Cisco Network Admission Control and Microsoft Network Access Protection Integration

Deployment Guide

Version 1.0

Introduction

This document provides an overview and deployment considerations for integration of the Cisco Network Admission Control (NAC) and Microsoft Network Access Protection (NAP) solutions (referred to here as NAC-NAP). This document is intended for network engineers and architects who are deploying NAC-NAP and need to understand the basics of Cisco NAC and Microsoft NAP integration and design.

Cisco Network Admission Control and Microsoft Network Access Protection Integration Overview

The Cisco NAC and Microsoft NAP solutions together provide the capability to gather identity and health-state information from an endpoint, determine the security policy compliance of the endpoint, provide remediation services, and enforce network access policies based on the compliance of the endpoint.

With the integration of these two solutions, an administrator can verify the health status of a Microsoft Vista client, provide remediation capabilities, and provide dynamic policy enforcement on the network infrastructure.

- For additional information about the Cisco NAC solution, see http://www.cisco.com/go/nac.
- For additional information about the Microsoft NAP solution, see http://www.microsoft.com/nap.

Goals of Interoperability

Cisco and Microsoft have collaborated to enable rich interoperability between the Cisco NAC and Microsoft NAP solutions. This interoperability enables customers to gain the benefits of both NAC and NAP while using and preserving their investments in their Cisco NAC network and Microsoft NAP desktop and server infrastructure. Primary features and benefits of the solution include:

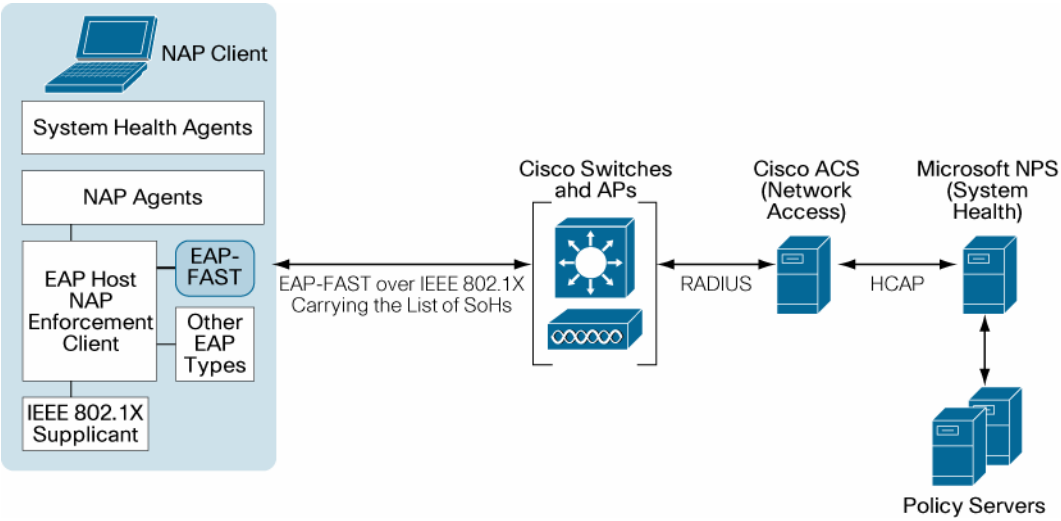
- Interoperability and customer choice
- Investment protection
- Single agent included in Microsoft Windows Vista
- Independent software vendor (ISV) integration ecosystem
- Agent deployment and update support
- Cross-platform support

Architecture

Working together, Cisco NAC and Microsoft NAP assess the state, or posture, of a host to prevent unauthorized or vulnerable endpoints from accessing the network. Typical hosts are desktop computers, laptops, and servers, but may also include IP phones, network printers, and other network-attached devices (Figure 1). This section discusses each component in the NAC-NAP interoperability architecture.

The NAC-NAP solution components include Cisco Secure Access Control System (ACS) version 4.2, Cisco 802.1X-capable Catalyst Switches, Microsoft Network Policy Server (NPS), and Microsoft NAP-enabled Vista operating system. The Cisco NAC Appliance does not support NAP at this time and is not part of the solution.

Figure 1. NAC-NAP Deployment Architecture



Host

- NAP client (Microsoft): The NAP client computer is a computer running Windows Vista or Windows Server 2008 that sends its health credentials as a list of statements of health (SoHs).

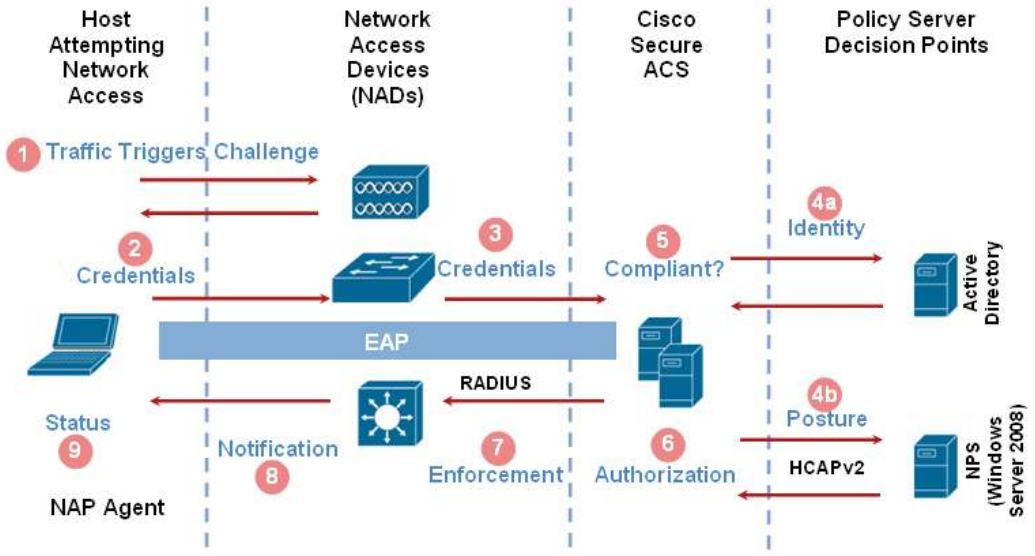
Enforcement

- Network access devices (Cisco): Network access devices (NADs) enabled for NAC (which include switches and wireless access points) provide network access to clients and serve as network enforcement points.

Decision and Remediation

- Access control server (Cisco): Cisco Secure Access Control Server (ACS) for Windows authorizes network access for clients by validating the administratively specified client attributes, which could include the identity of the user and the computer and the overall health state of the client. Cisco Secure ACS sends an access profile to the NADs to grant the appropriate level of network access for the client based on the authorization result. Note that validation of the client health state attributes and assignment of the overall client health state in the interoperability architecture are performed by the Microsoft Network Policy Server.
- Network policy server (Microsoft): A Microsoft Network Policy Server (NPS) validates the computer's system health and provides remediation instructions if needed.
- Health requirement servers (Microsoft or third party): Health requirement servers provide the current system health state for Microsoft NPSs. Policy servers integrate with Microsoft NPSs through the NPS system health validator (SHV) API (Figure 2).

