How Cisco IT Uses Intrusion Prevention to Protect User Endpoint Devices

Cisco Security Agent behavior-based protection adds essential layer of security to Windows desktops.

Cisco IT Case Study / Security and VPN / Endpoint Intrusion Prevention: This case study describes Cisco IT's internal deployment of the Cisco Security Agent to Windows desktop systems across the Cisco global network, a leading-edge enterprise environment that is one of the largest and most complex in the world. Cisco customers can draw on Cisco IT's real-world experience to help support similar enterprise needs.

"Security is no longer a 'network only' proposition. Rather, data must also be protected where it resides—the endpoint."
– Paul Mauvais, Cisco Senior Security Architect

CHALLENGE

The steep cost of viruses and worms, which includes both remediation and loss of productivity, is a powerful incentive for prevention. The number of virus attempts is increasing exponentially1. By one estimate, the global cost of viruses and worms in 2003 was US$28 billion and is expected to grow to $75 billion by 2007.

Cisco Systems® uses a multipronged approach to protect its network from various types of attacks, including use of Cisco® PIX® security appliances, Cisco Network-Based Intrusion Detection System, and antivirus software residing on desktops and e-mail gateways. None of these methods alone, however, is completely effective for protecting individual assets like PCs and handheld devices at the desktop level. Consider that firewalls that protect the Cisco network cannot prevent a sales engineer's laptop from becoming infected when plugged into a partner's or a customer's network. Nor can they prevent the spread of infection when a Cisco employee's laptop becomes infected at home and then is reconnected to the corporate intranet. "Security is no longer a 'network only' proposition," says Paul Mauvais, Cisco senior security architect. "Rather, data must also be protected where it resides—the endpoint." At different times, an endpoint such as a laptop might reside inside the Cisco network, at a customer site, or in an employee's home.

Antivirus software also has limitations for protecting individual PCs and servers. Although antivirus software is effective in warding off viruses with known signatures, it does not protect the desktop between the time the virus is introduced and when a new virus definitions file with the new signature is installed—by which time the harm is done. "Updating the signature definitions is a daily effort and not really a winnable game because you never can get ahead," says Mike Swartz, Cisco technical project manager. "Instead, it's a reactive process in which you're continually applying updates." Another limitation of antivirus software is that Cisco employees often move their laptops on and off the network, making it impossible to ensure that all computers are protected with the same virus definitions file at the same time.

The same problem applies to patches that vendors release for newly discovered operating system and application vulnerabilities. "Ideally, every patch that a vendor releases would undergo full quality assurance testing and a 'burn-in' period on a set of development servers before it ever touched our production server environment," says Mauvais. "But because of the escalating pace of both vulnerabilities and vendor fixes, the support staff needs to balance two

[1] CERT Coordination Center (CERT/CC), http://www.cert.org/stats/cert_stats.html

needs. One is to test this patch in development to make sure it won't crash or impede the production environment, and the other is to distribute the patch quickly so it will resolve the security vulnerability before it's exploited and requires time-consuming remediation."

Patching also poses logistical problems for the mobile and global Cisco workforce. Cisco employees who work for days or weeks at a customer site during an outbreak might not receive a patch during the critical period. "If Cisco sends out a patch at 1:00 p.m. Pacific time, that's the middle of the night somewhere else, so those employees won't receive it until the next day, when their network might already be infected," says Swartz. "Viruses and worms can infect much more quickly than we can patch."

To stop new attacks that attempt malicious activity, Cisco IT resolved to shift from a signature-based to a behavior-based solution. Policies allow normal application behaviors while preventing abnormal, potentially "bad" behaviors, such as when a downloaded file opens an e-mail address book.

