Network Access Control Whitepaper

Enterasys Network Access Control

Executive Summary

With the increasing importance Network Access Control (NAC) plays in an organization's overall network security posture, the purpose of this white paper is to explain how Enterasys takes an open-architecture, standards-based approach to NAC. Enterasys can secure any network from any vendor by intelligently sensing and automatically responding to security threats. Secure Networks™ from Enterasys identifies who and what is connected, where they are, and what their role is in the organization. The result is an assurance that users will have access to the network resources they need to do their jobs while critical business systems and processes are protected from misuse and compromise.

Enterasys' architectural approach embeds security in the network infrastructure and manages the heterogeneous network environment with centralized control. Through standards-based interoperability, IT organizations can leverage their existing investments and extend the lifecycle of products and technologies. Enterasys Secure Networks proactively manage whether a trusted user, a guest, or a device can connect to a network and what they are authorized to do once connected—all based on policy criteria such as device and user identity, business role, time of day, location, and health of the end system.

An effective NAC solution must be an integral part of an overall network security strategy designed to include:

- Identity services and authentication for devices and users

- Pre-connect and post-connect assessment of end-system health

- Automated isolation, quarantine and threat management

- Policy-based network usage and service authorization, including self-remediation

- Continuous threat analysis, prevention and containment

- Comprehensive compliance auditing

Many NAC offerings only address pre-connect issues without factoring in the importance of enforcing network usage and security policies while the end system is connected to the network. If a user or device does not pass assessment and authentication when connecting to Enterasys network equipment, they are prevented from accessing business-critical services and only allowed to access pre-determined remediation or guest services. When connected to another vendor's networking equipment, an Enterasys NAC solution can quarantine the end system in a Virtual Local Area Network (VLAN) using standards-based (RFC3580) methods.

Enterasys NAC supports agent-based and agent-less assessment services for end systems. This means that end systems running popular operating systems such as Windows, Solaris, Linux and MacOS, as well as end systems of any type, can be assessed for vulnerability and threat. Leveraging interoperability with leading vulnerability assessment technologies from Check Point, Microsoft, Tenable Network Security and Symantec, the Enterasys NAC solution offers a comprehensive solution of proactive network security by determining if an end system is compliant with an organization's network communications security requirements.

Secure guest access is provided in the Enterasys solution so organizations can safely and securely enable visitors or unmanaged users to connect to the Internet without threatening critical IT assets. Leveraging multiple authentication methods such as 802.1X, MAC-based and Web-based, as well as agent-based and agent-less assessment, any end system and user can be assessed and authenticated for connectivity to the network where they can securely access the services needed for their role in the business.

Once an end system has securely gained access to the network, continuous threat analysis and policy enforcement are provided through intelligent integration between the Enterasys NAC solution, the Enterasys Dragon® event detection solution and the Enterasys NetSight® Automated Security Manager application. The Enterasys Dragon solution includes intrusion detection (IDS), intrusion prevention (IPS), network behavioral anomaly detection (NBAD) and security information management (SIM) technologies. The Enterasys NetSight Automated Security Manager application provides an automated framework for aligning event detection with source location and threat mitigation. The result of this fully integrated approach is both pre-connect and post-connect security, dynamic intrusion response, and proactive prevention against zero-day attacks.

Enterasys' Secure Networks solution for NAC provides a comprehensive security capability that is practical, achievable, delivers rapid time to value and answers the following key questions:

- Can the network strictly enforce the authentication of any user or device without requiring forklift upgrades?

- Can the network be assured that an end system is safe and secure before it is allowed to access IT services?

- Can the appropriate network usage policies be automatically determined based on the type of end system and who might be using it—and can the network offer granular enforcement of policies right where the end system connects?

- Can the network react in real time when a threat appears from an end system previously allowed into the environment?

- Can the network keep track of where and when all types of end systems are communicating, and what IT resources they are utilizing?

- Does the network support open-architecture, multi-vendor interoperability?

- Is there management software to deliver the centralized visibility and control necessary to administer access-control policies across an entire enterprise?

Let us show you how our innovative products and technologies can enable you to effectively control access to your network and business applications and proactively protect the confidentiality, integrity and availability of your IT assets. Leading companies worldwide have deployed Enterasys Secure Networks solutions for NAC. Set up a time to see how our unique approach can increase your overall security posture while leveraging your existing investments. Call **(877) 801-7082** or **+1 (978) 684-1000** or visit **enterasys.com/securenetworks**.

Introduction

This paper addresses challenges facing IT organizations as they design and implement a Network Access Control (NAC) solution and proposes a unique open-architecture approach to meeting the performance, security and compliance requirements of a network infrastructure supporting policy-driven communications.

NAC is an industry term with a history of usage among network infrastructure vendors, operating system vendors and security software vendors. Network infrastructure vendors originally introduced access-control technologies as authentication and authorization solutions for controlling basic network communications from users and devices. Both user- and device-based credential systems enabled IT organizations to centrally administer who and what was allowed to communicate on the network. Over time this concept of controlling access to the network began to evolve to include a more sophisticated set of contextual information used to determine who and what is allowed to communicate on the network from a particular location at a particular time. Operating system vendors and security software vendors could provide information about the end system that could be used in addition to the credentials in the authentication process. Assessment of the "health" of an end system, including the threat that the end system might pose to the networked environment, and the vulnerability of the end system to become infected with a worm or virus, could be part of the context used in the authentication and authorization process.

From this multi-faceted approach to determining who and what should be allowed onto the network, and where and when an end system should be allowed to access came the industry promotion of the now commonly used term Network Access Control or NAC. Current NAC solutions can help protect an organization from undesirable network resource usage, unintentional and blatant security threats, and denial of service attacks from worms and viruses propagating through vulnerable end systems. NAC solutions can also help to enforce communication policies, allowing for better allocation of network resources so that the business processes are as efficient as possible. The benefit to an organization implementing a NAC solution is a more secure and efficient business environment. The challenge is in understanding the many technologies involved in the various NAC solutions on the market, and finding a true architectural approach that delivers several critical functions:

- Visibility and identity management of the various end systems connecting to a network

- Assessment of the end systems, both before they are allowed onto the network (pre-connect) and after they are allowed onto the network (post-connect)

- Ability to accurately enforce the appropriate network and application usage policies for all end systems, wherever they connect

- Remediation assistance for end systems and/or users not in compliance with the security and network usage policies

- Compliance reporting that details where end systems are (and have been) in the network and what they were doing on the network

With the criticality of today's network in supporting the business (and the significant increase in security threats potentially impacting the business), solutions that provide both proactive and reactive technologies to assure business continuity will provide a significant return on investment. Network Access Control is an essential element to an overall network security architecture to protect the confidentiality, integrity and availability of information assets.

Network Access Control – What Does it all Mean?

NAC is a term describing various technologies developed to control/restrict access by end systems to the network based on their "health." The basic concept is that dangerous or vulnerable (i.e., "unhealthy") end systems should not be allowed to communicate on the business network because they could pose a security risk to critical processes and services. A NAC solution would prevent an unhealthy end system from accessing the network in a normal manner until the health of the end system is determined.

The health check of a network-attached device is also known as end-system "assessment." End systems can be traditional PCs, printers, IP phones, IP security cameras, etc. An assessment should discover both the acceptable level of vulnerability and threat of an end system. Elements such as security patch level, anti-virus/anti-malware presence, anti-virus/anti-malware signature updates, applications running, open ports, etc., can all be investigated to determine the overall health of the end system.

A desirable NAC approach should allow for the assessment of any type of end system connected to the network. This is critically important with the increasing diversity in the network-connected end systems in typical networks. To have a comprehensive, proactive posture to network security, every end system connecting to the network (no matter what type of device) must be challenged by the NAC solution. The actual function of assessment can be provided by various applications. The assessment application may require an agent located on the end system itself, or may function completely independent of the end system in an agent-less manner.

Many vendors' NAC solutions currently do not rely on an end-system authentication challenge as part of the access-control process. Authentication should be a critical foundation to any NAC solution and is required to achieve scalability, flexibility, visibility and strong enforcement requirements of network usage and security policies. Once a user or a machine is authenticated (credentials have been verified) the authorization process takes place, altering the configuration of the source network physical port or virtual flow to enable communications based on a set of policy rules. Strong authorization technology should leverage additional layers of context such as location, time of day, MAC address and user identity overrides (the ability to override the authorization process results), resulting in a robust solution that is easier to align with business processes. The flexibility of multi-user, multi-method authentication in a vendor's NAC solution means you don't have to replace any of your edge switches in order to gain visibility and control over those attached users and devices.

After the end-system assessment and authorization process takes place, if it is determined that the end system is out of compliance with network security policies, the end system is placed into a network quarantine state. The quarantine policy enforcement process should involve very granular (i.e., flow-based) network communication policies (not just simple VLAN assignment). After all, putting all of the "unhealthy" end systems into the same quarantine VLAN just means they will cross-infect each other with new vulnerabilities. Network policies describe how incoming traffic on switch ports should be handled related to filtering, prioritizing and tagging.

Remediation is the act of rectifying a problem in order to become compliant with certain pre-defined policies. A remediation process as part of a NAC solution allows users placed in a network quarantine state to get back into compliance. It is important that the network user be engaged in the remediation process so that business process efficiencies can be maximized. When a user or their end system has a problem, they should be able to fix it without having to involve IT staff. This will keep IT help desks from being overwhelmed by end-system configuration/compliance issues. In order for this process to be effective, the NAC solution must provide user notification when an end system is put into network quarantine, and communication policies must be enforced as part of the quarantine state to allow secure communication to the services needed to get the end system into a compliant state.

Authentication, assessment, authorization, policy enforcement and remediation are all critical parts of a comprehensive NAC solution. There are many products and technologies available from a multitude of vendors that offer some of these parts. An integrated, open-architecture NAC solution will offer all of these critical parts working together in a fully integrated fashion to deliver important security.

