This chapter covers the following topics:

- Policing your information highway
- Begin by laying the framework
- Value is in the NAC partners
- Examples of admission control uses

CHAPTER 8

NAC Now and Future Proof for Tomorrow

Initial Network Admission Control (NAC) Framework implementations typically involve a solution that consists of partner NAC-enabled software that works with Cisco network infrastructure to limit security threats, such as worms and viruses, by focusing on validating host credentials and enforcing compliance. One of the many features NAC Framework provides is the capability to add the identity of both the user and host computer into the NAC enforcement decision mix.

This chapter describes additional capabilities that businesses can include with their future admission policies, requiring the network infrastructure to do the following:

- Use learned information about a host computer or user, or about where the computer or user resides on the network to determine rights and privileges that dictate resource authorization or access to certain data applications
- Detect company assets and enforce asset management policies by user or role
- Enforce regulatory compliance to protect client privacy and reduce the opportunity for leakage of business-sensitive data
- Automatically remediate noncompliant hosts and self-heal infected hosts

Policing Your Information Highway

Use NAC to police your information highway. NAC is analogous to a policeman who protects and enforces a variety of rules that users must abide by to have the privilege of traversing your information highway.

The traffic policeman's role and tools have evolved over time. During initial automobile use, policemen had fewer enforcement requirements and fewer tools to aid in their determination of compliance to the road rules. With increased automobile adoption, more rules and requirements were created to validate a minimum skill set for drivers as well as a minimum requirement for the automobile using the roads. Similarly, minimum compliance enforcement and identity verification are what many businesses will initially implement in their NAC deployments.

Compare the evolution of the modern traffic policeman's role and tools to NAC's protection and enforcement characteristics (noted in parentheses):

- The registration of the vehicle (host identity) by way of a vehicle identification number, or VIN (host serial number), the automobile license plate linked to the VIN (MAC address), an annual registration sticker to identify the tax paid for the privilege of driving the vehicle (accounting for billing to track who did what, where, and for how long).
- Vehicle inspection tag (host posture) that expires annually (host posture revalidation timer) to verify that the vehicle meets minimum standards to drive on the roads.
- Driver's license (user identity) that identifies that the driver has passed minimum driving skills. Sometimes a vehicle class (role or class of service) is assigned to indicate what type of vehicle a person can drive and to identify extra privileges. Physical characteristics are provided that identify the driver (user login) along with the expiration of the license (user identity revalidation timer).
- Police monitor the highway to ensure that drivers abide by road rules and do not exceed the maximum speed (posture compliance policy). Location can dictate a different set of rules (remote access versus LAN policy).
- When a violation occurs, the policeman assesses many criteria (credentials and policy). Besides the initial violation, he usually checks other database(s), such as outstanding arrest warrants, to determine compliance to other policies (external policy servers) before determining his action. For a minor violation, the driver might be warned but allowed to resume her journey without receiving a ticket (user notification stating out of compliance but network access allowed for now). Or, the policeman could determine that a more egregious violation, such as driving under the influence, or worse, such as a serious auto accident, occurred. The policeman can issue a ticket or tickets for the violation (application posture token for each posture credential).
- A driver might be required to appear in court (URL redirect) before a judge (policy server). The judge reviews the violations (application posture tokens) and sentences the driver based on the most severe violation (system posture token). In a simple case, the judge can issue a warning, fine, community service, or a temporary jail term (remediation in an attempt to make compliant). In severe cases, the judge can seize the driver's license, revoking her privilege to drive (no network access).
- The policeman (network access device [NAD]) enforces the judgment on the driver. The driver now has a record in a violation database; other police officers have access to the driver's history of violations (behavior trend).

Use NAC today to start policing your information highway. Start with a simple implementation, such as enforcing PC software compliance and validating user authentication. Over time, extend NAC's capability by adding more identity functionality to provide secure access to the ever-growing set of applications and system resources.

Begin by Laying the Framework

Businesses have two key areas of interest for their self-defending network: protecting their assets and thwarting misbehavior.

Asset Protection

Most businesses already have a software patch management process in place. Integrating software patch management processes with NAC can significantly improve the effectiveness of those processes. Before NAC, software compliance was not easily enforceable because host posturing did not exist. Users could stop updates from occurring or decide to update when they had time, which allows malware to spread even when software updates were made available to prevent such an outbreak. Being able to enforce software patch compliance is one of the initial major drivers for implementing NAC.

