OmniVPN Firewall User Reference

0. Preface

This document is a detailed description about Trlokom's OmniVPN firewall features. OmniVPN is the first end-to-end VPN product integrated with distributed enterprise firewall functions. The firewall is built around a fully stateful inspection engine that applies access control, Trojan detection, attack prevention, etc. functions.

Table of Contents

1. Access Control

1.1 Access control features

- Stateful inspection for TCP, UDP for each subnet
- Global stateful inspection for ICMP
- Allow/deny broadcast/multicast IP packets (no stateful inspection)
- Allow RSVP (no stateful inspection)
- Drop all other packets
- Stateful inspection for ftp, netmeeting, traceroute, and tftp.
- Block well-known trojans

1.2 Access control configuration

There are two sets of access control rules:

- global access control rules
- subnet based access control rules

Global access control rules apply to any source/destination IP address pair. Subnet based access control rules apply only to packets that match a certain subnet.

1.2.1 Configuring subnet based access control rules

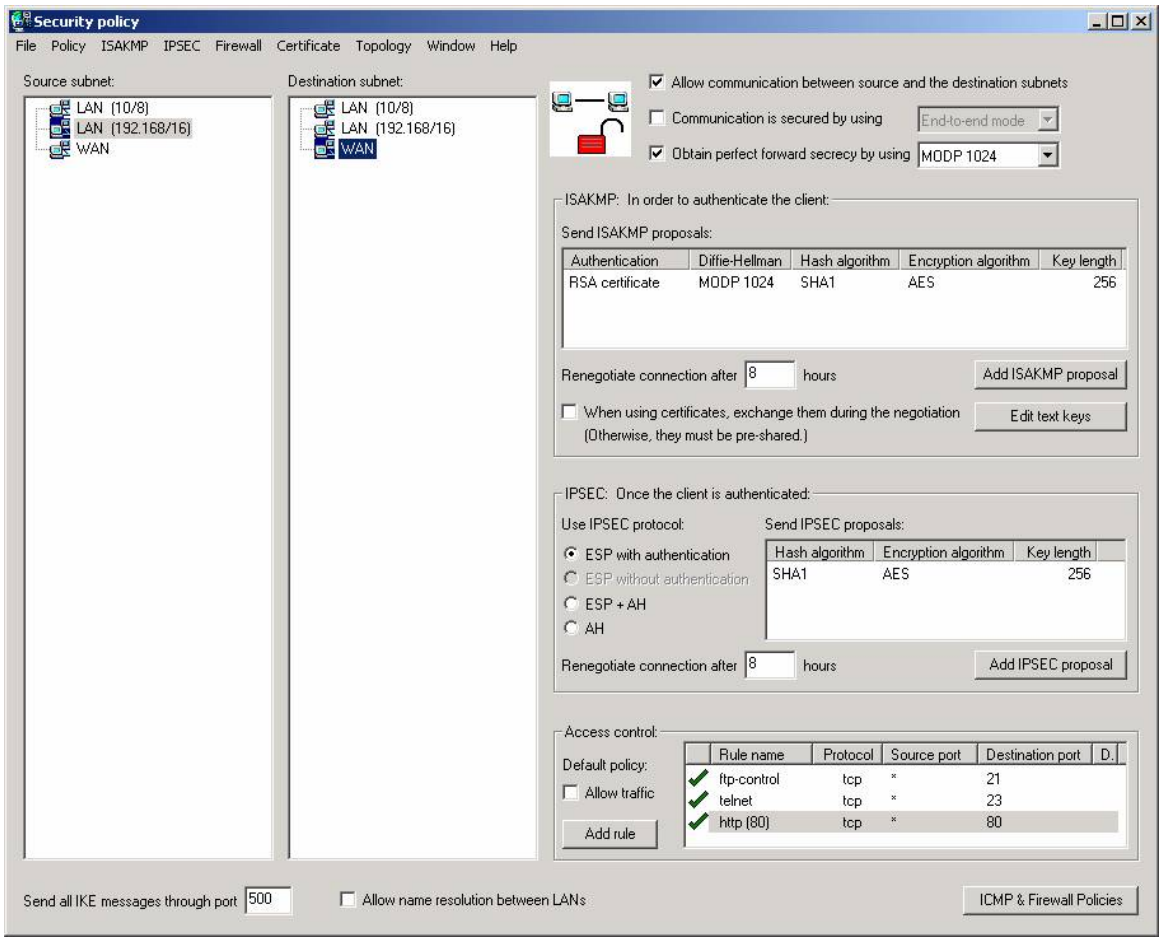


Figure 1: The SPD editor.

