

A photograph of a classical building facade with ornate architectural details, including columns and decorative moldings, set against a clear blue sky.

Network Access Control for Federal Employees and Contractors: Cisco Network Access Guardian

Network access control supports the missions of federal agencies, both by preventing the loss of intellectual property through insider threat and by avoiding infections that could threaten government continuity. For these reasons, network access control is mandated by the Homeland Security Presidential Directive 12 (HSPD-12), in the Federal Information Processing Standards (FIPS) 201 guidelines, and in Department of Defense (DoD) regulations such as DoD 8500.2 and JTF-GNO CTO 06-02. Every network access control solution must identify and authenticate users and enforce that the device security posture complies with agency policy. Ideally, to maximize agency productivity, the solution should automatically remediate noncompliant devices without requiring action from either the user or the IT group.

Executive Summary

Federal agencies have made progress in network access control by implementing solutions for identification verification, endpoint security, and network foundation security. Notably, agencies are in the process of implementing Personal Identification Verification (PIV) cards that comply with FIPS 201, and nearly all PCs and laptops are installed with antivirus software.

Despite this progress, today's approaches to network access control leave agency networks vulnerable to infection and insider threat. For example, PIV cards authorize users—but not their devices. Therefore, authorized employees can access the network even if they are using a laptop that is infected, lacks required software or patches, or otherwise does not comply with the agency security policy. Similarly, antivirus software mitigates the threat of viruses, spyware, and other malicious software, but it does not check a device for compliance with security policies intended to protect the device and agency network from future infection and attack. Agency security policies can stipulate the presence of required software, absence of unauthorized software, misconfiguration, software defects, and user account issues such as null passwords.

Cisco® Network Access Guardian, which includes McAfee Hercules Remediation Manager, is an all-in-one solution for HSPD-12 compliance and network access control in federal government agencies. It ensures that a user's identity is authenticated and the device is compliant with security policies before it is granted access to the network. When a user attempts to access the network using a PIV card, Cisco Network Access Guardian authenticates the user's identity, scans the device to determine if it complies with the agency's security policy, then automatically quarantines and remediates the device if required. With Cisco Network Access Guardian, agencies can choose from a rich set of compliance checks and more than 25,000 tested remedies to quickly create comprehensive, granular security policies.

This white paper, intended for federal agency business managers, describes the all-in-one solution for network access control for federal government employees and contractors. The first section explains the challenges of access control. The next section explains solution requirements to meet agency business needs and comply with HSPD-12. The white paper concludes with a scenario using Cisco Network Access Guardian and a description of how federal agencies can benefit from this solution.

Challenges of Network Access Control

Table 1 summarizes the challenges of network access control in federal government. Until now, agencies have had to deploy separate systems for each requirement, decreasing the effectiveness of network access control and increasing the management burden for the IT group.

Table 1 Four Requirements for a Network Access Control Solution

	Identify and Authenticate	Enforce Policy for Device Security Posture	Quarantine and Remediate	Enforce Role-Based Access
Value to Agency	Identify authorized users and devices and create associations between the two. For example, certain employees might be authorized for network access only on specified devices.	Scan devices for compliance with agency security policy before admitting them to network, enforcing a consistent policy across the entire network.	Isolate devices that are not compliant to prevent them from spreading infections, becoming infected, or becoming a point of entry for an attacker. Automatically remediate the device so that it conforms to policy.	Enable agency to develop and apply comprehensive access policies based on user's role, preventing a legitimate agency employee from accessing information and resources for which they are not authorized.
Risk If Not Present	Unauthorized employees can gain access to network resources and sensitive information.	A decentralized policy, configured and enforced on individual endpoints, can leave gaps, including inconsistent patch or signature requirements.	A noncompliant device that is not isolated can make the network vulnerable to infection or attack. If remediation is manual rather than automated, employees and IT staff spend more time than is necessary.	If role-based access policies are difficult to establish or use, employees might abandon them.

“Security policy enforcement and malware defenses at the traditional network perimeter are no longer sufficient to protect the information and systems connected to the internal network.”

