

# Comparative analysis

## **NETASQ** vs Fortinet











# Key advantages to NETASQ solutions

- ✓ Proactive when encountering threats
- ✓ High-performance architecture
- ✓ Maximum protection for businesses of all sizes
- ✓ Licenses for unlimited number of users
- ✓ Complete shield from threats
- ✓ Simplified vulnerability detection and auditing
- ✓ Simplified risk management
- ✓ Abnormal network behavior blocked

## Maximum protection for businesses of all sizes

NETASQ offers the highest level of protection throughout its whole range. All modes of protection are present by default, without the need to purchase additional options.

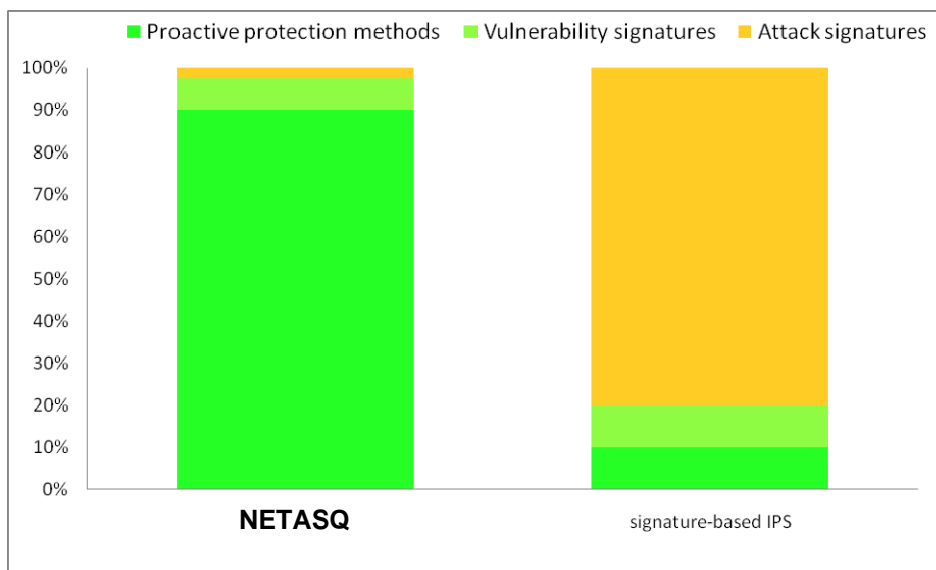
	Fortinet	NETASQ standard license
<b>IPS</b>	 As an option (Fortiguard)	 All IPS protection modes are available.
<b>Antivirus</b>	 As an option (Fortiguard)	 The embedded antivirus module includes a proactive engine and a database of more than 500 000 antivirus signatures.
<b>Antispam</b>	 As an option (Fortiguard)	 NETASQ's Antispam module combines reputation and heuristic analyses to eradicate SPAM.
<b>URL filtering</b>	 As an option (Fortiguard)	 NETASQ's URL filtering module is embedded in the product to ensure optimum performance.

## Effective intrusion prevention

NETASQ's intrusion prevention engine combines various technologies and more than 10 years' worth of research to arrive at delivering the highest level of security:

- ✓ Protocol analysis and security
- ✓ Behavioral analyses
- ✓ Proactive protection contextual signatures
- ✓ Contextual signatures for protection from threats and attacks.

Fortinet's IPS is based on a single signature database and communicates actively about its reaction time when a new threat appears. NETASQ's intrusion prevention technologies have been specially researched to provide proactive protection.





Distribution between the different categories of protection

	Fortinet	NETASQ
<b>Protocol IPS</b>	<p style="text-align: center;"><b>✗</b></p> <p>IPS largely inspired by Snort and signatures do not offer optimum protection from 0-day attacks</p>	<p style="text-align: center;"><b>✓</b></p> <p>NETASQ combines protocol analyses and protection signatures</p>
<b>Behavioral analyses</b>	<p style="text-align: center;"><b>✗</b></p> <p>Fortinet's IPS is based on the detection of ports, which is an ineffective method of protection</p>	<p style="text-align: center;"><b>✓</b></p> <p>NETASQ detects protocols in real time regardless of the port in order to detect any anomalies.</p>
<b>IPS Performance</b>	<p style="text-align: center;"><b>✗</b></p> <p>Activating Fortinet's IPS feature causes performance to plunge by 80%</p>	<p style="text-align: center;"><b>✓</b></p> <p>NETASQ's performance includes the activation of intrusion prevention</p>

## Case study of the Kaminsky DNS vulnerability

The exploitation of this vulnerability allows passing off false DNS responses for valid responses (DNS spoofing). The attacks work on the basis of being able to guess the random elements (DNS ID and UDP port) necessary for creating a response in the right format.

