

# Preparing Networks to Support the TIC Initiative

## Overview

In today's U.S. government organizations, CIOs are faced with numerous challenges beyond meeting their agency's mission, including data protection, operational efficiencies, regulatory compliance, and cost containment. The Trusted Internet Connection (TIC) initiative, mandated in November 2007 by the Office of Management and Budget (OMB), is one of many requirements that government agencies must meet. Cisco offers solutions to help agencies meet these very important requirements, and can assist in the planning and execution of a migration strategy to a TIC-compliant architecture.

Adoption of the TIC initiative will minimize the overall number of external data connections to the U.S. government including Internet access. This will be accomplished through sharing of resources (Internet portals), and creating new intranets to provide access to these Internet portals. This paper provides insight into the two main impacts of the TIC initiative on government agencies, shared Internet portals and WAN access strategies, and what agencies should consider when migrating to TIC compliance. The paper also suggests Cisco® solutions for secure, reliable network access and centralized monitoring capabilities. Cisco provides the highly available, intelligent infrastructure to help agencies comply with TIC requirements—while taking advantage of existing investments and readily available components.

## Introduction

### TIC Internet Gateway Consolidation

The objective of the TIC initiative is to tighten the U.S. government's network security by consolidating approximately 2758 (May 2008) external network connections down to less than 100 using highly secure gateways. The initial target was less than 50 external connections before the Department of Homeland Security (DHS) and OMB had an opportunity to review agency responses. The initiative will also improve the government's incident response capability through the establishment of centralized gateway monitoring at a select group of TIC Access Providers (TICAPs) using the DHS Einstein program.

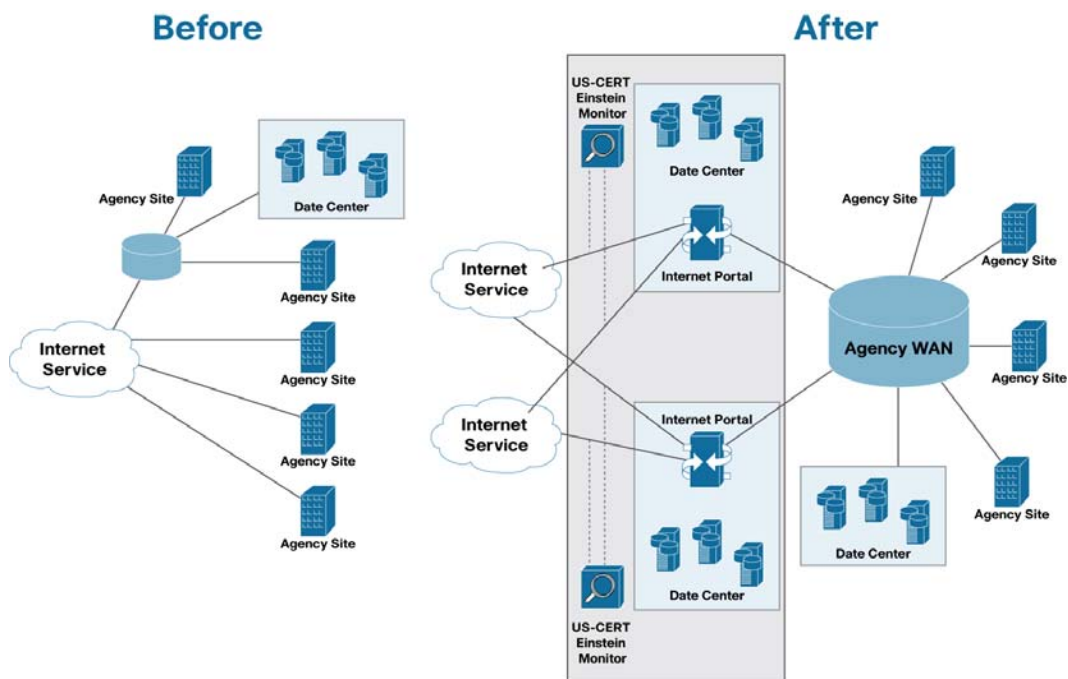
Departments and agencies were given an opportunity to select their preferred type of TICAP: Single-Service Provider, Multiservice Provider, or Seeking Service. Agencies were required to submit a statement of capabilities to GSA/DHS with their response by April 2008. In June 2008 US-CERT/ISS LOB issued the "Trusted Internet Connection Initiative Statement of Capability Evaluation Report" outlining the results of agency's TICAP preference. The report found that two agencies were selected as multiservice providers, 16 as single-service providers, and 121 seeking service.

