White Paper

Cisco Clean Access Improves Security for Education Networks

SUMMARY

Educational institutions face difficult challenges related to the protection of their information networks. The severity and frequency of worms and viruses have increased at the same time that dependence on the network for delivery of critical teaching tools and services has increased. These problems are exacerbated by three characteristics unique to these institutions and their networks:

- **Spiking**. Educational networks, especially those on campuses with residential halls, experience a surge of new users at the start of each semester. During times of worm and virus activity, helpdesks are often overwhelmed by the number of infected computers.
- **Values**. The underlying philosophy of educational institutions is often one of openness and shared learning. Imposing network controls similar to those used by corporations is inconsistent with these core values.
- **Diverse users**. Unlike corporate networks, which exist mainly to support employees, educational networks support a large array of constituents: students, faculty, administrators, visiting scholars, guests and community users, conference attendees, to name a few. Managing these diverse groups with their diverse needs represents a significant challenge.

Cisco Systems® has developed Cisco® Clean Access, a network admissions control (NAC) product that automatically detects, isolates, and cleans infected or vulnerable devices that attempt to access the network. With Cisco Clean Access, administrators can define security policies as broadly or narrowly as they like as they apply to a defined group of users. Cisco Clean Access aims to balance the unique network-related challenges educational institutions face with a robust, effective policy enforcement mechanism that dramatically reduces threats to the network.

Challenges

The emergence of the Blaster worm in late 2003 wreaked havoc among educational networks. Many incoming students imported the worm with their computers, most of which logged onto the school network within a short amount of time. Networks were severely disabled, some completely non-operative, for several weeks. Often, administrators repaired the network only to have it become infected again with the Blaster worm a short time later.

In response, schools instituted various programs to try to mitigate further network infection:

1. Require network users to install antivirus software, critical operating system updates from Microsoft, and other well-known remedies.

For years, institutions distributed CD-ROMs with all the appropriate files to network users. Following the Blaster worm, many schools established “responsible computing” guidelines that made the installation of these files mandatory, but they were difficult to enforce.

2. Register student computers and require authentication.

Requiring authentication on education networks was a significant departure from both the open-access culture of the Internet and of the institutions. But the benefits of knowing who and what was on the network seemed to justify the requirement. That said, registration and authentication merely establish the presence of a user and his or her computer – it does not determine whether the computer meets the security policies of the network.

3. Use of intrusion detection, intrusion protection, and monitoring solutions to identify infected computers

These monitoring solutions are effective for identifying infected computers, but they do little to alleviate the helpdesk burden. Rather, schools needed a two-fold solution: one that could find infected computers prior to allowing trusted network access and could also push the remediation effort back onto the user.

Solution Overview

Creating a more effective solution requires the installation of a network intelligent enough to protect itself from vulnerable and infected devices. An intelligent network would make network access contingent on complying with a defined set of security policies. Five components are required:

