
IBM
Ghaleb ZEKRI
Protection et prévention contre intrusion ou comment la technologie IBM sécurise vos infrastructures
TENDANCES LOGICIELLES D'ÉTÉ 2008
SESSION SPÉCIALE GESTION DES RISQUES OPÉRATIONNELS

IBM ISS protection platform

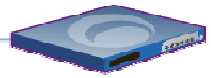
Among the most advanced and complete security architectures ever developed—delivering preemptive security

Protection platform

Enterprise Protection Products (Appliances and Agents)

All based upon the Proventia Unified Protection Architecture (UPA)

proventia network — Protection Appliances



Proventia Network MFS
"All-in-One" Protection Appliance
- *IDS/IPS*
- *FW / VPN*
- *AntiVirus (signature & behavioral)*
- *AntiSpam*
- *Web Filter*
- *Spyware*

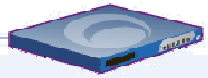
MX5010, MX3006, MX1004

Proventia Network Mail
Preemptive control and spam control for your messaging infrastructure
- *IPS*
- *AntiVirus (signature & behavioral)*
- *AntiSpam*
- *Clustering*

MS 3004

proventia network — Protection Appliances

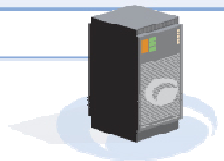
Proventia ADS Series –
"Anomaly/Behavioral" Protection and Network Visibility Appliances



Proventia Network IPS
Preemptive Security for Enterprise Networks
GX4002, GX4004, GX5008, GX5108, GX6116

Proventia Network IPS for Crossbeam
Performance up to 1 Gigabit per APM with load balancing across multiple APMs for added throughput

proventia server — Protection Agent



Proventia Server
"Multi-layered" Protection Agent
– Windows
– Linux

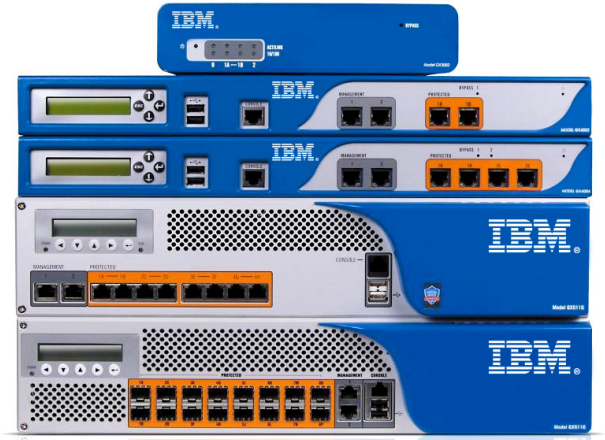
RealSecure Server Sensor
– Windows
– Solaris
– AIX
– HP-UX

proventia desktop — Protection Agent

Proventia Desktop
"All-in-One" Protection Agent
- *Firewall*
- *Virus Prevention System*
- *Antivirus (Signature base)*
- *Intrusion Prevention*
- *VPN Enforcer*
- *Buffer Overflow Protection*