Under the “Access control” area in the SPD manager window, the user can add the access control rules. There is a check button to specify the default rule for this SPD, which can be either "allow all traffic" or "deny all traffic." To add a specific access control rule:

- Click the add rule button and a window will pop up to configure the access control parameters.
- Enter the rule name.
- Enter protocol(TCP/UDP) name.
- Enter source port and destination port.
- The last parameter is a check box “Allow application to open dynamic ports”. This is to support application that support dynamically negotiated ports, such as Microsoft Netmeeting, etc.

To filter traffic by application protocols using dynamic negotiated ports, user need to enable the check box “Allow application to open dynamic ports”. The system will monitor the application program that has traffic matches this access control rule. If a

match is found, any NEW port opened by the application program will be allowed to send/receive traffic to/from any port of the same remote machine. The restriction is that the NEW port can receive from/send to only one remote port. This works fine for application as Microsoft Netmeeting. But will not work for dynamically allocated server port applications, such as RPC service, etc.

Currently there are no separate windows for incoming and outgoing rules. After the incoming (or outgoing) ACL rules are set, the user must select the source as the destination in the SPD editor window (Figure 1) and vice versa to set the ACL rules for outgoing (or incoming) connections.

1.2.2 Configuring global access control rules

There are several kind of global access control rules:

- ICMP rules
- Trojan definition
- DoS attacks

There is also a check box to allow user to disable the firewall function. In this case, OmniVPN performs VPN function only and no firewall rules are applied.

The “Protect against the following Trojan horses” window lists all the default Trojans the system can detects. User defined Trojans can be added by click the “Add” button.

The following is the description of ICMP rules. The attacks and Trojan definitions will be addressed in Section 2 and Section 3.

