VPNease Quick Installation Guide

Overview

Quick installation requires the following:

- A dedicated PC with at least 1 GHz CPU, 256 MB RAM, and 2 GB hard disk
- A client computer with a supported operating system (e.g. Windows XP/Vista, Mac OS X)
- 45 minutes for installation and testing

For comprehensive installation instructions, see www.vpnease.com/server-installation.html.

Step 1: Download and Burn Installation CD

Download the latest VPNease server ISO image and burn it to a CD or DVD. Please ensure that you burn the ISO image as is instead of creating a data CD containing the ISO image as a file.

Step 2: Check Server Requirements and Install

The VPNease server is installed on a dedicated PC with the following minimum requirements: 1 GHz CPU, 256 MB RAM, and 2 GB hard disk. The PC BIOS must be capable of booting from hard disks larger than 512MB which is the case for all modern BIOS versions. For details, see www.vpnease.com/server-requirements.html.

Boot from the VPNease server installation CD (you may need to change your BIOS boot settings for this), click **Install product**, select a hard disk for installation, and confirm installation. The installation process takes about 15 minutes. Once installation is complete, click **Reboot computer** to reboot, and remove the CD from the drive when it is ejected.

If you are familiar with VMware, you can also install VPNease server into a VMware guest. See www.vpnease.com/virtualization-products.html for details.

Step 3: Perform Initial Server Configuration

We suggest the following network configuration: the VPNease server is installed into the company intranet, to the same subnet where company servers reside. The company firewall is then configured to port forward connections from the company Internet connection to the VPNease server to allow VPN access from the Internet (see step 4 below).

Boot the VPNease server (you may need to change your BIOS boot settings for this). Login to the administrator interface and perform the following minimum configuration steps:

- Go to the **Network** page.
- Check the **Internet Connection** settings: you should either select DHCP or static address configuration. For static configuration you need to enter a static IP address, subnet mask, and default gateway, and enter a DNS server address manually to the DNS Servers group.
- Select a pre-shared key used for computer authentication and enter it into the **VPN Connection Settings → Primary pre-shared key field**.
- Click **Save changes**.

- Go to the **User Accounts** page.
- Add a VPN user by clicking on the plus sign in the **Users** group. Enter a username and a password for the user.
- Click **Save changes**.

The VPNease server status page shows all basic server information. The product will automatically request a demo license for 30 days, and the available demo license time is shown. Check the IP address of the Internet connection and write it down for later use.

Step 4: Configure Company Firewall

Write down the firewall's Internet IP address, as it is needed for VPN client use. Add port forwarding rules to the company firewall, to forward the following protocols and ports from the Internet connection to the VPNease server's IP address:

- UDP port 500 (IPsec)
- UDP port 4500 (IPsec)
- TCP port 80 (web UI, optional but recommended)
- TCP port 443 (web UI, optional but recommended)

Not forwarding TCP ports 80 and 443 disables access to the VPNease web user interface from the Internet. You can access the web user interface from the intranet instead. If you use client autoconfiguration from the intranet, edit the VPN connection properties afterwards, changing the VPNease server address from the intranet address to the Internet address.

Step 5: Configure and Test Client Computer

Select a laptop or desktop computer for testing the VPN connection. Connect the laptop to the Internet (not the intranet), open a browser window and enter the IP address of the firewall's Internet connection. Login to the web user interface with the VPN user's username and password (configured in step 3).

Configuring and testing the VPN connection depends on the client computer operating system:

- Windows XP: click **Autoconfigure**, run the downloaded executable, and reboot the computer. After reboot, open Network Connections, double click on the VPNease VPN icon, enter username and password, and click **Connect**.
- Windows Vista: similar to Windows XP, but the downloaded executable needs to be saved and run as an administrator. See the instructions on the web interface.
- Mac OS X: select **Mac OS X** from the menu on the left and follow configuration instructions.

You should now be able to access all your company resources through the VPN connection.

If a VPN connection cannot be established (e.g. you get Windows “error #768") check that IPsec services is running (Control Panel – Administrative Tools – Services). Some VPN clients disable Windows IPsec services during installation.

Note that if you want to test the VPN connection from the intranet for some reason, you need to use the VPNease server rather than the firewall's address in the web browser and the VPN profile. Port forwarding does not always work when connections are initiated from the intranet.