As agencies consolidate and/or remove their Internet connections, two dramatic results emerge. First, the consolidation will require new Internet portal architectures that meet all security and communication needs including support for multiple agencies and scalability to support the new traffic levels. As the Department of Defense discovered, consolidating Internet gateways required reworking the NIPRNet to support the load as Internet connections were shut down. Second, the new traffic flows will require, at a minimum, agencies to review/renew their routing architecture, and

will likely lead agencies to create an agency TIC backbone for access to these portals.

This paper will focus on TIC portal architecture and the interconnecting WAN infrastructure that agencies utilize for accessing the portals. Figure 1 demonstrates in generic terms the existing agency Internet connectivity and the new method required for TIC compliance.

**Figure 1.** Before and After View of the Impact of TIC on a Generic Agency

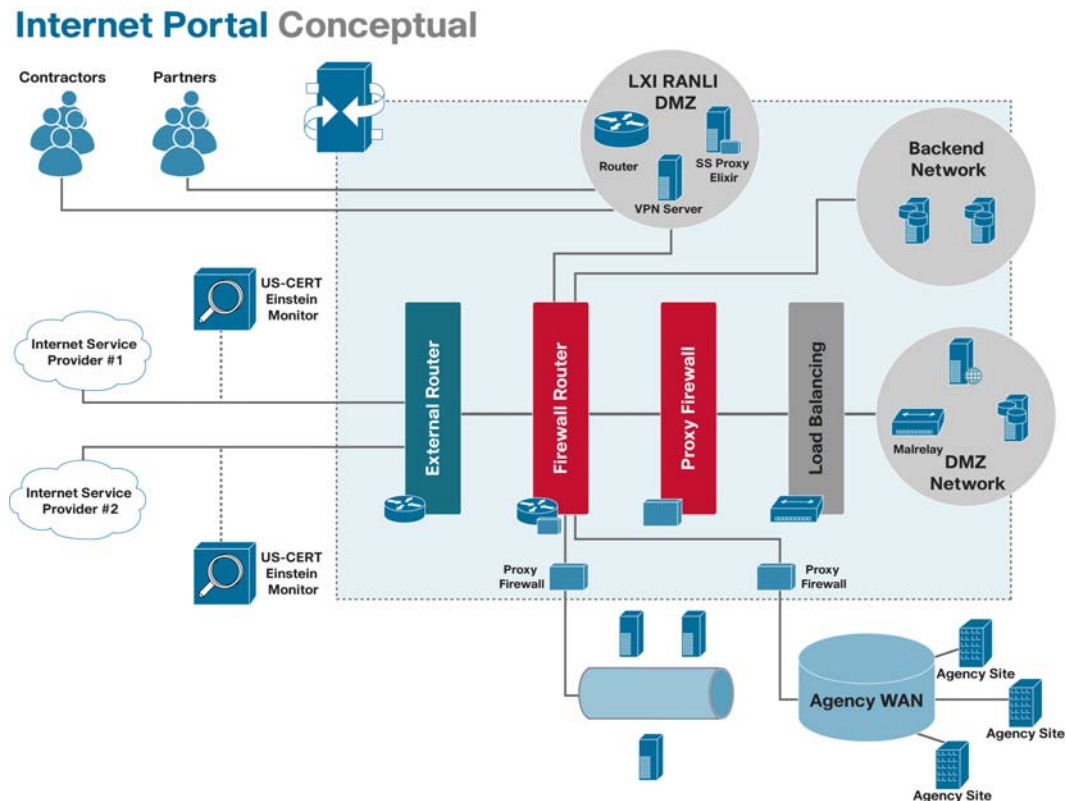


### Internet Portal Security Architecture

As network consolidation and modernization efforts continue to challenge the U.S. government, the TIC initiative provides direction for how the government can reduce its exposure to cyber threats while increasing situational awareness. The goal of reducing the number of portals within departments has been underway for some time. The use of a portal is a technological means to provide a common framework for access to the U.S. government, regardless of the systems (legacy or modernized) that may be accessed via the portal.