Figure 2. NAC-NAP Components and Authorization Process



How the NAC-NAP Interoperability Architecture Works

Upon connection to the network, the client provides a set of credentials that are validated to authenticate and authorize the appropriate level of network access. These client credentials include user and computer identity credentials in addition to health credentials. Clients that are noncompliant can be quarantined, remediated, or similarly treated before being granted normal network access.

In the interoperability architecture, the client, using the NAP agent, provides its credentials for validation. The list of SoHs along with user and computer identity is sent to a Cisco Secure ACS with Extensible Authentication Protocol–Flexible Authentication via Secure Tunneling (EAP-FAST) carried over IEEE 802.1x. If the NAP agent sends its list of SoHs to validate system health, the Cisco Secure ACS will send the list of SoHs to a Microsoft NPS for validation using the Cisco Host Credentials Authorization Protocol (HCAP). The Microsoft NPS evaluates the SoH responses (SoHRs) against the configured health requirements and returns the health validation results, which include the individual SoHRs and the overall client system SoHR (SSoHR), to the Cisco Secure ACS using HCAP. The Cisco Secure ACS evaluates all the credential validation results (which include user and computer identity in addition to the SSoHR) to select and send the appropriate access profile to the NADs to grant the authorized level of network access for the client. The Cisco Secure ACS also returns the SoHRs and the SSoHR to the NAP agent on the client with EAP-FAST carried over IEEE 802.1x. Noncompliant clients that are quarantined are automatically revalidated upon remediation to provide a transparent end-user experience.

NAC-NAP Solution Components

The Cisco NAC and Microsoft NAP solutions are integrated with a variety of Cisco and Microsoft software and hardware components, summarized in Table 1 and discussed here.

Table 1. NAC-NAP Components

Component	Type	Authentication Method
Microsoft Windows Vista with Service Pack 1	Operating system	
Cisco EAP-FAST Module	Authentication method module	IEEE 802.1x
Cisco Secure ACS for Windows and Solution Engine Version 4.2	Authentication, authorization, and accounting (AAA) policy server	Any
Microsoft Windows Server 2008 Network Policy Server	Policy server (part of Windows Server 2008)	Any

Component	Type	Authentication Method
Cisco Catalyst® 2960, 3560, 3750, 4500, 4900, and 6500 Series Switches	NAD	IEEE 802.1x
Cisco Aironet® 1100 and 1200 Series Wireless Access Points	NAD	IEEE 802.1x

For more information, please refer to following release note http://www.cisco.com/en/US/netsol/ns812/networking_solutions_sub_solution_home.html.

Microsoft Windows Vista with Service Pack 1

Interoperability of the NAC-NAP solution is available with Windows Vista with Service Pack 1; currently this is the only platform that supports this interoperability. Windows Vista introduces new services that enable NAP functions. The client architecture consists of a layer of system health agents (SHAs), the NAP agent, the host-based EAP NAP enforcement client, EAP methods for authenticating account credentials and indicating health status, and EAP supplicants that allow the client to send EAP messages over IEEE 802.1x.

Cisco EAP-FAST Module

In NAC-NAP architecture, EAP-FAST is deployed as the authentication method. EAP-FAST is one of the most secure tunneling EAP methods, and it was ratified as RFC 4851 in 2007. The Cisco EAP-FAST Module enables users to send both identity and health state information to the authentication server over IEEE 802.1x. This module can be installed using group policy on Microsoft Active Directory or through Microsoft Windows Update.

Cisco Secure Access Control Server for Windows 4.2

Cisco Secure ACS is an AAA server with RADIUS capabilities that extend beyond identity authentication to handle the authorization of health state credentials from a host. Cisco Secure ACS then maps the resulting policy decision to a network access profile that is provisioned on the NAD for enforcement. In NAC-NAP integration, Cisco Secure ACS is used to delegate health state authorization decisions to the Microsoft NPS to improve scalability, delegate the decision for a specific policy domain, or handle proprietary attributes. Cisco Secure ACS 4.2 supports NAC-NAP integration with enhanced HCAP to the Microsoft NPS.

Network Access Devices

NADs enforce network access based on an authorization policy from the AAA server and communicated through RADIUS attributes.

Upon detection of a host on a Layer 2 interface, the NAD attempts to establish communication with the agent on a host before sending a request to the AAA server to start the authorization process. The NAD and the agent communicate through a Layer 2 mechanism (IEEE 802.1x). The agent for a host response is forwarded by the NAD to the AAA server to initiate an access request. After the host trusts the AAA server and they negotiate a secure tunnel, the agent responds with its identity and health state credentials. The agent in this context is host-based EAP along with required modules such as EAP-FAST. In this process, the NAD acts as a relay agent between the host and AAA server for all messages in the exchange. When authorization is completed by the AAA server, the server sends a network access profile to the NAD for enforcement on the host.

Detection of a health state change on the Vista client triggers an IEEE 802.1x control packet to the NAD, resulting in reauthentication. With this technology, the client-side health status can be actively monitored and enforced using the IEEE 802.1x mechanism.

Table 2 lists supported platforms and versions

Table 2. Supported Platform List and OS Versions

Platform (Supervisor)	OS Type	OS Version
Cisco Catalyst 6500 Series Supervisor Engines 32 and 720	Cisco IOS® Software	Cisco IOS Software 12.2 (33) SXH or later
Cisco Catalyst 6500 Series Supervisor Engines 2, 32, and 720	Cisco Catalyst OS	Cisco Catalyst OS 8.6 (1) or later
Cisco Catalyst 4500 Series Supervisor Engine II-Plus, II-Plus-TS, II-Plus-10GE, IV, V, and V-10GE	Cisco IOS Software	Cisco IOS Software 12.2 (37) SG or later
Cisco Catalyst 4900 Series Switches	Cisco IOS Software	Cisco IOS Software 12.2 (35) SE or later
Cisco Catalyst 3570 and 3560 Series Switches	Cisco IOS Software	Cisco IOS Software 12.2 (35) SE or later
Cisco Catalyst 2960 Series Switches	Cisco IOS Software	Cisco IOS Software 12.2 (35) SE or later

Protocols

This section describes the protocols used in NAC-NAP integration.

