FISMA Compliance with Cisco Federal Solutions

Executive Summary

To meet compliance requirements of the Federal Information Security Management Act (FISMA), federal agencies must tie planning, processes, and technology together to make effective use of agency resources while protecting the confidentiality, integrity, and accessibility of mission-critical information systems.

A 2006 survey of federal IT security professionals, performed by Cisco with Market Connections, highlighted two key barriers to meeting FISMA compliance: budget and existing security architectures. Appropriating the budget for IT security initiatives is often a challenge, whether for commercial or governmental entities. And the risks are high. Major financial loss and even loss of life may result from inadequate security measures within the U.S. government IT enterprise.

The other key barrier to FISMA compliance is the existing security architecture. The notion that security "fixes itself" is now a barrier to FISMA implementation and strong evidence of a reactionary approach to federal IT security. Typically, for example, as security fixes such as operating system patches are applied to the environment, security officials would patch the security vulnerability for a short-term fix. The long-term fix, addressing security issues at an architectural level that allows for interoperability among security solutions and across enterprises, has not been a priority.

Cisco views long-term secure information assurance as a top priority for federal agencies. This white paper begins with a summary of FISMA challenges and the risk management framework. It then explores three key areas for agencies to target—configuration management, access control, and incident response—to improve not only FISMA compliance but also overall information security. Lastly, this white paper addresses these three key FISMA areas with the Cisco® Self-Defending Network solutions that are available to federal agencies.

The Self-Defending Network is Cisco's strategy to protect federal organizations from threats caused by both internal and external sources. This protection helps government organizations take better advantage of the intelligence in network resources, thus improving overall security while addressing FISMA requirements. Concerns that Cisco can address, helping to meet FISMA requirements, include unauthorized access, malicious code, scans and probes, improper usage, and denial-of-service attacks.

I. FISMA Challenges and Risk Management Framework

The Federal Information Security Management Act (FISMA) of 2002 is a set of standards that defines how federal agencies must implement security controls and policies to protect data.

In August 2006, Cisco performed the 2006 Federal IT Security Survey, which involved interviews with 200 federal IT decision-makers. More than 45 agencies and all branches of the military were represented in the respondent pool.

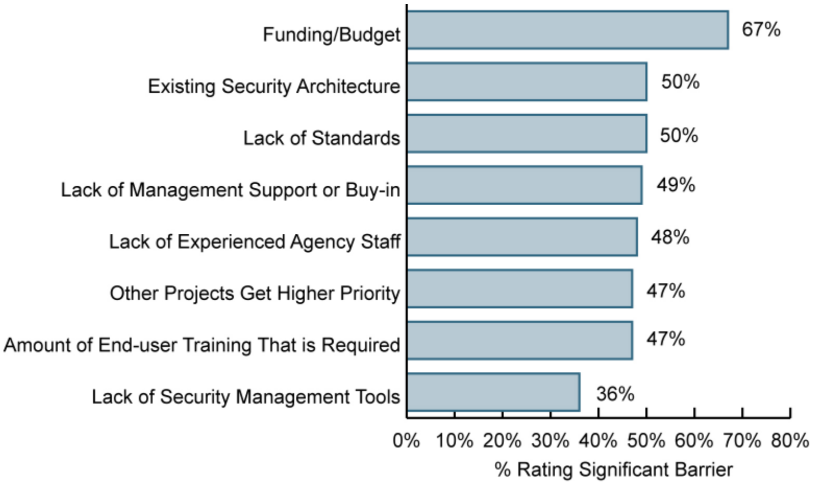
Top barriers specific to FISMA compliance: The greatest challenges in meeting FISMA compliance, according to these respondents, are management and staff issues, including management awareness, employee/management participation, and lack of personnel. Other barriers identified include understanding of regulations, security, and lack of tools and equipment. These barriers have become more evident as the number of incident reports have increased by 44 percent in one year, as reported by the Office of Management and Budget in its FY 2006 Report to Congress and shown in Table 1.

Table 1. FISMA Incident Reports to US-CERT

	FY 2005	FY 2006
Unauthorized Access	304	706
Denial of Service	31	37
Malicious Code	1,806	1,465
Improper Usage	370	638
Scans/Probes/Attempted Access	976	1,388
Investigation	82	912
Total Incidents Reported	3,569	5,146

Top barriers to improving network security in general: Two-thirds of the respondents identified lack of funding as the top barrier to improving network security capabilities. Other barriers rated as concerns by approximately half the respondents are security architecture, lack of standards, lack of management support/buy-in, lack of qualified staff, higher priority projects, requirements for high levels of end user training, and a lack of security tools, as shown in Figure

Figure 1. Top Barriers to Improving Network Security

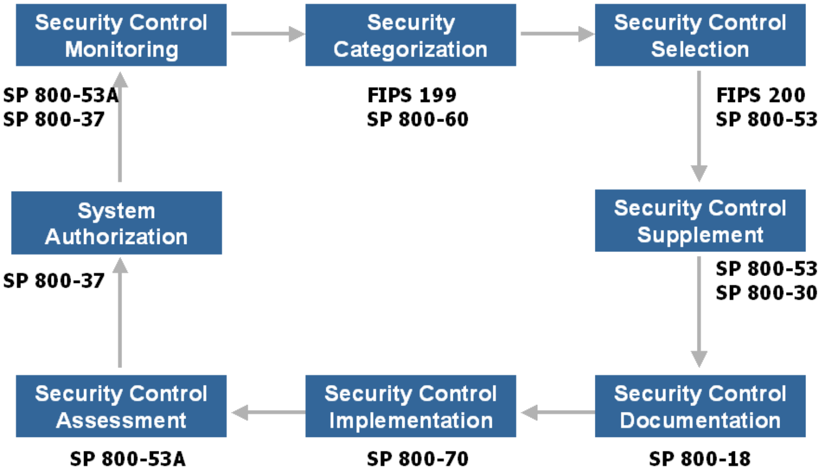


Fisma Risk Management Framework

FISMA's comprehensive Risk Management Framework focuses on a fundamental level of "security due diligence" for federal agencies and their contractors based on minimum security requirements and security controls.

The framework consists of eight steps that agencies must follow to be compliant with FISMA requirements. These steps are an iterative process, requiring continuous application and refinement throughout the information security process. The eight steps are briefly described in more detail in Appendix B and illustrated graphically in Figure 2.

Figure 2. Risk Management Framework Steps for FISMA Compliance


Security Control Monitoring
Security Categorization
Security Control Selection
SP 800-53A
SP 800-37
FIPS 199
SP 800-60
FIPS 200
SP 800-53
System Authorization
Security Control Supplement
SP 800-37
SP 800-53
SP 800-30
Security Control Assessment
Security Control Implementation
Security Control Documentation
SP 800-53A
SP 800-70
SP 800-18

II. Moving Beyond Compliance

The flexibility of the Risk Management Framework means that agencies can find different ways to comply with FISMA requirements. This flexibility offers both a challenge to auditors and difficulty in relating levels of compliance between agencies. There is more than one way to comply with the requirements.

Government auditors verify levels of FISMA compliance and provide compliance scores to federal agencies in key reporting areas. While FISMA report cards indicate adherence to FISMA requirements based on auditor assessments, Cisco contends that the real goal of federal agencies is true system and information security.

Cisco Compliance Philosophy

Agency officials recognize the complexity involved in meeting and maintaining regulatory compliance and understand that no single product or process achieves compliance. A comprehensive approach that encompasses planning, process, and technology is the key to gaining compliance.

- Planning happens within the federal agency, with assistance from compliance experts and trusted partners, like Cisco and Cisco’s partners.
- Processes are the day-to-day activities performed by agency staff.
- Technology consists of the tools that Cisco and partners bring to federal agencies.

Cisco recognizes the breadth of challenges federal agencies face in achieving true information assurance, and offers three key areas of focus for federal agencies, based upon the results of the 2006 Federal IT Security Survey:

- Configuration Management: Knowing what is in the network and the configuration profiles of all network equipment inventory is a primary starting point for information assurance.
- Access Control: Restricting access to the network based on precise rules helps to protect information.
- Incident Response: Tracking and logging activity on the network enables effective procedures for responding to incidents.

With Cisco's technology tools and consultative services, federal agencies can plan for information security and compliance and carry out the repeatable and measurable processes required to achieve FISMA compliance, as well as building a true information assurance architecture.

III. Cisco Solutions for FISMA Configuration Management

Problems and challenges with respect to IT security and FISMA compliance are many, including data integrity, threat protection, regulatory compliance, contingency, and reporting, among others. Although each issue is important, Cisco has identified three significant areas as key security challenges for CxOs and security administrators:

- Configuration Management and Reporting
- Access Control
- Incident Reporting

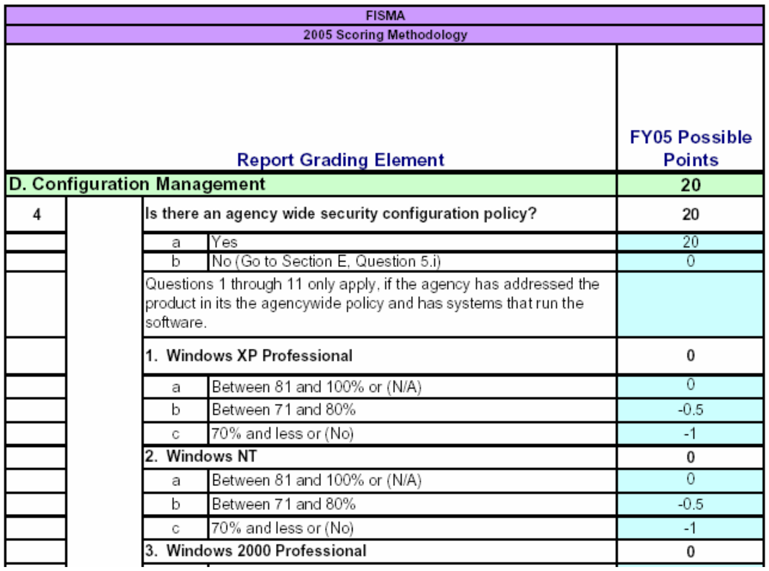
Configuration Management & Reporting

FISMA reported to Congress for 2006 that there were 10,595 information systems in operation, of which only 8144 (76 percent) had tested security controls. The number of systems grows each year, as does the number of elements composing them. This highlights the importance of consistent and compliant management of the growth and configuration of these systems.

