



Network Access Control Technologies and Symantec Compliance on Contact

Richard Langston, Sr. Product Manager,
Symantec Corporation

Network Access Control Technologies and Symantec Compliance on Contact

Contents

Summary	4
Introduction	5
What is Network Access Control?	6
Symantec Compliance on Contact	8
Symantec Enforcement Agents	10
Symantec Enforcers	10
Symantec Policy Manager	10
Symantec 802.1x-based NAC for LAN and wireless	11
Symantec DHCP-based NAC	13
Symantec Gateway NAC	14
Symantec On-Demand NAC for SSL VPNs	14
Symantec API integration	16
Cisco Network Admission Control	17
Cisco and Symantec together	19
Future efforts	21
Microsoft's Network Access Protection	21
Trusted Computing Group's Trusted Network Connect	22
Conclusion	23
References	24

Summary

Today, businesses must face the very real threat of their systems being compromised by misuse, misconfiguration, and malicious access. In fact, Gartner estimates that 20 percent of managed systems are already compromised.¹ Add to that their estimate that 20 percent of systems on corporate networks are entirely unmanaged, and it becomes clear that most enterprises are vulnerable to loss of productivity, leakage of confidential information, and other expensive (and potentially embarrassing) abuse.

Network Access Control (NAC) is a process designed to reduce security incidents and increase compliance by enforcing IT security policies as a prerequisite for network access. Although "Network Access Control" is a newly defined category, Symantec has blazed the trail in network access control technologies through the introduction of IPSec VPN and Gateway Enforcement solutions in 2001 and subsequently adding Self-Enforcement, On-Demand agents, and 802.1x LAN Enforcement in 2003. The expansion of enforcement methods continued through 2005 with the introduction of DHCP Enforcement and integration with Cisco's Network Admission Control solution. In 2006 Symantec maintained our growth pattern by offering Enforcer appliances and a Microsoft® DHCP plug-in solution to further enable enterprise deployments.

Today, Symantec has many large enterprise customers that have deployed complete NAC solutions. NAC solutions require multiple enforcement methods and policy flexibility to cover the entire enterprise network. Customers should carefully assess their environments and requirements against each possible solution. As an innovator in NAC solutions, Symantec provides the most comprehensive and flexible set of options for deploying Network Access Control to best fit the needs of the enterprise.

Several consortiums and standards have emerged that promise to create NAC standards for network infrastructure, authentication, endpoint security, and policy management vendors with which to integrate. Chief among these are Cisco's Network Admission Control (NAC), Microsoft's Network Access Protection (NAP), and the Trusted Computing Group's Trusted Network Connect (TNC) initiatives. Symantec is an active participant in each of these efforts and offers customers the capability of leveraging these standards to perform NAC functions. Symantec is in a unique position to simplify NAC customer implementations by unifying essential NAC policies in one place: the Symantec Sygate™ Policy Manager.

Network Access Control Technologies and Symantec Compliance on Contact

Customers that deploy Symantec Sygate Enterprise Protection and one of Symantec's current enforcement methods—Self-Enforcement, VPN Enforcement, 802.1x, or API Enforcement—can seamlessly integrate with these new technologies as they become available for general use in the LAN.

Introduction

Enterprises today face many IT challenges. Key among these are combating ever more frequent security incidents and striving to maintain regulatory compliance. Misuse, misconfiguration, and malicious access to critical corporate systems have reached epidemic levels. A common thread among these challenges is the need to ensure protection and control of the endpoint. Many security incidents, for example, are caused by simple desktop misconfigurations and out-of-date security patches. Similarly, controlling which applications can run on the endpoint (and where) goes a long way toward meeting regulatory challenges.

While existing technology, such as patch and vulnerability management systems, gives IT reactive ways to keep systems up-to-date, it does not address a key element of any real solution: keeping systems that are not up-to-date, or are otherwise non-compliant, off the network altogether, and creating a way to repair them without the intervention of IT desktop support or the help desk.

NAC technologies address this problem by auditing the security stance of endpoints before they connect and making appropriate updates before there is a connection to the standard corporate network. This keeps worms and viruses off the network and also allows enforcement of application-level security policy.

Deploying even the simplest NAC solutions requires a great deal of planning and ties together components from many different vendors. Symantec has been a pioneer in the NAC space, releasing Gateway Enforcer, our first product with NAC capabilities, in 2001. Since these first products, which were designed to protect corporate LANs from non-compliant VPN users, Symantec has expanded its NAC solutions to include On-Demand and LAN-based solutions. Along the way, Symantec has developed a unique perspective on how to build large-scale production NAC solutions that realize the promise of the technology: significant improvements in network availability and resiliency in the face of security incidents.

In this paper, we will look at the theory behind this technology, including the Gartner Group's definition of the NAC solution. We will also highlight many of the requirements Symantec has identified as critical for success, and industry efforts in the area such as Cisco's Network Admission Control, Microsoft's Network Access Protection, and the Trusted Computing Group's open platform for NAC, in detail.

What is Network Access Control?

Several industry analysts have weighed in on NAC technology, each with a different set of terminology and slightly different definitions of what NAC solutions should entail. For example, Forrester has coined “Network Quarantine,”² while Meta uses “Endpoint Access Control.”³

Gartner has also created a reference design for Network Access Control.⁴ This design is really a continuous process for evaluating endpoints, mitigating security problems, admitting systems to the network, and monitoring them on an ongoing basis for compliance with a set of globally maintained policies. Since the Gartner framework is one of the most complete, it is worth looking at the process it defines and also the pieces that are required to make NAC work.

