Table of contents

Introduction ............................................................3
The Network Immunity Solution ..................................4
Benefits of Network Immunity Solutions .....................4
Competitive advantages ...........................................7
Summary .................................................................8
Introduction

Current security threats
Today, networks are being attacked and threatened in devious and creative ways, now more than ever. Incidents range from viruses and worms to Trojan horses and internal sabotage.

Over the past decade, the primary network security strategy for many IT managers has been to invest in perimeter security defenses to protect against external threats. They believed that all threats were external, and that the network with the biggest moat at its network perimeter was the safest. Packet-filter routers, firewalls, applications proxies, and VPNs are all technologies that came of age during this time.

Vendors and customers came to see their network design as having a “hard crunchy shell with a soft chewy center.” That is, security strategies intentionally disregarded internal network edge security, assuming that (somehow) the internal network was inherently more secure. For many organizations, this assumption has backfired painfully.

Without adequate protection from internal threats, networks are susceptible to viruses, worms, user sabotage, and other attacks that can cause significant downtime, revenue loss, end-user dissatisfaction, and an increase in IT management bandwidth.

Solutions for internal threat protection
Current options available for customers to comprehensively detect attacks inside their network are usually costly, performance limited, and are marginal in security value.

Many customers today are protecting their networks by putting firewalls at the periphery of their network and antivirus software on client PCs. Unfortunately; their networks are vulnerable to advanced security threats, such as viruses and worms, since most firewalls are incapable of performing deep inspections to look for virus signatures. Firewalls do not perform Network Behavioral Anomaly Detection (NBAD) to look for network behaviors indicative of attacks. Likewise, PC antivirus software does not protect against zero-day virus attacks, not to mention the fact that many customers permit network access even to end users whose antivirus files aren’t up-to-date.

Other organizations have installed expensive technologies such as Intrusion Prevention System (IPS) devices in line with many distribution switch uplinks. Given the higher cost and lower performance of IPS compared to the switch networking infrastructure, it’s obvious that customers need a more efficient and affordable solution to gain visibility into internal threat activity.

HP Networking offers an alternative with Network Immunity Manager (NIM), a cost-effective software solution for managing internal network threats. Bringing security and the network together, NIM leverages internal attack detection in conjunction with external network and security information to monitor the network for internal threats. With the ability to pinpoint the source of security events, NIM leverages the network to mitigate those threats.
The Network Immunity Solution

HP Networking E-Network Immunity Manager has a rich toolset to manage internal network threat detection and response.

HP Networking NIM monitors security devices, access points, and switch ports across the network for internal network threats and allows administrators to set detection and response security policies. In addition, the NIM includes a central management system for firewall and IPS configuration of the HP Threat Management Services zl Modules.

By leveraging secure traffic monitoring technology built into HP switches, such as sFlow and Virus Throttle, HP Networking NIM performs NBAD to detect and respond to internal threats in both wired and wireless networks. Optionally, the NIM can remotely mirror suspect traffic to an IDS/IPS/UTM appliance for high-confidence detection of known viruses, using virus signature file matching. With NIM, IT managers enjoy broad coverage against internal attacks and a rich set of mitigation and offender tracking capabilities.

This easy-to-use security management tool turns access points and switch ports into security sensors, providing visibility to internal threat activity on the network and helps administrators to improve network availability.

Benefits of Network Immunity Solutions

Businesses need to maintain maximum network availability, meet regulatory compliance requirements, protect their investment in network hardware and management tools, and deploy affordable, efficient solutions. For companies who have invested in HP switches, the NIM meets these critical needs.
There are two ways to deploy attack detection with the NIM: in standalone mode or in conjunction with third-party security devices.

**NIM in standalone scenario (NBAD)**

- HP switches send sampled traffic using sFlow technology to NIM, which performs NBAD on the data to detect internal attacks.
- NIM can accept virus alerts from HP switches running Virus Throttle software that detect IP Fan Out virus behavior.

The NIM can detect the following types of internal threats:

- **Zero-day and known viruses or worms, similar to:** SQL Slammer, Code Red, Sasser, and MSBlaster.
- **Protocol anomalies, similar to:** Land attack, UDP Flood, and UDP Bomb.
- **Reconnaissance scans, similar to:** Port scanning, fping, SuperScan, and Nmap.
- **Network-based attacks, similar to:** DNS tunneling, Smurf, and IP spoofing.
- **Anomalous packet sizes, similar to:** Ping-of-death, Nmap, and Netcat.