Requirements of a Complete NAC Solution

To ensure effective implementation of a NAC solution several requirements should be met:

• Open architecture – Support of multi-vendor environments

• End-system inclusion – Support of any type of end system

• Multi-context authorization – Various attributes

• Policy enforcement – Role-based and quarantine

• Notification and remediation – User self-help

• Compliance reporting – Historical and real-time information

For a NAC solution to be effective, it must be deployable as an open architecture. The NAC solution must be able to support assessment of any type of device that may be connected to the network, and it must be able to provide increased security in environments that may have deployed equipment from more than one network infrastructure vendor. Assessment and authentication for only computers running certain operating systems or security agent software is simply not comprehensive enough to protect today's highly diverse enterprise environments. In order for the NAC solution to effectively secure a real-world network environment from threats and vulnerabilities originating from the variety of connected end systems, multiple vendors' assessment technologies must be incorporated. An assessment technology that is only suited for certain end systems leaves the network and the related services open to attack from end systems not included in the security posture. Multiple assessment technologies from separate software vendors must be capable of integrating with the NAC solution. This allows the NAC solution to draw upon the required assessment technology for whatever type of end system is connecting to the network.

In addition to the ability to leverage multiple assessment technologies for a comprehensive approach to proactive protection, a NAC solution should be effective in an environment with a mixed-vendor infrastructure. Real-world network environments may have several different vendors' infrastructure products deployed. A NAC solution must address end systems connected to different types of network switches—and from different vendors. A "forklift upgrade" of network communications infrastructure products is not a cost-effective way to deploy a comprehensive NAC solution, and should not be part of the equation. Standards-based technologies for authentication and policy enforcement (such as IEEE 802.1X and RFC3580) should allow a well-conceived NAC solution to be deployed in a network environment including several different vendors' infrastructure products.

Proven network security solutions are flexible and adaptable to provide business continuity for complex "real-world" networks. An open approach to deploying NAC enables a company to properly secure their network environment against vulnerabilities and threats from any end system connected to any network infrastructure product. This will ensure that a company can implement the end systems, applications and software important to their business needs without having to factor in network security dependencies—and their potential indirect costs.

The diversity of network-connected end systems is increasing significantly in today's business networks. With the realization of converged networks hosting a wide variety of business applications, the types of connected end systems continue to evolve. In a modern business network today it is likely that you will find end systems such as IP phones, surveillance cameras, building controls and even vending machines along with the traditional desktops, laptops and printers. With such diversity of connected end systems, it is critical that a well-architected NAC solution **includes all end systems**. In a network with a variety of types of end systems, security processes must not be locked into specific device types, operating systems or software. A printer, copier, IP phone or security camera can easily be infected and are as likely to be a point of infection and propagation of a security threat as a desktop or laptop connected to the network. A NAC solution must be able to provide proactive and reactive security for any end system. This includes technologies to assess, authenticate and authorize any end system, no matter what type of device and what operating system or applications are running on the device.

A strong NAC solution should be able to take into consideration many different attributes when determining the health, safety and purpose of an end system and, where applicable, the person using it. **Multi-context authorization** of end systems allows for more specific security measures to be enforced and also for better-focused network and application usage. End-system assessment alone is not enough to determine the authorization of a device and user to access the network and specific applications and services. The NAC solution should take into consideration additional contextual attributes such as device type, location of the connection, time of day, user and machine credentials, and business role of the device and the user. When factoring in multiple contextual attributes, a network communication policy can be enforced upon the end system providing very specific security and network communication rules. End systems can be restricted from communicating to applications that are not relevant to the type of device or the user's role. Specific quarantine rules can be enforced allowing secure communication to critical services needed to remediate a device, but without any possibility of adversely impacting other end systems or business communications. The more context in the authorization process of a NAC solution, the more precise and efficient the network communications and security will be.

A critical aspect of any NAC solution is the process of **policy enforcement**. Enforcing network communication and security policy rules right at the network connection point of an end system is the best way to ensure that the right devices and people are communicating to the right business application at the right time. It also ensures this is happening in a safe and secure manner so as not to adversely affect other devices, people and applications on the network. Policy rules should be granular in nature so that specific controls of threatening communications and application usage can be enforced anywhere in the network. If an end system is assessed to be dangerous or vulnerable, policy rules can be enforced to quarantine the end system so it does not endanger to the rest of the business environment. The quarantine policy rules should be more comprehensive than simply placing the end system's connection into a VLAN where other out-of-policy end systems are communicating. This can present additional risk to other end systems and a potential cross-infection distribution point for dangerous communications. The granular quarantine policy that is enforced should not have any specific topological dependencies (such as VLAN assignment). Specific policy rules for Layer 2 through 4 network communication should be enforceable so that an end system can be completely isolated from everything on the network except for the exact application services needed for notification or possibly remediation. This enforcement of policy should be dynamic and fully distributed throughout the network infrastructure. Policy rules should be enforced by the network infrastructure itself, right at the point of end-system connection. This ensures a scaleable and comprehensive policy framework as part of a NAC solution.

If an end system is determined to be threatening or vulnerable, **notification and remediation** become a critical part of the process. Enforcing a quarantine policy against an out-of-policy end system may prevent it from doing harm in the business network, but if the user of the end system does not understand that they have been put into this quarantine state (and why), they will likely assume that there is something wrong with the

communications network or the application services. Notification to a user of a quarantined end system prevents a flood of calls to the IT help desk and also enables the user to understand that they have an issue with their end system or their attempted communication. A well-architected NAC solution will include a process of system-driven notification to the user of the end system. This is typically presented through the common Web browser, or may use other services such as Instant Messaging or e-mail. The actual notification should include not only an explanation of the quarantine policy that is in effect against the end system, but also a description of the reasons(s) for the quarantine action and how a user might safely remediate the problem. This could be simple instruction for the user on how to go to a patch server or signature update server. It could also include instructions on how to turn off particular out-of-policy services or applications. Once a user has attempted remediation, they can be allowed to reattempt end-system assessment in order to get out of the quarantine policy state and enter a productive state of a specific business policy role.

A well-architected NAC solution collects and uses a great deal of information about connected end systems, users and network communications. Much of this information can be instrumental in assisting with compliance reporting. Because a NAC solution should be involved in the authorization of every network-connected end system, data can exist that can give not only real-time visibility to what is connected to the network and where, but also historical views of connected end systems. This can be extremely helpful when dealing with a compliance issue where a historical record is needed to explain where an end system has connected to a network, and what services it had access to. In addition, because a good NAC solution includes authentication of both end systems and the users running them, correlation can be reported on who was on the network at a particular time and at what location. NAC solutions that have granular policy enforcement capabilities can also report on the actual usage of the network and its resources by an individual end system and/or user. Comprehensive NAC solutions should not only assess and authorize end systems and users, but also report on important compliance parameters.

An Architectural Approach

Enterasys Networks provides an architectural approach to delivering Secure Networks. Unlike other vendors' approaches, Enterasys fully integrates a security-enabled infrastructure, advanced security applications and centralized visibility and control to enable IT organizations to deploy networks that will proactively and reactively mitigate risks to provide a highly available and secure business communications environment.
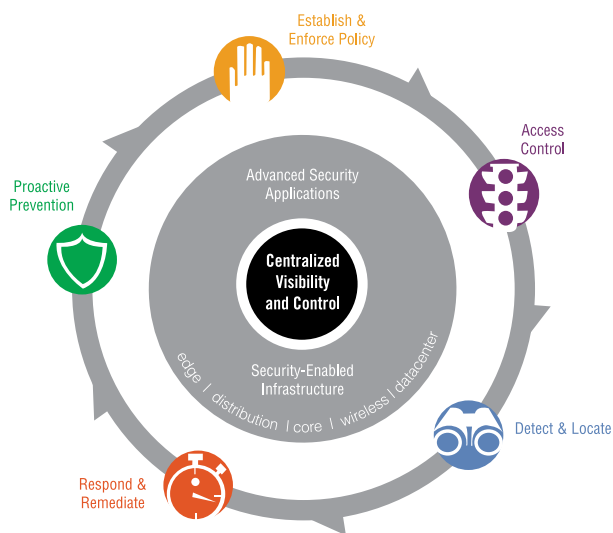
Advanced Security Applications

Intrusion Prevention and Network Access Control

Centralized Visibility and Control

Management Software

Security-Enabled Infrastructure

Switches, Routers, Wireless

From this architectural approach to delivering Secure Networks comes a significant amount of capability. The architecture enables network usage **policies** for users and devices to be **established** centrally and **enforced** throughout the network environment. These policies for network communication enable an IT organization to ensure the overall integrity of data communications and to restrict and isolate communications from un-trusted and dangerous end systems and users. Policies can be applied to communication from any type of end system connecting to the network.

The architecture will enforce **access control** of users and devices attempting to communicate on the network and to specific services. End systems of different types can be detected and identified once they connect to the network. Once an end system is identified, access to the network, as well as to specific services, can be controlled based on the type of end system, the organizational role of the end system and/or the person who may be using it, the location of the connection, the time of day, and the assessment of the end system's health and vulnerability. This allows any of the diverse types of end systems in a network today to be identified when they show up, and their communication on the network controlled to ensure secure and reliable access to appropriate services.

The architecture will **detect** threats and anomalies anywhere on the network and **locate** the exact source. Because of the increased business importance of the network infrastructure, it is critical that threats to critical services are detected and mitigated in a real-time fashion. Enterasys leverages patented technology to deliver a unique capability of detecting problems as they occur in the network and isolating the exact source of the problem. In a network of thousands of end systems, the exact source of a threat or network problem can be determined in just seconds.

