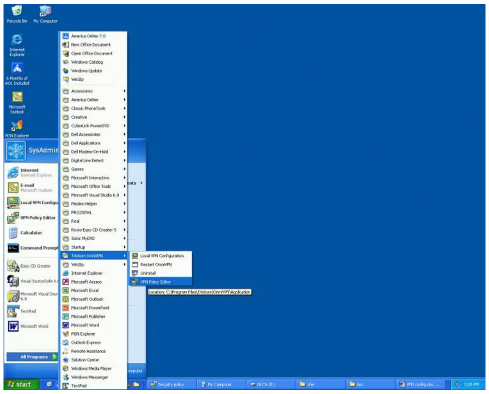
OmniVPN Configuration

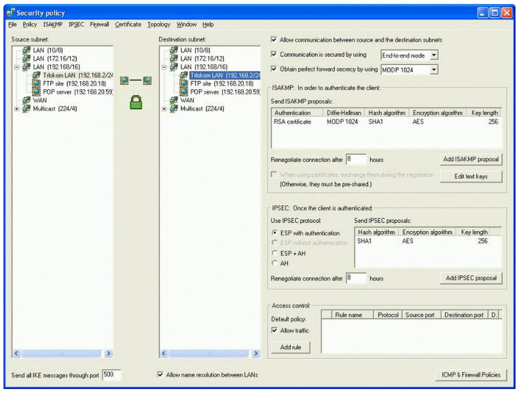
The VPN Policy editor application only runs on the “VPN Manager” node. It fully controls the security and firewall policies of the VPN. The “VPN Manager” also provides centralized monitoring of the entire OmniVPN network.

Starting the VPN Policy Editor

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



Location: C:\Program Files\Trlokom\OmniVPN\Application



☑ 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.

Send all IKE messages through port 500

☑ Allow name resolution between LANs

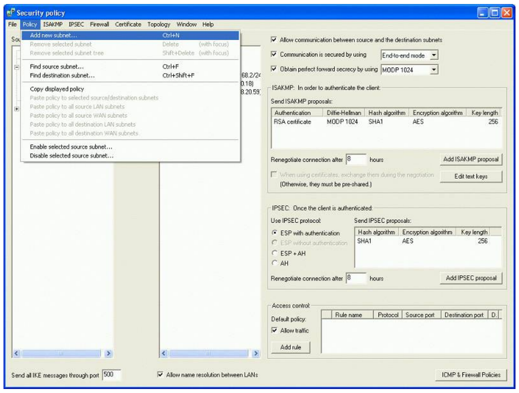
Figure 1A

Figure 1B

The bottom left corner of the SPD 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

The VPN policies are defined according to subnets. 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.


Security policy
File
Policy
ISAKMP
IPSEC
Firewall
Certificate
Topology
Window
Help
Add new subnet... Ctrl+N
Remove selected subnet Delete (with focus)
Remove selected subnet tree Shift+Delete (with focus)
Find source subnet... Ctrl+F
Find destination subnet... Ctrl+Shift+F
Copy displayed policy
Paste policy to selected source/destination subnets
Paste policy to all source LAN subnets
Paste policy to all source WAN subnets
Paste policy to all destination LAN subnets
Paste policy to all destination WAN subnets
Enable selected source subnet...
Disable selected source subnet...
Add ISAKMP proposal
Edit text keys
Add IPSEC proposal
Add rule
ICMP & Firewall Policies

☑ 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:

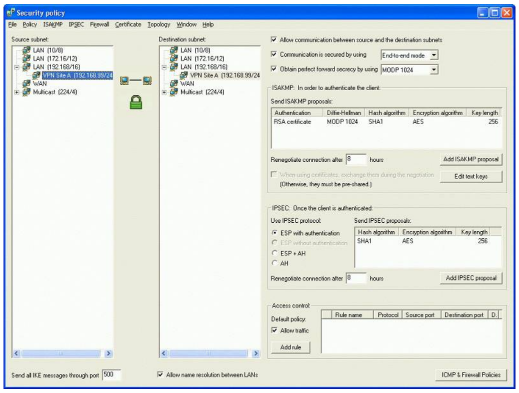
Default policy:
☑ Allow traffic

Rule name	Protocol	Source port	Destination port	D.

Send all IKE messages through port 500

☑ Allow name resolution between LANs

Figure 2A



Source subnet:
- LAN (10/8)
- LAN (172.16/12)
- LAN (192.168/16)
  - VPN Site A (192.168.99/24
- WAN
- Multicast (224/4)

Destination subnet:
- LAN (10/8)
- LAN (172.16/12)
- LAN (192.168/16)
  - VPN Site A (192.168.99/24
- WAN
- Multicast (224/4)

☑ 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

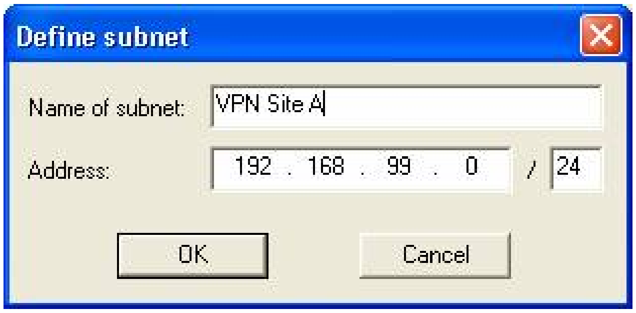
Rule name	Protocol	Source port	Destination port	D.

