Comprehensive LAN Security for the Banking Financial Services and Insurance Industries

Nevis Networks

Persistent LAN Security Solutions

Overview of the Banking Financial Services and Insurance (BFSI) Industry

Financial segment covers a continuum of institutions including banking, insurance, securities, reporting and so on. The challenges associated with these institutions are unique and possess increased economical risk at every step of internal and external transactions. Specific challenges that showed presence of internal origins viz. a malicious user with intent of tampering with the finances or a new worm entering the organization's network through infected USB drive, can pose grave problems for the entire network including ATMs, in addition to potential cyber attacks. Therefore this segment of industry faces distinctive challenges like threat-limited network availability, data access control and security, acquiescence with industry standards, regulations for infrastructure and security, and 24×7 network connectivity linked with external public or private networks. To address these challenges and prevent a possible blemish to company's brand image, it is imperative to adopt persistent LAN security through advanced Network Access Control Technology.

Typical Infrastructure

- Large number of concurrent users ranging from few thousands to hundreds of thousands
- Connections across distant areas: Users connect from various branches over WAN links crossing national and international boundaries.
- Number of branches varies from 10 to thousands depending upon the organization scale.
- Network speed varies depending upon the infrastructure.
- Authentication mechanisms like AD or LDAP which is distributed geographically.
- Patch management servers like WSUS, SCCM, LANDesk and so on.
- User machines typically use Windows operating system with all its flavors, with a few Mac and Ubuntu laptops
- Users largely do not have administrative rights to their host machines.
- Critical servers are located at the Headquarters or at a Central Branch.
- HA infrastructure is present in the core network.

Key Challenges

- Network control by limiting the access only for the organizational assets.
- Control on access by unknown machines with reporting in real-time.
- User compliance as per organizational policies: Viz. Operating System patch versions, Antivirus DAT file versions, Registry values, and so on.
- Isolation of non-compliant endpoints by quarantining.
- Auto-remediation to remediate the endpoint without user or administrator intervention.
- Monitoring for detection of malicious behavior (worms, viruses and zero-day threats) within the traffic reaching critical resources like Data Centre Servers.
- Subsequent blocking and notification of detected threat in real-time.
- Centralized viewing and monitoring of the entire network from a single monitoring console.

Nevis Solutions for the Pain Points

- Transparent User Authentication
    - Network access restricted only to successfully authenticated users.
    - Organization's owned asset verification is performed and only verified machines are allowed access MAC address verification against a pre-configured list before providing network access. This ensures that personal laptops do not get access to critical business servers located at the

headquarters.

- End-point Compliance
  - Restrict network access for machines compliant with organizational policies.
  - Quarantine and auto-remediation actions for non-compliant machines before providing the network access.
  - Ensures complete automation of this process without any human intervention.
- Group Membership Based Endpoint Compliance
  - Provides compliance checks based on user role with executive exemption for granular control
- Smart Policy Control Mechanisms
  - Configurable policies like pre-login, post-login, threat-quarantine and cei-quarantine used to restrict user access based on end point compliance and behavior
- Identity Based Policy Enforcement ensures users "see" only those network resources they are supposed to access. Attempts to check the existence of prohibited network resources get dropped and notified to the administrator.
- IPS ensures quick identification of infected machines and provides their automatic blocking.
- Traffic Anomaly (TA) ensures zero-day threats prevention action.
- N:M redundancy offering High Availability (HA) within the network.
- Centralized monitoring, reporting and configuration using Appliance Management Server ensure that the network administrator has full control and visibility of every machine inside the network.
  - A list of all non-compliant machines available in real-time
  - Central control for enabling required patch levels
  - Notifications with an ease to drill down to the end machine, user and IP address, to root cause and clean up the end-host.

Benefits & Outcome of the Solutions for Critical IT Needs

Nevis™ network security solutions equip the BFSI networks for the access control, transparency, visibility and the defense against malicious attacks which are the basic requirements of modern enterprise networks. It provides comprehensive network security, policy enforcement, and threat control management solutions. It also provides flexible deployment methods with scalable solutions. The NAC solutions offered by Nevis enable a bank, a financial service provider or an insurance organization to automatically enforce its security policies at the distant endpoint through a network of few thousands to millions of users and ATM machines across all national, international or geographically distant locations.

Effectively, every network session is logged for forensic analysis and every packet is deep inspected for potential threats. In case of any malicious attack, the rogue system is isolated and quarantined, besides generating an instant alarm. The whole solution integrates with other security components available at the institution namely Patch Management, Anti-virus management, Security Information and Event Management.

ROI from Nevis Security Technology

- Critical customer information safeguarded through enhanced security posture
- Better network availability and reliability - Attacks cannot bring down the network easily.
- Improved network performance

- Reduced support calls - Faster online transactions due to better hygiene of network
- Automation of several manual tasks
- Higher customer satisfaction
- Brand name and integrity assured

Deployment of Nevis Solution

The Nevis solution is an in-line solution comprising of a Nevis LANenforcer appliance (LE) and a LANsight management server (LS).

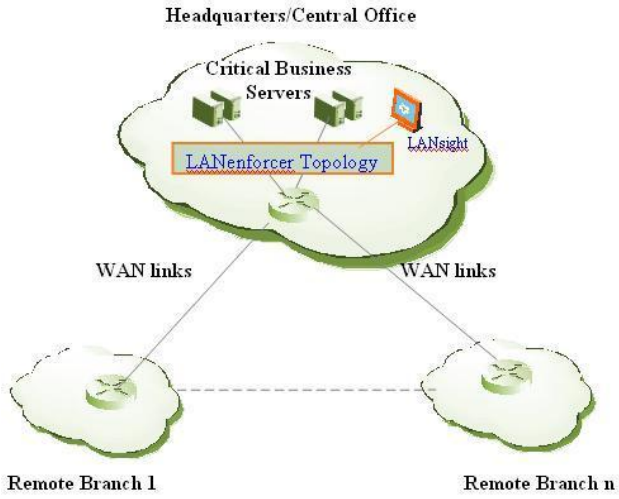
The LANenforcer Appliance is available in switch and appliance flavors:

- Transparent Appliance N2000/N3000 series – A bump-in-the-wire device
- Secure Access Switch N1000 series – Similar to a standard access switch

For the purpose of the BFSI segment where the critical servers are located at the headquarters and need to be protected from non-compliant end-users and machines, the N2000 series appliance is recommended. The Nevis LEs are deployed near the core switches before the data center such that all the traffic from end user machines necessarily passes through these devices. Effectively LE forms the choke point for all traffic before reaching the critical business servers (data center) of the organization.

The solution can be deployed in an N:M redundancy model depending on the requirement, where N is the number of active LEs and M is the number of standby LEs at any given point in time. This ensures complete High Availability of the network. If any of the active LE loses connectivity, the traffic and user sessions of this LE are switched to a secondary LE in the M pool. Active sessions are not broken in this process, ensuring that the end user does not see any impact of the connectivity failure.

The Nevis Subnet Load Balancer device can be deployed to balance the load between active LEs based on the subnets being used.



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