Securing Your VLAN Architecture

A LAN Security Best Practices Whitepaper

Nevis Networks

Persistent LAN Security Solutions

Executive Summary

Most security professionals agree that the perimeter disappeared years ago with the advent of remote computing, a growing mobile user community, and ubiquitous wireless network access points. As a result, efficient and reliable protection of critical LAN resources has become the most critical challenge for network security teams worldwide. Sophisticated insider attacks and blended threats demand that security controls be intelligent enough to detect, contain and prevent these threats, but remain flexible enough for effective control.

For many years, network administrators have turned to VLAN architectures to segment their user community into multiple security zones, leveraging their investment in switch technology. While not originally designed for security, VLANs can offer a level of logical data segregation without impacting user connectivity. Unfortunately, entirely depending upon VLAN architectures as a single aspect of a robust LAN security program is simply not viable considering today's cyber risk landscape. This technical brief will outline the strengths and weaknesses of VLAN deployments as well as introduce strategies for augmenting your VLAN security program.

1 Operational Benefits of VLAN Architectures

Implementing VLANs within a LAN infrastructure can simplify maintenance for the network administrator and improve performance for the user community. Additionally, initial VLAN setup and configuration is very straightforward – resulting in little to no impact to the end-user community. By allowing administrators to create multiple broadcast domains on a single switch, VLANs enable enterprises to make the most of their switching investment.

Specifically, VLANs provide multiple operational benefits:

- Logical separation of data to minimize impact of one user group on another;
- Logical separation of data to minimize impact of one application on another;
- Logical separation of data based on geography, department or line of business to support business process efficiency;
- Efficient use of non-contiguous IP addressing space.

2 The Myth of "VLAN Security"

This briefing is not designed to illustrate details associated with VLAN attacks. For detailed information on these attacks, please see @stake's Research Report on the Secure Use of VLANs at http://www.cisco.com/warp/public/cc/pd/si/casi/ca6000/tech/stake_wp.pdf or Steve A. Rouiller's SANS GIAC Practical Assignment at http://www.sans.org/reading_room/whitepapers/networkdevs/1090.php.

While VLAN's flexible creation of broadcast domains adds operational value, the security features of VLANs are simply not sophisticated enough to combat today's LAN-based threats. Effective proactive LAN security approaches now require that security controls be implemented as close to the user as possible – but remain transparent to users to ensure productivity. Even with the implementation of Private VLANs (PVLANs) to restrict host-to-host communication, application-based security exploits still pose risks to an infrastructure.

In fact, there are a number of well-documented attacks1 designed to bypass VLAN and PVLAN security including:

- VLAN hopping attacks
- 802.1q and ISL tagging attacks
- ARP poisoning attacks
- Layer 2 proxy attacks
- Spanning Tree Protocol (STP) attacks
- VLAN Trunking Protocol (VTP) attacks
- Cisco Discovery Protocol (CDP) attacks
- DoS or Impersonation attacks exploiting VMPS/VQP vulnerabilities

By not offering secure connectivity between users and business applications, VLANs and PVLANs are restricted by a number of limitations in combating these threats. These limitations include:

- **Lack of user identity awareness**
  VLANs are simply not designed to track user activity so VLAN administrators lack visibility into user activity patterns. Granular policy enforcement – down to the specific user and associated network resources – is not possible within the VLAN security architecture.
- **Limited host isolation**
  Hosts connected to isolated ports can easily bypass the port restrictions by initiating sessions via the router's interface in their subnet. They can also communicate with all devices connected via other subnets. Thus, even though PVLANs may help with data separation at a granular level, they are unable to effectively contain host-to-host attacks and malware infection.
- **Lack of threat protection**
  Without inspection of every packet that enters the VLAN the network is susceptible to a myriad of security risks. Some of these include:
  - Worms and viruses that can spread through the network, easily bypassing the security controls enforced by PVLANs and VLAN Access Control Lists (VACLs).
  - Malicious users that can perform reconnaissance sniff the network for sensitive information and launch DOS attacks.
  - BOTs that can roam freely along open paths.
- **Difficult and time-consuming to manage**
  Using PVLANs and VACLs for access control policy enforcement carries significant administrative overhead. Each user access policy must be mapped into a VLAN scheme with numerous VACLs per VLAN. The number of required VACLs can rapidly balloon into an unmanageable size – impacting administrative productivity, increasing chance of error and introducing considerable network latency. Initial VLAN administration can be relatively straightforward, but making changes to production configurations is anything but. In production environments, VLAN configurations are intended to be generally static so when changes are required, the process is complicated and slow to implement.

3 Integrating Security into Your VLAN Environment

Nevis Networks has designed ASIC-based LAN security systems that fully protect network assets from security threats by enforcing user identity-based access policies and providing persistent threat detection and protection. Developed for integration into existing topologies, Nevis LANenforcer products require no changes to your current VLAN or AAA configurations.

Nevis’ LANenforcer solutions augment VLAN network segmentation by providing user-level segregation for comprehensive and granular access control. Each user is placed in a Personal DMZ that protects them from threats on the network, and protects the network from the users. This level of control, which is unmatched in the industry, ensures that each user gets their own individual and appropriate view of the network and its resources and applications. It eliminates any threats the user might introduce inadvertently or maliciously onto the network -- before the threat can propagate to any other user or do harm to the network.

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. No client software is required, which makes deployment easy, eliminates the need for desktop software maintenance, and significantly lowers acquisition and operating costs.

By integrating LANenforcer™ within the network infrastructure, the following is enabled:

- Comprehensive user identity control, awareness, reporting
- Fastest and broadest threat detection and containment
- Simplified, centralized network security administration

Security Control	VLANs	Nevis LANenforcer
Host Integrity Checking	No	Yes
Role Based Access Control (per user/per port)	No	Yes
Comprehensive Threat Detection (per packet)	No	Yes
Microsecond Quarantine and/or blocking	No	Yes
Real-time User Activity Monitoring & Alerts	No	Yes
Third party access restriction	Manual	Dynamic

4 Summary

No one security approach can fully mitigate all risks to your LAN user community. While VLANs can provide one layer of segmentation within the infrastructure, their lack of user identity awareness makes this an unsuitable strategy on its own. Adding an additional layer of protection at the host and user level will ensure that key LAN resources are protected. This control layer should also be capable of deep packet-level inspection to ensure that threats are detected and dynamically contained. Finally, consider the IT administrative efficiencies gained – initially and over time - associated with fortifying the VLAN architecture and enhancing the LAN security program.

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