Portals can be defined in many ways. They control access to resources and data based on the rights of the user. Within a portal functionality is integrated into an architecture that meets requirements and provides the utmost protection of the data that is accessed via the portal. Using a purpose-built TIC architecture, objectives including security, management, connecting like and unlike systems, and bridging of distant functions are further supported. Figure 2 depicts common functionality found in a portal.

Figure 2. Conceptual Diagram of Internet Portal Connection



- **Internet connection:** The Internet connection is an exposure point for most agencies. It provides connectivity for external users (friend and foe) to access the agencies Internet portal and for internal users to access the Internet.
- **Internet access router:** The first and outermost point of control and contention for access to the portal is the router Internet transport terminates on. As a critical component to the overall system, the Internet access router serves as the first line of defense for an agency.
- **Web portal:** A web portal provides the functions to authenticate and identify its users and provides them with a personalized web interface for accessing information and services. These services can include the presentation of static and dynamic information, rendering of customized content, and real-time e-commerce transactions over encrypted sessions. Traditionally, web portals provided external users (such as customers and suppliers) access to an organization's resources, but they have since evolved to grant employees and contractors access to resources that are typically provided to those connected via intranet or remote VPN connections.
- **Extranet for B2B partners:** An extranet can be defined as a private intranet mapped onto the Internet or some other transport system separated from general public access. These connections are typically approved and accredited connections with a pre-existing security policy based on the mission that the business partner supports within the agency or department. The communications channel is secure and offers the ability to exchange data in a private manner. A demilitarized zone (DMZ) is typically used to stage information for use between organizations while also protecting the actual repositories of information on the intranet.
- **Remote access gateway:** Remote access module aims to extend the full class of enterprise

services to remote offices and teleworkers. Applications such as email, corporate extranet access, video and voice services, and online e-learning classes should all be available to users via the remote access solutions. Extending the office environment to alternative work locations allows for continuity of operations (COOP) during a multitude of unplanned events, and provides the flexibility to work from anywhere and at anytime.

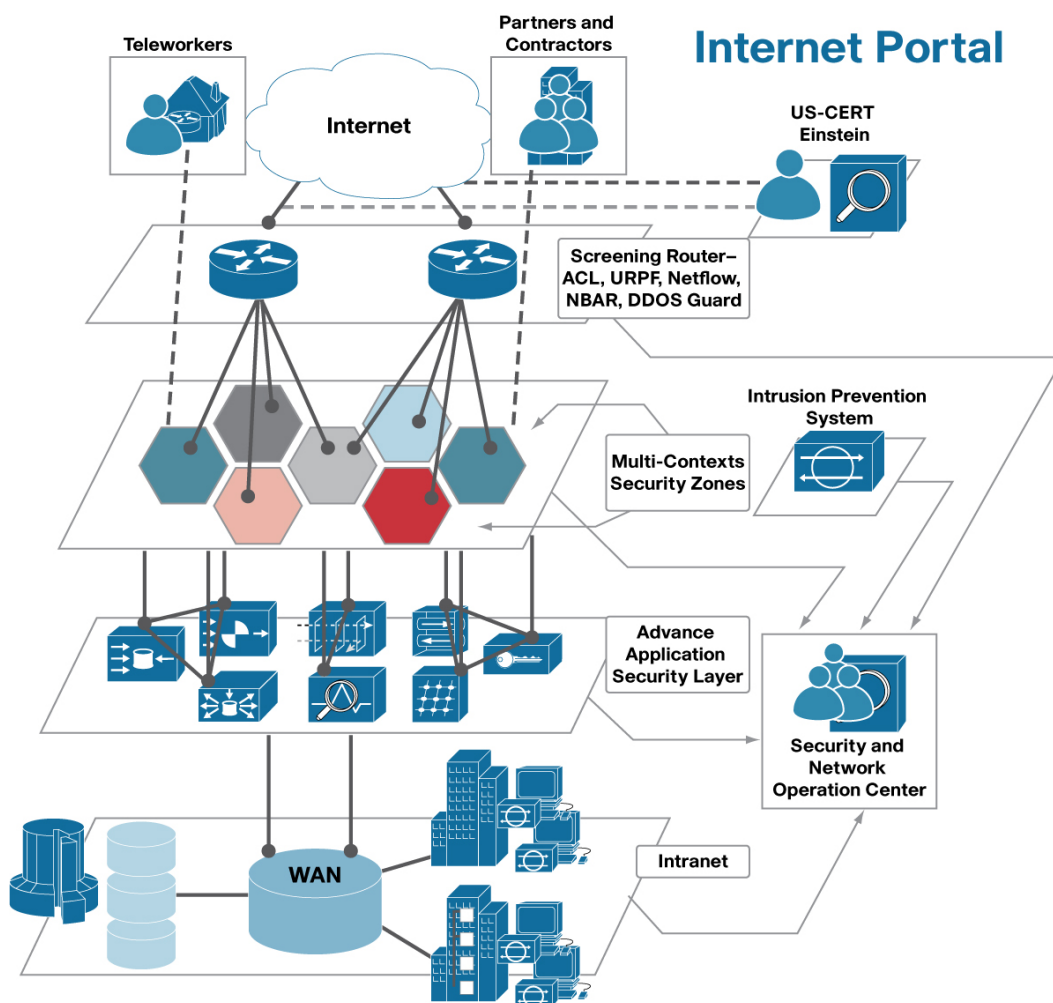
- **Application awareness:** The portal architecture should provide application-layer protocol translation capabilities. The purpose of this functionality is to further secure application requests and to translate the application protocols allowing access to the data in whatever format it resides within its legacy or existing schema/database.
- **US-CERT Einstein Monitoring:** As mandated by the OMB, TIC Internet portals allow for monitoring by the US-CERT Einstein program. Einstein does not eliminate the need for intrusion detection and prevention systems; rather, the 24-hour monitoring program aims to provide incidental information collection and situational awareness tools for government agencies. This macro-view provides US-CERT the ability to detect threatening attacks with greater accuracy and visibility to the overall scope of attacks.