	Fortinet	NETASQ
Detection of attack behavior	<b>x</b>	 "Targeted DNS spoofing attempt" alarm raised
Allowing a single valid response	<b>x</b>	 The behavioral analysis only allows one response in the event of an attack.

A search for "DNS spoofing" on the Fortiguard® website only displays one detection signature by the metasploit tool. There is no mention of a more thorough analysis.

**NETASQ's different behavioral analyses provide effective protection from the attack discovered by Mr Kaminsky.**

## High-performance architecture

NETASQ's architecture relies on the synergies between hardware architecture and the operating system. The Fortinet architecture combines dedicated hardware components (ASIC) and software analyses.

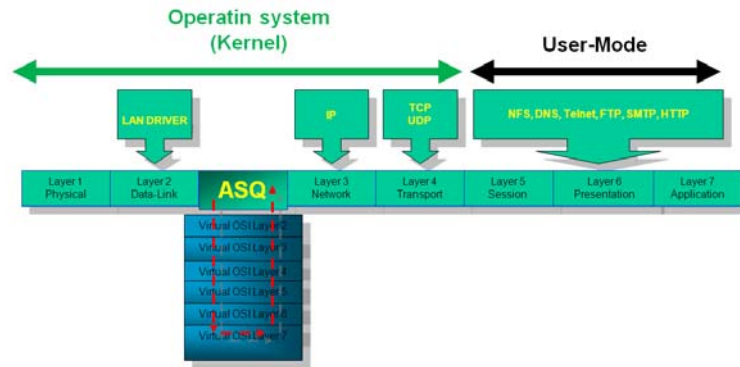
Fortinet actively communicates information about its hardware architecture. A technological choice like this would not have been out of place 10 years ago, but is irrelevant today because of the evolution of security needs:

1. Fortinet's network ASIC is **not used when intrusion prevention is enabled**.
2. Fortinet's content ASIC imposes many restrictions and **does not avoid changes in context and data duplication (software <-> hardware transfers)** thereby largely limiting the improvements in performance.

The gross performance that Fortinet highlights (Firewall and IPSec) degrades rapidly and drastically as soon as the slightest security scan is launched by software.

	Fortinet	NETASQ standard license
<b>Global performance</b>	<p style="text-align: center;">-</p> <p>The investment is spread out between the main processor and the dedicated circuits</p>	<p style="text-align: center;">+</p> <p>The use of powerful processors benefits from the analyses on the whole</p>
<b>IPS</b>	<p style="text-align: center;">-</p> <p>Execution of a software application</p>	<p style="text-align: center;">+</p> <p>Combination of analyses embedded in the operating system</p>
<b>Anti-spam</b>	<p style="text-align: center;">-</p> <p>Software analysis performed in several stages</p>	<p style="text-align: center;">+</p> <p>Heuristic analysis on the fly</p>
<b>URL filter</b>	<p style="text-align: center;">-</p> <p>Database hosted on the Internet</p>	<p style="text-align: center;">+</p> <p>URL database compiled in an optimized format and compared locally.</p>

NETASQ's architecture is based on the operating system's direct use of a powerful central processor. Intrusion prevention, carried out in the operating system, ensures optimum performance:

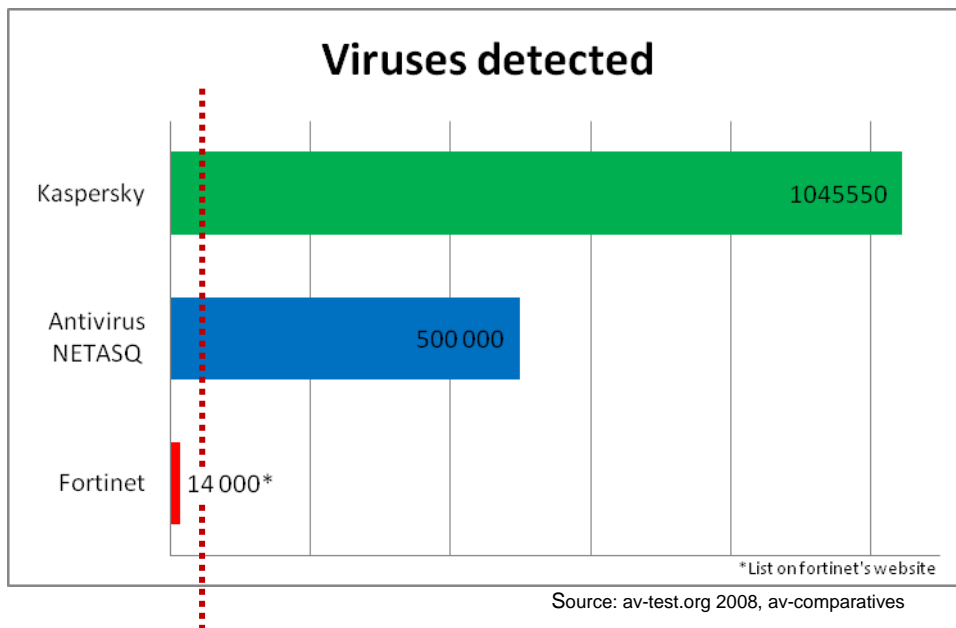


- ✓ No change in context (such as OS <-> analysis software)
- ✓ No data duplication
- ✓ Analysis on the fly, without software proxy

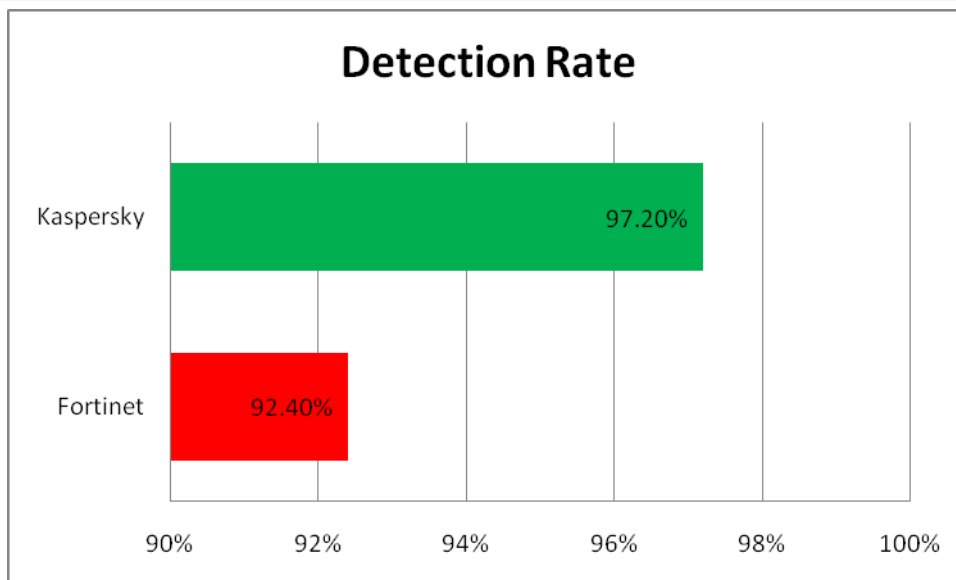
## Antivirus

In the standard version of its products, NETASQ provides an antivirus module (ClamAV-based) on all models. Kaspersky antivirus is also available. These 2 engines combine heuristic analyses and a full antivirus signature database.

Fortinet's antivirus is limited in terms of number of antivirus signatures due to the size of its architecture. It only integrates several thousand signatures ("wild list" principle). **In January 2009, 46 014 different viruses were detected, confirming estimates that an average of more than 30 000 viruses appear each month.** This average is indicated in the graph below with the following mark: ⋮



NETASQ's choice to optimize its architecture in order to guarantee the analysis of a full antivirus database has a positive effect on the detection rate, such as in the test presented below:



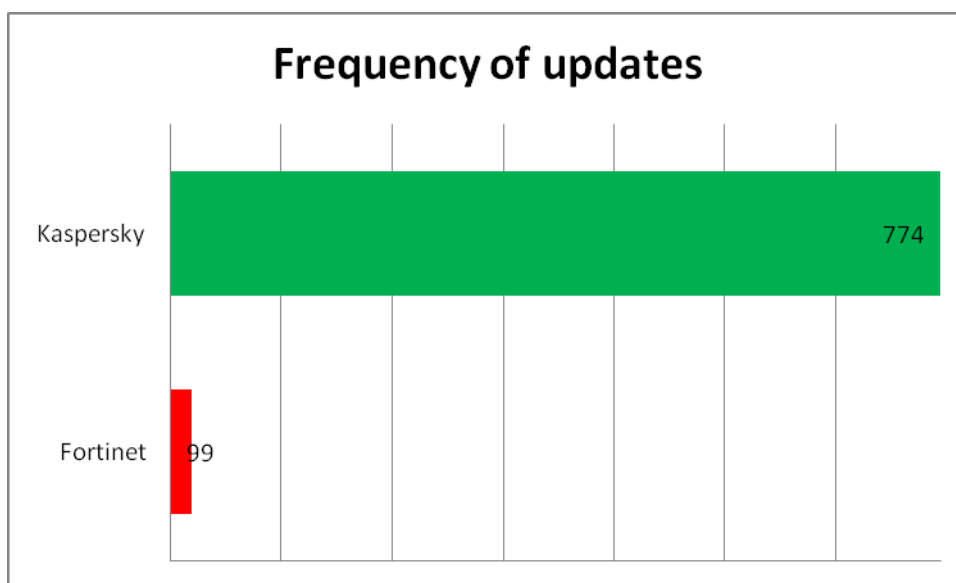
Source: av-test.org 2008

Another key factor is the responsiveness when an update is necessary:

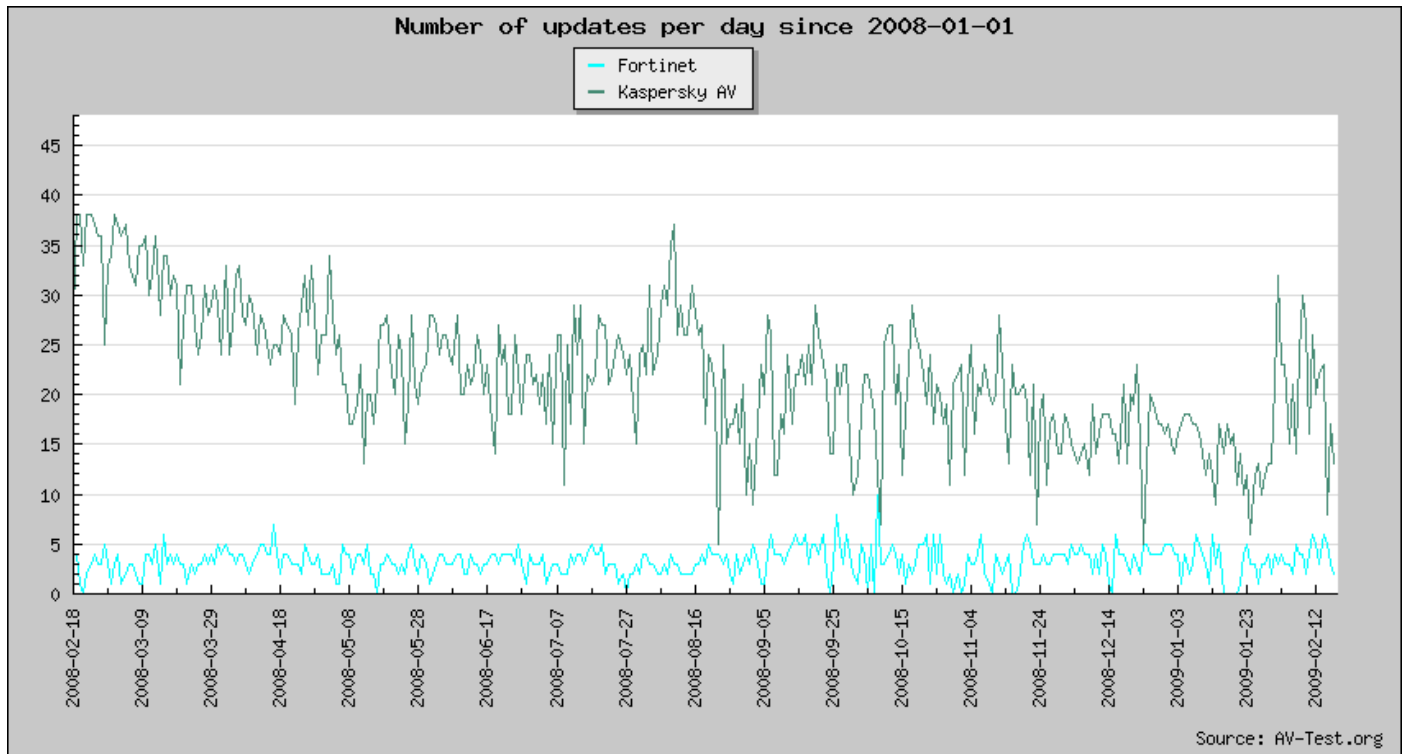
	Kaspersky	Fortinet
Average response time	 < 2 hours	 Between 2 and 4 hours

Source: av-test.org 2008

Lastly, the frequency of these updates is also an accurate indication of the evolution of an antivirus database:



Source: av-test.org 2008



The Austrian laboratory AV-Comparatives conducts tests twice yearly on antivirus solutions in order to analyze their level of detection of malicious codes during on demand comparatives.

**Ever since the first installation of this test in February 2004, Kaspersky Lab solutions have attained the “Advanced+” label, in other words, the best result.**

## URL filtering

NETASQ	Fortinet
<p>NETASQ directly embeds URL filter and Antiphishing rules on the product in order to prevent latency. URLs are downloaded in a binary format to ensure the highest processing speed.</p>	<p>Fortinet centralizes all queries in its datacenter. When the internet is accessed, the appliance will then query the Datacenter, thereby impacting latency. Web queries are in fact transmitted outside the company network.</p>

NETASQ has also partnered with a world expert in the field, Optenet, to provide a high quality URL database. The largest international enterprises, many telecoms operators and millions of users worldwide trust Optenet's expertise and use this technology.

Optenet has R & D centers across the whole of Europe, in Latin America, in the United States and in Australia, to guarantee a localized categorization of the different sites.

## NETASQ SEISMO: real-time risk management

Network protection is one of the foundations of high-level security. In addition to a multi-feature firewall and proactive protection techniques, making the network as secure as possible has become a daily objective. Risk management is a compromise between the risk in itself and the cost incurred in avoiding it. One of the most important factors in this field is the teams' level of information.

Network overview

- 87 vulnerabilities were detected on the monitored networks
- 19 of the vulnerabilities are critical
- 76 of the vulnerabilities are remote

Name	Family	Instance
Apache (Debian)	Web Server	1
Firefox	Web Client	9
FreeBSD	Operating System	1
HotBar HbInst	Malware	2
lighttpd	Web Server	1
Linux	Operating System	5
Microsoft Internet Explorer	Web Client	5
Microsoft Windows 2003	Operating System	1
OpenSSH	SSH	2
Postfix Server	Mail Server	1
Wget	Web Client	1

NETASQ firewalls use network information in real time to determine the risk borne by each user/network equipment. This unique engine, called SEISMO, forms part of the NETASQ Firewall/UTM operating system, and provides a totally new level of information.

This information guides the administrator to the solution in order to delete the risks detected. Automatic reports provide an accurate indication of the evolution of the risk in the company.

Name	Address	Users	Operating system	Vulnerabilities	Applications
Estelle	172.30.103.11	Estelle	Linux	7	2
Dave	172.30.103.13	Dave	Microsoft Windows	0	1
Bob	172.30.103.20	Bob	Linux	18	1
Admin_Host	172.30.103.1	Admin	Microsoft Windows	0	0
172.30.102.1	172.30.102.1		Microsoft Windows	0	0
172.30.103.16	172.30.103.16		Microsoft Windows	0	1
172.30.103.17	172.30.103.17		Microsoft Windows	0	1

Vulnerabilities (7)   Applications (2)   Events (3)   Connections   Alarms

Search:    Column:

Severity	Application name	Name
High	lighttpd 1.4.13	Lighttpd 'mod_fastcgi' Headers Handling Remote Code Execution Vulnerability
Moderate	lighttpd 1.4.13	Lighttpd File Descriptor Array Allocation Denial of Service Vulnerability
Moderate	lighttpd 1.4.13	Lighttpd Multiple Remote Denial of Service and Security Byblock Vulnerabilities
Moderate	lighttpd 1.4.13	Lighttpd 'mod_cgi' Remote Source Code Disclosure Vulnerability
Moderate	lighttpd 1.4.13	Lighttpd 'connection_state_machine()' Denial of Service Vulnerability

Detailed display of the vulnerabilities by user/host: each vulnerability is of course documented.

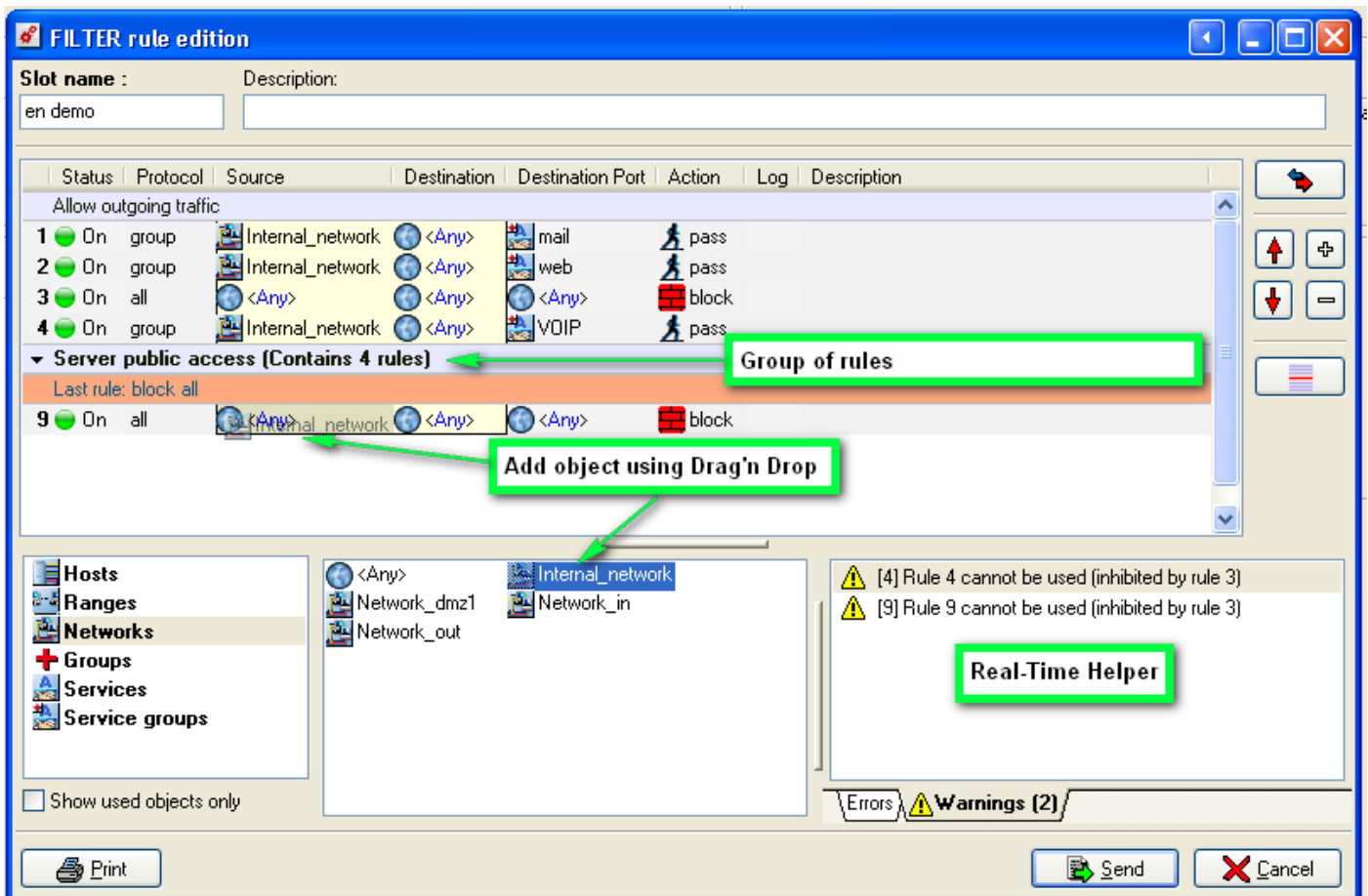
The real-time risk management that NETASQ provides is a decisive advantage for guaranteeing the highest level of security.

## Network features

	Fortinet	NETASQ
SNMP v3	<p><b>x</b></p> <p>SNMP v2 (unsecured version of the protocol)</p>	<p><b>✓</b></p> <p>NETASQ allows the use of SNMP v3</p>
Policy-based routing (PBR)	<p><b>x</b></p> <p>Dedicated policy</p>	<p><b>✓</b></p> <p>PBR is directly accessible from the filter policy.</p>
PPTP encryption	<p><b>x</b></p> <p>No choice of encryption method for PPTP tunnels</p>	<p><b>✓</b></p> <p>The PPTP server allows selecting different encryption algorithms.</p>
Authentication	<p><b>x</b></p> <p>Restricted choice of authentication mode</p>	<p><b>✓</b></p> <p>SSL, RADIUS, NTLM, KERBEROS, SPNEGO...</p>
QoS	<p><b>x</b></p> <p>There are only 3 levels for Fortinet (High, Medium, Low)</p>	<p><b>✓</b></p> <p>8 priority levels</p>

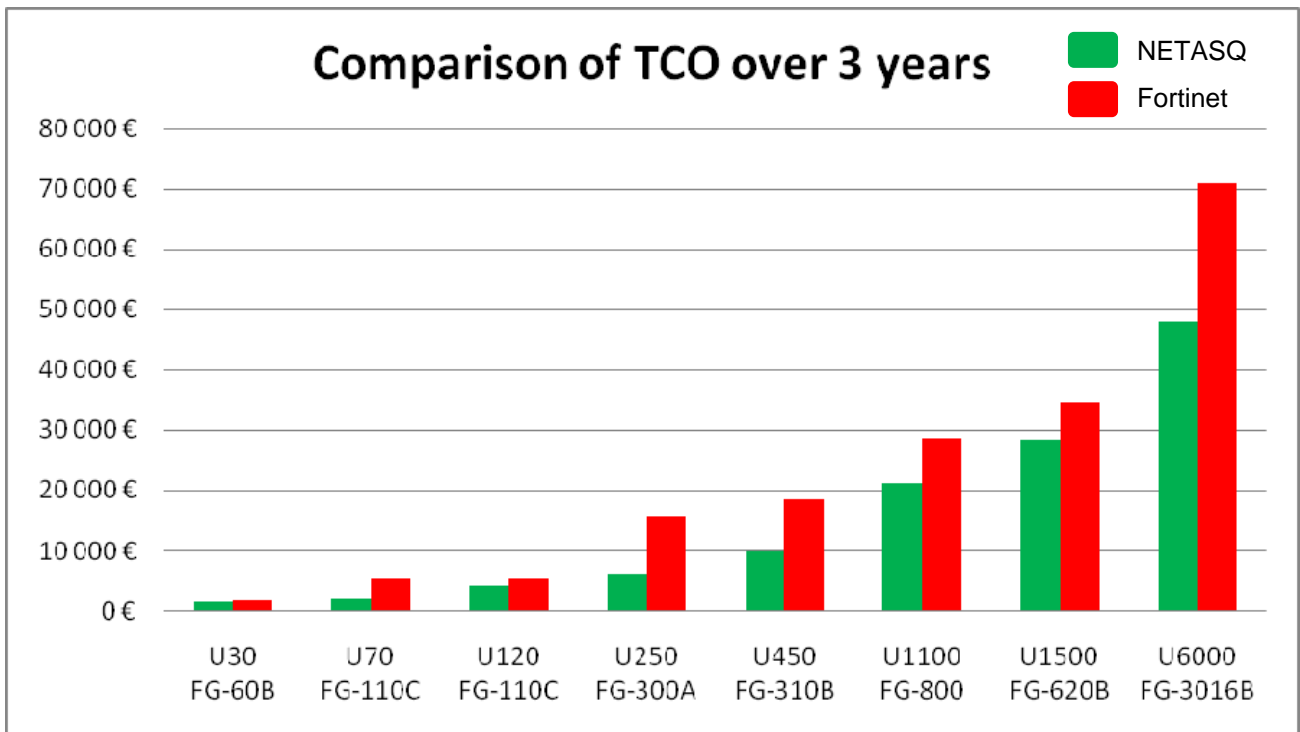
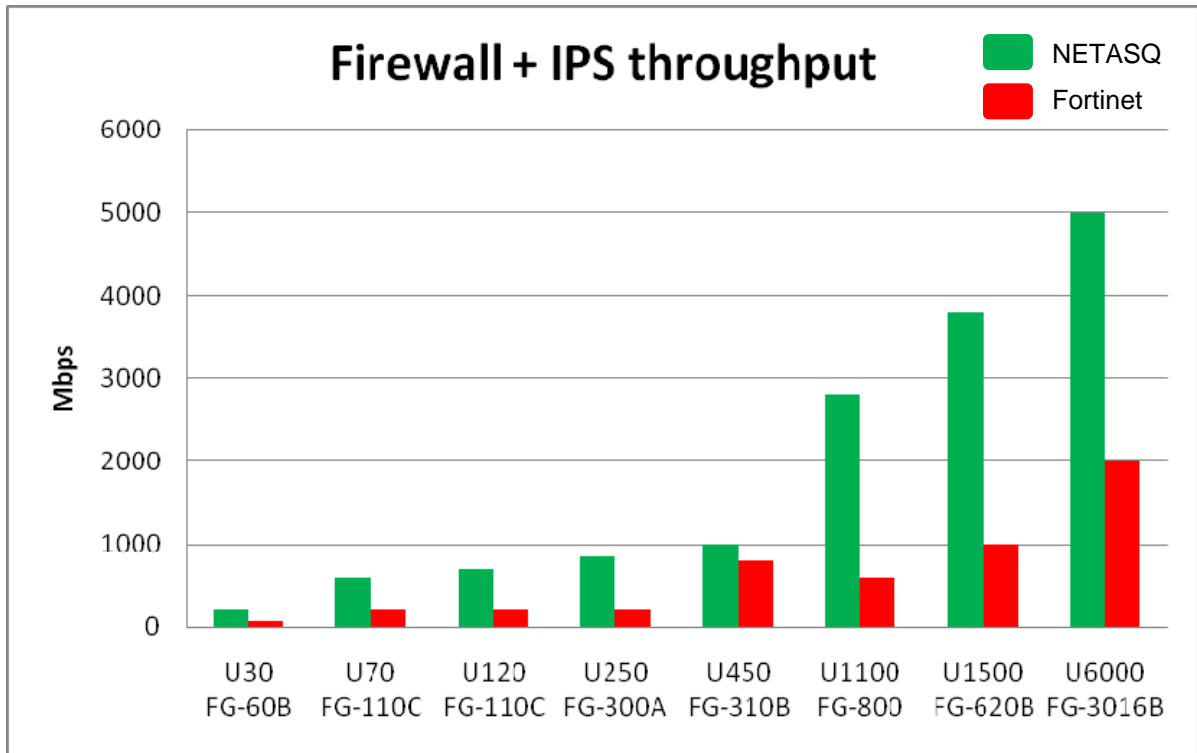
## Administration