Gartner’s NAC process starts with a definition of security policy. Policies outline the security configurations that administrators wish to enforce as a prerequisite for network access. These policies can include any system or third-party software configurations, depending on the needs of the organization.

Typical examples of policies that most enterprises will want to enforce include verification that operating system security patches are up-to-date, antivirus software is running and signature definitions are up-to-date, and endpoint firewall software is running and properly configured. Administrators may also want to perform more advanced checks for the presence of custom security software or special security configurations.

Once policies have been created, a baseline is used to compare the configured policy with systems connecting to the network. An important consideration is that this baseline evaluation must be run regardless of how systems connect to the network. LAN, WAN, wireless, IPSec, and SSL VPNs must all perform this baseline evaluation in order to secure the network.

Based on the results of the baseline, access control is used to give the connecting system the appropriate level of network access. For example, a system that is in compliance with the baseline will receive full access to the network. Systems that are not compliant will either be blocked outright, with no access to the network, or will be sent into a quarantine level of network access for the purpose of mitigation (more often referred to as remediation) to bring the system into compliance. In order for NAC to be of value, the mitigation process must be automated. In other words, systems need to be brought into compliance with security policy without calls to the help desk.

Network Access Control Technologies and Symantec Compliance on Contact

Once systems have undergone mitigation and been admitted to the network, a monitoring technology must be used to ensure that they remain in compliance and do not exhibit anomalous behavior. Systems exhibiting anomalous behavior must be sent into a containment (quarantine) area until they can be repaired.

Therefore, Network Access Control solutions need to:

1. Create a centralized view of security policy
2. Evaluate the security state of a system or user as it connects to the network
3. Implement network access and system remediation policies based on the state of the system
4. Continuously monitor the security state of systems once they are connected

In addition to Gartner's NAC framework capabilities, production NAC solutions need several more characteristics in order to meet the needs of today's large enterprises. These include:

- Available support for multiple access methods (remote access VPN IPSec, dial-up, SSL VPN, wireless, LAN, DHCP, 802.1x, Web access, etc.). In order to be successful, a NAC rollout must be able to guard all of the entrances to the corporate network from day one. Locking the front door won't keep anyone out if the back door or window (via wireless) is wide open.
- Enterprise-class scalability and manageability, including disaster recovery and redundancy to ensure that the NAC solution can scale to meet the needs and growth of the enterprise.
- Powerful information management tools for segregation of policies and management functions. Different roles within an organization often demand different sets of security configurations, and many large corporations delegate these policies to business units, but still want a global view of their policies.
- Flexible deployment strategies, with proven results. Features such as "learning mode" that allow NAC solutions to be first deployed in an audit mode significantly reduce the pain caused by introduction of these new IT practices.
- Extensible, customizable policies that allow administrators to create their own custom NAC rules without requiring help from their NAC vendor.

Network Access Control Technologies and Symantec Compliance on Contact

- Robust location-based policies that are needed to reduce the impact of NAC on the work practices of end users. For example, traveling users often need a much higher level of security when they are on a public network. In the office, this high level of security can interfere with corporate applications and information sharing (even printing). Similar examples apply to corporate wireless networks, field offices, and more.
- Multi-vendor, open solution that supports various technology components existing in enterprise networks today and for years to come. NAC technology is still evolving. There are deployable, proven approaches in the marketplace today. However, investing in a single technology such as Cisco NAC or Microsoft NAP may not yield the desired results.

Symantec Compliance on Contact

The intense focus on NAC technologies also led to several NAC efforts. Operating system and network vendors Cisco and Microsoft have weighed in with their own NAC architectures, and the industry as a whole has created the first set of standards for truly open NAC architectures in the form of the Trusted Computing Group's Trusted Network Connect (TNC) initiative. Symantec is actively involved in all of these efforts.

Using Symantec Policy Manager, IT administrators can centrally manage their network access policies. These policies include built-in checks for well-known antivirus software, personal firewalls, antispyware, operating systems, and security patches. There is also an advanced toolbox for creating custom checks based on files found on the system, applications that are running, registry settings, file dates and checksums, and the like. Adaptive policies allow different policies to be enforced, depending on what type of network connection the user is trying to use: Users connecting via IPSec VPN could be required to have a higher level of NAC compliance, since they are exposed to the public network.

For example, an organization can make policies requiring that any Windows® 2000 system have Service Pack 4, any Windows XP system have Service Pack 2, and all systems be running Symantec AntiVirus™ with up-to-date signature files. Or, they could mandate all of the above, plus other custom security applications and a custom registry key that is set by IT.

Once policies are created, they are enforced on network connect by Compliance on Contact.

Network Access Control Technologies and Symantec Compliance on Contact

Compliance on Contact enforces compliance at each connection point in the corporate network. This includes performing the full set of NAC baseline checks when users connect to the corporate network via IPSec VPN, SSL VPN, wired Ethernet, and wireless Ethernet. Figure 1 illustrates network connection points and the methods used by Compliance on Contact. This is Gartner's baseline step. See Table 1 for a look at supported and tested network infrastructure vendors.