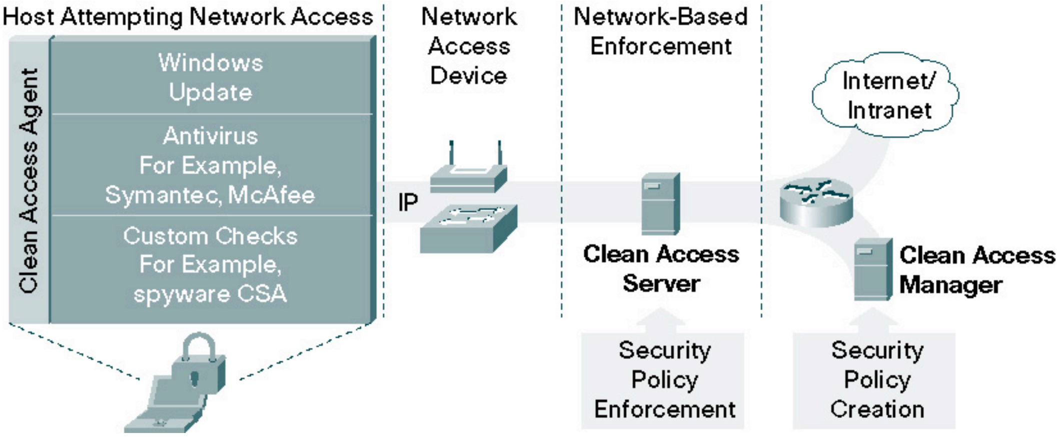
- **Recognize who (what type of user) and what (the device type) is connecting to the network**. As a foundation for controlling access to a network, each user should be authenticated, even if it is a "null" authentication for guest access. While most organizations already employ authentication systems for the use of applications, authentication should also be required in order to tailor network service privileges to the users' privileges. A reasonable network protection strategy should take full advantage of these existing systems.
- **Evaluate all systems that connect**. Two methods of interrogation – a network probe and a device scan – are the minimum requirements for robust network protection. A network probe looks at a computer's networking components with packets, then gauges the responses to expose software vulnerabilities or actual malicious code. The device scan, which is more powerful, thoroughly examines a device: its file system, configuration databases such as the Windows registry, and system memory. Both methods should be tailored to the profile of the user, determined by the user's relationship with the organization (for example, student, guest, faculty) and by the degree of threat the user poses to the network.
- **Quarantine noncompliant systems**. During the interrogation process, the user's network traffic should be quarantined away from other devices, yet given access to networked resources to facilitate remediation. Supplementary quarantining methods, such as by protocol, throughput, and session time, have the added benefit of ensuring that network bandwidth is not dominated solely by the scanning process.
- **Repair noncompliant systems without threatening the network**. Recognizing and quarantining vulnerable and threatening devices alone merely shifts the burden of repair onto the support organization. As a result, a usable solution would also have a scalable method of remediating the deficiencies on the user machine.
- **Simplify management**. Network administrators should be able to control the process of admitting users, dynamically responding to user behavior, and meeting the network's need. Management concerns may include the ability to monitor a user's session for information on the username, IP address, MAC address, and login time; terminate a user's session; and research a user's past admission to the network.

Many systems in the market, such as domain controllers, can authorize users to specific file shares but lack the crucial integration with network infrastructure to restrain user traffic or affect the security postures of un-managed users. Firewalls can authenticate and authorize a user, but lack the ability to interrogate and dynamically quarantine non-compliant users. Still others, such as patch management solutions, can interrogate and remediate, but are unable to authorize a user to different levels of access based upon policy compliance.

Cisco Clean Access Overview

Cisco Clean Access is a packaged solution that combines roles-based authentication, vulnerability assessment, policy enforcement, and distributed remediation into a single, easily deployed, NAC system. The Cisco Clean Access solution (Figure 1) is comprised of a Clean Access Manager (CAM), which can manage several Clean Access servers (CAS). There is also an optional agent, known as the Clean Access Agent (CAA).

Figure 1
Overview of the Clean Access Solution


Host Attempting Network Access
Clean Access Agent
Windows Update
Antivirus For Example, Symantec, McAfee
Custom Checks For Example, spyware CSA
Network Access Device
IP
Network-Based Enforcement
Clean Access Server
Internet/ Intranet
Clean Access Manager
Security Policy Enforcement
Security Policy Creation

Authentication Integration

Cisco CAM serves as an authentication proxy; that is, when users log on either through a captive Web portal login or using the CAM, the CAM acts as the authentication client requesting service from an authentication database. This architecture has many advantages:

- Because CAM becomes the authentication client (for example, a RADIUS or Lightweight Directory Access Protocol [LDAP] client), there is no need to replicate or synchronize authentication data. As a result, authentication setup requires less than a minute to configure.
- The trust relationship between network devices is greatly simplified. Once the authentication database trusts the CAM, its facility can be securely pushed to the other devices on the network under the protection of secure socket layers (SSLs). In addition, since the CAM does not house data, the scalability of the system relies on dedicated databases, further simplifying security.
- The architecture is flexible: since the CAM is simply an authentication client for the initial user's logon, multiple authentication instances can be used by the CAM so that decentralized organizations can unify their NAC system.

Currently, Clean Access supports RADIUS, LDAP (Active Directory), Kerberos, and Windows NT, as well as a local password database, a transparent Windows logon, an 802.1x passthrough, a null "guest" authentication, and a simple e-mail address query.

Roles-Based Access

The CAM can differentiate role assignment based on either the user's 802.1q virtual LAN (VLAN) tag or by recognizing a user's group identity as manifested by a RADIUS or LDAP attribute. In either scenario, the role assignment is transparent to users: they need only select the correct authentication type with the proper username and password. For example, members of a student group can be placed into a role with policies customized to meet their privileges, while the faculty group role has a different set of privileges upon network admission. Universities can establish separate roles for faculty, administrators, and students, resulting in differing levels of interrogation and authorization privileges.

