

Prescription for Faster FISMA Compliance: Transitioning from a Patchwork Approach to an Integrated Approach to Information Security

When the Federal Information Security Management Act (FISMA) was introduced in 2002, federal agencies began complying in the best way available at the time: deploying different “point” solutions for each of the functional controls defined by the National Institute of Standards and Technology (NIST). While this approach did improve security, results have fallen short of expectations for many agencies. Federal IT groups today struggle to manage and audit a diverse collection of security products as a single system, a challenge that escalates with each new product added. Now Cisco® offers an integrated approach to network security that is more effective and helps federal agencies accelerate compliance with FISMA and other security regulations. In a Cisco Self-Defending Network, solution components work together and are managed as a cohesive system that is distributed across and embedded within the network infrastructure. The benefits: better security, less management overhead, and greatly simplified audit preparation.

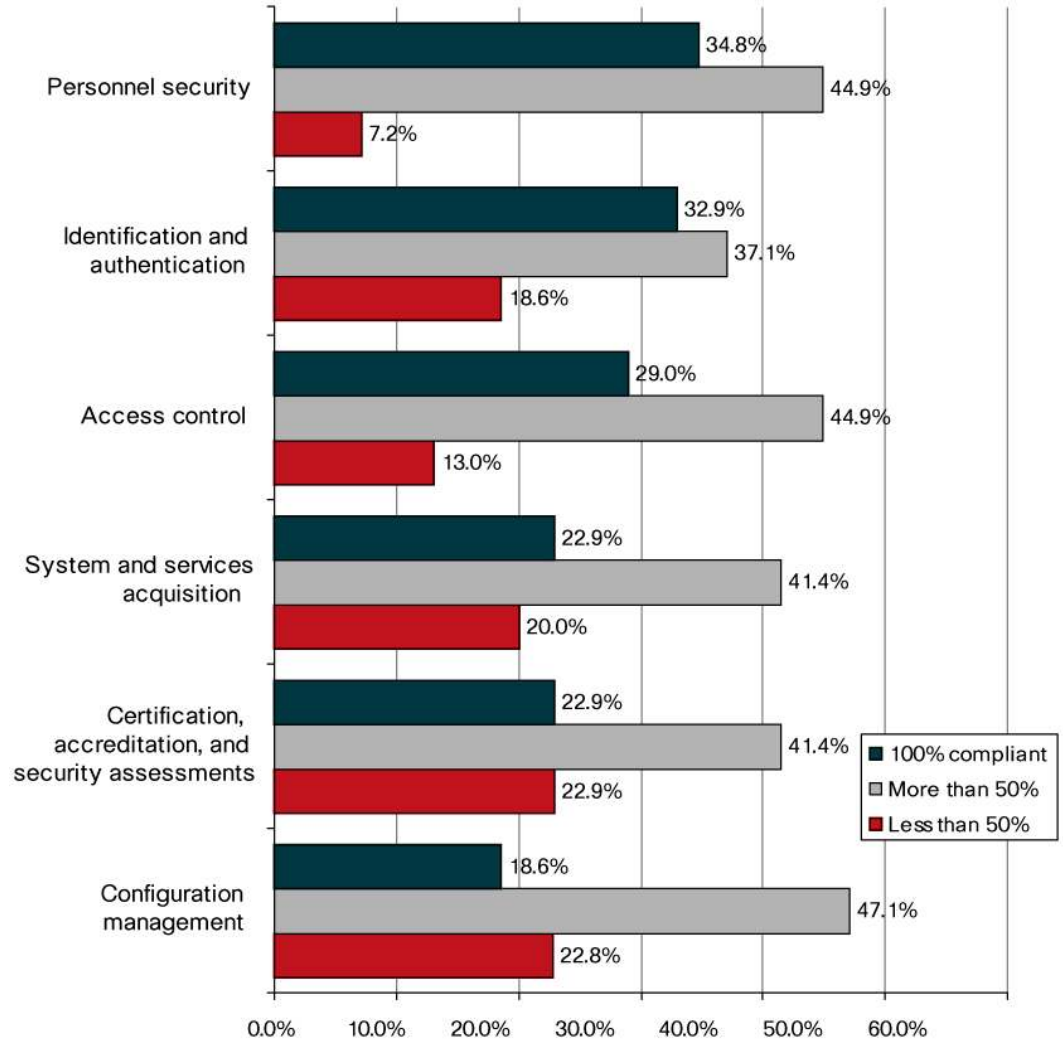
Executive Summary:

Why Adopt an Integrated Approach to Information Security?

