

Enterasys® Network Access Control Solution

Comprehensive Visibility with Policy-based Control for Any Network

Overview

Network Access Control (NAC), an essential component for any organization's overall security posture, mitigates the elevated risks from threats found in today's information technology environments. Many NAC implementations only provide 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. The Enterasys Network Access Control solution has been designed specifically to address this challenge, and to control access for every user, machine or other endpoint, all of the time.

Enterasys NAC provisions access to network resources and services based on context such as authenticated identity of the user or device, location, time, and the current / historical security posture of the device. Access privileges are granted based on these criteria; while non-compliant systems are quarantined for remediation or simply logged for future evaluation. The Enterasys NAC solution then continuously monitors users and endpoints to ensure they are behaving normally in compliance with acceptable use policies. Non-compliant systems are forced into a quarantine and remediation state to prevent propagation of threats across the network.

The Enterasys Solution

Enterasys leverages its Secure Networks™ architecture to deliver continuous threat analysis and containment that goes far beyond one-time health checks and authorization. Enterasys NAC is a single solution designed for multi-vendor / multi-technology network infrastructures. It provides simplicity in deployment, scalability in operation, effectiveness in risk mitigation, and ease of management. Enterasys NAC is standards based and designed using an open-architecture for maximum interoperability.

Implementing NAC (or any other security solution) forces changes to business processes and must be done with minimum disruption of day-to-day operations. For this reason, Enterasys NAC may be deployed in multiple stages to align with the security and business requirements of the organization. A first step is to deploy device and user authentication services, plus centralized management, auditing and reporting. This deployment may then be enhanced with end system health state and compliance assessment; and ongoing security assessment thereafter. Finally, automated threat management - including the isolation, quarantine and self serve remediation of non-conforming end systems - may be added.

Enterasys NAC is centrally managed by a single enterprise class management suite; ensuring that users and networked endpoints always have access to the appropriate network resources, while business critical systems and processes are protected from misuse and compromise. Enterasys' NetSight integrated software suite controls the NAC solution as a whole system vs. a disparate set of individual NAC components to reduce costs and greatly increase IT efficiency.

Benefits

Continuous Business Protection

- Only the right users have access to the right information from the right place at the right time
- Secure guest & contractor access
- Verify endpoint security posture
- Role-based security and priority
- Ongoing compliance health check

Investment Protection

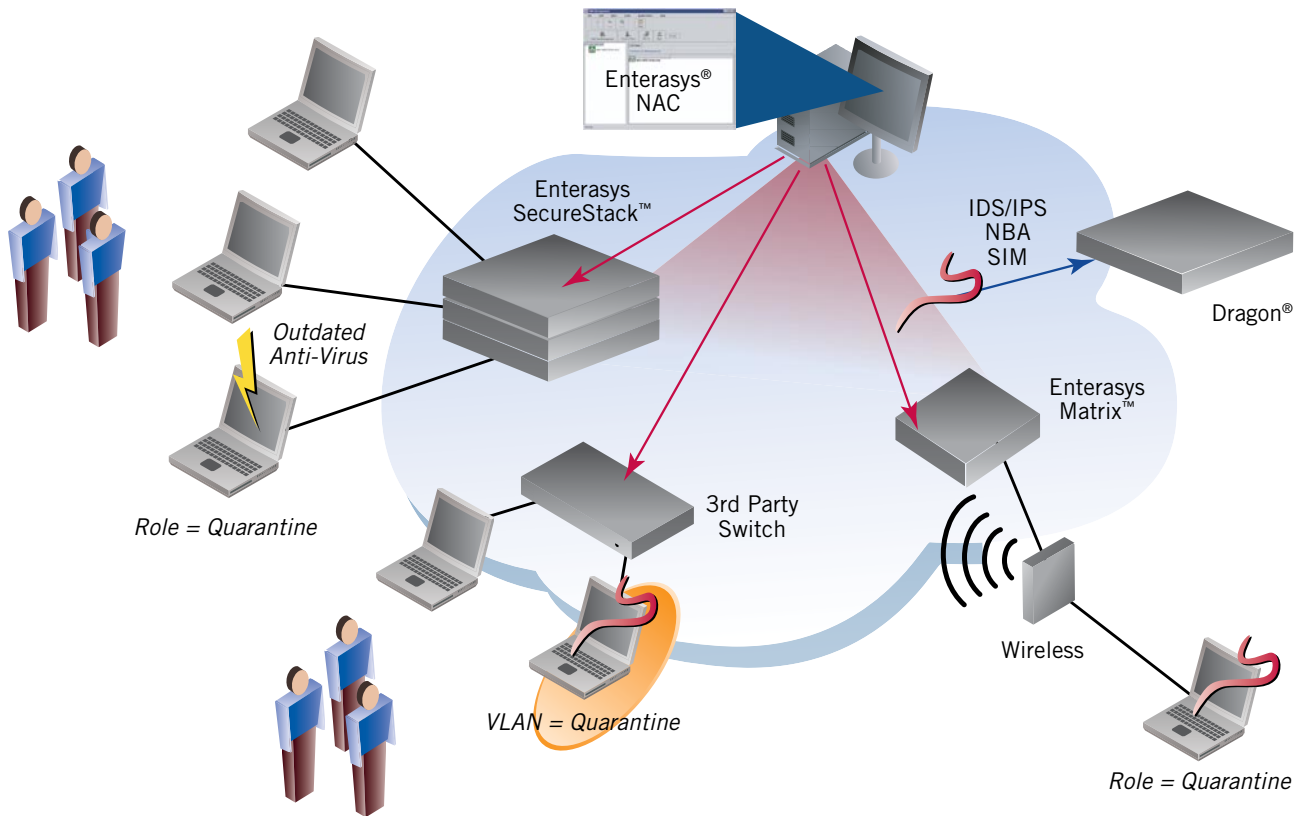
- Supports multi-vendor wired and wireless networks without requiring forklift upgrades
- Rapid deployment without requiring agents on your desktops or other disruptive configuration changes
- Standards-based architecture and proven interoperability with Microsoft NAP and TCG Trusted Network Connect

IT Operations Efficiency

- Do more with less via centralized visibility and control management software
- Proactively prevents new threats from entering the IT environment
- Phased deployment allows you to start with simple detection and location, add authentication and/or assessment, then automate remediation

Enterasys NAC includes a combination of in-band and out-of-band NAC technology integrated into a single cohesive solution. This flexible solution allows NAC traffic enforcement to take place directly at the access edge for intelligent infrastructure devices, and near the access edge at the distribution/aggregation layer for areas of the network with less capable or unmanaged switches.

Enterasys NAC intelligently integrates with NetSight Automated Security Manager, NetSight Policy Manager, Dragon Intrusion Detection/Prevention and Dragon Security Command Console. The end result is proactive visibility and control to comprehensively and proactively assure network security.



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.