Roles govern the policies that apply to each user group. These policies can specify, among other things:

- Traffic-filtering rules
- Bandwidth usage limits
- The length of a user session
- Interrogation types

The ability to coordinate user identity to network policy requirements and privileges is one of the most compelling features of the Cisco Clean Access solution.

Dynamic Authorization and Quarantine

An important feature of the CAS is its ability to dynamically change traffic policies as configured to correspond to a user's authentication status. The Clean Access Server operates as a role-based access firewall that can be deployed as a gateway or as a transparent device, such as a bridge. It can also reside out of the user's data path in some deployments.

The CAS regards each client as an IP and MAC pair so that traffic cannot subvert policies through IP spoofing. As the user authenticates (by way of a captive Web portal login or an agent), passes through interrogation, remediation, and quarantine to a fully authorized state, the traffic filtering policies that correspond to each user change dynamically as directed by the Clean Access Manager.

As an example of dynamic authorization, a successful network admission process would enable a member of a specific group (for example, faculty) to use specific protocols such as HTTP, HTTPS, Internet Message Access Protocol (IMAP), Post Office Protocol (POP), Simple Mail Transfer Protocol (SMTP), and Domain Name Service (DNS); have access to the file servers within the life sciences department; and use the Internet with unlimited bandwidth and for an unlimited time. An unsuccessful network admission process would result in that user being placed in a quarantine role that would likely limit his or her use of network protocols and access to resources other than necessary to the remediation of the specified vulnerabilities and threats.

Interrogation

Interrogation – or evaluation – of the threat posed by incoming devices is one of the core values of the Clean Access solution. Interrogation examines the security posture of a computer seeking admission onto the network; in particular, for the presence of:

- Scanning worms and other malicious code
- Software vulnerabilities
- Installed, running, and updated antivirus software

- Patching software or updated OS patches
- Specified configurations, such as requiring the Clean Access Agent or the Cisco Security Agent

Users experience the interrogation process through the following steps:

Step 1: A user accesses a captive portal Web login by opening a Web browser. The browser makes an HTTP GET request following a successful DNS resolution. If the CAA is used, it is launched to request a login – no browser is required.

Step 2: Under the Web access scenario, upon recognizing this HTTP GET, the CAS returns the user an HTTP 302 REDIRECT to its trusted IP address, where the user can enter his username, password, and optionally, his authentication server choice. Under the agent scenario, the user enters a username and password to authenticate.

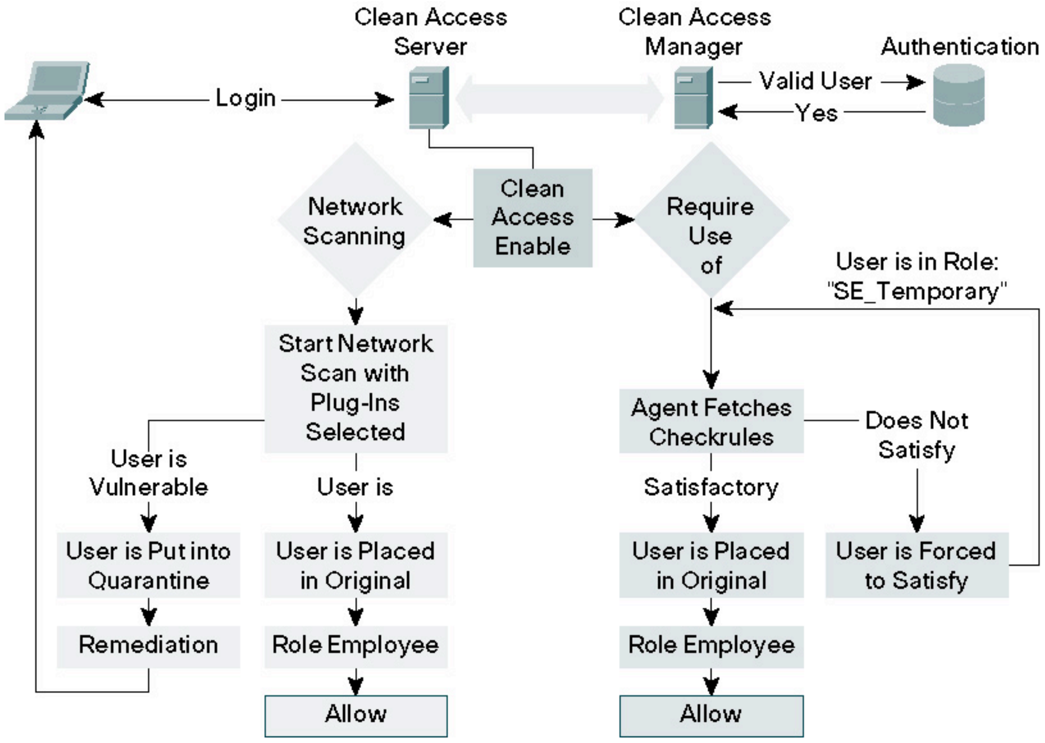
Step 3: The user device is then challenged and interrogated using two methods (Figure 2):

