Network Access Control (NAC)

End-to-end security and superior user experience

Product Overview

tbNAC is a complete standards-based, multi-vendor interoperable pre-connect and post-connect Network Access Control solution for wired and wireless LAN and VPN users. Using tbNAC, management configuration and reporting software, IT administrators can deploy a leading-edge NAC solution to ensure only the right users have access to the right information from the right place at the right time. tbNAC is tightly integrated with Intrusion Prevention System and SIEM to deliver best-in-class post-connect access control.

tbNAC advantage is business-oriented visibility and control over individual users and applications in multi-vendor infrastructures. NAC protects existing infrastructure investments since it does not require the deployment of new switching hardware or that agents be installed on all end systems. tbNAC performs multi-user, multi-method authentication, vulnerability assessment and assisted remediation. It offers the flexibility to choose whether or not to re-strict access for guests/contractors to public internet services only-and how to handle authenticated internal users/devices that do not pass the security posture assessment. The NAC assessment warning capability alerts users that they need to upgrade their system but can allow a grace period before they are quarantined.

tbNAC enables the homogeneous configuration of policies across multiple switch and wireless access point vendors. This capability significantly reduces the burden of policy lifecycle management and eases NAC deployment in wired and wireless heterogeneous infrastructures.

With tbNAC's flexibility, organizations have phased deployment options enabling immediate network protection and business value. For example, an organization can start with simple endpoint detection and location directory information, then add authentication and/or assessment and then automate remediation.

Highlights

- Complete solution featuring both physical and virtual appliances
- Range of policy configuration options enables a uniquely fine-grained network control and flexibility
- Comprehensive dashboard reporting and advanced notification engine
- Managed guest access control with sponsorship
- Protect corporate data by proactively preventing unauthorized users, compromised endpoints and other vulnerable systems from network access
- Effectively balance security and availability for users, contractors and guests
- Proactively control the security posture of all devices, including employee owned (BYOD), on the network
- Efficiently address regulatory compliance requirements
- Cost-efficient protection for enterprise remote offices
- Leverage existing assessment servers, authentication servers, software agents and identity sources avoiding forklift upgrades
- Enable business staff to easily sponsor guests and validate guest registration
- Protect physical and virtualized environments with flexible deployment-physical and virtual appliances

Fine – Grained Configuration Options

tbNAC configuration options provide an unparalleled range of choices for fine grained network control. These configuration options include time, location, authentication types, device and OS type and end system and user groups. For example, enterprises can write and enforce policies that grant a precise level of network access based on the type of system connecting, an employee's role in the organization, the location of a user at the time the user is connecting or the time of day. Device and OS type rules are particularly important in environments where users bring their own devices(BYOD). The enterprise can give these devices network access that is different than the access permitted corporate devices.

An enterprise's network is more secure with tighter control over who gains access, when and from what location. The granularity of these configuration options also provides flexibility for efficient deployment in large heterogeneous infrastructure.

Guest Account Services Included

tbNAC includes automated guest registration access control features to assure secure guest networking without burdening IT staff. NAC capabilities automate or delegate guest access management. Features such as expiration and account validity time control the guest account without any IT involvement. tbNAC provides a self registration portal for users to register multiple devices themselves offers advanced sponsorship capabilities such as email sponsorship and a simple portal for sponsors to use to validate guest registration. Location based registration allows guest access to be limited to specific connection points(SSID, port, switch) or group of connection points.

Identity-Aware Networking

In an identity-aware network a user's capabilities are controlled based on the user's identity and the access policies attributed to the user. tbNAC provides user identity functionality including discovery, authentication and role based access controls. Users are managed centrally in the identity system for the network and all connected applications. Users can be automatically added or deleted when they join or leave the organization.

Endpoint Baselining and Monitoring

All end systems in the network infrastructure should be incorporated in the network access control system for control to be most effective. tbNAC provides agent-based or agent-less endpoint assessment capabilities to determine the security posture of connecting devices. tbNAC aligned with industry standards works with multiple assessment servers, authentication servers and security software agents to match the needs of organizations who may have existing assessment technology.

Integrations

tbNAC provides a simple, open, programmable and centrally managed way to implement Software Defined Networking(SDN) for any network.

