

**End Node Security and Network Access
Management - Deciding Among
Different Strategies**

Whitepaper
v1.1

February 2006

Franjo Majstor
franjo@employees.org

**End Node Security and Network Access Management - Deciding Among
Different Strategies**

Index of Content

1. Introduction.....	4
1.1 Acronym Jungle	4
1.2 Problem Definition.....	4
2. End Node Security Solutions.....	5
2.1. Evolution	5
2.2. Trusted Network Connect Specification	5
2.2. Network Admission Control.....	9
2.2.1. Network Admission Control Overview	9
2.2.2. NAC Analysis	11
2.3. Network Access Protection	12
2.3.1. Network Access Protection Overview	12
2.3.2. Quarantine Enforcement Clients.....	15
2.3.3. NAP Analysis.....	16
2.4. Sygate Network Access Control	17
2.4.1. Sygate Network Access Control Overview	17
2.4.2. SNAC Analysis	18
2.5. Automated Quarantine Engine	18
2.5.1. Automated Quarantine Engine Overview	18
2.5.2. AQE Analysis	19
2.6. TippingPoint Quarantine Protection	20
2.6.1. TippingPoint Quarantine Protection Overview	20
2.6.2. TQP Analysis	21
2.7. Hybrid Solutions.....	21
3. End Node Security Solutions Comparison	22
4. Future Directions	23
5. Summary.....	24
6. List of Acronyms	25
7. References	25

Index of Exhibits

Exhibit 1: Trusted Network Connect Architecture	6
Exhibit 2: Layered Trusted Network Connect Architecture	7
Exhibit 3: TNC Architecture with Provisioning and Remediation Layer.....	8
Exhibit 4: Network Admission Control Architecture Components	10
Exhibit 5: NAC End Node Protocol Stack.....	11
Exhibit 6: NAC Access Control Flow	12
Exhibit 7: Network Access Protection Architecture	13
Exhibit 8: Interaction between Network Access Protection Components	14
Exhibit 9: NAP Client Architecture	16
Exhibit 10: SNAC Solution Overview.....	18
Exhibit 11: Automated Quarantine Engine from Alcatel	19
Exhibit 12: TippingPoint Quarantine Protection Action Steps.....	20
Exhibit 13: Private VLAN (PVLAN) Operation	21
Exhibit 14: End Node Security Solutions Comparison Table-1	22
Exhibit 15: End Node Security Solutions Comparison Table-2	23

1. Introduction

1.1 *Acronym Jungle*

Like almost in any industry, in the networking industry there are far too many technical acronyms. Security terminology is unfortunately not immune to that neither, and combined security terms with networking terms resulted in almost catastrophic amount of acronyms together and is most probably not going to be in the future neither. Therefore, an advance apology is given to beginner readers of this chapter with a recommendation to check the references and whenever reading one of the new terms in the latest "acronym jungle", to jump to an end of the article, where all acronyms are spelled out at one place.

1.2 *Problem Definition*

It would be easy, if acronyms would be the only problem. Nowadays, modern networks are amongst the others responsible for employee productivity, product manufacturing, receiving orders from customers and as such are business-critical systems that are, if not available or under attack, resulting in a denial of service, theft of sensitive information or exposure to regulatory penalties. Traditional perimeter-focused security architectures are today powerless against the infected endpoints that connect to enterprise networks from various different locations. Information security practitioners are dealing almost on daily basis with situations like the following. Sales persons when on the road frequently connects to an insecure hotel network or other public Internet service where their laptops could get exposed to a malware infection. Enterprise information technology departments have defined policies and equipped the salesperson's laptop with protections such as the latest Anti-Virus software, personal firewalls, host intrusion prevention, operating system configurations, and patches to protect the system against compromise. Unfortunately, those protections can be turned off, uninstalled, or may simply have never been updated to the laptop, leaving the salesperson's computer unprotected. Company guests and visitors would often use offered hospitality to connect via internal enterprise wired or wireless network to the Internet. Their portable equipment could in case they are not up to speed with a latest viral protection, be already compromised and as such could cause the compromise to the rest of the network resources they are connecting through.

These are just two examples out of the many and reality in the latest vulnerability statistics of the most popular computing equipment software platforms shows us that most of the time an unintentional user or guest visitor network usage caused an avalanche of problems to the rest of the network resources that are crucial for running the business.

Several initiatives started from the industry vendors and organizations have already addressed some problems of the individual endpoint security with applications like anti-virus agents and personal firewalls, while the connectivity of the end node to the network infrastructure got already a while ago the end node authentication via 802.1x protocol. However all of those mechanisms individually have been proven not to be sufficient to stop problems of the network resources under a threat so far. Hence, a group of solution efforts from the leading

market vendors as well as standardization organizations came out with several individual solutions to address the burning issue of both - integrity and policy compliancy of the end node towards accepted rules of behavior from the network infrastructure. Information security practitioners that are already today and will be even more in the future exposed to an end node to an infrastructure interaction problem, should be able to understand the essence of the issue and be capable to find a proper end node to infrastructure interactivity security mechanism that would fit their business environment.

2. End Node Security Solutions

2.1. Evolution

Initiatives to solve the end node causing availability, integrity and confidentiality problems to the rest of the network started by several combined vendor solutions, so no wonder that networking vendor, Cisco Systems as well as operating system vendor Microsoft came with their unique proposals. Several other end node antiviral software vendors joined the initiatives of both, while some other created their own solutions. Overall it has created the panache of closed efforts on the market locking the choice around the particular vendor solution. To move out of the closed group proposals, the Trusted Computing Group (TCG) organization of vendors came out with Trusted Network Connect (TNC) specification that describes the problem and gives the framework for the vendor interoperable solution. Even it came as an umbrella answer solution later, it well explains the detailed individual components of the system with their roles and functions, so it is the best to start with it explaining the concept of the future end node security solutions.

2.2. Trusted Network Connect Specification

The TNC architecture and specifications were developed with a purpose of ensuring the interoperability amongst the individual components for the solution provided by different vendors. The aim of the TNC architecture is to provide a framework within which consistent and useful specifications can be developed to achieve a multi-vendor network standard that provides the following four features:

- 1) *Platform Authentication*: the verification of a network access requestor's proof of identity of their platform and the integrity-status of that platform.
- 2) *Endpoint Policy Compliance (Authorization)*: establishing a level of 'trust' in the state of an endpoint, such as ensuring the presence, status, and upgrade level of mandated applications, revisions of signature libraries for anti-virus and intrusion detection and prevention system applications, and the patch level of the endpoint's operating system and applications. Note that policy compliance can also be viewed as *authorization*, in which an endpoint compliance to a given policy set result in the endpoint being authorized to gain access to the network.

3) *Access Policy*: ensuring that the endpoint machine and/or its user authenticates and establishes their level of trust before connecting to the network, leveraging a number of existing and emerging standards, products, or techniques.