### **Internet Portal Overview**

The security and protection of agency data (including employee information) is of the utmost concern for U.S. government agencies. A shared infrastructure model provides scaling and cost efficiencies by using high-performance hardware. However, to provide a high level of security, individual security policies are still required. Virtualization (multiple security policies or contexts supported on the same hardware) makes this possible. There are too many variables to accommodate multiple agencies or communities of interest with a single security policy. Security policies must be very granular and tailored to specific agency traffic characteristics in order to provide adequate security.

Consolidating many Internet connections and portals into a single portal will require network flexibility and agility. This is especially true when Internet portals will support other agencies, sub-agencies, and various communities of interest. Network components must be able to act in a coordinated fashion to protect assets.

Figure 3. Internet Portal



Depicted in Figure 3, the Internet portal solution provides defense in layers by decoupling the Internet portal into sub-components, each with discrete security capabilities and components. Grouping the similar attributes or requirements into their own security zones reduces the overall exposure to threats as fewer protocols are open for Internet scrutiny.

At the top layer Internet access routers provide connectivity to and from the Internet. In addition, they serve as a first layer of perimeter defense. In that capacity, they provide the preliminary screening of traffic in and out of the Internet portal by filtering out certain data and denying address-spoofing traffic. These routers can provide the first-level alert system, using NetFlow information, which baselines traffic patterns and detects traffic anomalies when they occur.

The next layer of the model contains the security zones where dissimilar security policies are separated into respective zones, and where those policies can be enforced. Traffic associated with communities of interest is sent to specific zones. Component virtualization provides the basis for having zones of varying policies and configurations, integrated in a single system. Each zone could be enabled to allow different policies based on needs and requirements of that community of interest. By utilizing the virtualization capabilities, a security administrator can segment logical networks into multiple zones, with a single physical infrastructure.

In this model, each zone supports its own security policy, interfaces, routing tables, firewall,

intrusion prevention, and deep packet inspection system. Multi-tier service-level agreements can be created by allocating and guaranteeing hardware resources for each zone. A true benefit of this architecture is the ability to deploy, create, and modify policy-based services quickly to meet critical demands.