API Integration	802.1x (W)LAN NAC Testing	On-Demand NAC Integration
Cisco	Cisco	Juniper
Juniper	Nortel	Array Networks
Checkpoint	Alcatel	AEP/Netilla
Aventail	Foundry	Aventail
Nortel	Aruba	Aruba
iPass	Extreme	V-One
	HP Procure	Trapeze Networks
	Enterasys	Nortel Networks

Table 1. Enforcement interoperability chart

Once the baseline is performed, access control is the next step in the solution. If systems are in compliance with policy, they are permitted on the network. The techniques used for access control will vary depending upon the type of connection. The Symantec agent will automatically perform a preconfigured operation to bring the system into compliance without user intervention. Once updated, the system will repeat the process and, since it is in compliance, will get access to the corporate network. See Figure 1 for a complete look at the process.

Compliance on Contact continues to monitor the status of the client, and will take action to contain the system if it falls out of compliance.

Symantec Network Access Control (SNAC) uses a three-tier architecture and consists of the following components: Symantec Enforcement Agents, Symantec Enforcers, and Symantec Policy Manager.

Symantec Enforcement Agents

Symantec Enforcement Agents are software installed on desktops, laptops, and servers on the network. These agents report to and receive their configuration from the Symantec Policy Manager and interact with the Symantec Enforcers to report the integrity of the endpoint. Agents are used to monitor policies and automate restoration of compliance to policies. They can be deployed onto endpoints running Microsoft Windows 2000 and above and can be installed on systems running Windows Server™ 2003.

Symantec Enforcers

Symantec Network Access Control Enforcers are a key component in Symantec's network access control capabilities. The Enforcers verify that a host is policy-compliant (e.g., agent is running, required patches installed, etc.) before allowing normal network access. There are three types of Enforcers: Gateway Enforcer, LAN Enforcer, and DHCP Enforcer. All Enforcers can be purchased in the form of an appliance or software. As an alternative to a DHCP Enforcer appliance or software-based DHCP Enforcer, Symantec offers a DHCP Enforcer plug-in that installs directly on Microsoft DHCP servers. This implementation enables the Microsoft DHCP server to act as the enforcement point.

Symantec Policy Manager

The Symantec Policy Manager is a software-based management console that administrators use to set policies that control Symantec Enforcers and Symantec Enforcement Agents. The Policy Manager allows administrators to create and manage policies, assign them to agents, view logs, and run reports. The Policy Manager runs on Microsoft Windows operating systems using an embedded database or can be integrated with a Microsoft SQL Server database. This Policy Manager is the same policy manager used to manage the Symantec Sygate Enterprise Protection product.

Symantec uses seven different technologies to accomplish the complete Universal NAC solution:

1. 802.1x standards-based approach for LAN and wireless
2. DHCP-based approach for LAN and wireless over any infrastructure
3. Gateway Enforcement—in-line API enforcement for any network
4. On-Demand applets for SSL VPNs via "Symantec On-Demand Agent"
5. API-based integration with IPSec VPNs
6. Cisco Network Admission Control v1 technology for Cisco routers
7. Self-Enforcement using Symantec Sygate Enterprise Protection

Here is a look at how each one works.

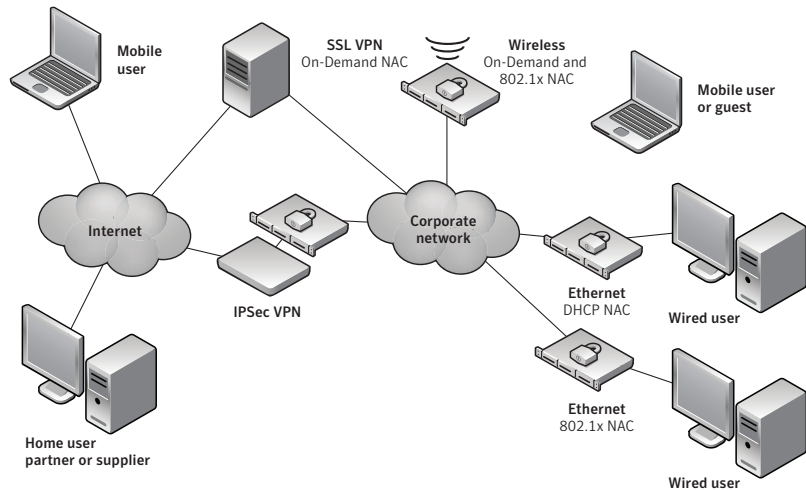


Figure 1. Symantec Universal NAC solution

Symantec 802.1x-based NAC for LAN and wireless

Symantec released one of the first LAN-based Network Access Control technologies in June 2004. This enhancement leverages the IEEE's 802.1x Admission Control Protocol, which is supported by nearly all wired and wireless Ethernet switch makers. Symantec uses this link-level protocol to evaluate endpoint compliance, provide automatic problem remediation, and admit compliant systems onto the corporate net.

802.1x is an authentication protocol designed to increase security by requiring users to provide valid credentials before accessing computer networks. The 802.1x protocol provides far more security than the usual Windows PC login because the network port—not just the PC—is locked from access prior to authentication. Users provide login credentials such as a user name and password, and the switch relays these credentials to an authentication server. Typically, this authentication server is a RADIUS server.⁵ If the credentials are correct, the RADIUS server will send the switch or access point a message authorizing the user's access to the network and configuring service attributes for the user's connection.

