OmniVPN Installation Guide

OmniVPN requires a flat network topology. This means that each LAN is directly connected to the Internet via either a router or a NAT. One machine on each LAN must be configured as an OmniVPN gateway. If the LAN is behind a NAT, you must either place the OmniVPN gateway in the DMZ of the NAT, or you must forward all the ports that you use from the NAT to the OmniVPN gateway. The former approach is easier and necessary in order to support applications that rely on protocols that dynamically negotiate ports, e.g., H.323.

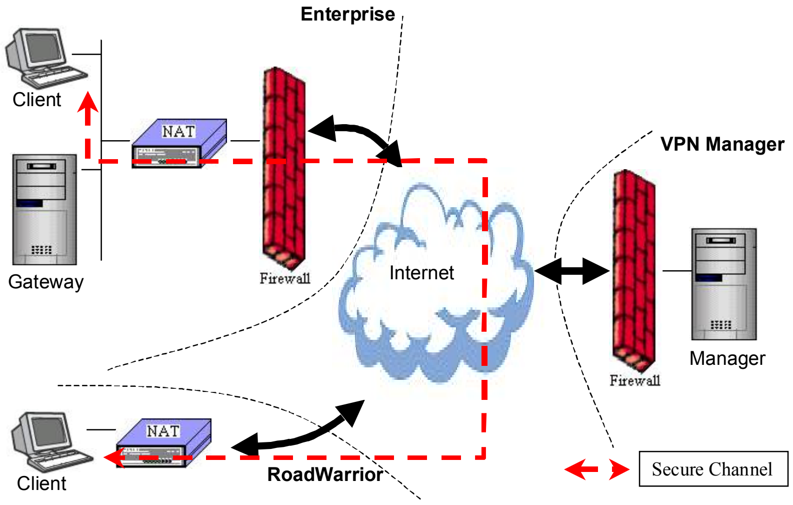


Figure 1A

Figure 1A shows a typical VPN setup.

One of the OmniVPN gateways must be designated as the OmniVPN Manager. From this machine, the entire VPN will be administered. This machine is the most crucial machine in the whole VPN. It is not only possible, but advisable, to have a separate globally reachable machine designated as the VPN manager. If the size of the VPN is small, then one of the gateways can be designated as the VPN manager instead.

Road warrior configuration for remote access is done as part of the client setup.

Note: OmniVPN includes an integrated, stateful inspection firewall. We strongly recommend that you use it because no other firewall can provide the same level of protection and control. However, if you do wish to use a different firewall, it should ideally be placed behind the OmniVPN gateway and must be configured to allow traffic from all other VPN subnets. If it must be placed outside OmniVPN gateway, then it must be configured to allow traffic from the routable addresses of the other OmniVPN gateways.

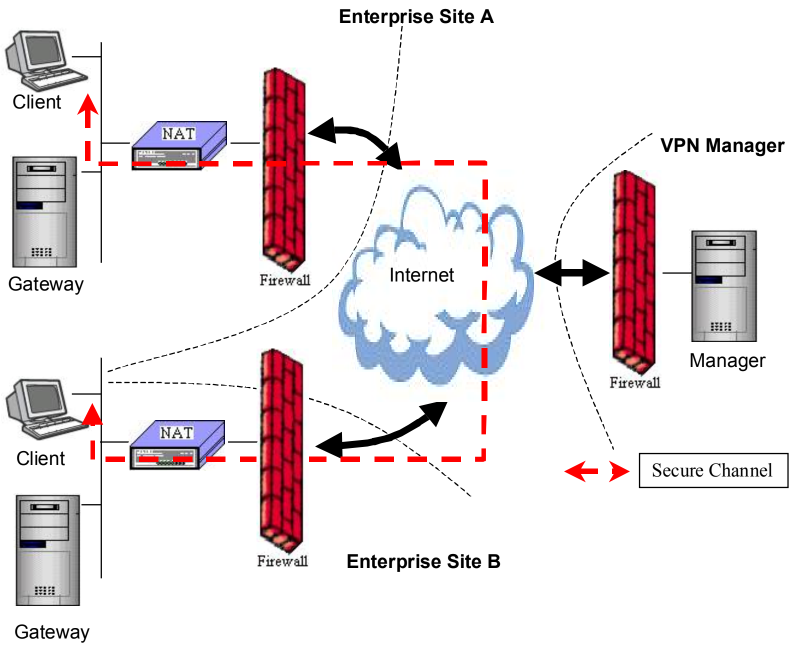


Figure 1B

Figure 1B gives a specific example of a site-to-site VPN. While this example shows the VPN manager as a separate entity, one of the gateways can be used as a manager.

The site-to-site feature is not available in the free version of OmniVPN. In this case, the Manager is the gateway for the single site.

Installation

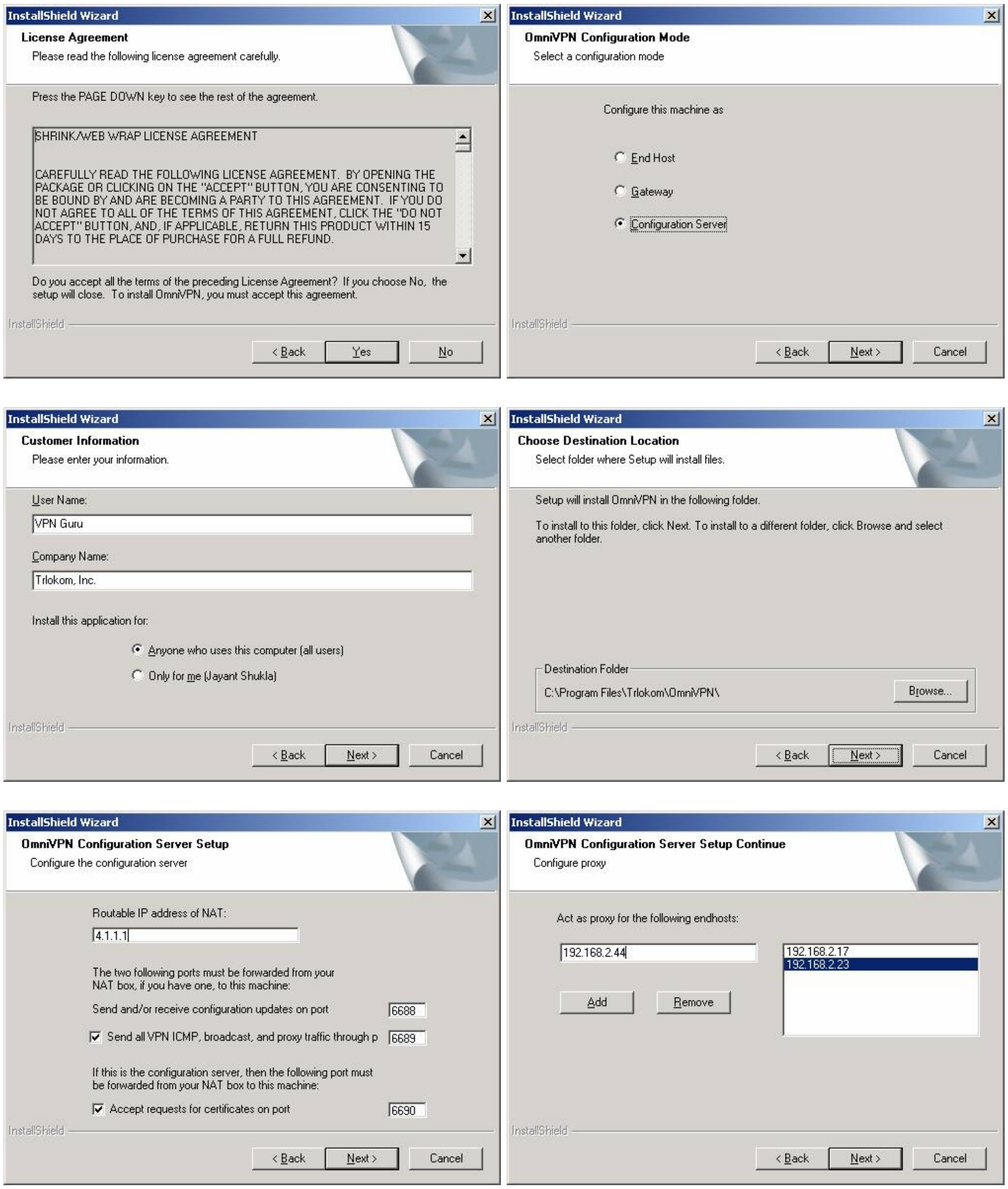
The installation procedure is simple. When the setup program starts, the user is given an option to install as the VPN Manager, a VPN Gateway, or a VPN client. Depending on the selection made by the user, the appropriate components of the VPN are installed and the user is prompted for the necessary configuration information.