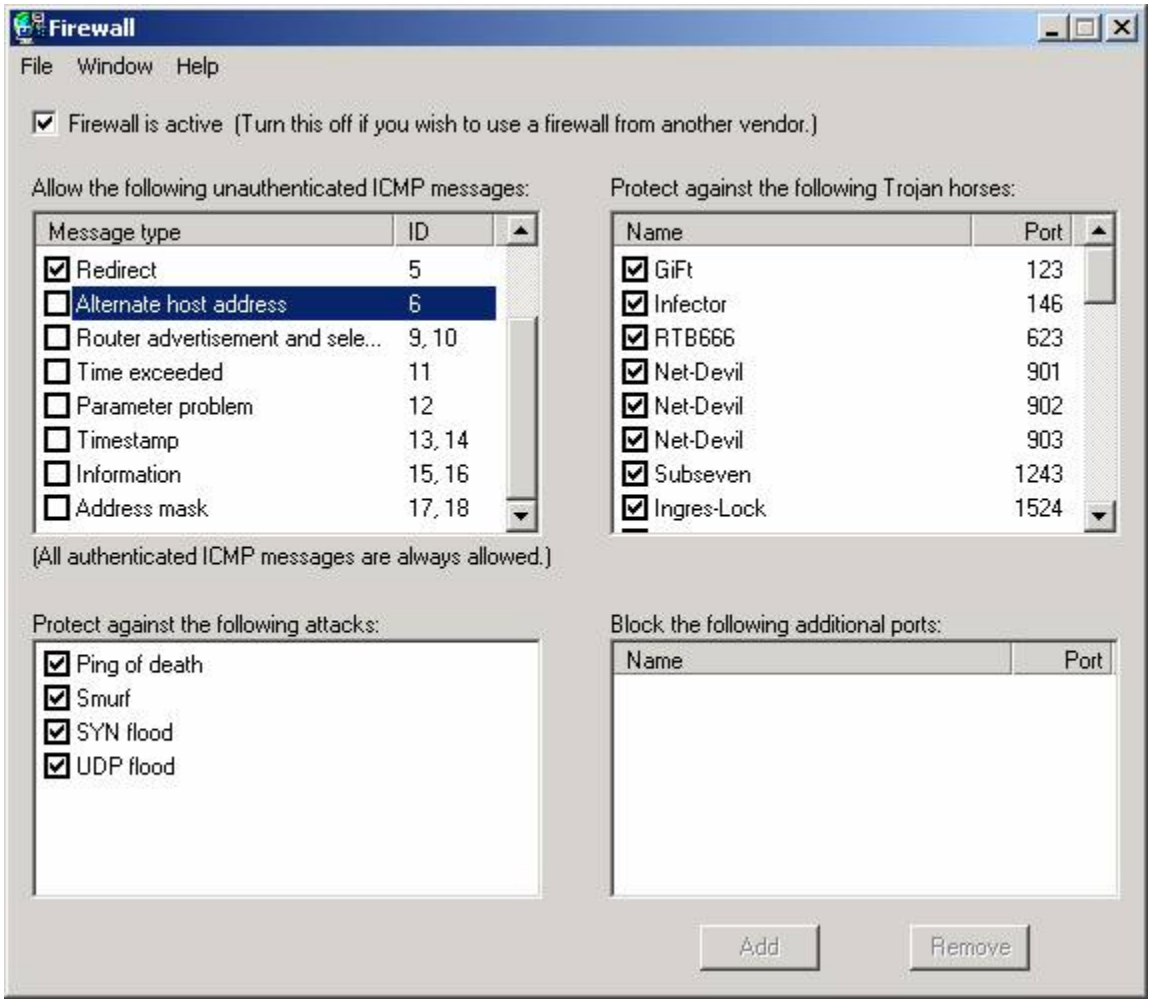


Figure 2

1.2.2.1 ICMP rules

OmniVPN always allows outgoing ICMP messages. User can choose to allow or deny any of the following incoming ICMP messages:

ECHO/ECHO reply	8, 0
Destination Unreachable	3
Source Quench	4
Redirect	5
Router advertisement	9
Router selection	10
Time Exceeded	11
Parameter Problem	12
Timestamp Request/Response	13, 14
Information Request/Response	15, 16
Address mask request/response	17, 18

2. Attacks Prevented/Detected

OmniVPN can detect/prevent the following attacks:

- ICMP flood

  If there are too many ICMP packets received in a period of time, it is an indication that there may be an ICMP flood attack. Typically the ICMP traffic in any network is less than 1% of the total traffic. Currently, the threshold is set to be 500 packet in a 5 seconds window. This translates to at most 1.2Mb/s bandwidth (assuming 1500 byte packets, which is unlikely for genuine ICMP traffic). Clearly this threshold is not ideal for gigabit or faster networks. In the next version, it will become configurable. The threshold of 500 packets per 5 second window seems to number for detection of ICMP flood.