During LAN enforcement, the Symantec agent on the endpoint uses 802.1x to transmit compliance information to the network switch, which relays it to a Symantec LAN Enforcer. This LAN Enforcer functions as a RADIUS proxy, verifying the compliance information and optionally consulting with a RADIUS server to verify user names and passwords or multifactor authentication.

If the system is not in compliance, the LAN Enforcer will place it in a quarantine network where it can be remediated without impacting any of the systems that are in compliance with policy. Once Symantec has performed the automated remediation function, the 802.1x protocol will attempt to re-authenticate the user. Since they are now compliant, access to the network will be given, as Figure 2 shows.

Transparent Mode simplifies 802.1x

One important detail about this approach to 802.1x-based Network Access Control is that it does not have to involve all the intricacies of a traditional 802.1x implementation. Administrators have the option of deploying an identity solution, with an 802.1x supplicant and RADIUS back end, or simply deploying the solution for machine-state (NAC) only, which Symantec calls Transparent Mode.

In Transparent Mode, the Symantec agent plays the role of 802.1x supplicant and transmits network access control information, in lieu of user identity information. The administrator simply configures the switch to use the Symantec LAN Enforcer as the RADIUS server, and it authenticates systems based on compliance with NAC policy. No other infrastructure is required. This is the easiest way to get started with a secure, VLAN-switching-based NAC solution.

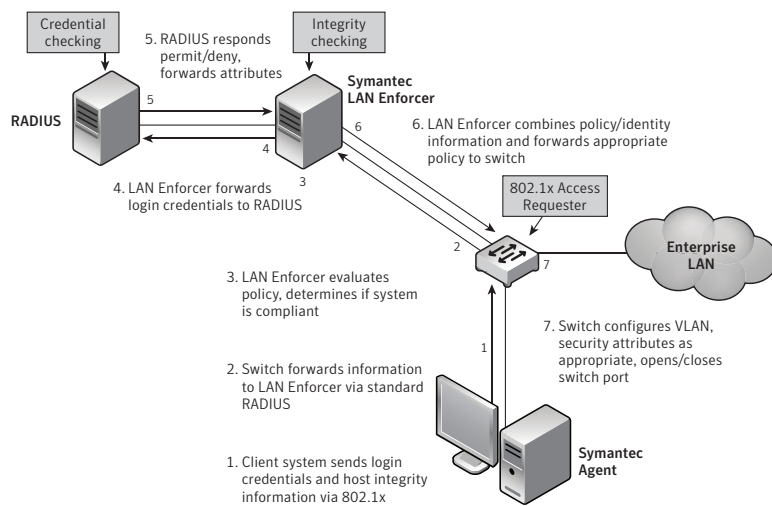


Figure 2. LAN enforcement process

Symantec DHCP-based NAC

802.1x-based NAC offers the maximum amount of security. However, it also requires that the switching infrastructure support 802.1x. Even if the switches support 802.1x, turning it on takes careful planning. The Symantec DHCP-based NAC is designed to address these issues by working in existing network environments with no upgrades of hardware or software.

The Symantec DHCP NAC is deployed in-line between the DHCP server and the network. It works by giving users a “non-routable” or “quarantine” IP address if they are not running an agent, or if their current NAC compliance status is not known. These IP addresses have reduced access to the network. This is accomplished in one of two ways. First, either clients are given special IP addresses in a different IP range, and access control lists are placed on routers to control which networks these special IPs can reach; or second, clients are given IP addresses on regular subnets, but with special static routes to the servers they need to access and no default route to the network as a whole.

Once clients have an IP address, the DHCP Enforcer communicates with the Symantec agent on the client to determine whether or not its policy is up-to-date and if it is in compliance with that policy. If it is not, the agent will trigger the required remediation action to bring itself into compliance. Once in compliance, the client will initiate a DHCP release and renew. Once the DHCP Enforcer receives the renewal request, it will contact the agent and determine that it is in compliance. The system will be granted a DHCP lease on the normal production network, allowing it full access to the network.

Since DHCP NAC works as an in-line DHCP proxy, it is compatible with any existing DHCP infrastructure. Deploying this NAC method involves dropping the Enforcer in front of the DHCP server(s), deciding on a quarantine IP address strategy, and making a few configuration changes on the DHCP server itself. See Figure 3 for an example packet flow.

Systems without agents can be granted network access two ways. First, a non-Windows exception can be made that exempts non-Windows clients from the NAC process. Second, a MAC address-based exemption list can be built. This MAC address list accepts wildcards, allowing the exemption of whole classes of systems such as IP phones using their Organizational Unique Identifiers.⁶