	Fortinet	NETASQ
<b>Global policy</b>	<p style="text-align: center;">✗</p> <p>One policy level</p>	<p style="text-align: center;">✓</p> <p>Global and local policy, with possibility of delegating</p>
<b>Reporting</b>	<p style="text-align: center;">✗</p> <p>Purchase of a dedicated product (FortiAnalyzer)</p>	<p style="text-align: center;">✓</p> <p>NETASQ solutions embed a full reporting module</p>
<b>Simplicity</b>	<p style="text-align: center;">✗</p> <p>Html table</p>	<p style="text-align: center;">✓</p> <p>NETASQ offers help for setting up security policies by indicating configuration errors and other alerts in real time.</p>
<b>Plug n Secure</b>	<p style="text-align: center;">✗</p> <p>More than 80% of Fortinet alarms are set to "pass", requiring manual configuration.</p>	<p style="text-align: center;">✓</p> <p>The automatic attachment of configuration profiles ensures a high level of security even in factory settings.</p>



Example of a NETASQ filter policy

# Range comparison



**Example: NETASQ U1100 vs FORTINET FG-800**

	FG-800	NETASQ U1100	difference
Firewall + IPS throughput (Mbps)	600	<b>2 800</b>	<b>466%</b>
VPN AES throughput (Mbps)	200	<b>450</b>	<b>225%</b>
Concurrent connections	400 000	<b>800 000</b>	<b>200%</b>
New connections / second	10 000	<b>20 000</b>	<b>200%</b>
10/100/1000 interfaces	4	<b>8</b>	<b>200%</b>
IPSec tunnels	3 000	<b>4 000</b>	<b>133%</b>

	FG-800	NETASQ U1100	Savings
Price of the appliance	15 295 €	10 990 €	<b>4 305 €</b>
1-year maintenance	16 845 €	15 000 € (with SEISMO)	<b>1 845 €</b>
3-year maintenance	28 655 €	21 137 € (with SEISMO)	<b>7 518 €</b>

**More than 7 500 € in savings over 3 years, with SEISMO included!**