Effective Access Control in the LAN: A Tool to Mitigate Insider Risk

A LAN Security Best Practices Whitepaper

Nevis Networks

Persistent LAN Security Solutions

Executive Summary

Information technology teams are facing increasing pressures to secure key company assets for a number of reasons – increased regulatory demands, higher prevalence of insider abuse, and exposures to data confidentiality and integrity by trusted users. Today, insider abuse incidents are on the rise, with unauthorized access to data considered one of the highest risks that enterprises face today.

Effective access control, based on user identity and access profiles, is the essential ingredient for mitigating these internal risks. Integrating user identity with network resource access is a proactive approach to reduce internal risks to data confidentiality, integrity and availability.

1 The Need for Controlled Access within the LAN

Despite increased user awareness and more security-savvy IT departments, attacks from insiders represent over 80% of security breaches today[1]. Solving this problem is challenging, considering that "trusted" users such as employees, contractors and partners are accessing critical resources from within – bypassing gateway security controls such as perimeter-based firewalls and IDS devices. Another contributing risk factor is the access granted to third parties from public areas within the enterprise such as lobbies, conference rooms, and even parking lots.

Typically, inside attackers are motivated by pursuit of profit, competitive advantage or vengeance from perceived job injustices or frustrations. As a result, these attacks are targeted against critical information assets – stealing data from a customer database, planting a "time bomb" on a mission-critical server, or installing backdoors within the infrastructure for access after termination. According to Gartner[2], the financial impact to an individual business of a single successful targeted attack will be 50 to 100 times greater than the impact of a successful worm or virus event.

Regulatory standards mandate stringent access control to enforce segregation of duties within a framework supporting the principle of least privilege. Additionally, privileged user monitoring and policy violation reporting are also important facets of a security compliance program, to demonstrate due diligence to auditors.

2 Access Control Implementation Best Practices

While existing business process should be evaluated in the context of the access control policy framework, a number of generic implementation best practices is recommended. These steps are summarized below:

1) *Authentication prior to network access*
   Whether users are local, mobile, or remote, authentication should be the first step in granting access to network resources. Additionally, requests for wired as well as wireless connections should also be prompted for authentication. Authentication mechanisms may include: 802.1x, RADIUS, TACACS, LDAP, MAC or captive portal. Key areas for authentication enforcement should include high-risk, open and public areas such as conference rooms and lobbies where unauthorized access may be easier to attempt.

---

1 CSI/FBI Security Survey, 2006

2 Gartner Report "Prevent Targeted Attacks"', 15 August 2005

2) *Link roles to network access*

Role-based access control, or RBAC, is one of the core security tenets. However, basing access controls on roles rather than identity is a far more coarse access control approach than controlling based on unique identity. For example, more than one user may share a role. With respect to network access, establishing a "guest" role that is associated with Internet-only privileges ensures that core network resources are protected from the snooping eyes of visitors and unauthorized users. Guest access can still be tracked by individual identity (based on characteristics such as MAC or IP address); however, having a single "guest" role simplifies administration by not requiring user authentication - while still enforcing policy.

3) *Link identity to network resource access*

As opposed to roles, identities are uniquely assigned on a per-individual basis. These unique identities are comprised of a combined set of identifying characteristics which may include: username, device name, IP or MAC address, or physical location. Additionally, each identity will be associated with a unique authorization profile – including group as well as user attributes typically managed within the directory services infrastructure (e.g. AAA server such as Active Directory).

These permissions should be limited based on the principle of least privilege – allowing access to only those network resources that are required for their responsibility matrix. For example, contractor identities should have significantly restricted access based on the duration of their contract, hours worked, as well as the specific applications, servers, and network resources that are required for their assigned projects. As demonstrated in Figure 1 – Joe's access is specifically tailored to those assets tied to his specific responsibilities as an employee within the Finance Department; whereas Sue in Technical Support is tailored to customer data and infrastructure - shared resources remain available to both.

