Nevis NETWORKS

Solution Brief

Identity-based Access Control to LAN Assets

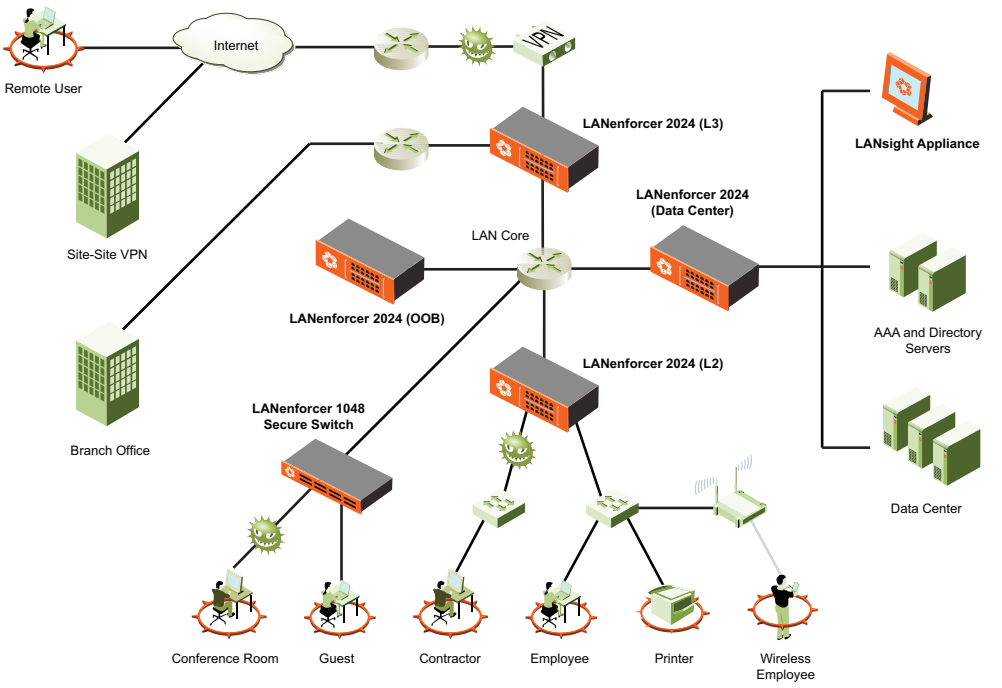
Mapping your organization's security policy to your LAN architecture

Controlling access to critical network applications and data is a primary objective of a network security architecture. Ensuring that only authorized users access sensitive systems is even more important given the extent that enterprise LANs are open to external users such as contractors, guests, remote users, and mobile systems. A natural approach to managing this problem starts with an understanding of the organization's security policy, or who really should have access to what. Unfortunately a real-world view of this problem does not correspond to traditional LAN security enforcement solutions, such as firewalls or IPS systems. Segmenting a LAN and creating chokepoints to access other subnets and resources is a complex, static and costly way to implement a security policy. Access based on physical location or network attributes also conflicts with the fact that users access the network from many points and potentially many systems. Such LANs are not adaptable to dynamic business requirements.

What is needed is a LAN security access control solution that maps easily to user and group based access policies as maintained within the organization, and is eadily integrated with existing user directories. Access control policies could be changed dynamically as business needs dictate, merely by changing a users profile. Packets traversing the network could be inspected and denied based not on mundane network attributes like MAC or IP address, but by the user that sent the packet. An optimal solution would enforce such policies at wire speed.

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 can be deployed at various network access points or in front of key assets like the datacenter. Security is provided for external employees as well as remote offices and other unmanaged endpoints such as 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 used to enforce application and data access control policies, LANenforcer examines each data packet from a user perspective, and denies packets with inappropriate destination address. The result is that unauthorized users, whether malicious internal employees, external users, or self-propagating worms, can not access, or even detect sensitive assets, even to probe for available ports or services.

LANenforcer is an in-line appliance, enforcing the enterprise access policies in real-time, at wire speed (10Gbps) without slowing network performance at all. Nevis is the only vendor that can accomplish this feat due to its proprietary LANsecure ASIC architecture which incorporates rapid, parallel, deep packet inspection algorithms. Out-of-band appliances can not provide true access enforcement and are easy to circumvent.

LANenforcer makes the management of security policies easy by integrating with existing user directories, such as LDAP, Radius and Active Directory. Changing group access privileges and adding access for a remote employee or contractor is easily added dynamically through the LANsight policy server. Rich reporting and simulation tools always let you know how your access rules are behaving and which users are accessing which resources. Even compliance audits now become a breeze to prepare for and manage, quickly proving how policies are enforced.

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