The FISMA Configuration Management control addresses policies and procedures, change control, monitoring of configuration changes, configuration settings, and access restrictions for configuration changes.

Agencies need a way to inventory, control, and track all changes to the information system. This control requires a policy that governs configuration changes and provides automated enforcement of the policy by the network. The ability to control and track changes also helps agencies identify security gaps in their current configurations, track and control changes, and pinpoint incorrect configurations in their environment. Figure 3 shows part of a sample report card for configuration management. Inventory tracking account for a lot of points in the FISMA Configuration Management reporting section.

Figure 3. Sample Report Card for Configuration Management



FISMA				
2005 Scoring Methodology				
Report Grading Element				FY05 Possible Points
D. Configuration Management				20
4			Is there an agency wide security configuration policy?	20
		a	Yes	20
		b	No (Go to Section E, Question 5.i)	0
			Questions 1 through 11 only apply, if the agency has addressed the product in its the agencywide policy and has systems that run the software.	
			1. Windows XP Professional	0
		a	Between 81 and 100% or (N/A)	0
		b	Between 71 and 80%	-0.5
		c	70% and less or (No)	-1
			2. Windows NT	0
		a	Between 81 and 100% or (N/A)	0
		b	Between 71 and 80%	-0.5
		c	70% and less or (No)	-1
			3. Windows 2000 Professional	0

Organizations must establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development lifecycles. They must establish and enforce security configuration settings for information technology products employed in organizational information systems.

Configuration management is a vital aspect of security assurance. Agencies must be able to perform this function centrally to have visibility of all IT system devices, and be able to control software changes to ensure the integrity of security related designs. Security administrators must validate that system inventory is accurate, ensure devices are operating within established best practice software configurations, have the ability to roll out mass changes, and be able to limit access for devices that do not comply with security configuration policies.

Cisco Configuration Management Solutions

There are three primary Cisco configuration management solutions that address the Configuration Management reporting section. Each solution has specific strengths in the area of configuration and change management:

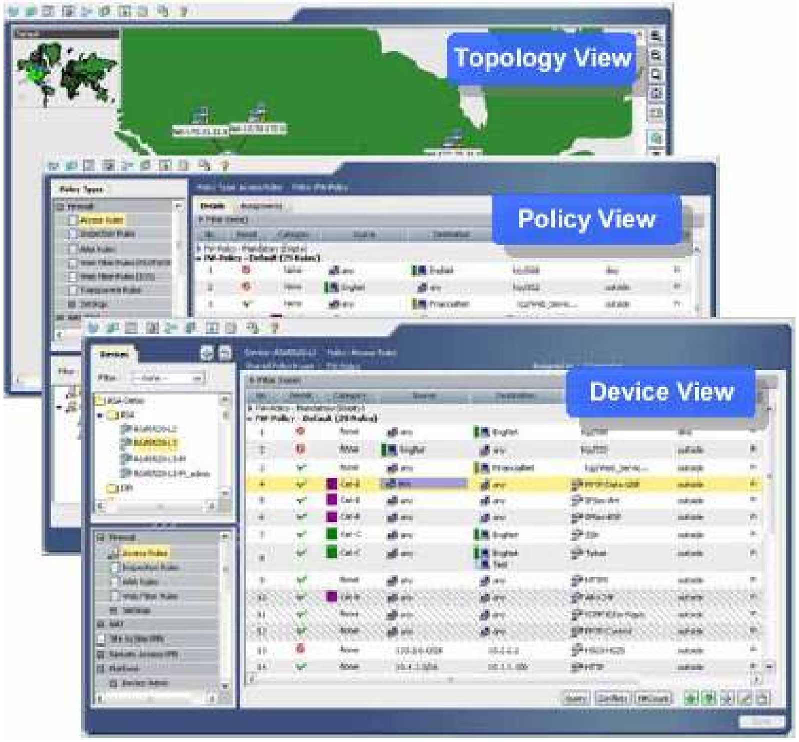
- Cisco Security Manager configures Cisco security features such as firewall, VPN, and intrusion protection system (IPS) on Cisco devices.
- Cisco Configuration Assurance Solution performs automated network audit, security, and policy compliance analysis.
- CiscoWorks Network Compliance Manager automates the configuration workflow, creates regulatory compliance reports, and audits devices and network changes against the compliance standards.

Cisco Security Manager is a powerful and easy-to-use solution to centrally provision all aspects of device configuration and security policies for Cisco firewalls, VPNs, and IPSs. As the centralized security configuration management tool, Cisco Security Manager provides an operationally efficient means to centrally configure thousands of remote Cisco security devices with a rich and easy graphical interface. It provisions Cisco firewall, intrusion prevention, and VPN encryption devices including Cisco router platforms running Cisco IOS® security software images, Cisco ASA 5500 Series Adaptive Security Appliances, Cisco PIX® security appliances, Cisco IPS 4200 Series sensors, and Cisco Catalyst® 6500 Series security services modules. The firewall or VPN policies apply across different Cisco platforms, without needing distinct policies for each individual device type.

For example, Cisco Security Manager can create a single firewall rule table, which applies to all Cisco security platforms. The administrator also has the flexibility to customize policies at the local device level or device group level when needed.

Cisco Security Manager offers multiple views that provide flexible methods to manage both devices and policies, including the ability to manage the security network visually on a topology map. Figure 4 shows the Topology view, Policy view, and Device view of Cisco Security Manager.

Figure 4. Cisco Security Manager Views



Cisco Security Manager centrally specifies which policies are shared and automatically inherited by new devices, to ensure that corporate policies are implemented consistently. When a setting is changed, Cisco Security Manager automatically applies the change to all affected network devices.

To configure VPN connections, it only takes a few clicks in the GUI interface to accomplish this across Cisco VPN devices. Site-to-site, hub-spoke, full mesh, or extranet VPN connections can be configured using this easy method. Both IP Security (IPsec) and DMVPN configurations are supported.

IPS management is fully integrated into Cisco Security Manager. This includes IPS device and policy views with context-sensitive menus, as well as content-based common IPS policies that allow the creation of enterprisewide policies that can be configured once and deployed to many. IPS signature policies and event action filters can be inheritable and assignable to any device. IPS management also includes policy rollback, a configuration archive, and cloning or creation of signatures.

Cisco Security Manager has the ability to assign specific tasks to each administrator during the deployment of a policy, with formal change control and tracking. It provides role-based access control, in which access rights can be defined for multiple administrators, with appropriate controls. Cisco Security Manager helps with operational functions such as software distribution or device inventory reporting.

Cisco Security Manager integrates with Cisco's incident response solution, the Cisco Security Monitoring, Analysis, and Response System (MARS), to correlate events with the associated firewall rules to help with quicker decision making and incident response.

Cisco Configuration Assurance Solution (CAS) completely automates end-to-end network and security configuration auditing, providing quick access to network integrity reports, security compliance assessments, access requirements validation, resiliency studies, and regulatory compliance reports. Through advanced analytics and network modeling, Cisco CAS builds a topology and load model of the production network, understanding device relationships and configuration dependencies, to identify:

- Security gaps and vulnerabilities
- Network and application survivability
- IP addressing issues
- Route map and attribute inconsistencies (such as HSRP and QoS)
- Regulatory noncompliance
- A wide variety of switching and routing protocol issues

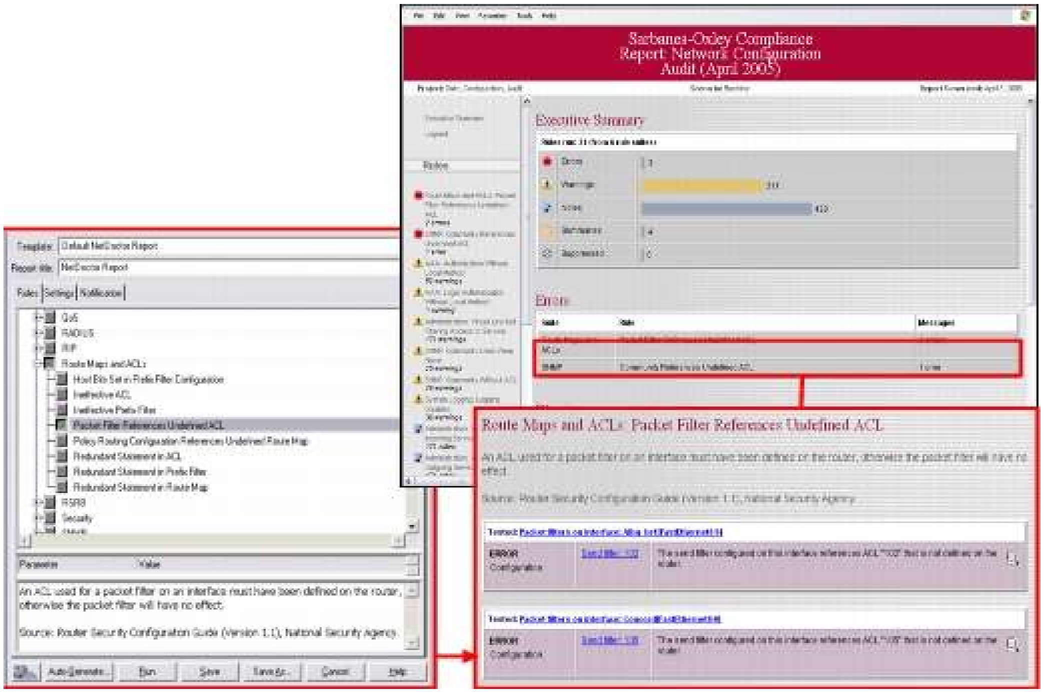
Cisco CAS detects configuration problems before they disrupt network operations by using an extensive library of nearly 600 rules, customizable and configurable to analyze individual devices, groups of devices, topology, traffic, security, and routing behavior.

Cisco CAS checks and reports compliance with internal IT and regulatory requirements such as NIST 800-53 and DISA STIG. It also supports key processes from popular IT governance frameworks, including ITIL/BS15000, ISO17799/BS7799, and NSA.

Cisco CAS allows network configuration audits to be executed automatically on a weekly, daily, or ad-hoc basis. Through integration with the CiscoWorks Network Compliance Manager, Cisco CAS can detect and identify configuration and security issues in near real-time, reducing windows of vulnerability to minutes, not days and weeks.