4) *Assessment, Isolation and Remediation*: ensuring that endpoint machines not meeting the security policy requirements for 'trust' can be isolated or quarantined from the rest of the network, and if possible an appropriate remediation applied, such as upgrading software or virus signature databases to enable the endpoint to comply with security policy and become eligible for connection to the rest of the network.

Basic TNC Architecture is illustrated in Exhibit 1.

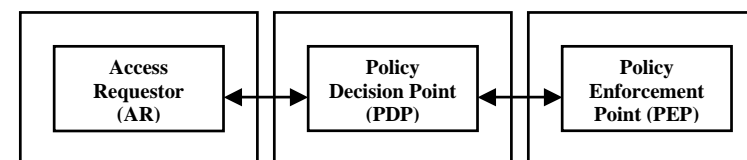


Exhibit 1: Trusted Network Connect Architecture

The entities within the architecture are: Access Requestor (AR), Policy Enforcement Point (PEP) and Policy Decision Point (PDP).

1. *Access Requestor (AR)*: The AR is the entity seeking access to a protected network.
2. *Policy Decision Point (PDP)*: The PDP is the entity performing the decision-making regarding the AR's request, in light of the access policies.
3. *Policy Enforcement Point (PEP)*: The PEP is the entity that enforces the decisions of the PDP regarding network access.

All entities and components in the architecture are logical ones, not physical ones. An entity or component may be a single software program, a hardware machine, or a redundant and replicated set of machines spread across a network, as appropriate for its function and for the deployment's needs. Entities of the TNC Architecture are structured in the layers. Layered TNC Architecture levels that are illustrated in Exhibit 2 are the following:

1. *The network access layer*: Components whose main function pertains to traditional network connectivity and security. Even though the name might imply, this layer does not refer to OSI network layer only but may support a variety of modern networking access technologies like switch port or wireless, as well as VPN access or firewall access.
2. *The integrity evaluation layer*: The components in this layer are responsible for evaluating the overall integrity of the Access Requestor with respect to certain access policies.

3. *The integrity measurement layer:* This layer contains plug-in components that collect and verify integrity-related information for a variety of security applications on the Access Requestor.

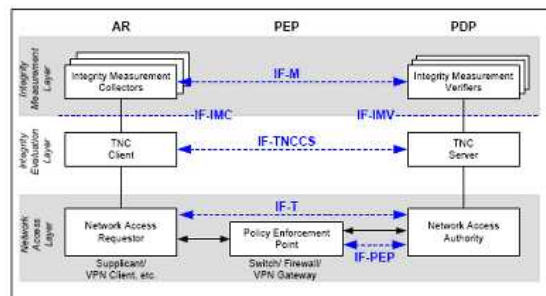


Exhibit 2: Layered Trusted Network Connect Architecture

The Access Requestor (AR) consists of the following components:

- *Integrity Measurement Collector (IMC):* The IMC is a component of an AR that measures security aspects of the AR's integrity. Examples include the Anti-Virus parameters on the Access Requestor, personal firewall status, software versions, and others. The TNC Architecture accommodates implementation situations where multiple IMCs reside on a single AR, catering for corresponding different applications.
- *TNC Client (TNCC):* The TNCC is a component of an AR that aggregates integrity measurements from multiple IMCs and assists with the management of the *Integrity Check Handshake* for the purpose of measurement and reporting of the AR integrity.
- *Network Access Requestor (NAR):* The NAR is the component responsible for establishing network access. The NAR can be implemented as a software component that runs on an AR, negotiating its connection to a network. There may be several NARs on a single AR to handle connections to different types of networks. One example of a NAR is the supplicant in 802.1x, which is often implemented as software on a client system or could be VPN client software as well.

The Policy Decision Point (PDP) consists of the following components:

- *Integrity Measurement Verifier (IMV):* The IMV is a component that verifies a particular aspect of the AR's integrity, based on measurements received from IMCs and/or other data.
- *TNC Server (TNCS):* The TNCS is a component that manages the flow of messages between IMVs and IMCs, gathers IMV action recommendations from IMVs, and combines those recommendations (based on policy) into an overall TNCS action recommendation to the NAA.
- *Network Access Authority (NAA):* The NAA is a component that decides whether an Access

Requestor (AR) should be granted access. The NAA may consult a TNC Server to determine whether the AR's integrity measurements comply with the NAA's security policy. In many cases, an NAA will be an AAA server such as RADIUS server, but this is not required.

And a third entity of the TNC Architecture that sits in the middle of the AR and a PDP is the Policy Enforcement Point (PEP) that consists of the following components:

- *Policy Enforcement Point (PEP):* The PEP is a typically the hardware component that controls access to a protected network. The PEP consults a PDP to determine whether this access should be granted. An example of the PEP is the Authenticator in 802.1x, which is often implemented within the 802.11 wireless access point. It could also be an 802.1x enabled switch port or a firewall as well as the VPN gateway.

Although not visibly evident within the TNC Architecture, one important feature of the architecture is its extensibility and support for the isolation and remediation of ARs, which do not succeed in obtaining network access permission due to failures in integrity verification. TNC Architecture with Provisioning and Remediation Layer that is illustrated in Exhibit 3 shows an additional layer addressing remediation and provisioning.

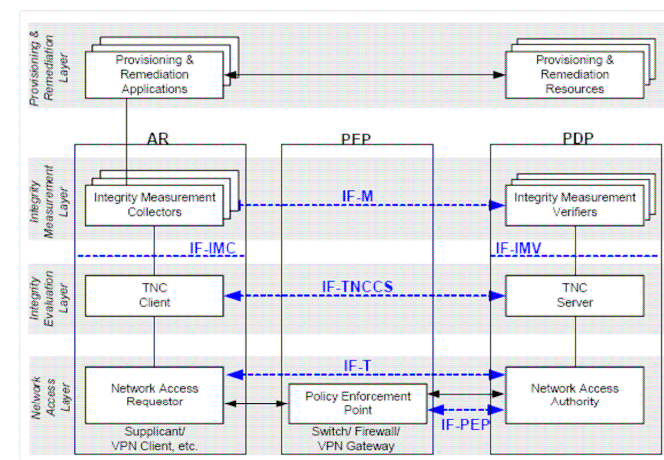


Exhibit 3: TNC Architecture with Provisioning and Remediation Layer

In order to understand the actions needed to remedy ARs that fail integrity verification, it is useful to view network connection requests in three basic phases from the perspective of integrity verification:

1. *Assessment:* In this phase, the IMVs perform the verification of the AR following the policies set by the network administrator and optionally deliver remediation instructions to the IMCs.