EAP

Extensible Authentication Protocol (EAP) is a request and response protocol that is capable of exchanging identity and authentication credentials between a host and an AAA server. EAP supports a variety of authentication methods including Microsoft Challenge-Handshake Authentication Protocol Version 2 (MSCHAPv2), certificate-based authentication, and public key infrastructure (PKI). EAP is defined in RFC 2284.

EAP-FAST

Flexible Authentication via Secure Tunneling Extensible Authentication Protocol (EAP-FAST) is a Transport Layer Security (TLS) based RFC 3748–compliant EAP method. A draft for EAP-FAST has been submitted by Cisco to the IETF and ratified as RFC 4851 in May 2007.

The tunnel establishment relies on a protected access credential (PAC) that can be provisioned and managed dynamically by EAP-FAST through an AAA server.

EAP-FAST uses symmetric key algorithms to achieve a tunneled authentication process. The tunnel establishment relies on a PAC that can be provisioned and managed dynamically by EAP-FAST through the AAA server.

- Phase 1: Use the PAC to mutually authenticate the host and server and establish a secure tunnel.
- Phase 2: Perform client authentication in the established tunnel.
- Phase 0 (optional): Enable the client to be dynamically provisioned with a PAC (used infrequently).

Additional information about EAP-FAST and the options available for NAC are discussed in the deployment section of this document.

HCAP

The Host Credential Authorization Protocol (HCAP) provides communication between an ACS and a NAC posture validation server. HCAP uses an HTTP(S) session to provide secure communication and exchange of EAP-based credentials between Cisco Secure ACS and vendor servers. In the NAC-NAP interoperability architecture, this protocol is used for communication between the Cisco Secure ACS and Microsoft NPS to transport SoH information.

Cisco Secure ACS forwards client credentials to one or more vendor servers and receives posture token response and optional notification messages from each vendor server.

NAC Assessment Methods

NAC-NAP integration can use a variety of methods to trigger identity and posture validation of hosts attempting to access the network. In most cases, the method used depends on the existing security policy and the type of NAD through which the host is attempting to connect. The NAC-NAP assessment methods include:

- Assessment using IEEE 802.1x
- Agentless hosts

The agentless host assessment method is discussed in a later section.

IEEE 802.1x Method

The IEEE 802.1x method uses the IEEE 802.1x protocol to provide identity information for user and host authentication with the addition of the EAP-FAST protocol to also transport posture information for the host. The IEEE 802.1x method triggers the assessment of a host through IEEE 802.1x on a Layer 2 switch port.

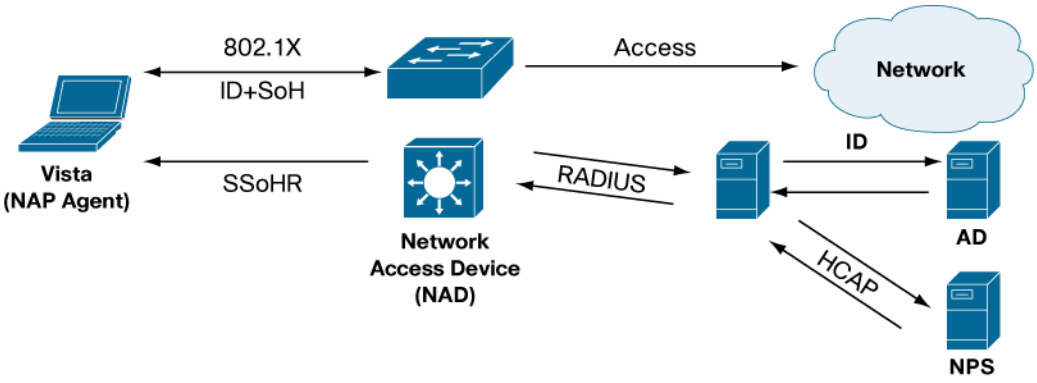
The IEEE 802.1x method in NAC-NAP integration requires a supplicant that supports EAP-FAST for the EAP method to carry identity and posture information in the TLS tunnel. The natively embedded supplicant on Windows Vista with Service Pack 1 supports the Cisco EAP-FAST Module and EAP–Generic Token Card (EAP-GTC), EAP-MSCHAPv2, and EAP-TLS as its inner authentication methods.

The identity information provided by IEEE 802.1x can include both user and machine information for the host. User and machine authentication are covered in the deployment considerations section of this document.

Policy enforcement for the IEEE 802.1x method is performed through dynamic VLAN assignment on the switch. The dynamic VLAN assignment is based on the posture token assigned. After the Cisco Secure ACS determines which posture token to assign to the host, the VLAN information is passed to the switch in RADIUS attributes 64, 65, and 81 as defined in RFC 3580. Access control lists (ACLs) are assumed to have been previously configured to properly segment the VLAN traffic.

Figure 3 and the following steps illustrate the NAC Layer 2 802.1x authentication process.

Figure 3. NAC Layer 2 802.1x Authentication Flow



1. IEEE 802.1x connection is set up between the NAD and the endpoint.
2. NAD requests credentials from the endpoint (EAP over IEEE 802.1x).
3. The credentials include the user, device, and posture.
4. Windows native supplicant service sends credentials to the NAD (EAP over IEEE 802.1x).
5. The NAD sends credentials to the AAA server (EAP over RADIUS).
6. User and device credentials are sent to authentication databases (Active Directory).
7. The AAA server proxies portions of posture authentication to the Microsoft NPS (HCAP).
8. The AAA server validates the credentials and determines authorization rights.
9. For example, visitors may be given GUEST access, and unhealthy devices may be given QUARANTINE access.
10. The AAA server sends authorization policy to the NAD (VLAN assignment).

11. Notification may also be sent to applications on the host.
12. The host is assigned to the VLAN and may then gain IP access (or be denied access or restricted).

With the IEEE 802.1x method, the session timeout value is used to initiate the reauthentication process. This value can be locally set on each switch or configured in the Cisco Secure ACS with RADIUS attribute 27. If the value is configured in the Cisco Secure ACS and the NAD is configured to accept AAA assignments, the Cisco Secure ACS value will override the default value configured in the switch.

Agentless Host Handling

An agentless host is a host that does not have a NAP agent or supplicant installed and therefore cannot participate in the identity and posture validation process. An unknown host, in a general sense, is a client without posture agent software. These clients may be IP devices such as IP phones, network printers, or other IP devices. Any PCs or workstations that do not have a NAC-NAP agent are also considered unknown hosts. This situation is most often encountered with contractor and guest computers, but it can also be encountered with managed hosts running non-Windows platforms, non-Vista Windows platforms, or others.

