Cisco Network Admission Control and Microsoft Network Access Protection Interoperability Architecture

Cisco Systems and Microsoft Corporation
Published: September 2006

Abstract

Cisco Systems®, Inc. and Microsoft® Corporation have developed an interoperability architecture that allows customers to deploy both the Network Admission Control (NAC) platform available from Cisco® and the Network Access Protection (NAP) platform being developed for Microsoft Windows Vista™ (now in beta testing) and Windows Server® code name "Longhorn" (now in beta testing). The result is a set of components that interoperate, allowing customers to enforce health requirements for network access using a combination of components from Cisco and Microsoft. This white paper describes the set of characteristics that will support the interoperability architecture and how the interoperability architecture works.

Contents

Interoperability Features and Benefits

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 will allow customers to realize the benefits of both NAC and NAP while using and preserving their investments in their NAC network and Microsoft NAP desktop and server infrastructure. Interoperability will be supported with the release of NAP in the future version of Windows Server, codenamed Longhorn, which is scheduled to be available in the second half of 2007. Primary features and benefits of the solution include:

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

Interoperability and Customer Choice

The interoperability architecture allows customers to deploy both NAC and NAP incrementally or concurrently. Deployment of heterogeneous NAC and NAP agent (the Cisco Trust Agent and the NAP Agent) environments is also supported. The client agent architecture will be transparent to the Cisco network devices enforcing network access.

Deploying both the Cisco Secure Access Control Server (ACS) and the Microsoft Network Policy Server (NPS) will be required for the initial interoperability release. However, Cisco and Microsoft have cross-licensed the NAC and NAP protocols, which provides the opportunity for both companies to respond to future market and customer requirements for a combined policy product.

Investment Protection

The interoperability architecture enables customer reuse and investment protection of their NAC and/or NAP deployments. For example, customers can begin deploying NAC today and integrate NAP into the environment concurrent with their deployment of Windows Vista and Windows Server "Longhorn."

Single Agent Included in Windows Vista

Computers running Windows Vista or Windows Server "Longhorn" will include the NAP Agent component as part of the core operating system, which will be used for both NAP and NAC. In addition to the native Extensible Authentication Protocol (EAP) methods and the 802.1X supplicant that are included with the Windows Vista and Windows Server "Longhorn" operating systems, an additional EAP-FAST method and EAPoverUDP supplicant will be provided to enable interoperability between NAC and NAP. The EAP-FAST method and EAPoverUDP supplicant will be developed by Cisco and distributed by Microsoft with Windows Update and Windows Server Update Services (WSUS) through the EAP Certification Program. Using 802.1X, EAPoverUDP, and EAP-FAST provides agent transparency for the NAC network infrastructure.

A single agent architecture for Windows Vista and Windows Server "Longhorn" greatly simplifies the deployment of a health infrastructure consisting of NAP components, NAC components, or a combination of the two.

Computers running Windows® XP with Service Pack 2 will need to run the Cisco Trust Agent for NAC and run the NAP Agent for NAP.

ISV Integration Ecosystem

To simplify the development of third-party health agent and health enforcement components for clients running Windows Vista, the NAP client APIs will serve as the single programmatic interface used for health reporting and enforcement for both NAP and NAC. This will facilitate the integration of applications that collect health information by ISVs.