Cisco offers two network admission control choices: NAC Framework and NAC Appliance. Traditionally, businesses adopt one of the two models.

Many businesses initially adopt the NAC Appliance method, which provides a simpler approach to detection and enforcement of host software. NAC Appliance is an all-in-one solution that allows a rapid deployment model using a self-contained endpoint assessment, policy management, and remediation services. It provides similar operating system compliance checks and policy enforcement but can operate in a multivendor network infrastructure. It does not use an integrated approach with NAC partners that provide additional host posturing and enforcement functionality like NAC Framework. Also, at the time of this writing, identity enforcement is not available with NAC Appliance.

Others might want to add more admission checks, such as identity and corporate asset enforcement, migrating to an integrated environment as their deployments and requirements mature.

NAC Framework uses an integrated approach, leveraging infrastructure that is used as the policy enforcement point. NAC Framework also leverages existing security solutions from other vendors, such as antivirus, remediation, patching, and auditing services. The NAC Framework model allows a more flexible admission policy that is typically more complex than NAC Appliance deployments.

With NAC Framework, in addition to software compliance, you can add Identity-Based Networking Services (IBNS) to your admission policy decision when using NAC-L2-802.1X. Combining user and host authentication as part of the network admission decision is the strongest authorization model. With today's mobile workforces, you need to control who can gain access to different parts of the network. Your policy might need to differ based on a wired or wireless device. With identity as part of the admission policy, you can provide predetermined IP addresses only to valid users and devices that successfully authenticate and have been verified as being compliant.

Many NAC partners provide IBNS capabilities that can plug into the NAC Framework today. For example, some IBNS solutions assign rights to resources based on the identity of a user, specifying the user's network access, shared resource access to servers and printers, access for file read and/or write, and ability to use specific software applications.

You might need an admission policy that can assign the appropriate rights based on when a device is used, where a device or user is physically located, or a combination of when, where, and who. Examples include the following:

- Internal wired policy versus wireless policy.
- Geography-based policy to preserve confidentiality of data by enforcing whether it can be accessed and/or retrieved based on host location. Different policies might be needed for:
  - VPN access from a public area, such as the airport, hotel, or coffee shop.
  - VPN access from a more private place, such as a remote or home office.
  - Region-based access to limit remote users from accessing locally significant information, such as files not allowed for export.
  - Time-of-day and day-of-week policy to limit access to sensitive areas outside normal business hours.

You can determine how you plan to enforce compliance on devices that you don't manage or control. You can determine whether you are going to include the ability to exempt devices that cannot interwork with NAC so that they can use the network. Different methods exist to accomplish registering and exempting devices that can't communicate their credentials. You can use a dynamic auditing strategy to scan unmanaged devices, or you can statically maintain an exception table.

Use NAC Framework if your initial NAC deployment requires the following:

- Deep vendor integration for assessment and/or remediation
- 802.1X for initial NAC deployment
- Too many NAC appliance servers and overlay devices to satisfy admission control solution for a large enterprise

If a rapid deployment model is required or a simpler management method is desired, use the NAC Appliance. It uses the Cisco Clean Access product to provide out-of-the-box functionality with preinstalled support for antivirus and Microsoft updates.

NAC Appliance uses a turnkey approach versus the more complex feature-rich NAC Framework model. While many see the value of NAC Framework, some don't need all the other capabilities today and prefer a more simplistic approach.

Cisco plans to move forward with additional features in both models as well as to build a tighter integration between NAC Framework and NAC Appliance. Both architectures will be able to coexist and be centrally managed by a common management interface.

