



Securing high-speed networks without sacrificing performance.

IBM Proventia® Network Intrusion Prevention System (IPS) GX6116



Product Highlights

- **A Raza Microelectronics network processing unit (NPU) specifically designed for high-speed processing of network packets**
- **64bit core processor and dual XEON® x86 processors examine traffic across all seven OSI layers**
- **High availability options for continuous protection**
- **Robust hardware redundancy for power supplies, data storage and cooling fans**
- **Vulnerability-based protection to stop threats before they impact business**

Securing high-speed networks without sacrificing performance.

Enterprise networks demand high performance. As the network core supports more advanced services, hardware features such as speed, throughput and low latency become even more important to business continuity and profitability. Information security also supports business continuity, but it cannot do so at the expense of network performance and availability. Intrusion prevention systems (IPS) can help enterprises meet compliance requirements and protect valuable business data, but network administrators cannot tolerate the negative impact many traditional IPS appliances have on the network. The solution that enterprises require merges network performance and availability with advanced threat protection. The IBM Proventia® Network Intrusion Prevention System (IPS) GX6116 from IBM Internet Security Systems (ISS) offers the best of both worlds—network performance and ahead-of-the-threat protection.

Engineered with three of today's biggest network pain points in mind—**Performance, Availability** and **Reliability**—the Proventia Network IPS GX6116 is designed to secure the network, maximize uptime and optimize throughput.

The Proventia GX6116 for greater performance

Many IPS appliances force network and security administrators to decide between performance and detection accuracy. IBM ISS designed the Proventia GX6116 with performance **and** accuracy in mind. To improve performance, the Proventia GX6116 separates processing the flow of data from inspecting data for threats.

Custom-built Architecture

IBM ISS designed the Proventia GX6116 with a purpose-built network processing unit (NPU) that keeps up with high-speed networks and high bandwidth requirements, and enables bounded latency thresholds and intelligent inspection technology. The Proventia GX6116 NPU can process traffic on eight segments at line speeds of up to 15 Gbps, while offering industry leading protection at up to 6 Gbps. Dual Xeon x86 processors provide deep packet inspection on all seven OSI layers.

As a feature of the NPU design, the Proventia GX6116 allows for higher bandwidth in one segment without starving bandwidth in another. The new hardware platform also enables the Proventia GX6116 to favor throughput and line rate speeds for smaller packets, affording 1 Gbps in each direction per segment. The NPU design not only provides assurances of low latency, it is also extremely resistant to dropping packets and can be configured to favor throughput over security should the network administrator determine such a course of action.

Technical Details

- XLR™ 732 Processor – eight fast 64bit cores operating on the flexible Microprocessor without Interlocked Pipeline Stages (MIPS) architecture
- 4-way multithreading
- Multi-level hierarchy cache
- Autonomous accelerators
- Point-to-point interconnects

Faster Communication

The Proventia GX6116’s distributed communication strategy helps avoid any data delays due to communication path processing limitations from the network IO to the NPU and x86 processors. The Proventia GX6116 architecture leverages the power of System Packet Interface Level 4, Phase 2 (SPI4.2) high-speed bus (HSB) interfaces, operating at up to 10 Gbps. One HSB communicates between the NPU and the x86 processors and the remaining two HSBs provide high-speed transport of data from 16 interface ports (eight ports per HSB) to the NPU.

Low Latency for Faster Throughput

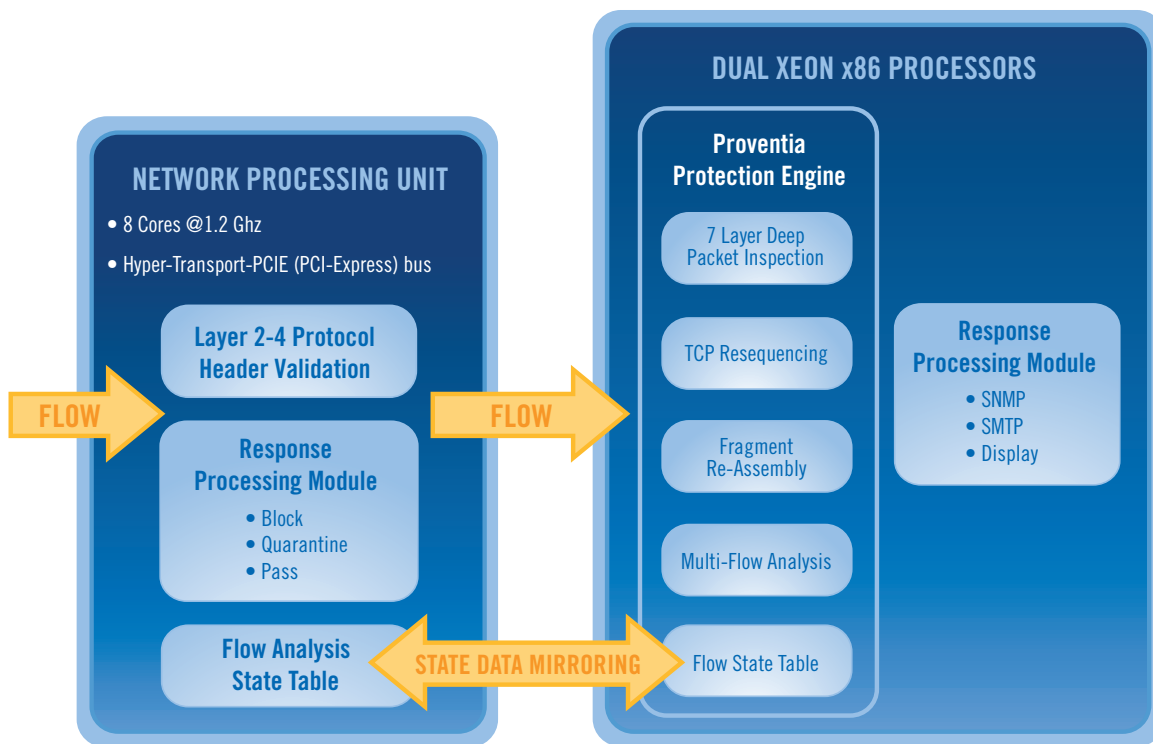
Every network administrator hopes to avoid latency problems, especially administrators running networks that support high-speed processing for VoIP or transactional databases. Routers and switches enjoy low latency because they do not perform deep

inspection. The Proventia GX6116 is designed to constrain latency while identifying and blocking threats based on the right combination of processing power, a high-speed architecture and overall design efficiency.

The Proventia GX6116 allows administrators to establish and modify latency thresholds so that traffic is not delayed due to high network volume. Maximum latency thresholds also put the network administrator in control of performance and acceptable levels of risk for the enterprise, as opposed to being confined by pre-determined settings.

The Proventia GX6116 for greater resilience and availability

Based on its NPU design, the Proventia GX6116 can maintain network traffic flow even in the unlikely event of a problem within the protection engine. While the NPU architecture is designed to resist failure, if the appliance does become



The Proventia GX6116 custom-built architecture with network processing unit and Dual Xeon processors.

overloaded, network administrators can choose to pass all traffic uninspected if they are comfortable assuming a certain level of security risk.

The network processing unit operates separately from Proventia's internal inspection processes. With a separate processor, the Proventia GX6116 has decoupled network traffic flows from deep packet inspection – another factor that helps provide superior performance and network availability.

Availability through Duplication

To avoid interrupting data flow in the case of a failure, the Proventia GX6116 offers high availability (HA) protection in both Active-Active and Active-Passive modes.

- **Active-Active HA** – In Active-Active mode, two Proventia GX6116 systems operate simultaneously, each processing the same data. Should one system fail, network traffic continues through the remaining Proventia GX6116 providing uninterrupted network protection.

- **Active-Passive HA** – In Active-Passive mode, only one Proventia GX6116 system is active and processing data. Should that system fail, the idle system becomes active and the network passes all data onto the waiting backup system.

Availability through Bypass Options

Should a hardware or software failure occur, the Proventia GX6116 can respond in one of three ways:

- **External Bypass** – A Proventia GX6116 appliance hardware failure can initiate an optional External Bypass mode, allowing all network traffic to continue to flow through the device without undergoing any additional inspection or processing.

- **Soft Bypass** – If the system detects a problem with the traffic flow sensor, such as a significant drop in incoming packets, the appliance initiates Soft Bypass mode. Soft Bypass mode operates as a congestion watchdog, automatically passing traffic until the sensor has recovered or maintenance has been performed.

- **Self-Policing CPU** – Should the CPU surpass operating temperature thresholds, the system throttles the CPU speed until the normal operating temperature range is achieved. In all cases described above, the Proventia GX6116 maintains a complete log of problems for later diagnosis.

Availability through Intrusion Prevention

The Proventia GX6116 helps maintain the availability of other network assets by stopping Internet threats before they impact business. The Proventia GX6116 helps organizations realize higher levels of system uptime, reduced maintenance costs and greater data security.

The Proventia GX6116 uses a combination of protection technologies to shield the network against a variety of threats. Rather than using signatures that detect only existing, known threats, the Proventia GX6116 uses vulnerability-focused algorithms to protect the network from entire attack categories, including:

- Worms
- Spyware
- P2P
- DoS/DDoS
- Cross-site scripting
- SQL injection
- Phishing
- Buffer overflow
- Web directory traversal

Proventia's vulnerability-centric approach to security helps reduce the number of false-positives generated, and is latency-friendly.

The Proventia GX6116 for greater reliability

The reliability of an IPS refers to hardware uptime as well as the integrity of its protection. Reliability of protection from a signature-based IPS is difficult to quantify since the technology can only react to existing threats. When new threats are unleashed, there is no precedent for protection. The Proventia GX6116 applies vulnerability-based protection, along with many other threat analysis techniques, making it capable of blocking entire categories of threats, whether known or unknown.

Reliability through Redundancy

The Proventia GX6116 offers device redundancy through backup components that automatically turn on in the unlikely event of a failure. For redundancy, the Proventia GX6116 includes:

1. **2 x 80G Hard Drives** – dual, mirrored hard drives designed to preserve data in case of a failure

2. **Redundant Power Supplies** – two hot-swappable power supplies in case of catastrophic power failure on one supply

3. **Redundant Cooling Fans** – dual cooling fans ensure the appliance continues to operate within environmental standards in the case of a single fan failure

Reliability through Design

The Proventia GX6116 security features include a protection toolkit consisting of a combination of identification and analysis techniques.

- Protocol analysis (140+ network and application protocols)
- Port assignments
- Heuristics
- Port following
- Protocol tunneling
- RFC compliance
- TCP reassembly
- Flow reassembly
- Statistical analysis
- Pattern matching

The identification category consists of tools that help the IPS accurately identify the protocol encountered within the network traffic. In the analysis category, tools analyze identified protocol traffic for malicious behavior, indicating what should be blocked or allowed.

With this protection toolkit, the Proventia GX6116 marries a number of protection methodologies to cover a larger threat landscape for a complete IPS solution.

Reliability through Research

While redundant power supplies and storage units are de-facto requirements for network and device resiliency, the Proventia GX6116 also offers built-in security intelligence from the IBM Internet Security Systems X-Force® research and development team. X-Force intelligence is infused into the Proventia GX6116 to help stop emerging threats and enhance the reliability of Proventia's protection. The X-Force is a world-renowned vulnerability and threat research organization.

IBM ISS also tracks Internet threat levels around the world from its Global Threat Operations Center (GTOC) in order to enhance the protection inherent in the Proventia GX6116 Network IPS. When new threats appear, GTOC security analysts are among the first to observe them and subsequently alert Proventia customers.

For More Information

To learn how the Proventia Network Intrusion Prevention System GX6116 can protect high speed networks without sacrificing performance, or to schedule an onsite demonstration, please visit www.ibm.com/services/us/iss.



© Copyright IBM Corporation 2007

IBM Global Services
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
05-07
All Rights Reserved

IBM and the IBM logo are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

Proventia and X-Force are trademarks or registered trademarks of Internet Security Systems, Inc. in the United States, other countries, or both. Internet Security Systems, Inc. is a wholly owned subsidiary of International Business Machines Corporation.

Other company, product and service names may be trademarks or service marks of others.

References in this publication to IBM products or services do not imply that IBM intends to make them available in all countries in which IBM operates.