—Phil Schacter,
Burton Group, March 22, 2006

The Value—and Limitations—of Endpoint Security Solutions

Endpoint security solutions include anti-x software (antivirus, antispyware, and others), personal firewalls, and host intrusion prevention systems. Infections persist in federal government despite the fact that nearly every agency-owned computer is installed with antivirus software. Agency infections commonly occur when a laptop, used by an employee at home or during travel, becomes infected and then spreads the infection when the employee reconnects it to the agency network. Even laptops that are protected with antivirus software can become infected—for example, if the employee misses a virus-signature update when traveling.

The Value—and Limitations—of Identification Verification

PIV cards can effectively protect against unauthorized access to agency networks, but they do not protect against insider threat and the loss of confidential information. In addition, PIV cards cannot prevent an authorized user from connecting with a device that became infected from off-network use, which is vulnerable to attack because it lacks an operating system patch, or which otherwise violates the agency's security policy.

The Value—and Limitations—of Network Foundation Security

Firewalls prevent external users from accessing the network through illegitimate ports. However, they do not block unauthorized users or malicious traffic from entering through legitimate ports. Intrusion detection systems and intrusion prevention systems can detect and stop harmful or anomalous traffic, but they do not prevent insiders from accessing information they are not authorized to view. In addition, detection often occurs after the fact, when malware has already entered the network or unauthorized information access has already occurred.



Requirements for Network Access Control in Federal Government

The following capabilities are required to protect network resources from unauthorized access and to help ensure the continuity of government by preventing network infection or attack.

Identifies User and Role

The network access control system must identify users and their roles in order to prevent unauthorized access and stop the loss of intellectual property. An effective solution needs the intelligence to permit different levels of access based on the user's role. Federal contractors, for example, might be given access to a separate VLAN that does not provide access to servers containing sensitive information.

Checks Device Security Posture

Infections persist even if devices are protected with anti-x software. Therefore, an effective network access control solution should check devices for compliance with the agency's security policy before every connection attempt. While every agency's security policy stipulates that a device must be infection-free, policies differ from one agency to another as to required or prohibited software, required operating system and software version levels and patches, registry settings, services to be started and stopped, and so on. An effective network access control solution for federal government should allow the agency to define its own policy, and even to define separate policies for employees and guests. For guests, including contractors and employees visiting from other agencies, it might be adequate to simply verify that the device is not infected and is installed with a specified version of an operating system and appropriate patches.

Quarantines and Remediates Devices

After authorizing the user and confirming that the device security posture conforms to policy, the network access control solution should swiftly grant access to the agency network. If the device is not compliant, however, the device must be quarantined—so that it does not spread an infection or become vulnerable to attack—and then remediated. Remediation might involve repairing the infection, installing or removing software, or changing settings.