Detecting Misbehavior and Dealing with It

Other components of the self-defending network can be optionally implemented to detect and defend against malicious behavior. Misbehavior can exist in many forms. It can be intentional or nonintentional actions from users, failing or compromised devices, or external misbehavior from hackers. Examples include the following:

- **Using an intrusion protection system (IPS), such as a network-based IPS (NIPS) or host-based IPS (HIPS), to defend in depth against misbehavior on the network and individual hosts**—An example of a HIPS is Cisco Security Agent (CSA) running on hosts that function as PCs and servers. CSA can recognize application behavior that can lead to an attack and can prevent its malicious activity. You can create custom profiles for the different roles of servers and users, providing various levels of protection based on device use. For example, servers used as shared resources might require a fixed and hardened security policy, such as not allowing software applications to be installed, preventing system configuration files from being altered, and not opening TCP ports other than the ones needed for the server's applications. In contrast, hosts operated by some users might need to add software to perform their jobs, while other users are not allowed to add software. Any behavior attempted beyond the profile's acceptable policy is not allowed. Use NAC to enforce the use of the HIPS application by making sure that it is enabled and up to date before allowing the host to access the network. For example, with the integration of NAC and CSA, dynamic policy decisions can be made based on information provided from CSA.
- **Using Cisco Secure Monitoring, Analysis, and Response System (CS-MARS) to analyze, monitor, and detect all types of events on your network and present them in a single networkwide topology view**—CS-MARS can detect anomalies that could be caused by a host generating huge amounts of traffic because of a worm infection. CS-MARS can work with the policy server to automatically shut down the affected section of the network to reduce exposure to others, shun an offending device, or force device remediation. Beginning with version 4.1, CS-MARS can correlate and report on IOS-based 802.1X authentication events from IOS, CatOS, and Access Control Server (ACS) devices. As a result, CS-MARS can act as the centralized NAC reporting engine for security operators to monitor authentication and device posturing policies. CS-MARS has many predefined NAC reports that can be easily interpreted by a help desk operator, providing a quick summary in a graphical view. For example, compliance reports can identify healthy or unhealthy devices. If more information is needed, the operator can query for details about the host or user to diagnose the problem.
- **Using Cisco IOS NetFlow, which is available in routers, to provide visibility across the entire network, capturing traffic data to aid in understanding typical traffic trends**—Changes in network behavior can indicate denial of service (DoS) attacks or anomalies such as viruses and worms. NetFlow works by tracking packet

flows between a given source and destination, which helps identify the path an attack is taking through the network. The NetFlow data can be exported and used by other applications or network management technologies such as CS-MARS.

These additional self-defending network technologies work in harmony with NAC and extend its capability by proactively protecting and defending the network, hosts, and users against misbehavior.

Value Is in the NAC Partners

One of the big challenges is that businesses typically use different technologies, often supplied by many vendors, to provide different methods of protection, and they often work independently of each other. Wouldn't it be nice to use a common framework that allows the many vendor technologies to plug in and interoperate with the networking infrastructure that controls access to only compliant hosts and valid users?

As the adoption of IBNS matures, businesses will want to increase their admission policy requirements to include more identity enforcement besides user authentication. It will involve using more applications and technologies to monitor and enforce acceptable use of their resources as well as to enforce acceptable behavior.

The value that NAC Framework provides over all other network admission methods comes from the many vendors who are NAC partners. Cisco believes in working with standards bodies such as the Internet Engineering Task Force (IETF) to make NAC available and work with many vendors.

From its inception, NAC Framework has allowed third-party vendor integration. It supports a variety of partner products and technologies using standards-based, flexible application program interfaces (APIs) that allow third parties to contribute solutions to a NAC Framework environment. Besides the options available today, a variety of new applications can be created as part of the NAC posturing process. Posture plug-ins can be created to allow communication between the vendor's client application and the Cisco Trust Agent. The Cisco Trust Agent can be customized to pass credentials for any type of characteristic by way of the Host Credentials Authorization Protocol (HCAP) or the Generic Authorization Message Exchange (GAME) Protocol to policy servers that decide the compliance level of a device or user. The policy server can send actions that are enforced by the NADs or even the vendor's client application.

NAC Framework uses the following security protocols:

- Standardized protocols such as Extensible Authentication Protocol (EAP), Protected EAP (PEAP), 802.1X, and RADIUS services are used for communications between network components and a variety of hosts.

EAP–Flexible Authentication via Secure Tunneling (EAP-FAST) is a Cisco-authored protocol that allows multiple credential types, such as user identity and posture credentials, to be chained together in a single authentication packet. This allows NAC-L2-802.1X to perform both user and machine identity authentication as well as posture validation.