Cisco CAS provides extensive reporting capabilities through an integrated Web-based Report Server, a central repository for reports encompassing documents, charts, tables, and images as shown in Figure 5. These comprehensive audit reports provide detailed assessments of network change, localization of problems, and recommendations for resolution.

Figure 5. Network Audit Reports



Sarbanes-Oxley Compliance Report: Network Configuration Audit (April 2005)

Executive Summary

Errors

Route Maps and ACLs: Packet Filter References Undefined ACL

An ACL used for a packet filter on an interface must have been defined on the router, otherwise the packet filter will have no effect.

Source: Router Security Configuration Guide (Version 1.1), National Security Agency

Template: Default NetDoctor Report

Report title: NetDoctor Report

An ACL used for a packet filter on an interface must have been defined on the router, otherwise the packet filter will have no effect.

Source: Router Security Configuration Guide (Version 1.1), National Security Agency.

Rules
Settings
Notification
QoS
RADIUS
RIP
Route Maps and ACLs
Host Bits Set in Prefix Filter Configuration
Ineffective ACL
Ineffective Prefix Filter
Packet Filter References Undefined ACL
Policy Routing Configuration References Undefined Route Map
Redundant Statement in ACL
Redundant Statement in Prefix Filter
Redundant Statement in Route Map
RSRB
Security
Parameter
Value
Auto-Generate...
Run
Save
Save As...
Cancel
Help
Rules
ACLs
ERROR
Configuration

These reports provide detailed results of the network audit, including informational reports summarizing network configuration characteristics such as deployed software releases and patch levels. Trending reports analyze the results of successive audits over time, allowing users to track progress and trace incidents. Access can be restricted by username and password.

Cisco CAS supports network security through configuration analysis and validation, with more than 150 rules for security-related issues. It includes rule suites for authentication, authorization, and accounting (AAA), access control lists, kerberos, RADIUS, TACACS+, SNMP, system logging, device administration, and others.

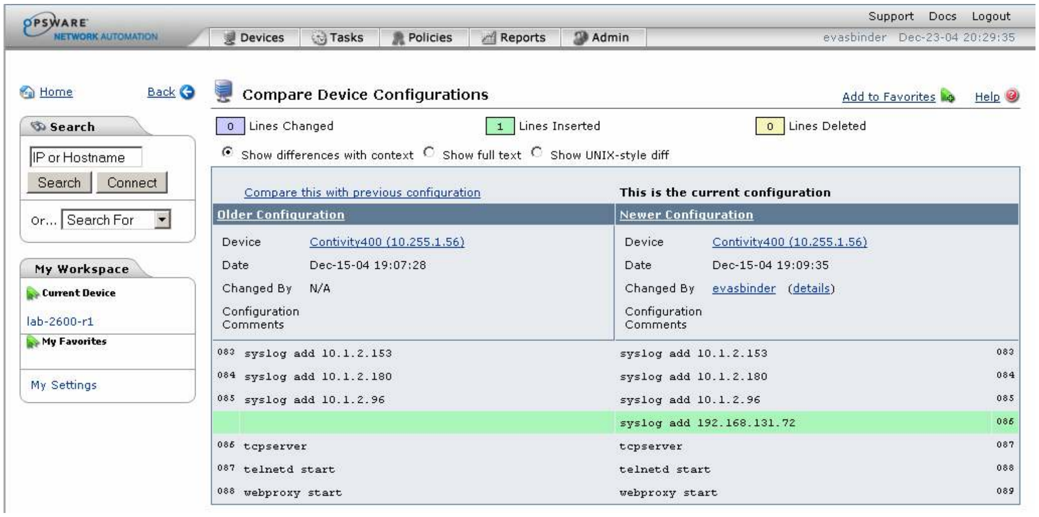
Configuration integrity can be checked under simulated failure conditions, to ensure that high-availability configurations meet operational objectives. Network security can also be tested with an automated port scan analysis that performs a nonintrusive vulnerability assessment under normal and failure network conditions.

CiscoWorks Network Compliance Manager (NCM) helps agencies meet FISMA requirements and enforce internal IT best practices in several ways:

- Tracks all configuration, software, and hardware changes to the network in real time
- Captures changes in a detailed audit trail
- Screens all changes against authorized policies immediately to verify whether changes comply with FISMA
- Identifies and corrects trends that could lead to problems such as network instability and service interruption
- Improves visibility of network changes

CiscoWorks NCM creates reports for auditing purposes, which focus on the configuration change management of the devices on the network. Figure 6 displays the Device Configuration comparison screen.

Figure 6. CiscoWorks Network Compliance Manager Device Configuration Comparison



Compare Device Configurations

0 Lines Changed 1 Lines Inserted 0 Lines Deleted

● Show differences with context ○ Show full text ○ Show UNIX-style diff

Compare this with previous configuration		This is the current configuration	
Older Configuration		**Newer Configuration**	
Device	Contivity400 (10.255.1.56)	Device	Contivity400 (10.255.1.56)
Date	Dec-15-04 19:07:28	Date	Dec-15-04 19:09:35
Changed By	N/A	Changed By	evasbinder (details)
Configuration Comments		Configuration Comments	

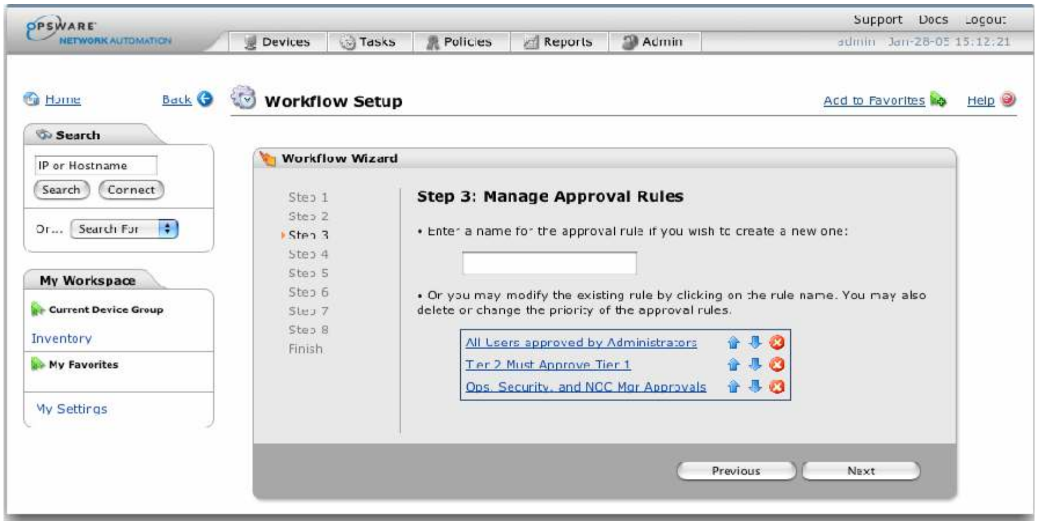
```
083 syslog add 10.1.2.153        syslog add 10.1.2.153        083
084 syslog add 10.1.2.180        syslog add 10.1.2.180        084
085 syslog add 10.1.2.96         syslog add 10.1.2.96         085
                                 syslog add 192.168.131.72    086
086 tcpserver                    tcpserver                    087
087 telnetd start                telnetd start                088
088 webproxy start               webproxy start               089
```

CiscoWorks NCM automatically validates new changes against appropriate policies before they are pushed to the network. Changes that are not compliant are not deployed.

CiscoWorks NCM automates the change review process, closing the gap between the approval of a change and the actual configuration change that is pushed to the network. It allows managers to enforce the approval of a change. Approvers can review the change in the context of the entire device configuration and the business units it will affect. Event notifications are sent to interested parties, giving network staff immediate visibility into unplanned and unauthorized changes.

CiscoWorks NCM also limits network configuration information to users on a need-to-know basis. It controls what information a user can view, what actions a user can perform on devices, and which devices a user can gain direct access to. Figure 7 shows the Approval screen.

Figure 7. CiscoWorks Network Compliance Manager Approval Screen



Step 3: Manage Approval Rules

- Enter a name for the approval rule if you wish to create a new one:

- Or you may modify the existing rule by clicking on the rule name. You may also delete or change the priority of the approval rules.

All Users approved by Administrators
Tier 2 Must Approve Tier 1
Ops, Security, and NCC Mgr Approvals

Improved Configuration Management Strategy

Cisco configuration management solutions improve configuration management and changes with consistent configuration management and clear visibility of related security capabilities. The central management capabilities give administrators scalable control of large IT networks, while automated policy enforcement ensures that required security configurations are employed by all devices allowed to access the network. Audit information and change visibility provide security administrators information for proactive and reactive situations. Visibility of device status, system changes, and security policy violations via detailed reporting tools enable effective application and management of IT security architecture.

IV. Cisco Solutions for FISMA Access Control Compliance

The government's mobile workforce is expanding rapidly as agencies realize the value of remote network access and encourage teleworking to support plans for continuity of operations. As a result, IT organizations are managing more mobile and remote devices than ever before. To protect confidentiality and prevent network disruption from attack or infection, IT groups need to validate that users are authorized to access systems and that the users' devices are infection-free and compliant with security policy.

In September 2006 US-CERT reported that 88.9 percent of security incidents were related to scans, probes, and attempted access. Agencies need both network-based access controls and role-based access controls that securely manage who and what can access the network, as well as when, where, and how that access can occur.

FISMA Access control addresses access policies and procedures, account management, and the associated tools and techniques for access enforcement and password control, systems notifications, separation of duties, session lock and termination, marking and labeling, and remote and wireless access.

Organizations must limit information system access to:

- Authorized users
- Processes acting on behalf of authorized users, or devices (including other information systems)
- The types of transactions and functions that authorized users are permitted to exercise

Cisco Access Control Solutions

Cisco access control solutions focus on three areas:

- Cisco Network Admission Control (NAC) allows comprehensive security policies to be translated into actionable rules and then reliably enforced.
- Cisco Unified Wireless Solution is an end-to-end architecture that integrates key security and wireless solutions to deliver standards-based network protection.
- Cisco Access Control Server (ACS) extends access security by combining authentication, user access, and administrator access with policy control within a centralized identity networking solution.

Cisco Network Admission Control (NAC) reduces and controls large-scale vulnerability-based exploits and attacks by ensuring that all endpoint devices enter the network with the proper protection installed and enabled. This is particularly useful for organizations in which corporate assets are individually controlled by the users to which they are assigned. These assets are easy targets for infections, which may substantially disrupt productivity if permitted to spread.