The architecture will **respond** to threats with pre-defined specific and measured action and will allow users to **self-remediate** when appropriate. Because of the architecture's ability to locate the exact source of a threat to the environment, an appropriate response can be taken. The response might vary based on the type of threat or network anomaly, and the Enterasys solution allows for measured response options including disabling a port, changing a VLAN, enforcing a specific set of communication policy rules, notification, and quarantine of an individual user or communication flow. In the cases where the problem being addressed involves a user, the architecture allows for the enforcement of specific policy rules to completely protect all critical network services, but still allow the user to self remediate so they can quickly become productive to the business.
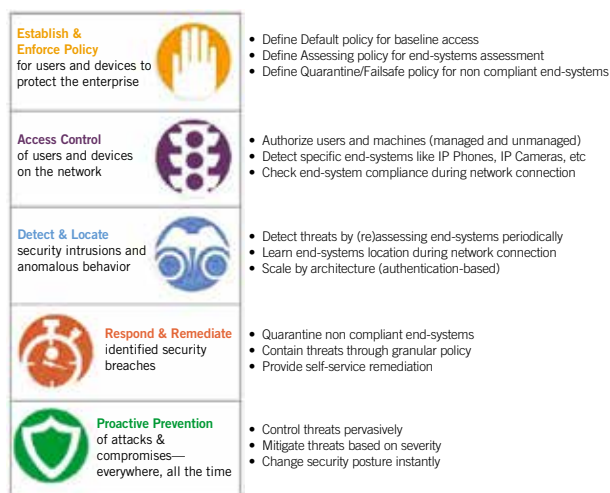
The architecture will **proactively** protect the business network from vulnerable and dangerous end systems, **preventing** them from compromising critical business services and other users and end systems. Defenses are established to protect the environment from known threats and network misuse. In addition, end systems of all types can be assessed for vulnerability and threat posture before they are allowed to communicate on the network. Because dangerous worms and viruses can infect and be spread by many different types of end systems, it is an important aspect of the architecture to be able to proactively protect the network environment from any dangerous end system.

With the advantage of the architectural approach to Secure Networks, IT organizations can deploy an Enterasys solution to ensure an effective and efficient business network environment.

Enterasys NAC Principles

The Enterasys NAC solution delivers all of the critical requirements to ensure a strong security posture and to protect critical business processes. Key technologies are leveraged to provide an open, scalable and comprehensive architecture for assessing, authenticating, authorizing and policing any end system connecting to the business communications network. The diagram below represents the Enterasys Secure Networks capabilities and their relationship to the Enterasys NAC solution.

Enterasys Secure Networks™ and NAC

Establish & Enforce Policy for users and devices to protect the enterprise	• Define Default policy for baseline access • Define Assessing policy for end-systems assessment • Define Quarantine/Failsafe policy for non compliant end-systems
Access Control of users and devices on the network	• Authorize users and machines (managed and unmanaged) • Detect specific end-systems like IP Phones, IP Cameras, etc • Check end-system compliance during network connection
Detect & Locate security intrusions and anomalous behavior	• Detect threats by (re)assessing end-systems periodically • Learn end-systems location during network connection • Scale by architecture (authentication-based)
Respond & Remediate identified security breaches	• Quarantine non compliant end-systems • Contain threats through granular policy • Provide self-service remediation
Proactive Prevention of attacks & compromises— everywhere, all the time	• Control threats pervasively • Mitigate threats based on severity • Change security posture instantly

From the Secure Networks architecture, Enterasys delivers a comprehensive NAC solution that addresses all critical requirements.

Open Architecture

Leveraging a longstanding commitment to standards-based technologies and open architected systems, Enterasys has designed its NAC solution to integrate and complement various NAC frameworks and assessment technologies. Enterasys is a Microsoft technology partner, and is committed to support and complement the Microsoft Network Access Protection (MNAP) strategy by leveraging 802.1X as a network authentication method. Microsoft NAP is Windows-centric and focuses on managed clients by requiring the presence of a NAP agent. Microsoft NAP leverages standards-based technologies such as DHCP, VPN, 802.1X and IPSec. Enterasys is a member of the Trusted Computing Group/Trusted Network Connect (TCG/TNC) working groups. The TCG/TNC is an industry standards group focused on the interoperability and integration of NAC-related technologies. Specific focus of the TCG/TNC is in the definition of a set of Application Programming Interfaces (APIs) to assist in the integration of various vendors' assessment technologies and network authentication and authorization. Enterasys has certified its Matrix™ and SecureStack switch families as appropriate Policy Enforcement Points (PEPs) with the TCG/TNC. In addition to working closely with industry groups focused on interoperability of NAC

technologies, Enterasys maintains partnerships with several vendors that offer leading end-system assessment technologies. Companies such as Tenable Network Security, Check Point Software and Symantec have important technologies that integrate with the Enterasys NAC solution.

An open approach to network infrastructure is also a critical aspect of an Enterasys NAC solution. Enterasys recognizes that networks can be made up of several vendors' infrastructure products. It is not a cost effective option to replace infrastructure products simply to get a working NAC solution. Enterasys' distribution-layer Matrix N-Series switches support multi-method and multi-user authentication capabilities. This means that a semi-intelligent or non-intelligent access-layer switch that does not support required end-system authentication for a NAC solution can be connected upstream to an Enterasys switch where individual user and device traffic flows can be authenticated using standards-based technologies. In addition, simple policies such as VLAN assignment can be enforced on any vendor's switch by using industry-standard dynamic VLAN assignment technology such as RFC3580. This allows end systems connecting to any vendor's access-layer switches to be included in an Enterasys NAC solution.

This openness of the architecture enables organizations to apply the best assessment technologies available with complete integration of authentication, authorization and enforcement of security and communication policies. There is no dependency in the Enterasys NAC solution restricting the assessment technologies that can be deployed, or the related end systems that can be assessed. It also enables organizations to evaluate NAC deployment without the added indirect cost of infrastructure replacement. An Enterasys NAC solution will increase the security posture of any network.

End System Inclusion

In order for a NAC solution to be effective, inclusion of all end systems in the network environment must be addressed. The Enterasys NAC solution takes an approach of supporting a diverse end-system environment, and providing integrated security and management regardless of what type of devices are connected to the business network.

Enterasys leverages two assessment models enabling NAC in a network environment. An agent-based assessment and an agent-less assessment are both critical to ensuring that any end system of any type can be included in the NAC process. There are several reasons why both assessment models are critical to a complete NAC solution. Security agents loaded onto managed end systems offer extensive assessment capabilities, but think about the types of end systems in a typical network that may not be able to load a software agent. What about end systems such as IP phones, security cameras or printers? If a security agent is not available for a device (or the operating systems running the device), an agent-less approach is the only way to assess the end system. Also consider end systems that could normally hold an agent, but are not under the control of the IT organization. In the case of guest networking (support for contractors, vendors, public, etc.), the desire may be to support minimal or specific network services, but to still ensure the safety and security of the network and the people using it. It is not enough to simply use a network usage policy to restrict the services a "guest user" is allowed to access. Because the guest is leveraging the same network infrastructure as the critical business users, it is important that proactive security measures are applicable to the guest just as they are to a "managed" user. This is another case where an agent-less approach to end system assessment can be critical to ensuring a comprehensive NAC strategy. Both the agent-based and the agent-less assessment models can be deployed and integrated together in the Enterasys NAC solution.

The agent-less model for end-system assessment does not require the installation of any sort of software security agent on the end system. This model supports various types of end systems such as PCs, IP phones, IP cameras, printers, etc., as well as multiple operating systems.

There are two variations of the agent-less model:

- **"Network-Based":** By leveraging a network-based vulnerability assessment engine such Tenable Network Security's Nessus, Enterasys NAC can provide integrated authentication, authorization and policy enforcement support. This model applies to traditional PC-type end systems, but is especially helpful in supporting the more diverse end system environments where nonuser-based end systems and end systems with non-traditional operating systems are present. The assessment requires no particular knowledge of the end system and is performed through remote communication with the end system. It should be noted that network-based assessment technologies require end-system firewall functions to be disabled.

- **"Applet-Based"** or **"Dissolvable Agent-Based":** By forcing the end system to download a Java applet, an ActiveX control or a dissolvable software agent, local assessment is performed while the end system is accessing a Web page. Enterasys leverages technology from Symantec and Check Point to perform end-system assessment from a software agent that is pushed to the end system through the network.

The agent-based model for end-system assessment requires the installation of a software agent on the end system. The software agent provides a "presence point" on the end system to communicate with the assessment server. The software agent typically provides the ability to check the presence and the configuration of antivirus, anti-spyware, personal firewall, and to perform deep system scans.

There are two variations of the agent-based model:

- **"Thin" Agent-Based Model:** The "thin" agent requires minimal resources and zero configuration on the client side (agents are preconfigured, installed and updated by the assessment server). The "thin" agent-based model is deployable in specific operating system environments based upon the assessment vendors' support for end systems.

- **"Thick" Agent-Based Model:** The "thick" agent provides a built in personal security solution such as personal firewall or host IDS. The "thick" agent-based model is typically Microsoft operating system-centric. It also may require significant resources (memory, CPU, etc.) on the client side. Enterasys NAC integrates with several technologies for "thick" agents:

  —Symantec with the Sygate Enterprise Protection product. Enterasys has certified Sygate Enterprise Protection across its product line (leveraging 802.1X/EAP).

  —Check Point with the Integrity product. Enterasys has certified Integrity across its product line (leveraging 802.1X/EAP).

  —Microsoft with the Network Access Protection (NAP) technology. Enterasys is actively testing NAP on Windows Vista and Windows "Longhorn" Server products, including 802.1X, DHCP and IPSec enforcement methods.

Leveraging industry-leading assessment technologies, the Enterasys NAC solution is positioned to include any type of end systems connected to the business network.

Multi-Context Authorization

Network authentication and authorization is a fundamental component of the Enterasys NAC solution. Enterasys implements mechanisms such as multi-user and multi-method Authentication/Authorization. Being able to authenticate multiple users (or devices) on a single physical switch port is important to the ability of authorizing differing services for different users and devices. An example of this would be a network switch port where an IP phone and a PC are both connected. The separate authentication of the two individual devices allows for network usage policies specific to the device and user to be authorized. Enterasys Matrix and SecureStack switches support multi-user authentication.

In addition, multi-user authentication allows the inclusion of switches without authentication capabilities in the infrastructure. Connecting non-authenticating switches to an Enterasys Matrix distribution-layer switch with multi-user authentication allows for individual users' traffic flows to be authenticated at the distribution layer. The result is a sort of "virtual port" authentication at the distribution layer of the network.