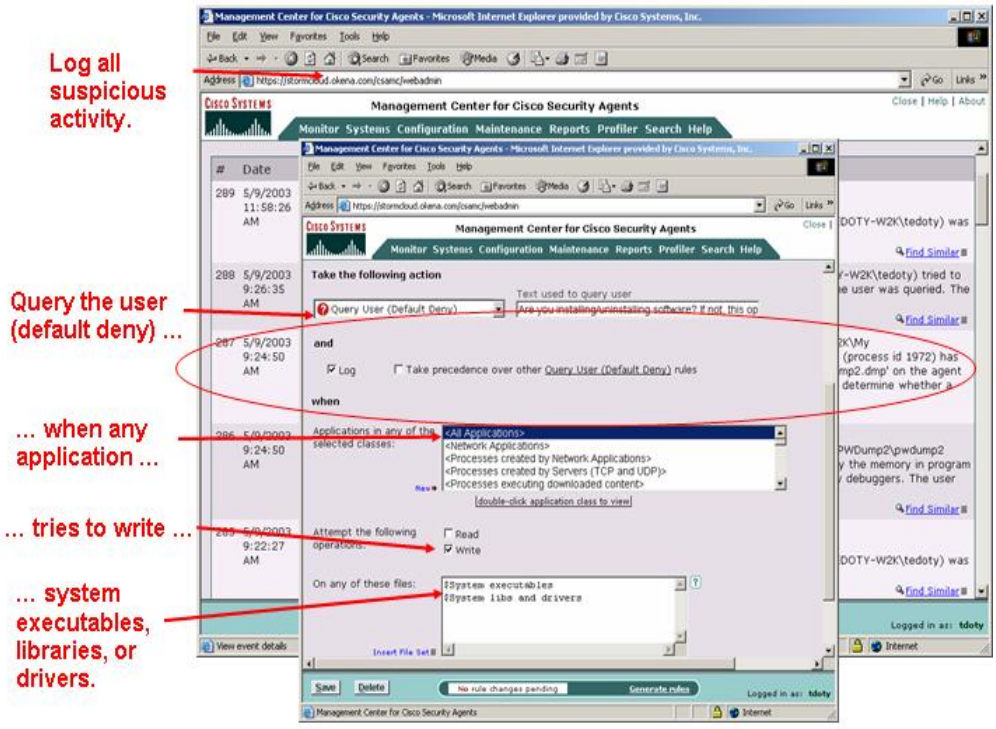
SOLUTION

Acknowledging the increasing damage that viruses and worms can inflict and the high cost of remediation, Cisco decided to implement an intrusion prevention solution on its employees' computers. Intrusion prevention systems provide all the features of a personal firewall plus more. A personal firewall allows or denies actions based on rudimentary rules, usually based on source or destination network addresses. Swartz explains, "For instance, if the personal firewall allows my computer to receive data from only one source, an e-mail server, my computer is safe from malicious intrusion because everything else is explicitly denied. But the limitation of a personal firewall is that malicious code can gain entry through a trusted source—for example, when it's attached to an e-mail. That's where the intrusion prevention solution comes in. If the e-mail application behaves in a way that's outside the norm, the solution gives the user or central administrator the option to deny that behavior."

The chief criterion for the intrusion prevention system for Cisco IT is maximum protection; but ease of use for employees is also a major requirement. "Most products we evaluated had a significant learning curve not only for IT but also for employees," says Mauvais. "We wanted a solution that was inconspicuous to employees so they wouldn't have a motivation to somehow disable the solution." Other key requirements were the scalability to support a user base of more than 50,000 users and centralized management for configuration and updates.

Based on these criteria, Cisco deployed the Cisco Security Agent, which provides built-in policies as well as the option to develop custom policies. For example, Windows system processes normally access Active Directory servers for authentication, but applications that are downloaded from the network typically should not access the user's address book. Built-in policies recognize bad behavior across a diverse set of applications and operating system versions. Administrators can customize policies to fine-tune the security posture for their own environment and applications. An advantage of Cisco Security Agent for Cisco IT is the relatively small set of rules to maintain. The few rules sets define when and how applications are allowed to access files, networks, and system registrations (see Figure 1).

