NAC – Beyond Endpoint Checking

Nevis Networks

Persistent LAN Security Solutions

Executive Summary

This white paper provides an overview of Network Access Control (NAC) and its role within a broader LAN security context. While consensus on the definition of NAC has been difficult to achieve, many industry analysts agree that NAC is a continuous process that starts with endpoint validation before allowing access to the network and adds persistent protection and policy enforcement after access has been granted. This paper is intended for enterprise network and security architects who are responsible for operational networks and for others who desire an understanding of the mechanisms necessary to implement effective access control policy enforcement.

1 Introduction

To compete in today's fast-paced competitive environment, organizations are increasingly allowing contractors, partners, and guests to access their internal enterprise network. These users may connect to the network through wired ports in conference rooms or offices, wireless access points, or remotely across a WAN connection. In allowing this open access for third parties, LANs become vulnerable. Third parties can introduce data privacy and network availability risks in a variety of ways from connecting with an infected laptop to unauthorized access of network resources to malicious activity. For many organizations, however, the operational complexity and costs to ensure safe third party network access has been prohibitive. Fifty-two percent of surveyed CISOs stated that they currently use a "moat and castle" security approach, and admit that defenses inside the perimeter are weak.[1]

Threats from managed and authorized users are also increasingly a cause for security concerns. Employees with malicious intent can launch denial of service attacks or steal confidential information by snooping the network or browsing network resources. As they access the corporate network, mobile and remote users inadvertently can infect the network with viruses and worms acquired from unprotected public networks. Hackers masquerading as internal users can take advantage of weak internal security to gain access to confidential information. According to a recent CSI/FBI Computer Crime and Security Survey, virus attacks caused the greatest financial losses to enterprises, followed by unauthorized access to internal assets and DOS attacks.[2]

To better deal with rapidly evolving and increasing incidents of LAN threats, organizations are moving towards combining proactive and reactive security measures deployed to protect the network from within the network. Specifically, proactive measures are applied before an endpoint or user is granted access to the network, while reactive measures are used to detect and isolate threats and policy violations. Organizations are looking to NAC as a framework to improve internal security. However, considering the different definitions of NAC, organizations should first identify the key functional requirements for pre-connect and post-connect security prior to making changes to their existing infrastructure or investing in a solution.

2 Understanding NAC

The definition of NAC has evolved significantly as organizations refine their business drivers for these projects and vendors develop functionality to meet these requirements. Most enterprises struggle with controlling and monitoring user access; implementing regulatory compliance requirements; securing guest access; and protecting

[1] March 30, 2005 Preventsys

[2] 2005 CSI/FBI Computer Crime and Security Survey

[3] NAC Vendors Square Off", http://www.networkcomputing.com/showArticle.jhtml?articleID=189602326, July 2006.

network resources from noncompliant endpoints. In fact, a recent CurrentAnalysis survey[3] indicates that the primary business drivers for NAC adoption include (in order of priority):

- 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

In order to address each of the above business drivers, many industry analysts agree that a NAC framework should provide security protections to users, endpoints, and the network beyond simple endpoint posture assessment. According CurrentAnalysis[4], there are five technology functions accepted and expected as part of NAC:

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 - Ongoing threat analysis and containment

Quite simply, controlling network access should be implemented continuously - with both pre-connect and post-connect security controls. Specifically, pre-connect security controls should include:

- Endpoint integrity verification[5]
- Host quarantine and remediation, if necessary
- User Authentication and authorization

Once the user is authenticated and granted access based on authorization criteria, post-connect security controls typically include:

- Access control policy enforcement – tying identity to network resources
- Continuous endpoint integrity verification
- Threat detection and containment
- Continual monitoring and policy violation alerting

Essentially, a successful NAC implementation views the entire user session holistically, including all steps where exposure to data integrity and network availability risks should be mitigated. These steps are described in more detail in the next section.

2.1 Endpoint Integrity Verification

To mitigate malcode risk from entering the network at all, the first step of NAC is the verification of the presence, currency, and enablement of specific security software and OS on endpoints before they are allowed to

[3] NAC Vendors Square Off", http://www.networkcomputing.com/showArticle.jhtml?articleID=189602326, July 2006.

[4] Ibid.

