VPN User Guide Summary

The VPN user guide explains how to configure policies for secure communication in a VPN.

The following topics are discussed in this manual:
- VPN Configuration
- Starting the VPN Policy Editor
- Adding VPN Sites and Subnets
- Setting the VPN Policy
- Defining IKE Policy
- Defining IPSec Policy
- Setting rules for WAN to LAN Communications and vice-versa
- Remote Access VPN Configuration
- VPN Monitoring and Logging
- VPN over Satellite links
- Certificate Management
- Troubleshooting & FAQ

The default policy in OmniVPN is to secure all communications and trust machines on the local subnet (machines that have OmniVPN installed on them or machines in the proxy list). Therefore, the factory setting for VPN security policies should be sufficient for almost all users.
OmniVPN Configuration

The VPN Policy editor application only runs on the “VPN Manager” node. It fully controls the security and firewall policies of all the computers in the VPN. The “VPN Manager” also provides centralized monitoring of the entire OmniVPN network.

Starting the VPN Policy Manager

To configure the VPN, start the “VPN policy manager”. This is accessible from the Start->All Programs->Trlokom OmniVPN->VPN Policy Manager, as shown in Figure 1A. Figure 1B shows a screen shot of the VPN Policy editor.

The bottom left corner of the policy editor displays the port number used by IKE. Trlokom’s OmniVPN enables a user to change the IKE port number if desired. The reason for changing the IKE port is to prevent the NATs with IPsec passthru from slowing down the number of IKE sessions. We recommend that port 6691 be used.
Adding Subnets (or Sites)

The VPN policies are defined according to subnets. Using these subnets to define the VPN policy is easier than using a separate mechanism for access control. The basic non-routable subnets are already available, and a user can add new subnets as necessary. Figure 2 shows how to add a new subnet. The “Policy” menu provides commands to add and remove subnets (Figure 1A). To edit an existing subnet, double-click it in either tree.

Figure 2A   Figure 2B

Selecting the “Add new subnet” menu item opens a new window (Figure 3). After the user has entered the subnet name (optional) and the address (required), the new subnet shows up in both the “Source” and “Destination” trees of the policy editor window (Figure 2B).

Figure 3

In this example we have added two subnets. The first subnet is named “VPN Site A” and has the IP address 192.168.99.0, and the second subnet is named “VPN Site B” and has the IP address 192.168.88.0. The two subnets could be the subnets for two corporate sites. For example, the “VPN Site A” may be in Boston behind the global IP address 166.19.68.40, and “VPN Site B” may be in Los Angeles behind the global IP address 65.213.57.72.
Setting the VPN Policy

To check the communication policy between any two subnets, select one subnet in the source and the other one in the destination tree as shown in Figure 5. A straight line between the two computer icons signifies that the communication between those two subnets is allowed. Just underneath that is an icon of a lock. If the lock is closed and green, the two subnets communicate with each other securely. If the communication between the two subnets is not secured, the lock is open, and its color is red. The status of communication is also reflected by the check boxes in the upper right hand corner of the policy editor window.

If communication between two subnets is to be secured, the user can use the “Transport mode”, the “Tunnel mode”, or the “End-to-end” mode. The “End-to-end” mode is similar to the “Transport mode” and provides NAT traversal and true end-to-end security. We strongly recommend that people use the End-to-end mode only. Figure 6 shows how the user can select a particular mode.
IKE Policy

Once the user has selected the mode to secure communication between two subnets, they can configure the ISAKMP and IPSec policies. By clicking on the “Add ISAKMP Proposal” button (Figure 7A), the window shown in Figure 7B pops up. Here the user can define the IKE Phase I authentication method and encryption policy.

The user must double-click an existing item if he/she chooses to edit it. The default lifetime of any security association (SA) will be 8 hours. The user can increase or decrease this lifetime as desired.
IPsec Policy

The addition of IPsec proposals is done in the same manner. Figure 8A and 8B shows the mechanism for adding a new IPsec proposal.

WAN to LAN communication

The communication from WAN (Internet) to LAN is blocked by default (Figure 9).

However, all communication from LAN to WAN is allowed (Figure 10). We strongly recommend that the security administrator use access control rules to limit the LAN to WAN access.
Figure 11A shows the access control window displayed when the “Add rule” button is clicked. If the user selects the http (port 80) from the pull-down menu, the outgoing http traffic will be blocked. The security administrator must be very careful here. The action taking by the access control rule depends on the state of the “Allow traffic” button. In this particular case, the “Allow traffic” button is checked and the rule for http becomes "block." A red cross sign appears next to the added rule to signify that traffic is blocked.

If the “Allow traffic” button is un-checked, the http rule will automatically become "allow" because it is pointless to have rules that are redundant with the default action.
Remote Access VPN Configuration

The central manager does not have to do much to configure remote access. The only responsibility of the central manager is to set the correct communication policy. **We suggest that a separate subnet be created for remote access users.** This makes policy definition for remote access users very easy. Figure 12 shows how a new subnet for remote access users can be added.

![Figure 12A](image1.png)  ![Figure 12B](image2.png)

To avoid routing conflicts, the subnet assigned for the remote access users must not be used anywhere else in the VPN.

Figure 13 shows how each remote access VPN client is given a unique IP address. The remote access client uses this IP address to connect to the VPN. This configuration is done through the “Local VPN configuration” application on each client.

If the remote access VPN client is connecting over a two-way satellite link, then the “Encapsulate all network traffic” box must be checked as shows in Figure 13.

![Figure 13](image3.png)
VPN using IPsec Tunnel Mode

While we strongly recommend that End-to-End mode be used for all communications, the user may wish to use the IPsec tunnel mode instead. This section will guide the user through the tunnel set up. (Note: Tunnel mode is much more difficult to configure than End-to-End mode.)

Currently, using tunnel mode means that the LAN communication will be unsecured because OmniVPN does not yet provide support for cascaded and nested tunnels. **In order to secure your LANs and WLANs, you must use End-to-End mode.**

**In the VPN policy editor:**

1) The SPD editor must be configured for tunnel mode between the two subnets, e.g., 192.168.10.0/24 -> 192.168.20.0/24 as shown in Figure 14A.

2) Policies must be created so that the gateways are able to communicate with each other using their global IP addresses.

   a. In the SPD Editor, create a new /32 subnet for each of the VPN gateways. These appear under WAN as shown in Figure 14B.

   b. Set the communication mode between the VPN gateways to either tunnel or transport mode.
On each gateway:

3) Two network interfaces are configured via their TCP/IP Properties dialogs:

   a. The WAN interface has a routable IP address, e.g., 101.101.101.20, and default gateway, e.g., 101.101.101.22, assigned by your ISP.
   b. The LAN interface has a non-routable IP address, e.g., 192.168.20.20, and does not have a default gateway specified, i.e., the input field is blank.

Figure 15 shows an example screen shot of the resulting gateway routing table.
On each end host:

4) Set the default gateway to the internal IP address of the VPN gateway.
   a. If the host’s IP address is assigned statically, set the default gateway’s IP address manually in the TCP/IP Properties dialog.
   b. Otherwise, configure your DHCP server to assign your OmniVPN gateway as the default gateway.

Figure 16 shows an example screen shot of the resulting host routing table.
VPN Over a Satellite Link

Trlokom’s OmniVPN 1.1.x will work over two-way satellite links when in road warrior mode. Any road warrior that accesses the Internet through a satellite link should have the “Encapsulate all network traffic” box checked in the VPN Configuration window. (Figure 17)
VPN Monitoring & Logging

Trlokom’s OmniVPN has several built-in utilities. These utilities help the administrator monitor the VPN status.

Network Topology

The VPN network topology can be viewed by clicking on “Window->Network topology”. This window shows the subnets and the global IP address that each one is behind. If there are any road warriors, they will appear in the bottom window which shows the IP address of each road warrior and the global address of the NAT that it is behind.

Figure 18
Certificate Management

The VPN manager and all gateways have a built-in certificate authority. The certificate management window can be invoked by clicking “Certificates->Manage certificates” in the policy editor window or clicking the “Manage certificates” button in the “Local VPN configuration” application window.

The top list displays the certificates that have been granted by the Certificate Authority (CA). You can revoke these by selecting them and clicking the Revoke button at the left of the list.

The "Active one-time certificates" list displays the one-time certificates that have not yet been used by a computer in the VPN to authenticate itself to the CA and obtain a permanent certificate. The "Revoked one-time certificates" list displays the one-time certificates that have been used. To transfer a certificate from one list to the other, select it and click the Revoke or Unrevoke button.

The list titled "Allowed to use one-time certificate" contains the IP addresses of computers that are allowed to authenticate themselves to the CA via a one-time certificate. If you check the option to allow any machine to use a one-time certificate, you do not need to enter any addresses explicitly. However, this is less secure because any machine that has a copy of the one-time certificates from your OmniVPN CD will be able to obtain a certificate and join your VPN. Of course, if you keep your OmniVPN CD in a safe place, this is unlikely to be a serious concern. However, it is always a good idea to turn off this option once you are done installing OmniVPN on all your computers in order to ensure that no more certificates are granted. The list to the right displays a history of which one-time certificate each computer used. If you see any IP addresses in this list that are not part of your VPN, then your CA has been compromised!

The bottom list contains the pre-shared text keys that particular computers can use to authenticate themselves to the CA. When a text key is used, it is automatically deleted from this list so that it cannot be re-used. Pre-shared text keys are primarily useful for allowing a remote gateway to obtain a certificate from the Manager. This avoids the need to use the same CD to install OmniVPN in different corporate offices.
Event Log

A detailed log of auditable events is kept at each client in the VPN. Each client reports the important local events to its local VPN gateway and that information is passed on to the VPN manager. Figure 19 shows a typical log file.

Figure 19

You can sort the events by any particular column by clicking on the column heading. The events are initially sorted by date, with the newest events at the top of the list.

The event severity is as follows:

- **Emergency**: System is unusable
- **Alert**: Problem requiring immediate attention
- **Critical error**: Serious problem
- **Error**: Problem
- **Warning**: Warning
- **Notice**: Important, normal event
- **Informational**: Miscellaneous events
- **Debugging**: Debugging output

The sole purpose of the value in the "ID" column is to provide a unique number so that you can look up more information about the event in the printed documentation.

If there is a number in the "Count" column, it indicates that the item is a summary of that many occurrences of the event. If an event occurs more than five times within three hours, OmniVPN begins recording only summaries to avoid overloading the event log. This is especially helpful during Denial of Service (DoS) attacks, because DoS attacks...
typically generate a very large amount of invalid network traffic which OmniVPN blocks.

The columns labelled as "Source IP," "Destination IP," etc. record the contents of the IP header of the received packet, which may have been modified by NATs. On the other hand, the columns labelled "True Source IP," "True Destination IP," etc. record the contents of the real IP addresses of the computers and real ports used by the network connection within the VPN.

The entire event log can be exported to a tab delimited text file and then imported into spreadsheets such as Excel. You can also export a portion of the event log by selecting the items that are of interest before exporting.
Troubleshooting

FAQ

Q: I have installed the necessary OmniVPN components without any problems, but the VPN is not working.

A. Refer to the checklist for OmniVPN installation: Common errors are:

- Not forwarding ports from the NAT to the ‘VPN Manager’ and ‘VPN Gateways’.
- Check the network topology from the ‘Policy Editor’ window. The network topology will tell you which VPN Gateways have registered and lists the VPN subnets and the global address of the NATs to reach those subnets.
- Another common error is that the security policy is set to not allow communication between two subnets. Start ‘Policy Manager’, select the appropriate source and destination subnets, and fix the security policy.
- If you are using Windows XP, do not use a Netgear network interface card (NIC). There is a bug in the Netgear software that prevents OmniVPN from working correctly.

Q: My VPN is working except for NetMeeting.

A. If NetMeeting is not working, there are two possible reasons:

- Check that the VPN Gateways are in the DMZ of their NATs.
- NetMeeting sometimes chooses a Trojan Port. Stop and re-start NetMeeting, and it should work.

Q: How do I know if my wireless LAN communication is secure?

A. Start the ‘Policy Editor’ on the VPN Manager. Select the LAN subnet in the source as well as the destination column. Check the policy. If the line connecting the two computer icons is a straight line and the padlock underneath is closed and green, your LAN communication is secure. If the padlock is red and open, your wireless network is not secure.

Q: I have a machine that is proxied for by the VPN Gateway, but I am not able to use that machine to connect to machines at other sites.

A. Check that the default gateway specified in the TCP/IP properties window on that machine is set to be the VPN Gateway. If this is set correctly, then try rebooting the machine to reset the routing table.
Q: *I have a two-way satellite link for Internet connectivity and my VPN is not working.*

A. Check the ‘Encapsulate all network traffic’ box in the VPN Configuration window of the machine using the satellite link. Also make sure that the computer is operating as a road warrior.

Q: *Why does it take so long to connect to the VPN when I turn on my laptop while travelling?*

A. It usually takes only a moment for OmniVPN to decide that it must be a Road Warrior. However, if one of the IP addresses in the list of potential OmniVPN gateways for End Host mode exists on the local subnet to which your computer is connected, then OmniVPN will first try to register with this machine. Only after this fails will OmniVPN switch to Road Warrior mode.

Q: *I changed my network interface card (NIC) or added a new NIC and now my VPN has stopped working.*

A. Reduce the MTU for your new NIC by 250. If there is no MTU value, set it to 1200. The MTU is set by using the program regedit.exe to change the value of "MTU" in all the sub-keys of the following registry key:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces
```

You should also change the ProtocolMTU and TunnelMTU values in all the sub-keys of the following registry key:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NdisWan\Parameters\Interfaces
```

All three MTU values have type REG_DWORD.