Global Information Assurance Certification Paper

Cisco Security Agent: Intrusion Prevention at the Endpoint

Barbara M. Taylor
June 16, 2004
GSEC Practical Assignment
(v.1.4b August 2002)
Option 1

CISCO SECURITY AGENT: INTRUSION PREVENTION AT THE ENDPOINT

Abstract

Worms, viruses, DOS attacks, buffer overflows, and Trojan horses are sources of danger to any computer network. Hackers will attack web servers, data servers, authentication systems, email servers and accounts, network devices such as routers and switches, and host computers. Any device, any operating system, and any application located on the network infrastructure are innately vulnerable.

Many protection systems have been designed and deployed to mitigate these vulnerabilities. The list includes anti-virus software, intrusion detection programs, authentication systems, and access control mechanisms. Cisco Security Agent, a tool of the CiscoWorks arsenal of network security utilities, is an endpoint intrusion prevention solution offered by Cisco Systems. This document explores network vulnerabilities and the components and behavior-based methods that Cisco Security Agent uses to prevent anomalous intrusion at the network endpoint.

SECTION I. INTRODUCTION

Speed of network attack propagation

In 2002 the CERT Coordination Center published a statement on the changes in network attack trends.[1] The consensus was that the speed of attack propagation was increasing rapidly, largely due to the automation of attack tools and the automated management of those tools.

The behavior of attacks is becoming more dynamic and sophisticated, allowing more rapid discovery of network vulnerabilities. Firewalls offer less network perimeter protection as intruders create new technologies to bypass hardened firewall configurations. Poorly secured routers can be used as attack platforms targeting internal and external networks.

Many network security symposia in 2004 also make this observation. Presentations routinely begin with an alert to the audience that vigilance is compulsory as hackers close the gap between the announcement of a vulnerability and the release of an attack against that liability. The most recent confirmation of this rapid convergence of a zero-day exposure/attack was at the April 2004 Microsoft Security Summit[2] in Dallas, Texas.

Cisco's Mitigation Tool

In response to the increased exposure and vulnerability of the corporate network infrastructure, Cisco has added an endpoint mitigation tool to its arsenal of network security tools. In May of 2003 Cisco purchased Okena, an intrusion detection software company. Okena's patent-pending software, StormWatch, was designed to detect and prevent anomalous network endpoint attacks.

Cisco's newsroom confirmed that "Cisco has announced that it is acquiring Okena, a developer of highly innovative behavior-based technology that goes beyond conventional desktops and server security solutions to protect companies against threats such as viruses, worms, Trojan horses and buffer overload attacks……Okena's technology goes beyond conventional host/desktop security by identifying and preventing known and unknown attacks before they can occur …..This is especially valuable in preventing 'Day-Zero' attacks, which are attacks perpetrated when known signatures do not exist."[3]

Public Announcements

Many Internet news services reported on Cisco's acquisition of Okena and the significance of Cisco Security Agent as a tool in the arsenal of security mitigation utilities. Trade on-line news postings said "The Cisco Security Agent for

Desktops aims to stop attacks on corporate PCs by looking for anomalous network behavior and blocking it, while Cisco Security Agent for Servers does the same for the heavy lifters of the corporate network."[4]

One significant advantage of the Okena technology is that it "aggregates and extends multiple endpoint security functions - Host-based Intrusion Detection (HIDS), distributed firewall, malicious code protection and operating system lockdown - in a single solution."[5]

GRID today and other news services reported "These additions underscore the Cisco security strategy to deliver advanced network protection by integrating security services throughout Internet Protocol (IP) networks, making them a transparent and manageable aspect of any network."[6]

This paper will describe the nature of common network attacks and Cisco Security Agent's methods of mitigating those attacks. The examples and screen shots are all relative to a Windows 2000 Advanced Server Cisco Security Agent Management Center installation. Many of the graphics were captured in a test lab environment.

SECTION II. IN THE BEGINNING

Public Internet

President George H. Bush signed an agreement that opened the Internet to general public access in 1992. Since that time networks have evolved and grown like an amoeba on steroids. The birth of the Dotcom revolution has spread the Internet and e-commerce into everyone's lives. Ease of access to banking and commercial records as well as other corporate information has inspired malicious threats to the confidentiality and integrity of that data. As corporations develop methods to secure their classified information, attackers meet the challenge with more sophisticated methods of assault.