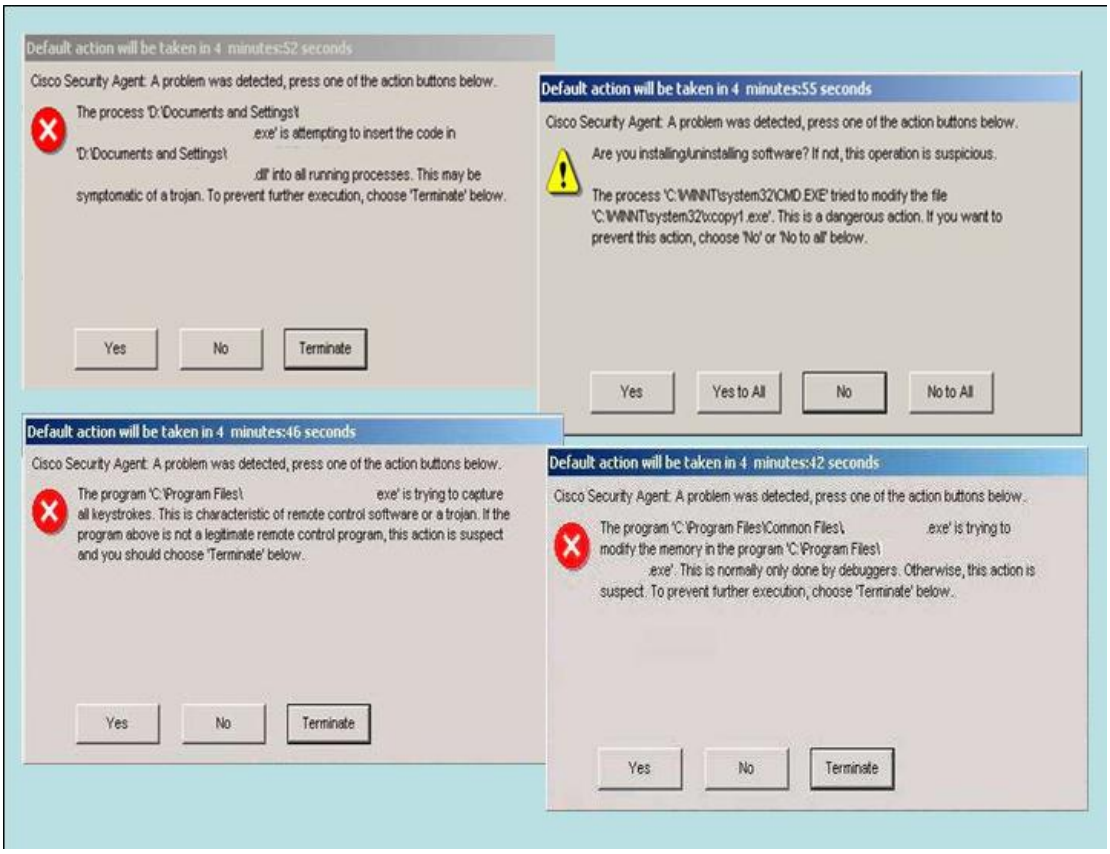
Figure 1. Sample File Access Control Policy



Cisco Security Agent blocks any action that violates rules and stores a log of violation attempts. The rule shown in Figure 1 states that Cisco Security Agent will query the user when an application tries to write a particular set of files. The system administrator can change the rules for a particular set of hosts.

For each type of deviation from expected application behavior, Cisco IT can configure Cisco Security Agent to allow the action, deny it outright without informing the user, or ask the user (see Figure 2). “Say a downloaded file is opening the user’s e-mail address book, which is a typical behavior for a virus,” says Swartz. “We might configure Cisco Security Agent to ask if the user wants to allow that action. As the default, we select the safer answer—no, in this case. The default is selected after a time-out period so that if employees aren’t at their computers when the action occurs, it’s automatically stopped.”

Figure 2. Cisco Security Agent User Dialog Boxes



Pilot

Before deploying Cisco Security Agent companywide, Cisco IT ran a 500-user pilot, the objective of which was to develop policies that did not impede productivity by asking too many questions about allowing application behaviors. Policy development was a vital prerequisite for success, given the diverse application environment at Cisco. “We were aware of about 1000 applications in use at Cisco, but during the course of the pilot we discovered that employees actually use closer to ten thousand,” says Mauvais. “The Cisco Security Agent event logs helped us to not only identify standard IT-distributed applications and their use, but also to identify commonly-used applications in other global theaters. We used this information to fine-tune the policies so that these applications ran smoothly in the final rollout.”

To plan and manage the pilot, Cisco IT assembled a project management team with representatives from the Personal Computing Solutions organization that handles PC support, engineering, information security (InfoSec), and the helpdesk support team of the Global Technical Resource Center. To recruit employees, IT posted a description of the project on the Cisco intranet and then selected 500 volunteers with a variety of job functions in different countries, including the United States, Canada, Europe, India, Australia, and Japan. Volunteers who agreed to provide specific types of information at predefined intervals were accepted into the pilot and instructed to download the Cisco Security Agent software from an internal Webpage for the pilot.

Next, IT set up a Windows 2000 server at Cisco headquarters San Jose, California, installed the Cisco Security Agent management software, and began developing policies. “For many applications, we selected the built-in policies in Cisco Security Agent,” says Swartz. To develop custom policies—either because a built-in policy was not provided or the built-in policy would be too intrusive to accommodate Cisco employees’ creative work styles—Cisco IT used the Profiler component of Cisco Security Agent, which creates a profile for normal application behavior. Pilot participants

were asked to run the application through its usual paces over the course of a day. Based on the sample, Cisco IT developed “allowed” actions and denied all others. “The profiling capability was very useful because Cisco uses a few complex applications that wouldn’t necessarily have built-in policies, such as Altiris, which we use for automatic desktop software deployment,” says Mauvais. “We thought we might have to profile all the thousands of applications in use at Cisco, but ultimately we only needed to profile four or five of the more complex applications. This was sufficient as a ‘starting point’ that we could refine after testing and analysis within the pilot environment.”

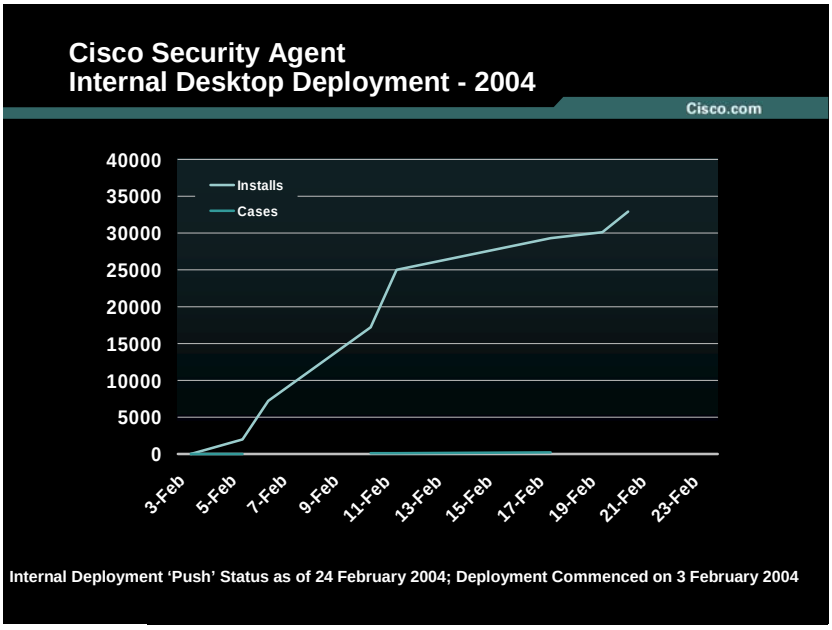
At the outset of the pilot, Cisco IT configured Cisco Security Agent in “test mode” so that it sent all messages directly to a management console rather than users’ desktops. The reason was to protect employees’ productivity. “Using test mode gave us the opportunity to see which messages cropped up often so we could decide whether we wanted to allow those behaviors without asking the user to confirm,” says Swartz.

The pilot took place from August 2003 to December 2003. “During the pilot we continually fine-tuned our policies,” says Mauvais. “The big surprise was that certain applications we had assumed were running a certain way had poor coding, which triggered popup alert messages. We resolved the problem by working with the vendors to develop workarounds.” While refining its policies, Cisco IT also fine-tuned its global support processes for Cisco Security Agent in the same manner that it does for other software, by defining criteria for escalation, internal service-level agreements, the mechanism used to distribute the software, and communications policies with users. “The four-month pilot with 500 users gave us the confidence that the initial policies would not impede employees’ productivity or overwhelm our support organization,” says Swartz.

Production

After the pilot, Cisco IT deployed five production servers for Cisco Security Agent..Cisco pushed the software to all employees worldwide as it does ordinarily, with Altiris, over the Cisco Application Content and Networking System (ACNS) distribution network (see figure 3).

Figure 3. Internal deployment of Cisco Security Agent



“In some cases we intentionally went with our own ruleset that to avoid impeding productivity or giving our employees a reason to uninstall,” says Mauvais. “We felt comfortable that we could quickly increase the security posture of the desktops if needed because we set the ‘poll time,’ which tells the agents how often to check for new policy or rule changes, to ten minutes,” says Mauvais. The strategy worked: “With our current policy, each user sees

an average of two or three events per day," says Swartz. "User acceptance has been good. With over 37,000 current users, only a couple of hundred of cases are open."

Education

To educate users on the value of the software and what to expect from it, Cisco IT published a series of articles in different internal publications, including the web information on the Cisco intranet, the IT newsletter, and various e-mail aliases within Cisco. Mauvais notes that active virtual communities are a very effective way to make people aware. "We're also in the process of compiling a layperson's guide to desktop computer security issues and how Cisco Security Agent relates to this for our user community," says Andrew Grant, lead engineer and security and stability lead with the Cisco IT Core Solutions Engineering department. "This will educate our less technical users on the proper use of the tools available to them to protect their desktop systems."

RESULTS

Cisco has deployed the Cisco Security Agent application to 37,000 desktops, with minimal impact on productivity and very low case volume. The solution proved its worth just two months after deployment, during the bagle.aa virus outbreak in late April 2004. "During the bagle.aa outbreak, our email virus protection was not updated for a short while," says Grant. "We deployed the virus updates as soon as we could, but we knew that they had been released too late to adequately cover the desktops. The first lines of defense were the e-mail servers, and the relevant teams were only minutes late in applying the correct filters. To add insult to injury, the virus had been sent from everyone in the company to everyone in the company. So we sat and watched the mail servers melt a little and braced ourselves as this was Cisco Security Agent's first real challenge."

Grant was pleased by the results. Of the 38,370 desktops running Cisco Security Agent, only 0.14 percent (about 50) became infected—and those only because the users clicked Yes twice when warned that a suspicious application was trying to write to the run key of their registry and trying to access e-mail resources. "Cisco Security Agent increased protection by a potential factor of 99.86 percent and an actual factor of 91.3 percent," says Grant. For a discussion of the difference between potential and actual, see "Lessons Learned" later in this document.

In addition, Cisco Security Agent has provided the following benefits:

- Cost savings—Cisco IT expects the solution to pay for itself quickly and many times over. "We compared the cost of the software to how much it would have cost us to clean up after viruses and worms," says Mauvais. "The return on investment business case was very clear." Cisco also expects to see a saving in overtime and downtime related to emergency patches for newly discovered vulnerabilities; these software patches are being released with increasing frequency "If we can roll out the patches, virus updates, and related security fixes to the production infrastructure on a weekly, monthly, or even quarterly basis, we'll save a lot of time and effort," says Mauvais. "When people are in a hurry, they miss things and accidents happen. In contrast, if they're given the time to follow proper systems management techniques and schedule updates rather than rush to deploy, we experience fewer applications issues, less downtime from installation mistakes, and less loss of revenue." Loss of revenue includes internal charges from users not having their desktops for a period of time or a server being down and unable to serve customers when they need it.
- Increased productivity—Cisco Security Agent has slowed the progress of recent viruses, even with the very liberal policies that Cisco IT chose for the deployment. When an action is denied, a message is sent to the central servers, which produce reports on demand as requested by IT. With early notification of new abnormal activity, Cisco IT can take early preventive action, minimizing the cost of infection.
- Detection of infected systems—"This was a surprise benefit of Cisco Security Agent," says Mauvais. "A few desktops were not protected with antivirus, either because the software had never been installed or had been deinstalled by the user. These users complained that their systems were running slower with Cisco Security Agent. We discovered the reason—infection—which caused Cisco Security Agent to detect many suspect

application behaviors."

- Confidence—"We have confidence that when the next malicious code or virus outbreak occurs, we will have a very robust layer of defenses in place," says Grant. "If the next bug gets past our e-mail gateway filters and our virus scanning software, we know that Cisco Security Agent is there on each desktop waiting to prevent it from spreading any further, as it did during the bagle.aa incident.

LESSONS LEARNED

"Take your time with policy testing and assemble the broadest variety of people and applications, because Cisco Security Agent concerns itself with the interactions among applications on a desktop," says Mauvais. "Be willing to start with a policy that's a bit weaker than what you eventually want, to help ensure user acceptance."

Mauvais also emphasizes that user education is critical to success. "Do what it takes to educate users thoroughly. There will be some application behaviors that you neither allow nor explicitly deny, but rather ask the user to decide. If they make uneducated choices, infections can still occur." Swartz concurs: "The impact of introducing Cisco Security Agent is comparable to that of introducing VPNs or wireless networking. The behavior-based architecture significantly alters the desktop and server paradigm. Therefore, it's worth it to spend as much time and effort as you can to educate users."

The critical importance of user education was clear during the bagle.aa virus outbreak in April 2004. Of 38,370 systems protected by Cisco Security Agent, only 620 users launched the executable file. "Of those, less than ten percent, 54 people, clicked Yes when Cisco Security Agent warned them that a suspicious application was trying to write to the run key of their registry, and some of these users clicked Yes again when warned that the application was trying to access e-mail resources," says Grant. "This taught us to never underestimate the need to educate users about IT security." Users should never open e-mail attachments that they are not expecting. If they do find themselves opening attachments, users should be made aware of the consequences of ignoring Cisco Security Agent warnings of suspicious activity when they are opening suspect attachments. Even a single compromised machine can spread a flood of infected e-mail throughout the corporation, resulting in lost work time and more time and money lost in cleaning up afterwards. Cisco plans to add increasing intelligence to Cisco Security Agent to mitigate threats without requiring user intervention. Still, reducing the number of infected machines by a factor of 90 percent was a significant win for Cisco IT and its deployment of Cisco Security Agent.

The bagle.aa incident also reinforced for Cisco IT the concept that the damage caused by an outbreak happens within the first few hours and tapers off dramatically afterwards. Grant notes that it is critical to limit the number of infected PCs as soon as possible, to reduce the time, cost, and effort of cleaning up after a virus attack. Achieving this requires multiple layers of protection, including mail server filters and desktop antivirus software. "Two days after the initial infection, I checked the mail servers," says Grant. "Only one or two more infections had occurred. I was pleasantly surprised because I expected a steady rate of infection for a few days as each theatre and time zone woke up. This didn't happen, which I attribute in large part to the effectiveness of Cisco Security Agent."

NEXT STEPS

Now that Cisco IT has deployed the Cisco Security Agent software and established processes for desktop support, help desk, and InfoSec, it plans to make the revising and improving the software policies. "As we continue to fine-tune our policies, we expect that Cisco Security Agent will be even more effective for us in stopping viruses or worms from spreading," says Mauvais. For further protection, Cisco IT intends to use Network Admission Control to allow network access only to those employees who have installed Cisco Security Agent.

Cisco IT next plans to install Cisco Security Agent on its internal and customer-facing Windows 2000 servers, including those that run Cisco CallManager and Cisco Unity™ software. The Cisco CallManager and Cisco Unity business units have developed their own policies for their servers. "Windows servers are just as important as desktops and just as vulnerable," says Mauvais. "Installing Cisco Security Agent is an essential part of our strategy to

ensure availability of voice over IP and other critical IP applications."

FOR MORE INFORMATION

To read the entire case study or for additional Cisco IT case studies on a variety of business solutions, visit Cisco on Cisco: Inside Cisco IT www.cisco.com/go/ciscoit

NOTE

This publication describes how Cisco has benefited from the deployment of its own products. Many factors may have contributed to the results and benefits described; Cisco does not guarantee comparable results elsewhere.

CISCO PROVIDES THIS PUBLICATION AS IS WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some jurisdictions do not allow disclaimer of express or implied warranties, therefore this disclaimer may not apply to you.

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.**