2. **Isolation:** If the AR has been authenticated and is recognized to be one that has some privileges on the network but has not passed the integrity-verification by the IMV, the PDP may return instructions to the PEP to redirect the AR to an isolation environment where the AR can obtain integrity-related updates. Isolation environment mechanisms could be:

- (a) **VLAN Containment:** VLAN containment permits the AR to access the network in a limited fashion typically for the purpose of the limited access and to allow the AR to access on-line sources of remediation data (e.g. virus definition file updates, worm removal software, software patches, etc).
- (b) **IP Filters:** In the case of IP filters, the PEP is configured with a set of filters which defines network locations reachable by the isolated AR. Packets from the AR destined to other network locations are simply discarded by the PEP.

3. **Remediation:** Remediation is the process of the AR obtaining corrections to its current platform configuration and other policy-specific parameters in order to bring it inline with the PDP's requirements for network-access.

The remediation process requires remediation provisioning application and resources that can be implemented in several forms. For example, that would be the Anti-Virus application software that communicates with sources of Anti-Virus parameters (e.g. latest AV signature files) or could be an agent that updates the latest patches from the ftp server that contains the latest patches. Note that in the current TNC Architecture document, remediation is out of scope and is treated briefly only for completeness.

Although integrity measurement and reporting is core to the value proposition of the TNC philosophy and approach, the TNC Architecture acknowledges other networking technologies as providing the infrastructure support surrounding the core elements of the TNC Architecture. Note that the TNC specification is not standardizing specific protocol bindings for these technologies but is rather defining only layer interfaces (as seen on the TNC Architecture Exhibit with an appendix IF-...) and is relying on already existing protocols, such as 802.1x, IPsec/IKE, PEAP, TLS for network access or RADIUS and DIAMETER for communication with and within PDP.

Even though that up to the moment of writing this chapter there was no commercially available nor widely deployed solution implementation based on TNC specification, TNC detailed architecture components description represent an open framework for vendor neutral solution where multiple vendors could provide an individual modules of the complete end node security solution. Several individual vendor or vendor alliances that have inspired the TNC specification work are described going further.

2.2. Network Admission Control

2.2.1. Network Admission Control Overview

Network Admission Control (NAC) architecture is an industry effort lead by Cisco Systems, that initially started as an interoperable framework between networking vendor and several

Anti-Virus vendors with a goal to isolate the most burning problem at a time - stop the virus and worm infection from infected hosts at their network connection points. NAC architecture achieves that by checking the end node security compliancy before admitting it to connect to the network.

Security policy compliance checks that NAC can perform include:

- Determining whether the device is running an authorized version of an operating system.
- Checking to see if the OS has been properly patched, or has received the latest hotfix.
- Determining if the device has Anti-Virus software installed, and whether it has the latest set of signature files.
- Ensuring that Anti-Virus technology is enabled and has been recently run.
- Determining if personal firewall, intrusion prevention, or other desktop security software is installed and properly configured.
- Checking whether a corporate image of a device has been modified or tampered with.

NAC architecture components that are illustrated in Exhibit 4 are:

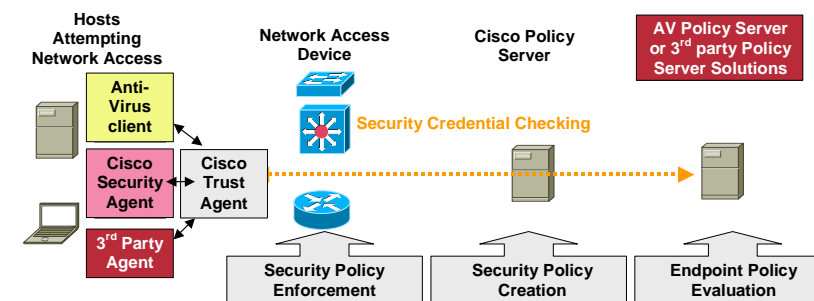


Exhibit 4: Network Admission Control Architecture Components

- **Endpoint Security Software** - NAC solution requires either Cisco Trust Agent or a third party software agent that is capable of executing the integrity checks on the end node and communicating that during the network access request phase.
- **Network Access Device** - a network access device like router, switch, VPN gateway, or firewall that can demand endpoint security "credentials" from the endpoint. This is in TNC terminology analogy of a Policy Enforcement Point.
- **Policy/AAA Server** - RADIUS server that evaluates endpoint security credentials relayed from the network access device and determine the appropriate access policy (*permit, deny, quarantine, restrict*) to be applied back to the network access device for the particular end node accessing the network.
- **Anti-Virus Policy Server** - third party server that evaluates particular policy like Anti-Virus policy. As NAC solution includes multiple vendors, third party policy servers could be used to check integrity of any application running on the end node system as well as hardware

components compliancy, however they need to interfaces to policy/AAA server that is under control of Cisco Systems and even though there is a plan to open and standardize it, that is still remaining to happen.

2.2.2. NAC Analysis

Even though that Endpoint Security Software of a NAC architecture uses standard communication protocols between the agent components and even that the interface software is provided free of charge by Cisco Systems, exchange of “security credentials”, as Cisco Systems refers to an end node integrity state check, is still not standardized. Standards-based technologies that are used are EAP, 802.1x, and RADIUS. In some cases, these technologies may need to accommodate specific enhancements to support the NAC solution. Cisco Systems expects to drive adoption of these enhancements through appropriate standards bodies.

The Cisco Trust Agent, Endpoint Security Software available from Cisco Systems, collects security state information from the operating system and multiple security software clients, such as Anti-Virus and Cisco Security Agent software clients, and communicates this information to the connected network, where access control decisions are enforced. The Cisco Trust Agent that has the closest equivalent role of the TNCC in the TNC Architecture has in the NAC architecture following three main responsibilities:

- Network Communications-Respond to network requests for application and operating system information such as Anti-Virus and operating system patch details.
- Security Model-Authenticate the application or device requesting the host credentials and encrypt that information when it is communicated
- Application Broker-Through an API, enables numerous applications to respond to state and credential requests

AV	CSA	Any
EAP/TLV API		
Broker & Security		
Comms: L2/3 Service		
EAP/UDP	EAP/802.1x	

Exhibit 5: NAC End Node Protocol Stack

End node protocol stack that is illustrated in Exhibit 5, shows several layers of an end node agent security software. Cisco Systems decided, for most probably faster time to market, to implement EAP over UDP protocol exchange first. EAP over UDP made NAC solution immediately available to work on the layer 3. That helped to nodes with an IP address that try to connect to the rest of the layer three network infrastructure to exchange EAP messages with the infrastructure and based on the overall exchange, get access to the network resources granted or not granted. In essence router from Cisco Systems, as the very first implementation phase of NAC architecture solution, understands EAP over UDP control messages and does EAP messages exchange with a Endpoint Security Software and Policy Server. Follow up phases brought the EAP over layer 2 that allowed NAC communication to network devices such as switches or wireless access points where authentication and policy

compliance messages exchange could happen even before the IP address is obtained. NAC communication flow is illustrated in Exhibit 6.

