Nevis NETWORKS

Solution Brief

Access Control for Wireless/Guest Networks

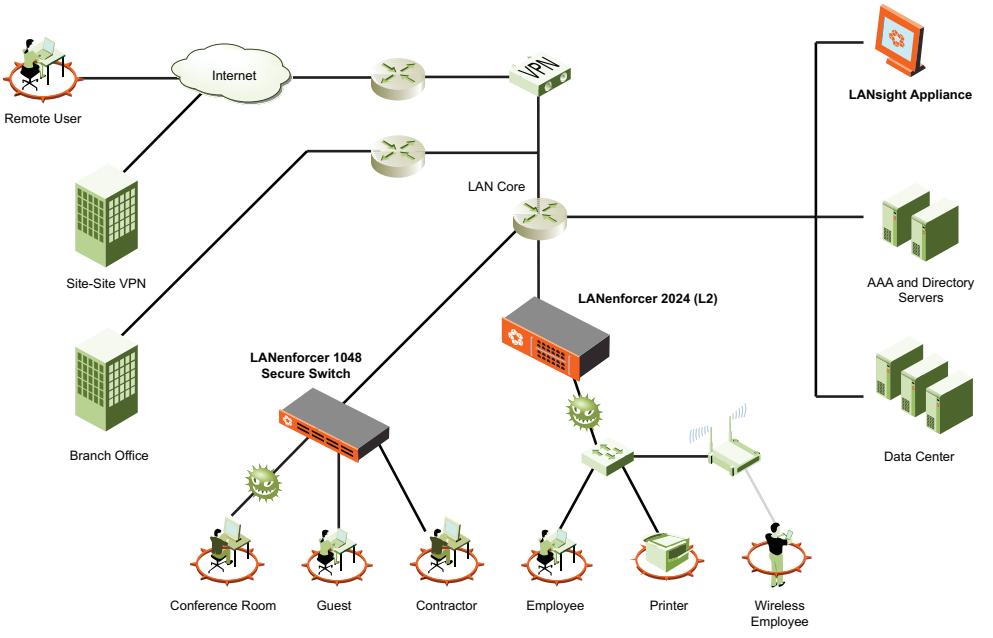
The Need for Enhanced Wireless Gateway and Guest Access Security

One of the most vulnerable network access points in the enterprise is the wireless LAN gateway and other access points, such as conference rooms, that can be used by guests, contractors and business partners. External systems that connect to the network through these access points are frequently not owned by the enterprise, and the users are often not employees. In most cases, it's not feasible for the enterprise to ensure that these external systems are running appropriate versions of operating systems, or anti-virus / anti-spyware software, and that they are up-to-date with current patch levels and signature files. This can expose the internal LAN to unacceptable risk from external viruses and other malware.

Protecting corporate assets, such as intellectual property and customer data is always a concern for network security managers. This problem is compounded in many installations by the location of the wireless gateway and other access points behind the corporate firewall so that these users are typically subjected to less scrutiny than other external systems. Once external users are allowed through the wireless gateway, what access restrictions to sensitive assets can be reasonably applied? An all-or-nothing approach to network access for all external users, which is common to many wireless gateway solutions, doesn't make sense, and the usual security policies that can be enforced on internal network systems either don't apply or can't be enforced. What enterprise LAN managers are looking for is a method to cloak sensitive network assets from specific classes of remote users so they can't be accessed, seen, or even probed for.

Solution Highlights:

- Remote endpoint health validation and quarantine
- Identity-based access control of remote users to internal network assets
- Intrusion detection system for threat containment
- Audit log for each user of resources accessed
- High-performance in-line appliance (10GBps)



The Nevis LANenforcer appliance provides all aspects of LAN security for wireless gateways and other unmanaged endpoints on the internal LAN. Security is provided for external systems such as those belonging to contractors, guests, and business partners.

"There are five key technologies enterprises should include in their NAC deployment strategy. The Nevis solution offers elements to support each of these requirements and differentiates itself through advanced persistent threat detection and containment."

Joel Conover
Research Director,
Enterprise Networks and Security

Current Analysis

The Nevis LANenforcer 1048 and 2024 are scalable rack-mounted devices that easily install into any network topology (both shown on top of the LANsight appliance).

The Nevis Networks LANenforcer™ LAN security solution

Nevis Networks is a leader in providing LAN security solutions that protect the internal core network from all threats arising from endpoint systems, whether internal or unmanaged external systems. The Nevis LANenforcer appliance forms a four-pronged countermeasure to defend against all categories of network security threats from untrusted systems accessing the internal network:

- **Endpoint validation**: pre-connect and post-connect authentication of the user and system and ensuring the health and compliance of the system's operating environment;
- **Identity-based access control**: ensuring that specified user groups and roles are constrained within the internal network to only specific systems and applications;
- **Threat containment**: going beyond ensuring anti-virus signatures are up to date, Nevis uses state-of-the-art deep packet inspection algorithms, including behavioral, protocol and traffic anomaly detection to protect against new malware attacks (worms, Trojans, bots, etc.);
- **User activity monitoring**: keeping a detailed audit trail of which users accessed which resources and systems for regulatory and compliance purposes.

When deployed in proximity to the wireless gateway, the Nevis LANenforcer defends the internal network from these external users, including validating that their systems comply with the network's system health policy, detecting and halting the spread of malicious malware, and preventing unauthorized system access by inappropriate groups. LANenforcer is easily deployed in-line to monitor all user traffic and provides the industry's only solution that performs the full range of LAN security services at wire-speed (10GBps).

LANenforcer performs the system scan to validate external client endpoints, as well acting as another identity-based firewall that screens users from critical resources based on role and group privileges. LANenforcer also performs inline intrusion detection and prevention (IDP) at wire speed based on its proprietary LANsecure™ ASIC, which dramatically raises the performance bar for all other competitive solutions.

A single LANenforcer appliance provides an extremely cost-effective solution because it can easily support up to 3000 users. Larger installations can be accommodated with multiple LANenforcer appliances.

Nevis Networks

Nevis Networks, Inc.
295 Bernardo Ave., Suite 100
Mountain View, CA 94043
www.nevisnetworks.com
(650) 254-2500

Nevis Networks International HQ
Delegate House
30 Hart Street
Henley on Thames, UK RG9 2AL
Tel: +44 1491 635 339

Nevis Networks India
C301 Pune IT Park
Bhau Patil Marg
34 Aundh Road
Pune 411020, India
Tel: +91 98450-05047