Cisco NAC allows organizations to enforce their security policies on all endpoint devices (managed and unmanaged) as they enter the network, regardless of:

- Access methods: connecting through the LAN, WLAN, WAN, or VPN
- Ownership: owned by the corporation, employees, contractors, and guests
- Device types: Windows, Macintosh, or Linux machines; laptops; desktops; PDAs; and corporate assets such as printers and IP phones
- Application configurations: registry key settings, services running, or system files
- Remediation models: no access, quarantine and remediation, automatic, user controlled

Access is permitted only to compliant and trusted endpoint devices, which can include PCs, servers, IP phones, wireless devices, and printers. Cisco NAC can deny access to noncompliant devices or redirect them to a quarantine and remediation area.

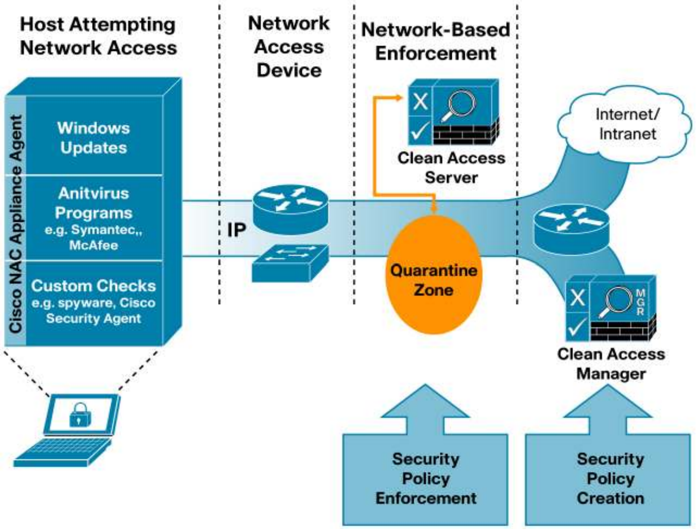
Cisco NAC can be rapidly deployed everywhere in an organization’s network, or it can be deployed in focused areas (such as remote access or wireless access networks) to resolve critical security concerns. Cisco NAC delivers endpoint compliance assessment, user identity authentication, policy management and enforcement, and remediation services in all types of network environments. It consists of the following components:

- NAC Manager provides a Web-based interface for creating security policies and managing online users. It can also act as an authentication proxy to authentication servers. Administrators can use NAC Manager to establish user roles, compliance checks, and remediation requirements. It communicates with, and manages, the NAC Server, which is the enforcement component.

- NAC Server is implemented at the network level and performs device compliance checks as users attempt to access the network. It can be implemented in-band or out-of-band, in Layer 2 or Layer 3, as a virtual gateway or as a real IP gateway, and can be centrally deployed or distributed throughout the network, therefore providing deployment flexibility for virtually any network environment.
- NAC Agent (optional) is a lightweight, read-only agent that runs on an endpoint machine. It performs a deep inspection of a local machine's security profile by analyzing registry settings, services, and files. Through this inspection, it can determine whether a device has installed and enabled a required hotfix, the correct antivirus software version, Cisco Security Agents (personal firewall/host intrusion detection/prevention systems) and other host security software. For unmanaged assets, the NAC Agent is downloadable in real time.

Cisco NAC can be deployed in an otherwise open environment so that onsite visitors and guests must meet certain security requirements before they can connect to the network. Cisco NAC can assign different types of network access depending on user credentials, so that, for example, onsite visitors and guests may be provided with general Internet access, but no access to the internal network. Figure 8 shows a typical Cisco NAC deployment.

Figure 8. Cisco NAC out-of-band deployment


Host Attempting Network Access
Network Access Device
Network-Based Enforcement
Cisco NAC Appliance Agent
Windows Updates
Anitvirus Programs e.g. Symantec,, McAfee
Custom Checks e.g. spyware, Cisco Security Agent
IP
Clean Access Server
Quarantine Zone
Internet/ Intranet
MGR
Clean Access Manager
Security Policy Enforcement
Security Policy Creation

Cisco NAC can control connections from a remote site. This is especially useful in dealing with partner connections, in which it is difficult or impossible to determine who is sitting behind a connection at a remote partner site.

The ability to control access after a user is authenticated provides a highly effective way to maintain security and protect confidential information. Cisco NAC enables users and their devices to achieve policy compliance so that they are proactively protected as they work in different environments. Cisco NAC quarantines noncompliant devices so that they are not compromised and used as a hiding place for malicious users to launch further attacks. Cisco NAC then updates the devices to bring them into compliance.

To minimize the inconvenience to end users, Cisco NAC Appliance supports single sign-on for VPN clients, wireless clients, and Windows Active Directory domains. Administrators can maintain multiple user profiles with different permission levels through the use of roles-based access control. The Cisco NAC authentication capabilities can track and audit user activities while on the network. The log information can be used to assist incident response, forensics, and analysis purposes.

Cisco Secure Wireless Solution is a business-ready, standards-based architecture that gives netkwork administrators confidence that data will remain private and secure. The Cisco Secure Wireless Solution is an end-to-end architecture that integrates key security and wireless solutions to deliver standards-based network protection. Critical features of the Cisco Secure Wireless Solution include:

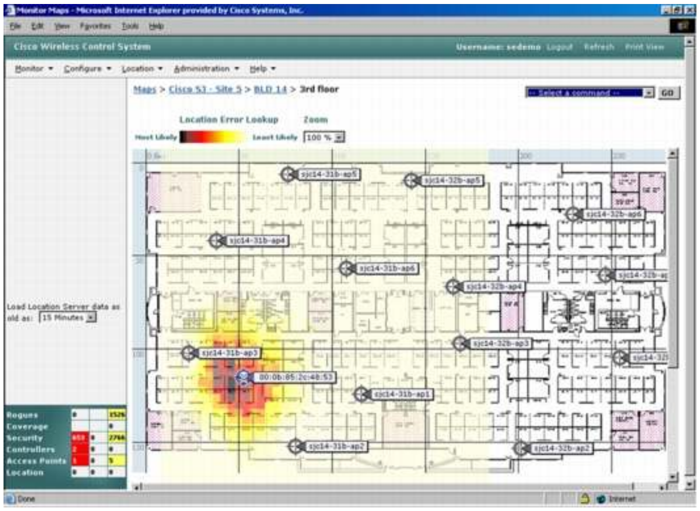
- Unified wired and wireless intrusion protection system/intrusion detection system (IPS/IDS)
- Client validation, posture assessment, and remediation
- Wireless single sign-on and 802.1X integration
- Granular control for secure guest access
- Host intrusion prevention
- Rogue detection through automatic RF monitoring
- Wireless security management

The first step in enabling accurate wireless threat detection and prevention is to ensure that authorized wireless infrastructure and users are properly identified to the network. This is done through use of IEEE 802.11i. The Cisco Secure Wireless Solution works with Cisco NAC to provide proper checks and authentication before granting access to the network.

The Cisco Secure Wireless Solution incorporates radio resource management (RRM) to continuously monitor the surrounding air space. This knowledge, combined with detection of all over-the-air wireless activity, enables the Cisco Secure Wireless Solution to immediately identify and prevent rogue access points and ad hoc networks. Deployment of Cisco Security Agent on wireless endpoints ensures that simultaneous connections to the enterprise wired network and wireless interface are prevented, so that client misassociations do not occur.

Cisco Unified Wireless Network Lightweight Access Points, whether servicing clients or configured as air monitors, scan for all Wi-Fi activity. If a managed access point detects another access point over the air that is not managed by a Cisco Unified Wireless Network controller, it is classified as a rogue. The location of the rogue is immediately plotted on the floor plan map (Figure 9). If investigated and found to be a neighboring wireless LAN, such as in a hotspot or adjacent business, the administrator can mark it as a “known external rogue.” Similarly, internal access points that are known, such as those in test environments, can be marked as “known internal rogues.”

Figure 9. Detected Rogue Access Points Displayed on a Map for Physical Removal


Monitor Maps - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
Cisco Wireless Control System
Username: sedemo Logout Refresh Print View
Monitor ▾ Configure ▾ Location ▾ Administration ▾ Help ▾
Maps > Cisco 53 - Site 5 > BLD 14 > 3rd floor
-- Select a command --
GO
Location Error Lookup
Zoom
Most Likely
Least Likely
100 %
Load Location Server data as old as: 15 Minutes
sjc14-31b-ap5
sjc14-32b-ap5
sjc14-32b-ap6
sjc14-31b-ap4
sjc14-31b-ap6
sjc14-32b-ap4
sjc14-32b-ap3
sjc14-31b-ap3
00:0b:85:2c:48:53
sjc14-31b-ap1
sjc14-31b-ap2
sjc14-32b-ap2
Rogues
Coverage
Security
Controllers
Access Points
Location
Done
Internet

Cisco Secure Wireless Solution detects ad hoc networks by looking at over-the-air packets and analyzing them for specific frames that indicate the connection is ad hoc, not infrastructure. Once an ad hoc network is detected, the Cisco Secure Wireless Solution can protect against it by sending disassociation frames to the clients to stop the network connection.

A unified strategy incorporating Cisco Security Agent software and the Cisco Secure Wireless Solution can be deployed to not only detect, but also prevent client misassociation. The Cisco Wireless Control System (WCS) detects and generates an alarm when a client connects to any rogue access point, enabling the administrator to take action. However, this particular threat can be eliminated by use of Cisco Security Agent software. Configuring Cisco Security Agent to prevent simultaneous use of the wired and wireless interfaces ensures that employees connected to the wired network do not accidentally create a bridge to their wireless enterprise.

As with any security solution, intuitive management tools are a prerequisite to maintaining a secure network. The Cisco Secure Wireless Solution uses Cisco WCS for wireless LAN planning, configuration, and management. Cisco WCS provides a foundation that allows IT managers to design, control, and monitor enterprise wireless networks from a centralized location, simplifying operations and reducing total cost of ownership.

Cisco WCS alerts network managers to security threats and provides a graphical view of the network, including the location and threat level of rogue access points. In combination with it, Cisco Security MARS recognizes and correlates real network attacks and provides actionable guidelines on how to stop them. The combination of these management capabilities provides a comprehensive and intuitive management framework.