As the role of the IP network in delivering agency services expands, so, too, does the importance of information security. Recognizing this, the government has introduced a spate of security regulations such as FISMA, Department of Defense (DoD) Directive 8500, and Homeland Security Presidential Directive 12 (HSPD-12). To comply, agencies are adopting specified security practices and undergoing regular audits to assess the effectiveness of their tactics.

Information security has improved since FISMA was introduced in 2002—but not as much as agencies might expect given the time and money they have invested. In a 2005 survey of federal agencies, no more than 35 percent of respondents said they would be fully compliant in any of the 17 areas of FISMA within 12 months; and nearly 25 percent said they would be less than 50 percent compliant in certification and configuration management (see Figure 1). In addition, the enormous effort required to manage security and prepare for annual security audits consumes IT resources that could otherwise be assigned to projects that further the agency’s mission objectives.

Figure 1. FISMA Compliance to Date: Help Wanted



An examination of existing approaches to network security suggests the following limitations:

- Inability of individual security systems to collaborate
- Lack of integration among security systems, which results in reactive rather than proactive threat management
- Management burden that increases with each new threat
- Expense of custom integration and maintenance,
- Time-consuming audit preparation

What can federal IT groups do to improve security and accelerate compliance with security regulations—without increasing the time and effort needed to manage security? One answer is to revise purchase criteria for security systems, emphasizing the product’s ability to integrate with other products for automated threat defense and unified management.

In fact, integrated security solutions are available to federal agencies today. The Cisco Self-Defending Network comprises security solutions designed to integrate with one another from the moment they are connected to the network, and without any integration efforts from IT. What’s more, the Self-Defending Network includes the tools to automate and simplify management and audits. By adopting network security solutions that are integrated by design, agencies ease the

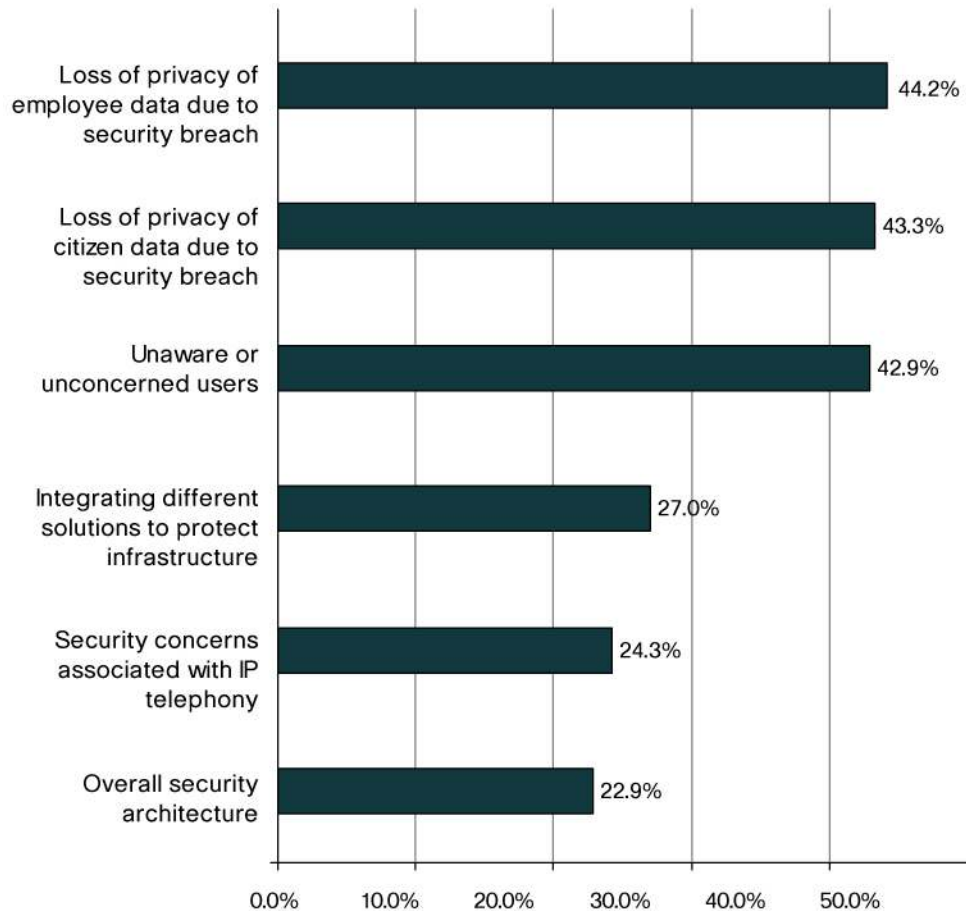
burden of securing their network and services, reduce deployment and management costs, and transform the ordeal of auditing into a more routine report-generation exercise.