1) **Install the VPN Manager.**
2) **Install the VPN gateways.**
3) **Install the VPN clients behind each gateway.**

Installation of the VPN clients behind a particular gateway can be simplified by creating an End Host Installer for the subnet. You will be asked about this at the end of the gateway installation process. Once the End Host Installer is created, copy it to a CD and use this new CD to install OmniVPN on the computers behind the gateway. This saves time because most of the parameters will be entered for you during the installation process.

VPN Manager

This is the first component of the VPN that the user must install. Installation of the VPN Manager is very similar to the VPN Gateway. In many instances the VPN Manager will also be the VPN Gateway for its subnet. Figure 2 shows the steps that the user will follow to install a VPN Manager.



InstallShield Wizard

License Agreement

Please read the following license agreement carefully.

Press the PAGE DOWN key to see the rest of the agreement.

SHRINK/WEB WRAP LICENSE AGREEMENT

CAREFULLY READ THE FOLLOWING LICENSE AGREEMENT. BY OPENING THE PACKAGE OR CLICKING ON THE "ACCEPT" BUTTON, YOU ARE CONSENTING TO BE BOUND BY AND ARE BECOMING A PARTY TO THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, CLICK THE "DO NOT ACCEPT" BUTTON, AND, IF APPLICABLE, RETURN THIS PRODUCT WITHIN 15 DAYS TO THE PLACE OF PURCHASE FOR A FULL REFUND.

Do you accept all the terms of the preceding License Agreement? If you choose No, the setup will close. To install OmniVPN, you must accept this agreement.

InstallShield

InstallShield Wizard

OmniVPN Configuration Mode

Select a configuration mode

Configure this machine as

○ End Host

○ Gateway

● Configuration Server

InstallShield

InstallShield Wizard

Customer Information

Please enter your information.

User Name: VPN Guru

Company Name: Trlokom, Inc.

Install this application for:

● Anyone who uses this computer (all users)

○ Only for me (Jayant Shukla)

InstallShield

InstallShield Wizard

Choose Destination Location

Select folder where Setup will install files.

Setup will install OmniVPN in the following folder.

To install to this folder, click Next. To install to a different folder, click Browse and select another folder.

Destination Folder

C:\Program Files\Trlokom\OmniVPN\

InstallShield

InstallShield Wizard

OmniVPN Configuration Server Setup

Configure the configuration server

Routable IP address of NAT: 4.1.1.1

The two following ports must be forwarded from your NAT box, if you have one, to this machine:

Send and/or receive configuration updates on port 6688

☑ Send all VPN ICMP, broadcast, and proxy traffic through p 6689

If this is the configuration server, then the following port must be forwarded from your NAT box to this machine:

☑ Accept requests for certificates on port 6690

InstallShield

InstallShield Wizard

OmniVPN Configuration Server Setup Continue

Configure proxy

Act as proxy for the following endhosts:

192.168.2.44

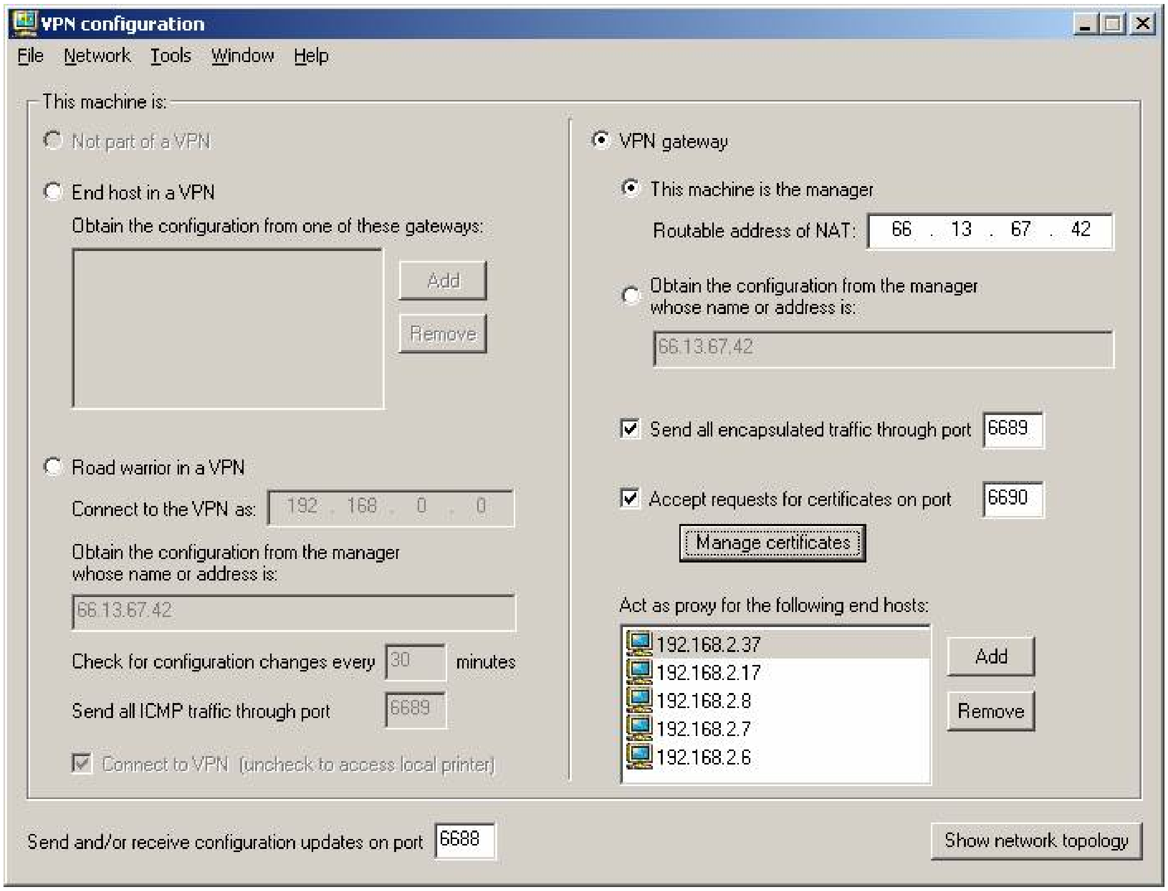
192.168.2.17
192.168.2.23

InstallShield

Figure 2

STEPS:

1) Select the VPN Manager installation.
2) Enter the user & company names.
3) Choose the location where the software will be installed.
4) The user must fill in the global IP address of the VPN Manager or the IP address of the NAT behind which the Manager resides and also the three ports that are used by the VPN.
5) List of nodes that the VPN Manager may be proxying for. This lists the nodes that are not capable of VPN communication but are part of the VPN. These computers need to have their default gateway (in TCP/IP properties) set to the OmniVPN gateway. The IP address of the NAT router must be in this list. (This window does not appear in the free version of OmniVPN. In this case, proxied hosts must be entered in VPNConfig after installation is complete.)



This machine is:

○ Not part of a VPN

○ End host in a VPN

Obtain the configuration from one of these gateways:

○ Road warrior in a VPN

Connect to the VPN as: 192 . 168 . 0 . 0

Obtain the configuration from the manager whose name or address is: 66.13.67.42

Check for configuration changes every 30 minutes

Send all ICMP traffic through port 6689

☑ Connect to VPN (uncheck to access local printer)

● VPN gateway

● This machine is the manager

Routable address of NAT: 66 . 13 . 67 . 42

○ Obtain the configuration from the manager whose name or address is: 66.13.67.42

☑ Send all encapsulated traffic through port 6689

☑ Accept requests for certificates on port 6690

Act as proxy for the following end hosts:

192.168.2.37
192.168.2.17
192.168.2.8
192.168.2.7
192.168.2.6

Send and/or receive configuration updates on port 6688

Figure 3

Figure 3 shows a typical VPN configuration window for the VPN manager.

Gateway

If the LAN is behind a NAT, the gateway will typically be located in the DMZ of the NAT. If the LAN uses routable IP addresses, then this is not an issue.

If the gateway cannot be placed in the DMZ of the NAT, then one must forward the desired service ports and some configuration ports to the gateway. If a LAN is connected to the Internet via a NAT, the configuration distribution port (TCP and UDP; default: **6688**) must be forwarded to the local OmniVPN gateway. You must also forward the encapsulated traffic port (UDP; default: **6689**), if you leave it enabled during installation.

You can choose to either have a separate Certificate Authority (CA) on each OmniVPN gateway, or you can have only a single CA on the OmniVPN Manager.

The former method allows the administrator of each LAN to install OmniVPN from a separate CD with a separate set of one-time use certificates. These one-time use certificates are used by each machine on the LAN to obtain a permanent certificate from the local OmniVPN gateway. The local OmniVPN gateway must use a pre-shared text key to obtain a permanent certificate from the OmniVPN Manager.

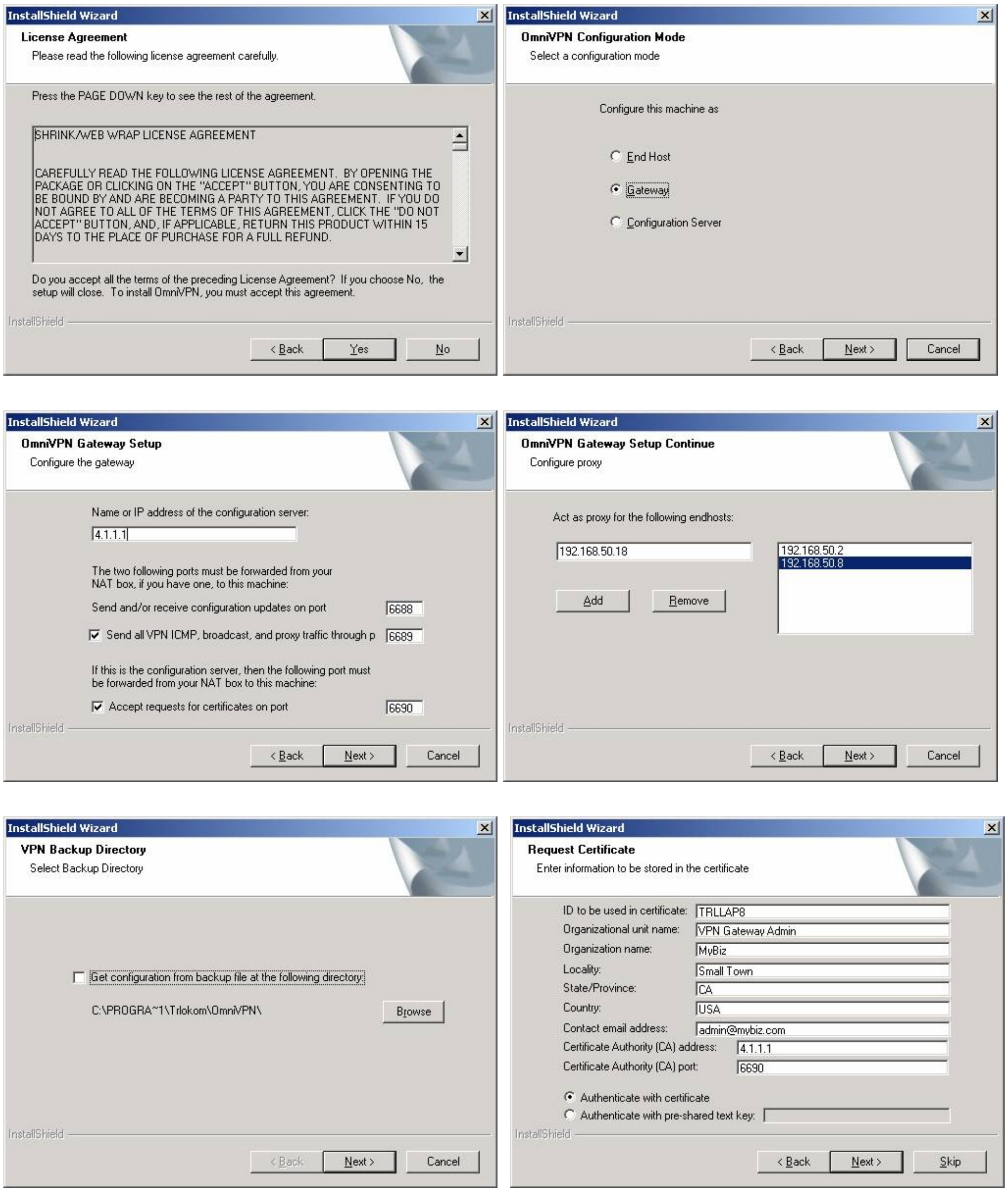
The latter method requires that the administrator of each LAN install OmniVPN from a copy of a single, master CD. All machines will use the same set of one-time use certificates to obtain permanent certificates from the CA on the OmniVPN Manager. With this method, the "Accept requests for certificates" option in the VPN Configuration window in the VPNConfig application should be turned off on all gateways except the Manager.