Helping enterprises secure their networks

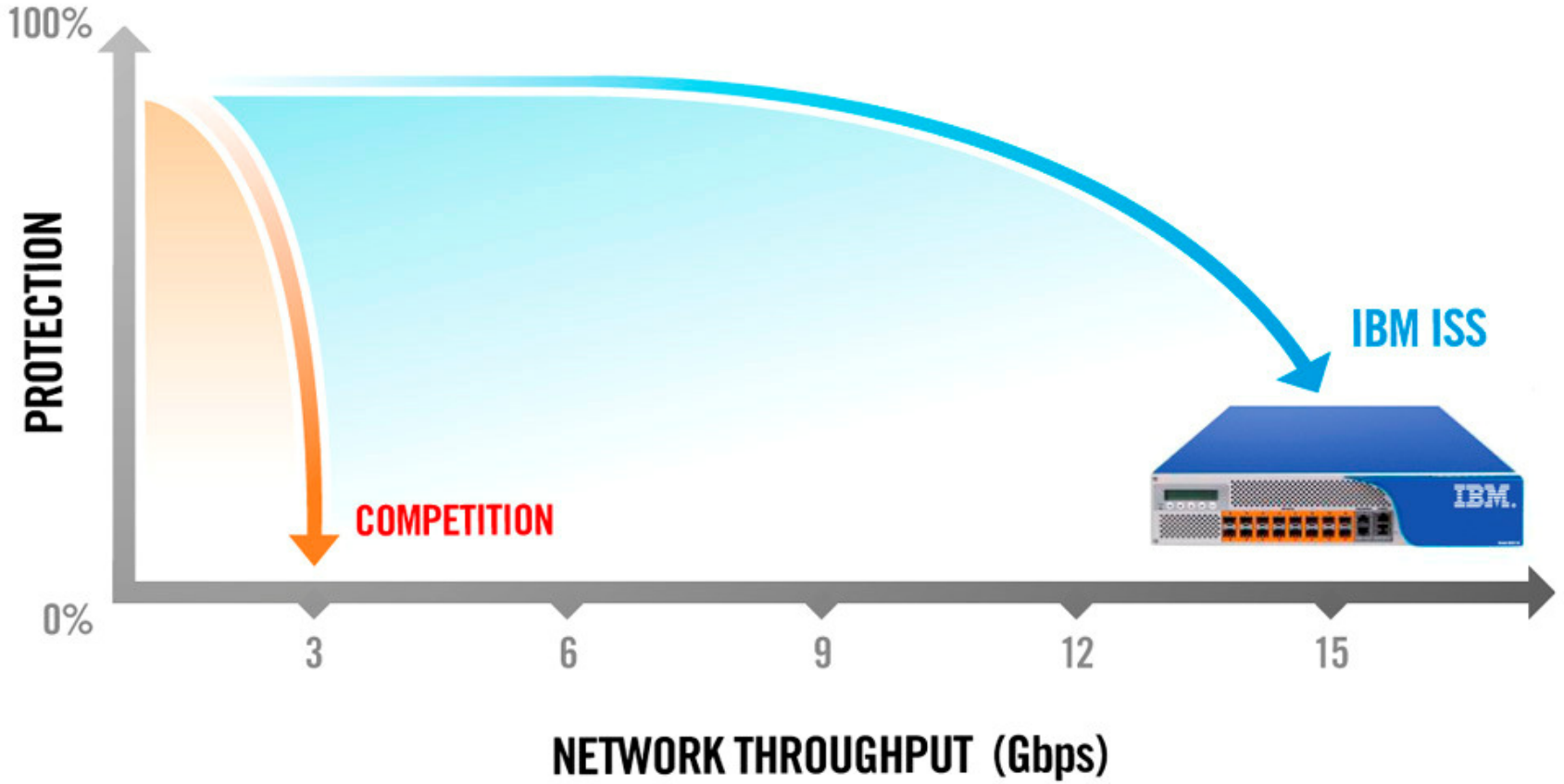
- IBM Proventia® Network Intrusion Prevention System (IPS)
  - Transparent, in-line network appliances block attacks while allowing legitimate traffic to flow unhindered
  - Comprehensive line of models available:
    - 10 Mbps—15 Gbps throughput capacity
    - Up to eight protected network segments



- IBM Managed Protection Services (MPS) for Networks
  - Deployment
  - Maintenance
  - Monitoring
  - Incident response

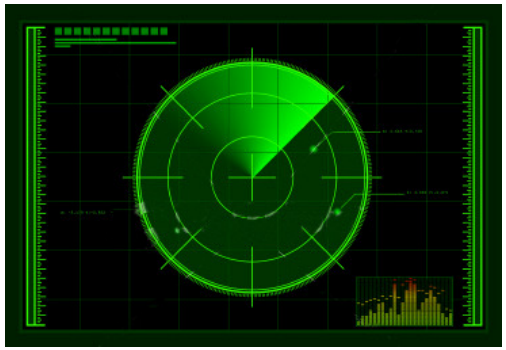
Proventia Network IPS performance

- Up to 15 Gbps throughput
- Latency as low as 150 microseconds



Proventia Network IPS Security

Vulnerabilities vs. Exploits



- Vulnerability - **an issue in a software product that enables a malicious individual to undermine the product's security and potentially cause harm.**

- Exploit **- a piece of software that is capable of granting or extending privileges on a computer system contrary to that system's design**

Proventia Network IPS security

Vulnerability research makes the difference!

- Protecting against *exploits* is *reactive*
  - Too late for many
  - Variants undo previous updates
- Protecting against vulnerabilities and malicious behaviors is *preemptive*
  - Stops threat at source
  - Requires advanced R&D