The Essential Role of Information Security in Federal Government

Strong security engenders trust. To confidently share information and resources—a central premise in many government reforms—all parties need to trust that the people allowed to access the network and information resources are who they say they are. Agencies want assurance that people’s access is limited to the applications and data for which they are authorized. They need to know that the devices people use to access the network use are infection-free and protected according to the agency’s security policy. And they are reassured if threat defense is automated rather than manual.

Just as good security facilitates collaboration, its absence can do harm. Loss of privacy and citizen data due to security breaches ranked as the number-one concern in a 2005 survey by Market Connections, Inc. (see Figure 2). To protect Continuity of Operations (COOP), agencies need to control constant and increasingly sophisticated attacks, including viruses, worms, spyware, and denial-of-service (DoS).

Figure 2. What Keeps Federal Agency Managers Awake at Night



The importance of security is underscored by federal security regulations—and the attention paid to compliance audits. Regulations stipulate that agencies must identify and rank the importance of the systems they use and apply implement stringent monitoring and auditing measures for the most critical systems. The General Accounting Office consolidates annual reports from each agency's Inspector General into an overall annual report to Congress, which is publicly available. Good agency scores help bolster citizen trust in government.

Value of Information Security: Preventing the Bad, or Enabling the Good?

Information security traditionally has been viewed as a drain on IT resources—a costly but necessary effort to protect against disruption and loss. Agencies can build a more compelling business case for adequate security funding when they also regard security as an enabler for Connected Government and other strategic initiatives. A fundamental tenet of Connected Government is information sharing, which requires trust. Network security enables trust between agencies by providing authentication, authorization, and assurance of information integrity.

Current Approaches to Information Security: Are They Working?

Current approaches information security in federal government are succeeding to some degree. The evidence is that government operations have continued to function despite unremitting attacks. Moreover, several attackers have been successfully prosecuted, demonstrating that the affected agencies were able to produce documentation of inappropriate network activities.

However, problems remain. As of February 2006, many federal agencies had still not earned As and Bs on their FISMA report cards. Government networks still experience various degrees of damage and disruption, and the costs of maintaining network security continue to escalate. Now is a good time to re-examine current approaches to network security in federal government—and how they help or hinder compliance.

Point solutions

Today it is common practice for departments within agencies to purchase point products to address a specific security need. One vendor's product is selected for firewalling, another's for intrusion prevention, and so on. Purchase decisions are often based primarily on features and performance, even though another product will soon likely equal or surpass the one selected. Unfortunately, a product's ability to collaborate with other products and share the same management interface seldom factors in to the purchase decision.