NAC-NAP Deployment Methodology

Cisco NAC and Microsoft NAP integration is a collaborative security solution. Careful planning by administrators will help them avoid issues that often delay deployments. The major areas for concern are:

- Complexity: NAC-NAP integration is a solution requiring many components and technologies to work together, often from multiple vendors. Just the mechanics of getting the agents, network access devices, and policy servers installed makes the solution complex. Methodically planning and testing exceptions for the large number of agentless devices and typical network access methods is critical to deployment so that entire device classes are not locked out of the network when NAC-NAP is first enabled.
- Culture: NAC is a fundamental change in the way users access the network and administrators manage it. Users must now authenticate every time they log in and run software, which could be perceived as an annoyance rather than proactive security. Administrators must understand how to segment their networks for production versus quarantine environments, which may require changes to their current architectures. Even within network, security, and IT departments, a large effort will likely be required to reach consensus on a single security policy governing network access.
- Politics: Management and IT security group will need to collaborate to define NAC-NAP policies and access control across the network. The authentication decisions enforced by NAC-NAP are based on security policies for operating system patches and software agents or applications that are typically outside the control of the network security and operations teams. Therefore, NAC deployments often require continuous communication and collaboration across two or more departments for all stages of the process. Depending on the working relationship between these organizations, the political challenges can dwarf those of the technology.

This section presents a methodology for planning your NAC-NAP deployment taking into account many of these challenges. The number of steps and variables to consider at each stage will be unique for your organization. By building upon incremental levels of success at each stage, you should be able to lead your organization through what will likely be the first of many such collaborative exercises as network, operating system, and application security boundaries continue to blur.

Identifying Use Cases

The first step in your deployment is to define your end goal and plan how you are going to reach it. You must answer these questions before configuring devices or installing any software. This process can take minutes or months, depending on the granularity of the policy, the amount of consensus required by the departments involved, and the number of exceptional use cases and devices.

Scope: Create use cases that define the scope of your deployment. To do so, answer these questions:

- What problems do you want NAC-NAP integration to solve?
- Where is your greatest risk of unauthorized or unpatched devices?
- Where do you want to enable NAC? For all LAN network edge endpoints? For wireless endpoints?
- Will you authenticate devices or users, or both?
- Do you have the authority to mandate and install required software on all hosts?
- What devices in your network are agentless (printers, copiers, sensors, cameras, etc.) and how will you identify them and allow them authorized access?

Security policy: Start by writing a basic security policy for your organization. Remember: If any administrator cannot quickly understand it, neither will your users. It is good to start thinking in terms of:

- Managed hosts and their required operating systems, agents, and applications
- Unmanaged hosts and how you will limit guests and contractors to only the Internet
- Agentless hosts such as printers, copiers, and other specialized, network-attached appliances
- Exceptional network access scenarios such as new assets, preboot execution environment (PXE) boot imaging, directory joins, and wake-on-LAN operations

Size: How large must you scale the deployment? In what time frame? Do you have the tools and resources to do the job?

Scalability and availability: Will the additional authentications require more AAA and directory servers to handle the load? Remote sites without a redundant link may be partially locked out without a redundant WAN link or local AAA server.

Best Practice:

An absolute minimum of two Cisco Secure ACSs should be included in any deployment for redundancy and availability.

Collaboration: Management and IT security group will need to collaborate to define NAC policies and access control across the network. Which teams will you need to work with for consensus and success? Depending on how your organization works, more than one of the following groups may be involved: information security, desktop, server, antivirus, directory services, security operations, and patch teams.

Success metrics: What objective measures you will use to demonstrate progress and return on investment (ROI) for your efforts? Increased network host visibility, secured public or semipublic ports, network access records for audits, rogue device detection, and enforced patch management are common.

Lab Integration and Verification

The next step is to integrate the necessary components and services in a nonproduction lab environment. Testing your use cases can easily take a week or more—longer if you want to verify long-term stability or conduct scalability testing for your environment.

Best Practice:
Thoroughly test all network access use cases in the lab to prevent surprises when you enable NAC-NAP in your production network. Handling of guests, contractors, and agentless devices are the most important cases.

Solution assembly: Complete and verify the configuration, integration, and operation of required solution components. Understand the mechanics of NAC-NAP protocols, policies, and logs for future troubleshooting.

Scenario testing: Verify that all network access scenarios identified in your planning work as expected with NAC-NAP. These scenarios include combinations of the following items:

- Network edges: LAN, WLAN, and guest portals
- Managed hosts: Desktops, laptops, IP phones, PDAs, printers, and many other network-attached specialized devices
- Platforms: Windows, Mac OS X, Linux, Pocket PC, or others
- Unmanaged hosts: Agentless, guest, new assets, reimaged hosts, and rogue devices
- Enforcement options: Segmentation and revalidation with VLANs and timers
- Remediation: Updating of noncompliant hosts with Windows updates, signature files, patch management, or other mechanisms

Pilot preparation: Determine the software update method and profile distribution method for modules required for NAC-NAP integration. Also distribute any digital certificates required to start your production pilot

Scalability and availability: Test and verify any scalability or failure scenarios that you anticipate. Determine what features or additional hardware you will use for successful failover.

NAC Pilot I: Small, Monitored Deployment

Hopefully, you tested a representative sample of network-attached devices and access methods in your lab environment and worked through any surprises. When migrating your NAC lab configuration to the production network, the most critical step is to not enforce compliance and maintain connectivity to the production network.

Best Practice:
Do not enforce network quarantine for noncompliant hosts when first enabling NAC-NAP in your production network. The goal at first is to allow full access after RADIUS authentication. You do not want to quarantine hosts until you can easily and successfully remediate them.

All hosts that connect to the network should obtain the same level of network access as they did before you enabled NAC-NAP. All IEEE 802.1x clients should be assigned to the production VLAN, and any agentless hosts should default to the production VLAN. Do not enforce compliance at this stage because you simply want to get the mechanics of the NAC-NAP infrastructure working in the production environment.

Infrastructure: Move the NAC-NAP server components or copy their configurations to the production network. Verify that any enforcement options such as quarantine VLAN assignment are disabled or reconfigured to allow production access.

Desktop deployment: Enable the NAP agent and install required modules on a small number of desktops; a recommended number is 5 to 20. Verify that there are no conflicts with any other desktop hardware or applications.

Enable NAC-NAP: Enable your chosen NAC-NAP method to authenticate users and devices. Verify that all devices have access and are not physically quarantined.

Public ports: Enable NAC-NAP for network ports in public spaces for a few printers or photocopiers and conference rooms. This step will test agentless devices and detect whether and when anyone plugs into ports in shared and open areas.

NAC Pilot II: Larger, Monitored Deployment

After the system has been working smoothly for a week or two in your production environment, you can increase the scale of your deployment. You can increase the number of managed hosts and add other network edges or locations. You should run this expanded pilot for several weeks without any major problems before moving to enforcement. You have several specific goals at this stage.