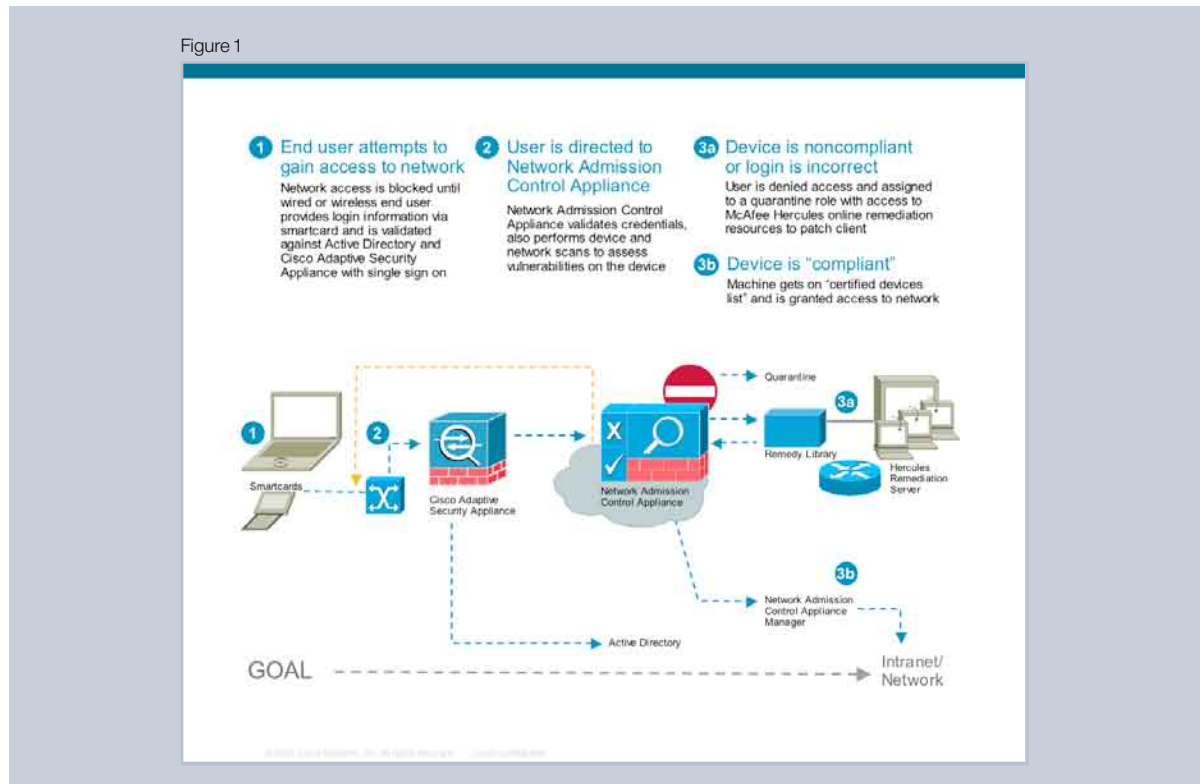
To protect the productivity of users and the agency IT staff, remediation should be rapid and completely automated. The first network access control solutions did not perform automated remediation. Instead, employees were directed to a Website that instructed them how to perform the required remediation, which took time. In other agencies, employees were instructed to call IT, which took even more time, both for the employee and the IT staff. The sidebar provides a checklist of requirements for an effective network access control system for government.

Solution Criteria for Network Access Control

- Promote employee productivity by providing a fast path to the network.
- Allow users to connect and disconnect frequently.
- Eliminate the need for users to perform remediation or call the help desk.
- Minimize the time that users have to wait for quarantined devices to be granted network access.
- Operate with wired and wireless networks, including VPNs and remote access.
- Provide robust auditing and reporting capabilities.

Solution: Cisco Network Access Guardian with McAfee Hercules

The Cisco Network Access Guardian with McAfee Hercules provides an all-in-one solution for compliance with HSPD-12, as well as enforcement, quarantine, remediation, and authorization. Following is a typical use scenario (Figure 1).



1. A federal employee or contractor inserts a PIV card to log in.
2. Within a few seconds, Cisco Network Access Guardian authenticates and authorizes the user based on role. A typical access policy might be:
 - Agency executives can access all servers.
 - Departmental employees and contractors can access specified departmental servers.
 - Guests and roaming users can access the Internet, only, in order to establish a VPN connection.

At the same time, Cisco Network Access Guardian scans the device to ensure compliance with the agency's security policy, which is hosted on the McAfee Hercules remediation server. The security policy can apply more than 25,000 predefined and tested remediation actions after checking for the following five categories of vulnerabilities:

- Unsecured accounts, including null passwords and passwords without forced expiration
- Unnecessary services
- Backdoors, including spyware
- Misconfigurations
- Software defects, such as missing patches

McAfee Hercules also includes DoD Security Technical Implementation Guide (STIG) policies for all Windows platforms. If the agency's device security posture requires remedies other than the 25,000 that are predefined in the Hercules system, the agency can define those remedies using the Hercules management console.

Guest Access for Contractors and Employees of Other Agencies

Cisco Network Access Guardian makes it easy to provide contractors or other visitors with secure, limited access to the agency network. When a visitor connects to the agency network, the host device receives an IP address but can initially connect only to the Cisco Network Access Control appliance. After opening a Web browser, visitors are directed to the agency's visitor Web page, where they enter a temporary username and password. The agency can customize the visitor page by including its security policy, agreement of compliance, or a button to install optional client software. After the visitor enters login credentials, Cisco Network Access Guardian authenticates the credentials using the agency's existing authentication system: RADIUS, Lightweight Directory Access Protocol (LDAP), Microsoft Active Directory, or other. Upon successful authentication, the solution applies the appropriate policies to the network switch port. These can include traffic control policies, timeout policies, access schedules, and more. The IP address and port remain the same throughout the session, so that visitors do not lose connectivity and do not need to take any additional action. The agency IT staff can monitor all guests' activity by consulting an event log that displays each visitor's username, login time, and MAC/IP or IP address.