Send all IKE messages through port 500

☑ Allow name resolution between LANs

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).

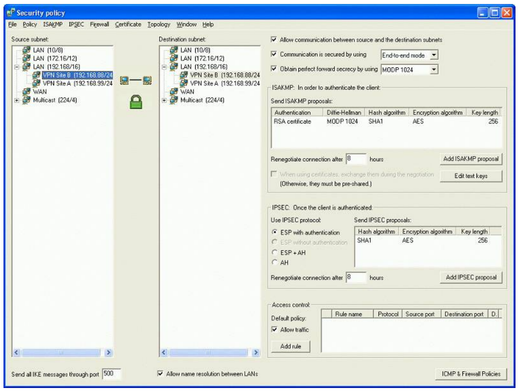


Name of subnet: VPN Site A

Address: 192 . 168 . 99 . 0 / 24

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.



Source subnet:
- LAN (10/8)
- LAN (172.16/12)
- LAN (192.168/16)
  - VPN Site B (192.168.88/24
  - VPN Site A (192.168.99/24
- WAN
- Multicast (224/4)

Destination subnet:
- LAN (10/8)
- LAN (172.16/12)
- LAN (192.168/16)
  - VPN Site B (192.168.88/24
  - VPN Site A (192.168.99/24
- WAN
- Multicast (224/4)

☑ 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.

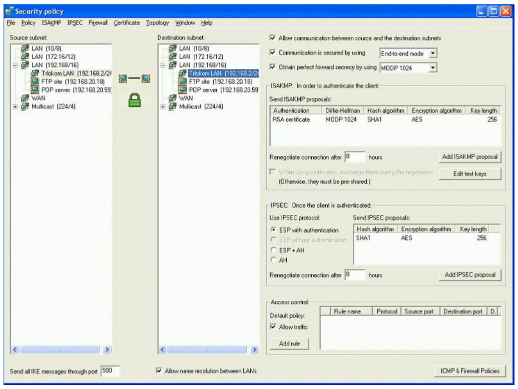
Send all IKE messages through port 500

☑ Allow name resolution between LANs

Figure 4

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.



Source subnet:
- LAN (10/8)
- LAN (172.16/12)
- LAN (192.168/16)
  - Trlokom LAN (192.168.2/24
  - FTP site (192.168.20.18)
  - POP server (192.168.20.59)
- WAN
- Multicast (224/4)

Destination subnet:
- LAN (10/8)
- LAN (172.16/12)
- LAN (192.168/16)
  - Trlokom LAN (192.168.2/24
  - FTP site (192.168.20.18)
  - POP server (192.168.20.59)
- WAN
- Multicast (224/4)

☑ 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.

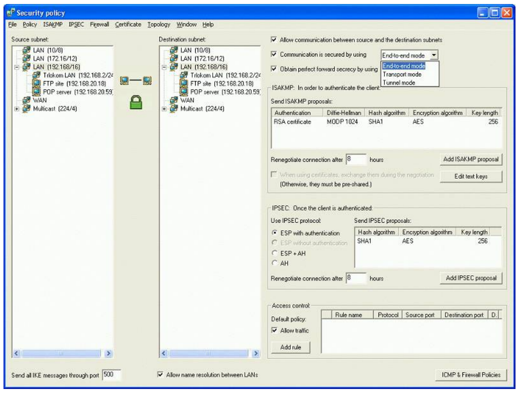
Send all IKE messages through port 500

☑ Allow name resolution between LANs

Communication policy between subnets

Figure 5

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.


Security policy
File Policy ISAKMP IPSEC Firewall Certificate Topology Window Help

Source subnet:

- LAN (10/8)
- LAN (172.16/12)
- LAN (192.168/16)
  - Trlokom LAN (192.168.2/24
  - FTP site (192.168.20.18)
  - POP server (192.168.20.59)
- WAN
- Multicast (224/4)

Destination subnet:

- LAN (10/8)
- LAN (172.16/12)
- LAN (192.168/16)
  - Trlokom LAN (192.168.2/24
  - FTP site (192.168.20.18)
  - POP server (192.168.20.59)
- WAN
- Multicast (224/4)

☑ Allow communication between source and the destination subnets

☑ Communication is secured by using: End-to-end mode

☑ Obtain perfect forward secrecy by using

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.

Send all IKE messages through port 500

☑ Allow name resolution between LANs

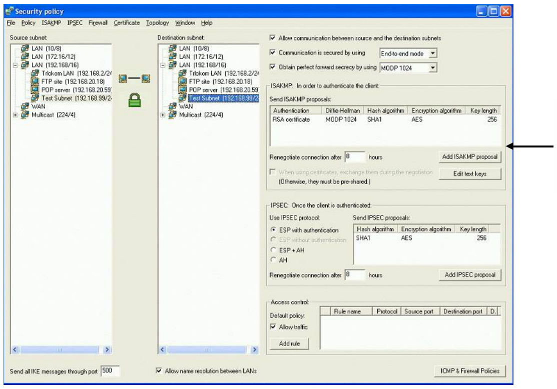
Figure 6

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.