[5] Many terms are used to refer to this NAC pre-connect security control: endpoint compliance checking, host posture assessment, endpoint integrity verification, etc. There has been no industry recognized standard; however, we will refer to this feature as endpoint integrity verification to maintain internal consistency.

join the network. Administrators define the minimum criteria necessary for compliance as it relates to Operating System patch level, Anti-virus software patch level, and Anti-spyware software patch level.

Security administrators also define remediation actions that should occur if an endpoint is found to be non-compliant. Typically, endpoints that do not meet compliance criteria are quarantined and are allowed to connect 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. Many organizations may choose to enforce remediation only for company-owned and/or managed endpoints.

There are several common approaches for verifying the integrity of an endpoint. Agent software may be deployed on all endpoints, network scans against the endpoint can be conducted, or lightweight, dissolvable clients can also be used. Installation and maintenance of agents on each endpoint puts significant strain on IT organizations. This approach also makes it nearly impossible to verify the integrity of unmanaged endpoints. On the other hand, network-based scans are less intrusive, but significantly less accurate due to personal firewalls and less efficient due to the nature of network scan protocols and technologies. The most desirable approach is one that balances user transparency with accuracy such as a dissolvable agent. This avoids administrative headaches associated with resident agents, as well as the false positives and sluggishness associated with network scans. In addition, a clientless approach allows organizations to easily validate the integrity of endpoints that belong to third parties desiring network access, before, during, and after access is granted.

2.2 User Authentication and Authorization

NAC 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. NAC should interoperate with existing directory services and authentication servers. When a user attempts to gain access to the LAN, NAC should challenge the user for appropriate credentials. Typically, a user-ID and password are used for user authentication.

2.3 Role-based Access Control Policy Enforcement

NAC 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 can provide information about a user's access rights and permissions based on role and group memberships which will provide the basis for the access control policy decision.

2.4 Threat detection and containment

Since endpoint integrity verification involves checking for the presence and currency of security software rather than the presence of malicious code, threat detection and containment after an endpoint is admitted to the network becomes critical to ensure network availability and data integrity.

2.5 Continual monitoring and policy violation alerting

Just as policy enforcement should be continuous, real-time monitoring of user access activity is essential to detect inappropriate activity by authorized users. Policy violation alerting and compliance reporting are necessary components of the access control framework to validate that security controls are working as intended. This information should also be used to provide feedback to the internal audit team to determine appropriate policy exceptions and updates to existing policy requirements.

3 Limitations of Pre-Connect NAC Alone

NAC point products that solely perform pre-connect endpoint integrity verification are not designed to be complete LAN security solutions. Pre-connect NAC products simply assure that current patch levels of the OS, Anti-virus software and Anti-spyware software are installed, but with today's current threat landscape, protection after a user is connected to the network is the most critical to ensure network availability, data integrity and confidentiality. Similarly, once the user is authenticated, pre-connect only NAC products fail to enforce access control policies or deliver visibility into a user's activity. Additionally, pre-connect only NAC products do not:

- Scan endpoint disks to check for threats such as BOTS, rootkits, and backdoors
- Provide separation of quarantined endpoints to prevent cross-contamination
- Detect and stop malicious user activity
- Allow visibility into each user's activities
- Detect and stop network-borne threats such as worms from propagating
- Detect and stop denial of service attacks
- Eliminate the zero day threat problem

Although pre-connect NAC plays an important role in LAN security, additional proactive and reactive security measures are required to complete the security process flow necessary to safeguard networks. The table below summarizes recent exploits that easily bypass the limited protection offered by pre-connect only NAC products. In each case, the multi-layered protection delivered by Nevis would have immediately contained and mitigated these risks.