Network probe. These probes detect software vulnerabilities or backdoors left by scanning worms and viruses. This interrogation technique works well for environments where the use of an agent is not accepted culturally and it does provide a great deal of efficacy. However, the depth and versatility of scanning is not equal to those systems using the CAS.

Agent-based interrogation. If the system has employed the CAS, the agent then examines a System Registry, File System, and Service and Application running in memory to determine compliance with security policies based on user role and/or device OS. The Agent can incorporate the network probe, although this may be viewed as redundant.

Figure 2

Diagram Illustrating the Two Interrogation Processes: Network Probing and Agent-Based Interrogation



The CAS is designed to overcome two common problems:

- Instead of attempting to intercept system calls or stand in the network stack, the CAA is a read-only agent that can assess the posture of the device without having any direct effect upon the stability of the system
- Instead of the agent acting on interrogation results, the CAA simply communicates the posture of the device to the Clean Access Server and Manager.

These two characteristics have helped eliminate conflicts between the agent and virtual private network (VPN) software or personal firewalls.

To simplify the task of determining appropriate system registry, file system, and service and application attributes, especially as they map to multiple operating systems and multiple loads of software, the Cisco Clean Access solution periodically downloads the configuration settings from a repository at Cisco Systems. Once configured, these updates take effect automatically.

Immediately upon deployment, Clean Access can automatically check for the latest critical Windows and antivirus updates from leading vendors. This unique capability results in deployments that take as little time as half a day.

Remediation

Simply identifying and stopping vulnerable machines from entering the network does little to improve productivity; one network attack could result in hundreds or thousands of infected computers that, even if quarantined, still require one-on-one, labor-intensive repair. As such, Cisco Clean Access includes remediation assistance for both Web-based logins and CAA logins.

Web-Based Logins

The remediation process for a Web-based login begins when a device is found to be vulnerable or threatening during the interrogation process. Those devices are automatically placed into a quarantine role, where a Web page alerts them, describes the vulnerability, and links to instructions and software resources. In this manner, the user can repair his or her own device without requiring the assistance of support staff.

This Web interface is customizable for the purposes of branding, including an acceptable use policy, or any other information the network administration would like to convey.

CAA Logins

When the user accesses the network through the CAA, the agent acts as a “wizard,” leading the user through a step-by-step process to remediate vulnerabilities one at a time. The CAA interface can also provide file pull-downs from the Clean Access Manager, customized instructions, and Web-link redirections so that the remediation process is convenient and takes advantage of preexisting infrastructure.

For example, a university may choose to distribute a large service pack as a file pull-down to reduce bandwidth demands while redirecting users to the Windows Update Website for larger numbers of smaller files. Or, the university may simply present instructions to the user through the CAA regarding the enablement of Windows automatic updates, then redirect users to a local Website for the download, installation, and update of antivirus software. A college or university may use a similar strategy to update guest devices, especially given the convenience of the Windows Update site, while relying on patching software for enterprise devices.

In short, the scalability of remediating users to a compliant posture for network admission stems from the ability to rely on the user’s own system resources to bring it into compliance.