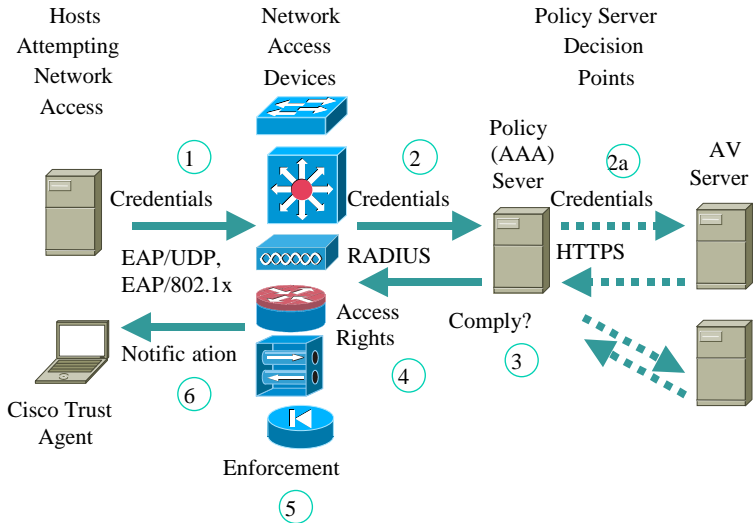


Exhibit 6: NAC Access Control Flow

Policy enforcement actions are directly dependent on the communication method between the end node software agent and the network node and were initially only permit, deny or quarantine access via simple layer 3 router access control list filter, while follow up phases introduced VLAN isolation too.

Both layer 2 and layer 3 end nodes which demand network access as well as network access devices themselves in the NAC solution would need to be up to date with a compatible software release to be a valid member of the NAC solution. In the mean time Cisco Systems also introduced the NAC appliances family of products, but its significance stays as one of the first integrity network access control implementers on the market. The NAC architecture brought an innovative break through in the capability that network access devices could police the state of the end node and make an intelligent decision before connecting it to the rest of the network, so no wonder that Cisco Systems leverage it as a crucial part of its Self-Defending Network strategy.

2.3. Network Access Protection

2.3.1. Network Access Protection Overview

Network Access Protection (NAP) solution coming from Microsoft next generation Windows server with a code name "Longhorn", provides policy enforcement components that help ensure that computers connecting to a network or communicating on a network meet administrator-defined requirements for system health. NAP uses a combination of policy validation and

network isolation components to control network access or communication. It can also temporarily isolate computers that do not meet requirements to a restricted network. Depending on the configuration chosen, the restricted network might contain resources required to update the computers so that they then meet the health requirements for full network access or normal communication. When it will be available for deployment, NAP will be able to create solutions for health policy validation, isolation, and ongoing health policy compliance.

NAP is at the point in time of writing this chapter defined with a core component of future Windows server and clients, quarantine server that will be Microsoft Internet Authentication Services (IAS), and one or more policy servers. NAP will work by controlling network access via multiple connectivity mechanisms as is illustrated in Exhibit 7.

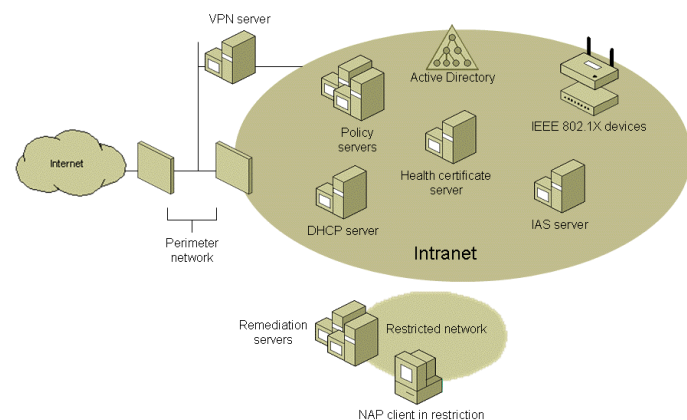


Exhibit 7: Network Access Protection Architecture

In the initial release, NAP will require servers to run Windows Server "Longhorn" and clients to run Windows Vista, Windows Server "Longhorn," or Windows XP with Service Pack 2. Network isolation components in the NAP architecture will be provided for the following network technologies and connectivity methods:

- Dynamic Host Configuration Protocol (DHCP)
- Virtual private networks (VPNs)
- 802.1x authenticated network connections
- Internet Protocol security (IPsec) with x.509 certificates

• *DHCP Quarantine* consists of a DHCP Quarantine Enforcement Server (QES) component and a DHCP Quarantine Enforcement Client (QEC) component. Using DHCP Quarantine, DHCP servers can enforce health policy requirements any time a computer attempts to lease or renew an IP version 4 (IPv4) address configuration on the network. DHCP Quarantine is the easiest enforcement to deploy because all DHCP client computers must lease IP addresses. However, DHCP Quarantine provides only weak network isolation.

• *VPN Quarantine* consists of a VPN QES component and a VPN QEC component. Using VPN Quarantine, VPN servers with VPN QEC component could enforce health policy requirements any time a computer attempts to make a Layer 2 Tunneling Protocol (L2TP) VPN connection to the network. VPN Quarantine provides strong network isolation for all computers accessing the network through an L2TP VPN connection.

• *802.1x Quarantine* consists of an IAS server and an EAP Host QEC component. Using 802.1x Quarantine, an IAS server instructs an 802.1x access point (an Ethernet switch or a wireless access point) to place a restricted access profile on the 802.1x client until it performs a set of remediation functions. A restricted access profile can consist of a set of IP packet filters or a virtual LAN identifier to confine the traffic of an 802.1x client. 802.1x Quarantine provides strong network isolation for all computers accessing the network through an 802.1x connection.

• *IPsec Quarantine* comprises a Health Certificate Server (HCS) and an IPsec QEC. The HCS issues x.509 certificates to quarantine clients when they are determined to be healthy. These certificates are then used to authenticate NAP clients when they initiate IPsec-secured communications with other NAP clients on an intranet. IPsec Quarantine confines the communication on the network to those nodes that are considered healthy and because it is leveraging IPsec, it can define requirements for secure communications with healthy clients on a per-IP address or per-TCP/UDP port number basis. Unlike DHCP Quarantine, VPN Quarantine, and 802.1x Quarantine, IPsec Quarantine confines communication to healthy clients after the clients have successfully connected and obtained a valid IP address configuration. IPsec Quarantine is the strongest form of isolation in Network Access Protection architecture.

NAP quarantine methods could be used separately or together to isolate unhealthy computers and Microsoft IAS will act as a health policy server for all of these technologies as is illustrated in Exhibit 8.