Add more hosts: Increase the number of managed hosts to 50, 100, or more. Also add exceptional cases such as guests, contractors, and more agentless appliances. Tweak revalidation timers on the Cisco Secure ACS as needed to meet your desired level of ongoing host checking.

Scalability and availability: Add hosts, access edges, and locations for more diversity in your deployment. There should not be any real stress on the servers at this point, but you should create an artificial outage to test the failover from one Cisco Secure ACS to another. Adjust load balancing to achieve the desired level of response.

Host registration: Create and test your process for adding new devices to the network, especially if they must be enrolled in Active Directory or added to a MAC authentication database.

Patch preparedness: Verify that your patching and remediation process works for your users regardless of whether it is automated or relies on web downloads or manual installation. You do not want to quarantine hosts until you can remediate them.

Support desk: Create and test your process for the internal support desk to troubleshoot problems for users who call with connectivity problems related to quarantining.

Log review: When analyzing your AAA logs, did you find any unexpected errors or chain of events? Did you detect any unexpected devices on your network? Are you ready to enforce quarantine for noncompliant devices?

NAC Pilot III: Small, Enforced Deployment

When you feel confident that your system is working smoothly and you have thoroughly communicated the potential for quarantine to your users, you can enable enforcement. This step should be a simple matter of changing the Cisco Secure ACS policy to download the quarantine VLAN. Be sure to alert your colleagues in the desktop, server, patch, and help desk groups of the pilot program and provide any new network access requirements for this pilot group.

Enable enforcement: Update and replicate the Cisco Secure ACS configuration for quarantine enforcement with VLANs.

Patch problems: Work through any problems with host patching if your deployment blocks a service.

Guests: Verify that guests can now reach only the Internet and no internal resources. If you are using a guest portal, this should be working.

NAC Production Deployment

You can now increase your production deployment with enforcement as you feel comfortable. Pay special attention to the load on your Cisco Secure ACSs and adjust revalidation timers or add servers as needed. Each time you expand to a new area, watch to be sure that new device types are addressed to prevent an avalanche of support calls.

NAC-NAP Policy Strategies

Cisco NAC and Microsoft NAP integration is a security solution for enforcing network access using a collaborative security policy for user identity, host identity, and host health state compliance. It is important to first understand and create a comprehensive security policy to define the goal of your network admission control effort.

Designing a Network Admission Policy

The basis of all AAA security technologies is assessment and control of who can access what, and when, and from where, and how. Traditionally, the “who” was simply a user or host identity in the form of as a username and password, digital certificate, one-time token password, or even biometrics. With NAC-NAP integration, AAA authentication can extend beyond user and host identity to include a complete compliance validation of the host’s posture: its hardware and software configuration. With the aid of security policy configuration on the Microsoft NPS, the network can verify the following items before permitting network access:

- State of personal firewall
- State of virus protection and its version
- State of spyware application and its version
- State of automatic updating
- State of security updating and its history

This evolution was necessary because viruses and worms can quickly and easily exploit vulnerabilities, on a large scale, present in unpatched operating systems and applications. This threat can be as much or more of a threat to an organization’s security and survival than a malicious user or hacker. Maintaining a computer system with the latest OS patches and security software updates is critical.

Policy Creation Requirements

The goal of deploying NAC-NAP integration is to prevent the problems associated with unauthorized and noncompliant network hosts. This authorization decision encompasses more than just identity and may involve compliance of the host OS and multiple client-side agents and applications. In larger organizations, the management and operations of identity servers, desktop software, server software, application administration, network security, and support are handled by separate teams of subject-matter experts. Bringing all these teams together to create and maintain a comprehensive and collaborative security policy can be time consuming and difficult.

A NAC-NAP security policy must be collaboratively built and maintained by representatives from your network (LAN and wireless) and information technology (desktop, server, applications, and support) teams. Decisions that must be made include:

- Who is responsible for policy creation and policy enforcement?
- What are the current requirements for network admission across the company? Are they the same across all access methods (wired, wireless, etc.)?
- What is your policy on unmanaged or nonstandard machines on your network (labs, guests, consultants, extranets, kiosks, etc.)?
- What are your current security policies for authentication and application compliance? Is this sufficient or do you want to increase the scope of validation?
- How do you perform network segmentation now? With VLANs?
- How often will the policy representatives meet to discuss ongoing policy updates and changes?

- What is the quorum for making changes, however small?
- Do you have management support for the business case of enforcing your security policy? Users do not like being managed, and you may face backlash.

After your organization has basic agreement on the kind of policy desired and how it will be created, you can begin to formally define it.

Policy Definition

Network admission policies are structured around several basic elements of the authorization decision. The list here explains each one and gives examples of instances and options.

Who: The identity and group of the network access requestor

- User identity: Differentiated access based on user and group or guest privilege
- Host identity: Differentiated access for corporate asset in contrast to unmanaged hosts
- Host health state: Hardware and software inventory and security software state

Where: Location with differentiated policy

- Geographic: City, country, or other region with specific policy rules or laws
- Logical: Logical location with unique security requirements such as a lobby, lab, or high security area

When: Contextual access restrictions and logged events for accounting and auditing

- Temporal: Time-of-day, day-of-week, and other time limitations
- Quotas: Session limits based on account balance, time, or active instances
- Logs: Auditing of resource use and security forensics

How: Network access method, its protocols, and policy requirements, if any

- LAN: Access through enabled IEEE 802.1x or Layer 2 switch port
- Wireless: Wireless access within and around buildings

What: Network authorization privileges and features based on the capability of the access method

- Open: No access requirements or restrictions
- Groups: Logical segmentation of the network based on groups or roles
- Extranet: Partner connectivity for outsourcing or sharing resources
- Assets: Printing services and other dedicated devices
- Guest: Internet-only guest access

Identity Credentials

Identity is the unique name of a person or device, or the combination of both, that is recognized by an authentication system. The identity credentials are objects, such as passwords or certificates, used in the authentication transaction. In the context of IEEE 802.1x, these credentials determine whether the authentication system recognizes the IEEE 802.1x supplicant on the switch and determines whether it has the correct credentials to gain access to the network and what the appropriate authorization is for the supplicant. As has been stated, the IEEE 802.1x method allows identity and posture credentials to be passed in one EAP conversation to make an admission decision on both types of credentials. A network administrator needs to understand that when using both methods, access is permitted within the Cisco Secure ACS only when identity credentials successfully authenticate the supplicant. If identity authentication fails, no posture credentials are checked, and the supplicant is denied access to the network.

To better understand this function, it is important to realize that there are generally two types of identity credentials that can be sent from the supplicant to the NAC system. This behavior has design implications for the device configuration depending on the type of credentials that are being checked.