Today's advanced viruses and Trojan horses require measures beyond the protection offered by firewalls and IPS devices alone. To address this need for security inside the perimeter, a third layer of defense is introduced where advanced application-level security appliances are coupled with security zones to increase the effectiveness of security measures. Following are some specific examples that demonstrate this point:

- To secure email, appliances such as the Cisco's IronPort® email security system can be used in conjunction with antivirus gateways to reduce spam, viruses, spyware, and phishing attacks directed at an email security zone.
- By coupling Cisco's Network Admission Control service and IPsec VPN concentrators with the B2B connections, agencies can enforce security posture policies such as OS version, hotfix level, and anti-virus signature updates, and can ensure the integrity and confidentiality of the connections.
- To secure the web portal where critical protection is needed at the service perimeter between un-trusted and trusted zones, a Cisco ACE XML Gateway with the integrated XML firewall should be used. An XML gateway provides a comprehensive XML threat defense system where it protects against identity, content-based, personnel, response-compliance, message-transport, and XML denial-of-service (DoS) attacks. In addition, it integrates easily with existing infrastructure such as directories, Stateful Switchover (SSO), Public Key Infrastructure (PKI), and network system management.

A multilayer security design integrates many layers of technology into a single security operations center. System monitoring must provide operators real-time analysis of individual device health and behaviors. A comprehensive monitoring system, such as Cisco Security Monitoring, Analysis, and Response System (MARS), can provide a situational awareness of the Internet portal by gathering data from these device information logs, IDS/IPS, and firewalls as well as traffic flows from routers. This awareness is critical in making decisions during an attack or service outage. Many outages are caused by human error rather than divisive attacks. Therefore, the monitoring system should provide access to audit-compliance capabilities along with fallback tools in the event of misconfiguration.

To summarize, the TIC and the Internet portal requirements will advance changes in security policies for all government agencies. For some agencies, making minor modifications to their existing practices will be enough to meet the TIC mandate, while others may need to revamp a major portion of their security policies and practices to become compliant. A defense-in-depth strategy based on a combination of secure connectivity, threat defense, and a trust and identity management system should be used to mitigate virus outbreaks, prevent unauthorized network access, and circumvent DoS attacks. This strategy provides safeguards needed to maximize network uptime and minimize threat impact.

## **WAN Consolidation—Challenges for Network Managers**

While the benefits of a TIC-compliant government are obvious, this initiative will require certain network modifications for both large and small agencies. In order for the OMB to meet its stated objective, many agencies will need to either consolidate or remove their Internet connections. As described earlier, departments or agencies will either need to be an Internet portal provider for their department, be an Internet portal provider for other departments or agencies, or they must utilize Internet portals from other providers. Removing external connections will impact most agency WANs, which will be required to accommodate new traffic flows or new connectivity.

Depending on an agency's existing infrastructure, WAN modifications can be as simple as adding new routes to the edge routers, or the more extreme case of creating a completely new access WAN to the new Internet portals. The following sections describe the modifications needed to facilitate TIC compliance.

### **Departments or Agencies with Many Internet Access Points**

In many departments, agencies, and sub-agencies, basic Internet connectivity consolidation will occur with the creation of two main Internet portals at the department level. All other Internet connections within the department including sub-agencies will be removed. In this scenario, either an existing department backbone will support access to the Internet portals or a new Intranet will be created to facilitate traffic flow. This approach was taken by the Department of Defense, which consolidated its Internet connectivity to 17 Internet POPs using the NIPRNet as the WAN backbone to provide intranet traffic between agencies and access to the Internet.

To facilitate a smooth transition to TIC compliance, departments will need to assess current traffic patterns and model new traffic patterns caused by the removal of the Internet connections. At the Internet portals, high-speed routers will be required to handle the consolidated Internet traffic. An intranet backbone will be needed to facilitate intra-agency communication and provide onramps for sub-agencies and remote agency sites to the Internet. In many cases, existing sub-agency networks can remain the same with current WAN implementation and security strategies. However, these new systems will need to be reviewed to ensure security policy integrity and minimize performance impact. Many agencies either utilize or are in the process of migrating to an IP MPLS network. This will help facilitate any changes that are required to an agency's WAN.

### **Departments or Agencies Using the Internet to Transport Intra-Agency Traffic**

Many smaller agencies utilize the Internet as a cost-effective IP transport for backhauling traffic to their department-level resources. Some small sites and branches also use that same Internet connection for Internet access. For these agencies, TIC compliance means using Internet portal services from either a different department acting as a multiservice TICAP, or a commercial service provider with the authority to become a TICAP.