The flexibility of the authentication methods used by Enterasys switches allows fully integrated network authentication in all environments, including both user- and machine-centric end systems. Enterasys switches support IEEE 802.1X, MAC-based and Web-based authentication methods.

Specific end systems such as IP phones or IP cameras can be detected automatically on the network and placed in a particular communication environment. Other end systems, for example printers, can be authenticated and authorized based on vendor and device code fields (in the MAC address), leveraging OUI masking functionality.

When an end system connects to the network, network authentication is enforced and the Enterasys NAC controller detects this. Through the Enterasys NAC solution, the end system will be placed in an "assessing" state by authorizing and enforcing the end system using an "Assessing" policy role or VLAN. While in this policy role, the end system is assessed to determine health and threat. Once the assessment server has completed the evaluation of the end system, it will communicate the assessment result to the authorization process, which will either quarantine the end system if it is non-compliant or force the re-authentication and the authorization of the end system, allowing it to communicate on the business network based upon its business role. The authorization process includes multiple variables such as location, time of day, presence of preconfigured MAC Address overrides, presence of pre-configured MAC location locks, etc.

Policy Enforcement

When an end-system is quarantined because of an assessment of non-compliance, the quarantine policy role is enforced at the network level by changing the switch port configuration. The quarantine environment is configured in such a way that network traffic will be contained, according to security rules that have been previously determined. The Enterasys NAC solution leverages several key policy enforcement capabilities from the Secure Networks architecture.

- **Default policy for baseline access:** Apply a default policy on network ports where end systems are connected. This default policy provides basic access to the network and will be overridden post-authentication for known users and end systems.

- **Assessment policy for end-systems assessment:** Using an "Assessing" policy role, apply granular policy rules to end systems restricting network communication to the applications needed for assessment. It is critical to control the environment where the end systems are placed during the assessment process. The communication rules are determined by the policies of the business environment and the security requirements. An assessment policy role might provide Internet and e-mail access during the assessment process but prevent access to critical servers and applications. In other cases, the assessment policy role may completely restrict the access to network resources until the end system is assessed to be healthy and safe and is authorized to communicate on the network.

- **Quarantine/Failsafe policy for non-compliant end systems:** Apply granular policy rules to quarantine end systems through a "Quarantine" policy role. Once an end system has been determined to be non-compliant, it is placed in quarantine. The specific communication policies of the quarantine

environment are determined by the security policies of the organization. The "Failsafe" policy is used when the "state" of an end system can not be determined (when it can't be scanned for vulnerabilities or when authentication/authorization process is not available).

- **Organizational role policy for authorized end systems/users:** After an end system and user are determined to be safe and secure (from the assessment process), specific business role-based communication policy rules are enforced at the network connection point. These policy rules enforce how an end system may use the network and what applications and services can be accessed. Specific security rules are also enforced to ensure post-connect threat analysis and containment security on an ongoing basis.

Notification/Remediation

With the Enterasys NAC solution, network-based notification and remediation can be integrated. Notification is a critical aspect of a NAC solution where an end system could be put into a type of quarantine network policy configuration. If a user's PC is suddenly put into quarantine and not able to access the types of services that are expected by the user, it is important that information of this event is available to IT, but also that the user is directly notified of the cause of service disruption. In the event of a quarantine action against a user's end system, the user will likely believe that there is a network communication problem if they are not notified about the action that was taken. Implementing a NAC solution that can quarantine without notifying the user, may inadvertently increase calls to the IT help desk from users who are not able to access needed services—and don't understand why the services are unavailable. The Enterasys NAC solution integrates a user-notification capability in the event of a quarantine action by the NAC system. Once an end system is put into a quarantine policy state, notification may be achieved by redirecting the non-compliant end system's Web traffic to a remediation Web page. The Web page can be maintained by the IT organization and can include details about why the end system has been quarantined and how a user may "fix" issues that are causing the non-compliant state. Although the end system may be able to access the network and the remediation Web page, the communication is specifically provisioned through a set of policy rules to ensure that while the user can be notified, there is no danger to the rest of the network.

In order for a user whose end system network connection has been placed into a quarantine state to regain access to all needed network services, they must first remediate the problem that actually caused the quarantine to occur in the first place. This is not always available to the user. Consider the situation where a user is acting maliciously and threatening the network and its services. Remediation may not be desirable, and instead a persistent quarantine policy may be enforced to keep the user from causing any harm to the IT environment. In other cases, where a user or end system is unintentionally violating a pre-determined security policy, it is desirable to have the user notified and then allowed to remediate the problem himself. The key to this process is the ability of the network to enforce a usage policy that completely protects all critical resources and other users, but allows access to key remediation assets such as Web servers with security patches. The Enterasys NAC solution allows a quarantine policy to be established with a very specific set of policy rules that can filter and control network traffic with specific source and destination characteristics as well as specific application identifiers (e.g., UDP/TCP "ports"). In addition, the Enterasys NAC solution will support an unlimited number of different quarantine policy roles, which means that the solution can support varying degrees of network usage restrictions depending upon the severity of the state of non-compliance or security breach. This is different than many NAC solutions that only offer a VLAN "parking lot" for end systems that need to be quarantined. Using the granular policy capabilities of the Enterasys switches, a specific set of policy rules can be enforced allowing rate limited access to a specific application or Web service while filtering all other traffic from the network. Any real-time threats to the network environment can be controlled while the user is applying the correct remediation to get the end system into compliance to operate safely on the network. Once the user believes that remediation is complete, a request can be made to the Enterasys NAC solution to reassess the end system for compliance and if no further problem exists, a network usage policy grants access to the business services.

This integrated technology allows the Enterasys NAC solution to implement remediation for both agent-based and agent-less end-system environments. Additionally, registration mechanisms can be implemented so unauthenticated users are prompted to register their end system's physical (MAC) address. Network access is granted to registered users following end-system assessment as well as network administrator permission.

Compliance Reporting

An important aspect of a NAC solution is the ability to quickly view the state of the network environment. IT administrators need information on who and what is attaching to the network; where and at what time are the devices connecting; are the devices safe and secure; are the users of the devices posing any threat to the network environment. Comprehensive real-time and historical information on the end systems and users communicating on the network is critical to understanding the state of compliance to any pre-determined policy.

The Enterasys NAC solution maintains a comprehensive set of important data that can be leveraged to quickly determine network usage and the threats and vulnerabilities posed by end systems of any type. Another important aspect of the Enterasys NAC solution is the ability to look at historical data on any end system. The Enterasys NAC solution can report on not only where an end system is connected currently, but also where it has been connected in the past, as well as who was using the end system and whether or not it was in compliance at the time. The data collected from the Enterasys NAC solution includes:

- 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*

From the data collected by the Enterasys NAC solution, IT administrators can account for end-system compliance in real time as well as historically. The reporting capabilities of the Enterasys NAC solution allow IT organizations to report on end-system compliance, justify technology expenditures and provide regulatory compliance information when required.

Enterasys NAC in Action

The Enterasys NAC solution involves several technologies and products cooperating in a fully integrated fashion to provide a comprehensive approach to proactive protection as part of an overall security architecture.

The following scenarios detail operation of the Enterasys NAC solution in various network environments.

Scenario 1: Intelligent Wired Access Edge

In the intelligent wired access edge use scenario, the edge switches that compose the network access layer are capable of providing authentication (802.1X, web-based, or MAC) for connecting end-systems. They are also capable of being an authorization point for these end-systems through Enterasys policy and/or dynamic VLAN assignment as specified in RFC 3580. For this use scenario, the NAC Gateway appliance is deployed for out-of-band network access control, leveraging the intelligent infrastructure devices in the access edge as the authorization point for connecting end-systems. It is important to note that Enterasys policy-enabled switches provide increased security over third-party switches that support RFC 3580. By using port-level granular traffic control, users quarantined with Enterasys policy can be restricted from communicating with other quarantined users, even if co-located on the same VLAN. In a Quarantine VLAN as implemented on third-party RFC 3580 capable switches, a quarantined user poses a threat to other quarantined users within the same Quarantine VLAN because the authorization point is usually implemented at the exit point of the VLAN via Access Control Lists (ACLs). In other words, Enterasys prevents systems with an unhealthy security posture from cross-infecting each other while in quarantine.
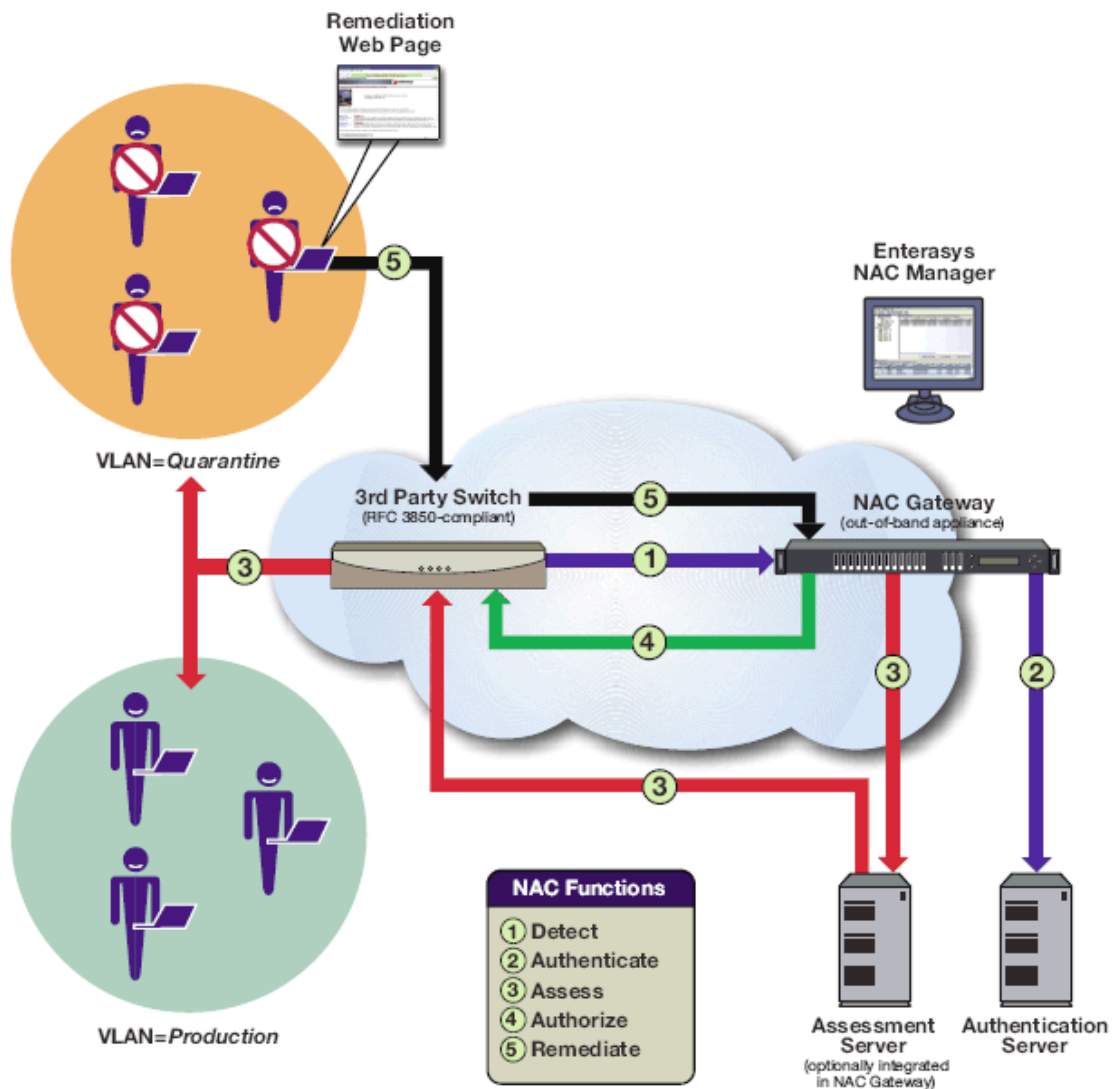
Policy-Enabled Edge