Agent Deployment and Update Support

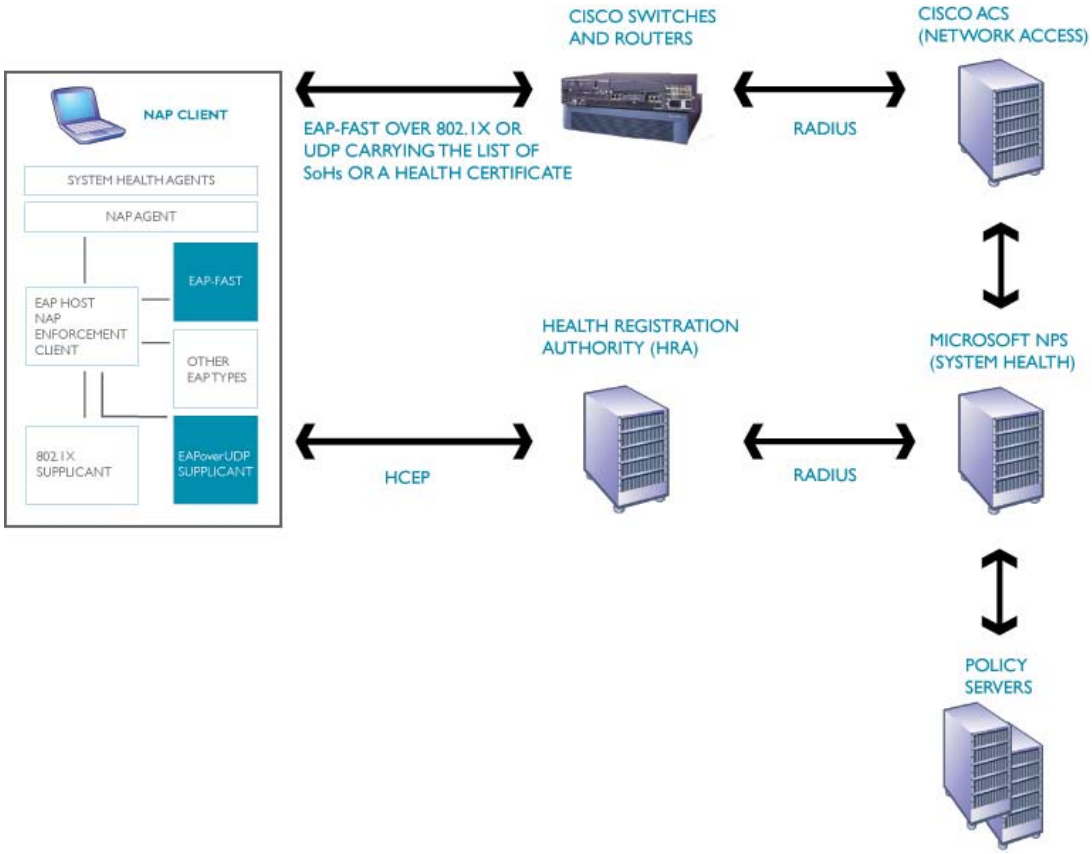
The customer experience and process for deploying the required agent components for interoperability with Windows Vista and Windows Server "Longhorn" will be similar to deploying typical Windows operating system services. The NAP Agent and 802.1X supplicant are native to the Windows Vista and Windows Server "Longhorn" operating systems, and the EAP-FAST and EAPoverUDP modules, developed by Cisco, will be distributed by Microsoft with Windows Update and Windows Server Update Services. Additionally, Group Policy configuration support for the agent components (including the EAP-FAST and EAPoverUDP modules) will be supported.

Cross-Platform Support

To support client operating systems other than Windows, Microsoft will license elements of the NAP client technology to third-party software developers. Cisco will continue to support and develop its NAC client (the Cisco Trust Agent) for non-Windows Vista and non-Windows Server "Longhorn" platforms and will continue to execute on its publicly stated direction to submit the Cisco NAC protocols for standardization through open standards processes.

Cisco NAC and Microsoft NAP Interoperability Architecture

Figure 1 shows the NAC and NAP interoperability architecture.



The NAC and NAP interoperability architecture consists of the following components:

- *NAP client (Microsoft):* The NAP client computer is a computer running Windows Vista or Windows Server "Longhorn" that sends its health credentials as either a list of Statements of Health (SoHs) or a health certificate. The client architecture consists of a layer of System Health Agents (SHAs), the NAP Agent, the EAPHost NAP Enforcement Client, EAP methods to perform account credential authentication and indication of health status, and EAP supplicants that allow the client to send EAP messages over 802.1X or UDP.

  To obtain a current health certificate, the NAP client uses the Health Certificate Enrollment Protocol (HCEP) to send a certificate request and its list of SoHs to the Health Registration Authority (HRA).