Generic Device Credentials

The first credential is called a device credential. With this authentication mechanism, the machine is authenticated in advance of the user of the computer. This type of credential is used if the device needs to gain access to the network to perform some function before user authentication, or if the device is not normally used by end users: for instance, servers or printers. The host can store device credentials (such as passwords) that the supplicant can access at device startup to authenticate itself to the NAC-NAP system.

Best Practice:

In deployments with IEEE 802.1x, use machine authentication with Active Directory to help enforce host restrictions before a user has logged on and after a user has logged off.

Microsoft Machine Credentials

Microsoft calls its device credential login mechanism machine authentication. Microsoft introduced the machine authentication facility to allow the client system to authenticate using the identity and credentials of the computer (Active Directory computer account ID or machine certificate) at boot time so that the client can establish the required highly secure channel to the domain to update and participate in the domain group policy object (GPO) model. Machine authentication allows the computer to authenticate itself to the network using IEEE 802.1x just after a PC loads device drivers at boot time.

User Credentials

At boot time, the Windows operating system uses machine authentication to authenticate using IEEE 802.1x and to subsequently communicate with Windows domain controllers to download machine group policies to alleviate the problem of domain GPOs being broken by the introduction of IEEE 802.1x.

After the user presses Ctrl+Alt+Delete, the logon dialog box is displayed on the screen to prompt the user for credentials. When this prompt is presented, a user can log in to the computer or the Windows domain, and the username and password used for login can be used as the identity credentials for IEEE 802.1x authentication. This second type of credential is commonly referred to as user authentication. Note that user credentials can also be provided with a user certificate.

Network Segmentation and Isolation

After the AAA server makes an authorization decision, it pushes the respective configuration policy to the NAD for enforcement on the host and user. The most common enforcement mechanisms are RADIUS session timers and VLAN assignments. These mechanisms allow network administrators to enforce their security policies using network segmentation to permit access only to authorized network resources. The enforcement features of the NAD depend entirely on the network access method and the NAD's hardware capabilities.

Segmentation

Before implementing NAC, you need to identify the network resources to which you are trying to permit or deny access and the mechanisms that are possible given the capability of your NADs and your network architecture. Using IEEE 802.1x on LAN switches and wireless access points to dynamically assign hosts to VLANs is a common method of network segmentation. This method helps ensure that hosts can talk only to other resources within the same VLAN and are subject to VLAN ACLs.

Isolation

Segmenting the network according to an identity and posture policy is a fundamental part of a NAC-NAP integration deployment. Just as critical is where in the network you choose to have NAC-NAP integration enforce these polices and effectively isolate any unauthorized hosts. To achieve isolation, NAC-NAP integration should be enabled at the very edge of your network to prevent a virus-infected host from touching any network hosts other than those used for antivirus and remediation. Using NAC-NAP in the distribution or core of the network may seem like a good way to reduce the number of NAC chokepoints that you need to manage, but this approach does little to contain a virulent host.

Multihost and Multidomain Authentication

IEEE 802.1x was created with the assumption that there should be only one host (MAC address) per port, making dynamic VLAN assignment straightforward. The use of hubs, IP phones with chained PCs, and hosts with VMware all stray from this model. Each of these scenarios can easily allow two or more MAC addresses on the same port. By default, when a IEEE 802.1x–enabled port encounters a second MAC address, it administratively shuts down the port for security, so if these scenarios are more the rule than the exception on your network, you should enable the switch features that allow multiple MAC addresses on a single switch port. Mutlihost mode allows multiple devices on a single switch port, and multidomain authentication (MDA) is specifically for IP phones with attached hosts and offers the capability to authenticate both IP phones and the endpoint behind the phones.

Agentless Host Options

One of the biggest hurdles faced by all NAC deployments is not how to authorize identity and posture credentials, but what to do in the absence of them. All the NAC policies that have been discussed so far assume that all network hosts can respond to challenges from the network for identity and posture credentials. However, a large number of network-attached devices do not, cannot, and never will support the various protocols required for network authorization. This class of devices includes everything from network printers and photocopiers to devices with embedded or hardened OSs to PCs with personal firewalls enabled. These devices, called NAC agentless hosts, can be handled in several ways and at different levels of the authentication process, as summarized in Table 3.

Table 3. Agentless Host Options

Agentless Method	Credentials	Pros	Cons
Guest VLAN	None	Easy default for guest access	• No authentication • No central log of access
MAC Authentication Bypass	MAC address	• Centralized address management • Wildcards supported • Lightweight Directory Access Protocol (LDAP)	• Weak identity authentication • Static list of addresses to maintain

Agentless Method	Credentials	Pros	Cons
		support available	
Web Authentication	Username and password	User authentication is stronger than MAC authentication	Requires user interaction

Guest VLAN

The guest VLAN is a Cisco switch feature to allow hosts without a supplicant to gain guest access through IEEE 802.1x–enabled ports. When the user first connects to a device, the switch will attempt an IEEE 802.1x conversation. Without a supplicant, the IEEE 802.1x frames are ignored, and the authentication process times out. Rather than default to no VLAN and no connectivity, the guest VLAN assumes a default level of network access for potential guests by assigning the port to an administrator-configured VLAN. This feature is configured per port for deployment granularity.

Best Practice:

MAC authentication bypass (MAB) with a default group assignment is recommended over the guest VLAN feature. The guest VLAN does not rely on RADIUS and therefore does not offer the visibility and centralized control provided by AAA services such as MAB.

MAC Authentication Bypass

Note: Be aware that MAC authentication is a relatively weak form of identity authentication and may be easily spoofed. It does not offer perfect security, but it is a first step toward segregation of known devices and unwanted rogue devices.

The most common method for handling agentless hosts on switches with IEEE 802.1x configured is the MAC authentication bypass (MAB) feature. MAB is also triggered after an IEEE 802.1x timeout. The switch sends a RADIUS request that includes the host's MAC address to the Cisco Secure ACS. The Cisco Secure ACS can then look up the MAC address and match the corresponding group assignment. MAB thus effectively provides a trusted device list for agentless hosts in your network. The benefit of this approach is that RADIUS provides a centralized notification method for all agentless hosts in your network. The downside is that you must create and maintain a list of all MAC addresses for all agentless hosts in your network. Use of wildcards in MAC addresses is allowed so you do not need to create individual entries for each and every device from a particular vendor.

Note: The guest VLAN and MAB features are triggered by the same condition, but the guest VLAN feature takes precedence since it is a static option locally defined on the NAD. Keep this in mind when choosing which method is best for your environment.

In addition to offering the MAB capability within the local Cisco Secure ACS database, Cisco Secure ACS 4.1 and later can run MAB against an external LDAP server. LDAP may enable easier integration with your existing network tools when you need to register and update new agentless devices on your network.