It is sometimes argued that product diversity limits potential exposure to any single product's flaws. The corresponding disadvantage, however, is that the proliferation of products and vendors within an agency—and the resulting lack of centralized management—actually creates new vulnerabilities. The reason: maintaining and auditing point products as a cohesive security system requires continual, arduous integration efforts, draining IT resources in an undertaking that is ultimately doomed to be less than satisfactory. Table 1 summarizes the drawbacks of the fragmented approach to security.

Table 1. Consequences of Today's Fragmented Approach to Network Security

High Costs	Complex Management	Burdensome Analysis and Auditing
<ul style="list-style-type: none"> • Integration • Training • Spares • Maintenance 	<ul style="list-style-type: none"> • Complexity of distributing and managing consistent security policy across all platforms • Increased risk of configuration error • Poor system wide management view • Time-consuming integration testing during product upgrades • Lack of synchronization in feature upgrades across different products 	<ul style="list-style-type: none"> • Difficulty of analyzing security incidents, which requires correlating high volumes of log data from diverse security products • Complexity of reconciling multiple log and report formats • Lack of automated report generation for auditors
<p>Consequences for Federal Government</p>		
<ul style="list-style-type: none"> • Slow incident response: reactive rather than proactive. • Failure to recognize patterns that signal an attack. • More widespread damage before the threat is contained. • Hampered inter-agency collaboration. • Vulnerability to infection, attack, and information theft. 		

In summary, the lack of integration in today's security solutions forces IT departments to spend vast amounts of time and resources on integration, interoperability testing, system configuration, monitoring, and auditing, which detracts from strategic programs such as Enterprise Architecture and other E-gov initiatives.

Reactive threat management

Threat management at most agencies is primarily reactive—not proactive. New antivirus definitions and operating system patches do not become available until a threat has been identified, reported, and fixed. Agency infrastructure remains vulnerable between the time the exploit appears and the vendor distributes the patches and IT installs them. Given that today's new threats can become big problems in a seconds or minutes, agencies can no longer afford delays of hours or days.

Automated patch management improves threat management somewhat by enabling IT to more quickly distribute patches to thousands of PCs and network devices. However, automated patch management does not prevent infections from spreading to the network. Employees can still unknowingly connect infected or unprotected laptops or portable disk drives to the network, for example. What agencies need is proactive protection: solutions that can recognize and stop unwanted application or user behavior, such as installing unauthorized software or opening a suspect link in an instant message. Behavior-based protection works whether or not the threat's digital signature is known.

Today's security management is reactive, as well. Every network device and security system produces voluminous event logs every day, and vendors use different formats. Therefore, identifying security incidents in order to react to them can take hours or days—or even not happen at all. The connection between two separate events in different parts of the network can easily escape human detection, especially when the clues are buried among tens of thousands of harmless events that took place around the same time. Even with certain automated incident identification solutions, formulating a corrective response typically requires highly trained staff and manual execution.

Remedy: Integrated, Collaborative, and Adaptive Security

In an integrated security solution, all devices connected to the network—routers, switches, PCs, workstations, IP phones, wireless access points, and so on—behave as part of a larger collaborative system. Agencies that adopt an integrated approach to security relieve IT personnel of the burden of custom integration, testing, and auditing, freeing them to improve security policy and implementation of controls or to work on the agency's strategic programs.

Identifying characteristics of an integrated approach to network security include the following:

- Automatically adapts to new threats
- Controls access to network resources
- Provides integrated monitoring, analysis, and response in multivendor environments

Let's examine each of these characteristics.

Automatically adapts to new threats

“Anti-x” technology automatically identifies and stops network threats such as viruses, spyware, DoS, phishing, and others. One example of an effective anti-x defense is behavior-based spyware mitigation. Rather than looking for disallowed applications or signatures—which are not known when a threat first emerges—the tool detects and stops disallowed behaviors, such as collecting keystrokes. (Agencies can also prevent employees' accidental violations of security policy, such as adding unauthorized software, attaching portable drives on USB ports, and clicking unsafe links in e-mails and instant message chats.) Another form of anti-x defense mitigates DoS attacks, enabling government continuity of operations during and after the attack. Yet another is automatic signature-definition updates from security service providers such as Trend Micro, which provides protection against new or resurgent threats without manual intervention from agency IT groups.