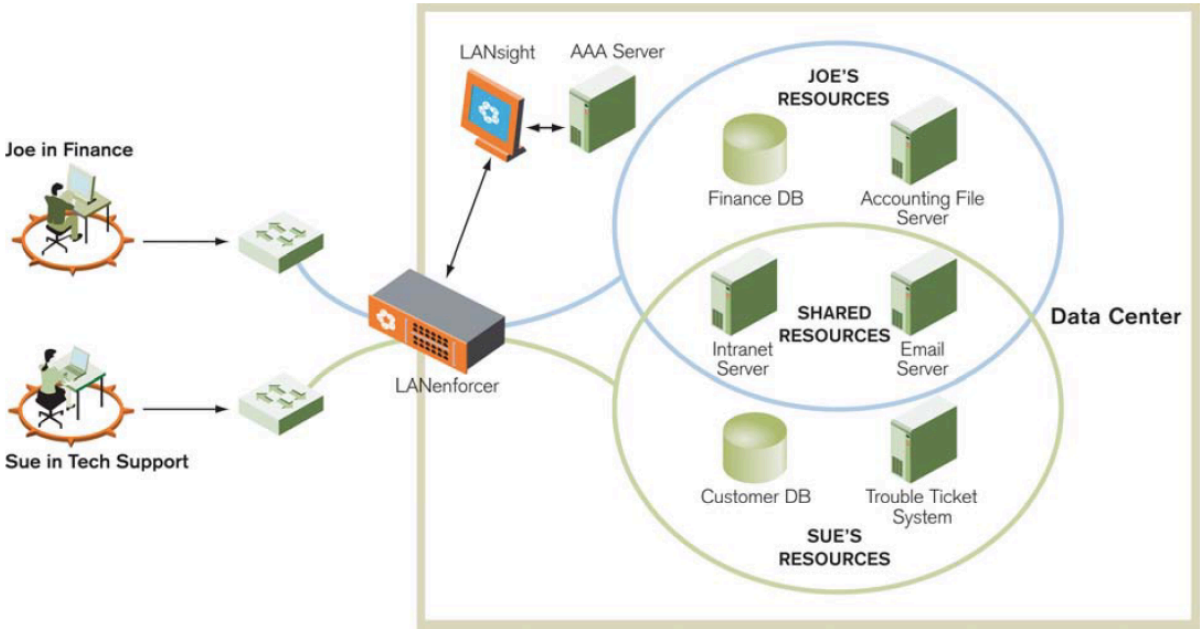

Figure 1 – Differentiated user access

4) *Post-connect access control policy enforcement*

Once the appropriate level of network access is granted based on the authorization profile, access control policies should be continually enforced. For example, network resources which are outside the scope of

certain users (e.g. contractors, guests) should remain invisible. Guests, contractors, and even employees should not have the ability to access file shares and other resources that remain outside of their job responsibilities. Preventing network browsing by unauthorized users is a proactive way to establish effective access control. Specifically, enforcing access control policy at the network level is a centralized and effective way of implementing this type of security control.

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 Drawbacks of Perimeter Defense Methodology

Some enterprises may consider deploying legacy, perimeter-based defense architectures within the LAN. This approach is flawed for a number of reasons. First of all, perimeter defense technologies such as gateway and DMZ firewalls and IDS/IPS systems are purpose-built to protect public networks against Internet-borne threats. The nature of the LAN environment puts this type of technology at significant disadvantage for a number of reasons outlined below.

- *Coarse, rather than granular access policies*
Most perimeter firewalls are designed to allow or deny traffic based on source and destination IP addresses, source and destination ports and protocols but typically lack application and user awareness. As a result, they would not be able to enforce policies based on user identity or restrict access at the application level. This also impacts their ability to offer detailed monitoring, reporting and alerting on malicious and inappropriate user activity.

- *Inbound vs. outbound paradigm is inappropriate*
Perimeter firewalls typically design their rule-base and access control list architecture within an inbound vs. outbound framework. This approach makes no sense in the LAN, where access patterns are omni-directional within a mesh infrastructure rather than a gateway context.

- *Performance limitations*
In order to keep pace with the speed of the LAN, security appliances need to perform at multi-Gbps in order to avoid latency on mission-critical services. Typically, gateway firewalls and IDS are designed to accommodate slower traffic (in the 1-2 Mbps range), based on their insertion point within the enterprise. This level of performance is simply untenable based on scalability and growth requirements for today's LAN infrastructure.

4 Summary

Insider threats such as unauthorized access to data and exposures to confidential data and intellectual property cost enterprises billions of dollars per year in liability, compliance fines, revenue loss and consumer confidence crises. These threats are becoming more targeted and more challenging, primarily based on the fact that they are

being engineered by authorized and trusted users such as employees, contractors, partners and sometimes even customers. The best approach to mitigating this risk is to deploy a LAN-optimized infrastructure designed to fortify your access control policy enforcement strategy to:

- Prevent access to unauthorized users
- Control and monitor activity by authorized users
- Detect inappropriate access by authorized users

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