Best Practice:

MAB is highly recommended over other locally defined agentless handling mechanisms such as static exceptions and guest VLAN. These methods lack the centralized visibility and control provided by MAB requests and databases.

Web Authentication

Another option for authenticating users without IEEE 802.1x supplicants is web authentication. A web authentication portal is essentially the same kind of browser-based authentication portal that you see in airports and hotels except that it is specific to your list of enterprise users. Although web authentication is an excellent option for guest access scenarios, it does not always work well in the LAN because of the number of userless devices. You cannot expect a printer or copier to submit its username and password in a web browser.

Preboot Execution Environment

The preboot execution environment (PXE), pronounced “pick-see,” is a means for remotely booting or reimaging devices over the network. PXE is a BIOS feature in many computers that, when enabled, will broadcast a boot request to the network successively for 4, 8, 16, and 32 seconds—for a total of 60 seconds—hoping for an IP address for the PXE server so it can download its operating system. If IEEE 802.1x is enabled, there is no network connectivity unless authentication is successful, or unless IEEE 802.1x times out and there is a default VLAN or guest VLAN assignment. Because of the default IEEE 802.1x timers, PXE usually times out before IEEE 802.1x. The current recommendation for accommodating PXE is to lower the NAD’s IEEE 802.1x timers to ensure that it expires before PXE:

```
dot1x timeout tx-period 15
dot1x max-req 3
```

NAC Scalability and Availability

Nearly every network has some form of AAA, but is usually only for VPN or wireless access. NAC changes this, requiring authorization upon network ingress for every host and subjecting the hosts to ongoing posture revalidation. The increased use of the AAA infrastructure has two implications: the AAA servers and their delegates must be scaled for the increased demand and made highly available as a critical network service. Failure to increase both the scalability and availability of the AAA infrastructure could prevent legitimate users and healthy hosts from being productive.

The Cisco NAC and Microsoft NAP solution architecture was designed for central management of an extensible security policy to enforce network access across a very large and heterogeneous network edge. Nevertheless, an understanding of the primary performance factors and anticipated bottlenecks within the architecture is critical for success, to help you determine which components are the most crucial, calculate how many of these components you need, and identify where to focus your performance tuning efforts.

Best Practice:

Build redundancy into the entire NAC-NAP infrastructure (Cisco Secure ACS, Microsoft NPS, etc.) so that a fail open configuration is not required. In the case of failure, verify the desired fail open or closed behavior using the Cisco IOS Software inaccessible authentication bypass (IAB) feature.

The scalability of a NAC deployment is measured by the number of authorizations completed within a time period, typically rated in transactions per second (TPS).

Users and Hosts

The size of your network, measured in users and hosts, is the first factor in determining the scale of your NAC infrastructure. This measurement provides an initial count of the minimum number of authorizations per day that you can expect on your AAA servers. If your organization’s security policy requires authentication of only user identity or only host posture, then you do not need to count both.

User behavior throughout the day must also be considered. In a single day, individual users may connect from home through VPN, come into the office and connect to the LAN, go to meetings and roam wirelessly, go back to their desks, restart their computers after installing updates, and check email through VPN at home again at the end of the day. Each of these events and more may trigger an additional authorization depending on the security policy and protocols used.

Individual users rebooting or roaming throughout the day should average to a normal load on the AAA services. The real problems are usage spikes, when hundreds or thousands of users request access in a relatively short period of time. A spike could result from a regular event such as everyone turning on their desktop computers at the start of the day, or from an unexpected one such as power outage, after which everything comes back online at the same time. Try to account for these events if they can be anticipated.

Another area of scalability affected by your number of users and hosts is the size of your server and storage systems. Along with the larger volume of transactions resulting from authentication, more RAM and disk storage will be needed on your backend servers. With so many new authentication events and regulations concerning privacy and auditing trails, long-term storage needs could grow quickly.

Cisco Secure Access Control Server 4.2

All requests for network admission must be authorized by the Cisco ACS, the only AAA server that currently supports all the NAC protocols and methods and the central policy engine for coordinating all NAC authorization decisions. For this reason, the Cisco Secure ACS is the single most important component in the architecture to consider when scaling a NAC deployment. Several factors greatly affect the capability of the Cisco Secure ACS to scale.

Best Practice:

Troubleshooting authorizations across multiple Cisco Secure ACSs is time consuming so all AAA records should be centralized in a single Cisco Secure ACS database or on a single syslog server.

Protocol Authorization Rates

You can choose among many different network authentication protocols. Each offers different levels of security and features that correspond directly to rates of authentication, and some are very simple and insecure request-and-response protocols, while others require many roundtrips between the host and AAA server to negotiate an encrypted tunnel and deliver the required credentials. Using the authorization rate of your authentication protocols and your TPS count, you can calculate the minimum number of Cisco Secure ACSs required for your deployment.

Reauthentication and Revalidation Timers

Timers used in NAC-NAP affect the scale of the network. Each timer has a global default value in the Cisco IOS Software of each NAD. These global Cisco IOS Software values can be overridden first by a Cisco IOS Software configuration command and second on a per-session basis from the Cisco Secure ACS. The use of conservative numbers—long intervals—is recommended at first, with the values lowered as authorization performance allows.

Session Timeouts and Revalidations

A session timeout (RADIUS attribute 27) triggers a complete revalidation of the user and host credentials in NAC. This is the most critical timer affecting AAA scalability because it controls the revalidation period for every host in the network.

Other Scaling Limitations

There are other limitations in Cisco Secure ACS configuration that do not hurt actual performance but do limit its capability to scale in some deployment scenarios.

Cisco Secure ACS has a maximum of 50,000 addressable entries for network access devices. Rather than using individual IP addresses for each NAD, you should consider using ranges of IP ranges. Use of a single wildcard entry (*.*.*.*) is recommended as a best practice to avoid having to continually update the list of NADs in the Cisco Secure ACS GUI.

MAB authentications are used in NAC agentless hosts scenarios to match MAC addresses within a whitelist. Cisco Secure ACS has a limit of 10,000 MAC addresses per network access profile.

Cisco Secure ACS can delegate host posture decisions to audit servers based on MAC address matches. Cisco Secure ACS supports up to 1024 MAC addresses per audit server configuration.