Timeline of well-known attacks

Unfortunately, the timeline from probe to paralysis of vulnerable systems grows shorter every month.

Examples of well-known attacks

	Vulnerability Announcement	Exploit Announcement	
2001 Nimda	3/29/2001[7]	12/18/2001[8]	(9 months)
2003 SQL Slammer	7/24/2002[9]	1/25/2003[10]	(6 months)
2003 MS Blaster	7/16/2003[11]	8/11/2003[12]	(26 days)
2004 Sasser	4/13/2004[13]	5/01/2004[14]	(18 days)

Cisco's Lifecycle of attacks

The following chart lists the five P's of Cisco's Lifecycle of Network System Attacks. In the first step network attackers **Probe** systems in an attempt to locate vulnerable networks. When such a network is identified, invaders try to **Penetrate** that system and transfer exploit code to a vulnerable device. Once an entrée has been gained, the attacker adds **Persistence** to his/her aggression by installing malicious code permanently on the vulnerable device. This code then **Propagates** itself to other network systems, extending the attack to other vulnerable neighboring devices. The result of this insidious assault is to **Paralyze** the targeted victims.

Cisco's Lifecycle of Network System Attacks[15]

Attack Action	Network Manifestation
Probe	Ping IP addresses Run traceroute on IP addresses Scan ports Sniff passwords Impersonate email users
Penetrate	Create email attachments Instigate buffer overflows Locate and utilize backdoors Utilize malicious Java applets and ActiveX controls Initiate compressed messages
Persist	Weaken security settings Install new files Modify or replace existing files Install malicious services Modify registry settings Register trapdoors

Propagate	Spread email attack Utilize network connections Utilize IRC capabilities Utilize FTP capabilities Infect file shares
Paralyze	Reformat disks Delete files Modify files Drill security holes Crash computers Create denial of service Consume work cycles Steal & expose confidential information

According to Cisco[16] and confirmed by many security seminars, the methods of attack in the Probe and Penetrate stages are constantly evolving. As operating systems and applications mature, the means to prod and poke them, testing for vulnerabilities, morphs. Protecting a network against these initial sorties is a constant battle of "catch-up" as attackers invent new methods of frontal assault.

In contrast, the latter three lifecycle phases have typical, predictable manifestations. Email, operating systems, files, shares, and connections are common targets. Cisco Security Agent is designed to analyze the behavior of the operating system and applications on the target device and handle undesirable, malicious behavior on the host as defined by CSA security policies. CSA is a type of Host Intrusion Detection System (HIDS) that uses these policies rather than the signatures of typical intrusion detection methods.

SECTION III. METHODS USED TO MITIGATE ANOMALOUS ATTACKS

Physical security

Many forms of network security have been employed at various layers of the OSI Model. The most obvious form of security is physical security. The best security for a computer and its data is to turn it off, unplug all interfaces, and lock it in a closet. Obviously, this is not appropriate in a production environment.

Corporate security policies often employ multiple levels of physical security. These involve limited access to locked server rooms and limited access by the public to corporate offices. Computer and projection screens are positioned to face away from public view through doorways or through windows. Access through drop ceilings is restricted. Multiple systems are often employed to thwart loss of information or disruption of service through simple theft of the hardware.

Perimeter security

Protection of the network infrastructure usually employs perimeter security. Methods utilized include firewalls, packet filters, proxy servers, and network intrusion detection systems positioned at the public interface. Access to the corporate network includes authentication, authorization and auditing of attempted admittance. Access control lists permit and deny the right of entry through address, port and protocol inspection. Network Address Translation (NAT) hides internal network addressing schemes from public scrutiny.

Policy-defined security zones

Network security policies often divide a corporate network into three zones to control network traffic. The WAN zone interfaces the Internet cloud and public traffic. The private, LAN zone is segregated for use by authenticated users. The employment of a Demilitarized Zone (DMZ) isolates corporate services permitted accessibility by both public traffic and the private LAN, such as a Web server and/or a DNS server. Separating network traffic into these zones allows configured control of access to corporate resources by area and thus aids in isolating and mitigating malicious attacks.