To edit an existing item, double click it.

The default lifetime of any security association (SA) will be 8 hours. The user can increase or decrease these lifetimes as desired.


Security policy
File Policy ISAKMP IPSEC Firewall Certificate Topology Window Help

Source subnet:

- LAN (10/8)
- LAN (172.16/12)
- LAN (192.168/16)
  - Trlokom LAN (192.168.2/24
  - FTP site (192.168.20.18)
  - POP server (192.168.20.59)
  - Test Subnet (192.168.99/2
- WAN
- Multicast (224/4)

Destination subnet:

- LAN (10/8)
- LAN (172.16/12)
- LAN (192.168/16)
  - Trlokom LAN (192.168.2/24
  - FTP site (192.168.20.18)
  - POP server (192.168.20.59)
  - Test Subnet (192.168.99/2
- WAN
- Multicast (224/4)

☑ 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

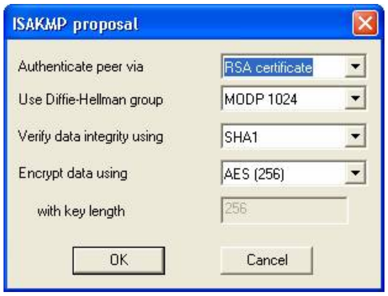
	Rule name	Protocol	Source port	Destination port	D.

Send all IKE messages through port 500

☑ Allow name resolution between LANs

Add new proposal

Figure 7A



Authenticate peer via: RSA certificate

Use Diffie-Hellman group: MODP 1024

Verify data integrity using: SHA1

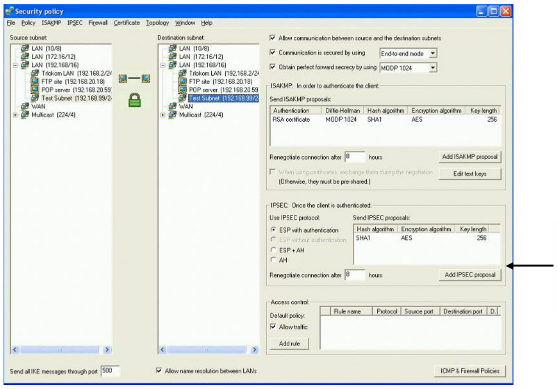
Encrypt data using: AES (256)

with key length: 256

Figure 7B

IPsec Policy

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


Security policy
File Policy ISAKMP IPSEC Firewall Certificate Topology Window Help

Source subnet:
- LAN (10/8)
- LAN (172.16/12)
- LAN (192.168/16)
  - Trlokom LAN (192.168.2/24
  - FTP site (192.168.20.18)
  - POP server (192.168.20.59)
  - Test Subnet (192.168.99/2
- WAN
- Multicast (224/4)

Destination subnet:
- LAN (10/8)
- LAN (172.16/12)
- LAN (192.168/16)
  - Trlokom LAN (192.168.2/24
  - FTP site (192.168.20.18)
  - POP server (192.168.20.59)
  - Test Subnet (192.168.99/2
- WAN
- Multicast (224/4)

☑ 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:

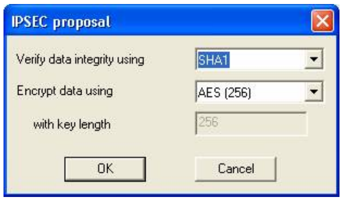
Default policy:
☑ Allow traffic

Rule name	Protocol	Source port	Destination port	D.

Send all IKE messages through port 500
☑ Allow name resolution between LANs

Add new proposal

Figure 8A

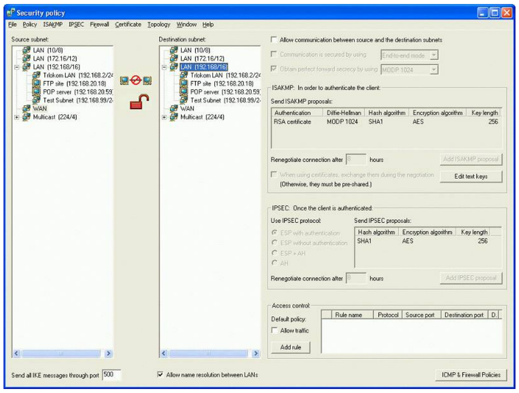


Verify data integrity using: SHA1
Encrypt data using: AES (256)
with key length: 256

Figure 8B

WAN to LAN communication

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


Security policy
File Policy ISAKMP IPSEC Firewall Certificate Topology Window Help

Source subnet:
- LAN (10/8)
- LAN (172.16/12)
- LAN (192.168/16)
  - Trlokom LAN (192.168.2/24
  - FTP site (192.168.20.18)
  - POP server (192.168.20.59)
  - Test Subnet (192.168.99/2
- WAN
- Multicast (224/4)

Destination subnet:
- LAN (10/8)
- LAN (172.16/12)
- LAN (192.168/16)
  - Trlokom LAN (192.168.2/24
  - FTP site (192.168.20.18)
  - POP server (192.168.20.59)
  - Test Subnet (192.168.99/2
- WAN
- Multicast (224/4)