- *Network access devices (Cisco):* NAC-enabled network access devices (which include switches, routers, wireless access points, VPN concentrators, and so on) provide network access to clients and serve as network enforcement points.
- *Access Control Server (ACS) (Cisco):* Cisco Secure ACS authorizes network access for clients by validating the administratively specified client attributes, which could include the identity of the user and/or the computer, and the overall health state of the client. Cisco Secure ACS sends an access profile to the network access device(s) 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 (NPS) (Microsoft):* A Microsoft NPS performs the validation of the computer's system health and provides remediation instructions if needed.
- *Health Registration Authority (HRA) (Microsoft):* An HRA obtains health certificates on behalf of NAP clients from a public key infrastructure (PKI) (not shown).
- *Policy servers (Microsoft or third party):* Servers that provide current system health state for Microsoft NPSs. Policy servers integrate with Microsoft NPSs through the NPS System Health Validator (SHV) API.

To accommodate this interoperability architecture, the NAP and NAC platforms will support the following:

- Cisco Secure ACS will pass the list of SoHs from the NAP agent to an NPS for overall client health validation.
- Microsoft NPS will support the Cisco Host Credentials Authorization Protocol (HCAP) to receive the list of SoHs from Cisco Secure ACS and return the list of SoH Responses (SoHRs).
- Cisco Secure ACSs will perform network access validation based on a health certificate.

How the NAC and NAP Interoperability Architecture Works

Upon connection to the network, the client will provide a set of credentials that will be validated in order to authenticate and authorize the appropriate level of network access. These client credentials can include user and/or computer identity credentials in addition to health credentials. Clients that are noncompliant can be rate limited, 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 (and optionally user and/or computer identity) is sent to a Cisco Secure ACS with EAP-FAST carried over 802.1X or EAPoverUDP. If a health certificate infrastructure is deployed, the client will send its health certificate to the Cisco Secure ACS for validation rather than sending a list of SoHs.

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 HCAP protocol. The Microsoft NPS evaluates the 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 will evaluate all of the credential validation results (which can include user and/or computer identity in addition to the SSoHR) to select and send the appropriate access profile to the network access device(s) to grant the authorized level of network access for the client. The Cisco Secure ACS will also return the SoHRs and the SSoHR to the NAP Agent on the client with EAP-FAST carried over 802.1X or EAPoverUDP. Noncompliant clients that are quarantined will be automatically revalidated upon remediation to provide a transparent end-user experience.

If the NAP client sends its health certificate rather than a list of SoHs, the Cisco Secure ACS will validate the certificate as the EAP-FAST session is established to determine the overall client health state. As in the case where a list of SoHs is used, EAP-FAST is carried over 802.1X or EAPoverUDP. Note that limited network access to the HRA is required for the client to acquire a health certificate. The Cisco Secure ACS will validate the health certificate along with any other required credentials (such as user and/or computer credentials) and send the appropriate access profile to the network access device(s) to grant the authorized level of network access for the client. If the client is noncompliant or if the client is unable to provide a health certificate, the client will be quarantined for remediation, and revalidation will occur automatically upon remediation.

To obtain a health certificate, the NAP client uses HCEP to send a certificate request and its list of SoHs to the HRA. The HRA sends the list of SoHs to the Microsoft NPS. The Microsoft NPS evaluates the SoHRs against the configured health requirements and sends the SSoHR and the list of SoHRs back to the HRA.

- If the NAP client does not need to be remediated, the HRA requests a health certificate from the PKI (not shown) and forwards it along with the SSoHR and the list of SoHRs to the NAP client.
- If the NAP client needs to be remediated, the HRA sends the SSoHR and the list of SoHRs to the NAP client. The NAP client performs the appropriate remediation and sends a new certificate request and its updated list of SoHs to the HRA.

Summary

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 will allow customers to realize 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. Interoperability will be supported with the release of NAP in Windows Server "Longhorn," which is scheduled to be available in the second half of 2007.

Related Links

See the following resources for further information:

- Microsoft Network Access Protection Web site at www.microsoft.com/nap
- Cisco Network Admission Control Web site at www.cisco.com/go/nac