

Network Access Control (NAC)

Identity-based NAC with IPS and SIEM Integration



Complete solution featuring both physical and virtual appliances

Range of policy configuration options enables uniquely fine-grained network control and flexibility

Comprehensive dashboard reporting and advanced notification engine

Managed guest access control with sponsorship

Unified policy management in heterogeneous wired and wireless environments

Product Overview

Enterasys Network Access Control (NAC) 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 Enterasys **NAC Gateway** appliances and/or **NAC Gateway Virtual Appliance** with **NetSight NAC** 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. Enterasys NAC is tightly integrated with the Enterasys Intrusion Prevention System (IPS) and Enterasys Security Information and Event Manager (SIEM) and Enterasys NetSight Automated Security Manager to deliver best-in-class post-connect access control.

The Enterasys NAC 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. Enterasys NAC performs multi-user, multi-method authentication, vulnerability assessment and assisted remediation. It offers the flexibility to choose whether or not to restrict 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. Businesses have the flexibility to balance user productivity and security. The NAC assessment warning capability alerts users that they need to upgrade their system but can allow a grace period before they are quarantined.

Enterasys NAC policies permit, deny, prioritize, rate-limit, tag, re-direct, and audit network traffic based on user identity, time and location, device type, and other environmental variables. Enterasys NAC supports RFC 3580 port and VLAN-based quarantine for Enterasys and third-party switches, plus more powerful isolation policies (which prevent compromised endpoints from launching attacks while in the quarantine state) on Enterasys switches. Enterasys NAC is

Benefits

Business Alignment

- 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

Operational Efficiency

- 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 options including appliances and virtual appliances

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 including third party tools
- Automate endpoint isolation, quarantine and remediation, plus ongoing threat analysis, prevention, and containment

Service and Support

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

There is nothing more important than our customers.

adaptable to any device using RADIUS for authorization with configurable RADIUS attributes such as Login-LAT or Filter ID. Enterprises can apply different policies depending on the RADIUS reject attribute. For example a different policy may be applied to user with an expired password than to a user who did not have an account. The solution offers unmatched interoperability, provides the widest number of authentication options, and supports Layer 2, Layer 3 and VPN access technologies.

Enterasys NAC 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 Enterasys NAC'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/authorization and/or assessment, and then automate remediation.

Fine-Grained Configuration Options

Enterasys NAC 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 infrastructures.

Guest Account Services Included

Enterasys NAC 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. Enterasys NAC provides a self registration portal for users to register multiple devices themselves. NAC offers advanced sponsorship capabilities such as email sponsorship and a simple portal for sponsors to use to validate guest registration. LDAP integration allows dynamic role assignment for authenticated registration. Authenticated registration allows enterprise network users to register devices and receive the proper role for non-802.1X capable devices. Multiple registration groups allow administrators to give different levels of access to different types of guests. 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. Enterasys NAC provides user identity functionality including discovery, authentication and role based access controls. Enterasys NAC integrates with identity sources such as Siemens Enterprise Communications HiPath DirX Identity and Microsoft Active Directory leveraging and extending the organization's existing directory investments. Users are managed centrally in the identity system for the network and all connected applications. The process of managing the user's lifecycle (e.g. enrollment, role changes, termination) can be automated and linked to other business processes with LDAP and RADIUS integration. Users can be automatically added or deleted when they join or leave the organization. Enterasys identity-aware networking capabilities provide stronger network security and lower operational cost.

Endpoint Baselineing and Monitoring

All end systems in the network infrastructure should be incorporated in the network access control system for control to be most effective. Enterasys NAC provides agent-based or agent-less endpoint assessment capabilities to determine the security posture of connecting devices. Enterasys NAC, 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. The agent-less capability does not require the installation of a software security agent on the end system and is typically used for end systems such as guest PCs, IP phones, IP cameras or printers. The Enterasys agent-less assessment scans for operating system and application vulnerabilities. The agent-based capability requires the installation of a software agent on the end system. The endpoint agent scans for anti-virus status, firewall status, operating system patches and peer-to-peer file sharing applications. The agent can look for any process or registry entry and automatically remediate. This combination of agent and agent-less capabilities in the Enterasys NAC solution enables more efficient management and reporting.

Notifications and Reporting

The advanced notification engine in Enterasys NAC 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. Notification is delivered through traps, syslog, email or web service. The notification engine has the ability to run a program triggered by a notification event. For example, integrated with the help desk application, NAC notification can be used to automatically map changes in the infrastructure to actions.

End-system reporting is simple with Enterasys NAC web-based end-system data views. NAC provides easy-to-use dashboards and detailed views of the health of the end systems attached or trying to attach to the network. Analysts responsible for monitoring end-system compliance can easily tailor the views to present the information in their preferred format. The reports can be generated as PDF files.

