

FOR IMMEDIATE RELEASE

Denise Barton
Nevis Networks, Inc
650-254-2577
dbarton@nevisnetworks.com

Kristin Kiltz
Engage PR
510-748-8200, ext. 204
kristin@engagepr.com

**Nevis Networks Locks Down Enterprise LANs With Comprehensive,
ASIC-Based LANenforcer Appliances**

*Nevis Appliance Family for the First Time Integrates All the Security Functions Necessary to
Ensure Network Availability, Protect Data Integrity and Privacy, and Assure Regulatory
Compliance*

MOUNTAIN VIEW, Calif. – November 14, 2005 – Both dramatically simplifying and fortifying LAN security, Nevis Networks today introduced its LANenforcer™ products, a family of ASIC-based LAN security appliances that fully protect network assets from security threats. The LANenforcer family delivers the broadest access control, deepest threat defense, and fastest threat response to create a Personal DMZ™ around every user on the LAN. Companies now can match business policies to network activity, protect network assets from unauthorized access, contain network security threats, and meet regulatory reporting and auditing requirements. The LANenforcer family’s LANsecure™ architecture integrates the functions of many point security products into a single appliance for the first time, simplifying deployment and operations. Nevis’ patent-pending LANsecure ASIC, the heart of the product architecture, delivers disruptive price/performance, providing parallel security processing at wire speeds.

(Editor’s Note: For more information about Nevis’ LANsecure architecture and ASIC see the release titled “Nevis Networks LANsecure Is First Architecture to Comprehensively Solve Multi-gigabit LAN Security Challenges,” also released today.)

“LAN security is a tremendous priority for enterprises. As the LAN has evolved from simple network transport to a mission critical enterprise asset, any network down time directly affects the bottom line,” said Charles Dauber, president and CEO of Nevis. “IT managers are inundated with LAN threats that are bypassing perimeter security defenses, including laptop-born worms and spyware, employee regulatory compliance issues, and guest and contractor resource access. Nevis’ LANenforcer products offer a comprehensive approach to LAN security that for the first time enables the IT department to fully lock down the enterprise LAN at LAN speed.”

Flexibly Deployed LAN Security Appliance Family

Nevis LANenforcer products were developed for easy integration into existing environments and require no changes to existing VLAN or AAA configurations. The family includes two series, each optimized for a different LAN deployment model:

- LANenforcer 1000 Series appliances operate at the network access layer to provide the most secure method for locking down the LAN. This deployment model adds a layer of security that surrounds each individual user, creating a Personal DMZ to protect him or her from network-borne threats, and vice versa.
- LANenforcer 2000 Series appliances are deployed transparently, aggregating existing access layer switches and enabling rapid rollout to a large number of users with unmatched price/performance.

“As a federally registered investment advisor, Financial Engines seeks to ensure the security and confidentiality of millions of individual customer records, and we take this duty extremely seriously,” said Dr. Matthew Todd, chief information security officer and vice president of risk and technical operations for Financial Engines, Inc. “Current solutions have limited scalability because they require time-consuming hands-on monitoring and the correlation of access control information. The Nevis LAN security appliances will make it easier to provide auditors with easy review and proof of due care, while simplifying day-to-day access control management.”

Comprehensive, Dynamic Access Control with No Client Software

Nevis' LANenforcer appliances link user, endpoint, network, and application access policy control into a single dynamic access control system, to ensure data integrity while simplifying security provisioning and monitoring. Unlike existing alternatives, no client software is required, which makes deployment easy, eliminates the need for desktop software maintenance, and significantly lowers acquisition and operating costs.

Access control begins the moment a user attempts to connect to the network. Automatically and transparently, the LANenforcer system begins a security audit of the user device, checking that it conforms to corporate endpoint security policies—that it is equipped with the most up-to-date anti-virus and anti-spyware applications and the latest operating system patches. Endpoints that fail security assessment are denied network access and automatically quarantined for remediation.

LANenforcer allows screened users network access by leveraging existing authentication policies and servers. The product family dynamically applies identity-based policy rules to

secure access to resources, services, and applications on the network and logs user activities for accountability and compliance.

“The clientless nature and the vendor neutrality of the Nevis solution are very attractive,” said Troy Moritz, senior security and infrastructure architect for one of the nation’s five largest insurers and a Fortune 500 company. “When 13,000 users rely on the network to be available, I want a LAN security solution that I can drop into an existing environment to protect ‘trusted’ employees as well as contractors and guests automatically—without special software for every device. I also want to control and neutralize threats in microseconds and receive a complete audit trail. The Nevis LANenforcer systems have the power, the visibility, and the access and threat control features to satisfy all these requirements.”

Deepest Threat Defense with Microsecond Threat Response

Nevis LANenforcer appliances use six methods of wire-speed parallel processing to simultaneously implement defense-in-depth for every endpoint. The threat-response mechanisms are: a stateful firewall; traffic, protocol, and behavior anomaly detection; threat signature matching; and automatic endpoint quarantine. Nevis can rapidly and accurately correlate events, triangulate on actual threats, and take action to prevent their spread. Microseconds can make a difference between rampant spreading or containment of malware; LANenforcer can shut down a worm in 150 microseconds—at least 20 times faster than alternative products.

“Enterprises face increased demands for security mechanisms to defend against a growing variety of threats and to meet increased scrutiny by internal and external auditors. Nevis’ approach provides both policy-based prevention of undesirable behaviors as well as better activity accountability through integrated logging and reporting. Overall the use of an integrated security appliance simplifies the network security architecture and reduces management overhead,” said Phil Schacter, vice president and group service director, Burton Group.

Pervasive Visibility into Every Endpoint

Nevis’ LANSight™ security manager provides enterprise-class, centralized security policy configuration, event correlation, and reporting for LANenforcer appliances, giving network administrators unprecedented control and visibility into security-related activity for every user on the LAN. LANSight integrates the configuration, monitoring, reporting, and analysis of multiple security functions into a single platform, enabling LAN-wide security policy management and reporting.

Advanced multivariate event correlation analysis transforms and consolidates security event data into concise, actionable security information—in real time. By handling up to 200,000 security events per second, LANenforcer enables a network administrator to pinpoint a problem quickly and respond appropriately, without having to sift through volumes of data.

For compliance purposes, the LANSight security manager provides the required level of accountability defined by regulatory guidelines and offers persistent and pervasive visibility into users' network activities and applications usage. The patent-pending event database and event correlation capabilities provide essential insight for root cause analysis, saving significant time and effort over the manual approaches required by existing network security products.

Pricing and Availability

Nevis LANenforcer products are currently in beta trials, and will be generally available in Q1 2006. Entry-level pricing for LANenforcer 1000 Series products is \$12,995; LANenforcer 2000 Series products start at \$34,995.

About Nevis Networks

Nevis Networks develops and markets ASIC-based LAN security appliances designed to help corporations protect information privacy and integrity, ensure network availability, and maintain regulatory compliance. With its patent-pending LANsecure architecture, the Nevis LANenforcer product family combines the most comprehensive access control, deepest threat defense, and fastest threat response to create a "Personal DMZ" around every user on the LAN. Nevis was founded in 2002 by seasoned executives with strong track records in security, semiconductor, and networking technologies, and has raised over \$40 million from veteran Silicon Valley investors New Enterprise Associates, BlueRun Ventures, and New Path Ventures. The company is headquartered in Mountain View, California, with an R&D center in Pune, India.

For more information, visit the Nevis Networks web site at www.nevisnetworks.com, or contact the company at (650) 254-2500.

###