Malware Type: Name	Business Impact	Detection Type Required	Nevis Feature
Virus: BlackWorm/Nyxem	300K+ systems infected	Anomaly Detection	☑
Rootkit: VirTool (DRM)	Exploited by websites and Trojans	Signature matching	☑
Spyware: CoolWebSearch	½ of all PCs infected	Signature matching	☑
Trojan: Exploit WMF	70+ variants, AV vendors slow to respond	Signature matching	☑
Worm: Zotob	$97K / outbreak; 13% companies worldwide	Combination of: Anomaly Detection & Signature Matching	☑

Top Malware Exploits within last 12 months

4 Deployment Considerations

NAC implementations vary according to where the policy and enforcement points are inserted into the network. Typically the choice is to deploy either an inline or an out-of-band architecture and the main differentiating factors between these approaches include:

- Where in the network the solutions are deployed
- The degree to which they are self-contained (don't rely on other network devices for enforcement)

- The granularity of user-awareness (with respect to access control policy enforcement, monitoring and accountability)
- The accuracy of threat detection and speed of containment once detected

4.1 Inline vs. Out-of-band

Inline NAC appliances are deployed between the wiring closet switch and the network core; they are distributed throughout a network, close to users. These devices function as both a policy decision point and an enforcement device (this is what is referred to above as "self-contained").

- Inline Appliances
  - Pros:
    - Integration of identity-based user access control policy decision and enforcement
    - Traffic visibility allows for detailed user activity monitoring (tying all traffic to specific users rather than just IP address)
    - In-depth packet inspection permits threat detection, prevention and control
    - Operating close to the user allows for rapid containment and remediation
    - Deployment requires no re-architecture of existing VLANs
  - Cons:
    - Requires more processing power to keep pace with LAN speeds.
    - Requires high availability (e.g. fail open/fail safe)

Out-of-band appliances are typically centrally located in a data center and connect to a switch in the core. Because they are not directly in the flow of traffic, they act ONLY as a policy decision point – policy enforcement is delegated to other infrastructure devices (usually the wiring closet switch in the distribution layer). According to a Forrester NAC report by analyst Robert Whiteley[6], "these solutions often provide several access control mechanisms, but typically sacrifice granularity because they are not in the network fabric." As a result, out-of-band appliances are typically more appropriate for a monitor-only use case.

- Out-of-Band Appliances:
  - Pros:
    - Perceived to be a less intrusive deployment (no bump in the wire)
    - Requires less processing power since policy enforcement is handed off from the appliance to switch equipment
  - Cons:
    - 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 headache: requires VLAN re-architecture

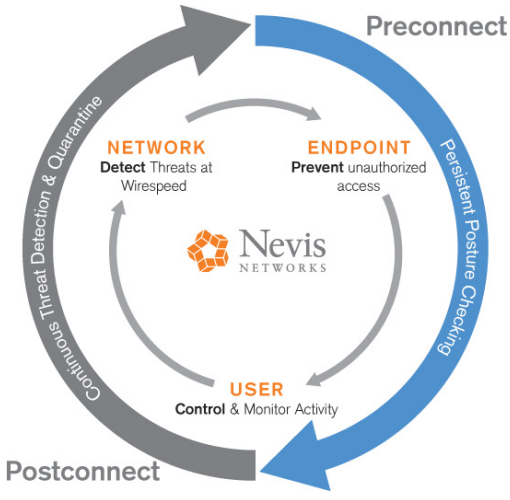
[6] Forrester Report, "Getting The NAC Of It: 2006 Network Access Control Adoption," May 12, 2006

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

5 Nevis' Persistent LAN Security

With the vision to embed security into the fabric of the LAN infrastructure, Nevis LANenforcer delivers continuous LAN security for:

- Endpoints – preventing unauthorized access by noncompliant systems
- Users – controlling and monitoring access to network resources
- Network – detecting, preventing, and controlling threats at the source



In these ways, the LANenforcer LAN security solution delivers complete NAC functionality to include persistent threat protection and access control policy enforcement - before, during and after network access is granted. Nevis' LANsight security policy and event management system enables real-time visibility into user and network activity for regulatory compliance and incident response. Nevis' high-performance ASIC-based LANsecure architecture means that application performance is not sacrificed for deep security protection.

Nevis offers complete and continuous NAC to organizations in the following specific ways.

Endpoint Integrity Verification and Remediation

Nevis uses a clientless approach to confirm endpoint integrity. Granular policies can be applied to remediate non-compliant endpoints. Consistent with implementation best practices, Nevis can be configured to perform periodic integrity verification and remediation after the endpoint has joined the LAN.