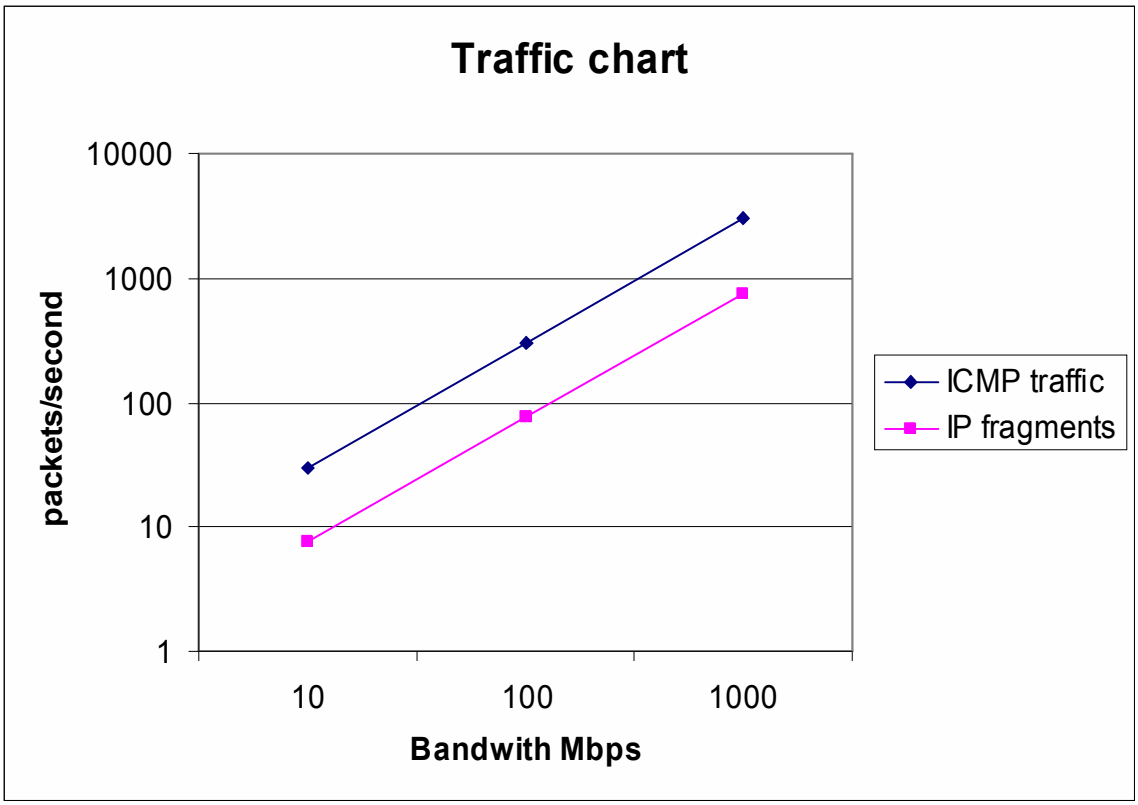
  After the system detects an ICMP flood, it will automatically drop following ICMP traffic, until it detects the ICMP traffic level returns to normal. Then ICMP packets will be re-enabled again. This mechanism ensures that the network can recover to its normal state.

- Fragment flood

  If there are too many fragmented packets received in a period of time, it is an indication that there may be a fragment flood attack. Currently, the threshold is set to be 500 packets in a 5 seconds window. In the next version, it will become configurable.

  After the system detects a fragment flood, it will automatically drop following IP fragments, until it detects the IP fragments level returns to normal. Then IP fragments will be re-enabled again.

  Theoretically, the threshold of ICMP and IP fragments is linear to the link capacity. The following is a chart of ICMP and IP fragments packet rate according to link capacity. It based on the Internet traffic statistics, which shows around 1% packets are ICMP and 0.75% packets are fragments.



- Packet flood attack to not-allowed ports.

  If dropped packets use too much bandwidth for a certain period of time, it's an indication there is a packet flood attack against the host. Typically firewalls drop less than 1% of the packets in absence of an attack. By setting the threshold at 5% we reduce the false alarm rate while catching DoS attacks quickly before they take up too much system resources.

- Tiny fragment and overlapped fragment attack

  There are two kind of attacks using malformed IP fragments, Tiny fragment attack and overlapping fragment attack. The details of these attacks are in RFC1858. Tiny fragment attack uses unusually small first fragment that does not cover the whole TCP header.

  The overlapped fragment attack use overlapped fragment offset to over write the content of the previous fragment by the next fragment. This could result in illegal packet to penetrate firewall or crash the destination system. OmniVPN will automatically detect these attacks and drop the malformed packets.