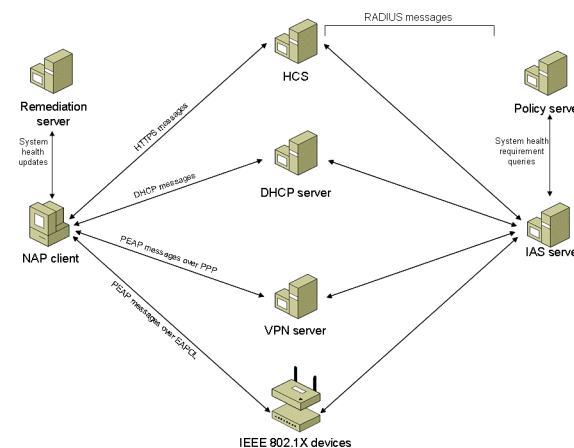


Exhibit 8: Interaction between Network Access Protection Components

There might be several System Health Agent (SHA) components that define a set of system health requirements such as SHA for antivirus signatures, SHA for operating system updates, etc. A specific SHA might be matched to a remediation server. For example, an SHA for checking antivirus signatures is matched to the server that contains the latest antivirus signature file. SHAs do not have to have a corresponding remediation server. For example, an SHA can just check local system settings to ensure that a host-based firewall is running or configured properly. To indicate the status of a specific element of system health, such as the state of the Anti-virus software running on the computer or the last operating system update that was applied, SHAs create a Statement of Health (SoH) and pass their SoH to the Quarantine Agent (QA). Whenever an SHA updates its status, it creates a new SoH and passes it to the Quarantine Agent.

To draw a parallel with the TNC specification, QA can be seen as an equivalent role to TNC Client, while the multiple SHAs are similar to IMVs and QECs are playing the role of NARs, as is described in more details further.

2.3.2. Quarantine Enforcement Clients

A Quarantine Enforcement Client (QEC) within a NAP client architecture is the one that requests in some way access to a network. During that phase it will pass the end node's health status to a NAP server that is providing the network access, and indicate its status according to the information obtained from multiple SHAs as illustrated in the NAP Client Architecture Exhibit 9.

The QECs for the NAP platform supplied in Windows Vista and Windows Server "Longhorn" will be the following:

- A DHCP QEC for DHCP-based IPv4 address configuration
- A VPN QEC for L2TP VPN based connections
- An EAP Host QEC for 802.1x authenticated connections
- An IPsec QEC for x.509 certificate based IPsec-based communications

• *DHCP QEC* is functionality in the DHCP client service that uses industry standard DHCP messages to exchange system health messages and restricted network access information. The DHCP QEC obtains the list of SoHs from the Quarantine Agent. The DHCP Client service fragments the list of SoHs, if required, and puts each fragment into a Microsoft vendor-specific DHCP option that is sent in DHCPDiscover, DHCPRequest or DHCPInform messages. DHCPDecline and DHCPRelease messages do not contain the list of SoHs.

• *VPN QEC* is a functionality in the Microsoft Remote Access Connection Manager service that obtains the list of SoHs from the Quarantine Agent and sends the list of SoHs as a PEAP-Type-Length-Value (TLV) message. Alternately, the VPN QEC can send a health certificate as a PEAP-TLV message.

• *EAP Host QEC* is a component that obtains the list of SoHs from the Quarantine Agent and sends the list of SoHs as a PEAP-TLV message for 802.1X connections. Alternately, the EAP Host QEC can send a health certificate in a PEAP-TLV message.

• *IPsec QEC* is a component that obtains a health certificate from the HCS and interacts with the following:

1. The certificate store to store the current health certificate.
2. The IPsec components of the TCP/IP protocol stack to ensure that IPsec-based communication uses the current health certificate for IPsec authentication.
3. The host-based firewall (such as Windows personal firewall) so that the IPsec-secured traffic is allowed by the firewall.

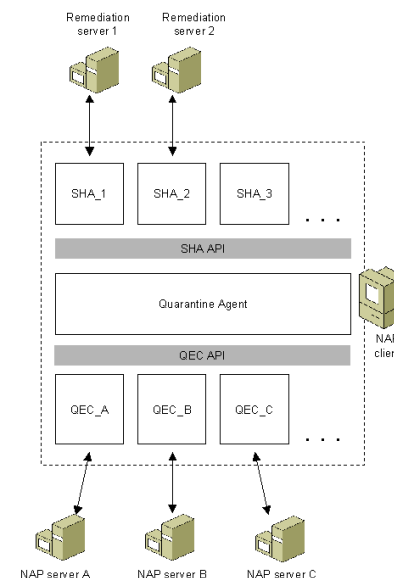


Exhibit 9: NAP Client Architecture

2.3.3. NAP Analysis

Microsoft with its proven track of showing how the complex things could be simplified to the level that they could be easily and widely deployed has certainly a significant role in end node integrity and policy compliancy solution evolution. When becomes available, NAP seems to be the lowest cost solution that will require only Windows XP Service Pack 2 to have the valid NAP clients considering the current Microsoft release policies where NAP solution will be most probably offered as a free server component with next generation server software. That means that the NAP solution could come after regular Windows server update along at no additional cost. It is also a fair to mention that NAP solution won't require any

proprietary or new hardware, as its strengths are all in software development and in particular in vendor specific protocol extensions, such as done with DHCP.

2.4. Sygate Network Access Control

2.4.1. Sygate Network Access Control Overview

Sygate is a vendor that came out with its own end node to network infrastructure interactivity solution and gave it a name Sygate Network Access Control (SNAC). In the mean time Sygate has been acquired by Symantec that initially kept the current Sygate solutions under the Sygate brand while expecting to re-brand the next version of the products and include additional functionality. However this solution description will be narrowed only to an initial SNAC concept that allowed enforcement of end node security in four ways:

1. Create SNAC Policies: Using the Sygate Policy Manager for central managed and deployed network access control policies that include templates for well-known Anti-Virus software, personal firewalls, anti-spyware, operating system configurations, and security patches.

2. Discover end node integrity status: Sygate Enforcers and Agents discover new devices as they connect to the network and then perform baseline end node integrity checks when they start-up, at a configurable interval, and when they change network locations.

3. **Enforce Network Access Controls:** At the time of network connection and for the duration of the network session, Sygate Enforcers apply network access controls to endpoints attempting to connect to the enterprise network. If end nodes are in compliance with policy, they are permitted on the network. If the end node is non-compliant, then it is either quarantined to a remediation network or blocked from network access.

4. **Remediate Non-Compliant Devices:** When an end node fails one or more integrity checks, the agent will automatically perform a pre-configured operation to bring the end node into compliance without user intervention. Administrators can customize the user interaction that occurs during the remediation process and even give the user the option to delay non-critical remediation actions for a range of time. Once remediated, the agent will automatically start the SNAC process again and, since the end node is now in compliance, will get access to the corporate network.