SECURITY

- Enable the strongest security with fine grained access control based on user, device, time, location and authentication type
- Assess end systems of any type for vulnerabilities or threats with agent-based or agent-less assessment
- Automate end point isolation, quarantine and remediation, plus ongoing threat analysis, prevention and containment

SERVICE & SUPPORT

- Industry-leading first call resolution rates and customer satisfaction rates
- Personalized services, including site surveys, network design, installation and training

Notifications & Reporting

The advanced notification engine in tbNAC provides comprehensive functionality and integrates with the workflows of other alerting tools already in place. Enterprises can leverage and extend their existing automated processes to further reduce operational costs. Notifications occur for end-system additions or state changes, guest registration, any custom field change and end-system health results. It is delivered through traps, syslog, email or web service. For example, integrated with the help desk application, NAC notification can be used to automatically map changes in the infrastructure to actions.

tbNAC Management

The software provides secure, policy-based NAC management. From one centralized location, IT staff can configure and control the NAC solution, simplifying deployment and ongoing administration. It also aggregates network connectivity and vulnerability statistics, audits network access activities and provides detailed reports on vulnerabilities in the network.

Management is simplified with a hierarchical structure that places end systems into administrative zones. It also provides centralized visibility and highly efficient anytime, anywhere control of enterprise wired and wireless network resources. Users of any of the popular mobile devices can use their smart phone or tablet to access NAC end-system view, system location and tracking information and much more, anytime anywhere.

Additional Features

- "Bring your own Device(BYOD)" control features including mobile device registration and session-based user login.
- IPv6 support for NAC implementation in networks with IPv6 end systems.
- Proven interoperability with Microsoft and Trusted Computing Group.
- Automatic endpoint discovery and location tracking by identifying new MAC addresses, new IP addresses, new 802.1X/Web-based authentication sessions or Kerberos or RADIUS request from access switches.
- Support for Layer 2 deployment modes and support for all NAC deployment models: intelligent wired edge, intelligent wireless edge, non-intelligent wired edge, non-intelligent wireless edge and VPN.
- tbNAC provides VPN support and with TechBridge SSA switch in distribution, provides more flexibility through policy.
- Support for external RADIUS Load Balancers allows the external load balancer to evenly distribute the load for servicing authentication requests and configuring switches across a group of NAC appliances.
- Support integration with IT workflows for automated streamlined operations
- Web-service based NAC simplifies integration with third party applications
- 1+1 redundancy for Layer 2 deployment modes: provides high-availability and eliminates as a single point of failure
- Risk level configuration allows flexibility in determining threat presented by the end system. This allows NAC administrator to define High Risk, Medium Risk and Low Risk thresholds based on local security policies and concerns.
- tbNAC is upgradable, allowing assessment to be integrated onto a single box with the other NAC functions. The appliances are capable of supporting both network-based and/or agent-based assessment.

Importance of Network Access Control

Network access control will not work for every organization, and it is not compatible with some existing security controls. But for organizations that have the time and staff to properly implement network access controls, it can provide a much stronger and comprehensive layer of protection around valuable or sensitive assets.

IT departments that use virtual machines as part of their data center can benefit from network access control, but only if they are vigilant about the rest of their security controls. Virtualization poses special challenges for NAC because virtual servers can move around a data center, and a dynamic virtual local area network (LAN) can change as the servers move. Not only can network access control for virtual machines open unintended security holes, it can make it challenging for organizations to adhere to data audit control standards. This is because traditional security methods locate endpoints through their IP addresses. Virtual machines are dynamic, and move from place to place, making them more complicated to secure.

Additionally, virtual machines are also very easy and fast to spin up, meaning that inexperienced IT administrators may launch a virtual machine without all of the proper network access controls in place. Yet another vulnerability occurs when virtual machines are restored from a rest state. If new patches appeared while the server was in the rest state, they may not be applied when the machine is redeployed. An increasing number of organizations are adding application security to their network security controls to ensure that everything on their network, down to the application level, is secure.

FOR MORE INFORMATION

About TechBridge

TechBridge is the World's leading Product & Solutions Company. Data Center Applications, Collaboration and Real Time Communication. DC Management and Monitoring, Disaster Management, Security, Collaboration and Cloud. Its market-leading Network Modernization, Unified Communications, Mobility and Embedded Communications solutions enable customers to quickly capitalize on growing market segments and introduce differentiating products, applications and services. We are an expert and leader in Government Solutions, Smart City Solutions, Data Centers and Large Enterprises. We do custom applications also, as per the customer requirements.

Certificates:-

ISO 9001

ISO 27001

ISO 20000

CMMi L3

Visit our Website: www.tech-bridge.biz

Mail us at: sales@tech-bridge.bizp

Address:- TechBridge Consultancy Services LLP
326, Tower B3, Spaze iTech Park, Sector-49, Sohna Road, Gurgaon-122018, Haryana