

Firewalls Netasq

Security
Management
by NETASQ

NETASQ
Secure Internet Connectivity



Security Management is handled by the ASQ, a Technology developed by NETASQ.

ASQ (Active Security Qualification) module:

ASQ is a technology which provides Netasq firewalls not only with a very high security level but also with very powerful tools to assist in configuration and maintenance.

ASQ is based on four different analysis methods:

- packet format analysis
- connection analysis
- global context analysis
- data applications programme analysis (level 7 of OSI model)

The analysis of packet format comprises an examination of compliance with the standards and RFC of all protocols managed by the Netasq firewall and a rejection of packets which could be used to generate hacking in some systems (by means of a known-attacks base). This analysis enables the firewalls to manage attacks with no context.

The connections analysis enables the security policy to be better applied at the filtering level (for example, by suppressing the opening of temporary ports for return packets) but it also makes the firewall configuration much easier and more intuitive (connection mode rather than packet mode, intelligent FTP mode, etc.). Connection management enables the firewall to provide records (logs); the statistics are more accurate and pertinent and the alarms are much clearer. Furthermore, an analysis of the connection content also, obviously, strengthens the firewall protection system by detecting specific types of hacking and their context

The analysis of the global context is the key to the power of ASQ technology. This precise and meticulous examination of all the activity on the network means that the firewall can help the user with configuration, simplify administration (the hybrid mode) and detect 'developed' attacks (attacks with context).

The data application analysis is the 'finishing touch' which enables the user to monitor data in transit by the protocols it has authorized. For example, it can prohibit access to certain web sites, mask SMTP banners etc. In terms of security the analysis of data applications verifies the consistency ('Stateful Application').

ASQ therefore regroups, correlates and analyses all the data obtained by the preceding methods and compares them with its global 'knowledge base). This is built on Stateful Inspection, on a hacking base and an in-depth knowledge of network layers and it opens up a multitude of possibilities for security, as well as for configuration and administration. Furthermore, it is a security for the rapid development of the product and a magnificent springboard for the future.

Management of hacking without context:

Hacking without context is the easiest to detect once you have a real research and development laboratory specialising in security which can extend a knowledge base of known hacking and develop appropriate counter-measures.

This type of hacking mainly comprises 'malformed' packets in which the 'options' field is configured 'unpredictably' or which some systems do not manage and which therefore entail abnormal operation, for example 'Land', 'Xmas Tree' and Null.

This category also includes address spoofing, remote analysis such as Queso and Nmap and certain DNS hacking such as Labell recursion attacks.

Management of hacking with context:

Some hacking is not based on the use of a malformed packet but on the behaviour of a machine when it receives several packets, which would be normal if received in isolation.

For example, a simple port scan consists in trying to initialise connections on a list of ports. A firewall without the necessary 'intelligence' will only allow a succession of normal packets to pass: a connection demand, therefore, will not trigger an alert, though the sender's behaviour may be construed as potentially hostile. SYN Flooding, which is a denial of service, is just one example from a list which, unfortunately, is growing daily. All the firewalls in the NETASQ range will protect you against this type of attack using counter-measures developed by the NETASQ team - a permanent security watch.

Management of potential unidentified hacking:

The ASQ was wholly designed to block the majority of known hackers but also to protect you against hackers not yet listed.

Thus the strength of the system's TCP/IP battery, the Firewall's thorough knowledge of network standards and protocols and the family structure of the embedded « knowledge base » mean that some types of packet or some forms of connection which could disturb systems or applications in the future are already detected as potential hacking by the Netasq firewall.

Analysis of application programme (level 7 of the OSI model)

In order to guarantee a level of security up to the programme application level, Netasq firewalls include the «Statefull Application programme» which allows the user to monitor data transiting through the authorized protocols and which also check the coherence of the commands given to certain sensitive applications, at the same time diminishing the flow rate as little as possible (unlike Proxie-type solutions).

This technology enables the user, for example, to prohibit access to certain WEB sites, to mask SMTP banners, to monitor certain FTP actions and prohibit the relaying of mail. In addition the firewall blocks all erroneous SMTP and DNS commands, thus limiting the risk of hacking at application programme level on the ports it manages.

A fully safeguarded system:

NETASQ firewalls are based on a completely secure hardware and software architecture.

The principle of «appliance»-type boxes guarantees the integrity and reliability of the operating system as well as the firewall application programme layer. The software section is already fully installed and the failures in security arising from faulty installation are therefore eliminated. In addition, the NETASQ research and development laboratory in the UNIX world have enabled us to design an operating system in which reliability is optimised.

The NETASQ box hardware concentrates wholly on the security options (filtering, hacking detection, encryption etc.) and optimises them.

Access to the system is protected by password and exchanges between the administration console and the firewall are encrypted in 128-bit TSL.

The firewall's default passwords are not generic; they are created randomly so that each firewall reaches the end client with a different password.

