



Delivering Persistent Network Access Control

Delivering Persistent Network Access Control

Executive Summary

Network Access Control (NAC), now an essential component for any organization's overall security posture, mitigates the elevated risks associated with the threats found in today's information technology environments. However, many NAC implementations provide only basic one-time access control, with some form of endpoint health check assessment. This is not enough. Network Access Control needs to be dynamic, persistent and ongoing. NAC solutions must provide granular security policies which can be enforced at any time, and which understand the context of the communications between the endpoint and the IT infrastructure.

This white paper proposes an open-architecture, standards-based approach to NAC that can secure a multi-vendor / multi-technology IT infrastructure. This architectural approach identifies which users and endpoints are connected, where they are located, and what their role is in the organization. It monitors ongoing behavior, detects non-compliant systems, and reconfigures the network in response to new threats and vulnerabilities. The net result is assurance that users have access to the IT resources required to work effectively, while business critical systems and processes are continuously protected from both intentional and unintentional compromise.

Network Access Control Deployment Challenges

Organizations face many challenges as they set out to design and deploy a Network Access Control solution that meets today's performance, security and regulatory compliance needs. The implementation must be an integral part of their overall IT security posture, and specifically must address the following concerns:

- Identity management and authentication for both users and end systems
- Initial and ongoing assessment of end-system health
- Automated isolation, quarantine and threat mitigation
- Network usage and service authorization governed by acceptable use policies
- Continuous and persistent threat analysis, prevention and containment
- Comprehensive compliance auditing and reporting

One key issue to consider is the ability of the NAC solution to strictly enforce the authentication of every endpoint without extensive upgrades to already deployed security appliances, switches and access points. Also IT should examine the solution's ability to enforce appropriate "acceptable usage policies" based on the type of end system and the organizational profile of each user. An optimum solution would be deployable in discrete stages to match the organization's business needs, and would minimize network security dependencies and their associated indirect costs.

Let us now explore each of these NAC deployment challenges in more detail and propose some best practice solutions.

Authentication

Support for standards-based authentication and policy enforcement (e.g. standards such as IEEE 802.1X and RFC3580) allows a NAC solution to be deployed in a network environment that includes several different vendors' infrastructure products, without requiring extensive upgrades to existing infrastructure.

In many organizations a full featured 802.1X environment is not a feasible option. In these situations a Network Registration solution may be used to automatically bind device identification (e.g. MAC Address) to user identification (e.g. Username) without IT intervention. Look for best-in-class Network Registration that supports a broad range of configuration options and provides flexibility of implementation. Characteristics of such a solution include:

- Network access credentials may be validated against an existing IT database by capturing User Name and Password authentication information during the device registration process
- Sponsored Registration is supported. An authorized user may sponsor a guest or visitor during the device registration process

-
- The maximum permitted number of devices (MAC addresses) per user may be specified, and, once that threshold is exceeded, additional devices associated with that user will not be granted network access
 - Network Registration may be implemented campus-wide or limited to specific segments of the network
 - A web-based administrative interface allows IT operations to populate the database of authorized username / password combinations, manually add or delete registered MAC addresses, and configure MAC white lists and black lists

Assessment

The impact of supporting a diverse end-system environment must be addressed, along with the challenge of providing integrated security and management regardless of what types of devices are connected to the network.

A best practice approach is to offer both agent-based and network-based NAC health assessment. Agent-based assessment, where a security agent is loaded onto managed end systems, offers a rich set of assessment capabilities. However, many end systems – including IP telephony handsets, security cameras and networked printers – may not support the organization's security agents. For these and similar devices, network-based security assessment provides a more optimal solution.

In the case of guest networking (support for contractors, visitors and other “non-employees”), the requirement may be to provide basic network services such as HTTP, VPN and POP access, while protecting the integrity of other users and business critical systems. This is another case where a network-based approach to end system assessment is critical to delivering a full-featured NAC solution.

Resource Authorization

Provisioning of access to network resources and services should be based on the “context” of the endpoint, i.e., the authenticated identity of the user or device, location, time, and the current / historical security posture of the device. Access to network resources and services should be provisioned based on these criteria, while non-compliant systems are quarantined for remediation or simply logged for future evaluation. The ideal NAC solution supports granular resource access control that includes:

- Resource containment, determining which resources an end user can access
- Protocol containment, determining which protocols the end user can use to access authorized resources
- Bandwidth containment, determining how much bandwidth the end user can use per application and per authorized resource

Real Time Threat Monitoring

A major weakness of many NAC implementations is the assumption that end systems once assessed and granted access remain “clean and healthy” from that point forward. There are many reasons why this is not the case – including proliferation of network borne attacks, malicious code embedded in email messages, or device security profile reconfiguration by the end user. Truly effective NAC solutions support continuous, persistent monitoring of end system behavior. This requires checking device activity against threat databases to detect known attack footprints; and measuring communication flows against baseline behaviors in order to detect Day Zero attacks. Threat information from many elements in the network should be normalized, correlated and prioritized in order to build a comprehensive threat assessment.

Reporting

It is fundamental to capture and report a comprehensive set of intelligence parameters that can be leveraged to quickly determine network usage, and the threats and vulnerabilities posed by end systems of any type. Specifically, threat and attack information should be reported and logged for forensics analysis, and attack session reconstruction should be enabled.

Behavior based information provides visibility into which applications are being used to access corporate resources, how much bandwidth is being used and which resources are being accessed by each end user. This information often proves critical for compliance auditing.