□ 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:

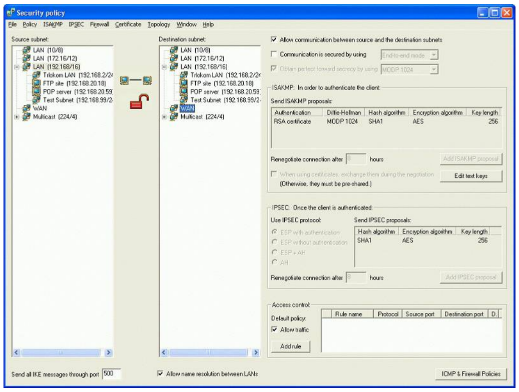
Default policy:
□ Allow traffic

Rule name	Protocol	Source port	Destination port	D.

Send all IKE messages through port 500
☑ Allow name resolution between LANs

Figure 9A

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.



☑ 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

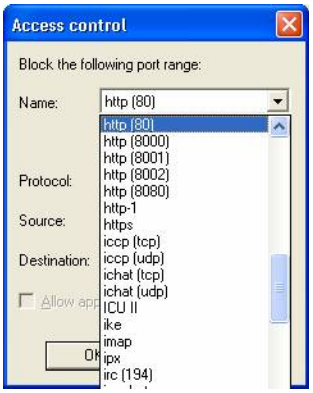
Rule name	Protocol	Source port	Destination port	D.

Send all IKE messages through port 500

☑ Allow name resolution between LANs

Figure 10

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.



Block the following port range:

Name: http (80)

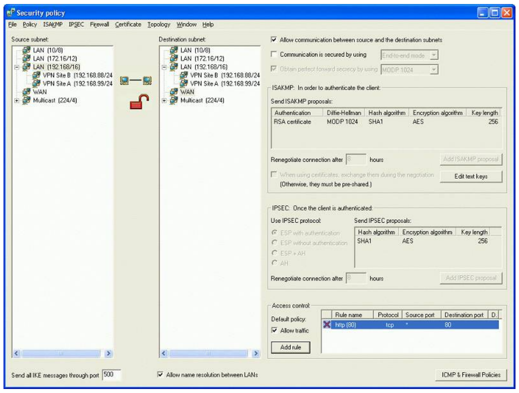
Protocol:

Source:

Destination:

☐ Allow app

Figure 11A



☑ 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.
☒	http (80)	tcp	*	80	

Send all IKE messages through port 500

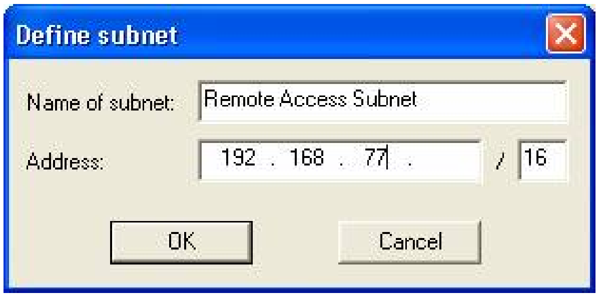
☑ Allow name resolution between LANs

Figure 11B

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

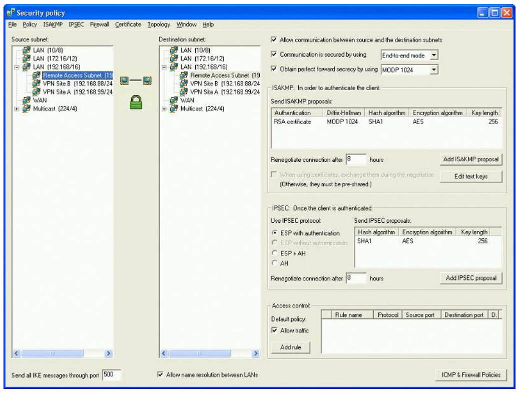
The central manager does not have to do much to configure remote access. The only responsibility of the central manager is to set the correct communication policy. **<u>We suggest that a separate subnet be created for remote access users</u>**. This makes policy definition for remote access users very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



Name of subnet: Remote Access Subnet

Address: 192 . 168 . 77 . / 16

Figure 12A



Source subnet:
- LAN (10/8)
- LAN (172.16/12)
- LAN (192.168/16)
  - Remote Access Subnet (19
  - VPN Site B (192.168.88/24
  - VPN Site A (192.168.99/24
- WAN
- Multicast (224/4)

Destination subnet:
- LAN (10/8)
- LAN (172.16/12)
- LAN (192.168/16)
  - Remote Access Subnet (19
  - VPN Site B (192.168.88/24
  - VPN Site A (192.168.99/24
- WAN
- Multicast (224/4)

☑ 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.