The following figure illustrates how the Enterasys NAC Gateway and the other Enterasys NAC components work together in a network with policy-enabled edge switches to provide a comprehensive NAC solution.
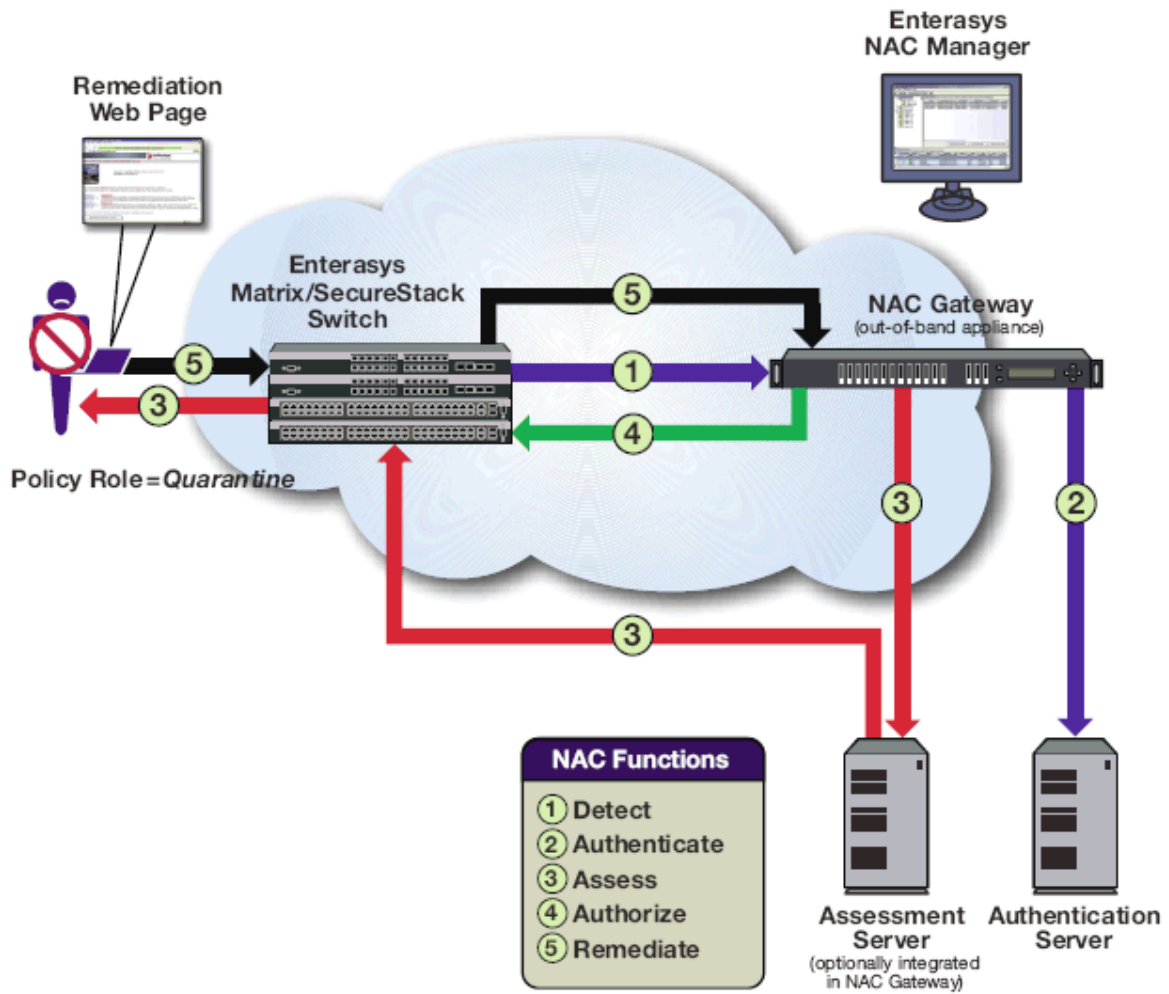
RFC 3580 Capable Edge

In this figure the Enterasys NAC Gateway and the other Enterasys NAC components provide network access control for a network with third-party switches that support RFC 3580.

Remediation Web Page

Enterasys NAC Manager

VLAN=Quarantine

3rd Party Switch (RFC 3850-compliant) ⑤ **NAC Gateway** (out-of-band appliance)

① ④ ③ ②

VLAN=Production

NAC Functions
① Detect
② Authenticate
③ Assess
④ Authorize
⑤ Remediate

Assessment Server (optionally integrated in NAC Gateway)   **Authentication Server**

Scenario 1 Implementation

In the intelligent wired edge use scenario, the five NAC functions are implemented in the following manner:

1. **Detection** – The user's end-system connects to the network. The edge switch sends a RADIUS authentication request (802.1X, web-based, or MAC authentication) with the associated credentials to the NAC Gateway.

2. **Authentication** – If the end-system is authenticating to the network using 802.1X or web-based authentication, the NAC Gateway proxies the RADIUS authentication request to a backend authentication (RADIUS) server to validate the identity of the end user/device. For end-systems that are MAC authenticating to the network, the NAC Gateway can be configured to either proxy the MAC authentication requests to the RADIUS server or locally authorize MAC authentication requests. If only MAC authentication is deployed on the network, and the NAC Gateway is configured to locally authorize MAC authentication requests, a backend RADIUS server is not required for the Enterasys NAC solution.

3. **Assessment** – After the identity of the end-system or end user is validated via authentication, the NAC Gateway requests an assessment of the end-system according to predefined security policy parameters. The assessment can be agent-based or agent-less, and is executed locally by the NAC Gateway's assessment functionality and/or remotely by a pool of assessment servers.

4. **Authorization** – Once authentication and assessment are complete, the NAC Gateway allocates the appropriate network resources to the end-system based on authentication and/or assessment results. For Enterasys policy-enabled edge switches, the NAC Gateway formats information in the RADIUS authentication messages that directs the edge switch to dynamically assign a particular policy to the connecting end-system. For RFC 3580-capable edge switches, the NAC Gateway formats information in the RADIUS authentication messages (in the form of RFC 3580 VLAN Tunnel attributes) that directs the edge switch to dynamically assign a particular VLAN to the connecting end-system. If authentication fails and/or the assessment results indicate a noncompliant end-system, the NAC Gateway can either deny the end-system access to the network by sending a RADIUS access reject message to the edge switch, or quarantine the end-system by assigning a Quarantine policy or VLAN to the end-system on the edge switch.

5. **Remediation** – When the quarantined end user opens a web browser to any web site, its traffic is dynamically redirected to a Remediation web page that describes the compliance violations and provides remediation steps for the user to execute in order to achieve compliance. After taking the appropriate remediation steps, the end user clicks on a button on the web page to reattempt network access, forcing the re-assessment of the end-system. At this point, the Enterasys NAC solution transitions the end-system through the entire NAC cycle of detection, authentication, assessment, and authorization, re-assessing the security posture of the end-system to determine if the remediation steps were successfully followed. If the end-system is now compliant with network security policy, the NAC Gateway authorizes the end-system with the appropriate policy or VLAN. If the end-system is not compliant, the end-system is restricted access to the network and the process starts again.

It is important to note that if the wired edge of the network is non-intelligent (unmanaged switches and hubs) and is not capable of authenticating and authorizing locally connected end-systems, it is possible to augment the network topology to allow implementation of out-of-band NAC with the NAC Gateway. This can be accomplished without replacing the physical edge of the network, by adding an intelligent edge switch that possesses specialized authentication and authorization features.
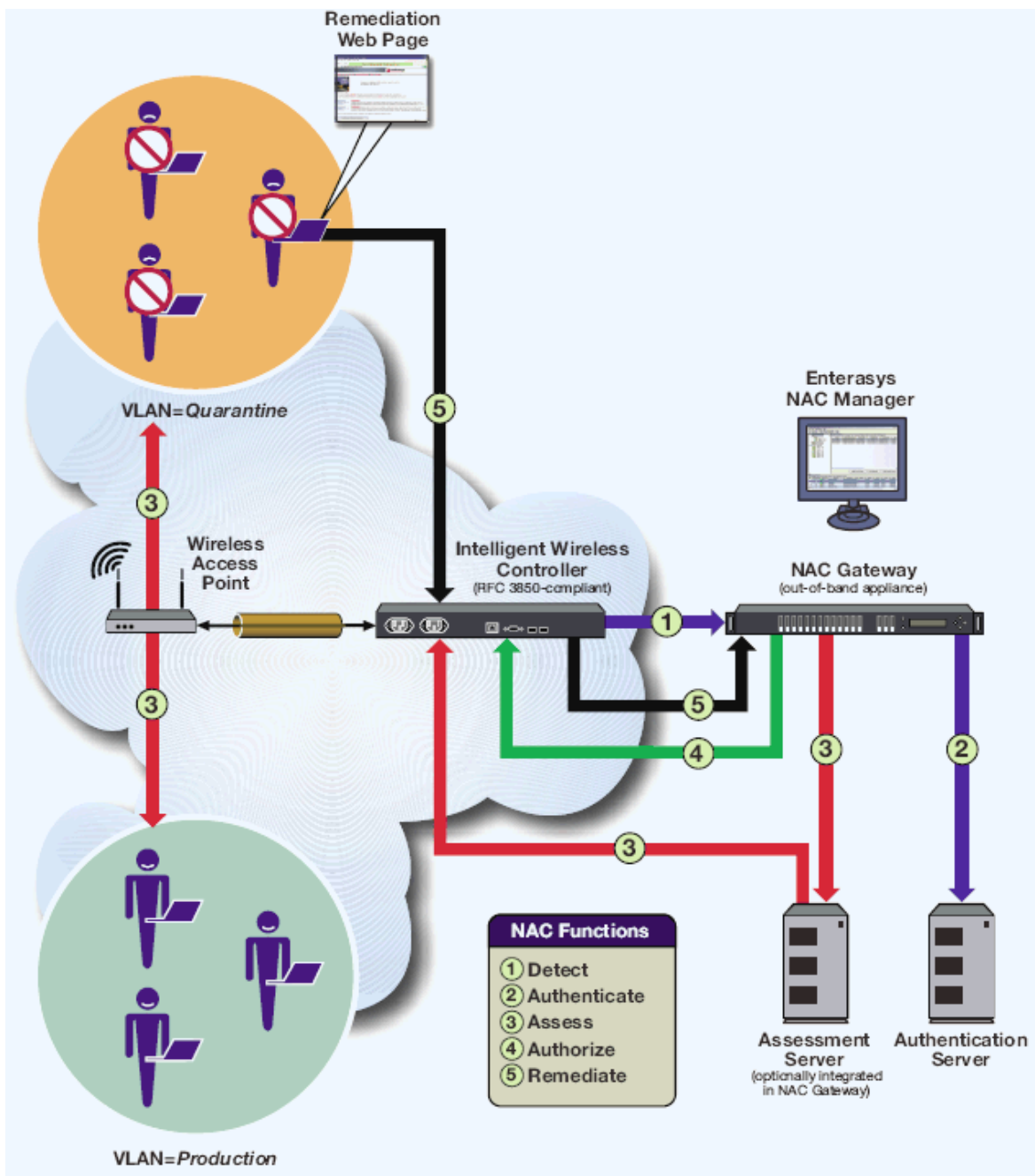
Enterasys Matrix N-series switches are capable of authenticating and authorizing numerous end-systems connected on a single port through its Multi-User Authentication (MUA) functionality and may be positioned upstream from non-intelligent third-party edge devices to act as the intelligent edge on the network. The Matrix N-series switch is capable of authenticating and authorizing multiple devices connected to a single port for a variety of network topologies, ranging from an IP phone cascaded with a PC on a single Matrix N-series port, to a stack of non-intelligent edge switches uplinked to a single Matrix N-series port where over 1000 end-systems connect. In this configuration, the Matrix N-series acts as the intelligent edge switch on the network, although not physically located at the access edge. Each individual end-system is authenticated using 802.1X, web-based, and/or MAC authentication and is subsequently authorized on the Matrix N-series inter-switch link to the access edge. By provisioning access to network resources on the Matrix N-series using MUA, end-system traffic destined to adjacent switches on the network can be securely contained with policy at the Matrix N-series port.

Scenario 2: Intelligent Wireless Access Edge

In the intelligent wireless access edge use scenario, thick Access Points (APs) or wireless switches with thin APs provide authentication and authorization for connecting end-systems. For this use scenario, the NAC Gateway appliance is deployed for out-of-band network access, leveraging the intelligent wireless infrastructure devices as the authorization point for connecting end-systems.
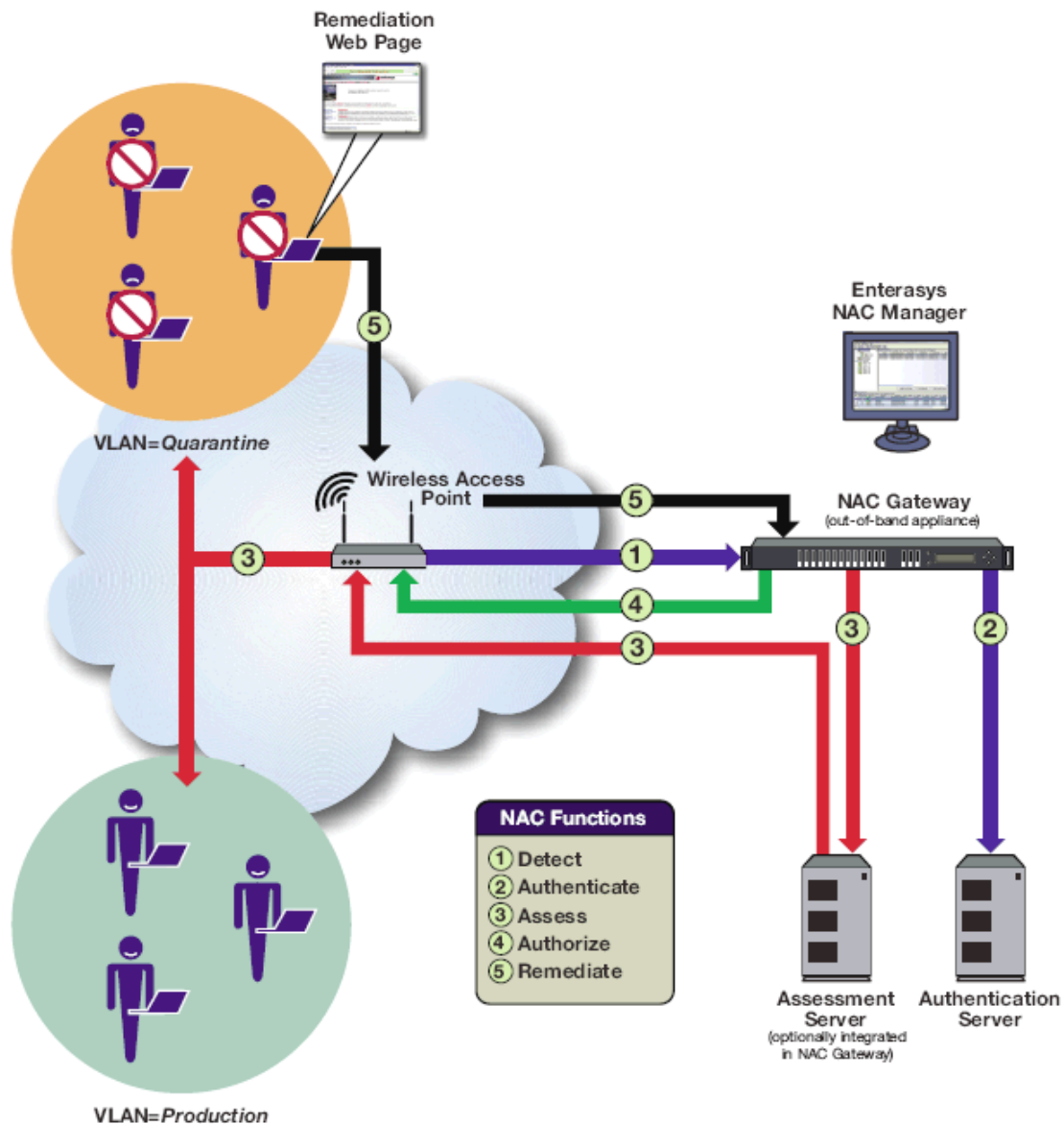
Thin Wireless Edge

In a thin wireless deployment, wireless switches tunnel end-system traffic to and from access points deployed on the network. Most thin wireless deployments are categorized under the intelligent wireless access edge use scenario because the wireless switches are capable of providing authentication (802.1x, web-based, or MAC) and are also capable of being an authorization point either through dynamic VLAN assignment as specified in RFC 3580 or application of user-based ACLs or policy. The following figure illustrates how the Enterasys NAC Gateway and the other Enterasys NAC components work together in a thin wireless deployment.

Remediation Web Page

VLAN=Quarantine

Wireless Access Point

Intelligent Wireless Controller
(RFC 3850-compliant)

NAC Gateway
(out-of-band appliance)

Enterasys NAC Manager

VLAN=Production

NAC Functions
1. Detect
2. Authenticate
3. Assess
4. Authorize
5. Remediate

Assessment Server
(optionally integrated in NAC Gateway)

Authentication Server

Thick Wireless Edge

In a thick wireless deployment, access points forward wireless end-system traffic directly onto the wired infrastructure without the use of a wireless switch. Thick wireless deployments may or may not be categorized under the intelligent wireless access edge use scenario depending on the functionality supported by the APs. The following figure illustrates how the Enterasys NAC Gateway and the other Enterasys NAC components provide network access control in a thick wireless deployment.