High availability :

- Management of a cluster (2 firewalls)
- Self-monitoring
- Mutual-monitoring
- Master – Slave Mode + Active – Passive Mode
- Automatic synchronization of the configuration
- Real Time Monitor

Main attacks and family attacks managed by Netasq Firewalls :

The aim of this part is to give a glimpse of our products' power in terms of security and not to give the whole list of the attacks managed by NETASQ firewalls. Some attacks which are not documented or have a different name, can also be managed by the firewall.

Furthermore, updates of our firewalls are evenly available, including new attacks detection.

Warning message	Description
'IP loopback address spoofing'	A packet coming from one of the network interfaces is pretending to come from the firewall.
'IP address spoofing'	A packet possesses an invalid source address on the interface used (Typically: pretending that a packet comes from an internal machine when in fact it comes from an external machine).
'broadcast packet'	A packet's destination is the network's Broadcast address. This packet may be legitimate, but might also be seeking to saturate the network
'multicast packet'	A packet's destination is an address corresponding to several machines on the network (a multicast address). This packet may be legitimate (videoconference, etc.), but may also be seeking to saturate the network.
'address from experimental class'	A packet's source address is an address reserved for tests, that should not be used under normal circumstances.
'bad IP options'	The packet contains errors and is therefore not valid. This type of packet may be the result of a problem on the source machine, but deliberately bad packets are occasionally used to test the reactions of destination machines.
'unknown IP options'	The packet contains unknown or rarely used IP options.
'unknown IP protocol'	Protocol other than TCP, UDP, ICMP and not covered by the Firewall.
'unknown internal network host'	The packet's destination is a non-existent machine. The source of this problem may be an error or an exhaustive search for possible addresses.
'oversize fragment [Jolt...]	A fragmented packet, once rebuilt, exceeds the maximum allowed size. This type of packet is used to force certain OSs, such as early Windows 95 versions or certain MacOS versions, to reboot.
'overlapped fragment [Teardrop, Nestea, Bonk, Syndrop...]	A packet's fragments are not distinct (the data from one fragment overwrite those of another fragment). This method is used in several types of attack, generally causing the machine to reboot.
'bad ICMP packet type'	The packet is an ICMP message of unknown type. This type of packet probably corresponds to a problem on the source machine, or to a test to study the response of the destination machine.

'ICMP response without request [Pong, Smurf...]'	An ICMP response has been received when no request has been sent. This type of message is often used to generate excess traffic to a machine or a network.
'invalid RIP packet'	A RIP packet (containing routing information) is invalid.
'Invalid TCP option'	The packet contains an invalid TCP option. This packet may be an error, but may also be used to study the response of the destination machine.
'Unknown TCP option'	The packet contains an unknown or rarely used TCP option.
'wrong TCP sequence number'	A TCP packet contains an incorrect sequence number. This may be an error (mainly at the end of connection), but may also be an attempted attack from a third party trying to pass as the contact.
'Wrong TCP checksum'	The packet's checksum does not correspond to that packer. The packet has probably suffered from a transmission error.
'multicast address with TCP'	A TCP packet has a multicast address as its destination (an address representing several machines). This type of packet should not exist.
'"xmas tree" packet'	An "xmas tree" packet (for which all options are activated) has been intercepted. The aim of this type of packet is to trigger the shutdown of the destination machine.
'"land" style packet'	A packet has requested a TCP connection whose source and target are identical (same IP address, same port). This type of attack blocks a large number of TCP implementations.
'source routing'	The packet forces the route to take. This option is rarely used outside of attempted attacks.
'nmap OS probe'	The nmap tool is used in an attempt to detect a machine's OS type.
'queso OS probe'	The queso tool is used in an attempt to detect a machine's OS type.
'Firewall policy detection [Firewalk, logroute]'	Special packets are generated in order to determine the exact path to a destination (Weak TTL field, incremented for each successive packet).
'port scan'	An abnormal number of connection attempts has been recorded. This generally corresponds to a scan of the machine's ports, providing information concerning the services provided.
'ICMP flooding'	ICMP packets are received massively. The cause may be a problem on the network, or an attack. The risk is network saturation.
'UDP flooding'	A machine sends an abnormal amount of UDP packets. This method may be used to saturate a server.

'TCP SYN flooding'	A machine makes several TCP connection requests, but never confirms these connections. This method is often used to saturate a server.
'UDP service loopback [Snork...]'	A packet attempts to generate a large volume of loopback traffic between two UDP services (for example two echos), possible on the same machine.
'DNS label recursion attack'	A "shield" DNS request has been built when decoding the packet. This type of request is intended to saturate a name server.
'Empty IP fragment'	One of the IP fragments contains no data
'Port 0 used in a connection'	A TCP or UDP packet contains the number of port 0 which must not be used.
'Windows bug on OOB data [Winnuke, Killwin...]	Anomaly in the TCP protocol (urgent data counter) which blocks some versions of Windows.
'possible small MSS attack'	The MSS size becomes so small that the system can no longer treat the frames. The system is therefore saturated and must undergo a DoS.