Controls access to network resources

Whether network users work in the office, telework from home, or are mobile, comprehensive Network Admission Control (NAC) ensures that only authorized users can access network resources. When a user attempts to connect to the network, NAC validates the user's identity and also verifies that the end device complies with the agency's requirements for antivirus software, operating patches, and so on. Non-compliant devices are automatically directed to a remediation site where they can install the required software.

Provides integrated monitoring, analysis, and response in multivendor environments

Ideally, all solution components in an integrated security solution share a common log format. Realistically, however, most agencies have existing security systems from multiple vendors that use different log formats. Therefore, the most effective integrated security system provides a monitoring, analysis, and response system capable of correlating log data from all security systems.

To meet current and future security challenges, federal government needs security solutions that are integrated by design. Network security solutions that are engineered to work together provide more comprehensive and better coordinated defense, cost less to deploy and manage, enable faster response to threats, and simplify the audit process (Table 2).

Table 2. Advantages of an Integrated Security System

Improves Security	Simplifies Management	Facilitates Analysis and Auditing
<ul style="list-style-type: none"> • Ensures consistent application of security policy across all elements of the system. • Protects against known threats with signature recognition • Protects against unknown threats with by stopping anomalous user and application behavior. • Adapts rapidly and automatically to threats—faster than a human can—limiting exposure. • Combines the respective capabilities of multiple components of the system for greater protection than the individual elements could provide if they were not integrated. 	<ul style="list-style-type: none"> • Can be managed from a single interface, saving time, reducing the risk of configuration errors, and preventing the administrator from overlooking potential warning signs. • Enables segregation of duties: different groups, such as network operations or security operations, can have their own access, views, and privileges. 	<ul style="list-style-type: none"> • Enables real-time monitoring, analysis, and response to security incidents by automatically correlating of events, even if reported from multiple vendors' devices. • Facilitates automatic generation of standard and customized reports needed by network operations, security operations, and Inspector General audits.
Advantages for Federal Agencies		
<ul style="list-style-type: none"> • Enables rapid, adaptive response to new threats—much faster than humans can respond. • Monitors critical infrastructure automatically and continuously. • Simplifies preparation of reports to support FISMA audits. • Reduces IT resource and management burden. 		

Cisco Integrated Security Solutions for Federal Government

Cisco has long been recognized as a leading provider of individual security solutions for firewalling, virtual private network (VPN), intrusion-prevention system, DoS mitigation, and more. More recently, in the early part the decade, Cisco embarked on an ambitious research-and-development program to create a comprehensive, integrated security portfolio. The result of this effort, the Self-Defending Network, is transforming the approach to network security in the public as well as the private sector.

Just as important as the industry-leading security products in the Self-Defending Network is the fact that they are integrated from the moment they are connected. The integrated approach closes coverage gaps, eliminates configuration inconsistencies, and reduces operator errors that can create vulnerabilities. In addition, IT groups spend less time testing for interoperability and enjoy coordinated feature upgrades, well-documented release notes, faster upgrades, more responsive customer service because of single-vendor support, and technical assistance response when necessary.

Defining the Self-Defending Network

The Self-Defending Network is Cisco’s strategy to protect an organization’s business processes and network by preventing, identifying, and adapting to security threats. It has three defining characteristics:

Integrated—Every network element acts as a point of defense and works together with the other elements to provide a secure and adaptive system. Routers, switches, appliances, and endpoints incorporate adaptive security capabilities, including firewalling, VPN, trust and identity capabilities, and IPS.

Collaborative—All network components and security solutions work together and collaborate to provide new means of protection. Security becomes a system involving cooperation among endpoints, network elements, and policy enforcement. Network Admission Control (NAC) is an

example of this principle. Endpoints are admitted to the network based on their adherence to security policy, which is then enforced by network devices such as routers and switches.

Adaptive—The network adapts to new threats and attacks by recognizing anomalous application and traffic behavior and stopping it automatically. Security services and network devices are mutually aware of each other, increasing security effectiveness and enabling proactive response to new types of threats. Improved management tools, diagnostic tools, and technology react faster to threats than humans can, and have become a necessary element of defense postures in federal networks.

Agencies that deploy Self-Defending Networks gain the following advantages:

- Accelerated regulatory compliance—Cisco solutions are available for each of the FISMA technical controls developed by NIST.
- Centralized monitoring and management of multivendor environments—Cisco Security Monitoring, Analysis, and Response (MARS) software monitors all security systems in the network, avoiding months of multivendor integration work and extending the life of existing security investments. It recognizes attacks, identifies the source, and in some cases provides a list of remedial actions, which IT can implement with a single click. Other management software, the Cisco Configuration Assurance Solution, transforms the yearly Inspector General audit from a resource-draining ordeal for IT into a routine report-generation exercise.
- Simpler deployment, a result of thorough testing—Cisco performs extensive regression testing to ensure that all solution components work together. Interoperability among all network and security components accelerates deployment, shortens the agency's testing process after the solution is deployed, and reduces deployment costs.
- Comprehensive services—Securing government networks requires attention not only to technology, but also people and processes. The Cisco Advanced Services Group provides a comprehensive suite of services, including planning, preparing, designing, implementing, operating, and optimizing. In addition, Cisco has developed a large ecosystem of leading security partners, such as professional service providers, value-added resellers, systems integrators, and product vendors whose solutions are integrated with Cisco's solutions. Partners include IBM, ThruPoint, EDS, Raytheon, and GTSI. Agencies that want to free up IT staff for strategic projects have the option to outsource some or all of their security solution design, implementation, and ongoing operations.

In addition to offering the Self-Defending Network, Cisco demonstrates unique credentials in security and federal environments:

- Federal customers can count on Cisco to be there in years to come. Annual global sales of security solutions exceed US\$1.5 billion.
- Cisco employs more than 650 people dedicated to serving the federal government, including more than 50 Certified Information Security Systems Professionals and 25 engineers with security Cisco Certified Internetwork Expert (CCIE®) certifications.
- One Cisco group is dedicated to customizing Cisco commercial off-the-shelf (COTS) products to meet the unique IT requirements of the U.S. Government.
- More than 1500 Cisco engineers continually develop and refine security solutions to address new threats and incorporate new technologies and standards.

- Cisco outpaces the industry on investment in R&D, and in three years has spent more than US\$148 million acquiring companies with leading security technologies.
- Cisco has a broad range of security certifications, including more than 37 Federal Information Processing Standards (FIPS) certifications, 13 National Information Assurance Partnership (NIAP) certifications, and others in progress.
- Cisco is the first vendor to offer Common Criteria-Certified VoIP and Optical solutions.

Getting There

Reflect on the issues your agency faces in improving security and maintaining or improving FISMA compliance and we think you will agree: adopting an integrated approach makes sense. But how to get there? The first step is to contact Cisco, whose federal security team will help develop a plan to meet your agency's individual challenges. Your Cisco representative can arrange an executive-level consultation with one of Cisco's Internet Business Solution Group experts, a briefing on a Cisco Security Posture Assessment and lifecycle management from Cisco Advanced Services, or a discussion and briefing with a federal security product sales specialist. We can also help you find a Cisco certified security partner to meet your needs. Regardless of the approach you select, Cisco aims to create a long-term relationship as your strategic security partner.

For more information on Cisco solutions for federal government, visit:

<http://www.cisco.com/go/federal>.

For more information on Cisco integrated security solutions and the Cisco Self-Defending Network,

visit: <http://www.cisco.com/go/security>.



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.

©2007 Cisco Systems, Inc. All rights reserved. CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0701R)