- At the time of this writing, the following NAC protocols are Cisco proprietary. Some of these protocols are going through the formal process of becoming standardized and could be standard by the time you read this:
  - EAP–type-length value (EAP-TLV) is an EAP extension that carries posture credentials and posture notifications between the host computer's posture plug-in agent and the Cisco policy server.
  - GAME is a proprietary protocol used by partner audit servers to scan a host that has no Cisco Trust Agent installed to determine software compliance. An audit server uses GAME to communicate compliance directly to a Cisco Secure ACS, which in turn enforces the appropriate security policy on the host.
  - HCAP is available for NAC partners to allow their external policy servers to interoperate with the Cisco Secure ACS and to be part of the admission policy decision.

Cisco also provides an API for Cisco Trust Agent, HCAP, and GAME that is available to licensed vendors. NAC partner vendors can write custom applications using the API to evaluate almost anything for admission.

NAC is simply the conduit that allows your infrastructure to police your information highway with the requirements of your choice.

Examples of Admission Control Uses

Businesses might use the following examples as part of future security policies for NAC to enforce. Some of these capabilities exist today in partner vendor products, while others require some development. All are possible with the use of custom applications that can plug into the NAC framework:

- Track and manage company assets
- Enforce the use of corporate-approved software
- Enforce operating system access control
- Enforce physical identification for higher security clearance
- Enforce a business policy or rule
- Enforce regulatory compliance
- Enact roles-based provisioning

- Enforce data restriction when external media is detected
- Use customized shared resources

The following sections cover these uses.

Tracking and Managing Company Assets

When a device is detected by the network, the serial number is checked with a policy server and a back-end database for validation. Only company-owned assets are allowed access to the network. If the host is assigned to a user, only the assigned user can successfully log in to the host computer. In addition, the database can be updated to provide a general location of where the host is logged in or was last logged in. The location can be determined by the NAD servicing it.

Enforcing Use of Corporate-Approved Software

Ensure that the host is running corporate-approved software (for example, corporate image). This could be determined by the host identity, such as the serial number, or by user identity. Use NAC to limit network access to users whose hosts are not running corporate-sanctioned software or image, regardless of application.

Enforcing Operating System Access Control

Protect operating system integrity by prohibiting access or changes to sensitive system files, system binaries, and registry settings. An example is to allow basic actions required by the operating system process but to prevent file manipulation by users or applications from the Windows system directory. Enforce the host firewall or require the use of Windows IPsec filtering to control the type of traffic, such as a shared server or PC, that reaches a host. A HIPS such as CSA can provide this type of hardening capability today. Use NAC to enforce an OS-hardening policy before the host is allowed access to the network.

Enforcing Physical Identification for Higher Security Clearance

For an extra layer of defense, add a physical authentication requirement to associate a specific host to a specific user when the user attempts to access extremely confidential information. The technology could use a portable USB smart token or even a biometric device to perform physical identification verification (PIV). The PIV device could scan and verify a user's fingerprint, palm, or even eye. An example of physical identification enforcement is where an admission policy requires a portable USB secure token to be present in the host that is attempting network access. The secure token requires a valid personal identification number (PIN) to be entered by the user for the host's security application to initiate the NAC validation process. After being successfully authenticated

with this physical identity credential, the user gets more privileges assigned with a higher security clearance from the policy server. This higher privilege remains active until the assigned time period expires or until the USB secure token is removed. NAC has configurable timers and/or uses EAP over LAN–Start (EAPoL-Start) with 802.1X to verify that the device is still compliant with the existing security policy. It can detect when a change occurs. Another option is to have the host application reinitiate the NAC process when it detects a change, such as removing the USB token, to lower the user's security clearance.

Enforcing a Business Policy or Rule

Your business might have rules for users that can be automated for a quick, consistent resolution. An example is a user that requires manager approval to access a certain server or file or to download company-provided software. The user who needs permission attempts access but is denied. However, the user can be automatically redirected to an application to submit the request. After the request is submitted, it is automatically routed electronically to the user's manager for approval and allows an expiration period to be assigned to this privilege. After approval is gained, the policy server raises the user's access privilege for a period of time and notifies the user by means of a pop-up or e-mail message that access to the server or file is now available.