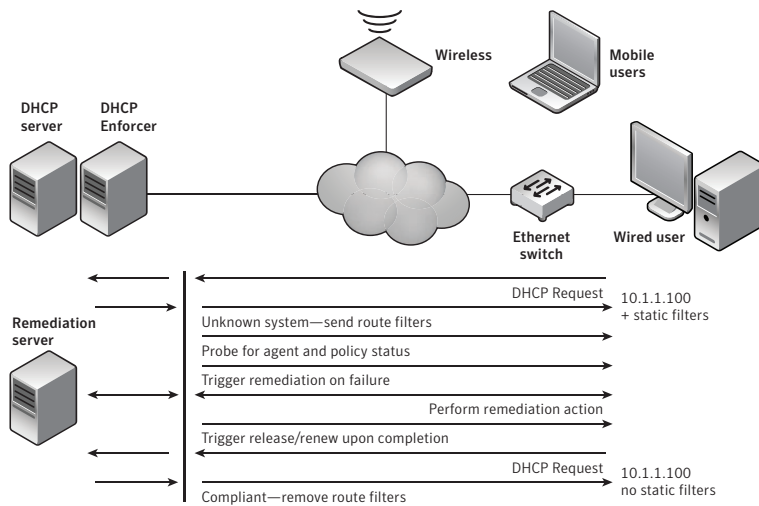


Figure 3. DHCP NAC packet flow

Symantec also offers the option to use a DHCP Enforcer plug-in that installs directly on Microsoft DHCP servers in place of an in-line DHCP Enforcer Appliance (or software-based DHCP Enforcer). This implementation involves a simple plug-in that installs directly on Microsoft DHCP servers and that enables the Microsoft DHCP server to act as the enforcement point. This option eliminates the need to implement an in-line DHCP Enforcer.

Symantec Gateway NAC

Administrators may also want to control access to critical network resources, such as the data center or WAN links to remote offices. The Symantec in-line Gateway Enforcer accomplishes this task. It functions by intercepting traffic and permitting it through based on configured policy. If systems are not compliant with the policy, they can be prohibited from accessing network resources that are behind the Enforcer.

Symantec On-Demand NAC for SSL VPNs

The introduction of SSL VPNs created the need for an additional NAC component that was Web-oriented. To meet this need, Symantec developed the Symantec On-Demand Protection (SODP). SODP includes a Java™-delivered, on-demand NAC component that can evaluate the policy status of a system without the need for a pre-installed, permanently resident agent. SSL VPN gateways

can deliver this agent via their Web authentication page and ensure that systems are compliant before they are allowed access to the corporate resources controlled by the gateway. Juniper, Array Networks, Netilla, and Avenail are a few of the SSL VPN vendors that include SODP-based NAC support in their products.

Guest access

One of the largest challenges of any NAC solution is the admission of guests onto the network. How should the NAC solution safely verify that the guest system does not represent a threat to their network, and what level of network access should a guest be given?

By far the most accurate way to assess any endpoint is to deploy a software agent to audit the endpoint's configuration. Since it is unlikely that visitors will want to install a full-time NAC agent, such as the Symantec Enforcement Agent, onto their laptop, a temporary, on-demand agent is needed.

The primary challenge with on-demand agents is the delivery method for the agent. Deploying an in-line device reduces network performance not only for guests, but also for all hosts. This can be a serious issue for wired Ethernet deployments; it is less of an issue for wireless LANs, where speeds are lower. SNAC overcomes this problem by leveraging the guest VLAN capabilities of modern Ethernet switches, along with the Symantec Gateway Enforcer and Symantec On-Demand Protection agent.

Guests connecting to the network are unable to perform the expected 802.1x or Transparent Mode authentication with the switch and LAN Enforcer. Once this happens, the switch will place the user in the guest VLAN. At this point, administrators have a choice to make: If guests need only Internet access, then this VLAN can be provisioned to provide only this level of access.

If guests need access to the corporate network, a Gateway Enforcer can be used. The untrusted interface is connected to the guest VLAN, and the trusted side is connected to the production network. Users without an agent will be directed to a Web server where they can download the SODP agent. This agent will perform basic NAC compliance checks. It is flexible enough to easily accommodate stringent policies or more flexible ones such as "make sure the user has any antivirus product, and that it is up-to-date." Basic user authentication can also be performed at the time of the download, to enforce that only authorized guests have access to corporate resources. Only traffic from compliant systems will be permitted to pass through the gateway onto the production network (see Figure 4).

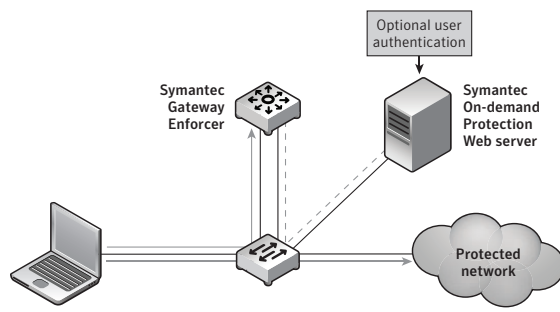


Figure 4. Symantec NAC guest access

Of course, these two models can be combined, so that unauthorized users can only get Internet access and authorized users can access the corporate network. This would be accomplished by implementing the appropriate network architecture and placing the gateway at the appropriate location.

Another simple solution to the guest access problem is to place the Gateway Enforcer directly in line in special circumstances such as wireless and conference room networks. In this topology, the appliance is placed between the conference room switches (or VLANs) and the corporate network. This will force all users through the appliance. Corporate users will authenticate using their agents, and guests will download SODP as explained above. The appliance can forward traffic at rates of up to 1 gigabit per second and can be deployed in redundant topologies.

Symantec API integration

When users connect into the network by IPSec VPN, an API is used to communicate to the Symantec Security Agent installed on the remote system and determine if the system is in conformance with policy. In order for this NAC method to work, the IPSec VPN gateway must support Symantec's Universal Enforcement API. Symantec works with most VPN vendors to ensure compatibility with this API, including Cisco, Nortel, Juniper, Aventail, AEP Networks, and Array Networks. In situations where the VPN gateway does not support the Symantec API, Symantec's in-line Gateway Enforcer can be inserted into the network behind the VPN to perform this function.