3a. If the device is noncompliant, McAfee Hercules quickly and automatically remediates the device—without any action from the user or from IT. Any violation of the security policy can be remediated, with activities such as:

- Removing infections
- Installing required software, such as Cisco Security Agent, or patches
- Implementing hardening techniques and security best practices such as disabling unnecessary accounts, stopping unnecessary services, starting services, or others

3b. If the user is authorized and the device posture acceptable, Cisco Network Access Guardian grants limited or full network access based on the agency's policy for the individual or group.

4. After remediation is complete, Cisco Network Access Guardian grants limited or full network access based on the agency's policy for the individual or group.

Benefits of Cisco Network Access Guardian and McAfee Hercules for Federal Agencies

Simplified Deployment and Support

Because it is an all-in-one solution, Cisco Network Access Guardian can be deployed more rapidly than separate solutions for user authorization and device security-posture checking, which must be integrated. Support requirements are very low because all authorization and remediation is automatic. Employees do not need to take any action and therefore do not need help-desk support. This frees up agency IT groups to focus on strategic projects.

Reduced Network Downtime, Increased Availability

By checking the device security posture before permitting access, Cisco Network Access Guardian helps prevent infections that can interrupt the network. This increases network availability and employee productivity. Agencies can configure Cisco Network Access Guardian to require higher levels of compliance for agency-owned laptops, while still accommodating access by guests or mobile contractors whose devices meet minimum requirements.

Prevention of Loss of Intellectual Property from Insider Threat

In 2002, the U.S. Secret Service and the Computer Emergency Response Team began a collaborative effort to examine insider threat—that is, incidents perpetrated by current or former employees or contractors who intentionally exceed or misuse an authorized level of network, system, or data access in a manner that affects the security of the organization's data, systems, or daily business operations. The Cisco Network Access Guardian solution helps prevent insider threat by authenticating users and their devices before granting network access, and then enforcing the agency's access controls. An employee in the Inspections department, for example, might be granted access to departmental databases but not to the human resources database.

Increased Productivity for Employees and IT Groups

Employee productivity is not interrupted during login or remediation because both activities occur quickly and without any action from the employee. Users can connect and disconnect throughout the day as needed. The productivity of IT employees increases as well, because they no longer need to travel to employee offices and perform remediation. The agency IT group now only needs to define the device posture security policy when the software is deployed.

Access to Latest Vulnerability Intelligence

The McAfee Remediation Security Group continuously researches emerging vulnerability information and rapidly builds new remedies for supported operating systems, applications, and devices. The group correlates and distills vulnerability information from multiple sources into a single reference. After determining the appropriate remedy and testing it, McAfee makes the information available online to its customers. McAfee usually distributes action packs and remedies the same day it discovers a vulnerability. The McAfee team also creates policy enforcement templates based on industry best practices and can build custom templates for specific customer needs.

Conclusion

Traditional identification and authorization solutions ignore the device posture, exposing government networks to infections and making them vulnerable to insider threat. Traditional remediation solutions impede agency productivity by requiring either the employee or the IT group to take action. Cisco Network Access Guardian with McAfee Hercules overcomes the limitations of previous solutions. Together, they provide an easy-to-use, flexible solution for network access control that can enforce any agency's unique device security policy. The joint solution protects network resources without any cost to productivity, because user and device validation and remediation occur without any action from the user or the IT group. Using Cisco Network Access Guardian with McAfee Hercules, government agencies can achieve better access control, reduced risk of insider threat, and increased network availability, all of which help the agency fulfill its mission.

For more information, visit www.cisco.com/go/federal or contact the Cisco Center of Excellence at email: coe-cnag@cisco.com.