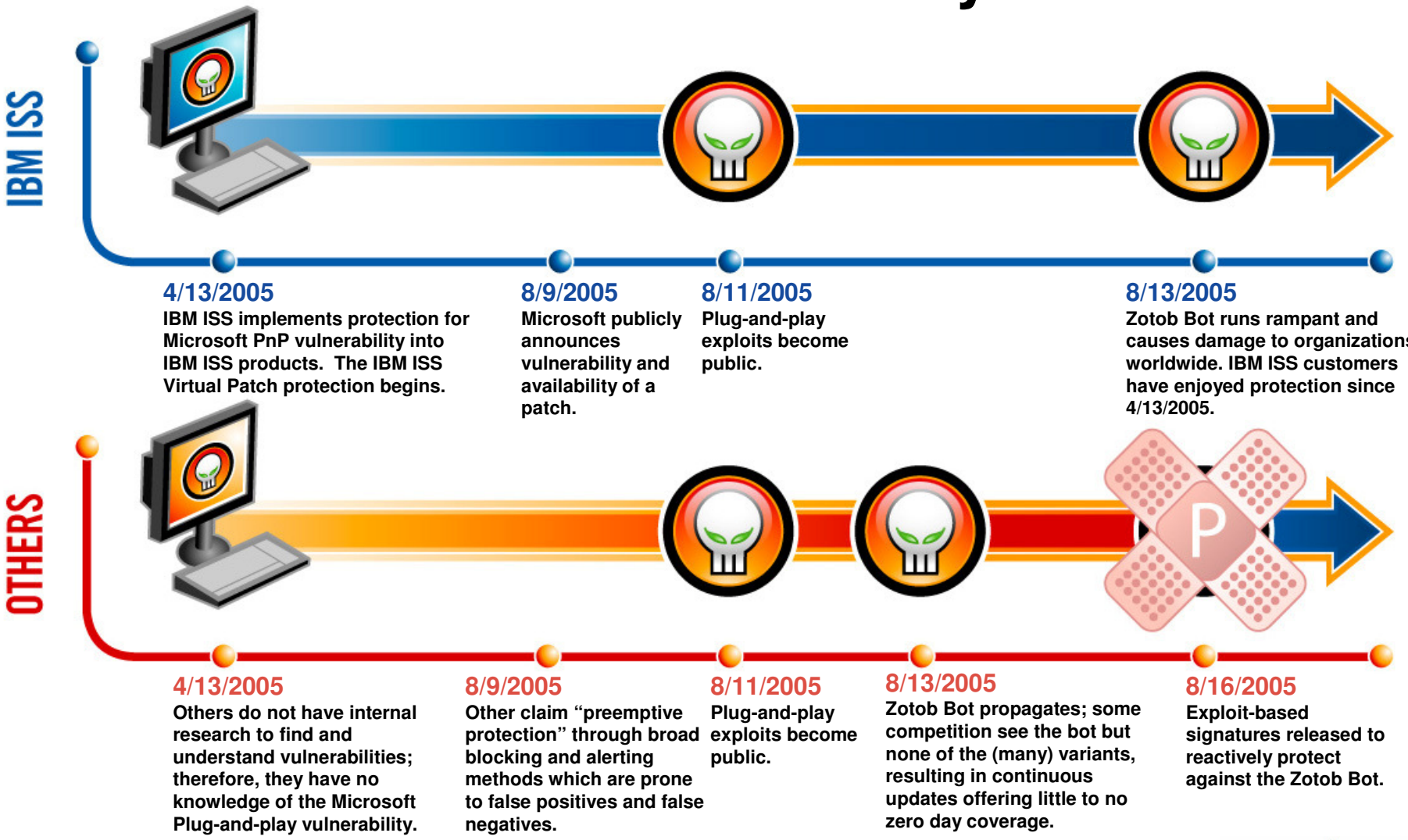
Proventia Network IPS security

How is it different from "reactive" security and "zero day" protection?

- Holes in the roof = vulnerabilities
- Reactive security:
  - Identifying the raindrops that have already started coming in through the hole in your roof
  - Applying a patch during the storm
- Preemptive security is a vulnerability-based approach:
  - Intensive research is applied to discover the hole in the roof
  - A patch is applied to the hole to protect against any kind of rain – all while the sun's still shining …

weeks or months ahead of the storm

Proventia Network IPS security



Proventia Network IPS security

How it Works

- Deep inspection of network traffic
- Identifies & analyzes 177 network and application layer protocols and data file formats

What it Prevents

- Worms
- Spyware
- P2P
- DoS/DDoS
- Cross-site Scripting
- SQL Injection
- Buffer Overflow
- Web Directory Traversal

Protocol Analysis Module (PAM)

Vulnerability Modeling & Algorithms	RFC Compliance
Stateful Packet Inspection	TCP Reassembly & Flow Reassembly
Protocol Anomaly Detection	Statistical Analysis
Port Variability	Host Response Analysis
Port Assignment	IPv6 Native Traffic Analysis
Port Following	IPv6 Tunnel Analysis
Protocol Tunneling	SIT Tunnel Analysis
Application-Layer Pre-Processing	Port Probe Detection
Shellcode Heuristics	Pattern Matching
Context Field Analysis	Custom Signatures
Proventia Content Analyzer	Injection Logic Engine

Proventia Network IPS security

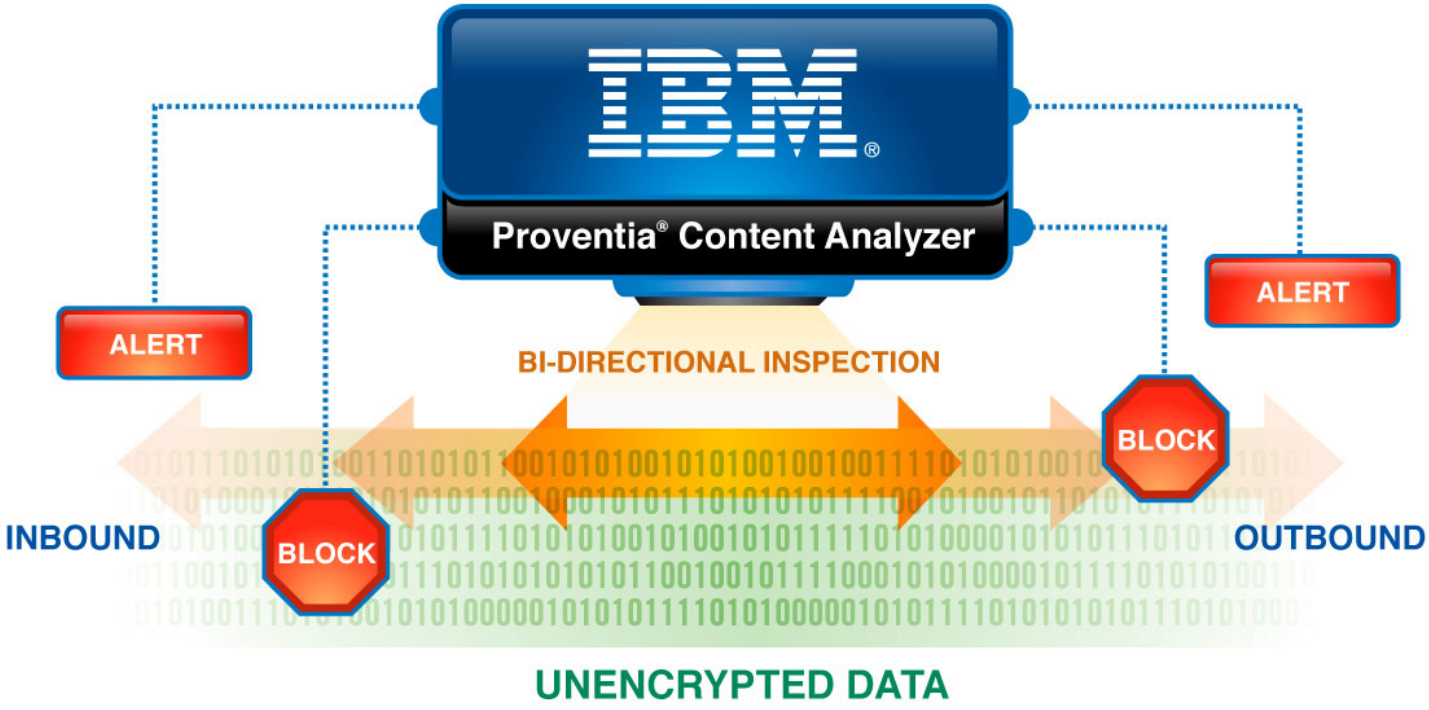
Proventia Content Analyzer

- **Monitors and identifies unencrypted personally identifiable information (PII) And other potentially confidential information**
- **Provides capability to explore data flow through the network to help determine if any potential risks exist using up to 16 different signatures**
- **Supports compound data-set search string inspection and inline/passive bi-directional inspection modes**
- **Inspects content in compound documents including PDFs, ZIP and GZIP files over 10 different protocols**
- **Complement to data security strategy**
- **Utilizes robust inspection capabilities of Protocol Analysis Module (PAM)**
- **Leverages new and existing market leading IBM Proventia® Intrusion Prevention System (IPS) technology**

Proventia Network IPS security

Proventia Content Analyzer - How it works

Inspects both inbound and outbound unencrypted data, either generating alerts when flagged data are found, blocking the traffic from being transmitted, or both.



Proventia Network IPS security

Proventia Content Analyzer – At a Glance

SIGNATURES
Credit Card Number
Name
Date
U.S. Dollar Amount
Email Address
Social Security Number
U.S. Phone Number
U.S. Postal Address
8 User-Defined

PROTOCOLS
*AOL IM
*Microsoft Messenger
*Yahoo Messenger
*IRC
HTTP
FTP
SMB
*SMTP
*IMAP
*POP3

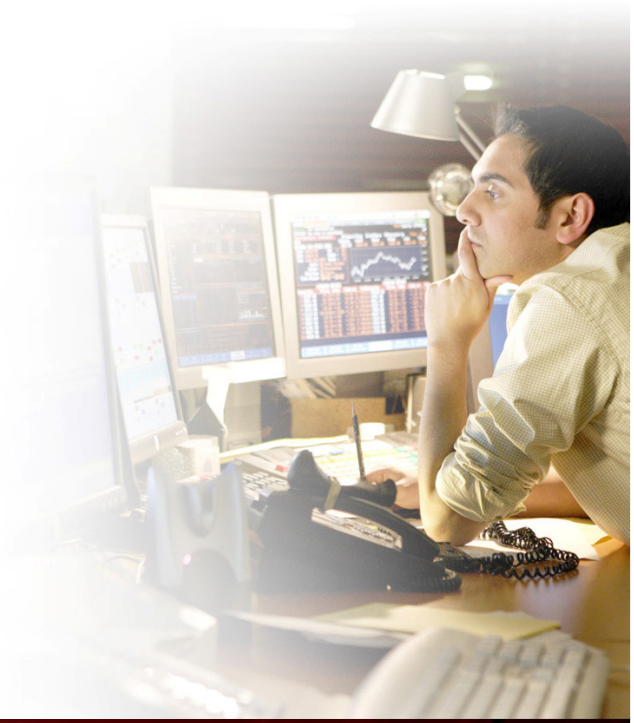
CONTENT
Microsoft Office Documents
PDF
Text
RTF
XML
HTML
GZIP
ZIP

*Provides for inline inspection of attached files.