Once inside the perimeter defenses, additional layers of internal packet filters further test the traffic. Network administrators also establish host intrusion detection systems and virus scanners. Virtual Private Networks (VPNs) are used to protect confidential network traffic into the network from WAN sources and as it travels throughout the LAN.

Logging

Extensive logging documents network activity from authentication, authorization and accounting mechanisms such as RADIUS and TACACS+ servers. Logging also records network intrusion detection system (NIDS) and host intrusion detection system (HIDS) auditing.

Cisco Security Agent

Cisco Security Agent focuses on protecting servers and workstations as endpoint devices. The intent is to provide intrusion prevention by analyzing operating system and application behavior. Configurable CSA policies reside on the endpoints to permit, deny or question attempted modifications to the network system, its applications and files.

SECTON IV. WHY USE CISCO SECURITY AGENT?

The Northstar Group represents several Cisco products on the Internet. As a sales pitch, Northstar states that "The Cisco Security Agent aggregates and extends multiple endpoint security functions by providing host intrusion prevention, distributed firewall, malicious mobile code protection, operating system integrity assurance, and audit log consolidation all within a single agent package."[17]

Cisco Security Agent acts like a personal firewall and host intrusion detection system, providing many firewall and HIDS features including

- intrusion detection and prevention of attacks from recognized and unrecognized locations
- port blocking at inbound and outbound vulnerable ports
- buffer overflow prevention against known and unknown buffer overflow attacks
- protection against worm attacks and other suspicious email content
- application masquerade prevention, blockage of application DLL injection
- creation of an active content sandbox to isolate Java, Javascript and ActiveX applications utilized in potential web-based attacks
- vigilant application activity tracking that controls which application versions can run
- correlation of the local and global activities of applications

Built in to the behavior detection system of CSA is an automatic correlation feature.[18] Correlation looks for patterns of

- multiple behaviors on a target device in reference to a specific application
- an activity on that device targeting several applications
- small probes to multiple machines in the network

Subtle probes into a network may include single pings to various devices to identify active addresses and thus map the network. When individual activities are recognized as part of a global pattern, i.e., correlated, an alert is generated.

If each unique local action were to generate an alert, there would be many false alarms, false positives. Downloading a file, executing an application, opening email software, and sending an email should not generate alerts each time they occur; they are normal, valid, benign activities. When the CSA correlation feature detects these events in sequence – typical of worm activity – possible malicious activity is recognized and denied. Activity correlation reduces the number of false positives and the number of logged alerts.

Cisco Security Agent does not use or depend on signatures as do intrusion detection systems. Instead, configurable policies are pushed from the CSA Management Center to network clients. Thus, CSA professes to be a “zero-update” system that does not rely or depend on the computer network industry to provide signatures to identify and mitigate specific attacks. There is no time lag as with a “signature update race”. Network administrators can react immediately to a potential assault by configuring a CSA policy against it. Therefore, Cisco Security Agent offers the possibility of “zero-day” security.

SECTION V. COMPONENTS OF CISCO SECURITY AGENT

Cisco Security Agent is a combination of components similar in design to Simple Network Management Protocol (SNMP):

- Management center software – Cisco Security Agent Management Center (CSA MC), a component of CiscoWorks VPN/Security Management Solution (VMS).
- Agent software “kits” – Cisco Security Agent (CSA)
- Security Policies

Additional integral instruments of the CSA system include

- Event Logs and Alerts
- A SQL Database Engine
- A Web browser

Each of these components is described below.