- IP options and unknown IP options

  IP options can be a big security risk. OmniVPN provides two levels of protection.
  - Block all packets with option.
  - Block packets with unknown IP option. The 25 known IP options are listed below and packets with any other IP option will be discarded.

```
#define IPOPT_EOL         0     /* end of option list */
#define IPOPT_NOP         1     /* no operation */
#define IPOPT_RR          7     /* record packet route */
#define IPOPT_TS          68    /* timestamp */
#define IPOPT_SECURITY    130   /* provide s,c,h,tcc */
#define IPOPT_LSRR        131   /* loose source route */
#define IPOPT_SATID       136   /* satnet id */
#define IPOPT_SSRR        137   /* strict source route */
#define IPOPT_RA          148   /* router alert */
#define IPOPT_ESEC        133   //Extended security
#define IPOPT_CIPSO       134   //commercial security
#define IPOPT_ZSU         10    //Experimental Measurement
#define IPOPT_MTUP        11    //MTU probe
#define IPOPT_MTUR        12    //MTU reply
#define IPOPT_FINN        205   //experimental flow control
#define IPOPT_VISA        142   //experimental access control
#define IPOPT_ENCODE      15
#define IPOPT_IMITD       144   //IMI Traffic Descriptor
#define IPOPT_EIP         145   //Extended Internet Protocol
#define IPOPT_TR          82    //trace route
#define IPOPT_ADDEXT      147   //Address extension
#define IPOPT_SDB         149   //Selective Directed Broadcast
#define IPOPT_NASPA       150   //NSAP Addresses
#define IPOPT_DPS         151   //Dynamic Packet State
#define IPOPT_UMP         152   //Upstream Multicast Packet
```

- UDP flood attack

  If there are too many UDP packets received in a period of time, it's an indication that there is an UDP flood attack. Currently, the threshold is set to be 50Mbps, which is about half of the bandwidth of a 100Mbps Ethernet link, in a 5 seconds window. In the next version, it will become configurable.

  After the system detects an UDP flood, it will automatically drop following UDP traffic, until it detects the UDP traffic level returns to normal. Then the UDP packets will be re-enabled again.

3. Event Logging

3.1 Event log features

The agent running on the host sends event log messages to the policy manager. The policy manager receives log messages from all the hosts. The communication between policy manager and hosts are encrypted using IPsec.

There are eight event log levels. Only those logs that are below the current event log level get logged. The level definitions follow the syslog convention. They are:

```
LOG_EMERG       /* system is unusable */
```

```
LOG_ALERT       /* action must be taken immediately */
LOG_CRIT        /* critical conditions */
LOG_ERR         /* error conditions */
LOG_WARNING     /* warning conditions */
LOG_NOTICE      /* normal but significant condition */
LOG_INFO        /* informational */
LOG_DEBUG       /* debug-level messages */
```

3.2 General format of event log messages

The general format of event log message is show in Figure 3.

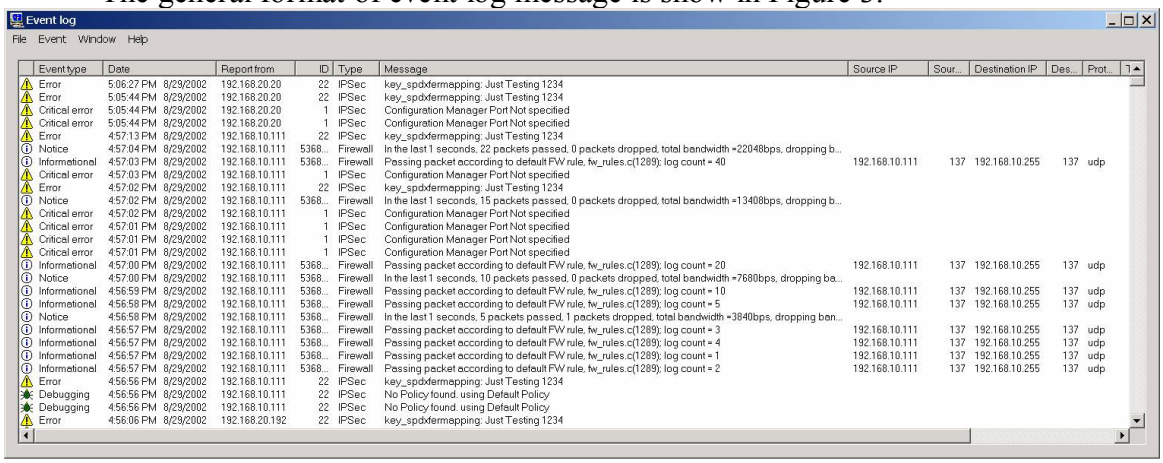


Figure 3

3.3 Log message category

- Statistics
  OmniVPN keep tract of the number of total/dropped packets, and bandwidth usages. It's useful for monitoring network usage. This log is generated every 10 minutes.
- Attacks
  Shows what attack it is and also gives the action taken if firewall can prevent it.
- Trojan horses
  Shows Trojan port. Also, if applicable, shows the Trojan name and the application program name that associates with the Trojan port.
- Socket open/close
  Whenever an application open or close a socket, a notice level event will be generated.
- Connection creation/deletion
  Whenever a connection is created or destroyed, a notice level event will be generated.
- Packet dropping
  Whenever a packet is drop, an event log is generated including the protocol, src/dst IP addresses and src/dst ports of the dropped packet.
- Packet passing