In either case, if the LAN containing the OmniVPN Manager is connected to the Internet via a NAT, the certificate authority port (TCP and UDP; default: **6690**) must be forwarded to the OmniVPN Manager.

Figure 4 shows the steps a user will follow to install on a VPN gateway.

STEPS:

1) Select the VPN Gateway installation.
2) Enter the routable IP address of the VPN Manager along with the port numbers.
6) Enter the IP address of the nodes for which this gateway will proxy. These computers need to have their default gateway (in TCP/IP properties) set to the OmniVPN gateway. <u>The IP address of the NAT router must be in this list</u>.
3) Decide if the VPN configuration is to be read from a local file.
4) Enter information to obtain a certificate.



InstallShield Wizard

License Agreement

Please read the following license agreement carefully.

Press the PAGE DOWN key to see the rest of the agreement.

SHRINK/WEB WRAP LICENSE AGREEMENT

CAREFULLY READ THE FOLLOWING LICENSE AGREEMENT. BY OPENING THE PACKAGE OR CLICKING ON THE "ACCEPT" BUTTON, YOU ARE CONSENTING TO BE BOUND BY AND ARE BECOMING A PARTY TO THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, CLICK THE "DO NOT ACCEPT" BUTTON, AND, IF APPLICABLE, RETURN THIS PRODUCT WITHIN 15 DAYS TO THE PLACE OF PURCHASE FOR A FULL REFUND.

Do you accept all the terms of the preceding License Agreement? If you choose No, the setup will close. To install OmniVPN, you must accept this agreement.

InstallShield Wizard

OmniVPN Configuration Mode

Select a configuration mode

Configure this machine as

○ End Host

● Gateway

○ Configuration Server

InstallShield Wizard

OmniVPN Gateway Setup

Configure the gateway

Name or IP address of the configuration server: 4.1.1.1

The two following ports must be forwarded from your NAT box, if you have one, to this machine:

Send and/or receive configuration updates on port 6688

☑ Send all VPN ICMP, broadcast, and proxy traffic through p 6689

If this is the configuration server, then the following port must be forwarded from your NAT box to this machine:

☑ Accept requests for certificates on port 6690

InstallShield Wizard

OmniVPN Gateway Setup Continue

Configure proxy

Act as proxy for the following endhosts:

192.168.50.18

192.168.50.2
192.168.50.8

InstallShield Wizard

VPN Backup Directory

Select Backup Directory

□ Get configuration from backup file at the following directory:

C:\PROGRA~1\Trlokom\OmniVPN\

InstallShield Wizard

Request Certificate

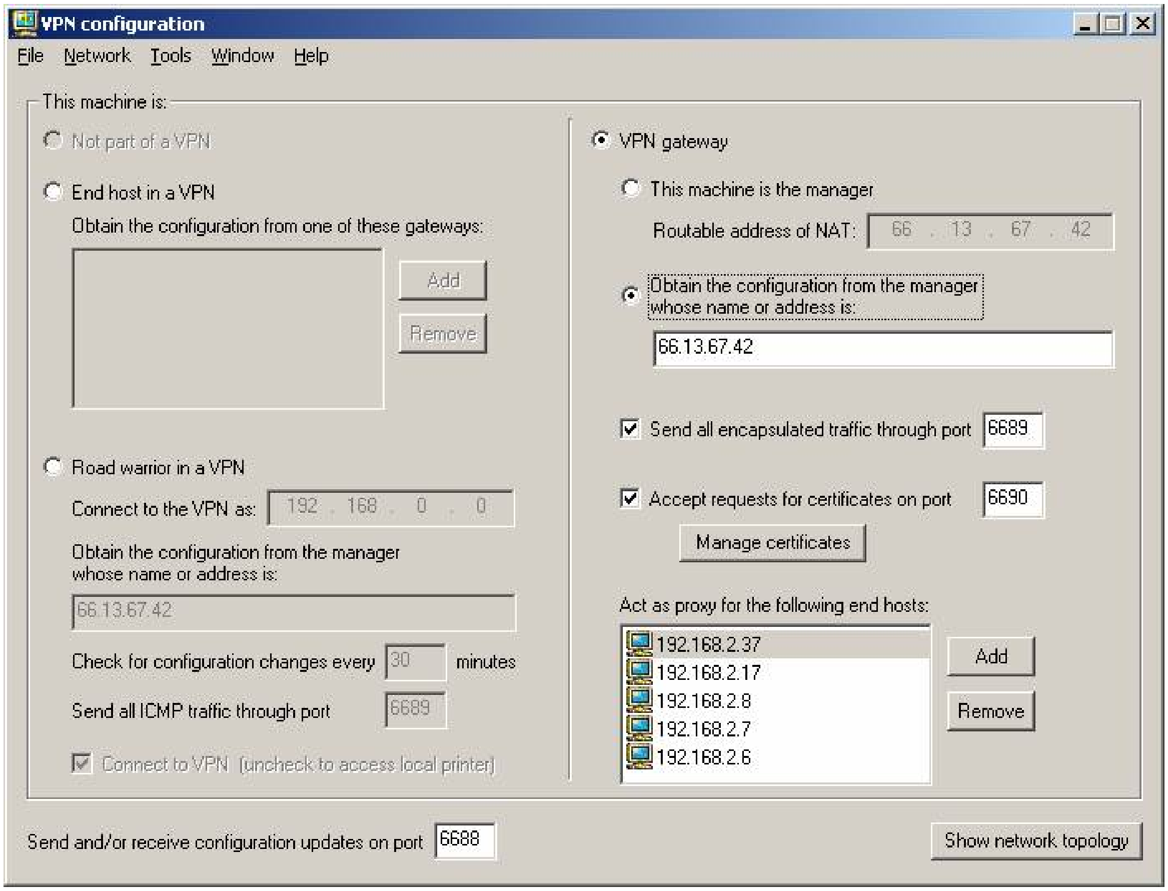
Enter information to be stored in the certificate

