Application Recognition and Policy Compliance

Nevis Networks

Persistent LAN Security Solutions

Executive Summary

A complete LAN Security solution includes network access control, malware prevention, and user activity monitoring and control. An integrated approach can effectively secure the internal network against threats and security policy violations and ensure an organization's network activity is in compliance with stated policies.

A critical aspect of enforcing network policy compliance is ensuring that only safe, authorized applications and protocols are allowed on the network. The benefits of a strong application recognition and policy enforcement solution include:

- Keeping the network secure from potential threats in hard-to-secure application streams
- Maximizing network capacity and providing quality of service (QoS) for latency sensitive applications such as voice and video
- Closing potential data leaks through unauthorized data transfer applications and protocols that limit content visibility
- Ensuring compliance by enforcing corporate communications policies for applications such as Instant Messaging (IM) or other peer-to-peer (P2P) applications

The requirements for application recognition and control solutions include sufficient application coverage, reporting tools, and, perhaps most importantly, adequate performance so that application analysis and remediation can occur without compromising LAN network speeds of 10 Gbps or more.

1 Policy Enforcement: The Intersection of Identity and Application Awareness

As organizations confront a dissolving network perimeter to accommodate mobile, external and remote users, as well as non-employees and unmanaged endpoints, they are forced to focus on the security policies enforced on their internal network. Traditional network security appliances (switches, firewalls, and IPS systems) focus on packet-level and flow-based details such as IP addresses, port numbers and system identifiers.

Network security policies, however, are defined around users and applications, concepts which traditional security devices have little visibility to. In order to be able to control user access to the network and system resources, as well as to contain the spread of malware, the Nevis Networks LANenforcer™ system is built on a foundation of both user identity and application awareness. LANenforcer systems analyze network traffic and associate each stream with a specific user ID on a particular machine, as well as identifying the underlying application and protocol of the session.

Armed with this additional intelligence, Nevis' LANenforcer can enforce policies by either blocking unauthorized activity, or logging the transgressions.

2 Application Recognition in the LANenforcer System

The primary objective of application recognition is to provide insight into which applications each user is utilizing and then to detect unauthorized activity which presents either a security or compliance risk. Common P2P applications provide an un-auditable communication channel between users inside and outside the organization, and are a prime example of applications that may need to be restricted in many corporate networks

(unlike email which conforms to retention policies). Other application streams are prone to hiding undetectable threats that can propagate quickly throughout an unsuspecting network, or can take advantage of vulnerabilities on sensitive systems.

Nevis' LANenforcer is built with application-level intelligence to recognize and build policies around the following key applications:

- Peer-to-peer (P2P) Applications:
  - Skype
  - BitTorrent
  - Gnutella
  - Kazza
- Instant Messaging (IM) Applications:
  - Yahoo! IM
  - MSN
  - AOL IM (AIM)
  - GTalk
  - Live Messenger
  - Windows Messenger

Organizations that decide to roll-out application-oriented policies have a number of effective remediation steps upon the identification of an offending session. Nevis can accomplish this because the LANenforcer appliance understands the application and has visibility to the user launching the application. Together, this information allows network administrators to specify remediation policies that include:

- User quarantine, such as to a restricted VLAN with limited access policies
- Dropping the packet flow, leaving other legitimate user activity unaffected
- Dynamically adding access control rules stopping traffic between the source and destination IP addresses
- Generating an alarm that can be configured to an appropriate severity level
- Alerting the administrator to review the P2P/IM applications accessed by the user

LANenforcer also provides detailed reporting capabilities aligned around both users and applications to easily demonstrate compliance with existing policies over extended periods of time, or to isolate incidents and policy breaches to specific users in real time.

3 Performance is the Critical Factor

Application-level intelligence becomes impractical in a network security solution if the packet analysis and identification algorithms compromise network performance. The Nevis LANenforcer operates as an in-line security appliance and can remediate all events at 10 Gbps, or true wire speed, without degrading network throughput or introducing latency. The additional packet analysis to determine the underlying application and associate it with a specific user is accomplished in the Nevis LANsecure™ ASIC that is designed with a signature pattern-matching engine. Applications are identified by signature analysis within the first few packets of each flow initiated by the user.

Remediation policies, such as dropping packets or terminating the flow can thus be initiated within microseconds. The vast majority of applications are classified within the first packet of each flow and subsequent packets of the same flow are automatically tagged by LANsecure at wire speed.

This approach and the resulting performance should be carefully compared with that of other in-line LAN security appliances with application recognition capabilities. These products are not equipped with signature analysis (pattern matching) capabilities, and therefore rely only on behavior and protocol analysis to determine the underlying application. This technique requires the analysis of many more packets within the flow to match behavior characteristics, and provides a less certain application match. The resulting overhead in analyzing the data flow degrades throughput dramatically. For this reason such products cannot support application recognition for a large number of users, nor under heavy network loads. Competitive product testing has indicated that with application inspection turned on, performance of a competitive 10 Gbps-rated switch/appliance degrades to well under 1 Gbps, and often as low as 300 Mbps (3-10% of full LAN wire speed).

4 Conclusion

Application recognition is a critical feature for QoS and policy enforcement in today's LAN security environments. The majority of application-related policies in enterprise networks are primarily concerned with the classification and QoS for P2P, IM, voice and video applications, which are often a source of risk from both a security and compliance perspective.

Nevis combines application recognition with identity awareness for a complete policy solution, offering a broad spectrum of supported applications, remediation alternatives and relevant reports. When performance is considered, Nevis offers the industry's only practical solution for application recognition and policy enforcement from an in-line appliance based on the combined capabilities of behavioral analysis and signature matching that allows it to perform at wire speed without compromising network performance.

About Nevis Networks

Nevis Networks provides innovative LAN security systems designed to help corporations protect information privacy and integrity, ensure network availability, and maintain regulatory compliance. Nevis LANenforcer product family integrates NAC with the deepest threat containment at wirespeed to create a "Personal DMZ" around every user on the LAN.

Nevis Networks
Sai Trinity Unit 6, 6th Floor East Wing,
Survey no 146/2/1A+2B/1
Pashan Circle, Pashan,
Pune 411021, INDIA
http://www.nevisnetworks.com