Network Protection v4

The challenge

There is little doubt that organizations today must protect their networks from malicious threats to their corporate and customer data. With more information moving in and out of networks from a variety of sources, the risk of infection from malware is high. Norman delivers the most effective protection available for enterprise and industrial networks.

The solution

Norman Network Protection is a comprehensive, high performance security appliance that helps organizations to effectively protect critical IT infrastructure against cyber criminals.

Key Benefits

Out of the box antimalware turnkey solution: Delivers everything you need to protect your network against malware in one appliance.

Quick setup: Norman Network Protection appliences can be easily set up with a first-time configuration wizard.

Integrated security management: Norman Network Protection appliences come with integrated gateway management, offering the ability to centrally manage multiple NNP gateways from a single console.

URL blocking: Prohibits access to unwanted web sites, preventing users from being exposed to threats and inappropriate content.

Full Duplex 10Gb/s Network performance and true 64-bit Linux multithread support: Ensures high availability of business-critical applications with up to 10Gb/s Ethernet throughput and high performance antimalware scanning utilize true Linux 64 bit multithread support.

High availability solution*: Norman Network Protection high availability solution enables organizations to survive system or application failures with no discernible interruption to business-critical applications. NNP supports different levels of fail-over options for high-availability networks. Entry level fail-over can be provided with a Silicom Bypass Server network adapter. For enterprise level fail-over NNP delivers a 2-node hardware fail-over solution.

Enhanced Security: Looking for malware where no other solution is able to! Thousands of malicious files are using network protocols to get deeper into your network. With NNP, for the first time, you are able to prevent spreading on frequently used network protocols like RPC, Windows file sharing protocols in addition to the traditional internet protocols.

Latency - not a problem: Traditional proxy solutions have several drawbacks. The most important consequence is the latency in data traffic created by the proxy itself. A proxy holds back the entire stream of files, while NNP avoids this problem by only holding back the necessary data needed to perform a malware scan.

Prevention: When the NNP appliance detects a malicious file in transfer on your network, it actively terminates the file transfer and blocks the specific network path to prevent other users or systems from accessing the same file.

Transparency: NNP operates on Layer 2 in the network and is transparent to the IP traffic. No IP reconfiguration of your network is needed, just add an address for the administration interface and NNP is instantly protecting your network.

FEATURES

GENERAL:
- Deployable anywhere in the network
- Easy installation and maintenance
- Highly scalable hardware platform
- Mirror port / SPAN port support
- Support for 10Gb/s networks
- Supports unlimited number of VLANs
- High Availability
- Redundancy/fail-over solution on software & hardware

MALWARE SCANNING:
- Realtime malware scanning of network traffic
- Automatic outbreak prevention and damage control
- Malware source detection and isolation
- Proactive protection with Norman SandBox®, Norman DNA Matching and Norman Exploit Detection inside
- Realtime analysis of unknown malware via Norman SandBox® log
- Automatic scan engine and signature update
- Unmatched protocol scanning capabilities; FTP, HTTP, SMTP, POP3, RPC, TFTP, IRC and Windows file sharing

OTHER FEATURES:
- Optional blocking of MSN traffic and BitTorrents protocol
- Customizable content/URI blocking
- Multi-tiered traffic blocking or exclusion based on IP-address, MAC-address or VLAN ID
- Supports SNMP-based management systems
- Multithreaded application with multi-CPU support
- Runs on Linux
- Available as hardware and software based solution

"What was especially interesting for Arla Foods was that the system could be implemented without requiring major changes to the existing equipment."

Jens Roed Andersen, Chief Information Security Officer at Arla.

In-line or out-of-band? Your choice.

You can implement NNP based on your preferences. If you prefer to be able to prevent malware from entering your network you can put the NNP in-line in your infrastructure. Otherwise you can use NNP to monitor the traffic on a mirror port on a switch and only get alerts when malware is detected.

Centralized management

Centralized management of the NNP is performed by the Norman Endpoint Manager (NEM), a powerful web based graphical security operations center.

The Norman Endpoint Manager provides a central console for multiple NNP's, and keeps the desired configuration and security level through policies. This enables IT administrators to easily manage several NNP's security state remotely making use of policy templates which are fully configurable to keep control of the networks' security state and receive outbreak alerts from any point in the infrastructure.

NEM gives real time statistics and reports, presenting detected and blocked malware, system statistics and network statistics. This real-time information includes source end destination, address fields, protocols used for transport and detected malware signature or class. The incident log shows currently blocked URL's where malware has been detected.

With NEM, the IT administrator can deploy Norman Network Protection and Endpoint Protection clients, and manage them all through security policies. With the built-in policy tool, the administrator can keep the desired security state throughout the whole network. Being proactive is the only way to stay secure. With Normans SandBox® technology targeted attacks and never previously seen malware will be detected. The Norman SandBox® Technology is a virtual environment where programs may perform in safe surroundings without interfering with the real processes.

	NNP-R210-75	NNP-R210-250	NNP-R610-UL
Nodes protected	75	250	Unlimited users
Processor	Intel Xeon X3450 Processor (2.66GHz, 8M Cache, Turbo, HT) 1 S	Intel Xeon X3450 Processor (2.66GHz, 8M Cache, Turbo, HT) 1 S	Intel Xeon X5550 Processor (2.66GHz, 8M Cache, 6.40 GT/s QPI, Turbo, HT), 1333MHz Max Memory
RAM	4GB Memory (2x2GB Dual Rank UDIMMs) 1333MHz 1 S	4GB Memory (2x2GB Dual Rank UDIMMs) 1333MHz 1 S	6GB Memory for 1 CPU (3x2GB Dual Rank UDIMMs) 1333MHz
Hard drive	250GB SATA	250GB SATA	2x73GB SAS 10k 2.5" HD Hot Plug. Raid 1
Network	4x10/100/1000Mb/s Ethernet	4x10/100/1000Mb/s Ethernet	4x10/100/1000Mb/s Ethernet
OPTIONS			
*HA	yes	yes	yes
Processor			Intel Xeon X5550 Processor (2.66GHz, 8M Cache, 6.40 GT/s QPI, Turbo, HT), 1333MHz Max Memory
RAM			12GB RAM, 24GB RAM
Network Card	Gigabit Ethernet Bypass Server Adapters for failover option (copper and fiber)	Gigabit Ethernet Bypass Server Adapters for failover option (copper and fiber)	Gigabit Ethernet Bypass Server Adapters for failover option (copper and fiber). 10Gb NIC copper and fiber
Power Supply			Redundant Power Supply

NORMAN SANDBOX® is a revolutionary way to detect new and unknown malware in a proactive way.

NORMAN DNA MATCHING is a proactive method for identifying the viral profile of all kinds of malicious programs.

NORMAN EXPLOIT DETECTION is a technology for detecting malware exploiting vulnerabilities in widely used document types.

virus BULLETIN

"Providing such simple and unproblematic malware protection, along with an excellent, again very straightforward control system, makes this an extremely user-friendly weapon in the fight against malware problems in business networks, as well as a powerful one. We look forward to investigating a wider range of appliances to see how they match up to this impressive effort from Norman."

NETWORKcomputing

"The NNP clearly has a number of advantages over traditional gateway security devices as it can be deployed across a much wider range of network scenarios.

Installation doesn't get any easier, it is transparent in operation and the Norman SandBox® technology provides a very strong security barrier."

NORMAN®

www.norman.com   Norman SandBox® US Patent Number 7,356,736