SNAC solution that performs periodic host integrity checks, when an end node starts up, at a configurable interval, and when it changes network locations, to discover its security state works through the Sygate Enforcement Agent (SEA) that could be seen as the analogy of the AR in the TNC specification. Components of the SNAC solution are illustrated in Exhibit 10.

Sygate also enhanced SNAC to Universal NAC System that combines SNAC with solution for securing unmanaged devices, with several different enforcement mechanisms to extend SNAC protection to every type of network access (VPN, wireless, routers, DHCP, etc), and on all endpoints, including laptops, desktops, servers, guest systems and embedded devices.

Sygate Universal NAC System's enforcement methods include:

1. Self-Enforcement when computers leave the network
2. API-Based integration with dialers and VPNs

3. Gateway Enforcement for in-line enforcement on any network
4. On-Demand agents for guests accessing the network
5. DHCP-based approach for LAN and Wireless over any infrastructure
6. 802.1x standards-based approach for LAN and wireless networks
7. Cisco NAC technology for Cisco routers

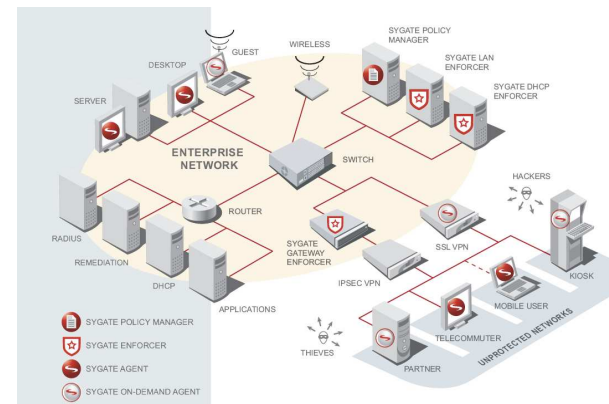


Exhibit 10: SNAC Solution Overview

2.4.2. SNAC Analysis

SNAC solution puts a lot emphasis on the client agent software as the vital component of the solution and even though Sygate is a member of Cisco Systems NAC initiative, it also has its own SNAC appliance as well as backend policy servers, that as already mentioned will most probably become part of the enhanced Symantec product portfolio. For an 802.1x access method, SNAC relies, like many other solutions on third party 802.1x clients such as Funk Software (that in the mean time got acquired by Juniper Networks) Odyssey client or Meetinghouse Aegis client, that on top of the additional inline gateway device represent an extra costs in the overall deployed SNAC solution.

2.5. Automated Quarantine Engine

2.5.1. Automated Quarantine Engine Overview

Alcatel was one of the first vendors that came out with solution that is complementary to so far described ones. Main difference is that it does not require any agent-based software on the end node device to be able to detect, block or isolate the infected end node. Alcatel has devised a way to implement the concepts of automated end node isolation by allowing an

intrusion detector to pass information to their OmniVista central network management system. OmniVista then works with an integrated *Automatic Quarantine Engine* (AQE) module to apply policies and place the infected system into a penalty VLAN where it can no longer infect the rest of the network. AQE solution is illustrated in Exhibit 11.

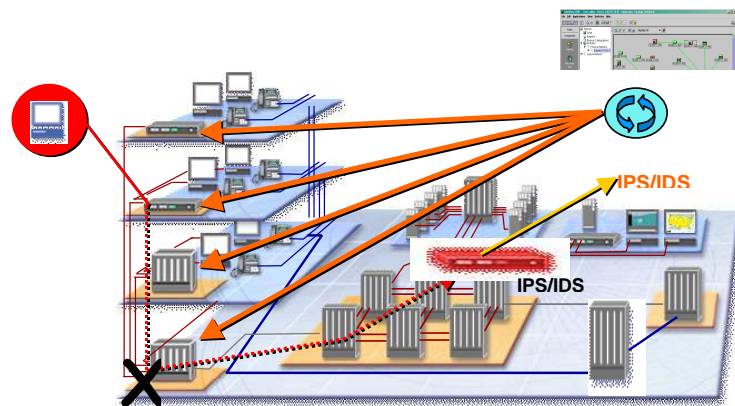


Exhibit 11: Automated Quarantine Engine from Alcatel

Based on the input from a detection sensor such as Intrusion Detection/Protection System (IDS/IPS) sensor and the Alcatel's home grown layer two media access control (MAC) address trace back mechanism, AQE solution is capable of dynamically reconfiguring the access switch to allow or limit access of the particular end node to the rest of the network. This is done via SNMPv3 commands communicated to a switch infrastructure to shut down the port or put additional filtering mechanisms: either VLAN configuration or simple access list filter for particular node accessing the network.

Important part is that the AQE transparently and dynamically applies policies to an individual switched port based on the device behavior accessing the port. The automatic reconfiguration reduces the response time to security threats and removes the need to have a network engineer create and apply an isolation policy (VLAN, ACL) to manage network access, which minimizes the need for manual configuration and application of network user policies. Once the infected system is isolated, the network administrator is notified and given choices on how to handle the infected system.

2.5.2. AQE Analysis

AQE solution is unique in the way that it works with IDS/IPS as an alerting mechanism to trigger the blocking, isolation or protection configuration changes on the access switches port level. Being agent-less solution, makes it quite powerful and complementary option to all other agent based proposals on the market and as such very interesting alternative where end node software is not possible or difficult to install due to legacy or not supported end node software or any other reasons. Alcatel also claims that from a switch network infrastructure viewpoint, their solution is fully interoperable with other vendor switches, which makes it also attractive and open solution for the modern end node access management. Missing part

in AQE solution is that it has only automated isolation, blocking and quarantine parts while end node notification or remedy with a return of a cured node must be done manually by the system operator.

2.6. TippingPoint Quarantine Protection

2.6.1. TippingPoint Quarantine Protection Overview

Similar to AQE solution, TippingPoint, now a division from 3Com, came out with a agent-less solution based on their homegrown Intrusion Protection Systems (IPS). TippingPoint Quarantine Protection (TPQ) uses network-based IPS mechanism to detect and stop the viral infection coming from the network attached infected end node. As an inline device to a traffic flow, IPS could stop the viral infection detected on the traffic flow coming from infected end node and if combined with a network infrastructure could apply blocking function based on the switch port, MAC address or IP address on the edge switch or router. Quarantine function could happen via VLAN isolation and being inline-based solution, TPQ provides also a remedy possibility by doing HTTP URL redirection. TPQ solution is illustrated in Exhibit 12.

