

Embedded Security

with Standards-Based Interoperability

As Interviewed By John Siefert



Trent Waterhouse
Vice President



Q

How does Enterasys define Network Access Control?

A

Enterasys takes an architectural approach: we embed security in every wired/wireless and switched/routed connection with standards-based interoperability. This leverages existing investments and avoids planned obsolescence.

Proactive management. Enterasys® Secure Networks™ proactively manage whether a guest, user, or any device can connect to a network and what they are authorized to do once connected – all based on policy or role criteria such as identity, time, and location. Enterasys believes any NAC architecture should include four basic functions:

- Pre-connect and post-connect assessment and authentication,
- Automated isolation, quarantine, and remediation,
- Policy-based authorization and compliance audit, and
- Continuous threat analysis, prevention, and containment.

Beyond pre-connect issues. Many NAC offerings only address pre-connect issues without addressing policy-based visibility and control of users, devices, and applications after they connect to the network. If a user or device does not pass assessment and authentication, they are individually isolated on Enterasys network equipment or, when connected to another networking hardware vendor's environment, placed into a quarantine virtual local area network (VLAN) using RFC 3580 methods.

Q

40% of the 300 early adopters surveyed in our recent study said a key NAC feature is to “provide controlled access for unmanaged users.” How does Enterasys enable this?

A

Secure guest access is provided by Enterasys Secure Networks solutions so organizations can enable visitors or unmanaged users to connect to the Internet without threatening any other IT assets.

Enterasys offers agent or agentless assessment services for Windows, Solaris, Linux, and Mac OS. These determine if

a network client is compliant with an organizations minimum security requirements through interoperability with CheckPoint (Zone Labs), Lockdown, Microsoft, Nessus, and Symantec (Sygate) vulnerability assessment tools.

The Enterasys NAC architecture then performs pre-connect authentication via 802.1X (user & machine), MAC (machine), and web-based (user) identity methods that use RADIUS/LDAP along with unique contextual authentication based on location, time, and mobility restrictions of a user or device. Based on the results of the authentication, a policy is dynamically created for the user or device. Enterasys can uniquely authenticate multiple users/devices connected to a single port.

Q

Ongoing threat analysis and containment is considered another key factor in a NAC solution. How does Enterasys’ Secure Networks solution ensure this?

A

Continuous threat analysis and containment is provided through intelligent NAC integration with Enterasys’ Dragon intrusion detection, intrusion prevention,

Visit the NAC Battleground Online: www.nacbattleground.nwc.com

network behavioral analysis and security event information management solution to deliver dynamic intrusion response, automated enforcement of acceptable use policy, and proactive prevention of zero-day threats.

Enterasys can secure any network by intelligently sensing and automatically responding to security threats. Secure Networks understand who and what is connected, where they are, and what they are doing as well as how users and devices relate to the business – thus assuring that users can do what they need to do without being able to do harm.

Q In our research, 37% and 36% of respondents, respectively, cited HIPAA and SOX as drivers behind their NAC decision making. How is Enterasys taking federal compliance issues into consideration in product development?

A Enterasys Secure Networks NAC solutions help you comply with governmental regulations such as BASEL, CALEA, HIPPA, Payment Card Industry, Data Security, and SOX by providing auditing, surveillance, and reporting aligned with regulatory needs.

With Enterasys, you can intelligently and automatically ensure that the right users are accessing the right IT resources from the right place at the right time while protecting you and your information.

If isolated or quarantined, the user is presented with a Web page with options for automatically remediating the problem, such as applying a patch or updating virus signature files. Once connected to the network, centralized visibility and control authorization of network resource utilization (quality of service [QoS], access control list [ACL], rate limiting) is provided based on the authenticated identity and policy of the user, machine, or other device. Enterasys enables and documents these enforcement capabilities to facilitate regulatory compliance.

Q The Secure Networks Architecture is at the core of Enterasys' NAC play for the enterprise. What differentiates it from other approaches in the market?

A The Secure Networks NAC advantages can be summarized as follows:

- Standards-based, open architecture with a commitment to interoperability with Trusted Computing Group, Cisco, and Microsoft approaches to NAC,
- Integration with multivendor networking hardware, assessment engines, remediation servers and intrusion detection/prevention systems,
- Granularity beyond ports and VLANs to individual flows, devices and users,
- Works in static-IP or non-IP protocol environments, since it is not DHCP-based,
- A comprehensive solution that ensures the integrity and performance of IT services and the business users who rely on them.

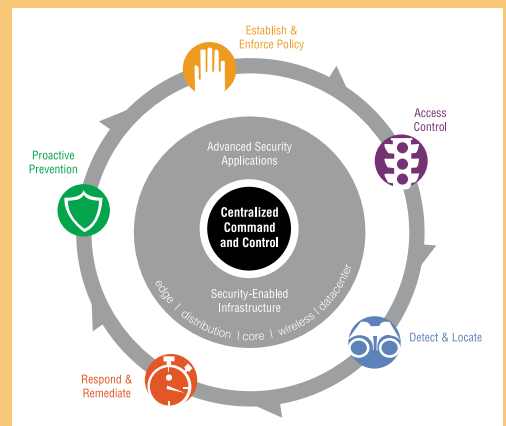
www.enterasys.com
(877) 801-7082

Hot

What's Online

Learn More About Secure Networks

Enterasys Secure Networks offer policy-based visibility and control of your users, devices, and applications to protect you and your information in a way that is practical, achievable, and able to deliver rapid time to value.



The granular authentication, authorization, and audit of individual traffic flows in our solution gives you unmatched control over who can do what from where at a particular time. Secure Networks enable you to automatically enforce acceptable usage policies for users and applications. Our patented technology

- Detects and locates threats to your organization's IT assets,
- Automatically responds to isolate those threats and remediate them, and
- Can proactively prevent new threats from entering your environment.

What that means to you is worm and virus quarantine, DDOS attack prevention, and DHCP/DNS/Gateway protection. You can assure that your network delivers converged voice/video/data traffic and secure guest access with automated enforcement of company policy or government regulation for compliance purposes. And you control access to internet, email, or other applications while preventing hosting or downloading of inappropriate or illegal content.