DNS lookups go over the VPN connection regardless of the routes that are set.
- Definitions are unordered. They only apply the description that most closely matches the packet being routed.

### Example

Suppose your LAN's IP addresses are 17.x.x.x addresses. If you make no routing definitions, every VPN client's network traffic (such as web browser URL requests, LPR printer queue print jobs, and file server browsing) is routed from the client computer through the VPN tunnel to the 17.x.x.x LAN.

You decide that you don't want to manage all traffic to web sites or file servers that aren't located on your network. You can restrict what traffic gets sent to the 17.x.x.x network, and what goes through the client computer's normal Internet connection.

To limit the traffic the VPN tunnel handles, enter a routing definition designating traffic to the 17.x.x.x network as private, which sends it through the VPN tunnel. In the routing definition table you'd enter 17.0.0.0 255.0.0.0 Private.

All traffic to the LAN is now sent over the VPN connection and, by default, all other addresses not in the definitions table are sent over the client computer's unencrypted Internet connection.

You then decide that there are a few IP addresses in the 17.x.x.x range that you don't want accessed over the VPN connection. You want the traffic to go through the client computer's Internet connection and not pass through the VPN tunnel. The addresses might be outside the firewall and not accessible from the 17.x.x.x LAN.

As an example, if you want to use addresses in the range 17.100.100.x, you would enter an extra routing definition as follows: 17.100.100.0 255.255.255.0 Public.

Because the address definition is more specific than 17.x.x.x, this rule takes precedence over the broader, more general rule, and traffic heading to any address in the 17.100.100.x range is sent through the client computer's Internet connection.

In summary, if you add routes, any routes you specify as private go over the VPN connection, and any declared as public do not go over the VPN connection. All others not specified also do not go over the VPN connection.

**To set routing definitions:**

1. Open Server Admin and connect to the server.
2. Click the triangle to the left of the server.

   The list of servers appears.
3. From the expanded Servers list, select VPN.
4. Click Settings, then click Client Information.
5. Click the Add (+) button.
6. Enter a destination address range of the packets to be routed by specifying:

   A base address (for example, 192.168.0.0)

   A network mask (for example, 255.255.0.0)
7. From the Type pop-up menu, select the routing destination.

   *Private* means to route client traffic through the VPN tunnel.

   *Public* means to use the normal interface with no tunnel.
8. Click OK.
9. Click Save.

## Limiting VPN Access to Specific Users or Groups

By default, all users on the server or in the master directory have access to the VPN when it is enabled. You can limit VPN access to specific users for security or ease of administration. You can limit access to VPN by using Mac OS X Server's Access Control List (ACL) feature.

ACLs allow you to designate service access to users or groups on an individual basis. For example, you can use an ACL to permit a user to access a specific file server or shell login, while denying access to all other users on the server.

**To limit VPN access using ACLs:**

1. Open Server Admin and connect to the server.
2. Click Settings, then click Access.
3. Click Services.
4. Select "For selected services below."
5. In the service access list, select VPN.
6. Select "Allow only users and group below."
7. To reveal a Users and Groups drawer, click the Add (+) button.
8. Drag users or groups to the access list.
9. Click Save.

## Limiting VPN Access to Specific Incoming IP Addresses

By default, Firewall service blocks incoming VPN connections, but you can provide limited VPN access to certain IP addresses for security or ease of administration.

You can limit access to the VPN by using Mac OS X Server's Firewall service. When configuring the firewall for L2TP and PPTP you must configure GRE, ESP, and IKE to permit VPN access through the firewall.

**To limit VPN access by IP address:**

1. Open Server Admin and connect to the server.
2. Click the triangle to the left of the server.

   The list of services appears.
3. From the expanded Servers list, select Firewall.
4. Click Settings.
5. Select Advanced, then click the Add (+) button.
6. From the Action pop-up menu, choose "Allow."
7. From the Protocol pop-up menu, choose an option.

   If you use L2TP for VPN access, choose UDP.