Cisco Secure Access Control Server (ACS) is a highly scalable, high-performance access control server that operates as a centralized RADIUS and TACACS+ server. It extends access security by combining authentication, user access, and administrator access with policy control within a centralized identity networking solution, allowing greater flexibility and mobility, increased security, and user-productivity gains.

Cisco Secure ACS enforces a uniform security policy for all users regardless of how they access the network. It reduces the administrative and management burden involved in scaling user and network administrator access to the network. By using a central database for all user accounts, Cisco Secure ACS centralizes the control of all user privileges and distributes them to hundreds or thousands of access points throughout the network.

As an accounting service, Cisco Secure ACS provides detailed reporting and monitoring capabilities of network users' behavior and keeps a record of every access connection and device configuration change across the entire network. Cisco Secure ACS supports a broad variety of access connections, including wired and wireless LAN, dialup, broadband, content, storage, voice over IP (VoIP), firewalls, and VPNs.

Cisco Secure ACS provides a centralized identity networking solution and simplified user management experience across all Cisco devices and security management applications. It helps to ensure enforcement of assigned policies by allowing network administrators to control:

- Who can log into the network
- The privileges each user has
- Security audit or account billing information
- Access and command controls for each configuration's administrator

Cisco Secure ACS addresses concerns about compliance, supporting compliance features associated with administrator permission and audit reports:

- Administrative constraints on log settings restrict administrators from disabling certain types of logging.
- Forced administrator password change at logon prompts administrators to change the password at configurable time intervals.
- Administrator password policy provides a mechanism to enforce a configurable minimum password length and mix of characters (upper/lower case, numeric, punctuation).
- Forced administrator password change for stale account enforces password change when the administrator has not logged on in for a specified number of days.
- Generation of entitlement reports provides a report that shows all administrator privileges.
- Password history for administrators prevents administrators from reusing passwords.

Improved Access Control Strategy

Cisco's access control solutions provide tactical and strategic IT security capabilities by controlling individual user access, ensuring that devices connecting to the system comply with current software security policies, securing devices that connect by wireless access, and regulating changes of configuration and software to multivendor network infrastructure.

V. Cisco Solutions for FISMA Incident Response Compliance

Worms or virus outbreaks can spread globally in just minutes. Although these attacks can bring networks down and cause business disruption, the greater threat is when sensitive information is stolen. Both external thieves and malicious insiders gain access and steal information. Therefore, early detection and proactive response are crucial for protecting agency data, assets, and information systems and for ensuring confidentiality of data and communications.

The FISMA Incident Response control addresses policies and procedures, incident handling, incident reporting, and incident response assistance, including forensic services and automated tools.

Organizations must:

- Establish an operational incident-handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities
- Track, document, and report incidents to appropriate organizational officials and/or authorities

The need for an incident-handling capability within agency organizations that crosses agency boundaries has never been greater. Standard reporting and uniform operating procedures permit agencies and the Computer Emergency Response Team (US-CERT) to be better positioned for assessing risks, addressing vulnerabilities, reducing overall costs, and meeting the security challenges of federal agencies' information infrastructure. FISMA requires agencies to report security incidents to the US-CERT.

NIST Special Publication 800-61 reminds federal agencies that prevention, keeping the number of incidents low, is important to protect their business processes, mission, and reputation. If security controls are insufficient or security policies are not enforced, large numbers of incidents can occur with overwhelming consequences.

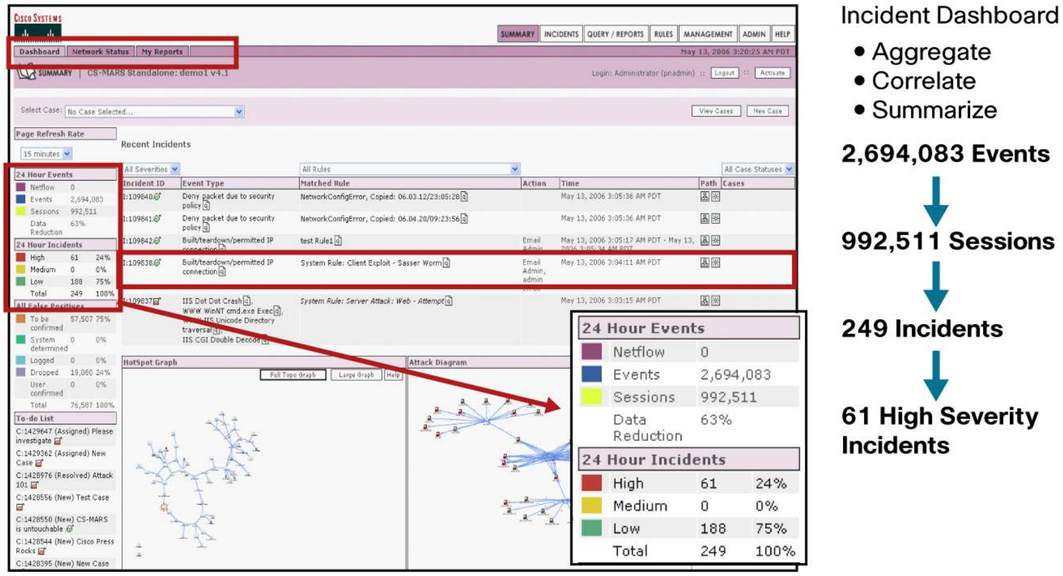
Cisco Incident Response Solutions

For the best incident response, the network needs central intelligence to intelligently react to an incident, and the network devices need to identify and alert the central intelligence entity. With this approach, Cisco incident response solutions include Cisco Security MARS and Cisco Intrusion Prevention System (IPS).

Cisco Security Monitoring, Analysis and Response System (MARS) works with your existing network and security investments to identify, isolate, and recommend precise removal of offending elements. It also helps maintain internal policy compliance and can be an integral part of your overall regulatory compliance solution.

Cisco Security MARS transforms raw network and security data into intelligence that can be used to subvert valid security incidents and maintain compliance. This easy-to-use family of threat mitigation appliances enables operators to centralize, detect, mitigate, and report on priority threats using the network and security devices already deployed in your infrastructure. Figure 10 shows the intelligent operation that Cisco Security MARS automatically performs.

Figure 10. Cisco Security MARS Incident Intelligence



Incident ID	Event Type	Matched Rule	Action	Time	Path	Cases
I:109840	Deny packet due to security policy	NetworkConfigError, Copied: 06.03.12/23:05:28		May 13, 2006 3:05:36 AM PDT		
I:109841	Deny packet due to security policy	NetworkConfigError, Copied: 06.04.20/09:23:56		May 13, 2006 3:05:36 AM PDT		
I:109842	Built/teardown/permitted IP connection	test Rule1	Email Admin	May 13, 2006 3:05:17 AM PDT - May 13, 2006 3:05:34 AM PDT		
I:109838	Built/teardown/permitted IP connection	System Rule: Client Exploit - Sasser Worm	Email Admin, admin	May 13, 2006 3:04:11 AM PDT		
I:109837	IIS Dot Dot Crash, WWW WinNT cmd.exe Exec, WWW IIS Unicode Directory traversal, IIS CGI Double Decode	*System Rule: Server Attack: Web - Attempt*		May 13, 2006 3:03:15 AM PDT		

24 Hour Events		
🟪 Netflow	0	
🟦 Events	2,694,083	
🟨 Sessions	992,511	
Data Reduction	63%	
24 Hour Incidents		
🟥 High	61	24%
🟨 Medium	0	0%
🟩 Low	188	75%
Total	249	100%
All False Positives		
🟧 To be confirmed	57,507	75%
🟩 System determined	0	0%
🟦 Logged	0	0%
🟪 Dropped	19,080	24%
User confirmed	0	0%
Total	76,587	100%

To-do List
C:1429647 (Assigned) Please investigate
C:1429362 (Assigned) New Case
C:1428976 (Resolved) Attack 101
C:1428556 (New) Test Case
C:1428550 (New) CS-MARS is untouchable
C:1428544 (New) Cisco Press Rocks
C:1428395 (New) New Case

Incident Dashboard
- Aggregate
- Correlate
- Summarize

2,694,083 Events

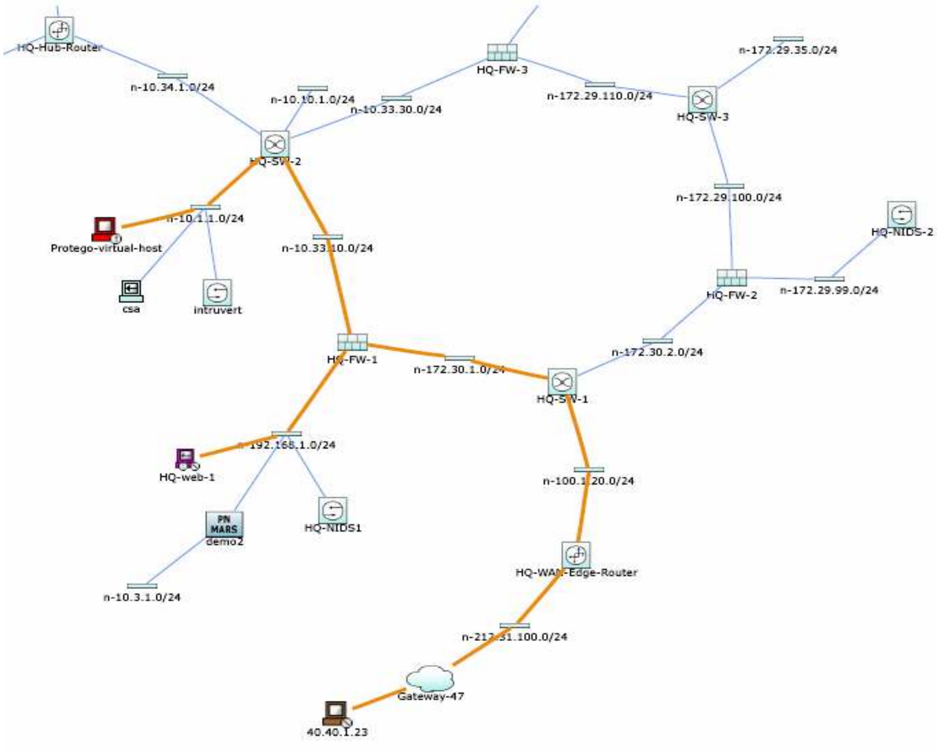
992,511 Sessions

249 Incidents

61 High Severity Incidents

Cisco Security MARS obtains network intelligence by understanding the topology and device configurations from routers, switches, and firewalls, and by profiling network traffic. The system's integrated network discovery function builds a topology map containing device configuration and current security policies, which enables it to model packet flows through your network, as shown in Figure 11.