NetSight NAC Management

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

NAC management provides additional value through its integration with other Enterasys NetSight capabilities and Enterasys security products. For example, NAC management seamlessly integrates with NetSight policy management to enable “one click” enforcement of role-based access controls. The IP-to-ID Mapping feature binds together the User, Hostname, IP address, MAC and location (switch and port or wireless AP and SSID) along with timestamps for each endpoint—a key requirement for auditing and forensics. IP-to-ID Mapping is also used by NetSight Automated Security Manager to implement location-independent distributed intrusion prevention and by Enterasys Security Information and Event Manager (SIEM) or other third party SIEM/IPS solutions to pinpoint the source of a threat. NAC management in NetSight provides centralized visibility and highly efficient anytime, anywhere control of enterprise wired and wireless network resources. OneView, the unified control interface, enables simplified troubleshooting, help desk support tasks, problem solving and reporting. 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.

Enterasys NAC Gateway

The Enterasys NAC Gateway controls endpoint authentication, security posture assessment and network authorization. For authentication services, the Enterasys NAC Gateway acts as a RADIUS proxy, or RADIUS server for MAC Authentication, which communicates with the organization’s RADIUS authentication services (e.g. interfaces with Microsoft Active Directory or another LDAP-based directory service). The Enterasys NAC Gateway supports 802.1X (Extensible Authentication Protocol), MAC, Web-based and Kerberos Snooping (with certain restrictions) authentication. For endpoint assessment, the Enterasys NAC Gateway connects to multiple security assessment servers.

For authorization services, the Enterasys NAC Gateway communicates RADIUS attributes to the authenticating switch. This allows the switch to dynamically authorize and allocate network resources to the connecting endpoint based on authentication and assessment results.

The Enterasys NAC Gateway appliance also stores NAC configuration information and the physical location of each endpoint. It easily scales to support redundancy and large NAC deployments. Enterasys NAC Gateway models are available to meet the needs of different-sized implementations.

Assessment for the NAC Gateway is separately licensed and includes both agent-based and agent-less assessment.

Enterasys NAC Gateway Virtual Appliance

Enterasys NAC Gateway Virtual Appliance provides all the powerful endpoint authentication, security posture assessment and network authorization capabilities built on VMware®. Deploying NAC Gateway Virtual Appliance, enterprises gain all the benefits of network access control with the advantages of a virtual environment — cost savings from using existing hardware and reduced time to value. Available with different sizing options for central locations as well as remote sites.

Assessment for NAC Virtual Appliance is separately licensed and includes both agent-based and agent-less assessment.

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 NAP and Trusted Computing Group TNC.
- 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 five NAC deployment models: intelligent wired edge, intelligent wireless edge, non-intelligent wired edge, non-intelligent wireless edge, and VPN.
- Enterasys NAC provides VPN support and, with an Enterasys SSA switch in distribution, provides more flexibility through policy.
- Management options can be tailored to existing network management schemes and security requirements.
- Support for multiple RADIUS and LDAP server groups allows administrators to identify the server to which a request is directed.
- Macintosh agent support for agent-based assessment.
- Open XML API's support integration with IT workflows for automated streamlined operations
- Web-service based NAC API simplifies integration with third party applications.
- 1 + 1 Redundancy for Layer 2 deployment modes: provides high-availability and eliminates the NAC Gateway as a single point of failure
- Risk level configuration allows flexibility in determining threat presented by the end system. Fine grained control allows NAC administrator to define High Risk, Medium Risk, and Low Risk thresholds based on local security policies and concerns.
- The Enterasys NAC Gateway is upgradable, allowing assessment to be integrated onto a single box with the other NAC functions. The upgraded appliances are capable of supporting both network-based and/or agent-based assessment.

Specifications

NetSight NAC Management

Enterasys NetSight provides the management capabilities for NAC. NetSight is available for 32-bit operating systems:

Windows (qualified on the English version of the operating systems)

Windows Server® 2003 w/ Service Pack 2

Windows XP® w/ Service Pack 2 or 3

Windows Vista® (Service Pack 1 Optional)

Windows Server® 2008 Enterprise

Windows Server® 2008 Enterprise 64-bit (as 32-bit application)

Linux

Red Hat Enterprise Linux WS and ES v4 and v5

SuSE Linux versions 10 and 11

Hardware Requirements

Recommended P4-2.4 GHz, 2GB RAM

(User's home directory requires 50MB for file storage)

(Windows Vista requires 2GB RAM)

Free Disk Space - 1GB

Remote Client

Recommended P4-2.4 GHz, 1GB RAM

(Windows Vista requires 2GB RAM)

Free Disk Space - 100MB

(User's home directory requires 50MB for file storage)

Supported Web Browsers:

Internet Explorer version 7 and 8

Mozilla Firefox 2.0 and 3.0

Java Runtime Environment (JRE) 1.5 or higher

(Windows Vista requires JRE 1.6 or higher)

Enterasys NAC Gateway

Physical Specifications

Height: 1.68" (4.26 cm); Width: 18.99" (includes rack latches) (48.24 cm); Depth: 30.39" (includes PSU handles and bezel) (77.2 cm); Weight: 39 lbs (17.69 Kgs)