- Clientless scan and remediation steps
  When an endpoint attempts to connect to the network, a dissolvable integrity agent is automatically downloaded. This lightweight agent scans the endpoint for required OS security patches; Anti-virus software engine, configuration, and signature file levels; as well as Anti-spyware software policy compliance. It then communicates the values of these parameters to the LANsight policy management system. The LANsight uses these values to determine, based upon predefined policies, whether to grant access to the endpoint or to quarantine it, this decision is then pushed to the LANenforcer security appliance for enforcement.

  After the endpoint passes the integrity check, the user is authenticated. If the authentication fails, the user is denied access. If the user is authenticated, but the end point is not in compliance with corporate policies, the quarantine policy is applied allowing access to the appropriate remediation servers – configurable by the organization. If the user is authenticated and the end point is compliant, network access is granted according to the user's authorization credentials.

- Ongoing endpoint integrity verification
  After initial verification occurs, endpoints may become non-compliant due to a variety of reasons, such as release of a new version of Anti-virus software with critical patches or users disabling Anti-spyware software on their endpoint. The LANenforcer can be configured to scan endpoints that have been admitted, on an ongoing basis. This capability ensures timely discovery and remediation of endpoints that become noncompliant after they have been admitted network access, providing additional LAN security protection and ensuring compliance with computing standards.

User Authentication and Authorization

Nevis provides one of the most effective and granular authentication architectures in the industry, including a variety of options to authenticate users and the ability to work with existing directories and authentication systems.

- LDAP integration
  Nevis' LANsight security manager integrates with existing authentication, authorization, and accounting (AAA) and directory infrastructures to identify users and retrieve information about their existing group memberships and credentials.

- Captive Portal support
  When a user attempts to connect to the network from a compliant endpoint, LANenforcer interoperates with the existing authentication infrastructure by automatically providing an authentication challenge. Based on the response received from the legacy system, access is granted, restricted or denied. In

addition, LANenforcer can fetch user role and privilege information from many AAA servers such as Microsoft's Active Directory.

- Standalone operation
  LANsight offers the flexibility for the administrator to create a local user identification database, rather than import this information from the existing AAA infrastructure. A unique user-ID and password is assigned to each user. Users can be associated with multiple roles and groups, with network access policies defined for each.

- 802.1x support
  Nevis supports 802.1x user authentication. When a LANenforcer is enrolled with a LANsight, all 802.1x authentication requests are directed to LANsight, which maintains the central configuration for accessing RADIUS authentication servers.

- MAC address authentication
  Nevis enables authentication of unintelligent network devices, such as printers and copiers, via MAC address.

Identity-based Access Control

Once authenticated by NAC, users are only allowed access to specific resources, servers, or subnets within the LAN, depending on their specific identities. The administrator can specify highly granular user access policies based on pre-built policy templates. Access policies associated with each user's identity or multiple identities, are enforced, independently of where users connect to the network.

Microsecond Threat Detection and Containment

With today's sophisticated and multi-layered attack patterns and methodology, a multi-tiered approach to threat containment provides the most complete protection. For example, signature matching is only able to detect known threats, making it necessary to use anomaly detection to catch unknown threats for which signatures do not yet exist. Nevis integrates multiple well-known threat detection methods and deploys them in parallel to provide the most complete security protection.

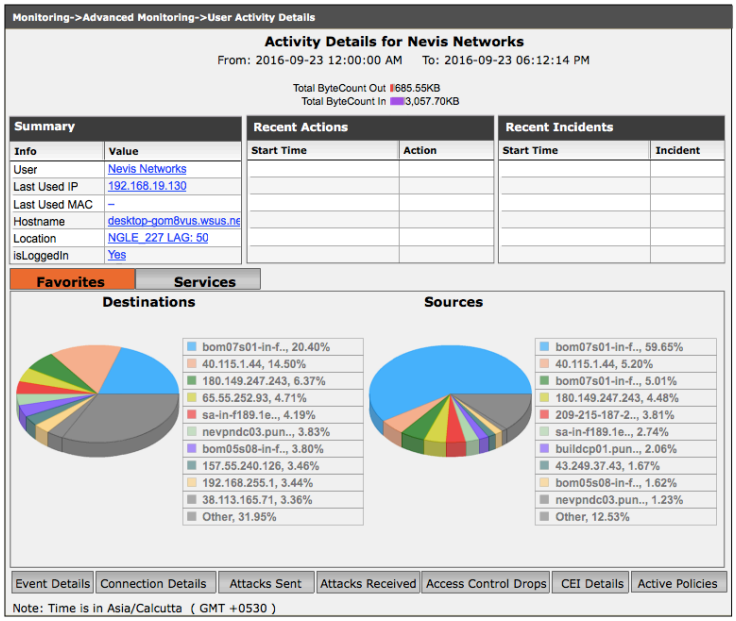
These are:

- Stateful Firewall
- LAN-optimized IP including:
  - Signature Detection
  - Protocol Anomaly Detection
  - Traffic Anomaly Detection
  - Behavioral Anomaly Detection
- Layer 2 – Layer 7 Security

LAN availability is critical in order to ensure user productivity in accessing and managing mission-critical assets. Providing a threat detection layer of protection after a user gains access provides complete and continuous protection against those malware exploits that bypass endpoint security controls. As soon as the LANenforcer detects malicious activity, a user or an endpoint can be restricted and reported, effectively isolating the threat at the source before it has the opportunity to spread. Nevis uniquely performs this deep level of

inspection and threat containment at wirespeed, ensuring that end-to-end application response time is not affected, even when full security inspection is enabled.

Centralized Management and Reporting



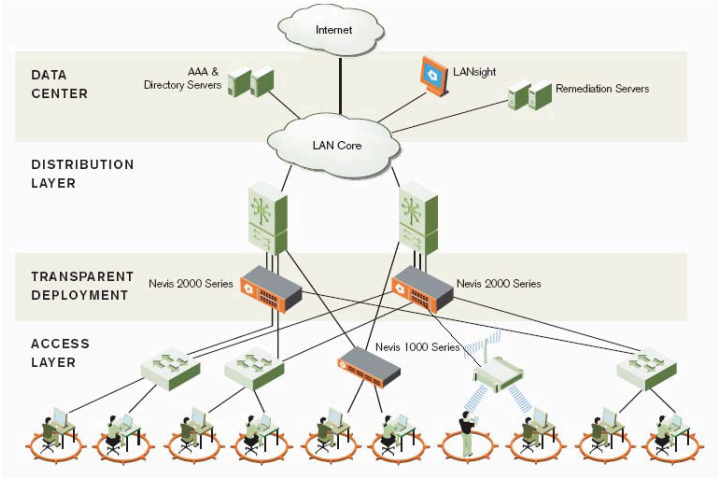
Nevis LANsight security management system centralizes and streamlines security policy management, reporting, and incident response. For example, with the click of a mouse, administrators can examine suspicious users' activity history plus their ongoing activities in real time. After quickly determining which assets the suspicious user accessed, administrators can investigate the full context of the incident – from both a real-time as well as historical view and quickly identify root cause.

LANsight also provides a single log repository that stores records of every endpoint connection and user activity. The ability to generate configuration reports, client integrity check reports, and traffic reports gives administrators a flexible and effective strategy for analyzing security events and user activities. These reporting facilities make it easy for organizations to demonstrate due diligence to auditors with respect to regulatory requirements..

LANSight's powerful patent-pending event correlation engine performs multivariate event correlation across security policy, user, device, user activities, application, LANenforcer appliances and threat detection. This allows administrators to rapidly respond to ongoing threats by quickly identifying the root cause of security incidents.

Comprehensive LAN Security at Wirespeed

Today's enterprise LANs commonly operate with gigabit and multi-gigabit links between the wiring closet and aggregation switches. To fully secure a LAN, any security device residing within the LAN must be capable of enforcing security polices at multi-gigabit speed and with virtually no latency.



The LANsecure architecture embedded in Nevis' LANenforcer products addresses this need with its patent-pending ASIC technology that – for the first time – enables affordable access control and threat defense at up to 10 Gbps with full security processing enabled.

6 Conclusion

Both pre-connect and post-connect security controls are necessary to meet today's security and compliance requirements. In addition to mitigating malware risks, enterprises need to implement identity-based network access control to prevent the threat of unauthorized access to mission-critical data. Centralized security policy configuration, management and reporting provide real-time and historical visibility needed for fast problem resolution and tracks user activity. By combining both pre-connect endpoint integrity verification and user authentication with proactive threat detection and containment, Nevis is the first and only comprehensive LAN security solution that delivers full security protection and visibility for users, endpoints, and the network.

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