Scaling Calculations

The following recommendations provide guidelines for scaling Cisco Secure ACS for a Cisco NAC deployment. The number of Cisco Secure ACSs required to support a specific size of user database depends on many factors. Assume a minimum of one transaction per day per user on average. Increase the average transaction count based on some of these anticipated timers and behaviors:

- RADIUS session timeout value
- VPN remote access logins
- Multihomed access on wired and wireless network interfaces
- Wireless roaming
- Restarts due to patches and general operating system and application glitches
- Multiple devices per user (desktops, laptops, PDAs, etc.)
- Frequency with which the host posture changes

With this initial count, you can now approximate the number of transactions per day:

```
Transactions_per_Day = Transactions_per_User_per_Day x Number_of_Users
```

Convert this value to TPS by dividing by the number of seconds in a day:

```
Transactions_per_Second = Transactions_per_Day/(24 x 60 x 60)
```

From this average transaction rate and the Cisco Secure ACS authentication protocol performance numbers, you can estimate the minimum number of Cisco Secure ACSs required:

```
ACS_Count = Transactions_per_Second/ACS_Protocol_Authorization_Rate
```

This number is an absolute minimum since it is an average for all times of the day, assumes a continual 100 percent load, and does not account for server downtime due to policy replication, maintenance, and an occasional link failure. Divide the final Cisco Secure ACS count by 0.4 to account for some of the unknowns until actual rates and loads can be verified. Weighting the protocol authorization rates with your mix of network access methods may help you refine the final Cisco Secure ACS count.

Load Balancing

To improve the performance of Cisco Secure ACS in a NAC-enabled environment, the Cisco Secure ACSs can be configured for both load balancing and failover. Load balancing and failover can be configured in several ways:

- Cisco IOS Software RADIUS server failover
- Cisco IOS Software server load balancing (SLB)
- Load balancing and failover through the use of a Cisco CSS Content Services Switch or a Cisco Content Switching Module

Cisco IOS Software RADIUS Server Default Failover

Authentication server failover has been possible in Cisco IOS Software since Release 12.1. The concept requires that multiple RADIUS authentication servers be configured in the NAD. If three RADIUS servers are configured and RADIUS server 1 fails, then the NAD automatically, after a preconfigured number of retries and timeout periods, contacts RADIUS server 2 to authenticate the two clients. Similarly, if RADIUS server 2 fails, then the NAD attempts to authenticate clients using RADIUS server 3.

Several command options are available that provide better control over the performance of the NAD while attempting authentication:

- Timeout: Number of seconds a NAD waits for a reply to a RADIUS request before retransmitting the request; the default value is 5 seconds
- Retransmit: Number of times a RADIUS request is resent to a server; the default value is 3 times
- Deadtime: Number of minutes that a RADIUS server not responding to authentication requests is passed over by requests for RADIUS authentication; the default value is 10 minutes

Configuring appropriate values for these three settings can help improve the authentication performance of the NAD. To reduce the time required to fail over from one Cisco Secure ACS to another, values should be chosen that are short enough to initiate failover but not so short that they cause the NAD to unnecessarily timeout and mark a server as nonresponsive. Testing has shown that the default values provide good performance for NAC during Cisco Secure ACS failover. If necessary, reduce the retransmit tries from 3 to 2, the timeout from 5 seconds to 3 seconds, and the deadtime to 2 minutes. These settings provide 6 seconds before the NAD decides that the AAA server is not responding and moves on to the next server. These settings also provide 2 minutes for the nonresponsive server to recover or restart.

The **aaa group server** command provides a way to group existing server hosts, enabling you to select a subset of the configured server hosts and use them for a particular service. More information about configuring multiple RADIUS servers in Cisco IOS Software can be found at http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/prod_configuration_guide09186a008017d583.html.

Cisco IOS Software RADIUS Server Load Balancing

RADIUS SLB is available on the Cisco 7200 Series Routers and the Cisco Catalyst 6500 Series Switches and can be achieved through Cisco IOS Software. To optimize the performance of the AAA server group for NAC authentication, the load-balancing algorithm should be set to Weighted Least Connections (from the default Weighted Round Robin). When a client first accesses one of the virtual servers, that client's IP address is added to the Cisco IOS Software SLB database for a specific group. The client's IP address is then associated with the physical server chosen for the first RADIUS access request. Subsequent requests from that client for either virtual server always go to the same physical server. This configuration causes the sticky database to store its entries for 86,400 seconds of inactivity.

RADIUS Server Load Balancing Using Cisco CSS Content Services Switch

A network load-balancing device such as the Cisco CSS Content Services Switch or Cisco Content Switching Module (CSM) can also be employed in a similar fashion to balance authentication requests from the NADs to the Cisco Secure ACSs. In this configuration, the NADs point to one or more IP addresses representing the pool of servers balanced behind the Cisco CSS or CSM.

Note: Although you can configure failover between sites, the best deployment includes local failover systems on the same LAN. This configuration provides fast, reliable authentication for the local network. Load balancing can be accomplished in the same manner.

Load Balancing

Load balancing across a centralized pool of servers is the best strategy for simultaneously increasing the scalability and availability of a network service. The one exception is when you have a highly distributed network with several large offices or many remote offices. In this case, use smaller pools of servers spread across each of the larger, regional offices. This approach helps ensure that if connectivity to the headquarters or a large regional office fails, the other regional offices can act as secondary servers until service is restored.

Inaccessible Authentication Bypass or Critical Authentication

Even with load balancing across multiple regional offices, highly distributed topologies or countries with poor WAN connections may still experience WAN outages. Such outages are often a concern for banks and retail stores with hundreds or thousands of remote sites. When an outage occurs, users are effectively locked out of the network, because an unreachable AAA server means that authorizations cannot be completed successfully.

For this reason, Cisco has developed the Cisco IOS Software IAB feature, also known as critical authentication or fail open or closed. This configuration option gives the administrator a port-specific option to have the switch port fail open or fail closed, whichever security policy requires, in the event of an outage. After connectivity to the AAA service is restored, all IAB sessions are authenticated normally.

Failed-Authentication VLAN

Another port-based configuration option for switches is the failed-authentication VLAN. If the user repeatedly fails to authenticate, the switch places that user in a default, failure VLAN. The failed-authentication VLAN is configurable but is often set to the same VLAN that is used for guest access to allow basic connectivity. This scenario most frequently occurs when contractors and guests who connect to your network have an IEEE 802.1x supplicant but their trusted root certificate configuration or identity credentials do not work for your network. Rather than fail authentication and leave them without any VLAN assignment and therefore no connectivity, the failed-authentication VLAN still allows them basic guest access.

Conclusion

Cisco and Microsoft have collaborated to enable rich interoperability between the Cisco Network Admission Control (NAC) and Microsoft Network Access Protection (NAP) solutions. This interoperability enables customers to gain the benefits of both NAC and NAP while using and preserving their investments in their Cisco NAC network and Microsoft NAP desktop and server infrastructure. NAC-NAP integration dramatically improves security by helping ensure that endpoints (laptops, PCs, PDAs, servers, etc.) conform to security policy to proactively protect against worms, viruses, spyware, and malware.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C07-491729-01 05/09