Remediation
Web Page

Enterasys
NAC Manager

VLAN=*Quarantine*

Wireless Access
Point

NAC Gateway
(out-of-band appliance)

NAC Functions

1. Detect
2. Authenticate
3. Assess
4. Authorize
5. Remediate

Assessment
Server
(optionally integrated
in NAC Gateway)

Authentication
Server

VLAN=*Production*

Scenario 2 Implementation

In the intelligent wireless access edge use scenario, the five NAC functions are implemented in the following manner:

1. **Detection** – The user's end-system connects to the network. The wireless switch or thick AP sends a RADIUS authentication request (802.1X, web-based, or MAC authentication) with the associated credentials to the NAC Gateway.

2. **Authentication** – If the end-system is authenticating to the network using 802.1X or web-based authentication, the NAC Gateway proxies the RADIUS authentication request to a backend authentication (RADIUS) server to validate the identity of the end user/device. For end-systems that are MAC authenticating to the network, the NAC Gateway may be configured to either proxy the MAC authentication requests to the RADIUS server, or locally authorize MAC authentication requests. If only MAC authentication is deployed on the network and the NAC Gateway is configured to locally authorize MAC authentication requests, a backend RADIUS server is not required with the Enterasys NAC solution.

3. **Assessment** – After the identity of the end-system or end user is validated via authentication, the NAC Gateway requests an assessment of the end-system according to predefined security policy parameters. The assessment can be agent-based or agent-less, and is executed locally by the NAC Gateway's assessment functionality and/or remotely by a pool of assessment servers.

4. **Authorization** – Once authentication and assessment are complete, the NAC Gateway allocates the appropriate network resources to the end-system based on authentication and/or assessment results. For Enterasys policy-enabled wireless switches and access points, the NAC Gateway formats information in the RADIUS authentication messages that directs the edge switch to dynamically assign a particular policy to the wireless end-system

on the wireless switch or AP, depending on the type of wireless implementation. For RFC 3580-capable wireless switches and APs, the NAC Gateway formats information in the RADIUS authentication messages (in the form of RFC 3580 VLAN Tunnel attributes) that directs the edge switch to dynamically assign a particular VLAN to the wireless end-system. If authentication fails and/or the assessment results indicate a noncompliant end-system, the NAC Gateway can either deny the end-system access to the network by sending a RADIUS access reject message, or quarantine the end-system by assigning a Quarantine policy or VLAN to the wireless end-system.
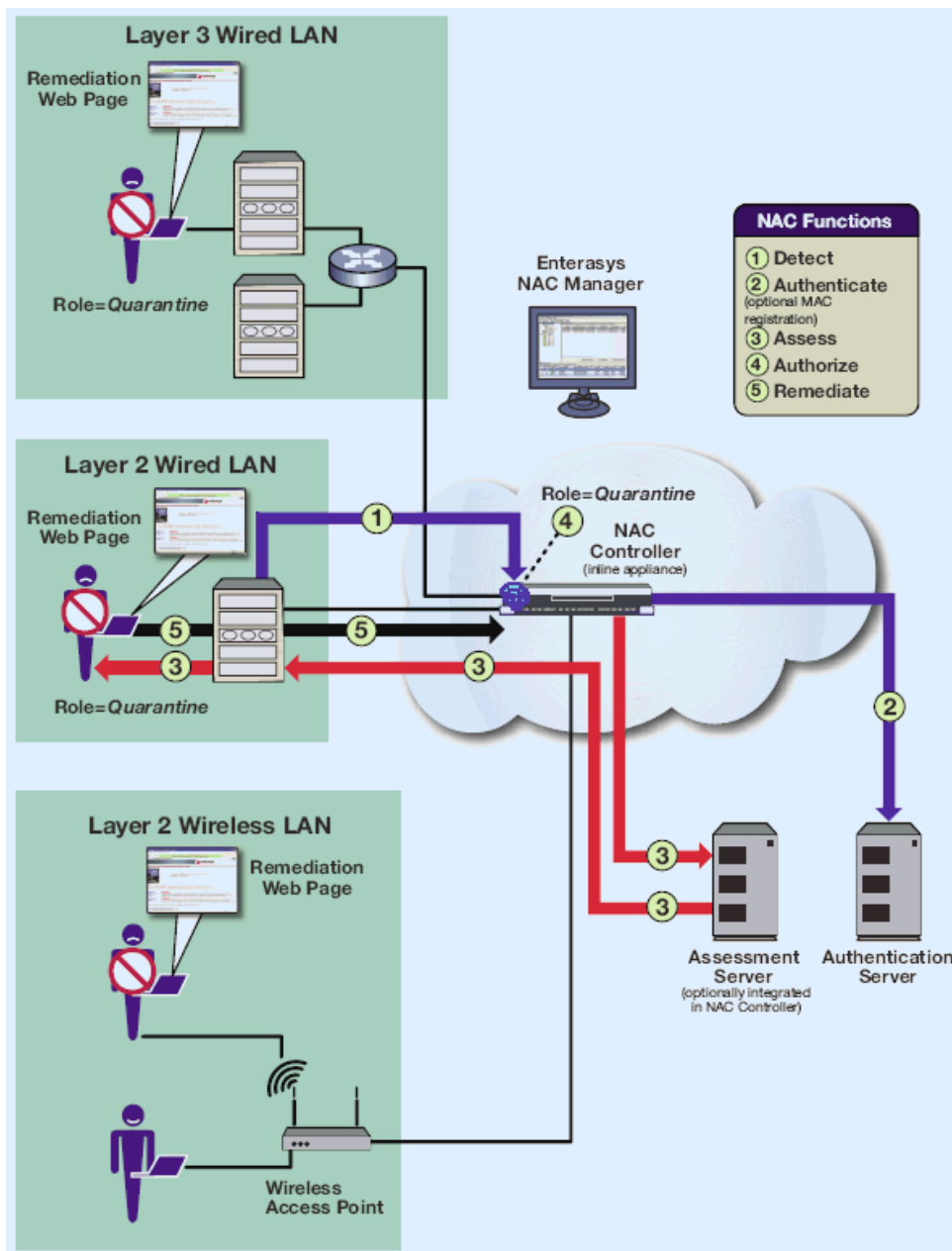
5. **Remediation** – When the quarantined end user opens a web browser to any web site, its traffic is dynamically redirected to a Remediation web page that describes the compliance violations and provides remediation steps for the user to execute in order to achieve compliance. After taking the appropriate remediation steps, the end user clicks on a button on the web page to reattempt network access, forcing the re-assessment of the end-system. At this point, the Enterasys NAC solution transitions the end-system through the entire NAC cycle of detection, authentication, assessment, and authorization, re-assessing the security posture of the end-system to determine if the remediation techniques were successfully followed. If the end-system is now compliant with network security policy, the NAC Gateway authorizes the end-system with the appropriate access policy. If the end-system is not compliant, the end-system is restricted access to the network and the process starts again.

It is important to note that if the wireless edge of the network is non-intelligent and not capable of authenticating and authorizing wireless end-systems, it is possible to augment the network topology to implement out-of-band NAC with the NAC Gateway. This can be accomplished without replacing the physical edge of the network, by adding an intelligent edge switch that possesses specialized authentication and authorization features.

Enterasys Matrix N-series switches are capable of authenticating and authorizing numerous end-systems connected on a single port through Multi-User Authentication (MUA), and may be positioned upstream from non-intelligent third-party wireless APs to act as the intelligent edge on the network. The Enterasys Matrix N-series switch is capable of authenticating and authorizing over 1000 end–systems uplinked to a single Matrix N–series port from an AP, a set of APs, or wireless switches. In this configuration, the Matrix N–series acts as the intelligent edge switch on the network, although not physically located on the access edge. By provisioning access to network resources on the Matrix N-series via MUA, end-system traffic destined to adjacent switches on the network can be securely contained at the Matrix N-series port.

Scenario 3: Non-intelligent Access Edge (Wired and Wireless)

In the non-intelligent access edge use scenario, the edge switches and access points that compose the network access layer are not capable of authenticating and authorizing the connecting end-systems on the network. In this scenario, inline NAC is implemented by positioning the NAC Controller at a strategic point in the network topology, as the authorization point for end-system traffic enforcement. The NAC Controller may be positioned directly within the VLAN where end-systems are connected or across one or more routed boundaries. When the NAC Controller is positioned within the VLAN where end-systems are connected, each device is uniquely identified by its associated MAC address. When the NAC Controller is positioned across a routed boundary (for example, behind a WAN router located in an enterprise's central site), each end-system is identified by its associated IP address. The following figure illustrates how the NAC Controller and the other Enterasys NAC components work together in the non-intelligent edge to provide network access control.

Layer 3 Wired LAN

Remediation
Web Page

Role=Quarantine

Layer 2 Wired LAN

Remediation
Web Page

Role=Quarantine

Layer 2 Wireless LAN

Remediation
Web Page

Wireless
Access Point

Enterasys
NAC Manager

NAC Functions
① Detect
② Authenticate
(optional MAC
registration)
③ Assess
④ Authorize
⑤ Remediate

Role=Quarantine

NAC
Controller
(inline appliance)

Assessment
Server
(optionally integrated
in NAC Controller)

Authentication
Server

Scenario 3 Implementation

In the non-intelligent access edge use scenario, the five NAC functions are implemented in the following manner:

1. **Detection** – The user's end-system connects to the network and transmits data traffic onto the network that traverses the NAC Controller. This traffic is sourced from a MAC address or IP address not previously seen by the controller.

2. **Authentication** – One of two configurations may be implemented on the NAC Controller for end user authentication. Authentication can be disabled altogether, trusting that the downstream infrastructure devices authenticated the end-system to the network (802.1X authentication to the wireless LAN, web-based authentication to the wired LAN). Alternatively, MAC registration can be implemented, where an end user username and password and/or sponsor username and password must be validated against a backend LDAP-compliant database before network access is permitted.