Proventia Network IPS security (con't.)

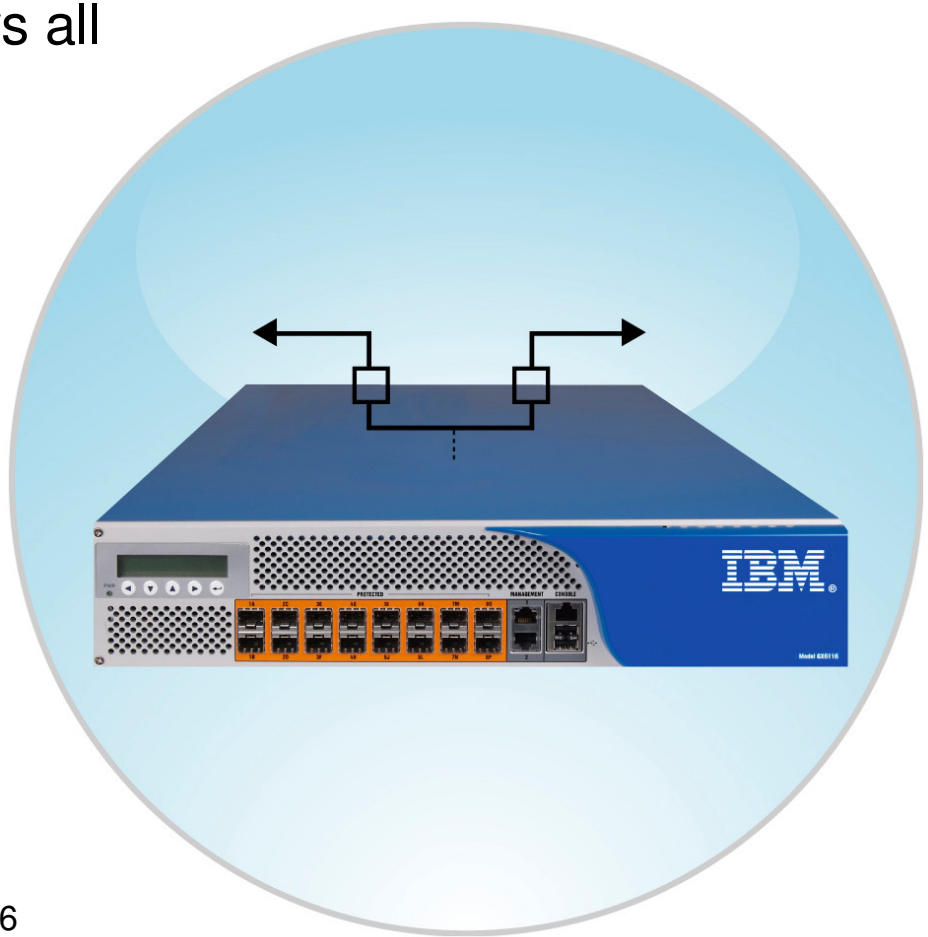
Backed by the industry-leading IBM ISS X-Force® research and development team:

- Original vulnerability research
- Public vulnerability analysis
- Malware analysis
- Threat landscape forecasting
- Protection technology research



Proventia Network IPS reliability

- Automatic bypass operation allows all traffic to pass in the event of:
  - Hardware failure
  - Power failure
  - Software crash
- Redundant components*
  - Hard drives
  - Power supplies
  - Cooling fans

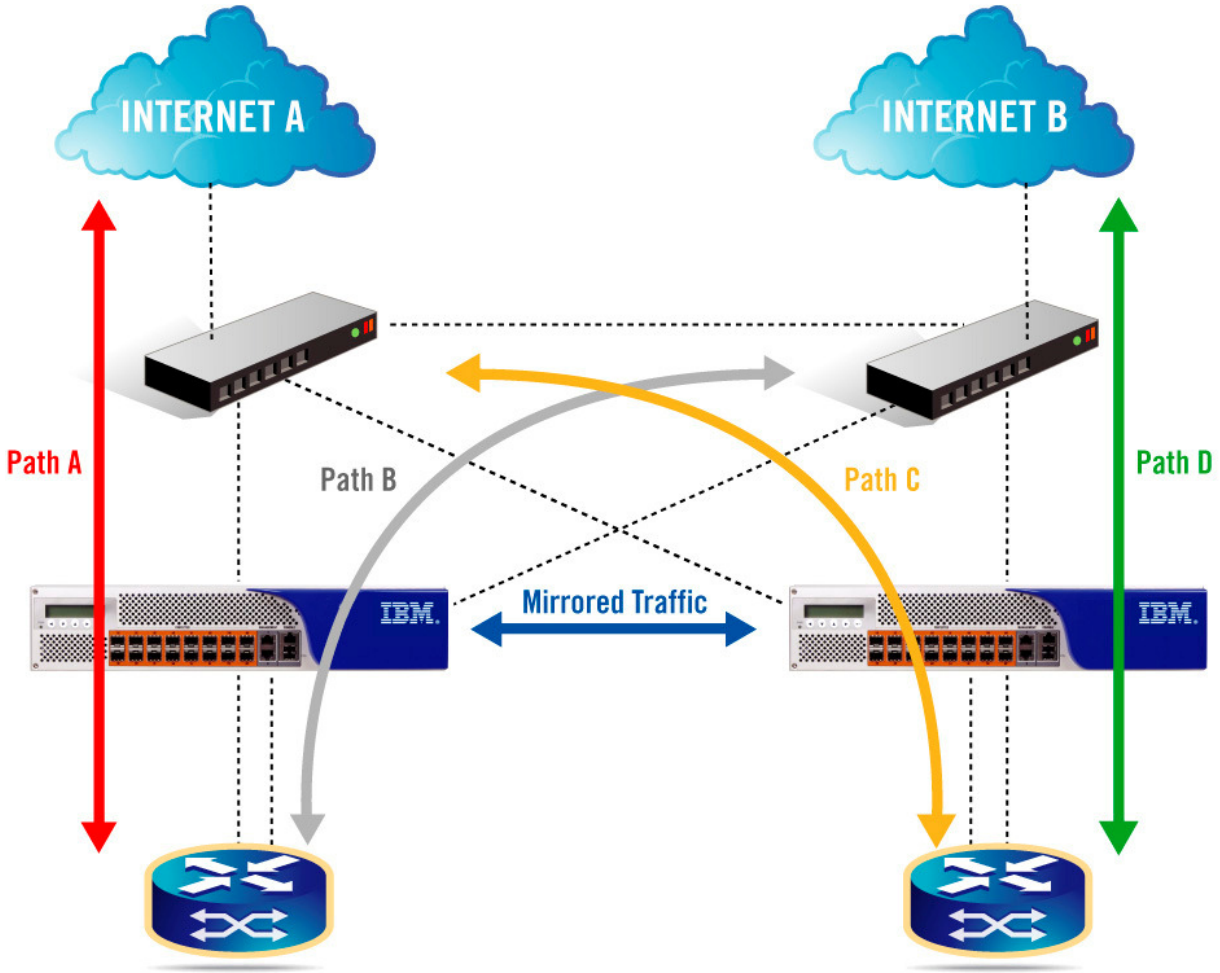


*Available in GX5008, GX5108, GX5208 and GX6116

Proventia Network IPS reliability (con't.)

High Availability (HA)

- Support for multiple configurations
  - Active—active
  - Active—passive
- Full state maintenance on failover



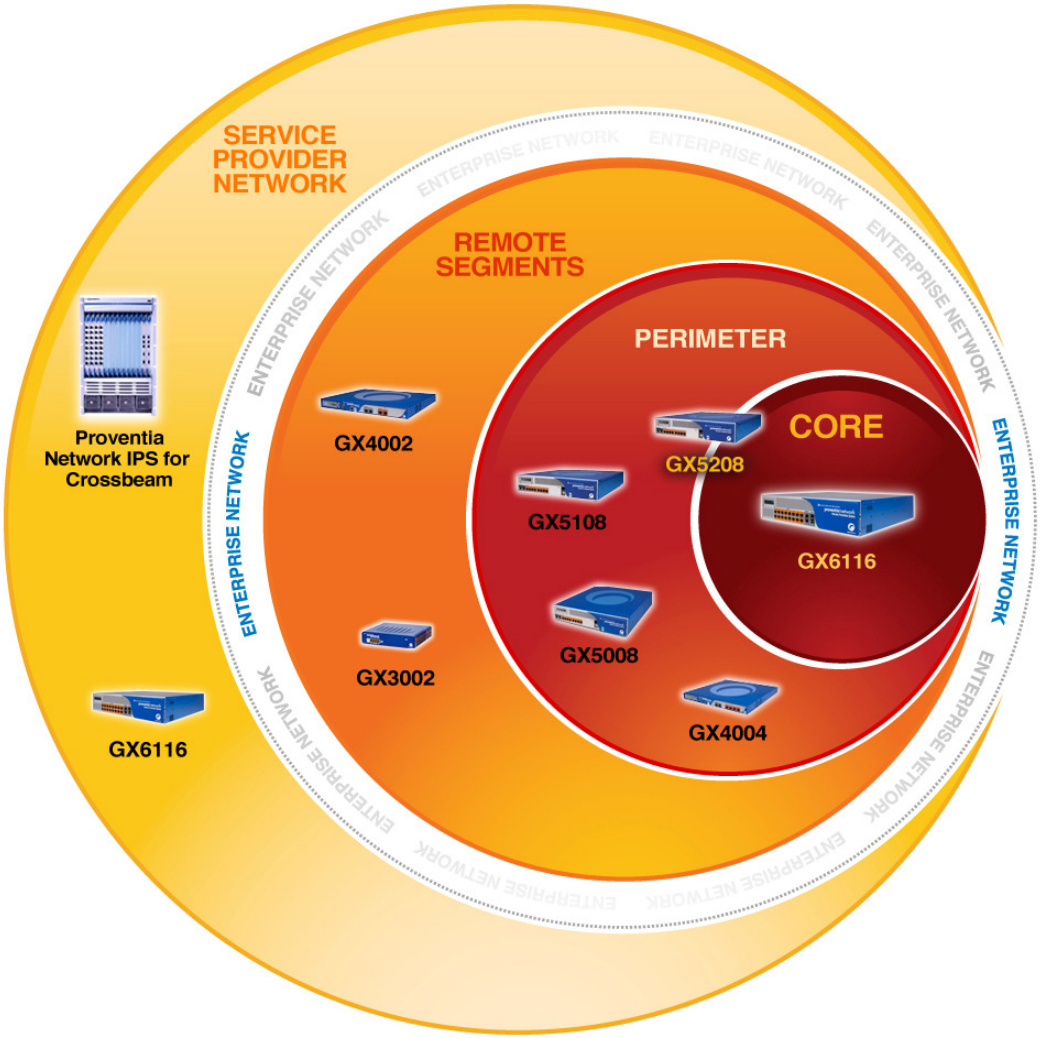
Proventia Network IPS reliability (con't.)

- Active—active HA
  - Requires active-active network infrastructure
  - Maintains your HA network design
  - Supports asymmetrical routing
    - Will not miss split attacks
- Active—passive HA
  - Requires active-passive infrastructure
  - Primary appliance is active and inspecting traffic
  - If primary is interrupted, secondary appliance becomes active link

Proventia Network IPS deployment

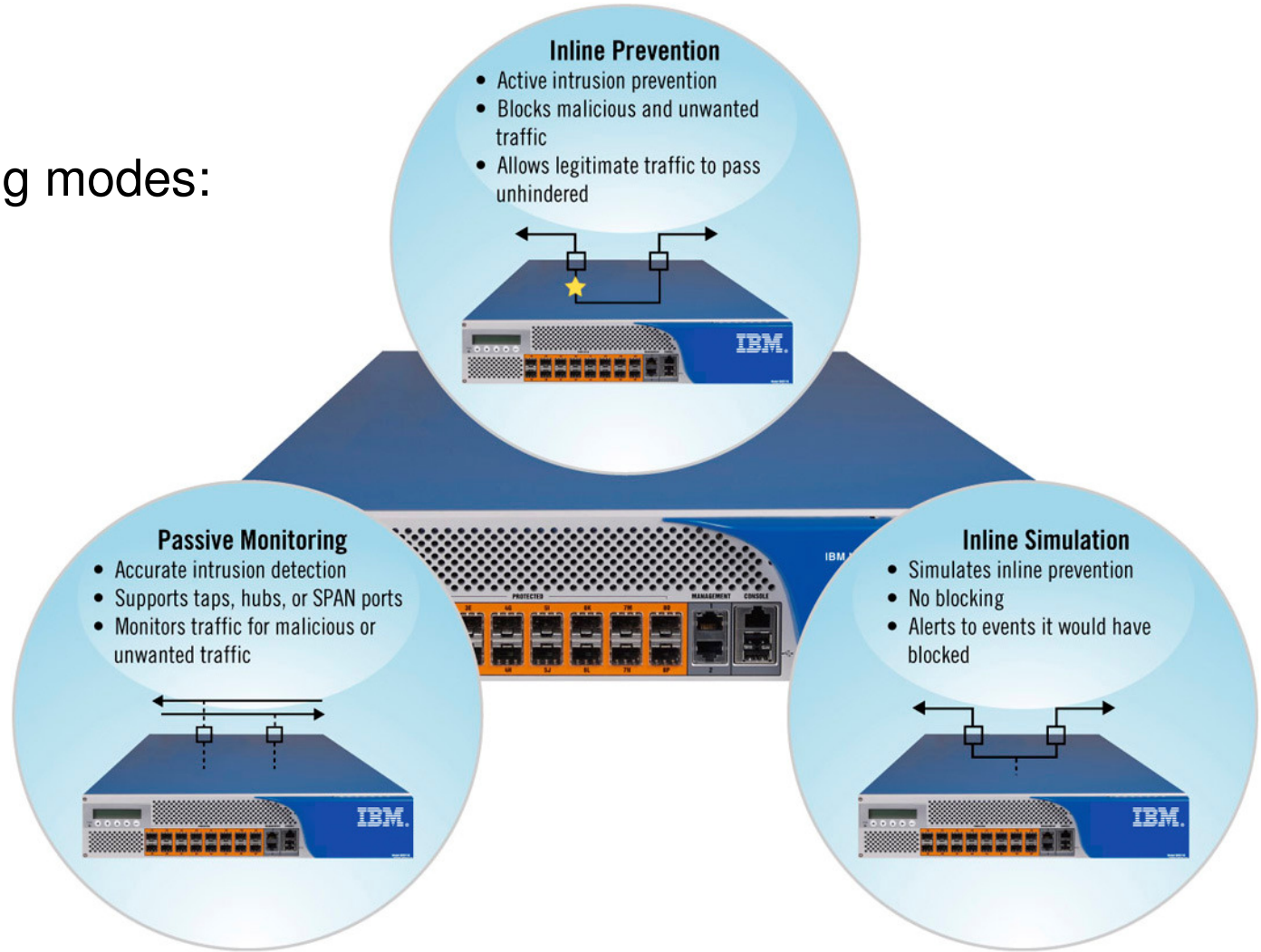
Proventia Network IPS offers a deployment solution for every layer of the network

Layer 2 Architecture **means simple deployment, with no reconfiguration of the network required**



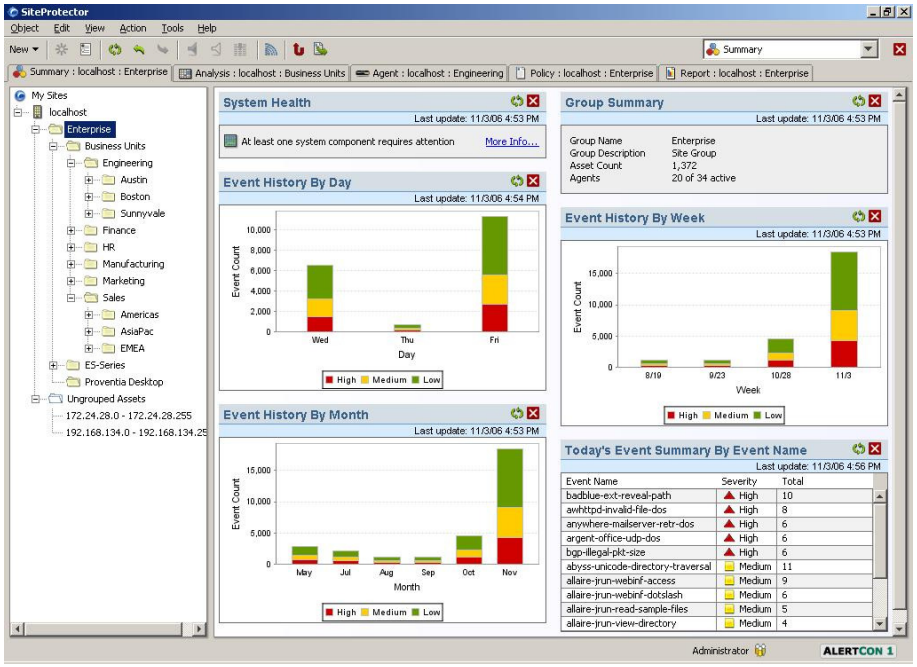
Proventia Network IPS deployment (con't.)

Three operating modes:



Proventia Network IPS management

- Browser-based local management interface (LMI)
- Central management through IBM Proventia Management SiteProtector™ system
  - Simple, powerful configuration and control
  - Robust reporting, customized event viewing and event correlation
  - Comprehensive alerting and response options
  - Scheduled data retention to be used for compliance efforts
  - Highly scalable to accommodate hundreds of Proventia Network IPS appliances



Proventia Network IPS confidence

Customers Trust Proventia
17 of the world's largest banks
15 of the largest governments around the world based on GNI
11 of the world's largest public insurance companies
13 of the world's largest IT companies

The Industry Gives Proventia Top Ratings
Gartner Network IPS Appliances Magic Quadrant Leader 2005
Frost & Sullivan IDS/IPS Market Leadership Award 2005, 2006, 2007
Frost & Sullivan Network Security Company of the Year Award 2006
SC Magazine Security Company of the Year 2006
SC Magazine Best Integrated Security Solution 2006

Proventia is Certified by Leading Independent Testing Organizations
NSS Approved IPS + Enterprise 2006
NSS Approved IPS + Branch Office 2006
The Tolly Group Up To Spec Certification 2005

IBM

Question ?

Question ? Question ?

Question ?

Question ?

Question ? Question ?

Merci !

TENDANCES LOGICIELLES D'ÉTÉ 2008

SESSION SPÉCIALE GESTION DES RISQUES OPÉRATIONNELS