Combating the Evolution of Insider Attacks with Persistent LAN Security

by Shane Buckley, Chief Operating Officer

Nevis NETWORKS

2/8/2007

In just a few years, attack patterns have evolved from shotgun approaches like mass-mailer viruses to sophisticated, targeted attacks. Motivations have also changed significantly. Bragging rights are no longer sufficient pay-off; today's attackers are now seeking financial gain. These attacks are increasingly successful based on limitations in today's defense-in-depth network security provisions, which they are specifically designed to circumvent. This article will analyze the anatomy of today's evolving threat spectrum and describe how persistent LAN security using network access control is essential to staying one step ahead.

Insider Attacks Evolve—and Worsen

The news is not good for IT departments combating threats to network security. Personal information on 800,000 people was obtained from a UCLA database as recently as November 2006. Someone hacked into a TransUnion Credit Bureau server and stole the personally identifiable credit information of more than 1,700 individuals. An employee at UBS planted "time bombs" on some 2,000 servers to cripple operations and send the company's stock plummeting, which he had sold short in a scheme to get rich. Two Ohio University network administrators were fired for not taking "the necessary proactive steps to protect confidential information" after a security breach allowed access to 367,000 files containing personal information.

There are more incidents, of course, among the many reported. And then there are the many more incidents that go unreported with upwards of 75% of all organizations failing to admit security breaches, according to the 2006 Computer Security Survey issued by the Computer Security Institute and the U.S. Federal Bureau of Investigation (FBI). But as new legislation that mandates reporting goes into effect, expect the number of incidents to rise considerably. The Privacy Rights Clearinghouse recently estimated that the total number of exposed records containing personal information now exceeds 100 million. The Ponemon Institute estimates that the per-record cost of compromised data in 2006 to be $182, up over 30% from the previous year.

The new pattern in these attacks is abundantly clear: financial gain. And the culprits are increasingly the organization's "insiders"—the employees, contractors and business partners working inside the network's perimeter protections. Over half of the Chief Information Security Officers surveyed by *Preventsys* stated that they currently use a "moat and castle" security approach, and admit that defenses inside the perimeter are weak. The result, according to the 2005 FBI Computer Crime Survey, is that nearly half of all respondents reported experiencing intrusions from within the organization.

Protection Within the Perimeter With Network Access Control

The need for persistent LAN security employing some form of network access control—or NAC—derives from the ongoing struggle organizations have controlling and monitoring user access, conforming with regulatory requirements, securing guest access, and protecting network resources from noncompliant endpoints. While consensus on what constitutes persistent LAN security has been elusive to date, most industry analysts now concur it is a continuous process that starts with endpoint validation before allowing access to the network, then adds constant protection and policy enforcement after access has been granted. Indeed, the definition of "NAC" is itself evolving as organizations refine their business drivers and vendors develop functionality to meet these requirements. A recent CurrentAnalysis survey shows the primary business drivers for adoption of LAN security to be (in order of priority):

Whitepapers
Conferences
Subscriptions
Free Trial
Subscribe/Renew
Email Format
Unsubscribe
Directories
Geographic
Start-ups
Optical
Silicon
Security
About
Advertising
Editorial Calendar
Submit News
Link to Us
Privacy Policy
Contact Us
Archive Search
About Us

The enforcement of access control policies

The ability to address security compliance requirements

The ability to provide controlled access of unmanaged users, including partners and contractors

To address each of the above business drivers, many industry analysts agree that a LAN security framework should provide protection for users, endpoints and networks beyond simple endpoint posture assessment. According to *CurrentAnalysis*, there are five technology functions generally accepted and expected to be included:

1.Pre-connect host posture assessment

2.Host quarantine and remediation

3.Network access control based on user identity

4.Network resource control based on identity and policy

5.Post-connect assessment with ongoing threat analysis and containment

As these functions indicate, controlling network access should be implemented persistently—with both pre-connect and post-connect security controls. Specifically, pre-connect security controls should include: endpoint integrity verification; host quarantine and remediation, as necessary; and user authentication and authorization. Once users are authenticated and granted access based on authorization criteria, post-connect security controls should include: access control policy enforcement that ties identity to network resources; continuous endpoint integrity verification; threat detection and containment; and continual monitoring and policy violation reporting.