- NIM’s NBAD capability doesn’t rely on signature file matching in the same manner as antivirus or IPS, but rather detects behaviors symptomatic of viruses, worms, or malicious users.
Third party security devices scenario

• NIM can accept security attack alerts from select third-party devices, such as IDS/IPS and UTM appliances, that have already been deployed in strategic locations. This allows organizations to leverage existing security infrastructure without having to do anything more than sending security alerts to the NIM.

• NIM can bring suspect traffic to a security device for inspection by leveraging Intelligent Remote Mirroring feature from HP, present on ProVision-based switches. This allows the security device to be virtually deployed anywhere within the network at a moment’s notice. The security device can then inspect the traffic and generate alerts that are subsequently consumed by the NIM for correlation, mitigation, and logging purposes.

Response

• As security events occur, NIM can be configured at multiple response levels, from just quietly recording events as they unfold to taking multiple active mitigation actions against the threat.

• NIM can be configured to send emails when one or more events of interest occur.

• NIM can respond to attacks on a per-access point or per-port basis, based on the policies set by the IT administrator. The spectrum of responses include:
  – Quarantine the attacker on a VLAN
  – Bandwidth rate limit the port that originated the attack
  – Lockout the attacker’s MAC address
  – Shutdown the attacker’s port
  – Mirror suspicious traffic to security device

Security management

The Network Immunity Solution supports these security management features:

• Policy management—Utilizes the PCM Automation Manager to create and manage mitigation policies based on event source, location, time, action, and other alert parameters

• Security event collection and suppression—Collects security alerts from anomaly detection, HP switches, and third-party security devices in a single management tool, and suppresses duplicate alerts to trigger a single action for a flood of alerts

• Security dashboard—Provides a real-time view of security activities, mitigation actions taken, and offender details across the network over various time intervals

• Whitelist (exempt list)—Allows you to create a set of IP addresses, MAC and DNS names that are exempted from mitigation actions

• Configuration cleanup—Provides automatic rollback response configurations from HP switches and wireless access points after the policy expires

• Security auditing—Utilizes PCM Audit Logging to log any changes to policy configurations and network devices

Reporting

The Network Immunity Solution can provide security policy reports and offender tracking reports for forensics. The Network Immunity Solution supports these reporting features:

• Data Mining—Generate network, offender, and alert-based tabular reports with various degrees of information granularity

• Custom Reports—Generate reports from the PCM database schema to assist with regulatory compliance.
Flexible deployment
To provide flexible deployment, NIM supports several use models:
• Network behavior anomaly detection and response—Use NIM to detect unknown or zero-day attacks and mitigate threats at the HP network edge.
• Active intrusion prevention and response—Prevent attacks using an inline IPS/UTM appliance; mitigate threats at the network edge using NIM.
• Passive intrusion detection and response—Detect attacks using an offline IDS/UTM appliance and mitigate threats at the HP network edge using NIM.

Scalability
The Network Immunity Solution provides broad coverage for small or large switch and access point coverage.
• Monitoring—Up to 10,000 edge nodes across the wired and wireless network.

Third-party IDS/IPS/UTM device support
NIM supports these third-party IDS/IPS/UTM devices:
• Cisco IPS 4200 series sensor
• ISS Proventia G Series IPS appliances
• Fortinet UTM appliances TippingPoint IPS (excluding SMS and ZPHA models)

Industry-leading warranty
• 90-day media warranty (software)

Competitive advantages
NIM has a simple, efficient, and affordable architecture that provides broad coverage of internal threat protection for wired and wireless networks. Comprised of several components, NIM utilizes security monitoring technology that is built into HP switches.

NIM differentiates itself from the competition by:
• Providing wired and wireless support. Other solutions are designed to function only in a wired or wireless environment, but not both
• Making full use of the security capability of the switch and access point infrastructure. Many HP infrastructure devices include built-in sFlow sampling technology and/or Virus Throttle
• Offering a rich set of response options, as compared with most competitors’ limited set of response actions
• Supplying more security with less complexity. HP has always differentiated itself by providing advanced and intuitive technologies
Summary

HP Networking E-Network Immunity Manager (NIM) is the Defense component of the HP Networking ProActive Defense security strategy in building trusted network infrastructures. Together with HP Networking Access Control solutions such as Identity Driven Manager, NIM provides security at the edge of the network where users connect. NIM defends the network against internal threats by detecting and responding to internal threats. In addition, NIM includes a central management system for firewall and IPS configuration with the HP Threat Management Services zl Modules.

The HP Networking E-Network Immunity Solution provides:

• Enhanced network availability
• Affordable and efficient scalable solution with few components
• Internal threat management
• Zero-day attack protection
• Increased value of current investment in HP switches
• Offender tracking capabilities
• Internal threat coverage for both wired and wireless networks

The HP Networking E-Network Immunity Manager helps customers deploy the right security solutions based on their individual needs.