Historical data analysis for every end system provides another key tool for auditing and threat assessment. Key vectors to capture for each end system include:

- MAC Address – *The physical address of the end system*
- Switch IP Address – *The switch in the network where the end system attached*
- Switch Port Index – *The port on the switch where the end system connected*
- Switch Port – *The “name” of the switch port where the end system is connected*
- IP Address – *The last known IP address of the end system*
- Authentication Type – *The method used to authenticate the end system*

-
- State – *The authorization state of the end system*
 - Reason – *The reason for the authorization state of the end system*
 - Username – *The username of any user leveraging the end system*
 - First Seen – *The first recognition of the end system on the network*
 - Last Seen – *The most recent recognition of the end system on the network*
 - Last Scanned – *The last time that the end system was assessed*

By analyzing this data IT administrators can easily account for end-system compliance in real time as well as historically. IT Operations and Security teams are empowered to report on end-system compliance, justify technology expenditures and provide regulatory compliance information when required.

NAC Standards Activities

The networking industry is developing a number of important standards and frameworks that support vendor interoperability and open Network Access Control. For example, Microsoft® is working with many of the industry players to ensure seamless interoperability with its Network Access Protection (MNAP) solution. Microsoft Network Access Protection leverages 802.1X as a network authentication method, and relies on other standards-based technologies. In addition, the Trusted Computing Group / Trusted Network Connect (TCG/TNC) initiative focuses on the interoperability and integration of NAC-related technologies. The open TNC architecture enables end user organizations select the best assessment technologies available, with the assurance of system-wide integration of authentication, authorization and enforcement of security and communication policies.

When selecting a NAC vendor insist on compliance with these and other standards. This will enable the organization to scale a NAC deployment without the added hidden cost of infrastructure replacement.

Enterasys Network Access Control

Enterasys offers an open-architecture, standards-based approach to Network Access Control, and delivers a NAC solution that supports both initial and ongoing assessment for all end systems. And Enterasys NAC is designed for staged deployment to provide the right level of functionality for each phase of your NAC rollout.

Enterasys NAC supports both network-based and agent-based health state assessment; authorizes network usage based on a broad range of context, security and business enablement policies; assists the secure remediation of non-compliant endpoints; and eases the burden of regulatory compliance.

Enterasys NAC enables an organization to select best-of-breed assessment technologies from industry-leading vendors, and fully integrates with policy-enforcement capabilities of Enterasys' Secure Networks™.

Return on investment is a key consideration for every CIO. Enterasys NAC leverages innovative multi-method and multi-user authentication, plus policy and VLAN-based enforcement (RFC3580) to implement a comprehensive NAC solution using your existing network equipment. No forklift upgrades or burdensome agent deployments are required. Enterasys delivers the most cost-effective, comprehensive NAC deployment available today.

The table below summarizes the key attributes of the Enterasys Network Access Control solution.

Enterasys NAC Attributes			
Open Architecture	<ul style="list-style-type: none"> • IEEE • IETF • Microsoft NAP • TCG/TNC 	<ul style="list-style-type: none"> • Multi-User Authentication • Distribution-Layer Policy • Software APIs • 3rd Party Assessment 	<ul style="list-style-type: none"> • Matrix & SecureStack Switches • NetSight Management Software • Enterasys NAC Gateway • NetSight NAC Manager
End System Inclusion	<ul style="list-style-type: none"> • IEEE 802.1X • MAC-based Authentication • Web-based Authentication • CEP Detection 	<ul style="list-style-type: none"> • Agent-based Assessment • Agent-less Assessment 	<ul style="list-style-type: none"> • Matrix & SecureStack Switches • Enterasys NAC Gateway • NetSight NAC Manage
Multi-Context Authorization	<ul style="list-style-type: none"> • IEEE 802.1X Authentication • MAC-based Authentication • Web-based Authentication • CEP Detection 	<ul style="list-style-type: none"> • OUI Masking / Authentication • Multi-User Authentication • Role-Based Policy Configuration 	<ul style="list-style-type: none"> • Matrix & SecureStack Switches • NetSight Policy Management • Enterasys NAC Gateway
Policy Enforcement	<ul style="list-style-type: none"> • Traffic Filters • Rate Limits • Flow Isolation • Dynamic Policy Enforcement 	<ul style="list-style-type: none"> • Intrusion Detection • Flow Isolation • Threat Mitigation 	<ul style="list-style-type: none"> • Matrix & SecureStack Switches • NetSight Policy Management • Enterasys NAC Gateway • Dragon IDS/IPS/DSCC
Notification and Remediation	<ul style="list-style-type: none"> • Layer 4 Policy Rules • Web Redirect • Application Filtering • Dynamic Policy Enforcement 	<ul style="list-style-type: none"> • End-System Registration • User-Initiated Reassessment 	<ul style="list-style-type: none"> • Matrix & SecureStack Switches • NetSight Policy Management • Enterasys NAC Gateway • Dragon IDS/IPS/DSCC
Compliance Reporting	<ul style="list-style-type: none"> • End-System Location • End-System Assessment State • User Identity 	<ul style="list-style-type: none"> • Historical – Location/Assessment State • Scan History 	<ul style="list-style-type: none"> • Enterasys NAC Gateway • NetSight NAC Manager • Dragon IDS/IPS/DSCC

Contact Us

For more information, call Enterasys Networks toll free at **1-877-801-7082**, or +1-978-684-1000 and visit us on the Web at enterasys.com



© 2007 Enterasys Networks, Inc. All rights reserved. Enterasys is a registered trademark. Secure Networks is a trademark of Enterasys Networks. All other products or services referenced herein are identified by the trademarks or service marks of their respective companies or organizations. NOTE: Enterasys Networks reserves the right to change specifications without notice. Please contact your representative to confirm current specifications.



Delivering on our promises. On-time. On-budget.