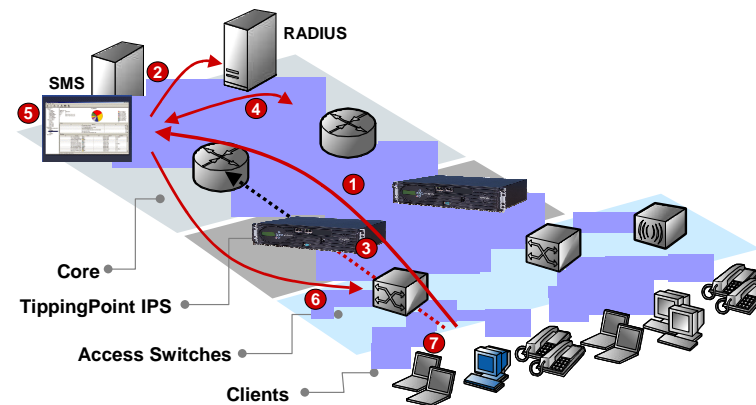


Exhibit 12: TippingPoint Quarantine Protection Action Steps

Flow of action goes through an end node connecting to a network and authenticating via TippingPoint Security Management System (SMS) and RADIUS server, while IPS engine detects the intrusion activity. Based on the configured policy action SMS resolves the IP address to a MAC address and could instruct the blocklisting or policing the access on the ingress access device.

2.6.2. TQP Analysis

Technologically speaking, IPS based quarantine system is as in inline solution and is as such avoiding end node software installation issue. That makes TQP easier to scale for a large number of end nodes. On top of that TPQ is also as well as Alcatel AQE an end node operating system independent solution that gives an additional benefit of protecting non-user based end nodes, such as printers, faxes or IP phones. Biggest concern with both mentioned IPS based solutions: TQP as well as AQE is that the end node that is infecting the infrastructure could also infect the other nearby end nodes residing on the same segment before it could be blocked or isolated from the network. Solution to that issue is however also possible and is actually existing in the infrastructure functionality itself in a form of so called Private Virtual Local Area Networks (PVLAN). Operation of the PVLAN is illustrated in Exhibit 13.

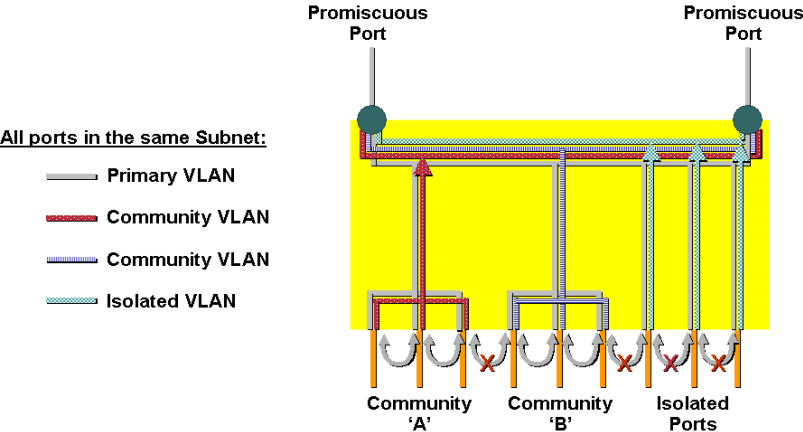


Exhibit 13: Private VLAN (PVLAN) Operation

Even though not standardized, PVLAN functionality that exists in almost any switch vendor product is, if the application traffic flow that permits, a very efficient mechanism to force the traffic from the network edge or access layer devices through the IPS systems. IPS that are typically hierarchically aggregated at a network distribution layer than prevent the end nodes infecting each other, by isolating them before they access the rest of the network resources.

2.7. Hybrid Solutions

All previously mentioned solutions are definitely not the only ones on the market. For instance, Enterasys has created both agent and network-based Trusted End System (TES) solutions where they combine their switches with a policy server and end node agents from Check Point/Zone Labs or Sygate. Other option Enterasys provides is to use a vulnerability-patch assessment tools from Nessus to perform the end node scan checks upon the network

connections and than provide similar functions as NAC, NAP or TNC. Foundry and Extreme also offer network admission solutions with Sygate's client, while Vernier Networks, a startup originally focused on wireless security, recently announced its EdgeWall security appliances that performs network admission control as well. Intel, HP, and Nortel also announced their solution for the end node and network access management protection that are very similar or aligned with already previously mentioned ones. All of that just shows that the industry players are seriously considering solving the problem of the end node to network infrastructure interaction. At the same time, unfortunately, it also shows the panacea of solutions that are even though in some cases combined still mostly isolated from each other. All that makes not an easy task with any strategic decision for information security practitioners that are dealing with burning virus infections at current point in time.








3. End Node Security Solutions Comparison

Information security practitioners are already facing or will, due to pressure for immediate solution, definitely face in the very near future a decision making point which solution to use or deploy, hence comparison tables of currently available offers might help to compare them to each other as well as make a clear picture of the offered features and functionalities.

Features Solution	Requires Dedicated HW	Isolation	Access Media Supported	Remedy
TNC	No	VLAN/ACL	Open	Out of Scope
NAC	Yes/No*	VLAN/ACL	802.1x, 802.1x/UDP, IPsec VPN	3 rd party
NAP	No	Subnet, VLAN, ACL	802.1x, L2TP VPN, IPsec VPN, DHCP	3 rd party
SNAC	Yes	VLAN, ACL	802.1x, 802.1x/UDP, L2TP VPN, IPsec VPN, DHCP	Yes
AQE	No**	Port block, MAC filter, VLAN, ACL	IP	3 rd party
TQP	No**	Port block, MAC filter, VLAN, ACL	IP	URL redirection to 3 rd party
TES	Yes	Port block, MAC filter, VLAN, ACL	802.1x, IP	Yes

* NAC requires Cisco router or switch infrastructure; Cisco also released dedicated NAC appliance
** No dedicated infrastructure HW needed, while both TQP and AQE require dedicated IDS/IPS for malware activity detection

Exhibit 14: End Node Security Solutions Comparison Table-1

Features Solution	Requires End Node Software	End Node OS Supported	Requires SW/HW Upgrade	PVLAN recommended
TNC 	Yes	Open Specification	Once Implemented - Yes	No
NAC 	Yes	Microsoft only	Yes	No
NAP 	No*	Microsoft only	Yes	No
SNAC 	Yes	Microsoft only	Yes	No
AQE 	No	Any	No	Yes***
TQP 	No	Any	No	Yes***
TES 	Yes/No**	Microsoft / Any**	Yes/No**	No

* Bundled with Microsoft OS

** Enterasys TES has agent-based and network-based options

** PVLAN usage is not required, however is strongly recommended

Exhibit 15: End Node Security Solutions Comparison Table-2

4. Future Directions

Even though current proposals are giving promising outcome, looking a bit forward into future shows that there are still several open issues that are just outlined in no order of importance but rather as missing components that needs to be solved.