Whenever a packet is passed, an informational level event log is generated including the protocol, src/dst IP addresses and src/dst ports of the passed packet.

4. Trouble Shooting

4.1 FAQ

Q: My default policy is allowing all traffic, when I send traffic between 2 ports that are not in the blocked port list, the packet still gets dropped.
A. This is most likely that the used ports are in the Trojan list. OmniVPN will automatically block all traffic from/to Trojan ports even the default rule is to allow all traffic. If you are absolutely sure that the application you are using is safe, you can remove the port from the Trojan list and the application will work.

Q: I am using an OmniVPN proxy to do firewall for one of my host. I am not able to use Microsoft Netmeeting even though I allow Netmeeting in the access control list.
A. Netmeeting is a dynamic port allocation application. The OmniVPN works for this kind of applications only when it's installed on the host. Since proxy do not have local host's application information, Netmeeting won't work for host firewalled through proxy. Next version of the Firewall will support Netmeeting for the proxy case as well.

4.2 Trouble shooting error messages

Message ID	Error message	Explanation	Problem resolution
536871215	Drop an ICMP echo reply message	This is caused by the global ICMP rule settings.	To allow ICMP echo reply messages, check the "Echo" checkbox in the firewall window.
536871216	Drop an ICMP destination unreachable message	This is caused by the global ICMP rule settings.	To allow ICMP destination unreachable messages, check the "Destination unreachable" checkbox in the firewall window.
536871217	Drop an ICMP source quench message	This is caused by the global ICMP rule settings.	To allow ICMP source quench messages, check the "Source quench" checkbox in the firewall window.
536871218	Drop an ICMP redirect message	This is caused by the global ICMP rule settings.	To allow ICMP redirect messages, check the "Source quench" checkbox in

			the firewall window.
536871219	Drop an ICMP echo request message	This is caused by the global ICMP rule settings.	To allow ICMP echo request messages, check the "Echo" checkbox in the firewall window.
536871222	Drop an ICMP timestamp message	This is caused by the global ICMP rule settings.	To allow ICMP timestamp messages, check the "Timestamp" checkbox in the firewall window.
536871222	Drop an ICMP time exceeded message	This is caused by the global ICMP rule settings.	To allow ICMP time exceeded messages, check the "Time exceeded" checkbox in the firewall window.
536871223	Drop an ICMP parameter problem message	This is caused by the global ICMP rule settings.	To allow ICMP parameter problem messages, check the "Parameter problem" checkbox in the firewall window.
536871224	Drop an ICMP timestamp request message	This is caused by the global ICMP rule settings.	To allow ICMP timestamp request messages, check the "Timestamp" checkbox in the firewall window.
536871225	Drop an ICMP timestamp reply message	This is caused by the global ICMP rule settings.	To allow ICMP timestamp reply messages, check the "Timestamp" checkbox in the firewall window.
536871226	Drop an ICMP information request message	This is caused by the global ICMP rule settings.	To allow ICMP information request messages, check the "Information" checkbox in the firewall window.
536871227	Drop an ICMP information reply message	This is caused by the global ICMP rule settings.	To allow ICMP information reply messages, check the "Information" checkbox in the firewall window.

