



NETASQ

Corporate Presentation

Summer 2009

Hacen Ledad

International Account Manager

Tel : +33 (0)1 46 21 84 13

Cell : +33 (0)6 08 02 17 28

Fax : +33 (0)1 46 21 82 31

email : hacen.ledad@netasq.com

Web : www.netasq.com



From the beginning in 1998...

NETASQ's *Vision*

NETASQ's objective is to be the *European leader* of *hardware security solutions* aimed at protecting *SMB* networks, as well as *remote sites* of large enterprises and public administration.



NETWORK SECURITY

IPS . FIREWALL . ANTIVIRUS . ANTISPAM . ANTISPYWARE . QoS . CONTENT FILTERING



MAIL SECURITY

ANTIVIRUS . ANTISPAM . ANTISPYWARE

International Presence

- Available in 30+ countries
- Direct Sales focus on Europe
 - Offices in Belgium, France, Italy, Spain
- 2-tier distribution
 - EMEA, Asia/Pacific
 - 300+ Distributors, Resellers, and Integrators
 - 6000+ customers
 - 35,000+ UTM appliances

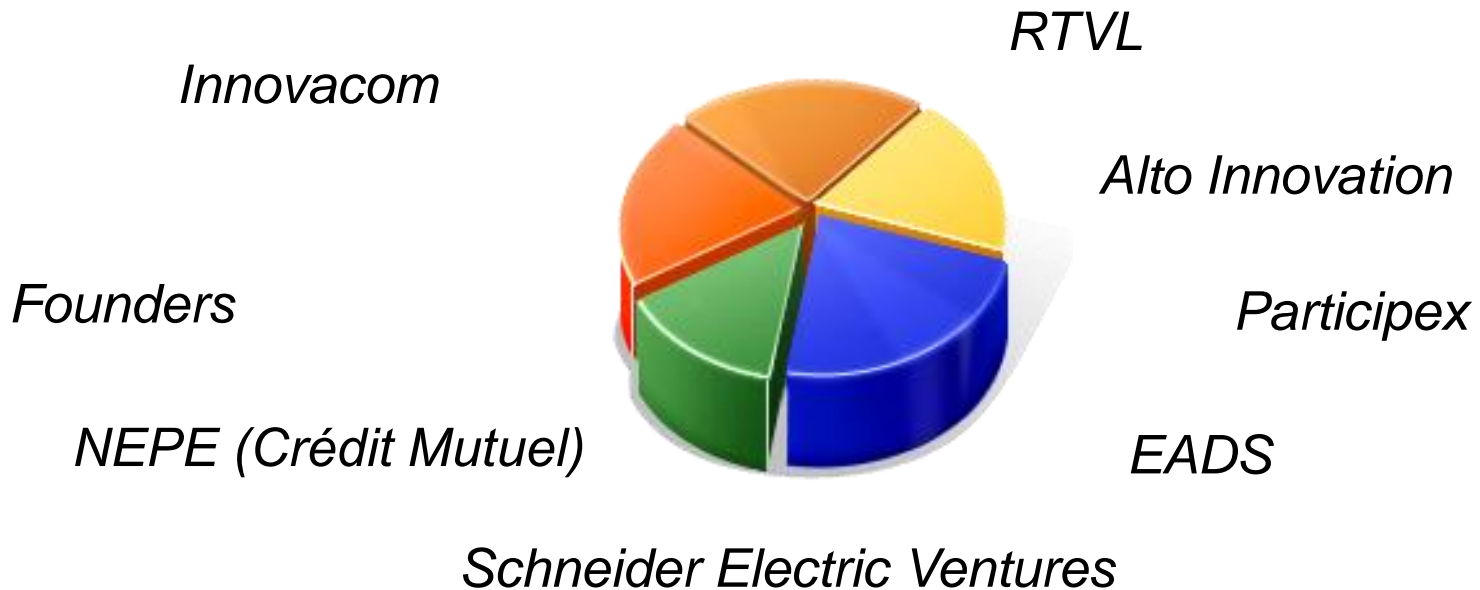


UTM = Unified Threat Management

Share Holders

Including :

- Odyssee Ventures (Caisse d'Epargne)
- SGAM (Société Générale)
- SPEF (Natexis/Banque Populaire)