ID to be used in certificate: TRLLAP8
Organizational unit name: VPN Gateway Admin
Organization name: MyBiz
Locality: Small Town
State/Province: CA
Country: USA
Contact email address: admin@mybiz.com
Certificate Authority (CA) address: 4.1.1.1
Certificate Authority (CA) port: 6690

● Authenticate with certificate

○ Authenticate with pre-shared text key:

Figure 4



VPN configuration

This machine is:

○ Not part of a VPN

○ End host in a VPN

Obtain the configuration from one of these gateways:

○ Road warrior in a VPN

Connect to the VPN as: 192 . 168 . 0 . 0

Obtain the configuration from the manager whose name or address is: 66.13.67.42

Check for configuration changes every 30 minutes

Send all ICMP traffic through port 6689

☑ Connect to VPN (uncheck to access local printer)

● VPN gateway

○ This machine is the manager

Routable address of NAT: 66 . 13 . 67 . 42

● Obtain the configuration from the manager whose name or address is: 66.13.67.42

☑ Send all encapsulated traffic through port 6689

☑ Accept requests for certificates on port 6690

Act as proxy for the following end hosts:

192.168.2.37
192.168.2.17
192.168.2.8
192.168.2.7
192.168.2.6

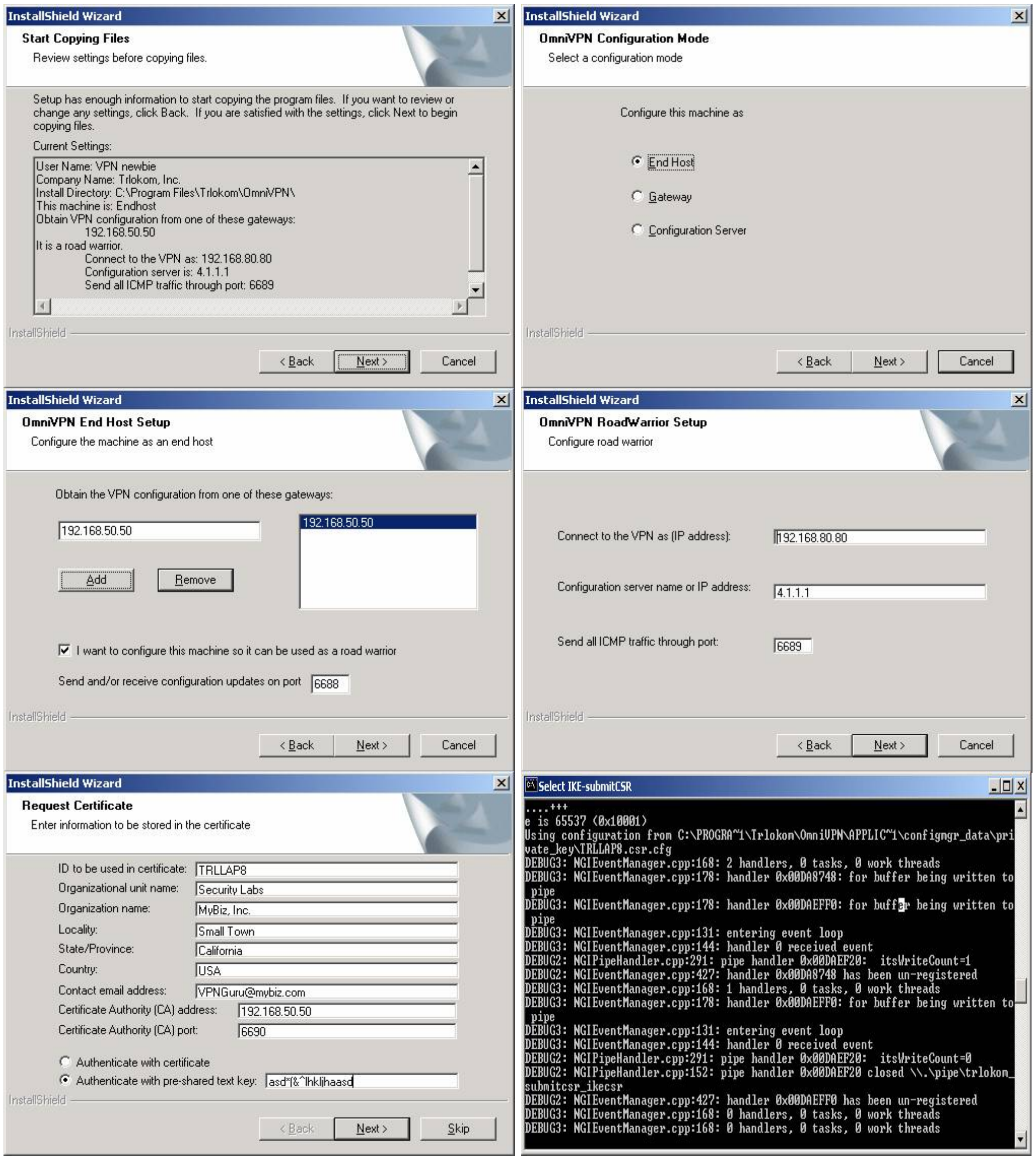
Send and/or receive configuration updates on port 6688

Figure 5

Figure 5 shows a typical VPN configuration window for the VPN Gateway. Note that one VPN Gateway may be the VPN Manager in certain deployments.

VPN Client

Figure 6 shows the steps a user will follow to install a VPN Client.



Start Copying Files

Review settings before copying files.

Setup has enough information to start copying the program files. If you want to review or change any settings, click Back. If you are satisfied with the settings, click Next to begin copying files.

Current Settings:

```
User Name: VPN newbie
Company Name: Trlokom, Inc.
Install Directory: C:\Program Files\Trlokom\OmniVPN\
This machine is: Endhost
Obtain VPN configuration from one of these gateways:
            192.168.50.50
It is a road warrior.
            Connect to the VPN as: 192.168.80.80
            Configuration server is: 4.1.1.1
            Send all ICMP traffic through port: 6689
```

OmniVPN Configuration Mode

Select a configuration mode

Configure this machine as

● End Host
○ Gateway
○ Configuration Server

OmniVPN End Host Setup

Configure the machine as an end host

Obtain the VPN configuration from one of these gateways: 192.168.50.50

192.168.50.50

☑ I want to configure this machine so it can be used as a road warrior

Send and/or receive configuration updates on port 6688

OmniVPN RoadWarrior Setup

Configure road warrior

Connect to the VPN as (IP address): 192.168.80.80

Configuration server name or IP address: 4.1.1.1

Send all ICMP traffic through port: 6689

Request Certificate

Enter information to be stored in the certificate

ID to be used in certificate: TRLLAP8
Organizational unit name: Security Labs
Organization name: MyBiz, Inc.
Locality: Small Town
State/Province: California
Country: USA
Contact email address: VPNGuru@mybiz.com
Certificate Authority (CA) address: 192.168.50.50
Certificate Authority (CA) port: 6690

○ Authenticate with certificate
● Authenticate with pre-shared text key: asd*[&^lhkljhaasd

Select IKE-submitCSR

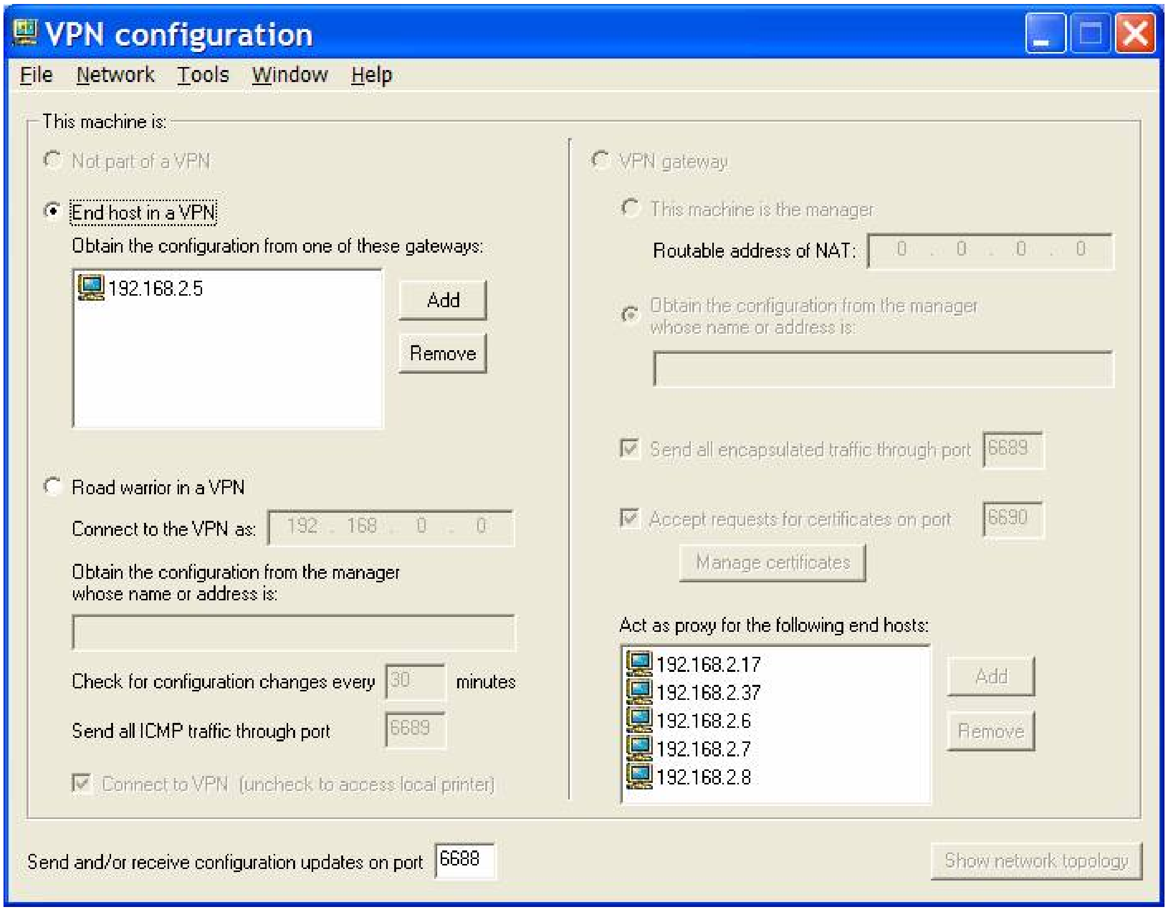
```
....+++
e is 65537 (0x10001)
Using configuration from C:\PROGRA~1\Trlokom\OmniVPN\APPLIC~1\configmgr_data\pri
vate_key\TRLLAP8.csr.cfg
DEBUG3: NGIEventManager.cpp:168: 2 handlers, 0 tasks, 0 work threads
DEBUG3: NGIEventManager.cpp:178: handler 0x00DA8748: for buffer being written to
 pipe
DEBUG3: NGIEventManager.cpp:178: handler 0x00DAEFF0: for buffer being written to
 pipe
DEBUG3: NGIEventManager.cpp:131: entering event loop
DEBUG3: NGIEventManager.cpp:144: handler 0 received event
DEBUG2: NGIPipeHandler.cpp:291: pipe handler 0x00DAEF20:  itsWriteCount=1
DEBUG2: NGIEventManager.cpp:427: handler 0x00DA8748 has been un-registered
DEBUG3: NGIEventManager.cpp:168: 1 handlers, 0 tasks, 0 work threads
DEBUG3: NGIEventManager.cpp:178: handler 0x00DAEFF0: for buffer being written to
 pipe
DEBUG3: NGIEventManager.cpp:131: entering event loop
DEBUG3: NGIEventManager.cpp:144: handler 0 received event
DEBUG2: NGIPipeHandler.cpp:291: pipe handler 0x00DAEF20:  itsWriteCount=0
DEBUG2: NGIPipeHandler.cpp:152: pipe handler 0x00DAEF20 closed \\.\pipe\trlokom_
submitcsr_ikecsr
DEBUG2: NGIEventManager.cpp:427: handler 0x00DAEFF0 has been un-registered
DEBUG3: NGIEventManager.cpp:168: 0 handlers, 0 tasks, 0 work threads
DEBUG3: NGIEventManager.cpp:168: 0 handlers, 0 tasks, 0 work threads
```

Figure 6

STEPS:

1) Select end-host installation,.
2) Enter the IP address of the local gateway. In the same window, the user can select if the host needs to be configured to allow remote access to the VPN (Road Warrior).
3) If this option is selected, an IP address must be entered which the client will use to connect to the VPN when acting as a Road Warrior. One also enters the routable IP address of the VPN Manager and the port number on which to send ICMP traffic.
4) The user is prompted with a dialog box to obtain a certificate from the local gateway. The authentication method can be either based on pre-shared text keys or one-time certificates. If one is using a single CA, as discussed earlier, then routable IP address of the OmniVPN Manager can be used instead of the local gateway.
5) While the certificate is being requested/issued, a command line window will appear. This window disappears once the certificate is obtained.

In order for the host to obtain its permanent certificate, the gateway must allow the host to obtain a certificate. In the “Manage Certificate” window on the gateway, the host name must appear in the list of hosts that can obtain a certificate from the CA. A simpler, but less secure option is to turn on the "Allow any machine to use a one-time certificate" checkbox.



This machine is:

○ Not part of a VPN

● End host in a VPN

Obtain the configuration from one of these gateways:

- 192.168.2.5

○ Road warrior in a VPN

Connect to the VPN as: 192 . 168 . 0 . 0

Obtain the configuration from the manager whose name or address is:

Check for configuration changes every 30 minutes

Send all ICMP traffic through port 6689

☑ Connect to VPN (uncheck to access local printer)

○ VPN gateway

○ This machine is the manager

Routable address of NAT: 0 . 0 . 0 . 0

● Obtain the configuration from the manager whose name or address is:

☑ Send all encapsulated traffic through port 6689

☑ Accept requests for certificates on port 6690

Act as proxy for the following end hosts:

- 192.168.2.17
- 192.168.2.37
- 192.168.2.6
- 192.168.2.7
- 192.168.2.8

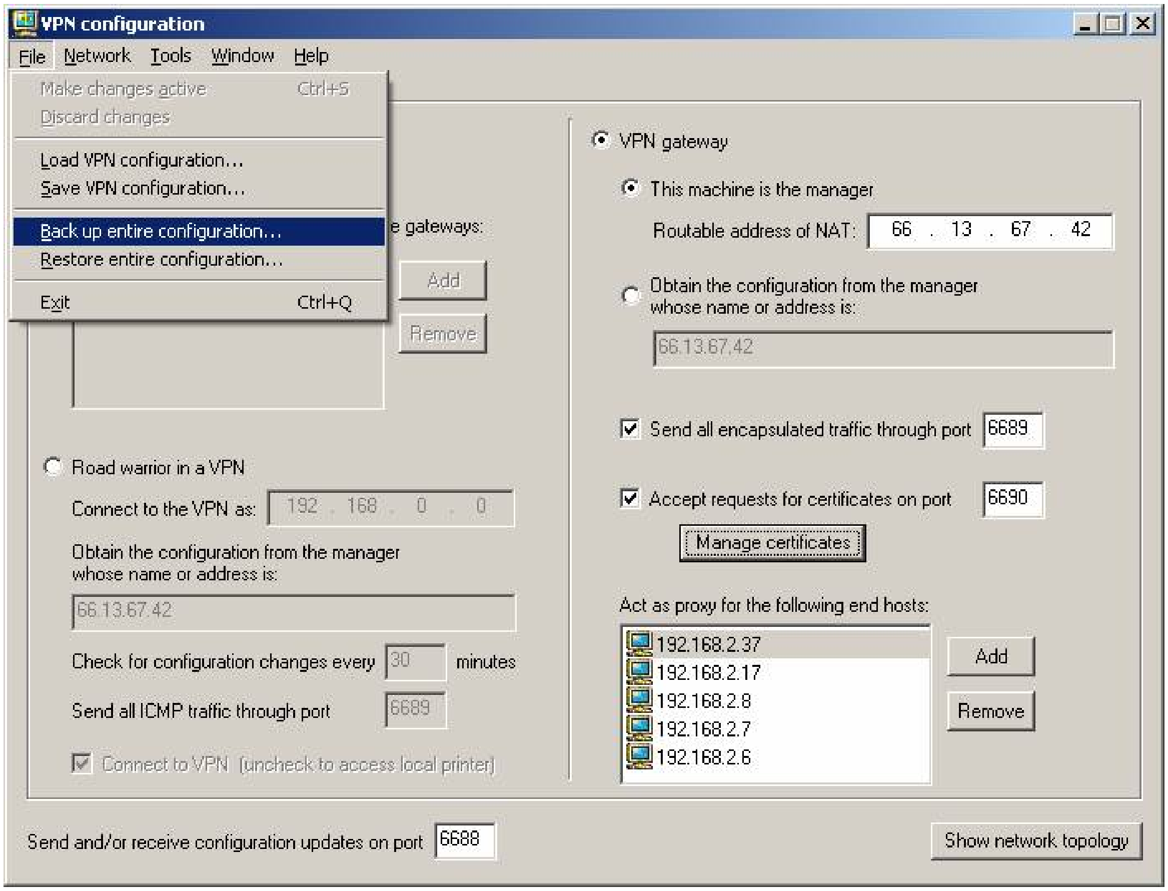
Send and/or receive configuration updates on port 6688

Figure 7

Figure 7 shows a typical VPN configuration window for the VPN Client.

IMPORTANT

Once the VPN has been configured, a backup should be made of the configuration files on each gateway and on the central manager. Use the menu item in the VPN configuration window (as shown in Figure 8) and select the "Back up entire configuration option". The backup configuration file can be used to restore the VPN configuration in the event of a system upgrade or crash.


VPN configuration
File
Network
Tools
Window
Help
Make changes active Ctrl+S
Discard changes
Load VPN configuration...
Save VPN configuration...
Back up entire configuration...
Restore entire configuration...
Exit Ctrl+Q
e gateways:
Add
Remove
Manage certificates
Add
Remove
Show network topology

○ Road warrior in a VPN

Connect to the VPN as: 192 . 168 . 0 . 0

Obtain the configuration from the manager whose name or address is: 66.13.67.42

Check for configuration changes every 30 minutes

Send all ICMP traffic through port 6689

☑ Connect to VPN (uncheck to access local printer)

● VPN gateway

● This machine is the manager

Routable address of NAT: 66 . 13 . 67 . 42

○ Obtain the configuration from the manager whose name or address is: 66.13.67.42