The Five Essentials of Persistent LAN Security

A robust implementation of persistent LAN security ideally views the entire user session holistically, and addresses all areas where exposure to data integrity and network availability risks can be mitigated. Here is an overview of the five technology functions deemed essential to a persistent LAN security solution.

1. Endpoint Integrity Verification – To mitigate malware risk from entering the network at all, the first step requires verifying the presence, currency and enablement of operating system and security software on endpoints before they are permitted to connect to the network. Administrators define the minimum criteria necessary for compliance as it relates to patch levels for operating system, anti-virus and anti-spyware software. Security administrators also define the remediation actions that should occur if an endpoint is found to be noncompliant. Typically, endpoints that do not meet compliance criteria are quarantined with a connection only to remediation servers for installation of updates and required patches. One consideration for a remediation strategy is to determine how to treat unmanaged users and endpoints; some organizations choose to enforce remediation only for company-owned and/or managed endpoints.

2. User Authentication and Authorization – LAN security solutions are designed to ensure that only authenticated users gain access to the network. In most scenarios, an AAA infrastructure, such as Microsoft Active Directory, LDAP or RADIUS, is used to store user authentication information. The solution should, therefore, interoperate with existing directory services and authentication servers. When a user attempts to gain access to the LAN, the LAN security system should challenge the user for appropriate credentials. Typically, a user-ID and password are employed for user authentication.

3. Role-based Access Control Policy Enforcement – LAN security solutions are designed to ensure that only authenticated users gain access to the LAN. In most scenarios, the AAA infrastructure contains the requisite information about a user's access rights and permissions based on role and group memberships, which provides the basis for the LAN security policy decision.

4. Threat Detection and Containment – Since endpoint integrity verification involves checking for the presence and currency of security software rather than checking directly for the presence of malicious code, ongoing threat detection and containment after an endpoint is connected to the network becomes critical to ensuring network availability and data integrity.

5. Continual Monitoring and Policy Violation Alerting – Just as policy enforcement should be continuous, real-time monitoring of user access activity is essential to detecting inappropriate activity by authorized users. Policy violation alerting and compliance reporting are necessary components of the persistent LAN security framework to ensure security controls are working as intended. This information can also be used as feedback for the internal audit team when determining appropriate policy exceptions and making changes to existing policy requirements.

The "In's" and "Out's" of LAN Security

Another consideration in the evolution of persistent LAN security technology is whether this layer of protection should be inline with all traffic, or out-of-band. The table below provides a basic comparison between these two diametrically opposed alternatives.

Characteristics	Inline LAN Security	Out-of-Band LAN Security
Deployment	Distributed, close to the user	Centralized, upstream from user
Role-based Access Control (RBAC)	Provided by user identity-based policy decision and enforcement ("self-contained")	Provided by VLANs – requires VLAN re-architecture; depends on switch for enforcement
Threat Detection	In-depth packet awareness to detect and contain threats in real-time	Not available – lacks packet awareness
User Visibility and Accountability	Granular monitoring of user, endpoint and network activity	Weak – lacks post- admission awareness
Maintenance and Administration	Policy decision and enforcement integration results in unified configuration and facilitates root cause system analysis	Lack of integration for policy enforcement adds complexity to implementation, administration and troubleshooting procedures
Performance Requirements	Purpose-built ASIC required for wire-speed and avoid latency	Less functionality means that off-the-shelf processors are sufficient
Appropriate Use Case	Pre- and post-connect; monitor only and enforcement modes	Pre-connect; monitor only

Inline LAN security appliances are deployed between (or as) the wiring closet switch and the network core. As such, they are distributed throughout a network, close to users, where they can function as both a policy decision point and an enforcement device (the reference to "self-contained" in the table). Inline appliances offer several advantages:

- Integration of identity-based user access control policy decision and enforcement
- Complete traffic visibility for detailed user activity monitoring (tying all traffic to specific users rather than just IP addresses)
- In-depth packet inspection to permit threat detection, prevention and control
- Operation close to the user to allow for rapid containment and remediation
- Deployment that requires no re-architecture of existing VLANs