Figure 11. Cisco Security MARS Topology Map

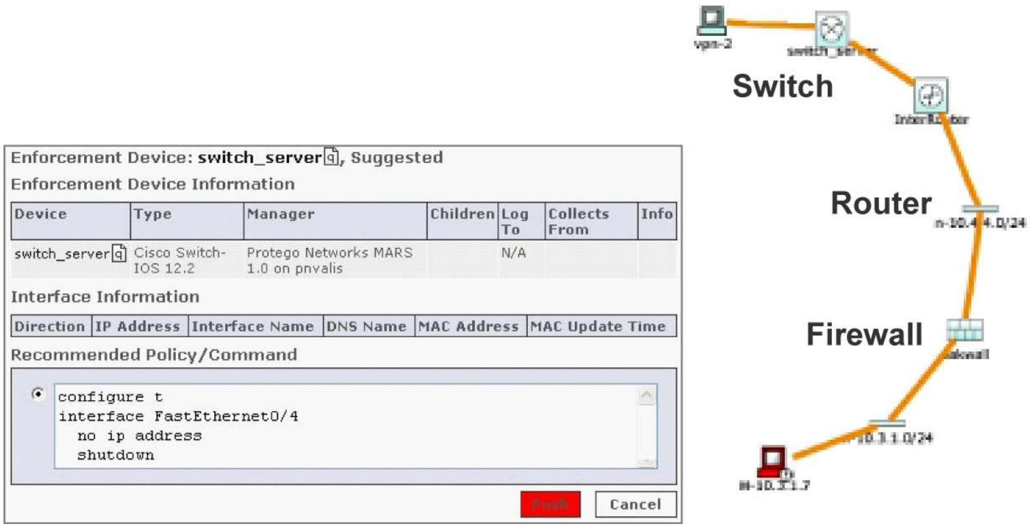


The appliance centrally aggregates logs and events from:

- Network devices such as routers and switches
- Security devices and applications such as firewalls, IDSs, vulnerability scanners, and antivirus applications
- Hosts such as Windows, Solaris, and Linux syslogs
- Applications such as databases, Web servers, and authentication servers
- Network traffic such as Cisco NetFlow

Cisco Security MARS features an easy-to-use analysis framework that streamlines the conventional security workflow, providing automated case assignment, investigation, escalation, notification, and annotation for daily operations and specialized audits. It can graphically replay attacks and retrieve stored event data to analyze previous events. The system fully supports ad-hoc queries for real-time and subsequent data-mining efforts. It can map the intrusion and supply recommended actions to take on the network, as displayed in Figure 12.

Figure 12. Cisco Security MARS intrusion mapping and action recommendation



Enforcement Device: **switch_server**, Suggested

Enforcement Device Information

Device	Type	Manager	Children	Log To	Collects From	Info
switch_server	Cisco Switch-IOS 12.2	Protego Networks MARS 1.0 on pnvalis		N/A		

Interface Information

Direction	IP Address	Interface Name	DNS Name	MAC Address	MAC Update Time

Recommended Policy/Command

●

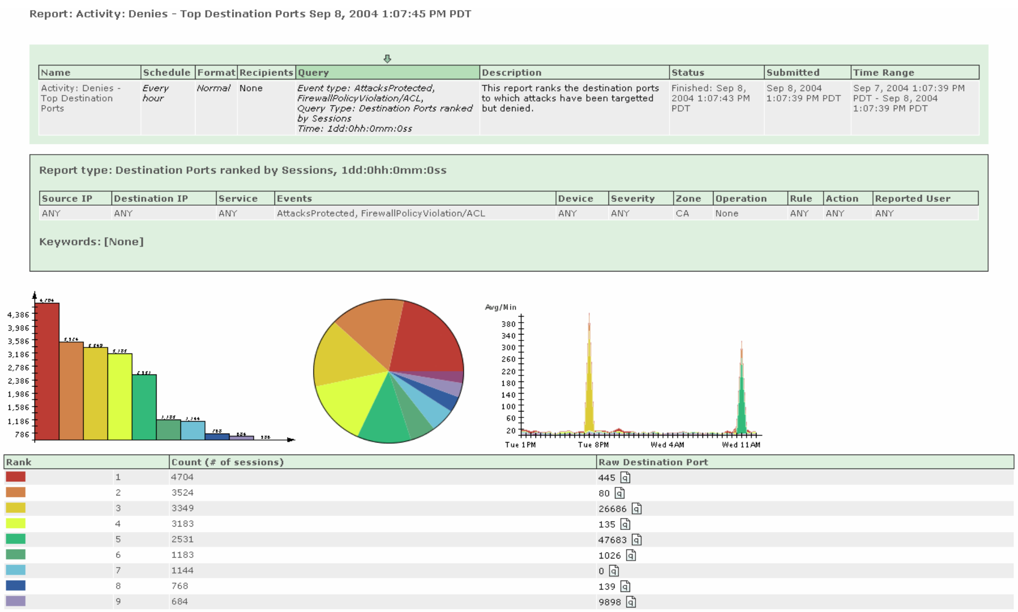
```
configure t
interface FastEthernet0/4
  no ip address
  shutdown
```

Cisco Security MARS offers numerous predefined reports to satisfy operational requirements and assist in FISMA efforts. An intuitive report generator can modify the more than 80 standard reports or generate new reports to build:

- Action and remediation plans
- Incident and network activity
- Security posture and audit
- Departmental reports-in data, trend, and chart formats

These reports also show the health of the network and incident occurrences, as shown in Figure 13. Both batch and e-mail reporting are enabled.

Figure 13. Cisco Security MARS Reporting Capabilities



Report: Activity: Denies - Top Destination Ports Sep 8, 2004 1:07:45 PM PDT

Name	Schedule	Format	Recipients	Query	Description	Status	Submitted	Time Range
Activity: Denies - Top Destination Ports	*Every hour*	*Normal*	None	*Event type: AttacksProtected, FirewallPolicyViolation/ACL,* *Query Type: Destination Ports ranked by Sessions* *Time: 1dd:0hh:0mm:0ss*	This report ranks the destination ports to which attacks have been targetted but denied.	Finished: Sep 8, 2004 1:07:43 PM PDT	Sep 8, 2004 1:07:39 PM PDT	Sep 7, 2004 1:07:39 PM PDT - Sep 8, 2004 1:07:39 PM PDT

Report type: Destination Ports ranked by Sessions, 1dd:0hh:0mm:0ss

Source IP	Destination IP	Service	Events	Device	Severity	Zone	Operation	Rule	Action	Reported User
ANY	ANY	ANY	AttacksProtected, FirewallPolicyViolation/ACL	ANY	ANY	CA	None	ANY	ANY	ANY

Keywords: [None]

Rank		Count (# of sessions)	Raw Destination Port
🟥	1	4704	445
🟧	2	3524	80
🟨	3	3349	26686
🟨	4	3183	135
🟩	5	2531	47683
🟩	6	1183	1026
🟦	7	1144	0
🟦	8	768	139
🟪	9	684	9898

Cisco Intrusion Prevention System (IPS) provides protection for both network devices and endpoints.

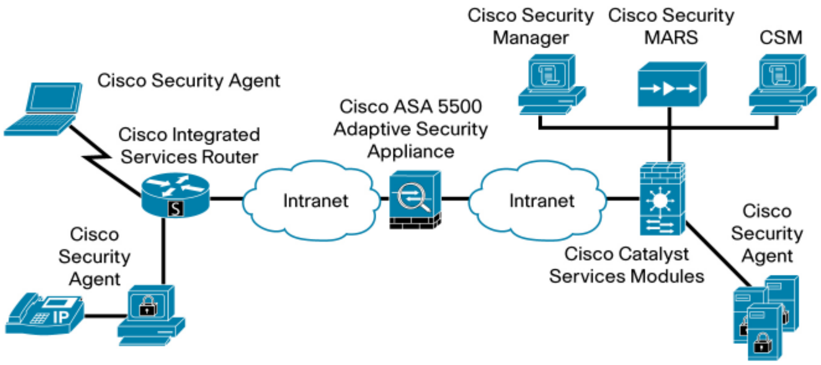
Cisco IPS solutions accurately identify, classify, and stop malicious traffic, including worms, spyware, adware, network viruses, and application abuse, before they affect business resiliency.

Cisco IPS solutions defeat threats from multiple vectors, including network, server, and desktop endpoints. The solutions range from purpose-built appliances and integrated firewall and IPS devices to service modules for routers and switches. Cisco IPS solutions protect the network from policy violations, vulnerability exploitations, and anomalous activity through detailed inspection of traffic at Layers 2 through 7, across the network.

Cisco IPS solutions employ a systemwide security ecosystem that assesses and reacts to threats. This collaborative system includes cross-solution feedback linkages, common policy management, multivendor event correlation, attack path identification, passive/active fingerprinting, host-based (Cisco Security Agent) IPS collaboration, load-balancing capabilities, and visibility into encrypted traffic.

A Cisco IPS solution delivers inline intrusion prevention capabilities, integrated at key points in the network, allowing for protection of your network's critical assets and data. Figure 14 shows how IPS technology can be strategically deployed throughout the network architecture, providing comprehensive prevention and protection.

Figure 14. Cisco IPS Solutions



Cisco IPS solutions provide strict control of application usage and policy conformance through traffic inspection, including instant messaging and peer-to-peer applications; strict HTTP enforcement; Port 80 inspection; and traffic filtering based on MIME types and OS fingerprinting. Policy violations are also managed by assessing user and endpoint contextual information.

Cisco's anomaly detection feature detects worms by learning the usual traffic patterns of the network, then scanning for anomalous behavior. Fast-propagating network worms scan the network to infect other hosts. For each protocol or service, the anomaly detection program studies what is normal scanning activity and accumulates this information in a threshold histogram and an absolute scanner threshold. The scanner threshold specifies the absolute scanning rate above which any source is considered malicious. Cisco IPS solutions detect infection characteristics based on dynamic learning capabilities of network usage.

