Nevis NETWORKS

Solution Brief

Datacenter and Critical Asset Protection

The Need for Increased Datacenter Access Control

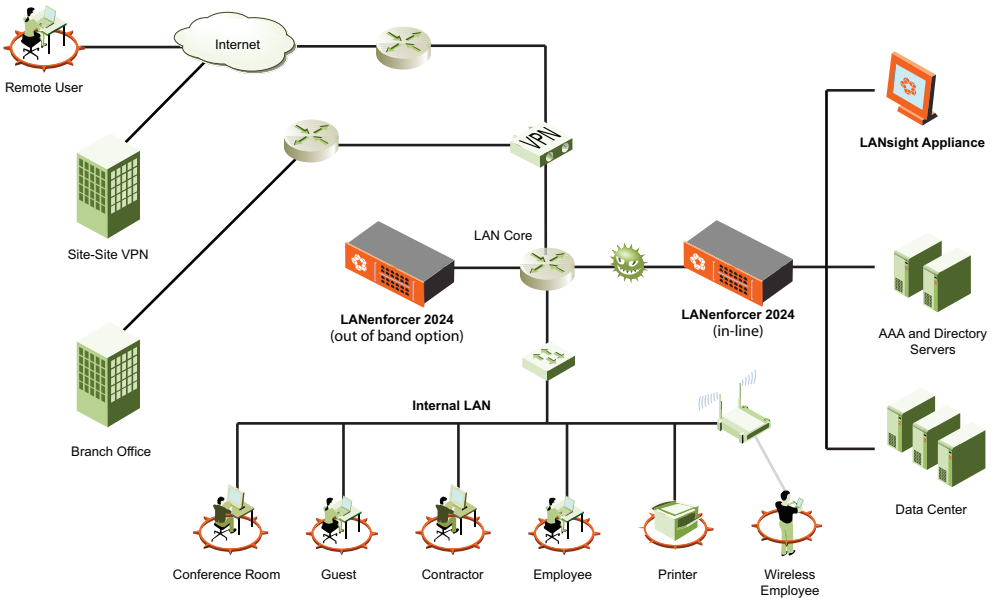
Perhaps the most important goal of a network security infrastructure is to protect an organization's critical data assets. Unauthorized internal access to intellectual property or customer data can cause millions of dollars in losses and regulatory fines, or both. Achieving this goal has become a more costly and time consuming task as the network perimeter dissolves and enterprises open up their internal LAN networks to external users, unmanaged systems, mobile devices, contractors, guests, business partners, et al. Restricting access to sensitive data assets from these "untrusted" users and systems accessing the LAN becomes a complex problem and renders most network security solutions designed to isolate trusted internal systems and users from hostile Internet obsolete.

A security model is required that allows administrators to build access policies based on a user's identity and group affiliations rather than based on the location of the user or the user's system (such as the IP address, subnet or VLAN the user is using). Firewalls, which can easily partition networks and restrict access to particular internal domains, lack key features to build policies around user identities, so there is no way to differentiate access, for example, for a contractor and an key employee accessing the network from the same conference room.

Once external users are allowed onto the network, what access restrictions to sensitive assets can reasonably be applied? An all-or-nothing approach doesn't meet obvious business requirements, and a more granular policy is difficult to impossible to enforce given to existing LAN architectures. An ideal solution to protecting the datacenter needs to also consider a wide range of threats that includes malicious unauthorized users, as well as viruses, worms and Trojans that unhealthy endpoints can unleash on the internal network.

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 forms a complete access policy enforcement and LAN security solution to protect critical datacenter assets from untrusted and unmanaged endpoints throughout the enterprise network.

"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 front of the datacenter, LANenforcer forms an impenetrable shield to unauthorized users, based on identity or group. Acting as an identity-based firewall, traffic is filtered out by the appliance so that critical servers are completely cloaked from unauthorized users and rogue processes so that they can not even be located or probed for. In addition, the LANenforcer appliance keeps malware threats out of the datacenter through its intrusion prevention capability, identifying and stopping worms and other threats in milliseconds.

Because LANenforcer is a wire-speed, in-line network security appliance, it forms a critical gateway to the datacenter to filter unauthorized traffic and enforce access policies. As a critical pass-through point, both performance and continuous operational capability are of prime importance to keep your datacenter available and business running. LANenforcer is designed with complete operational failover in mind, allowing the appliance to failover to a high-availability spare. To ensure maximum throughput, Nevis has designed a custom ASIC that analyzes network traffic at 10Gbps so there is no decrease in bandwidth or performance penalty by introducing the appliance in-line. A single LANenforcer appliance provides an extremely cost-effective solution for 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