Cisco Network Admission Control

Cisco Network Admission Control is an architectural framework and roadmap for NAC technology.⁷ Within the Network Admission Control initiative, Cisco has focused on building protocols and interfaces that can be used by multiple vendors to provide a complete NAC solution. As such, the Cisco Network Admission Control framework requires software from several different vendors to build a complete solution.

Their solution consists of the Cisco Trust Agent (CTA), which must be deployed on all their endpoints. The CTA is responsible for communication with Cisco's NAC-enabled router, reporting the security status of the endpoint as reported in turn by third-party security agents. Second, Cisco's AAA server, Cisco Secure Access Control Server (ACS), authenticates the endpoints and brokers any communication required with back-end third-party policy servers to verify the endpoint's security policy compliance. Thirdly, Cisco NAC-enabled networking equipment is required. Cisco supports CNAC on their newer, higher-end switches and routers. There are different levels of CNAC compatibility, so architects need to be very careful when planning CNAC rollouts—all features may not be available on all platforms.

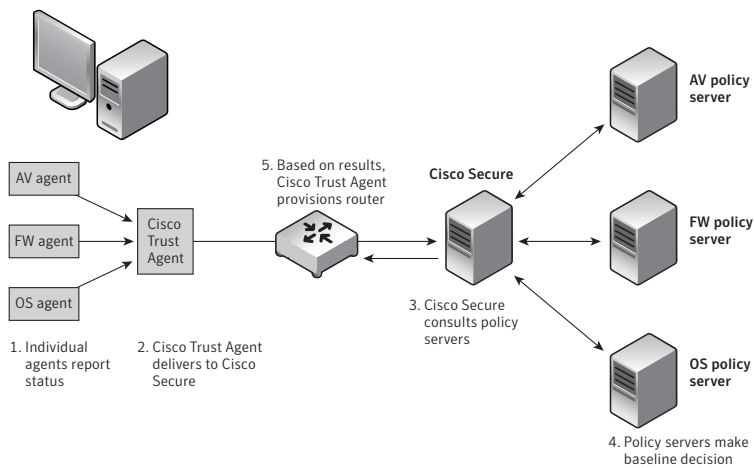


Figure 5. Cisco NAC components and decision-making flow

Network Access Control Technologies and Symantec Compliance on Contact

Cisco's NAC architecture encompasses elements that reside on the client PC, a network transmission protocol the client uses to communicate with the Cisco ACS, a server-to-server protocol, and a set of messages that ACS uses to provision the switch.

As mentioned above, on the client side, Cisco's architecture consists of a "posture assessment" agent called the Cisco Trust Agent, which requires third-party plug-ins to report the status of the endpoints. The Cisco Trust Agent cannot enforce the policies if the system (like a laptop) is connecting to a non-NAC-enabled network. Each plug-in is created by an individual security or OS vendor and separately reports its status. A separate plug-in may be needed for each individual security component: antivirus, antispymware, host IDS, patch, endpoint firewall, and others.

The decision-making component of Cisco NAC is similarly distributed. The Cisco Trust Agent reports its information to Cisco's ACS RADIUS server. This server, in turn, delivers the security information received from the individual plug-ins to corresponding policy servers in the back end: one each for antivirus, firewall, patch, and so on. ACS then collects these responses and makes an ultimate policy decision about what level of network access to give the endpoint. Remediation is the responsibility of the third-party security agents. Figure 5 illustrates version 1 of Cisco's NAC.

There are several drawbacks with this distributed approach. The task of putting together a real solution will fall on the administrator. There are also many components to the system; each application has its own agent and policy server. Too many components mean too many points of failure—especially at network connection time—reducing the effectiveness of the solution and resulting in more network downtime. From a total cost of ownership perspective, each time the administrator wants to change a policy, he or she will need to determine which policy server needs to be updated and make the changes there. Sometimes these policies may also require changes to the Cisco ACS. All these various server elements will need to be running at all times and responding with minimal latency to endpoint integrity messages in order to avoid impacting users' network access experience.

Also, elements need to be Cisco NAC-aware in order to report their status. If the administrator wants to monitor something without an agent, he or she will need to rely on another agent that is Cisco NAC-aware in order to do so. Managing several Cisco NAC-aware components will increase the complexity of maintaining a Cisco NAC solution.

There are also several network infrastructure–related issues for customers to sort out. The issue of how to support non-Cisco hardware is one of these dilemmas. Cisco has plans to submit some components of the protocols to standards bodies at some time in the future. Whether a single standard will be adopted by all vendors remains to be seen.

Many of these problems can be eliminated by using Symantec’s Compliance on Contact technology, either by itself or in conjunction with Cisco’s Network Admission Control.

Cisco and Symantec together

Customers can choose to use Cisco’s NAC framework with Symantec’s mature agent and policy server products. Customers who deploy Symantec’s Compliance on Contact technology via Cisco’s NAC transport will enjoy the advantages of Compliance on Contact via enforcement methods available through NAC-enabled components. Advantages include the central administration of security policies and monitoring compliance to overall endpoint security posture.