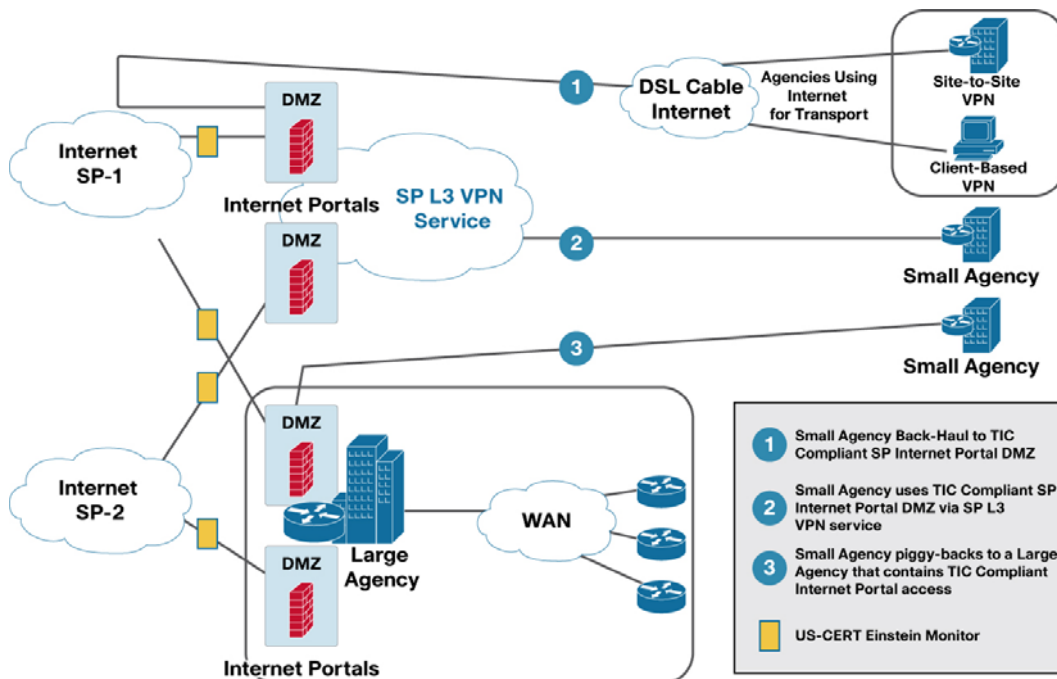
In this model, intra-agency communication can be supported via the Internet with FIPS 140-2 approved encrypted IPsec VPN between sites. However, since the TIC will no longer permit "split tunneling," all agency Internet-bound traffic must traverse an Internet portal before leaving agency network boundaries. An alternative is to create an overall agency backbone (such as an IP MPLS WAN) and then the Internet is accessed via an Internet portal. In either scenario, the impact on these agencies includes the creation of one or two hubs which will connect all agency sites together in support of an agency backbone. These two hub sites are then used as connection points for this smaller agency to the TICAP. Various options for doing this are shown in Figure 4.

Traffic patterns will likely be substantially different in this new design, so agencies must perform

due diligence before and during the migration process. Security solutions will need to be evaluated and possibly rebuilt to support this dramatically different model.

Figure 4 highlights several options for small agencies that require TIC-compliant Internet access, but lack the operational and financial capabilities to own and manage a TIC-compliant Internet portal.

**Figure 4.** Options for TIC-Compliant Internet Access



## Conclusion

As U.S. government agencies plan their migration toward compliance with the OMB mandate to consolidate Internet connections and reduce exposure to cyber threats, two architectural challenges must be addressed. First the consolidation or elimination of these connections will require a new, scalable Internet portal architecture that meets all security and communication needs for multiple agencies. Second, the new traffic patterns will require agencies to optimize their routing architecture, and likely compel agencies to create a TIC backbone for access to these portals. Cisco has comprehensive, cost-effective solutions meeting the requirements for agencies of all sizes.

Cisco has proven, deployed solutions available to address these architectural challenges. U.S. government agencies can receive support from Cisco in the planning, testing, and deployment of a TIC-compliant architecture. Investing more than US\$5 billion annually in research and development, Cisco is prepared to bring networking and collaboration to new heights and provide the best support possible in serving the U.S. government.



**Americas Headquarters**  
Cisco Systems, Inc.  
San Jose, CA

**Asia Pacific Headquarters**  
Cisco Systems (USA) Pte. Ltd.  
Singapore

**Europe Headquarters**  
Cisco Systems International BV  
Amsterdam, The Netherlands

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](http://www.cisco.com/go/offices).

CCDE, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo 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. (0812R)