Improved Incident Response Strategy

The ever-present threat of intrusion and infection from malicious software mandates that a reliable IPS is included as a first line of defense and is interoperable with other security architecture and solutions. Because intruders historically have been able to penetrate the best of front-line defenses, agencies should have complete visibility of their IT system and network topology, such as provided with Cisco Security MARS, with the ability to visualize the attack path and be able to quickly identify the source of the attack and respond with Cisco IPS solutions.

VI. Summary

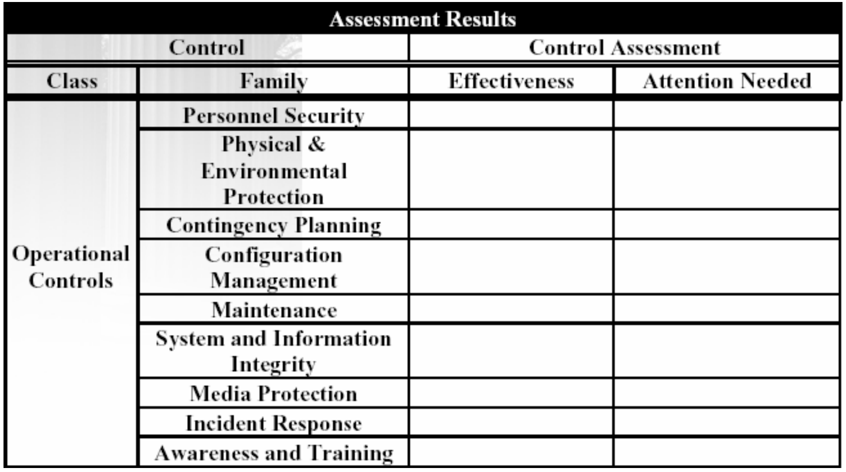
Cisco is focused on the security assurance challenges facing the industry and as recognized by FISMA. Cisco solutions have been designed to address these security needs with inherent flexibility to accommodate the ever-changing data security environment. This white paper shows how Cisco security solutions can help ensure the protection of information systems, enabling agencies to develop scalable and manageable security strategies and maintain FISMA compliant plans and processes. The three areas of focus are configuration management, access control, and incident response.

FISMA mandates awareness and overall strategies for assuring the security of federal IT systems and networks, and Cisco has designed interoperable solutions for enterprisewide security architecture strategy. The task of assuring information security on large and disparate systems is a daunting challenge for agency CxOs; therefore it is crucial that well-designed security architecture is complemented with manageable processes and reporting capabilities.

By presenting solutions for security issues that are common to all entities, both federal and commercial, Cisco demonstrates vital solutions that are part of an end-to-end strategic security architecture. For agencies that want to take security beyond compliance to true information assurance, Cisco offers these security solutions. For further information about Cisco security solutions, or a demonstration of Cisco solutions services, please contact your Cisco account manager or security specialist.

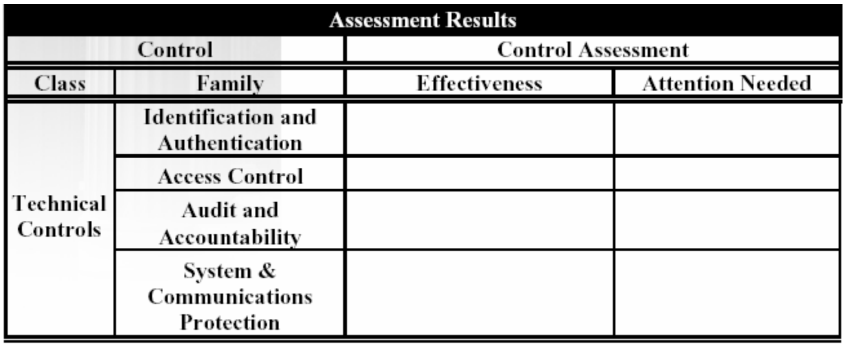
Appendix A. FISMA Audit Assessments

Operational Control Assessment



Assessment Results			
Control		Control Assessment	
Class	Family	Effectiveness	Attention Needed
Operational Controls	Personnel Security		
	Physical & Environmental Protection		
	Contingency Planning		
	Configuration Management		
	Maintenance		
	System and Information Integrity		
	Media Protection		
	Incident Response		
	Awareness and Training		

Technical Control Assessment



Assessment Results			
Control		Control Assessment	
Class	Family	Effectiveness	Attention Needed
Technical Controls	Identification and Authentication		
	Access Control		
	Audit and Accountability		
	System & Communications Protection		

Appendix B. Risk Management Framework

The following paragraphs briefly outline the eight iterative steps of the Risk Management Framework that agencies must follow to be compliant with FISMA requirements.

Categorize the Information Systems (FIPS 199, SP 800-60)

As the first and most important step in the Risk Management Framework, security categorization affects all other phases, from Security Control Selection to level of effort in Security Control Monitoring. Categorization gives agencies an accurate inventory of the assets in the agency. Careful and effective categorization, which requires participation of key officials (Chief Information Officer, Senior Agency Information Security Officer, authorizing officials, mission/system owners), results in the effective use of resources to protect systems at appropriate levels.

An incorrect information system impact analysis and categorization results in one of two scenarios:

- Overprotection of the information system, which wastes valuable security resources
- Underprotection of the information system, which places important operations and assets at risk

New FISMA language (Dec 06) stresses impacts on external agencies as well as national interests. “The organization also considers potential impacts to other organizations and, in accordance with the USA PATRIOT Act of 2001 and Homeland Security Presidential Directives, potential national-level impacts in categorizing the information system.”

Agencies define the category of the system based on the impact that a loss of security of that system could have on the agency. Impact levels are low, moderate, or high.

- Low Impact: the loss of confidentiality, integrity or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
- Moderate Impact: the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
- High Impact: the loss of confidentiality, integrity, or availability could be expected to have a catastrophic adverse effect on organizational operations, organizational assets, or individuals.

Effective categorization of federal information systems should result in distribution that looks like a normal or bell curve, centered on moderate impact.

The following steps are required to categorize information systems:

1. Define an asset.
2. Identify assets within the organization.
3. Prioritize assets.
4. Define categories for each asset, starting with the top priority assets.

Select the Minimum Security Controls (FIPS 200, SP 800-53)

Agencies establish baseline security controls for simplicity of application across low, moderate, or high impact systems. Security controls are the management, operational, and technical safeguards or countermeasures required to protect the confidentiality, integrity, and availability of an information system. These baseline controls provide a minimum level of protection for information systems.

1. Select common security controls (agency infrastructure-related controls or controls for common hardware/software platforms) as a corporatewide exercise with the participation of key officials.

The careful selection of common security controls can save the agency significant resources and facilitate a more consistent application of security controls across the enterprise. Agency officials assign responsibility for the development, implementation, assessment, and tracking of the controls and ensure that the resulting information is available to all interested parties.

2. Select common controls for all similarly categorized information systems (low, moderate, and high impact).
3. Assign responsibility for common control development, implementation, assessment, and tracking (or documentation of where controls are employed).

Refine the Security Control Set Based On Risk Assessment (SP 800-53, SP 800-30)

Once baselines are established, agencies refine those baselines for specific systems based on risk assessment to provide adequate protection on a system-by-system basis. Information system owners must supplement the common portion of the security control with system-specific controls as needed to complete security control coverage based on risk assessment results.

The tailored baseline represents the starting point for determining the needed level of security due diligence to be demonstrated by an organization toward the protection of its operations and assets. In many cases, additional security controls or control enhancements will be needed to address specific threats to and vulnerabilities in an information system or to satisfy the requirements of applicable laws, Executive Orders, directives, policies, standards, or regulations.

1. Identify control gaps.
2. Assign additional security controls beyond baseline as necessary.

Agency officials need to carefully document tailoring activities and decisions leading to tailored controls with reasoned justifications to defend the adjustments to auditors as necessary.

Document the Security Controls In The Systems Security Plan (SP 800-18)

Documenting tailored security controls captures the security controls for the information systems in a security plan. Appendix B provides a detailed look at security controls.

The systems security plan captures the baseline and tailored security controls for the information system.

1. Write systems security plan.

The security plan defines system name and identifier, categorization, owner, authorizing official, other designated contacts, security responsibility, operational status (operational, under development, undergoing major modification), information system type, general purpose/description, system environment, interconnection, laws/regulation/policies affecting the system, security controls, completion and approval dates, and ongoing plan maintenance.

2. Obtain approval of security plan from predetermined responsible official.
3. Maintain systems security plan by updating based on changes to the information systems controls.

Implement the Security Controls (SP 800-70)

System owners implement security controls documented in the security plan and apply security configuration settings.

1. Determine local operational and product requirements.
2. Obtain new or updated checklists.
3. Review, test, and document checklist in local environment.
4. Apply checklist to information system.

Assess the Security Controls (SP 800-53A)

Once the controls have been implemented, agencies assess that the tailored controls are meeting security requirements. Agency executives determine security control effectiveness (controls implemented correctly, operating as intended, meeting security requirements) during this step in the Risk Management Framework.

Agencies determine acceptable risk levels and authorize the operation of the information system based on the results of the assessment.

1. Assess control implementation.
2. Evaluate that security requirements are being met.
3. Identify control gaps.

Determine Agency-Level Risk and Risk Acceptability (SP 800-37)

System owner and responsible executives determine risk to agency operations, agency assets, or individuals based on the vulnerabilities in the information system and any planned or completed corrective actions to reduce or eliminate those vulnerabilities. If acceptable, the responsible executive authorizes information system operation.

1. Conduct risk assessment.
2. Verify, validate, and confirm assessment results.
3. Identify control gaps.
4. Prepare final security accreditation decision letter.

Updating Controls as a Result of Continuous Monitoring (SP 800-53A, SP 800-37)

This last step in the Risk Management Framework requires agencies to continuously track changes to the information systems that may affect security controls and reassess control effectiveness. This step transforms certification and accreditation from a static to a dynamic process, and requires a strategy for monitoring selected controls under a defined plan. Continuous monitoring provides a general understanding of needed security improvements for a system, and should lead to more effective annual reporting of FISMA compliance.

1. Test security controls.
2. Review test results.
3. Revise existing controls as necessary.

Appendix C. FISMA Security Controls

The National Institute for Standards in Technology (NIST), the standards authority for FISMA, has issued Special Publications SP 800-53, “Recommended Security Controls for Federal Information Systems,” and SP 800-30, “Risk Management Guide for Information Technology Systems,” which identify areas that require security controls and provide minimum standards for each. Agencies will consider technical, management, and operational security controls to prevent, limit, or deter threat-source damage to an organization’s mission. These controls provide a solid model for agencies to follow as they follow the steps in the Risk Management Framework, particularly in Phase 2 as defined in this white paper.