By uniting policy administration in one management console, the entire NAC solution is dramatically simplified, both in terms of deployment complexity and ongoing support. Instead of installing multiple plug-ins on each endpoint and managing separate policy servers for each security element, a single agent and policy server are needed, as shown in Figure 6.

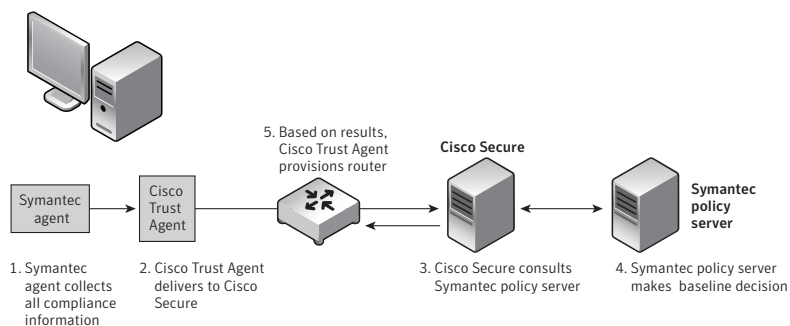


Figure 6. Symantec simplification of Cisco NAC

Furthermore, the problem of how to support a non-Cisco network infrastructure is also eliminated by the joint Cisco/Symantec solution. The Symantec LAN Enforcers and central policy management system are designed to be used in mixed environments. Individual endpoints or sections of the network can run any of the various modes of policy enforcement independently of the other sections. This allows almost any type of network infrastructure to be deployed and a consistent set of policies to be enforced through the Symantec solution. If Cisco NAC is the preferred network protocol for enforcement, it could be deployed throughout the enterprise, and other enforcement methods (such as API or 802.1x) could be deployed in sections of the LAN where other vendors' networking equipment exists.

If uniformity of enforcement techniques is desired, Symantec's API and 802.1x solutions can be used throughout the network, even on the Cisco equipment. In this case, a single solution can be used for NAC compliance throughout the enterprise, as shown in Figure 7. The approach any given enterprise should choose will depend on the type of equipment (authentication solutions, switches, VPN, dial-up, etc.) they have installed and their own preference of protocols.

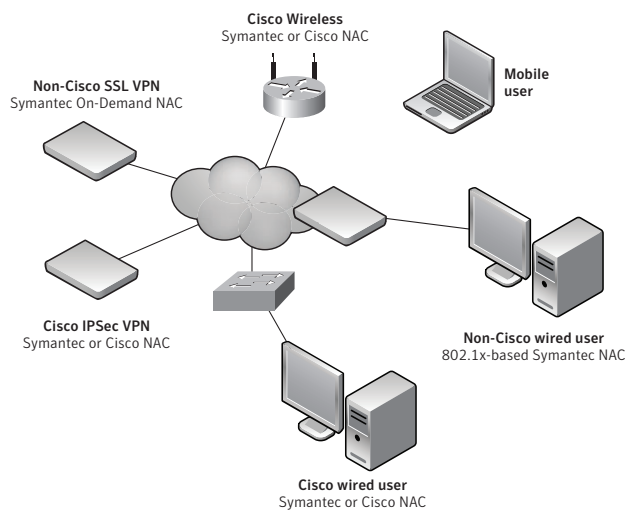


Figure 7. Typical best-of-breed network

NAC Method	Symantec Support
Gateway Enforcement	June 2001
API Enforcement	December 2001
Self-Enforcement	August 2003
On-Demand Enforcement	September 2003
802.1x (W)LAN Enforcement	February 2004
DHCP Enforcement	Mid-2005
Cisco NAC	Mid-2005
Microsoft NAP	Longhorn

Table 2. Symantec NAC methods review

Future efforts

More proposed solutions to Network Access Control loom on the horizon. Microsoft and the Trusted Computing Group have both announced their own approaches to this problem as well.

Microsoft's Network Access Protection

Microsoft has weighed in on Network Access Control, with its own Network Access Protection (NAP) architecture.⁸ Like the Cisco NAC architecture, NAP is a framework upon which third-party vendors can build complete NAC solutions.

From a functional perspective, Microsoft and Cisco have designed very similar frameworks. Each has components that perform similar functions and high-level solution diagrams that look nearly identical. For example, instead of Cisco Trust Agent, Microsoft has the Quarantine Agent; instead of Cisco ACS RADIUS server, Microsoft has the IAS RADIUS server. Details regarding the compatibility between these two architectures are not available yet, leaving customers without a clear NAC direction. Similarly, vendors of security and antivirus software products must do twice as much work to be able to support both of these frameworks. It is worth noting that Symantec LAN Enforcer today supports both Microsoft IAS and Cisco ACS, enabling the network architects to keep their network authentication architecture intact while introducing/overlaying either NAC framework onto their infrastructure.

Network Access Control Technologies and Symantec Compliance on Contact

The Microsoft NAP solution is only expected to support newer Microsoft operating systems, possibly only Windows XP SP2 and above. This presents two implementation problems:

1. How will older systems, which are often more vulnerable to exploit, be kept off the network if they are not compliant?
2. How will compliance be ensured for non-Microsoft products?

Microsoft is bundling support for the NAP solution into the Windows Server “Longhorn” operating system, which is not expected before 2007. Until that time, no production-quality NAP components will be available. So far, over 35 industry companies, including Symantec, have joined Microsoft’s NAP initiative and plan to release products around the time that Longhorn ships.