☑ Send all encapsulated traffic through port 6689

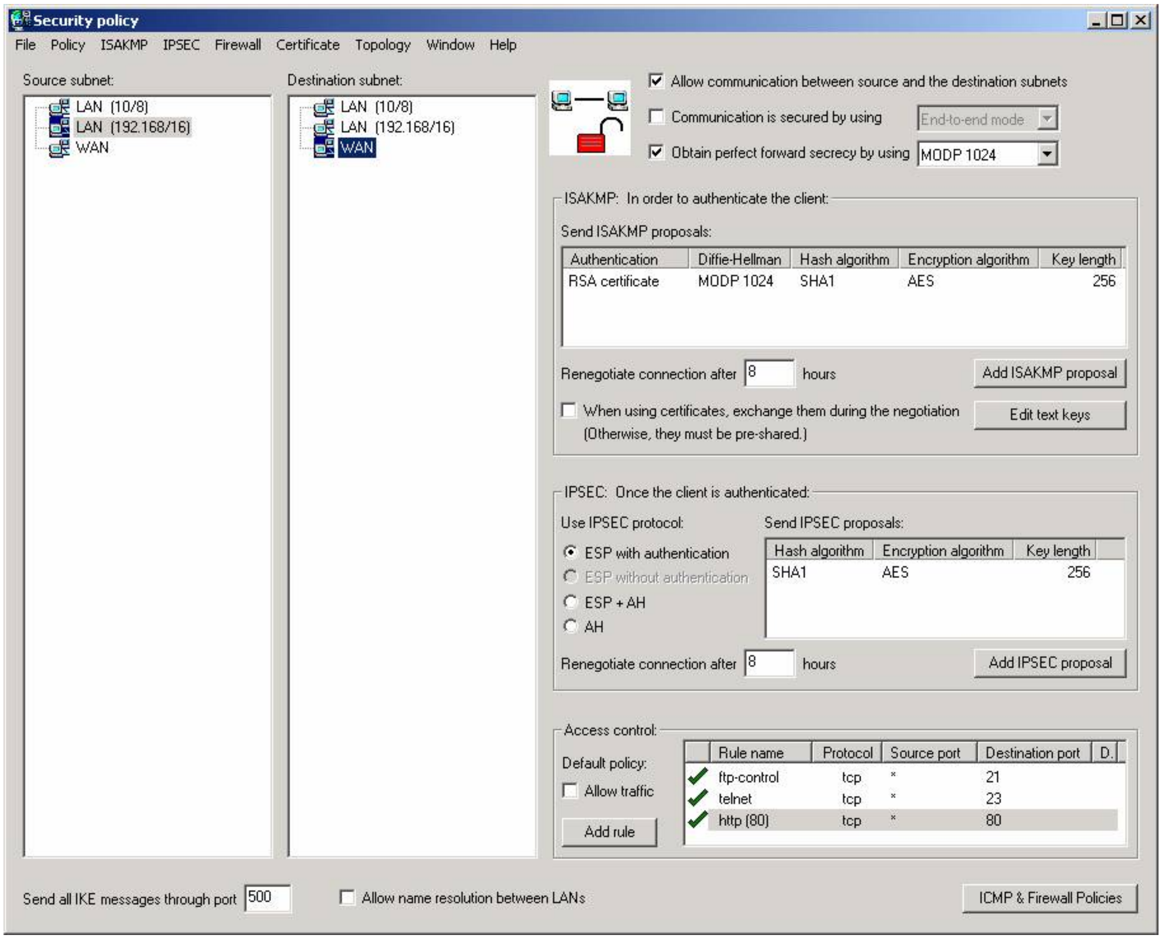
☑ Accept requests for certificates on port 6690

Act as proxy for the following end hosts:

- 192.168.2.37
- 192.168.2.17
- 192.168.2.8
- 192.168.2.7
- 192.168.2.6

Send and/or receive configuration updates on port 6688

Figure 8



Source subnet:

- LAN (10/8)
- LAN (192.168/16)
- WAN

Destination subnet:

- LAN (10/8)
- LAN (192.168/16)
- WAN

☑ Allow communication between source and the destination subnets

□ Communication is secured by using End-to-end mode

☑ Obtain perfect forward secrecy by using MODP 1024

ISAKMP: In order to authenticate the client:

Send ISAKMP proposals:

Authentication	Diffie-Hellman	Hash algorithm	Encryption algorithm	Key length
RSA certificate	MODP 1024	SHA1	AES	256

Renegotiate connection after 8 hours

□ When using certificates, exchange them during the negotiation (Otherwise, they must be pre-shared.)

IPSEC: Once the client is authenticated:

Use IPSEC protocol:

● ESP with authentication
○ ESP without authentication
○ ESP + AH
○ AH

Send IPSEC proposals:

Hash algorithm	Encryption algorithm	Key length
SHA1	AES	256

Renegotiate connection after 8 hours

Access control:

Default policy:

□ Allow traffic

	Rule name	Protocol	Source port	Destination port	D.
✓	ftp-control	tcp	*	21	
✓	telnet	tcp	*	23	
✓	http (80)	tcp	*	80	

Send all IKE messages through port 500

□ Allow name resolution between LANs

Figure 9

Figure 9 shows the Security Policy Editor window. The SPD editor application runs on the VPN manager only. For details on how to use the SPD editor to configure VPN and firewall rules, please read the firewall user guide document.

The default settings automatically will give you a working VPN if you use non-routable IP address on your local subnets. All incoming traffic from the Internet is blocked by default.

We strongly recommend that the “End-to-end” mode be used for all secure communication.

Troubleshooting

Before you attempt to obtain a certificate, you must configure the Certificate Authority (CA) to allow the computer on which you are installing OmniVPN to connect to the CA. This is done via the VPNConfig application in the VPN Configuration window. Make sure that the "Accept requests for certificates" checkbox is checked, and then click on the "Manage certificates" button in the VPN Configuration window. Either add the IP address to the list of machines allowed to use one-time certificates or check the "Allow any machine to use a one-time certificate" checkbox. If you need to use a pre-shared text key instead, simply add it to the bottom list in the window.

If, after entering the information for the certificate, the error message "unable to connect" is displayed, please check that the address and port of the CA that you have to chosen to use are correct and that the CA is enabled. You can check this by running VPNConfig on the CA computer. Also check that your network is working correctly, i.e., that you can ping the CA when encryption is not required between the CA and the machine on which you are installing OmniVPN.

Checklist

1) VPN Manager software installed on a globally addressable machine. If the VPN manager is behind a NAT, then it should be in the DMZ of that NAT.
2) One gateway designated for each VPN subnet.
3) Each VPN gateway is in the DMZ of its NAT or has a routable IP addresses.
4) VPN gateways know the IP address of the VPN Manager. (VPNConfig window)
5) VPN gateways know the Configuration and Encapsulation ports. These numbers must match with the ones on the VPN Manager. (VPNConfig window)
6) OmniVPN software installed on each client. VPNConfig window lists the IP address of the VPN gateway for that client.
7) VPNConfig at the client also indicates that the client is an end-host in the VPN.
8) Client has a valid certificate. (click “manage certificates” button in the VPNConfig window of the Gateway)
9) Proxied clients have their default gateway (in TCP/IP Properties dialog) set to the local OmniVPN gateway.

Upgrading

OmniVPN's centralized management system allows the entire VPN to be upgraded quickly and easily. In the VPN Policy Editor, simply select the "Distribute software upgrade..." item from the File menu and then follow the instructions in the resulting dialog. The upgrade packages will then be distributed to all computers in the VPN.

After OmniVPN has been upgraded, every computer will automatically reboot. It is therefore best to schedule the upgrade during a time when the computer network is not being heavily used. This will minimize the disruption and also allow time for manually upgrading any computers that fail to automatically upgrade correctly.

To check the status of the upgrade process, use the "Show software upgrade status..." item on the File menu. This opens a window displaying the IP addresses of the clients to which the upgrade package was sent but which have not yet re-registered. Installing the upgrade package can take some time, but if this window is not empty after about ½ hour, then the remaining machines should be checked to see if an error occurred. The simplest way to recover from an error is usually to uninstall the old version of the software and then install the new version.

Note that the upgrade status must be checked separately on each OmniVPN gateway because each gateway is responsible for upgrading the computers on its subnet.