Enforcing Regulatory Compliance

Some businesses must comply with industry or government regulations, such as the Gramm-Leach-Bliley Act (GLBA), the Sarbanes-Oxley (SOX) Act, and the Health Insurance Portability and Accountability Act (HIPAA). NAC can enforce features such as password control, identifying the user, and allowing only those users with the proper identity to access business- or client-sensitive information. You could enforce a user's PC to initiate the built-in screen saver after ten minutes of inactivity. You could even guarantee that a password setting is used to regain the display. Extra steps such as these can automatically ensure that the host is secure, even when the user steps away. Use NAC to enforce PC functions such as this by means of a custom API that detects the settings and sends credentials to a policy server that enforces compliance.

Enacting Roles-Based Provisioning

Policy based on job type or device type provides a consistent set of common rules or privileges organized by groups. Privileges can include network access rights, file read/write privileges, common use of software or web applications, work time, and day schedule. When changes are made to the role, it provides a quick and consistent policy change to a common group of users/hosts. Use NAC to enforce a policy to a user or host from a policy

server that controls access to a variety of resources. If role privileges are changed, the policy server can initiate a revalidation of those users who require enforcement of the new policy.

Enforcing Data Restriction When External Media Is Detected

Controlling read/write access to sensitive information with removable media can prevent loss of business-sensitive information or client financial or health data. An example is an application on a host that detects whether an external storage device, such as USB flash drive or external drive, is present. The host initially authenticated successfully when the device was not present. A host's application detects a change and initiates a NAC revalidation with the policy server. New credentials are sent. The admission policy for the device has changed and does not allow removable USB storage devices. It denies the user access to certain areas of the network, or it can prevent the downloading of certain types of files tagged as confidential, such as patient records. The offending host is not allowed to access the restricted area or perform downloads while the external device is present. When the external storage device has been removed from the host, the application detects this and a revalidation reoccurs. The policy server now grants full read/write access to the host and user. NAC works with other software applications to enforce policy and report user activity (for example, if a user attempts to save files tagged confidential to his host's hard drive without the external device plugged in and then transfers the files to the storage device later). The security software application such as CSA can be programmed by a user's profile to prevent the transfer of files to the hard drive and/or report this type of event.

Using Customized Shared Resources

Some businesses have a 24/7 multiple-shift operation in which employees share common resources, including desks, host computers, and telephones. Each work shift, an employee picks a free desk and successfully logs in to a host, which is associated with a phone and a desk. The user's identity is associated with a virtual machine that has personal settings and assigned applications with access to his personal files. The IP phone is configured for extension mobility, allowing the user to log in and activate his personal extension, feature buttons, and voice-mail settings to that phone. The desk has been checked out to the user and is logged as being unavailable for others to use. During the employee's work shift, his desk devices are personalized for his use. An auditing system keeps track of where the employees work, the hours worked, and the resources they use. This can serve to track usage for department billing and accounting for payroll use, and serve as a measurement for historical trends reporting. At the end of his shift, the user logs off the host and phone, which restores him to a defaulted guest access state, waiting for the next shift. Use NAC to associate an authorized user, host, and applications together, especially for users who do not have dedicated devices. Enforce software compliance and secure file access in this virtual environment.

These examples are just a sample of what can become part of your admission policy decision to help you police your information highway. Advanced identity and compliance capabilities can exist by including NAC-enabled vendor applications. Even if you don't need these advanced capabilities today, be assured that when you implement the Cisco NAC Framework, it sets the foundation to flexibly add a variety of future enforcement decisions to your network admission policy.

Summary

Use NAC to police your information highway by enforcing admission control rules for hosts and users that traverse your network.

Begin by laying the framework to use learned information about a host, user, or user's location on the network to control network access based on the user's compliance to the admission policy. *Use posture + identity = best access control*.

NAC can leverage existing network infrastructure, security software services, and security policies to provide enforcement points to disperse locations.

For those network-attached devices that are not NAC capable, use other methods, such as an audit server, which can scan hosts and determine software compliance and then communicate the result to the policy server to determine their admission rights.

Don't limit NAC to just enforcing software compliance; NAC can do much more. It is simply the conduit to allow your infrastructure to police your information highway with the requirements of your choice. Integrate other applications, available from Cisco NAC partners, as part of the compliance checking and enforcement process. In addition, create applications using the API to detect and enforce any type of identity characteristic that is important for your business.

No two NAC Framework implementations will be alike. NAC Framework provides the most flexible and feature-rich network admission control solution, adaptable to your needs for today and in the future.