In the same way that Symantec supports Cisco NAC seamlessly alongside other NAC technologies, Symantec plans to support NAP along with other technologies as well, allowing customers to deploy the technology they feel best fits their needs.

Trusted Computing Group’s Trusted Network Connect

The Trusted Computing Group, a consortium of over 80 IT industry companies, has sponsored the Trusted Network Connect standard.⁹ This standard is similar in intent and architecture to the Microsoft and Cisco efforts; however, it has been shaped by all of the companies that are part of the consortium, which any company can join. In this way, the TNC specification represents a truly open standard that is intended to operate on any type of network hardware infrastructure and any host operating system. See Figure 8 for a summary of the components of each architecture.

	Symantec Only	CNAC	NAP	TNC
Central Agent	Symantec Protection Agent	Cisco Trust Agent	Quarantine Agent	Integrity Agent
Enforcement Points	802.1x, VPN, SSL, In-Line, DHCP	L3 routers, L2 later	MSFT-only DHCP, more later	802.1x initially
Multiple policy agents per system?	Not required	Posture Plug-In	System Health Agents	Integrity Agent Plug-In
Policy aggregation server required?	Not required	Cisco ACS RADIUS Server	Microsoft IAS RADIUS Server	Integrity Server
Multiple policy servers required?	Not required	Posture evaluation servers	System Health Verifiers	Integrity Server Plug-In

Figure 8. NAC architecture components summary

Network Access Control Technologies and Symantec Compliance on Contact

Open standards have been the key to success in the growth of the Internet and IT technologies. An open standard for NAC should encourage the development of NAC agents for other operating systems, either by OS vendors themselves, third parties, or the open source community. A standards-based approach to this problem would also reduce the burden on individual companies wishing to make their products NAC-ready. A single effort would be needed, instead of porting to two or more competing architectures.

The Trusted Computing Group is also responsible for developing the Trusted Platform Module (TPM). This hardware component is used to increase the security and trustworthiness of endpoint computer systems. Many vendors, including HP and IBM, are shipping systems with TPM support today. Ultimately, the TCG will be incorporating support for the TPM into the TNC standard.

Once TNC standards include the TPM, corporate IT administrators will be able to determine with much greater certainty that a given computer requesting access to the network is indeed the system it is claiming to be and that the information they are relaying is, in fact, true. The TNC standard is the only one with a roadmap toward ensuring the authenticity of the client/server NAC communication. This will be a big benefit and will increase the security of the network.

Conclusion

Network Access Control technology has the promise to dramatically reduce both the number and severity of security events and aid in regulatory compliance. Although there is a significant amount of uncertainty surrounding the direction of NAC standards, Symantec's Compliance on Contact technology delivers on the promise of NAC today by enforcing policy via a variety of network protocols and access methods. This flexible approach to the problem helps ensure the success of implementations as well as IT investment protection.

By partnering with Cisco, Microsoft, and the Trusted Computing Group, Symantec offers a solution that doesn't make administrators choose among these three architectures, and even allows administrators to use the best elements of each to solve their network access problems.

References

- ¹ Greg Young, John Pescatore, *Securing the Network Perimeter Is More Important Than Ever*, March 23, 2005; Gartner ID Number: G00126635
- ² Laura Koetzle and Robert Whiteley, *Making Sense of Network Quarantine*, Forrester, August 2004.
- ³ Tom Scholtz, *The Benefits of an Information Security Architecture*, Meta Group, December 2004.
- ⁴ Pescatore, Nicolett, and Orans, *Protect Your Network with Network Access Control*, Gartner, Inc., 2004.
- ⁵ <http://en.wikipedia.org/wiki/802.1x>.
- ⁶ <http://isp.webopedia.com/TERM/O/OUI.html>.
- ⁷ Cisco Network Admission Control, Cisco, www.cisco.com/en/US/netsol/ns466/networking_solutions_package.html.
- ⁸ *Microsoft Network Access Protection*, Microsoft, www.microsoft.com/windowsserver2003/technologies/networking/nap/default.mspx.
- ⁹ *Trusted Network Connect*, Trusted Computing Group, [www.trustedcomputinggroup.org/downloads/TNC_NI_collateral_10_may_\(2\).pdf](http://www.trustedcomputinggroup.org/downloads/TNC_NI_collateral_10_may_(2).pdf).

About Symantec

Symantec is the world leader in providing solutions to help individuals and enterprises assure the security, availability, and integrity of their information.

Headquartered in Cupertino, Calif., Symantec has operations in more than 40 countries.

More information is available at www.symantec.com.

For specific country offices and contact numbers, please visit our Web site. For product information in the U.S., call toll-free 1 (800) 745 6054.

Symantec Corporation
World Headquarters
20330 Stevens Creek Boulevard
Cupertino, CA 95014 USA
+1 (408) 517 8000
1 (800) 721 3934
www.symantec.com

Copyright © 2006 Symantec Corporation. All rights reserved. Symantec, the Symantec logo, Sygate, and Symantec AntiVirus are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Microsoft, Windows, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Java is a trademark or a registered trademark of Sun Microsystems, Inc., in the U.S. or other countries. Other names may be trademarks of their respective owners. Printed in the U.S.A.
09/06 10753676