World Class *Customers*

Financial



Industry



Utilities



Services



Public



35,000+ UTM appliances in use by more than 6,000 customers

World Class *Distribution Channel*



Some of our Value Added Distributors



300+ resellers in 30+ countries

Some of our Reseller Partners



World Class *Technology Partners*



Top 12 Reasons *NETASQ is Chosen*

- **Comprehensive Approach**

- Unified security
- Endpoint protection
- Integrated best-of-breed
- Built-in business functionality

- **Proactive Solutions**

- Unique intrusion prevention engine
- Active security
- Simplicity

- **Scalability**

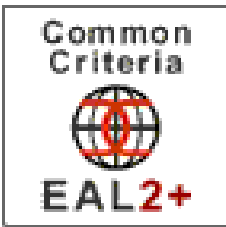
- A straightforward choice
- True security up and down the line
- Add a local touch

- **Proven Performance**

- European leader
- Award-winning



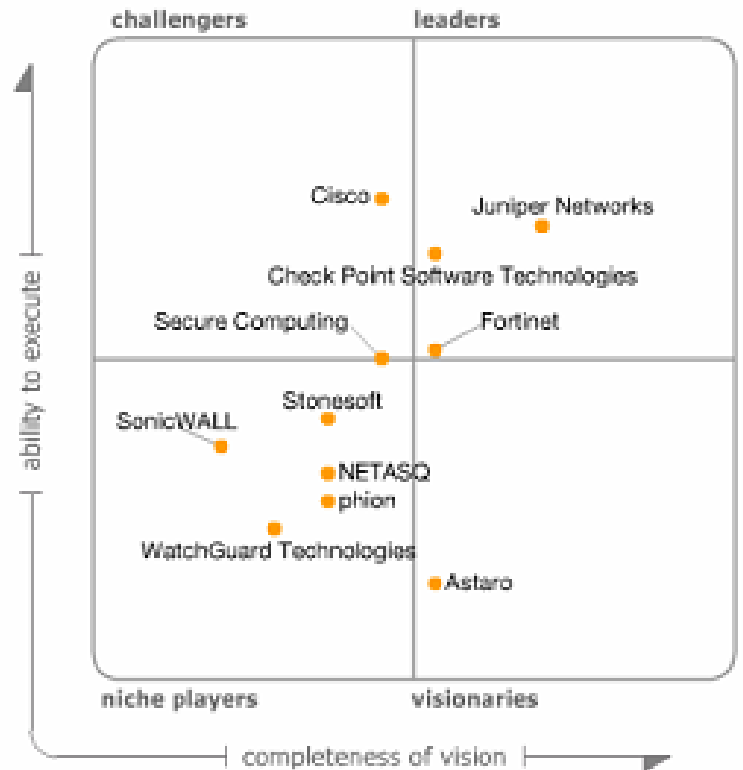
Market Recognition :



✓ Award as the Best Product in the IT Newspaper for 3 consecutive years.

MAGIC QUADRANT

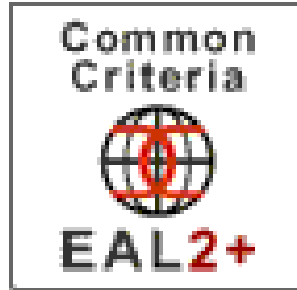
Figure 1. Magic Quadrant for Enterprise Network Firewalls, 2H07



As of September 2007

Source: Gartner (September 2007)

Certifications actuelles :



✓ **DCSSI : CAUTION and Qualification standard**

✓ **Range of product targeted: Firewall/IPS, IPSEC, Management and Authentication.**

✓ **Europe : EU Restricted**

✓ **Standard for the whole Europe**

✓ **OTAN : NATO VPN Restricted (Ambre Color)**



Evolutions Certification en 2008 :

✓DCSSI (Q4 – 2008):



✓New Certification for the Netasq V8.x:

New CC v3.1

Firewall/IPS Level EAL4+

Entire Product

(VPN+Firewall/IPS) level EAL3+



✓NATO (Q2 – 2008) :

✓NATO Restricted Firewall (Green)

✓NATO Restricted VPN (Green)



Threats From Everywhere



Viruses

Privacy threats

Trojan horses

Hackers

Do you have an effective means of keeping your business running smoothly by eliminating all threats and annoyances?

Intrusions

Popups

Phishing

Cookies

Spam

Spyware

Worms

Unsuitable websites

NETASQ's Mission

To provide solutions offering “**zero tolerance**” security that is:
reliable; **easy** to buy, deploy,
update and manage;
and has an excellent
quality/price ratio.





All-in-One Network Security

NETASQ UTM F-Series



NETWORK SECURITY

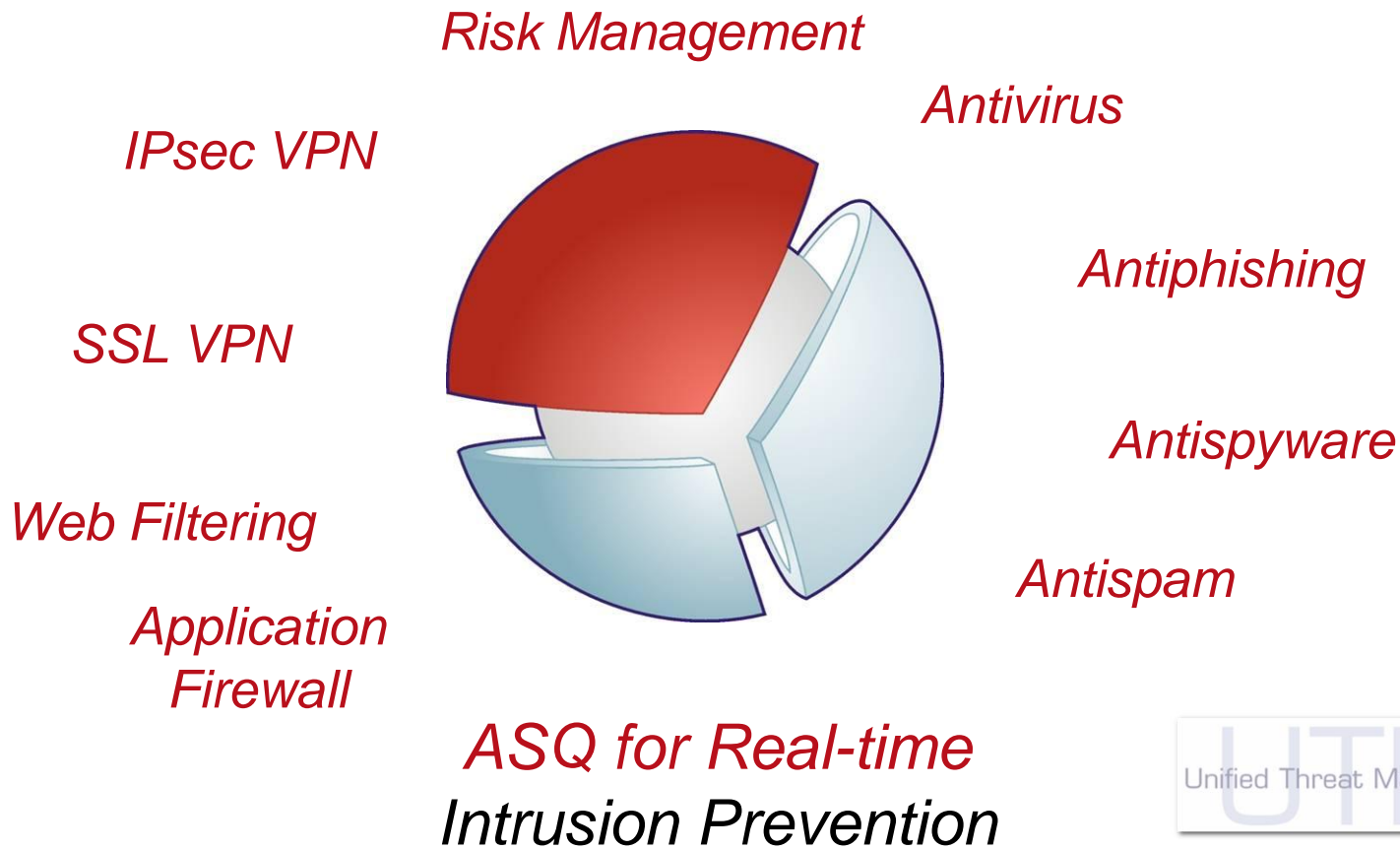
IPS . FIREWALL . ANTIVIRUS . ANTISPAM . ANTISPYWARE . QoS . CONTENT FILTERING

Market Drivers

- Need to protect critical data and systems
 - Block viruses, spyware
 - Prevent attacks
- Need to increase productivity
 - Remove distraction of spam
 - Minimize Internet misuse
- Need to maximize network infrastructure ROI
 - Eliminate bandwidth hogs
 - Improve network performance
- Need to avoid legal liability
 - Protect business reputation
 - Ensure professional working environment

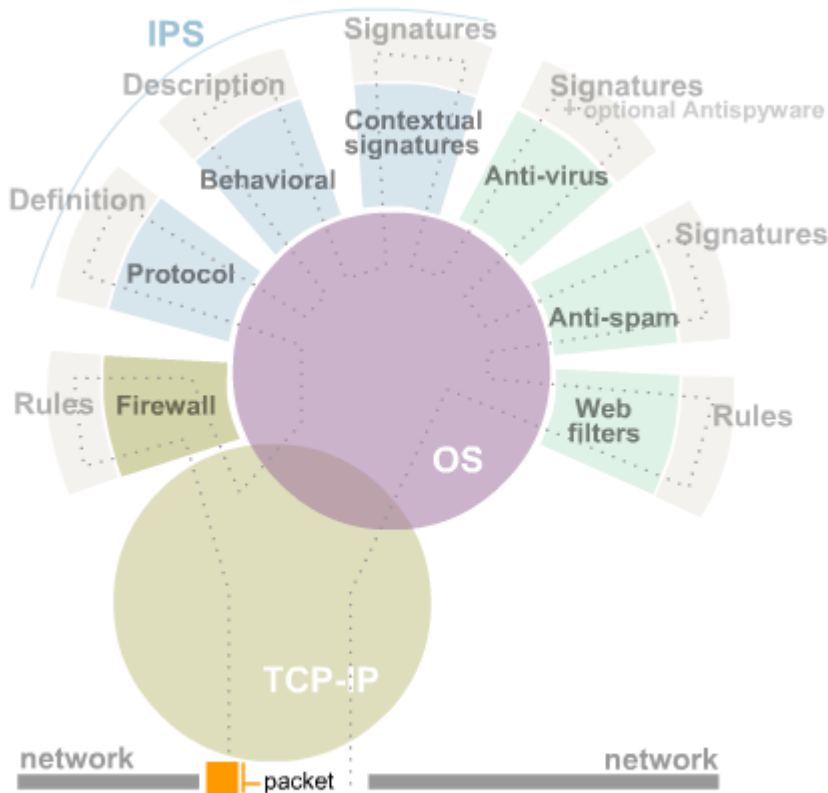


NETASQ Offers *Unified Security*



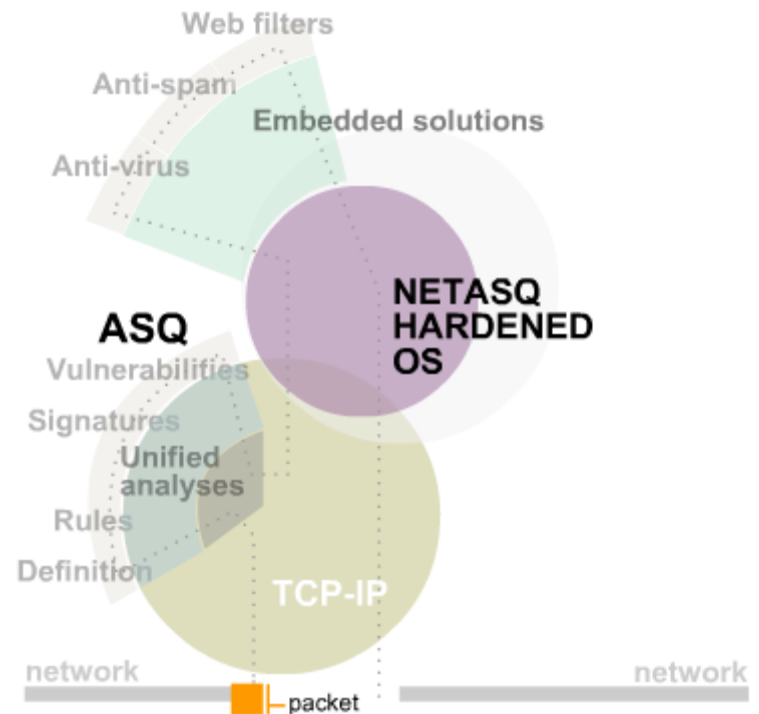
NETASQ Engine versus *Classic IPS*

Classic UTM Architecture



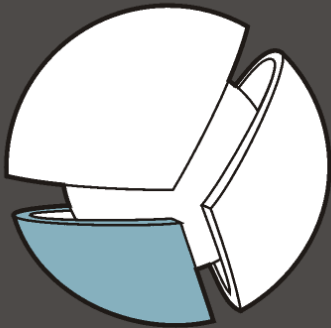
CLASSIC UTM ARCHITECTURE	0
request for modules	

NETASQ UTM Architecture



NETASQ UTM ARCHITECTURE	0
request for modules	

Technology: Real-Time IPS



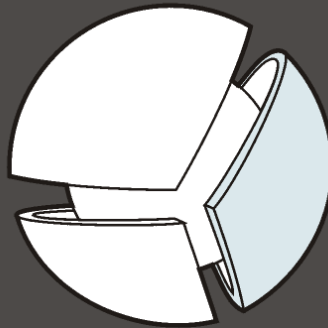
Protocol Analysis

Traffic Anomaly Prevention

- * Spoofing
- * Malformed / Illegal Packets
- * Invalid Protocol Headers
- * Data Evasion
- * 0-Day Threats

Application-level Protection

- * Malformed / Illegal Packets
- * Invalid encoding in URL
- * Data Evasion
- * Buffer overflows
- * 0-Day Threats



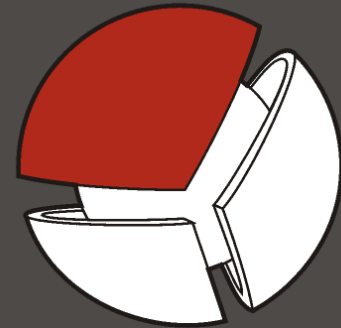
Heuristic Analysis and Filtering

Statistical and behavioral Analyses

- * Flooding
- * OS probe
- * Firewall policy detection
- * Backdoor
- * Port scan

Traffic filtering

- * Handling optimization (SKIP)
- * Flooding prevention (BLUE)
- * Advanced Filtering Policy
- * Stateful Engine



Contextual Signatures

Attacks

- * Vulnerable Applications
- * Vulnerable Operating Systems

Content

- * P2P(Kazaa, eDonkey,...)
- * Instant messaging

Functioning

- Performances
 - ASQ functions in Kernel mode
 - Analysis until level 7 of the OSI model
 - Real-time analysis (puts the packets in buffer and analyses them)
- Security
 - ASQ functions in Kernel mode
 - Analyzes the VPN traffic
 - Protocol analysis
 - Global context analysis
 - Connection
 - Application
 - Analyzes to different OSI levels
 - Contextual Signatures
 - ASQ detects and BLOCKS the attacks and intrusion in real-time

Contextual Signatures: Example



Multiple specialised signatures bases:
very low false positive rate

ASQ configuration

ASQ configuration

00: default | default | Reset to default | Last modification: 03/11/2004 10:59:40

Alarms - Protocol

Category	Action	Reaction	Dump	Level	Message	Help
ip	Block	None	<input type="checkbox"/>	Major	Usurpation d'adresse de bouc	
	Block	None	<input type="checkbox"/>	Major	Usurpation d'adresse IP	
	Pass	None	<input type="checkbox"/>	Ignore	Paquet broadcast	
	Pass	None	<input type="checkbox"/>	Ignore	Paquet multicast	
	Block	None	<input type="checkbox"/>	Ignore	Adresse de classe expériment	
	Block	None	<input type="checkbox"/>	Minor	Mauvaise option IP	
	Block	None	<input type="checkbox"/>	Minor	Option IP inconnue	
	Block	None	<input type="checkbox"/>	Minor	Protocole IP non analysé	
	Pass	None	<input type="checkbox"/>	Ignore	Machine du réseau interne inc	
	Block	None	<input type="checkbox"/>	Major	Débordement de fragment	
	Block	None	<input type="checkbox"/>	Major	Recouvrement de fragment	
	Block	None	<input type="checkbox"/>	Minor	Routage par la source	
	Block	None	<input type="checkbox"/>	Major	Fragment IP de taille nulle	
	Block	None	<input type="checkbox"/>	Minor	Port 0 utilisé comme service	
	Block	None	<input type="checkbox"/>	Major	Petit fragment	
	Block	None	<input type="checkbox"/>	Major	Utilisation de l'adresse privée	
	Block	None	<input type="checkbox"/>	Minor	Usurpation d'adresse IP sur ur	
	Block	None	<input type="checkbox"/>	Minor	Utilisation de la plage d'adress	
	Block	None	<input type="checkbox"/>	Minor	Utilisation de l'adresse broadc	
	Block	None	<input type="checkbox"/>	Ignore	Protocole IP invalide	
	Block	None	<input checked="" type="checkbox"/>	Minor	Somme de contrôle IP invalide	
	Block	None	<input type="checkbox"/>	Ignore	Analyse de fragment IP	
	Pass	None	<input type="checkbox"/>	Ignore	Protocole GRE local	
	Pass	None	<input type="checkbox"/>	Ignore	Protocole IPsec ESP local	

Default configuration ▾ [See index of alarms help](#)

Apply... | Send | Cancel

NETASQ's *Vision*

What more can be done
to secure your network ?



Network risks

- Every Day, dozens of new vulnerabilities (network, system, etc...) are discovered and published
- Most of them are followed by an exploit, potentially dangerous for your system



Network risks

Bulletin Identifier	
Bulletin Title	Oracle
Executive Summary	
Maximum Severity	Critical
Impact of Vulnerability	
Detection	Micro
Affected Software	

bzip2 Remote Denial of Service Vulnerability

2007-10-17
<http://www.securityfocus.com/bid/13657>

OpenOffice TIFF File Parser Multiple Integer Overflow Vulnerabilities

2007-10-17
<http://www.securityfocus.com/bid/25690>

Oracle Balsa Fetch Command Remote Stack Buffer Overflow Vulnerability

2007-10-17
<http://www.securityfocus.com/bid/25777>

Microsoft Subversion Date Parsing Buffer Overflow Vulnerability

2007-10-17
<http://www.securityfocus.com/bid/25386>

Oracle Valve Software Half-Light Multi-Threaded Buffer Overflow Vulnerability

2007-10-17
<http://www.securityfocus.com/bid/8300>

Netgear HP-UX OpenSSL Unspecified Local Denial Of Service Vulnerability

2007-10-17
<http://www.securityfocus.com/bid/26093>

Cisco TIBCO SmartPGM FX Multiple Remote Vulnerabilities

2007-10-17
<http://www.securityfocus.com/bid/26092>

Nortel Networks PC Client Soft Phone Message Parsing Module Buffer Overflow Vulnerability



code execution if a user
 ve fewer user rights on the

will not require a

less

- The question is :

**How can I get the best security with all these security vulnerability published every day and that I don't understand for most of them
????**

The answer can be :



But.....

NETASQ SEISMO *Customer Value*

- Do you want to eradicate 100% of risk from your network?
- YES. Pinpointing, prioritizing and making intelligent decisions about threats will help you control and reduce them.



NETASQ
SEISMO helps you to make
the right threat response decisions
to manage your network risks!

NETASQ SEISMO *Reseller-MSSP Value*

- Network protection is more complex than ever.
- Global security solutions must have more than just strong Firewall and IPS protection.
- Security officers need to add real-time risk management.



NETASQ

SEISMO helps your customers
to make the right threat response
decisions to manage their network risks!

Since 2007, NETASQ Seismo

- is:
 - a tool to help the security manager make decisions in real time
- that :
 - gathers key data from the company's network in order to reduce :
 - the associated risk level
 - whether it fits the security policy
 - minimizes the impact on performance
- to :
 - help the security manager deal with the paradox of his designation



NETASQ U Series

X5 IPS Throughput





x2

CONCURRENT SESSIONS



NETASQ U Series

Upsize Security Standards

Conclusion



Questions