536871228	Drop an ICMP address mask request message	This is caused by the global ICMP rule settings.	To allow ICMP address mask request messages, check the "Address mask" checkbox in the firewall window.
536871229	Drop an ICMP address mask reply message	This is caused by the global ICMP rule settings.	To allow ICMP adrress mask reply messages, check the "address mask" checkbox in the firewall window.
536871230	Drop an ICMP router solicitation or router advertisement message	This is caused by the global ICMP rule settings.	To allow ICMP router solicitation or router advertisement message, check the "router solicitation, advertisement" checkbox in the firewall window.
536871247	Firewall detects an attack	This attack message is used when an unrecognized attack occurs.	User usually should not see this message.
536871248	A memory allocation for firewall module failed		
536871249	Miscellaneous firewall error		
536871238	The packet is dropped according to access control rules	This is caused by either matching a specific access control rule if the default access control rule is "allow all" or the default access control rule if the default is "block all."	To block traffic: If the default access control rule is "allow all," click on the "Add rule" button in the Security Policy window to add an access control rule. If the default access control rule is "block all," select the rule that allowed the packet to pass and press the "Delete" key.
536871241	The packet is dropped according to an access	This is caused by one of the access control rules.	To allow traffic, select the rule that allowed the packet to pass

	control rule		and press the "Delete" key.
536871281	The packet did not match any specific allow rule, hence got dropped by default	This is caused by default access control rule.	To allow traffic, there are two options: 1) Click on the "Add rule" button in the Security Policy window to add an access control rule. This is the correct approach because it does not change the default access policy. 2) **NOT** recommended: Change the default access control check box to allow all traffic. Care must be taken here as this might cause either security problems or access control problems with other applications. Note that changing the default policy will reverse the setting for all rules in the list.
536871242	A connection entry is deleted from the connection table	For a TCP connection, this happens after a connection is closed. For a UDP connection, this happens when there is no UDP traffic on that connection for more than 3 minutes. For an ICMP connection, this happens when an ICMP reply message is received.	
536871243	A new connection is created	For a TCP connection, this happens after the first SYN packet is sent or received. For a UDP connection, this happens when a UDP packet is received and does not match any existing connection. For an ICMP connection, this happens when an ICMP request message is sent.	

536871244		This is a statistics message. It shows, over the last period of time, how many packets passed, how many packets were dropped, and the total bandwidth usage.	
536871245		This is an informational message. An application program has closed a socket.	
536871246		This is an informational message. An application program has opened a socket.	
536871274	Firewall detects a UDP flood attack	Too many UDP packets were received in a period of time. This is an indication that there is a UDP flood attack. Currently, the threshold is set to be 50mbps, which is about half of the bandwidth of a 100mbps ethernet link, in a 5 seconds window. In the next version, it will be configurable.	After the system detects a UDP flood, it will automatically drop all UDP traffic until it detects that the UDP traffic level has returned to normal. Then the UDP packets will be passed again.
536871275	Firewall detects an ICMP flood attack	Too many ICMP packets were received in a period of time. This is an indication that there is an ICMP flood attack. Currently, the threshold is set to be 500 packet in a 5 seconds window. In the next version, it will be configurable.	After the system detects an ICMP flood, it will automatically drop all ICMP traffic until it detects that the ICMP traffic level has returned to normal. Then ICMP packets will be passed again.
536871276	Firewall detects an IP fragment flood attack	Too many fragmented packets were received in a period of time. This is an indication that there is a fragment flood attack. Currently, the threshold is set to be 500 packet in a 5 seconds window. In the next version, it will be configurable.	After the system detects a fragment flood, it will automatically drop all IP fragments until it detects that the IP fragments level has returned to normal. Then IP fragments will be passed again.
536871277	Firewall detects a tiny IP fragment attack	These are two kind of attacks using malformed IP fragments. The details are in RFC1858. Tiny fragment attacks use an unusually small first fragment that does not cover the whole TCP header. The overlapped fragment attack uses overlapped	OmniVPN will automatically detect these kind of packets and drop them.

		fragment offsets so the second fragement overwrites the content of the first fragment. This can result in illegal packets.	
536871278	Firewall drops a packet with IP option	IP options are a big security risk. OmniVPN provides two levels of protection. The user can choose to block all packets with options or only packets with unknown options.	
536871279	Firewall drops a packet with unknown IP option		
536871214	Stateful connection table is full	The connection table entry is full. No more connections can be recorded.	This can be caused by a DoS attack. The connection entry table should never overflow under normal network usage.