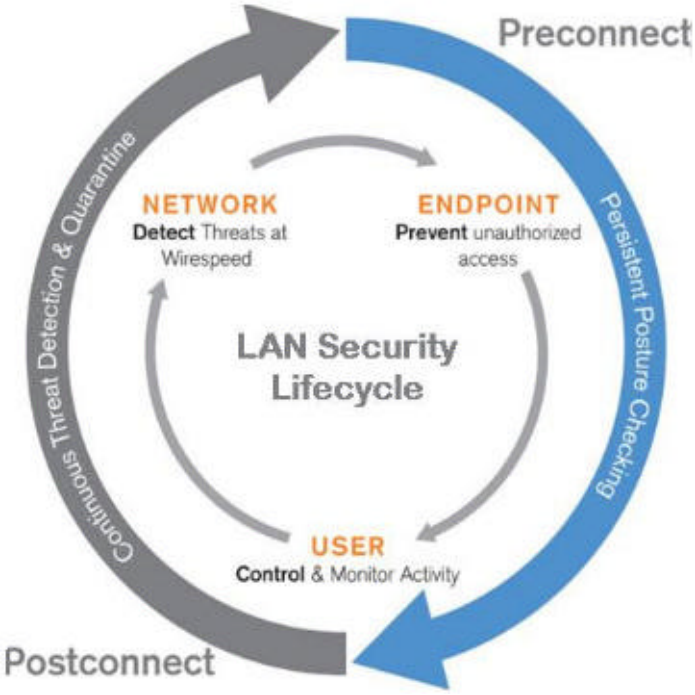
An inline LAN security appliance must, of course, have sufficient processing power to keep pace with LAN data rates and offer a redundant, high availability configuration to eliminate a potential single point of failure.

Out-of-band LAN security appliances are normally centrally located in a datacenter, where they connect to a switch tap or mirror port. The out-of-band solution has two main advantages: it is less intrusive to deploy (no "bump" in the wire); and it requires less processing power since policy enforcement is handled by the switching equipment. But because it is not directly in the flow of traffic, an out-of-band system can act only as a policy decision point with the following disadvantages:

- Limited access control capabilities (reliant upon switch functionality)
- No post-admission access control or threat detection functionality
- Root cause analysis is cumbersome ("Is it the switch or is it the appliance?")
- Deployment complexities (requires VLAN re-architecture)

The LAN Security Lifecycle

The comprehensive nature of persistent, inline network access control can be summarized by the LAN Security Lifecycle depicted in the diagram below.



Conclusion

Protecting the perimeter and mitigating malware risks, while both necessary, are no longer sufficient to combat today's evolving (and increasingly profit-driven) insider attacks. Which is why a growing number of organizations are implementing identity-based network access control to mitigate the threat of unauthorized access to mission-critical data. The early adopters have learned that the best way to meet strict compliance requirements is to combine pre-connect endpoint integrity verification and user authentication with proactive and inline post-connect threat detection and containment.

Centralized security policy configuration, management and reporting is also proving to be essential to providing the real-time and historical visibility needed to resolve problems quickly and track user activity continuously. Waiting for various NAC "marketectures" to mature is simply too risky given the increasing frequency and impact of insider attacks. With persistent LAN security having proved its worth as an essential layer of enterprise network security inside the WAN perimeter protections, Infonetics expects the demand for LAN security solutions to increase by a factor of 10 from 2005 to 2008.

About the Author

Shane Buckley is Chief Operating Officer at Nevis Networks. Prior to joining Nevis, Buckley served as vice president of enterprise at Juniper Networks where he managed the company's worldwide enterprise sales and marketing strategies. Prior to Juniper, Buckley was the international president for Peribit Networks (acquired by Juniper Networks in 2005) where he setup direct operations in 18 countries to sell and support customers. He also held the position of CEO of Conduit Software, where he developed the company's strategic direction and managed operations. Earlier in his career, Buckley was a vice president at 3Com Corporation and established sales and marketing presence in Ireland, growing the business to $25 million in two years. He holds a degree in electronic engineering from the Cork Institute of Technology in Ireland.

About Nevis Networks

Nevis Networks provides innovative ASIC-based LAN security systems 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 integrates NAC with the deepest threat containment at wirespeed 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 design, 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 additional R&D centers in Pune, India and Beijing, China.

Send us your response to this article.

Learn How to Get Your Column Published on this Site