- Policy server protocols are not standardized but closed into vendor-to-vendor API and same goes for the remedy solutions that are even out of the scope of the TNC specification.
- 802.1x protocol usage deployment is still very low.
- DHCP extensions are vendor specific. That makes requirement to have a DHCP client and server from the same vendor, which leads to a locking solution with a single vendor and away from an interoperable scalable solution where different components of the solution could be provided by different vendors.
- EAP methods used are still under development. PEAP even though in the stable IETF draft at a point in time of writing this chapter is still not standardized, hence its implementations are not always interoperable while new methods such as EAP-FAST are already on the horizon.
- All layer 3 solutions are only IPv4 based and have no solution on how to solve the problem with coming new protocols such as IPv6. Other clients than Microsoft OS

based like, mobile phones, pda's or legacy OS systems are not covered in most agent-based solutions.

- Most solutions so far are not focusing on the malicious user, but rather on accidental problem. While this might be sufficient for the start, follow up developments that need to stop the malicious attacks either need to be specified or will again be driven into different proprietary extensions.

All of above are important points to be solved while the main issue going forward will be to get the major players commit to development of the interoperable, modular solution such as defined in TNC specification. That is obviously not expected to happen over the night for obvious reason: once lucrative network infrastructure business now under fear of becoming commodity still heavily drives closed solution that makes the differentiations and competitive points among the vendors.

5. Summary

Will automated end node protection mechanism be an ultimate solution for all sizes? Most probably not, but will certainly add an additional level in the layered security architecture approach that information security practitioners could effectively use to mitigate the security problems. However, every network admission solution today is proprietary, and puts information security practitioners into a trap of an isolated single vendor solution. The Trusted Network Connect specification gives a hope to promote interoperability, but de facto standards will likely be driven by the major players in the networking infrastructure and desktop software market. In essence it is important to understand that end node control methods that were discussed in this chapter are by design doing end nodes integrity and policy compliancy checking and with that increasing the security level of the rest of the network. Information security practitioners should also be aware of what different options could and could not achieve and be able to distinguish their potential benefits as well as be aware of their disadvantages and limitations.

Key dilemma stays with two sides: end node with agent or agent-less deployment. While agent-based solutions promise resolution to all issues they also get stacked with a scalability and deployment. On the other hand, agent-less solutions make intermediate and fast cure for a burning problems, however do not necessarily automate and solve all necessary components. It is also important to look into future development and acceptance of 802.1x based solutions versus DHCP-extended solutions. In 802.1x case, solutions are on a solid ground with a standard based access control protocol. Even though well defined for authentication part, 802.1x still struggles with variety of different EAP methods and hence is, maybe with exception of wireless world, facing issue of wider acceptance together with a scalability of deployment. DHCP as a protocol has no authentication built in it at all, however DHCP vendor extensions might fulfill the promise of easy and scalable deployment due to its simplicity and possible faster and wider acceptance. At the current point in time there is no final conclusion of where to go, so it stays on the shoulders of information security practitioners to closely watch and follow the developments and outcomes, while where needed, armed with knowledge from this chapter, deploy the solutions that fit their immediate business demands.

6. List of Acronyms

AAA	Authentication Authorization Accounting
ACL	Access Control List
AR	Access Requestor
AQE	Automated Quarantine Engine
DIAMETER	Not an acronym
DHCP	Dynamic Host Configuration Protocol
EAP	Extensible Authentication Protocol
HCS	Host Certificate Server
IAS	Internet Authentication Service
IETF	Internet Engineering Task Force
IDS	Intrusion Detection System
IMC	Integrity Measurement Collector
IMV	Integrity Measurement Verifier
IPS	Intrusion Protection System
L2TP	Layer 2 Tunneling Protocol
MAC	Media Access Control
NAA	Network Access Authority
NAC	Network Admission Control
NAR	Network Access Requestor
NAP	Network Access Protection
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PEAP	Protected Enhanced Authentication Protocol
PVLAN	Private Virtual Local Area Network
RADIUS	Remote Authentication Dial-In User Service
SNMP	Simple Network Management Protocol
QEC	Quarantine Enforcement Client
QES	Quarantine Enforcement Server
SHA	System Health Agent
SHC	State Health Certificate
SNAC	Sygate Network Access Control
SoH	Statement of Health
TCG	Trusted Computing Group
TES	Trusted End System
TLV	Type-Length Value
TNC	Trusted Network Connect
TQP	TippingPoint Quarantine Protection
TES	Trusted End System
VPN	Virtual Private Network
VLAN	Virtual Local Area Network
UDP	User Datagram Protocol

7. References

AEQ - Automated Quarantine Engine: <www.alcatel.com/enterprise/en/products/ip_networking/crystalsec_security/pdf/AutoQuarantineEngine.pdf>

NAC - Network Admission Control: <www.cisco.com/go/nac>

NAP - Network Access Protection: <msdn.microsoft.com/library/default.asp?url=/library/en-us/wcecomm5/html/wce50conNetworkAccessPointNAP.asp>

SNAC - Sygate Network Admission Control: <www.sygate.com/news/universal-network-access-control-snac_rls.htm>

TNC - Trusted Network Connect: <www.trustedcomputinggroup.org/downloads/TNC>

TCG - Trusted Computing Group: <www.trustedcomputinggroup.org/home>

HP news: <www.techworld.com/security/news/index.cfm?NewsID=3128>

Enterasys Trusted End-System Solution: <www.enterasys.com/solutions/secure-networks/trusted_end_system>

Nortel: <www.nortel.com/corporate/news/newsreleases/2004d/12_13_04_microsoft_alliance.html>

Trusted Network Connect - can it connect? Ellen Messmer, NetworkWorld.com, May 2005
<www.networkworld.com/weblogs/security/008721.html>

Cisco NAC vs. Microsoft NAP, by Andrew Conry-Murray, 03/01/2005, IT Architect,
<www.itarchitect.com/shared/article/showArticle.jhtml?articleId=60401143>

NAC vs. NAP, by Roger A. Grims, September 5th 2005, Infoworld
<www.infoworld.com/article/05/09/05/36FEbattlesecurity_1.html>

Introduction to Network Access Protection, Whitepaper, Microsoft Corporation, Published June 2004, Updated July 2005.

Network Access Protection Platform Architecture, Whitepaper, Microsoft Corporation, Published June 2004, Updated July 2005.

A Tamper-Resistant, Platform-Based, Bilateral Approach to Worm Containment
D. Durham, G. Nagabhushan, R. Sahita and U. Savagaonka, Technology@Intel Magazine.

Jerry Bryant, Weblog: Network Access Protection (NAP) Architecture, posted on April 26, 2005, <msmvps.com/secure/archive/2005/04/26/44630.aspx>

A Mirage Networks White Paper, Strengthening Defense-in-Depth from Inside Out with NAC, <www.miragenetworks.com/pdfs/wp_Strengthening_Defense.pdf>, September 2005.