Power

Wattage: 717 Watt (high output), 570 Watt (Energy Smart); Voltage: 90- 264 VAC, autoranging, 47- 63Hz

Environmental Specifications

Operating Temperature: 10° to 35°C (50° to 95°F) with a maximum temperature gradation of 10°C per hour. Note: For altitudes above 2950 feet, the maximum operating temperature is de-rated 1°F/550 ft; Storage Temperature: -40° to 65°C (-40° to 149°F) with a maximum temperature gradation of 20°C per hour; Operating Humidity: 20% to 80% (non-condensing) with a maximum humidity gradation of 10% per hour

Agency and Regulatory Standard Specifications

Safety

UL 60950-1, CSA 22.1 60950, EN 60950-1, and IEC 60950-1, NOM

Electromagnetic Compatibility

FCC Part 15 (Class A), ICES-003 (Class A), BSMI, KCC, VCCI V-3, AS/NZS CISPR 22 (Class A), EN 55022 (Class A), EN 55024, EN 61000-3-2, EN 61000-3-3

Enterasys NAC Gateway Virtual Appliance

Packaged in the .OVA file format defined by VMware and must be deployed on a VMware ESX(TM) 4.0 server or ESXi(TM) 4.0 server with a vSphere(TM) 4.0 client.

Virtual appliance requires 12 GB of memory, four CPUs, two network adapters, and 40 GB of thick-provisioned hard drive space.

NAC Assessment Agent OS Requirements

Supported operating systems for end systems connecting to the network through an Enterasys NAC deployment that is implementing Enterasys agent-based assessment.

- Windows 2000
- Windows 2003
- Windows 2008
- Windows XP
- Windows Vista
- Windows 7
- Mac OS X (Tiger, Leopard)

Certain assessment tests require the Windows Security Center which is only supported on Windows XP SP2+, Windows Vista, and Windows 7.

Ordering Information

NetSight NAC Management

Part Number	Description									
NS-NAC	NetSight NAC Management. Requires existing Enterasys NetSight NS-CON-50 or NS-CON-U license.									
Part Number	NetSight with NAC Management									
	Devices	Thin APs	Number of Concurrent users	NetSight Capabilities Included						
				NAC	Console (including Wireless Mgmt)	OneView	Policy	Automated Security (ASM)	Inventory	Mobility
NMS-5	5	50	25	✓	✓	✓	✓	✓	✓	✓
NMS-10	10	100	25	✓	✓	✓	✓	✓	✓	✓
NMS-25	25	250	25	✓	✓	✓	✓	✓	✓	✓
NMS-50	50	500	25	✓	✓	✓	✓	✓	✓	✓
NMS-100	100	1000	25	✓	✓	✓	✓	✓	✓	✓
NMS-250	250	2500	25	✓	✓	✓	✓	✓	✓	✓
NMS-500	500	5000	25	✓	✓	✓	✓	✓	✓	✓
NMS-U	Unrestricted	Unrestricted	25	✓	✓	✓	✓	✓	✓	✓

NAC Gateway

Part Number	Description
NAC-A-20	Enterasys NAC Gateway 3,000 endpoints, optional on-board assessment
NAC-V-20	Enterasys NAC Gateway Virtual Appliance 3,000 endpoints, optional on-board assessment
NAC-VB-20	Enterasys NAC Virtual Gateway Bundle with 4 NAC Gateway Virtual Appliances (500 endpoints each), optional on-board assessment

NAC Assessment

Part Number	Description
NAC-ASSESS-LIC	Enterasys NAC Assessment, includes both agent-based and agent-less assessment

Transceivers

Enterasys transceivers provide connectivity options for Ethernet over twisted pair copper and fiber optic cables with transmission speeds from 100 Megabits per second to 10 Gigabits per second. All Enterasys transceivers meet the highest quality for extended life cycle and the best possible return on investment. For detailed specifications, compatibility and ordering information please go to: <http://www.enterasys.com/products/transceivers-ds.pdf>.

Warranty

As a customer-centric company, Enterasys is committed to providing quality products and solutions. In the event that one of our products fails due to a defect, we have developed a comprehensive warranty that protects you and provides a simple way to get your products repaired or media replaced as soon as possible.

Enterasys NAC comes with a one year warranty against manufacturing defects. Software warranties are ninety (90) days, and cover defects in media only. For full warranty terms and conditions please go to <http://www.enterasys.com/support/warranty.aspx>.

Service & Support

Enterasys Networks provides comprehensive service offerings that range from Professional Services to design deploy and optimize customer networks, customized technical training, to service and support tailored to individual customer needs. Please contact your Enterasys account executive for more information about Enterasys Service and Support.

Additional Information

For additional technical information on Enterasys NAC <http://www.enterasys.com/products/advanced-security-apps/enterasys-network-access.aspx>

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



© 2011 Enterasys Networks, Inc. All rights reserved. Enterasys Networks reserves the right to change specifications without notice. Please contact your representative to confirm current specifications. Please visit <http://www.enterasys.com/company/trademarks.aspx> for trademark information.