Deployment

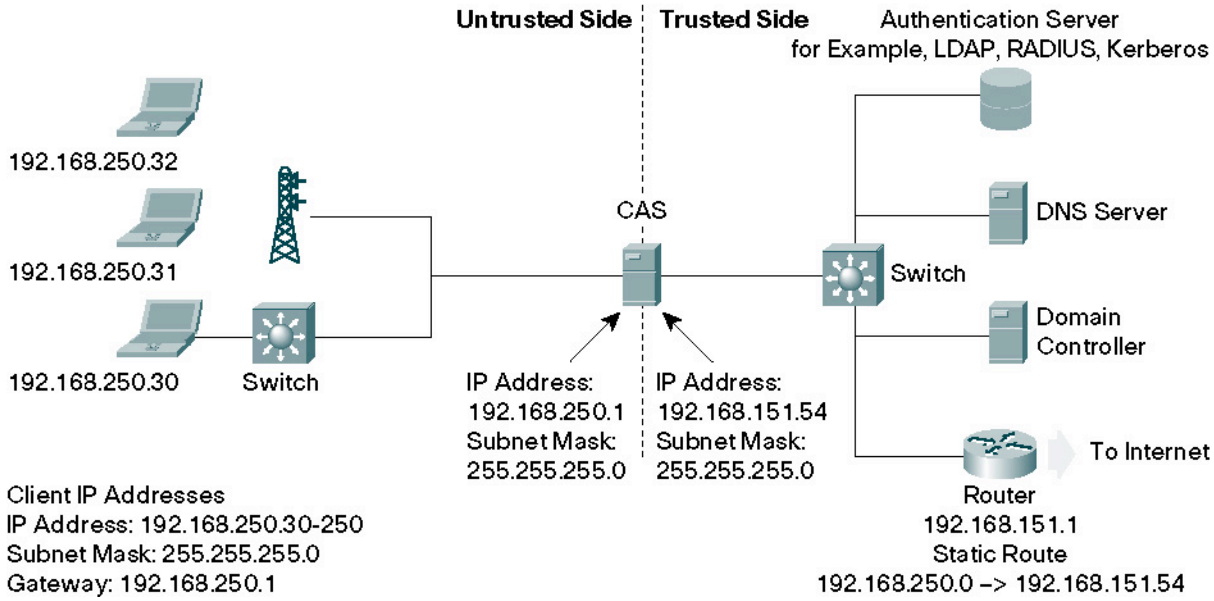
Cisco Clean Access can be deployed in-band for greater control and granularity over user traffic or out-of-band for greater throughput and flexibility. In an in-band deployment, the CAS sits in the routing path while the CAM would likely reside in a network operations center (NOC) with other management utilities. The CAM would require only a path to the authentication servers and each individual CAS on the network. In an out-of-band deployment the user traffic is in-band only for the evaluation and remediation functions; at other times, traffic traverses the switch.

In-Band Gateway Deployment

The simplest deployment involves using the CAS as the user's gateway where multiple networks can be managed by terminating their 802.1q VLAN trunk on the untrusted side of the CAS (Figure 3). This usually allows for easy deployment in most networks that have a multilayer switch-block that terminates at the core.

Figure 3

Cisco Clean Access in a Real IP Gateway Deployment



During deployment, when both the trusted and untrusted ports of the CAS are connected to a core router, networks can be easily moved over the CAS one at a time by removing routing capability from the VLAN and transferring the gateway IP address to the untrusted physical interface of the CAS with the appropriate routing changes in addition.

When the CAS is deployed as a gateway, it can become either a Dynamic Host Configuration Protocol (DHCP) relay or a DHCP server. When the CAS is configured as a DHCP server, it can be used to automatically generate and allocate thousands of small subnets to users entering the network so that a virtual point-to-multipoint topology is created from the perspective of the users' operating systems. For example, if the administrator chose to generate 30-bit subnets, it would appear to the user's operating system that they were the only device in their network so that scanning traffic would have to traverse the CAS where it could be filtered, thus containing an outbreak.

The advantages of deploying the CAS as a gateway include:

- The ability of the CAS to act as gateway for protected subnets
- The ability to provide a trusted interface in which the CAS is designated as static route for untrusted subnets
- The ability of the CAS to perform DHCP services, or act as a DHCP relay