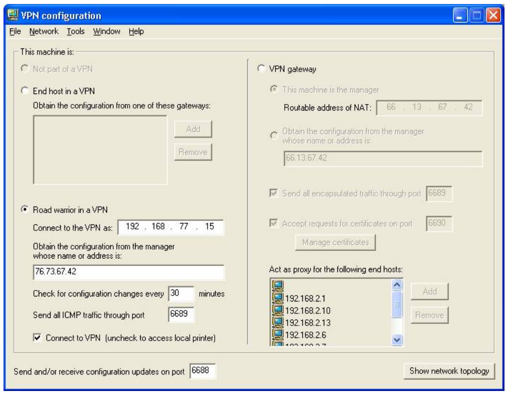
Send all IKE messages through port 500

☑ Allow name resolution between LANs

Figure 12B

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 at the client.



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 . 77 . 15
Obtain the configuration from the manager whose name or address is:
76.73.67.42
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:
- 192.168.2.1
- 192.168.2.10
- 192.168.2.13
- 192.168.2.6

Send and/or receive configuration updates on port 6688

Figure 13

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. (It is much more difficult to configure than End-to-End mode.)

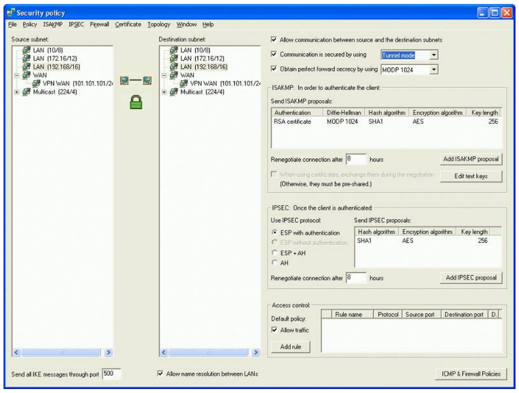
Currently, using tunnel mode means that the LAN communication will be unsecured because OmniVPN does not yet provide support for cascaded and nested tunnels. **In order to secure your LANs and WLANs, you must use End-to-End mode.**

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.



☑ Allow communication between source and the destination subnets
☑ Communication is secured by using Tunnel 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

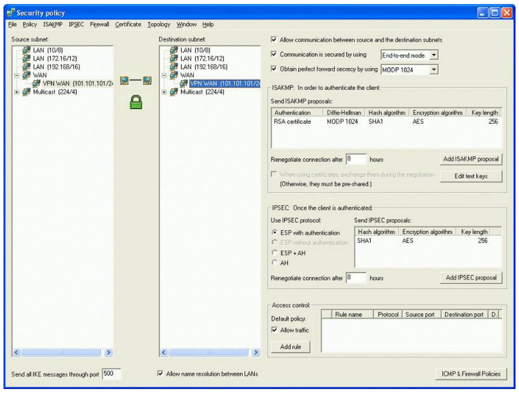
Renegotiate connection after 8 hours

Access control:
Default policy:
☑ Allow traffic

	Rule name	Protocol	Source port	Destination port	D.

Send all IKE messages through port 500
☑ Allow name resolution between LANs

Figure 14A



☑ 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.

Send all IKE messages through port 500
☑ Allow name resolution between LANs

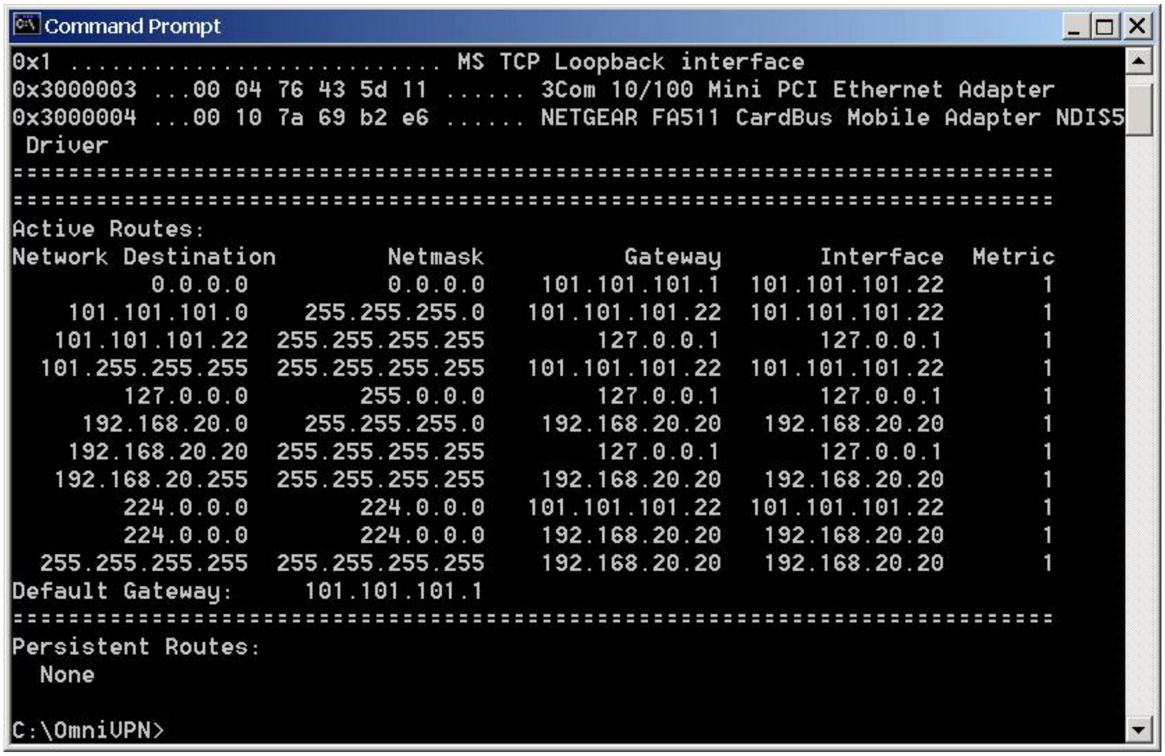
Figure 14B

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.



```
0x1 ........................... MS TCP Loopback interface
0x3000003 ...00 04 76 43 5d 11 ...... 3Com 10/100 Mini PCI Ethernet Adapter
0x3000004 ...00 10 7a 69 b2 e6 ...... NETGEAR FA511 CardBus Mobile Adapter NDIS5
 Driver
===========================================================================
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0    101.101.101.1  101.101.101.22       1
    101.101.101.0    255.255.255.0   101.101.101.22  101.101.101.22       1
   101.101.101.22  255.255.255.255        127.0.0.1       127.0.0.1       1
  101.255.255.255  255.255.255.255   101.101.101.22  101.101.101.22       1
        127.0.0.0        255.0.0.0        127.0.0.1       127.0.0.1       1
     192.168.20.0    255.255.255.0    192.168.20.20   192.168.20.20       1
    192.168.20.20  255.255.255.255        127.0.0.1       127.0.0.1       1
   192.168.20.255  255.255.255.255    192.168.20.20   192.168.20.20       1
        224.0.0.0        224.0.0.0   101.101.101.22  101.101.101.22       1
        224.0.0.0        224.0.0.0    192.168.20.20   192.168.20.20       1
  255.255.255.255  255.255.255.255    192.168.20.20   192.168.20.20       1
Default Gateway:     101.101.101.1
===========================================================================
Persistent Routes:
  None

C:\OmniVPN>
```

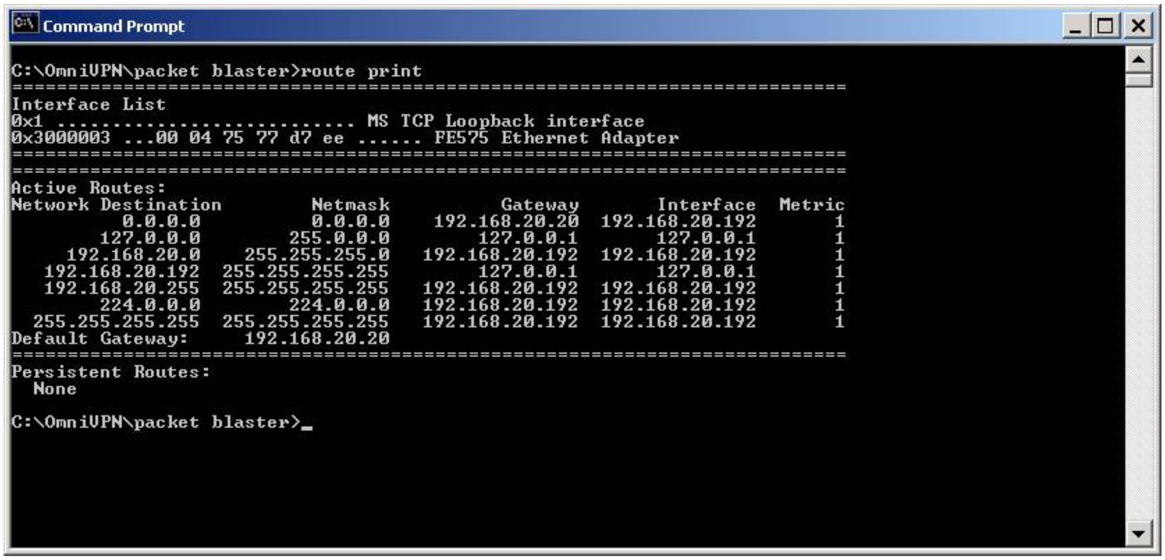
Figure 15

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.



```
C:\OmniVPN\packet blaster>route print
===========================================================================
Interface List
0x1 ........................... MS TCP Loopback interface
0x3000003 ...00 04 75 77 d7 ee ...... FE575 Ethernet Adapter
===========================================================================
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0    192.168.20.20  192.168.20.192       1
        127.0.0.0        255.0.0.0        127.0.0.1       127.0.0.1       1
     192.168.20.0    255.255.255.0   192.168.20.192  192.168.20.192       1
   192.168.20.192  255.255.255.255        127.0.0.1       127.0.0.1       1
   192.168.20.255  255.255.255.255   192.168.20.192  192.168.20.192       1
        224.0.0.0        224.0.0.0   192.168.20.192  192.168.20.192       1
  255.255.255.255  255.255.255.255   192.168.20.192  192.168.20.192       1
Default Gateway:     192.168.20.20
===========================================================================
Persistent Routes:
  None

C:\OmniVPN\packet blaster>_
```

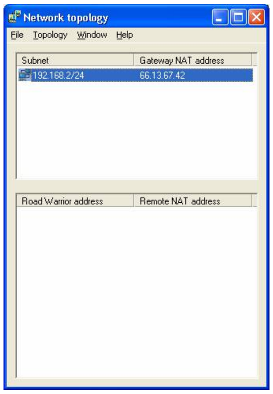
Figure 16

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.



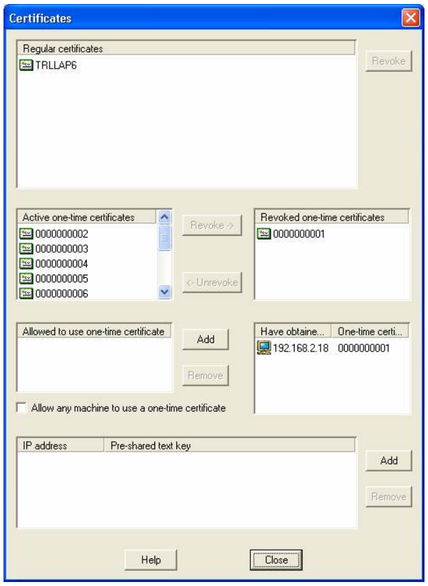
Subnet	Gateway NAT address
192.168.2/24	66.13.67.42

Road Warrior address	Remote NAT address

Figure 17

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.



Regular certificates
TRLLAP6

Active one-time certificates
0000000002
0000000003
0000000004
0000000005
0000000006

Revoked one-time certificates
0000000001

Allowed to use one-time certificate

Have obtaine...	One-time certi...
192.168.2.18	0000000001

☐ Allow any machine to use a one-time certificate

IP address	Pre-shared text key

Figure 18

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.

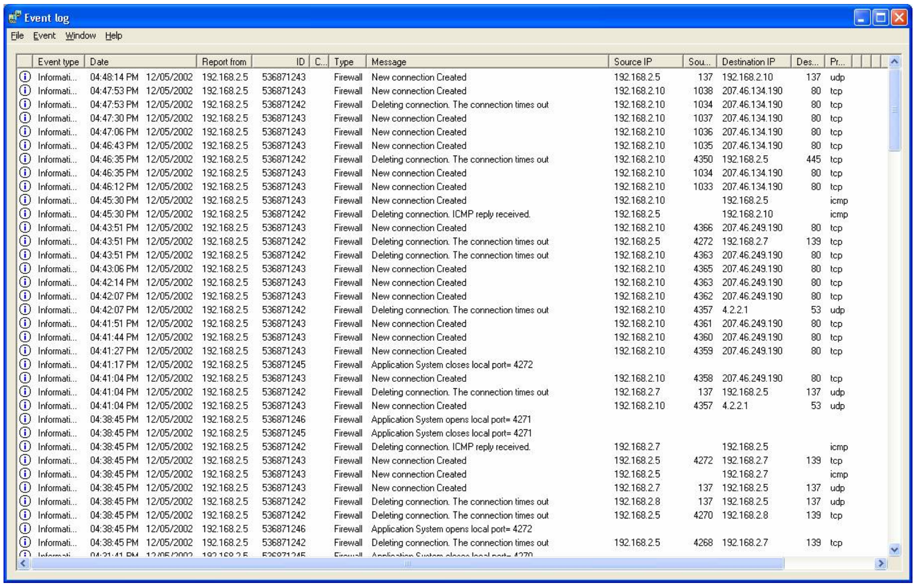
The "Active one-time certificates" list displays the one-time certificates that have not yet been used by a computer in the VPN to authenticate itself to the CA and obtain a permanent certificate. The "Revoked one-time certificates" list displays the one-time certificates that have been used. To transfer 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 on the Manager and the remote gateway.

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.



	Event type	Date	Report from	ID	C...	Type	Message	Source IP	Sou...	Destination IP	Des...	Pr...
ⓘ	Informati...	04:48:14 PM 12/05/2002	192.168.2.5	536871243		Firewall	New connection Created	192.168.2.5	137	192.168.2.10	137	udp
ⓘ	Informati...	04:47:53 PM 12/05/2002	192.168.2.5	536871243		Firewall	New connection Created	192.168.2.10	1038	207.46.134.190	80	tcp
ⓘ	Informati...	04:47:53 PM 12/05/2002	192.168.2.5	536871242		Firewall	Deleting connection. The connection times out	192.168.2.10	1034	207.46.134.190	80	tcp
ⓘ	Informati...	04:47:30 PM 12/05/2002	192.168.2.5	536871243		Firewall	New connection Created	192.168.2.10	1037	207.46.134.190	80	tcp
ⓘ	Informati...	04:47:06 PM 12/05/2002	192.168.2.5	536871243		Firewall	New connection Created	192.168.2.10	1036	207.46.134.190	80	tcp
ⓘ	Informati...	04:46:43 PM 12/05/2002	192.168.2.5	536871243		Firewall	New connection Created	192.168.2.10	1035	207.46.134.190	80	tcp
ⓘ	Informati...	04:46:35 PM 12/05/2002	192.168.2.5	536871242		Firewall	Deleting connection. The connection times out	192.168.2.10	4350	192.168.2.5	445	tcp
ⓘ	Informati...	04:46:35 PM 12/05/2002	192.168.2.5	536871243		Firewall	New connection Created	192.168.2.10	1034	207.46.134.190	80	tcp
ⓘ	Informati...	04:46:12 PM 12/05/2002	192.168.2.5	536871243		Firewall	New connection Created	192.168.2.10	1033	207.46.134.190	80	tcp
ⓘ	Informati...	04:45:30 PM 12/05/2002	192.168.2.5	536871243		Firewall	New connection Created	192.168.2.10		192.168.2.5		icmp
ⓘ	Informati...	04:45:30 PM 12/05/2002	192.168.2.5	536871242		Firewall	Deleting connection. ICMP reply received.	192.168.2.5		192.168.2.10		icmp
ⓘ	Informati...	04:43:51 PM 12/05/2002	192.168.2.5	536871243		Firewall	New connection Created	192.168.2.10	4366	207.46.249.190	80	tcp
ⓘ	Informati...	04:43:51 PM 12/05/2002	192.168.2.5	536871242		Firewall	Deleting connection. The connection times out	192.168.2.5	4272	192.168.2.7	139	tcp
ⓘ	Informati...	04:43:51 PM 12/05/2002	192.168.2.5	536871242		Firewall	Deleting connection. The connection times out	192.168.2.10	4363	207.46.249.190	80	tcp
ⓘ	Informati...	04:43:06 PM 12/05/2002	192.168.2.5	536871243		Firewall	New connection Created	192.168.2.10	4365	207.46.249.190	80	tcp
ⓘ	Informati...	04:42:14 PM 12/05/2002	192.168.2.5	536871243		Firewall	New connection Created	192.168.2.10	4363	207.46.249.190	80	tcp
ⓘ	Informati...	04:42:07 PM 12/05/2002	192.168.2.5	536871243		Firewall	New connection Created	192.168.2.10	4362	207.46.249.190	80	tcp
ⓘ	Informati...	04:42:07 PM 12/05/2002	192.168.2.5	536871242		Firewall	Deleting connection. The connection times out	192.168.2.10	4357	4.2.2.1	53	udp
ⓘ	Informati...	04:41:51 PM 12/05/2002	192.168.2.5	536871243		Firewall	New connection Created	192.168.2.10	4361	207.46.249.190	80	tcp
ⓘ	Informati...	04:41:44 PM 12/05/2002	192.168.2.5	536871243		Firewall	New connection Created	192.168.2.10	4360	207.46.249.190	80	tcp
ⓘ	Informati...	04:41:27 PM 12/05/2002	192.168.2.5	536871243		Firewall	New connection Created	192.168.2.10	4359	207.46.249.190	80	tcp
ⓘ	Informati...	04:41:17 PM 12/05/2002	192.168.2.5	536871245		Firewall	Application System closes local port= 4272					
ⓘ	Informati...	04:41:04 PM 12/05/2002	192.168.2.5	536871243		Firewall	New connection Created	192.168.2.10	4358	207.46.249.190	80	tcp
ⓘ	Informati...	04:41:04 PM 12/05/2002	192.168.2.5	536871242		Firewall	Deleting connection. The connection times out	192.168.2.7	137	192.168.2.5	137	udp
ⓘ	Informati...	04:41:04 PM 12/05/2002	192.168.2.5	536871243		Firewall	New connection Created	192.168.2.10	4357	4.2.2.1	53	udp
ⓘ	Informati...	04:38:45 PM 12/05/2002	192.168.2.5	536871246		Firewall	Application System opens local port= 4271					
ⓘ	Informati...	04:38:45 PM 12/05/2002	192.168.2.5	536871245		Firewall	Application System closes local port= 4271					
ⓘ	Informati...	04:38:45 PM 12/05/2002	192.168.2.5	536871242		Firewall	Deleting connection. ICMP reply received.	192.168.2.7		192.168.2.5		icmp
ⓘ	Informati...	04:38:45 PM 12/05/2002	192.168.2.5	536871243		Firewall	New connection Created	192.168.2.5	4272	192.168.2.7	139	tcp
ⓘ	Informati...	04:38:45 PM 12/05/2002	192.168.2.5	536871243		Firewall	New connection Created	192.168.2.5		192.168.2.7		icmp
ⓘ	Informati...	04:38:45 PM 12/05/2002	192.168.2.5	536871243		Firewall	New connection Created	192.168.2.7	137	192.168.2.5	137	udp
ⓘ	Informati...	04:38:45 PM 12/05/2002	192.168.2.5	536871242		Firewall	Deleting connection. The connection times out	192.168.2.8	137	192.168.2.5	137	udp
ⓘ	Informati...	04:38:45 PM 12/05/2002	192.168.2.5	536871242		Firewall	Deleting connection. The connection times out	192.168.2.5	4270	192.168.2.8	139	tcp
ⓘ	Informati...	04:38:45 PM 12/05/2002	192.168.2.5	536871246		Firewall	Application System opens local port= 4272					
ⓘ	Informati...	04:38:45 PM 12/05/2002	192.168.2.5	536871242		Firewall	Deleting connection. The connection times out	192.168.2.5	4268	192.168.2.7	139	tcp

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, whereas 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 for importing 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.