General Objectives

Management Security Controls

Preventive

- Assign Responsibility
- Document Control Plans
- Implement Personnel Controls
- Conduct Awareness Training

Detection

- Implement Security Controls

- Periodic control Reviews
- Periodic System Audits
- Ongoing Risk Management
- Address & Accept Residual Risk

Recovery

- Provide Support Continuity
- Incident Response Capability

Operational Security Controls

Prevention

- Control Media Access
- Limit External Distribution
- Control Viruses
- Safeguard Data Center Facility
- Secure Wiring Closets
- Provide Data Backup Capability
- Off Site Data Storage
- Protect PCs/Laptops
- Protect from Fire Damage
- Emergency Power (UPS)
- Control Humidity & Temperature

Detection

- Provide Physical Security
- Environmental Security

Technical Security Controls

Supporting

- Identification
- Crypto Key Management
- Security Administration
- System Protections

Preventive

- Authentication
- Authorization
- Access Control Enforcement
- Non-repudiation
- Protected Communications
- Transaction Privacy

Detection & Recovery

- Audit
- Intrusion Detection & Containment
- Proof of Wholeness
- Restore Secure State

Virus Detection & Eradication

Specific Objectives

NIST has identified 17 security control “families” or categories. Each category has specific security control types for which NIST has defined minimum standards for security control.

The following table identifies the specific control types for which NIST has documented minimum standards for security control within each of the 17 control families.

FISMA Security Controls

Management
CA-1 Certification, Accreditation, and Security Assessment Policies & Procedures
CA-2 Security Assessments
CA-3 Information System Connections
CA-4 Security Certification
CA-5 Plan of Action and Milestones
CA-6 Security Accreditation
CA-7 Continuous Monitoring
PL-1 Security Planning Policy and Procedures
PL-2 System Security Plan
PL-3 System Security Plan Update
PL-4 Rules of Behavior
PL-5 Privacy Impact Assessment
RA-1 Risk Assessment Policy and Procedures
RA-2 Security Categorization
RA-3 Risk Assessment
RA-4 Risk Assessment Update
RA-5 Vulnerability Scanning Not Selected
SA-1 System and Services Acquisition Policy and Procedures
SA-2 Allocation of Resources
SA-3 Life Cycle Support
SA-4 Acquisitions
SA-5 Information System Documentation
SA-6 Software Usage Restrictions
SA-7 User Installed Software
SA-8 Security Design Principles
SA-9 Outsourced Information System Services
SA-10 Developer Configuration Management
SA-11 Developer Security Testing
Operational

AT-1 Security Awareness and Training Policy and Procedure
AT-2 Security Awareness
AT-3 Security Training
AT-4 Security Training Records
CM-1 Configuration Management Policy and Procedures
CM-2 Baseline Configuration
CM-3 Configuration Change Control
CM-4 Monitoring Configuration Changes
CM-5 Access Restrictions for Change
CM-6 Configuration Settings
CM-7 Least Functionality
CP-1 Contingency Planning Policy and Procedures
CP-2 Contingency Plan
CP-3 Contingency Training
CP-4 Contingency Plan Testing
CP-5 Contingency Plan Update
CP-6 Alternate Storage Sites
CP-7 Alternate Processing Sites
CP-8 Telecommunications Services
CP-9 Information System Backup
CP-10 Information System Recovery and Reconstitution
IR-1 Incident Response Policy and Procedures
IR-2 Incident Response Training
IR-3 Incident Response Testing
IR-4 Incident Handling
IR-5 Incident Monitoring
IR-6 Incident Reporting
IR-7 Incident Response Assistance
MA-1 System Maintenance Policy and Procedures
MA-2 Periodic Maintenance
MA-3 Maintenance Tools
MA-4 Remote Maintenance
MA-5 Maintenance Personnel
MA-6 Timely Maintenance
MP-1 Media Protection Policy and Procedures
MP-2 Media Access
MP-3 Media Labeling
MP-4 Media Storage
MP-5 Media Transport
MP-6 Media Sanitization
MP-7 Media Destruction and Disposal

PE-1 Physical and Environmental Protection Policy and Procedures
PE-2 Physical Access Authorizations
PE-3 Physical Access Control
PE-4 Access Control for Transmission Medium
PE-5 Access Control for Display Medium
PE-6 Monitoring Physical Access
PE-7 Visitor Control
PE-8 Access Logs
PE-9 Power Equipment and Power Cabling
PE-10 Emergency Shutoff
PE-11 Emergency Power
PE-12 Emergency Lighting
PE-13 Fire Protection
PE-14 Temperature and Humidity Controls
PE-15 Water Damage Protection
PE-16 Delivery and Removal
PE-17 Alternate Work Site
PS-1 Personnel Security Policy and Procedures
PS-2 Position Categorization
PS-3 Personnel Screening
PS-4 Personnel Termination
PS-5 Personnel Transfer
PS-6 Access Agreements
PS-7 Third-Party Personnel Security
PS-8 Personnel Sanctions
SI-1 System and Information Integrity Policy and Procedures
SI-2 Flaw Remediation
SI-3 Malicious Code Protection
SI-4 Intrusion Detection Tools and Techniques
SI-5 Security Alerts and Advisories
SI-6 Security Functionality Verification
SI-7 Software and Information Integrity
SI-8 Spam and Spyware Protection
SI-9 Information Input Restrictions
SI-10 Information Input Accuracy, Completeness, and Validity
SI-11 Error Handling
SI-12 Information Output Handling and Retention
Technical
AC-1 Access Control Policy and Procedures
AC-2 Account Management
AC-3 Access Enforcement
AC-4 Information Flow Enforcement
AC-5 Separation of Duties

AC-6 Least Privilege
AC-7 Unsuccessful Login Attempts
AC-8 System Use Notification
AC-9 Previous Logon Notification
AC-10 Concurrent Session Control
AC-11 Session Lock
AC-12 Session Termination
AC-13 Supervision and Review—Access Control
AC-14 Permitted Actions w/o Identification or Authentication
AC-15 Automated Marking Not SelecTED
AC-16 Automated Labeling
AC-17 Remote Access
AC-18 Wireless Access Restrictions
AC-19 Access Control for Portable and Mobile System
AC-20 Personally Owned Information Systems
AU-1 Audit and Accountability Policy and Procedures
AU-2 Auditable Events
AU-3 Content of Audit Records
AU-4 Audit Storage Capacity
AU-5 Audit Processing
AU-6 Audit Monitoring, Analysis, and Reporting
AU-7 Audit Reduction and Report Generation
AU-8 Time Stamps Not Selected
AU-9 Protection of Audit Information
AU-10 Non-repudiation
AU-11 Audit Retention
IA-1 Identification and Authentication Policy and Procedures
IA-2 User Identification and Authentication
IA-3 Device Identification and Authentication
IA-4 Identifier Management
IA-5 Authenticator Management
IA-6 Authenticator Feedback
IA-7 Cryptographic Module Authentication
SC-1 System and Communications Protection Policy Procedures
SC-2 Application Partitioning
SC-3 Security Function Isolation
SC-4 Information Remnants
SC-5 Denial of Service Protection
SC-6 Resource Priority
SC-7 Boundary Protection
SC-8 Transmission Integrity
SC-9 Transmission Confidentiality
SC-10 Network Disconnect

SC-11 Trusted Path
SC-12 Cryptographic Key Establishment and Management
SC-13 Use of Validated Cryptography
SC-14 Public Access Protections
SC-15 Collaborative Computing
SC-16 Transmission of Security Parameters
SC-17 Public Key Infrastructure Certificates
SC-18 Mobile Code
SC-19 Voice Over Internet Protocol

References

FISMA

This document references relevant FISMA documentation, especially standards published by NIST, which is the authority for FISMA security standards, applicable to all federal agencies for non-national security data and data systems.

- http://csrc.nist.gov/publications/nistpubs/index.html; listing of FIPS and SP publications
- FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004
- FIPS 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006
- SP 800-18, Guide for Developing Security Plans for Federal Information Systems, February 2006
- SP 800-30, Risk Management Guide for Information Technology Systems, July 2002
- SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems, May 2004
- SP 800-53, Recommended Security Controls for Federal Information Systems, December 2006
- SP 800-53A, Guide for Assessing the Security Controls in Federal Information Systems, April 2006
- SP 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories, June 2004
- SP 800-70, Security Configuration Checklists Program for IT Products, May 2005
- NIST National Vulnerability Database: http://nvd.nist.gov/statistics.cfm
- US-CERT Quarterly Trends and Analysis Report: Sept 1, 2006

Cisco

Additional information can be found online at the Cisco Website, with specific information about the solutions described in this document, as listed below:

- http://www.cisco.com, Cisco corporate Website listing all product information
- Cisco Security Manager: http://cisco.com/application/pdf/en/us/guest/products/ps6498/c1161/cdccont_0900aecd8062c063.pdf

- Cisco Configuration Assurance Solution: Cisco information presentation (CAS-FISMA.ppt, 03/02/2007)
- Cisco Network Compliance Manager: http://cisco.com/en/US/products/ps6923/index.html
- Cisco Network Compliance Manager: Cisco information presentation (FISMA_Whitepaper_NCM.pdf: 05/18/2007)
- Cisco Network Admission Control: http://cisco.com/en/US/netsol/ns466/networking_solutions_package.html
- Cisco Network Admission Control: http://www.cisco.com/cdc_content_elements/flash/nac/demo.htm
- Integrated Secure Wireless Managed Services: http://www.cisco.com/en/US/products/ps6814/products_ios_protocol_option_home.html
- Cisco Access Control Server: http://www.cisco.com/en/US/products/sw/secursw/ps2086/index.html
- Cisco Network Compliance Manager: http://cisco.com/en/US/products/ps6923/index.html
- Cisco NetFlow: http://cisco.com/en/US/tech/tk812/tsd_technology_support_protocol_home.html
- Cisco Monitoring Analysis and Response System: http://cisco.com/en/US/products/ps6241/index.html
- Cisco Intrusion Prevention System: http://cisco.com/en/US/products/sw/secursw/ps2113/index.html

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

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 C11-434964-00 10/07