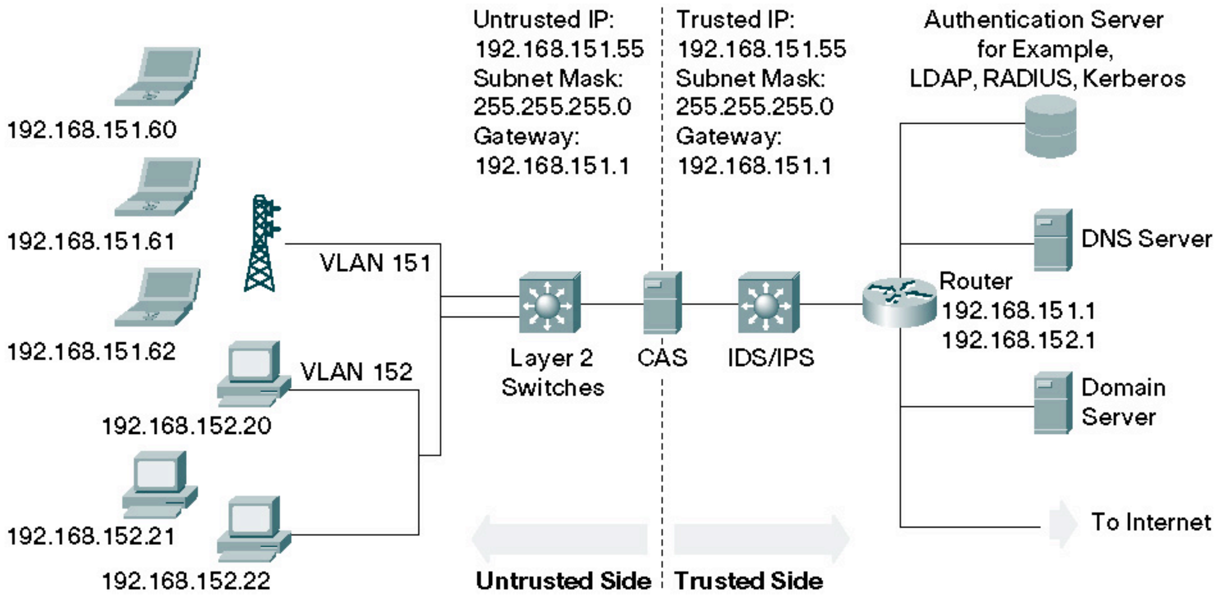
The advantages of being deployed as a virtual gateway include:

- The ability to function well in a star topology network where there is centralized routing
- Ideal for situations in which protected subnets are in the process of being designed
- Requires no physical network changes, only configuration changes

In-Band Bridge Deployment

The CAS can also be deployed in a transparent, or bridging, mode. In this deployment, it can sit on the physical link between two switches. Or, with the appropriate VLAN tagging applied to the ingress and egress traffic on each side of the CAS, this bridging can be accomplished in the same physical topology as with the CAS adjacent to the core switch. The CAS can also employ an optional DHCP strategy as a counter-measure to the spreading of scanning worms. In the transparent mode deployment of the CAS, as would be expected, DHCP broadcasts are forwarded transparently.

Figure 4
Cisco Clean Access in a Virtual Gateway Deployment



The advantages of deploying the CAS as a bridge include:

- Small footprint
- Elimination of the need to define static routes on main router or alter gateways
- Serves as an idea configuration in cases where the network topology is such that there already exists a single point of VLAN aggregation

Monitoring and Management

The CAM gives administrators significant control over the monitoring and management of the system. The administrator has a real-time capability to:

- Track user information by IP address, MAC address, or login time
- Terminate users' sessions individually, or by groups
- Manually or periodically remove users from the list of certified devices-and require recertification-to ensure the currency of policy compliance

System logs allow for fast and easy searching of events to simplify forensic work, while Clean Access reports provide a quick status of the interrogation of the network devices to highlight successes and failures. All management of the Clean Access system is handled through a task-oriented Web interface, which eliminates the need for administrators to learn additional command line interfaces.

Summary

As more and more security threats come from within the network through user systems, the necessity of enforcing security policies as a condition of network access escalates. While various point products-patch management systems, internal firewalls, endpoint security-address certain aspects of this problem, Cisco Clean Access represents a holistic approach by relying on identity management, obtained through authentication; user roles and groups; network functions, such as redirection and quarantine; and an intuitive remediation system to provide network security.

For More Information

For more information about the Cisco Clean Access solution, visit http://www.cisco.com/go/cca, send questions to cca-questions@external.cisco.com, or contact your local account representative.

CISCO SYSTEMS

Corporate 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: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
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

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on **the Cisco Website at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica Croatia • Cyprus • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe