

Cisco Security Agent with Intrusion **Protection** for Remote Corporate Users

Increasingly, employees are working remotely from corporate offices. Some of these users are mobile workers accessing corporate applications like e-mail from hotel rooms, airports, or customer offices. Others are teleworkers working from home. Often, these users access the corporate network through the Internet instead of using a dialup modem. All of these users are exposed to probes or attacks from the Internet, and none are protected by the central corporate firewall. Remote users whose computers are compromised provide attackers with a point of entry into the corporate network.

The introduction and growth of the centrally managed personal firewall (sometimes referred to as “distributed firewall”) market demonstrates the desire of IT departments to reduce these risks. To meet customer needs, the following important features are typical of several personal firewall products available today:

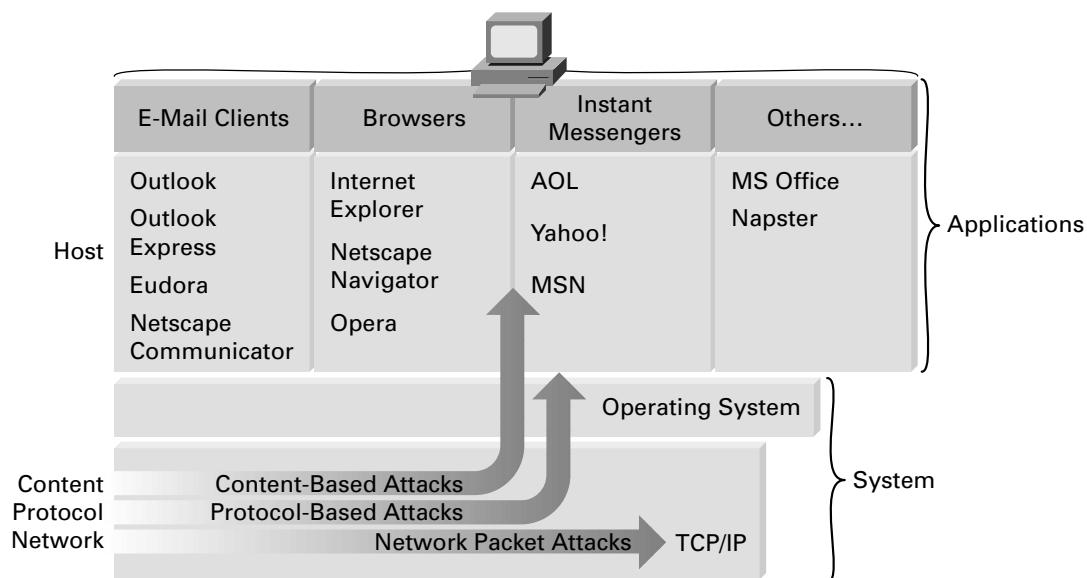
- Port blocking
- Centralized network security policy management

- Centralized reporting
- Intrusion detection (not offered by all products)
- The ability to control which applications can use the network (not offered by all products)

These features only address a subset of the risks facing remote users. Most distributed firewall features focus exclusively on network attacks such as attempts to connect to applications on the computer. However, many other risks are present from attacks through malicious content payloads such as e-mail attachments or JavaScript, or from protocol attacks like buffer overflow attacks on network applications.



Figure 1
Application Attacks



When resources are protected by traditional personal firewalls, the protection usually stops at the network; when an attack compromises an application, the host is completely vulnerable. If a personal firewall allows a service to execute, the software providing the service must be up to date and configured properly. When the application is accessed over the network, the personal firewall cannot protect the application. And the personal firewall cannot control application usage of the network beyond simple port or IP address control. Other standard personal firewall disadvantages include:

- Intrusions masquerading as authorized applications might bypass personal firewall security. For example, Foundstone's "Firehole" attack can allow other applications to impersonate Internet Explorer to make authorized connections¹.
- Most security events generated by personal firewalls are unremarkable and not part of any malicious intent. This can make it difficult for companies to judge the effectiveness of the personal firewall².
- A personal firewall does nothing to protect client applications that use the network. For example, a recent Internet Explorer hole allows a basic HTML attack to compromise the operating system³. Other examples include the ability of users to download potentially infected files through Instant Messenger, and e-mail snooping through embedded HTML in the message body⁴.

1. Firehole can be found at:
<http://keir.net/firehole.html>.
TooLeaky can be found at:
<http://tooleaky.zensoft.com>.

2. "Study: Constant security fixes overwhelming IT managers," *Computerworld*, November 30, 2001,
http://www.computerworld.com/itresources/rcstory/0,4167,STO66215_KEY73,00.html

3. CERT Advisory CA-2001-36, "Microsoft Internet Explorer Does Not Respect Content-Disposition and Content-Type MIME Headers",
December 16, 2001,
<http://www.cert.org/advisories/CA-2001-36.html>

4. "Privacy group warns of e-mail wiretap", *CNN.com*, February 5, 2001,
<http://www.cnn.com/2001/TECH/internet/02/05/email.wiretap.idg/>



The NIMDA attack illustrates the blended threat risk. The NIMDA worm was a multifaceted attack that used multiple avenues—HTTP, e-mail, and shared folders. Systems that were protected at the network level from HTTP attacks were often vulnerable through e-mail, or through vulnerable Web browsers. Because the Cisco[®] Security Agent distributed firewall includes an intrusion prevention capability, it is able to control attack propagation and damage even after it has entered a system. The Cisco Security Agent stopped NIMDA—even after it entered a system—because NIMDA’s activity was beyond the scope of normal behavior. The attack executed buffer overflows in applications and tried to e-mail itself to other targets. Even though Cisco Security Agent does not contain attack signatures, and NIMDA was an attack that had never been seen before, the Cisco Security Agent stopped the attempts of malicious activity.

The Cisco Security Agent Prevents All Classes of Attack

The Cisco Security Agent satisfies the basic requirements for a personal (distributed) firewall, blocking network-based attacks against remote users. It also goes beyond these traditional features by preventing damage from protocol and malicious content attacks. In addition, the firewall offers the following advantages over personal firewall products from other vendors:

- *Active content sandbox* protects Web browsers from subversion using mobile code like Java, JavaScript, and ActiveX
- *E-mail worm protection* blocks e-mail worm attacks like NIMDA or GONER
- *Application masquerade prevention* protects against “application hijacking” using a dynamic link library (DLL) control hook as done by the “Firehole” and “Tooleaky” attacks
- *Application policy control* allows preventing risky user behavior within applications, such as downloading files using an instant messaging application
- *Buffer overflow protection* protects against known and unknown buffer overflow attacks
- *Application execution control* allows central specification of which applications can run, can use the network, and cannot use the network
- *Location-aware protection* allows normal network use such as file sharing, in the office, while preventing risky network use when at a remote location
- *Zero-update intrusion detection* detects and blocks attacks without the need for signatures. Because signatures are not required to prevent intrusions—unlike other intrusion detection products—there is no window of exposure when an attack is circulating but the vendor has not yet created signatures. There is also no administrative burden associated with installing signatures and keeping them current.

Cisco Security Agent Features

The following features, performance benchmarks, and product attributes can be compared to those offered by other personal firewall products to determine the level of adherence to your specific network security requirements.



Basic Network Security Features

Inbound and outbound port blocking—The distributed firewall policies in the Cisco Security Agent control all aspects of network traffic, including all inbound and outbound connections. The Cisco Security Agent also controls traffic based on protocol, port, and communicating host address. Unlike other personal firewall products, it allows control based on which application is attempting the activity—for example, an administrator could allow Web browsers to connect to remote Web servers but prohibit e-mail clients from doing so.

Protection from fragmented packet attacks—The Cisco Security Agent protects against numerous Layer 3 attacks, including packet fragments. This not only blocks denial-of-service (DoS) attacks like WinNuke or SMBDie, but defeats port scans and operating system fingerprinting (nmap) attacks as well.

Protection from attacks using “evasion” techniques—The Cisco Security Agent is immune from methods commonly used to evade intrusion detection systems (IDSs)⁵.

Intrusion detection and prevention—Known and unknown attacks are detected and automatically blocked by the agent. Because the Cisco Security Agent contains an intrusion protection system that uses behavioral policies to enforce appropriate system behavior, no intrusion detection signatures are needed. Other intrusion detection products release new signatures to detect and block new attacks. Unfortunately, these updates are often released infrequently, resulting in a considerable time period where the computer is vulnerable because no signature is yet available.

Because the Cisco Security Agent intrusion detection and prevention does not rely on signatures, the protection provided by the firewall is not dependent on how rapidly new signature updates are made available. Deploying frequent, sizable signature updates to large numbers of client desktop or laptop computers is not only difficult to manage, but also consumes large amounts of network bandwidth. This gives Cisco Security Agent a higher level of protection, and results in a zero-update architecture, where no signature updates need to be managed.

Configurable IDS rules—The Cisco Security Agent focuses on preventing, rather than detecting, intrusions. The behavioral policies that make up the system are highly customizable by the administrator.

Application execution protection—The Cisco Security Agent can control which applications are allowed to execute. The rules allow extremely granular control over not only which applications can execute, but also which versions of applications can execute. It can also control which DLL versions are allowed to run.

Location-aware protection—The Cisco Security Agent allows normal network use—for example, sharing files between computers—while in the office, but prevents these risky activities when the computer is in a remote location.

5. “IDS Evasion with Unicode”, Eric Hacker, *Bugtraq security mailing list*, January 3, 2001, <http://www.securityfocus.com/infocus/1232>



Advanced Security Features

“Sandbox” protection for Web browsers and e-mail clients—The Cisco Security Agent prevents content-based attacks delivered by mobile code like Java, JavaScript, and ActiveX against Web browsers and other end-user network applications. Users are protected against malicious content while they browse, read e-mail, or chat online.

E-mail worm prevention—The Cisco Security Agent detects and blocks attempts to send mass e-mail containing potentially malicious attachments. Not only does it block these attempts by strictly controlling access to resources like the Microsoft Outlook address book, but it also reports malicious e-mail attachments to the central manager, which updates a system-wide Global Quarantine List. This quarantine list is deployed to all agents, resulting in agents being inoculated even if that particular worm has never attacked them.

Protection against both known and unknown buffer overflow attacks—The Cisco Security Agent detects and blocks buffer overflow attacks against any application running on the protected computer. Because the detection is based on how applications execute code, and not on analysis of packet contents, it will block both known buffer overflow attacks and unknown ones. Even attacks that use IDS evasion techniques will be blocked. The distributed firewall’s advanced buffer overflow protection blocks not only the better-known stack overflows, but the more difficult heap overflows as well.

Application masquerade prevention—In one of the latest attack techniques against personal firewall products, a malicious application attempts to masquerade as a trusted application through a mechanism such as DLL Injection⁶. Because this allows the malicious program code to appear to be running inside the trusted application, the firewall will be fooled into thinking that the malicious code is part of the trusted program. Thus, the malicious application will be able to bypass the firewall controls (for example, to access the network). Cisco Security Agent detects and blocks all DLL Injection attacks, protecting not only against unauthorized network access, but also against local password theft attacks.

Configurable instant messaging controls—The Cisco Security Agent offers application policy control, which gives companies the ability to control, with a high level of specificity, which aspects of an instant messenger application are used within their organizations. For example, Cisco Security Agent can allow text messaging but can explicitly forbid the transfer of files through the instant messenger system, while continuing to allow file transfers using other mechanisms such as browser or FTP. It can allow instant messenger clients to only use approved, corporate instant messenger servers, or to transfer documents only when they are using internal instant messenger servers.

Operating system lock-down—The Cisco Security Agent hardens the Windows operating system, preventing attacks from modifying critical operating system binary files or configuration settings. Because this capability does not require the use of cryptographic analysis of file system contents, it adds virtually no performance impact to the system.

Audit log consolidation—The Cisco Security Agent provides detailed logging of attacks. It can also collect Windows Event Log and Security Log entries such as bad logon attempts.

6. *PWDUMP2* from the Bindview Razor security team steals passwords from Windows NT and Windows 2000 computers (http://razor.bindview.com/tools/desc/pwdump2_readme.html).

For a discussion of DLL injection attacks to bypass personal firewall protection, visit:
<http://keir.net/firehole.html>



Open and customizable—Application security measures are controlled by policies. The policies are composed of a set of rules that specify how applications may access network, file system, registry, or COM system components. Although the Cisco Security Agent provides default policies for distributed firewall and desktop application protection, all of these policies are customizable, and administrators can easily define new policies through the browser-based GUI.

Management Features

Central management of agent—Policies for the Cisco Security Agent are defined centrally and automatically pushed out to the agents residing on servers and to the desktops requiring protection.

Manage-from-anywhere solution for administrators—Cisco Security Agent management is based on HTTP and HTTPS, so all management can be handled from any location using a standard Web browser.

Works in a Dynamic Host Configuration Protocol (DHCP) environment—Agents are not identified by IP address, which typically changes often in DHCP environments. Rather, each agent is assigned a globally unique identifier (GUID) that does not rely on IP address. Therefore, all central management functions such as grouping, policy assignment or modification, or agent update will reach the intended agents, even if those agents' addresses change.

Central alerting—All agent events are sent to the management console, where alerts are centrally generated.

Configurable alerting—Alerts are reported to a central console; all client events report to the Cisco Security Agent management console, which in turn generates alerts to a central customer console. All events generated by client agents can be configured to alert through e-mail, pager, Simple Network Management Protocol (SNMP) trap, flat log file, or a custom programmatic interface.

Secure communications between agents and the management console—All communications between the management console and agents is performed using Secure Sockets Layer (SSL) over configurable ports.

Central policy definition and local policy enforcement—If agents are disconnected for a period of time, all policy enforcement will continue to be performed locally. When the agent is reconnected, new policies and updates will automatically be installed. Agent updates are automatically pulled from the management console at configurable intervals.

Remote installation and automatic configuration—The initial agent software may be deployed via HTTP, Short Message Service (SMS), or other corporate software distribution mechanisms. All further policy and software updates are done automatically through the agent polling mechanism.

End users are isolated from security policies—The end user does not have direct access to the Cisco Security Agent, and cannot change policy locally. The Cisco Security Agent enforces a centrally defined policy that is cached locally on the agent. This policy cannot be viewed or modified by the client user.

Optional notification of end user when under attack—All security events are stored locally on the client, and also sent to the central management console. The client can optionally be notified of policy violations using a waving flag in the Windows taskbar. If desired, the Cisco Security Agent can be configured so that it is invisible to end users.

Reduced logging and no false-positives—Because the Cisco Security Agent is a customizable, behavior-based policy system, there are no false positives. Policies may be easily adapted to specific computing environments.



Forensics and System Assurance for Remote Computers

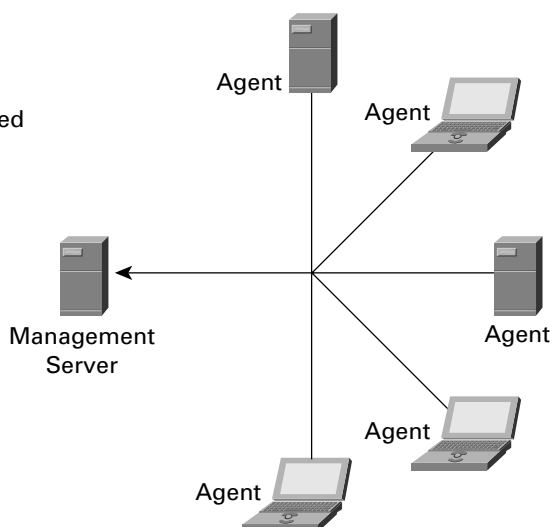
Figure 2

Cisco Security Agent Architecture

- Stop attacks
- Enforce Policy
- Collect Activity Information as Required

- Forensic investigation of Application Behavior
- Build New Policy to Protect or Control New Applications

- Identify All Applications Installed or Run On System
- Identify “Missing” or Unused Security Agents Like A/V Scanners
- Identify Systems Not Protected by StormWatch Agents



One common complaint of traditional personal firewalls is that while application control allows specification of known “good” applications, the number of possible applications that users will install is much larger. The problem is much larger than cursory inspection would suggest, because there are many application versions and patch levels to consider. Users become annoyed when their (nonmalicious) applications are blocked by the firewall, or administrators are forced to be overly permissive about which applications they allow to run.

The problem for administrators is that they have not had an easy way to identify what applications are installed and used, nor to investigate what behaviors applications perform. This makes it difficult to build a list of known good applications in the presence of previously unknown applications.

It has also not been possible to monitor whether approved applications have been used properly; for example, whether antivirus scanners are run and regularly updated with the latest signatures. This is made even more difficult when many systems are physically remote.

The Cisco Security Agent framework allows the Cisco security agents to work cooperatively with other Cisco products—resident on the Cisco Security Agent central management server—to allow administrators to easily manage these issues.

The Cisco Security Agent Profiler uses existing Cisco security agents to identify the state of all applications on all remote systems, including:

- Which applications are installed on which computers
- Which of these applications are run
- Which of these use the network, as clients or as servers
- Whether desired applications such as antivirus scanners are not installed or running
- Whether undesired applications such as peer-to-peer file sharing applications are running



- Whether there are any remote systems that are unprotected by Cisco security agents (requires installation of the Cisco Security Agent on critical internal servers such as e-mail, Domain Name System [DNS], or DHCP; Cisco Security Agent Profiler identifies all systems that do not have Cisco security agents communicating with these servers)

Cisco Security Agent Profiler performs detailed forensics examination of any application on any computer. It observes the application's live behavior—all files accessed, whether for read or write; all network connections, whether inbound (server) or outbound (client) along with the address of the remote computer; all registry access, whether for read or for write; and all COM object loading. Cisco Security Agent Profiler collects information about the application's behavior, summarizes it in a report for the administrator, and generates a policy to allow controlling it.

Using the Cisco Security Agent framework, administrators can centrally:

- Identify remote computers not protected by personal firewall agents
- Identify remote computers not running system security products like antivirus scanners
- Identify remote computers not running antivirus signature updaters like Symantec's LiveUpdate
- Identify remote computers missing critical system security updates like service packs or hot fixes
- Identify remote computers not running any application that the organization's policy mandates
- Identify unauthorized or unknown applications that are installed or run on remote computers
- Identify which behaviors unknown applications perform when they are run—separating unknown but malicious applications from unknown but benign ones
- Control which behaviors applications are allowed to execute, or which functions they can perform, based on observed behavior analysis.

Both the Cisco Security Agent and Cisco Security Agent Profiler are installed on the Cisco Security Agent management server and use the existing firewall agents—no additional installation on remote systems is required.

Superior Capability, Superior Network Security

Going beyond basic—or even advanced—firewall capabilities, the Cisco Security Agent adds remote investigation and control. It offers superior protection that avoids the limitations of traditional personal firewall products. With its broad network security coverage combined with deep system analysis, the Cisco Security Agent gives administrators powerful network security for remote computers.

The Cisco Security Agent provides uncompromising intrusion prevention for enterprise environments. It helps prevent intrusions from executing and offers security without signatures. Cisco security agents, residing on critical servers and desktops, go beyond standard personal firewall products by invoking the proprietary Intercept Correlate Rules Engine (INCORE) architecture to provide safe access to required resources. INCORE intercepts an application's resource requests to the operating system, correlates the behavior within its rules engine, and makes a real-time allow/deny decision according to the customer's application security policy. The agent's ability to proactively repel new attacks directly on the servers and desktops to be protected makes it a central component to a customer's security policy. The Cisco Security Agent is an entirely new standalone layer of defense, one that does not burden IT departments with the continual management of signature updates.



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.
Capital Tower
168 Robinson Road
#22-01 to #29-01
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 Web site at www.cisco.com/go/offices**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
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

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems, and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site 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.
(0304R) BU/LW4850 07/03