   If you use PPTP for VPN access, choose TCP.
8. From the Service pop-up menu, choose VPN L2TP or VPN PPTP.

   The relevant destination port is added to the Port field.
9. (Optional) Select the "Log all packets matching this rule" checkbox.
10. From the address pop-up menu of the Source section, choose Other and enter the source IP address range (using CIDR notation) that you want to give access to VPN.

    You can also specify a port in the Port field of the Source section.

    Computers that have an IP address in the IP address range that you specified in the source IP address field, communicating on the source port you specified, can connect to the VPN service.
11. From the Destination Address pop-up menu, choose the address group that contains the VPN server (for the destination of filtered traffic).

    If you don't want to use an existing address group, enter the destination IP address range (with CIDR notation).
12. From the Interface pop-up menu that this rule applies to, choose "In."

    "In" refers to the packets coming into the server.
13. Click OK.
14. Click the Add (+) button.
15. From the Action pop-up menu, choose "Allow."

16 From the Protocol pop-up menu, choose a protocol or Other.

If you are adding GRE or ESP, choose Other and enter "any" in the field.

If you are adding VPN ISAKMP/IKE, choose UDP.

17 From the Service pop-up menu, choose a service.

If you are adding GRE, choose "GRE - Generic Routing Encapsulation protocol."

If you are adding ESP, choose "ESP - Encapsulating Security Payload protocol."

If you are adding VPN ISAKMP/IKE, choose "VPN ISAKMP/IKE." Destination port 500 is added to the Port field.

18 From the Address pop-up menu of the Source section, choose "any."

19 In the Port field of the Source section, enter "any."

20 From the Address pop-up menu of the Destination section, choose "any."

21 In the Port field of the Destination section, enter a port number.

If you are adding VPN ISAKMP/IKE, enter 500 if it is not already shown.

22 From the Interface pop-up menu, choose "Other" and enter "any" in the Other field of the Interface section.

23 Click OK.

24 Repeat steps 14 through 23 for GRE, ESP, and VPN ISAKMP/IKE.

25 Click Save to apply the filter immediately.

## Supplementary Configuration Instructions

The following section describes procedures for optional scenarios. They require integration with an existing directory service or with third-party authentication services.

### Enabling VPN-PPTP Access for Users in an LDAP Domain

In Mac OS X v10.5, you can use a command-line tool to enable PPTP-VPN connections for users in an LDAP domain.

This resolves a situation where users can establish a VPN connection using PPTP to a Mac OS X Server that, when established, is not used by network traffic. This situation affects Mac OS X Server v10.3, v10.4, and v10.5.

**To enable VPN-PPTP access for users in an LDAP domain:**

1. Run the tool `/usr/sbin/vpnaddkeyagentuser` as root, with the LDAP node (directory where users are present) name as the argument.

   For example, if the server running the VPN service is the LDAP master, enter the following command in Terminal:

   ```
   $ sudo /usr/sbin/vpnaddkeyagentuser /LDAPv3/127.0.0.1
   ```

   If the server running the VPN service is not an LDAP master and the LDAP directory is on a different computer, use the IP address of the LDAP server in the command.

   For example, if the LDAP server address is 17.221.67.87, enter the following command in Terminal:

   ```
   $ sudo /usr/sbin/vpnaddkeyagentuser /LDAPv3/17.221.67.87
   ```

2. When prompted, enter the username and password.

   If the VPN server is the LDAP master, enter the administrator name and password of the server.

   If the LDAP directory is on a different server, enter the administrator name and password of the server that hosts the LDAP directory (or the administrator name and password used to add users to the LDAP directory in Workgroup Manager).

   The tool adds a user to the LDAP directory and sets up configuration elements in the VPN Server so it can support PPTP.

3. In the VPN Service Settings pane of Server Admin, configure PPTP.

4. Start VPN Service.

### Offering SecurID Authentication with VPN Server

RSA Security provides strong authentication. It uses hardware and software tokens to verify user identity. SecurID authentication is available for L2TP and PPTP transports. For details and product offerings, see www.rsasecurity.com.

VPN service supports SecurID authentication but it cannot be set up from Server Admin. If you choose this authentication tool, you must change the VPN configuration manually.

**Set up SecurID:**

1. From your SecurID server, copy the sdconf.rec file to a new folder on your Mac OS X Server named /var/ace.

   There are several ways to do this. The following illustrates one method:

   a. Open Terminal (/Applications/Utilities/).

   b. Enter `sudo mkdir /var/ace`.

   c. Enter your administrator password.

   d. In the Dock, click Finder.

   e. From the Go menu, choose Go > Go to Folder.

f Enter: `/var/ace`.

g Click Go.

h From your SecurID server, copy the sdconf.rec file into the "ace" folder.

i If you see a dialog indicating that the "ace" folder cannot be modified, click Authenticate to permit the copy.

2 Enable EAP-SecurID authentication on your VPN service for the protocols you want to use it with.

To use it with PPTP, enter these two commands in Terminal (each only one line):

```
# sudo serveradmin settings
     vpn:Servers:com.apple.ppp.pptp:PPP:AuthenticatorEAPPlugins:_array_index
     : 0 = "EAP-RSA"
# sudo serveradmin settings
     vpn:Servers:com.apple.ppp.pptp:PPP:AuthenticatorProtocol:_array_index:0
     = "EAP"
```

To use it with L2TP, enter these two commands in Terminal (each only one line):

```
# sudo serveradmin settings
     vpn:Servers:com.apple.ppp.l2tp:PPP:AuthenticatorEAPPlugins:_array_index
     : 0 = "EAP-RSA"
# sudo serveradmin settings
     vpn:Servers:com.apple.ppp.l2tp:PPP:AuthenticatorProtocol:_array_index:0
     = "EAP"
```

3 Complete the remaining VPN service configuration tasks using Server Admin.

## Monitoring VPN Service

This section describes tasks associated with monitoring a functioning VPN service. It includes accessing status reports, setting logging options, viewing logs, and monitoring connections.

### Viewing a VPN Status Overview

The VPN Overview gives you a quick status report for enabled VPN services. It tells you how many L2TP and PPTP clients are connected, which authentication method is selected, and when the service was started.

**To view the overview:**

1 Open Server Admin and connect to the server.

2 Click the triangle to the left of the server.

The list of servers appears.

3 From the expanded Servers list, select VPN.

4 Click Overview.

## Changing the Log Detail Level for VPN Service

You can choose from two levels of detail for VPN service logs:

- **Nonverbose**: These logs describe only conditions where you must take immediate action (for example, if the VPN service can't start up).
- **Verbose**: These logs record all activity by the VPN service, including routine functions.

By default nonverbose logging is enabled.

**To change the VPN log detail to verbose:**

1. Open Server Admin and connect to the server.
2. Click the triangle to the left of the server.

   The list of servers appears.
3. From the expanded Servers list, select VPN.
4. Click Settings, then click Logging.
5. Select "Verbose logging" to enable verbose logging.
6. Click Save.

## Viewing the VPN Log

Monitoring VPN logs helps you make sure your VPN is running properly. VPN logs can help you troubleshoot problems. The log view shows the contents of the /var/log/ppp/vpnd.log file. You can filter the log records with the text filter box in the Log pane of VPN.

**To view the log:**

1. Open Server Admin and connect to the server.
2. Click the triangle to the left of the server.

   The list of servers appears.
3. From the expanded Servers list, select VPN.
4. Click Log.

## Viewing VPN Client Connections

You can monitor VPN client connections to maintain secure access to the VPN. By viewing the client connection screen, you can see:

- Users connected
- IP address users are connecting from
- IP address your network assigned to users
- Type and duration of connections

You can sort the list by clicking the column headers.

**To view client connections:**

1. Open Server Admin and connect to the server.
2. Click the triangle to the left of the server.

   The list of servers appears.
3. From the expanded Servers list, select VPN.
4. Click Connections.

## Common Network Administration Tasks That Use VPN

The following sections describe common network administration tasks that use VPN service.

### Linking a Computer at Home with a Remote Network

You can use VPN to link a computer to a remote network, giving you access to it as if it were physically connected to the LAN. The following is an example of a linked computer configuration:

- **User authentication**: The user can authenticate with a name and password.
- **Desired VPN type**: L2TP
- **Shared secret**: prDwkj49fd!254
- **Internet or public IP address of the VPN gateway**: gateway.example.com
- **Private network IP address range and netmask**: 192.168.0.0–192.168.0.255 (also expressed as192.168.0.0/24 or 192.168.0.0:255.255.255.0)
- **DHCP starting and ending addresses**: 192.168.0.3–192.168.0.127
- **Private network's DNS IP address**: 192.168.0.2

The result of this configuration is a VPN client that can connect to a remote LAN using L2TP, with full access rights.

**Step 1: Configure VPN**

1. Open Server Admin and connect to the server.
2. Click the triangle to the left of the server.

   The list of servers appears.
3. From the expanded Servers list, select VPN.
4. Click Settings, then click L2TP.
5. Enable L2TP over IPsec.
6. In the "Starting IP address" field set the beginning IP address of the VPN allocation range.

   It can't overlap the DHCP allocation range, so enter 192.168.0.128.

7 In the "Ending IP address" field set the ending IP address of the VPN allocation range.

It can't overlap the DHCP allocation range, so enter 192.168.0.255.

8 In the IPSec Authentication section enter the shared secret (prDwkj49fd!254).

The shared secret is a common password that authenticates members of the cluster. IPSec uses the shared secret as a preshared key to establish secure tunnels between the cluster nodes.

9 Click Save.

10 Click Client Information.

11 Enter the IP address of the internal LAN DNS server (192.168.0.2).

12 Leave routing definitions empty.

All traffic from the client will go through the VPN tunnel.

13 Click Save.

14 Click Start VPN below the Servers list.

**Step 2: Configure the firewall**

1 Create an address group for the VPN allocation range.

For more information, see "Creating an Address Group" on page 90.

2 Open the firewall to external VPN connections by enabling L2TP connections in the "any" address group.

For more information, see "Configuring Services Settings" on page 88.

3 Configure the firewall for the VPN address group, permitting or denying ports and services as needed.

4 Save your changes.

5 Start or restart the firewall.

**Step 3: Configure the client**

This example is of a Mac OS X client using Network preferences.

1 Open System Preferences, then click Network.

2 Click the Add (+) button at the bottom of the network connection services list and then choose VPN from the Interface pop-up menu.

3 From the VPN Type pop-up menu, choose "L2TP over IPSec".

4 Enter a VPN service name in the Service Name field, then click Create.

5 Enter the DNS name or IP address in the Server Address field.

**Server Address**: gateway.example.com

**Account Name**: *<the user's short name>*

6 Click Authentication Settings and enter the following configuration information:

**User Authentication**: Use Password *<user's password>*

**Machine Authentication:** Use Shared Secret <prDwkj49fd!254>

7 Click OK.

The user can now connect.

## Accessing a Computing Asset Behind a Remote Network Firewall

Accessing a single computing asset behind a firewall differs from permitting a client computer to become a node on the remote network.

In the previous example, the VPN user's computer becomes a full participant in the remote LAN. In this scenario, the asset to be accessed is a single file server, with the VPN user's computer having no other contact with the remote LAN.

This scenario assumes information in the section "Linking a Computer at Home with a Remote Network" on page 141, and adds:

- **File server IP address**: 192.168.0.15
- **File server type**: Apple File Sharing

For this scenario, the procedure is similar to that use for "Linking a Computer at Home with a Remote Network" on page 141, with these exceptions:

- In Step 1, part 12, don't leave the routing definitions empty.
- Create a Private route with the IP number of the file server (192.168.0.15 / 255.255.255.255).
- In Step 2, part 3, configure the firewall to only accept Apple File Sharing Protocol connections and DNS from the VPN address group.

VPN users who are now logged in through the VPN gateway can access the file server, and no other network traffic can go through the encrypted gateway.

## Linking Two or More Remote Network Sites

You can use a VPN to link a computer to a main network, and you can also link networks.

When two networks are linked they can interact as if they are physically connected. Each site must have its own connection to the Internet but the private data is sent encrypted between the sites.

This type of link is useful for connecting satellite offices to an organization's main office LAN.

### About the Site-To-Site VPN Administration Tool

Linking multiple remote LAN sites to a main LAN requires the use of a command-line utility installed on Mac OS X Server named `s2svpnadmin` ("site-to-site VPN admin").

Using `s2svpnadmin` requires the use of (and facility with) the Terminal, and the administrator must have access to root privileges through `sudo`. For more about `s2svpnadmin`, see the `s2svpnadmin` man page.

Linking multiple remote LAN sites to a main LAN can require the creation of a security certificate. The tool `s2svpnadmin` can create links using shared-secret authentication (both sites have a password in their configuration files) or certificate authentication. To use certificate authentication, you must create the certificate before running `s2svpnadmin`.

Site-to-site VPN connections can be only made using L2TP/IPSec VPN connections. You cannot link two sites using PPTP and these instructions.

This example uses the following settings:

- Desired VPN type: L2TP
- Authentication: Using shared secret
- Shared secret: prDwkj49fd!254
- Internet or public IP address of the VPN main LAN gateway ("Site 1"): A.B.C.D
- Internet or public IP address of the VPN remote LAN gateway ("Site 2"): W.X.Y.Z
- Private IP address of site 1: 192.168.0.1
- Private IP address of site 2: 192.168.20.1
- Private network IP address range and netmask for site 1: 192.168.0.0–192.168.0.255 (also expressed as192.168.0.0/16 or 192.168.0.0:255.255.0.0)
- Private network IP address range and netmask for site 2: 192.168.20.0–192.168.20.255 (also expressed as192.168.20.0/24 or 192.168.0.0:255.255.0.0)
- Organization's DNS IP address: 192.168.0.2

The result of this configuration is an auxiliary, remote LAN, connected to a main LAN using L2TP.

#### Step 1: Run s2svpnadmin on both site gateways

1. Open Terminal and start `s2svpnadmin` by entering:

   ```
   $ sudo s2svpnadmin
   ```

2. Enter the relevant number for "Configure a new site-to-site server."
3. Enter an identifying configuration name (no spaces permitted).

   For this example, you could enter "site_1" on site 1's gateway, and so on.
4. Enter the gateway's public IP address.

   For this example, enter A.B.C.D on site 1's gateway and W.X.Y.Z on site 2's gateway.

5 Enter the other site's public IP address.

For this example, enter W.X.Y.Z on site 1's gateway and A.B.C.D on site 2's gateway.

6 Enter "s" for shared secret authentication, and enter the shared secret: ("prDwkj49fd!254").

If you are using certificate authentication, enter "c" and choose the installed certificate that you want to use.

7 Enter at least one addressing policy for the configuration.

8 Enter a local subnet network address (for example, 192.168.0.0 for site 1, 192.168.20.0 for site 2).

9 For the address range, enter the prefix bits in CIDR notation.

In this example, the CIDR notation for the subnet range is 192.168.2.0/24 for site 1, so you would enter 24.

10 Enter a remote subnet network address (for example, 192.168.20.0 for site 1, 192.168.0.0 for site 2).

11 For the address range, enter the prefix bits in CIDR notation.

In this example, the CIDR notation for the subnet range is 192.168.2.0/24 for site 1, so you would enter 24.

12 If you want to make more policies, indicate it now; otherwise, press Return.

If you had more sites to connect or a more complex address setup (linking only parts of your main LAN and the remote LAN), you would make more policies for this configuration now.

Repeat policy steps 7 through 12 for the new policies.

13 Press "y" to enable the site configuration.

You can verify your settings by choosing to show the configuration details of the server and entering the configuration name (in this example, "site_1").

14 Exit `s2svpnadmin`.

### Step 2: Configure the firewall on both site gateways

1 Create an address group for each server with only the server's public IP address.

In this example, name the first group Site 1 and enter the public IP address of the server. Then name the second group Site 2 and enter the public IP address of the other server.

For more information, see "Creating an Address Group" on page 90.

2 Open the firewall to external VPN connections by enabling L2TP (port 1701) connections and IKE NAT Traversal (port 4500) in the "any" address group.

For more information, see "Configuring Services Settings" on page 88.

3 Create the following Advanced IP filter rules on both site gateways:

| Filter Rule 1 | Setting |
|---|---|
| Action: | Allow |
| Protocol: | UDP |
| Source Address: | Site 1 |
| Destination Address: | Site 2 |
| Interface: | Other, enter "isakmp" |

| Filter Rule 2 | Setting |
|---|---|
| Action: | Allow |
| Protocol: | UDP |
| Source Address: | Site 2 |
| Destination Address: | Site 1 |
| Interface: | Other, enter "isakmp" |

| Filter Rule 3 | Setting |
|---|---|
| Action: | Allow |
| Protocol: | Other, enter "esp" |
| Source Address: | Site 1 |
| Destination Address: | Site 2 |

| Filter Rule 4 | Setting |
|---|---|
| Action: | Allow |
| Protocol: | Other, enter "esp" |
| Source Address: | Site 2 |
| Destination Address: | Site 1 |

| Filter Rule 5 | Setting |
|---|---|
| Action: | Allow |
| Protocol: | Other, enter "ipencap" |
| Source Address: | Site 1 |
| Destination Address: | Site 2 |

| Filter Rule 6 | Setting |
|---|---|
| Action: | Allow |
| Protocol: | Other, enter "ipencap" |
| Source Address: | Site 2 |
| Destination Address: | Site 1 |

| Filter Rule 7 | Setting |
|---|---|
| Action: | Allow |
| Protocol: | Other, enter "gre" |
| Source Address: | Site 1 |
| Destination Address: | Site 2 |

| Filter Rule 8 | Setting |
|---|---|
| Action: | Allow |
| Protocol: | Other, enter "gre" |
| Source Address: | Site 2 |
| Destination Address: | Site 1 |

For more information about creating advanced rules, see "Configuring Advanced Firewall Rules" on page 93.

These rules permit the encrypted traffic to be passed to both hosts.

4 Save your changes.

5 Start or restart the firewall, as needed.

### Step 3: Start VPN service on both site gateways

1 For both VPN gateways, open Server Admin and connect to the server.

2 Click the triangle to the left of the server.

The list of services appears.

3 Select VPN from the expanded Servers list.

If you used `s2svpnadmin` correctly, the Start button should be enabled and ready to use.

4 Click Start VPN.

You should now be able to access a computer on the remote LAN from the local LAN. To verify the link, use `ping` or some other means.

## Where to Find More Information

**For More Information About L2TP/IPSec**

The Internet Engineering Task Force (IETF) is working on formal standards for L2TP/IPsec user authentication. For more information, see www.ietf.org/ids.by.wg/ipsec.html.

**Request for Comment Documents**

Request for Comments (RFC) documents provide an overview of a protocol or service and details about how the protocol should behave.

If you're a novice server administrator, you'll probably find some of the background information in an RFC helpful.

If you're an experienced server administrator, you can find all technical details about a protocol in its RFC document.

You can search for RFC documents by number at the website www.ietf.org/rfc.html.

- For L2TP description, see RFC 2661.
- For PPTP description, see RFC 2637.
- For Kerberos version 5, see RFC 1510.