3. **Assessment** – After the identity of the end-system or end user is validated by authentication, the NAC Controller requests an assessment of the end-system according to predefined security policy parameters. The assessment can be agent-based or agent-less, and is executed locally by the NAC Controller's assessment functionality and/or remotely by a pool of assessment servers.

4. **Authorization** – Once authentication and assessment are complete, the NAC Controller allocates the appropriate network resources to the end-system

based on authentication and/or assessment results. This is implemented locally on the NAC Controller by assigning a policy to traffic sourced from this end-system. If authentication fails and/or the assessment results indicate a noncompliant end-system, the NAC Controller can either deny the end-system access to the network or quarantine the end-system by specifying a particular policy on the NAC Controller.

5. **Remediation** – When the quarantined end user opens a web browser to any web site, its traffic is dynamically redirected to a Remediation web page that describes the compliance violations and provides remediation steps for the user to execute in order to achieve compliance. After taking the appropriate remediation steps, the end user clicks on a button on the web page to reattempt network access, forcing the re-assessment of the end-system. At this point, the Enterasys NAC solution transitions the end-system through the entire NAC cycle of detection, authentication, assessment, and authorization, re-assessing the security posture of the end-system to determine if the remediation techniques were successfully followed. If the end-system is now compliant, the NAC Controller authorizes the end-system with the appropriate access policy. If the end-system is not compliant, the end-system is restricted access to the network by assigning a policy to the end-system on the NAC Controller, and the process starts again.

Scenario 4: VPN Remote Access

In the VPN remote access use scenario, VPN concentrators act as a termination point for remote access VPN tunnels into the enterprise network. For this use scenario, the NAC Controller appliance is deployed to authorize connecting end-systems on the network and implement network access control. The following figure illustrates how the Enterasys NAC Controller and the other Enterasys NAC components work together in a VPN remote access deployment to provide a comprehensive NAC solution.
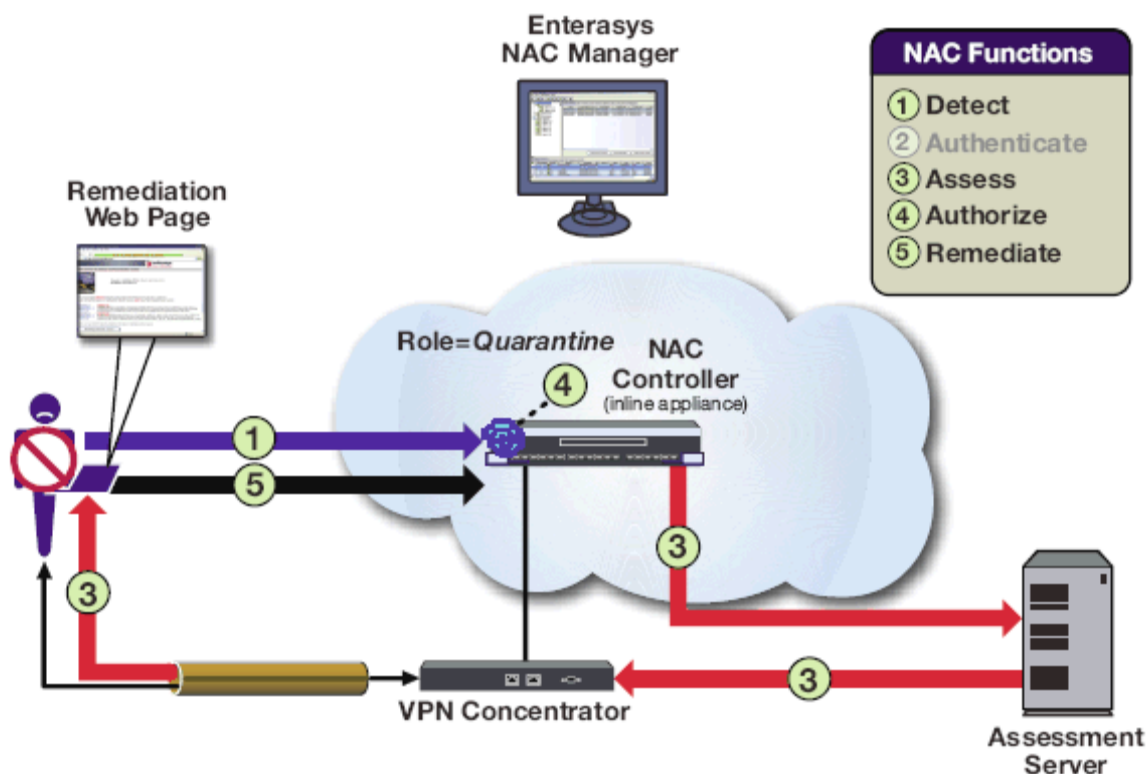
Scenario 4 Implementation

In the VPN remote access use scenario, the five NAC functions are implemented in the following manner with the deployment of the Enterasys NAC Controller for inline network access control.

1. **Detection** – The user's end-system successfully establishes a VPN tunnel with the VPN concentrator, and the VPN concentrator transmits unencrypted data traffic onto the network that traverses the NAC Controller. This traffic is sourced from an IP address not previously seen by the controller.

2. **Authentication** – Authentication is most likely disabled altogether on the NAC Controller, trusting that the downstream VPN concentrator authenticated the connecting user.

3. **Assessment** – The NAC Controller requests an assessment of the end-system according to predefined security policy parameters. The assessment can be agent-based or agent-less, and is executed locally by the NAC Controller's assessment functionality and/or remotely by a pool of assessment servers.

4. **Authorization** – Once authentication and assessment are complete, the NAC Controller allocates the appropriate network resources to the end-system based on authentication and/or assessment results. This is implemented locally on the NAC Controller by assigning a policy to traffic sourced from the end-system. If authentication fails and/or the assessment results indicate a noncompliant end-system, the NAC Controller can either deny the end-system access to the network, or quarantine the end-system by assigning a particular policy on the controller.

5. **Remediation** – When the quarantined end user opens a web browser to any web site, its traffic is dynamically redirected to a Remediation web page that describes the compliance violations and provides remediation steps for the user to execute in order to achieve compliance. After taking the appropriate remediation steps, the end user clicks on a button on the web page to reattempt network access, forcing the re-assessment of the end-system. At this point, the Enterasys NAC solution transitions the end-system through the entire NAC cycle, re-assessing the security posture of the end-system to determine if the remediation techniques were successfully followed. If the end-system is now compliant with network security policy, the NAC Controller authorizes the end-system with the appropriate access policy. If the end-system is not compliant, the end-system is restricted access to the network by assigning a policy to the end-system on the NAC Controller, and the process starts again.

Enterasys delivers a comprehensive set of technologies to enable a comprehensive NAC solution. The table below shows the technologies required to meet the needs of a NAC solution and the Enterasys products that deliver the required technologies.

Network Access Control Requirement	Technologies/Features		Enterasys Products
Open Architecture	• IEEE • IETF • Microsoft NAP • TCG/TNC	• Multi-User Authentication • Distribution-Layer Policy • Software APIs • 3rd Party Assessment	• Matrix/SecureStack Switches • NetSight Management Software • Enterasys NAC Gateway • NetSight NAC Manager
End System Inclusion	• IEEE 802.1X • Mac-Based Authentication • Web-Based Authentication • CEP Detection	• Agent-Based Assessment • Agent-Less Assessment	• Matrix/SecureStack Switches • Enterasys NAC Gateway • NetSight NAC Manage
Multi-Context Authorization	• IEEE 802.1X Authentication • Mac-Based Authentication • Web-Based Authentication • CEP Detection	• OUI Masking/Authentication • Multi-User Authentication • Role-Based Policy Configuration	• Matrix/SecureStack Switches • NetSight Policy Management • Enterasys NAC Gateway
Policy Enforcement	• Traffic Filters • Rate Limits • Flow Isolation • Dynamic Policy Enforcement	• Intrusion Detection • Flow Isolation • Threat Mitigation	• Matrix/SecureStack Switches • NetSight Policy Management • Enterasys NAC Gateway
Notification and Remediation	• Layer 4 Policy Rules • Web Redirect • Application Filtering • Dynamic Policy Enforcement	• End-System Registration • User-Initiated Reassessment	• Matrix/SecureStack Switches • NetSight Policy Management • Enterasys NAC Gateway
Compliance Reporting	• End-System Location • End-System Assessment State • User Identity	• Historical – Location/Assessment State • Scan History	• Enterasys NAC Gateway • NetSight NAC Manager

Summary

Network Access Control is a key component of any network security solution. The need to understand the identity and health of an end system before it connects to the network is critical in ensuring business continuity and overall security. Enterasys offers an open-architecture, standards-based approach to Network Access Control and delivers a solution that meets the most critical security needs of any organization.

The open-architecture approach of the Enterasys NAC solution enables an organization to use best-of-breed assessment technologies from industry-leading vendors and assure that they will fully integrate with the authentication, authorization and policy-enforcement capabilities of Secure Networks.

Deploying an Enterasys NAC solution will ensure visibility and control of whom and what is allowed to connect to the network. Dangerous and non-compliant end systems are isolated and kept from negatively impacting the business processes that the network supports. The Enterasys NAC solution provides a comprehensive approach to the requirements of assessing any end system, authorizing network usage based on a variety of important context, enforcing security and business communication policies, notifying out-of-compliance end users and assisting them in safe and secure remediation, and providing significant compliance data.

With an Enterasys NAC solution, there is no need to replace installed infrastructure products. Leveraging its innovative multi-method and multi-user authentication, as well as VLAN-based policy enforcement (RFC3580), Enterasys can implement a comprehensive NAC solution within your current network environment. Enterasys' commitment to an open-architecture and standards-based approach delivers the most cost-effective, comprehensive NAC deployment available today.

And because the Enterasys NAC solution is an integral part of the Secure Networks architectural approach to network security, customers can be assured of both pre-connect and post-connect security through proactive and reactive technologies—all integrated into one easy-to-manage architecture.

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

Thought Leadership
Patented Innovation

enterasys®
S e c u r e   N e t w o r k s™

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