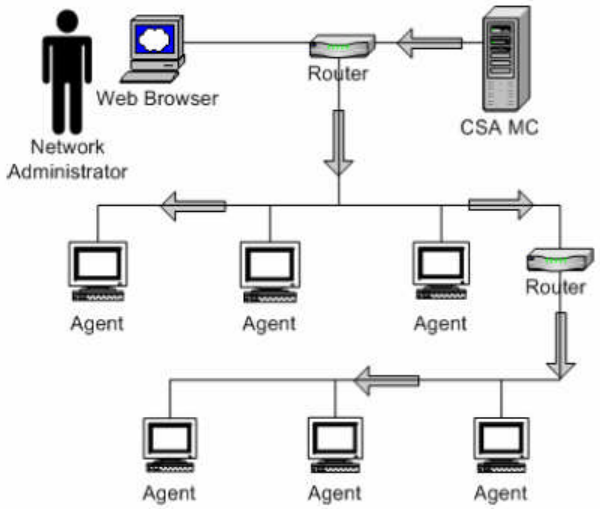

Figure 1 Major components of the Cisco Security Agent system[19]

The Management Center

The Cisco Security Agent Management Center (CSA MC) is one of many components of CiscoWorks VPN/Security Management Solution (VMS). It is the "core management software that provides a central means of defining and distributing policies, providing software updates, and maintaining communications to the agents."[20]

In this system, the CSA Management Center resides on a selected Windows 2000 "superserver". The server must be running Microsoft Internet Information Services (IIS), Domain Name System (DNS), and either Microsoft SQL Server 2000 or Microsoft SQL Server Desktop Engine (MSDE). Appropriate Service Packs must be present for the operating system and SQL applications: SP3 or later. WINS support is also suggested.

According to one reference, the operating system for the CSA Management Center can be "Windows 2000 Professional, Server, or Advanced Server with SP3, and with Terminal Services turned off."[21] However, 1 GB of RAM, a 1 gHz or faster Pentium processor and a minimum of 11 GB of free hard drive space (2 GB of this for virtual memory) are strongly recommended hardware parameters. It is unlikely that this combination of hardware and software would be applied to a Windows 2000 Professional box. The Cisco Security Agent Data Sheet[22] suggests that Windows 2000 Server or Advanced Server should be the operating system of choice for the CSA MC. Windows 2003 operating systems are not yet mentioned in the literature.

Agent software

An Agent software kit resides on selected mission-critical network clients: servers and workstations. The agent deployment to the client may be configured for intrusion detection only (IDS mode), or for behavior-based intervention. The desktop computers may be from the Windows network workstation family: Windows 2000, Windows NT, or Windows XP. The Cisco Security Agent Data Sheet[23] recommends the Windows NT and Windows 2000 servers and the Sun Solaris UNIX servers as mission-critical candidates for the CSA Server Agent.

Windows agent hardware platforms must have 128 MB of RAM, a Pentium 200 mHz or faster processor and a minimum of 15 MB of free hard drive space. The device can access the network locally through an Ethernet network adapter or remotely via a dialup connection.

Solaris agent hardware platforms are required to have a minimum of 256 MB of RAM, an UltraSPARC 500 mHz or faster processor, and a minimum of 15 MB of free hard drive space. The computer can access the network via an Ethernet connection.

Security Policies

Default security policies are installed with CSA MC. These policies are a combination of rules defining permitted normal application and operating system behavior and denied abnormal behavior that may be malicious. The policies are part of Agent kits. One Agent kit is installed on the Management Center. A kit is pushed to each MC-identified endpoint device. A user at the endpoint device may be allowed to interact with the CSA software and choose to accept the changes noted in a policy alert dialog.

There are 30 – 40 default rules included as part of the installation package. The default policies can be modified using default or modified rules. The administrator may also create new policies.

Event Logs and Alerts[24]

The CSA Management enter collects extensive event logging information and stores the records in various locations on the management system.

Detailed events are monitored for the four CSA common rule types:

- File access control
- Network access control
- Registry access control
- COM component access control

Cisco Security Agent rules and policies are detailed in Section VI.

CSA utilities such as Event Log, Event Monitor, and Event Log Management display logging information collected from clients. Filter settings include filtering by date and time, by host, and by Rule ID. Also included are filtering by the seven well-known network severity levels:

- Emergency
- Critical
- Alert
- Error
- Warning
- Notification
- Informational

The following screen shot was captured during a test of the CSA Management Center software. The severity levels noted are Alert and Warning.

Notice the red flag waving in the system tray. A CSA policy violation has been detected. Policy violations are discussed in Section VI.

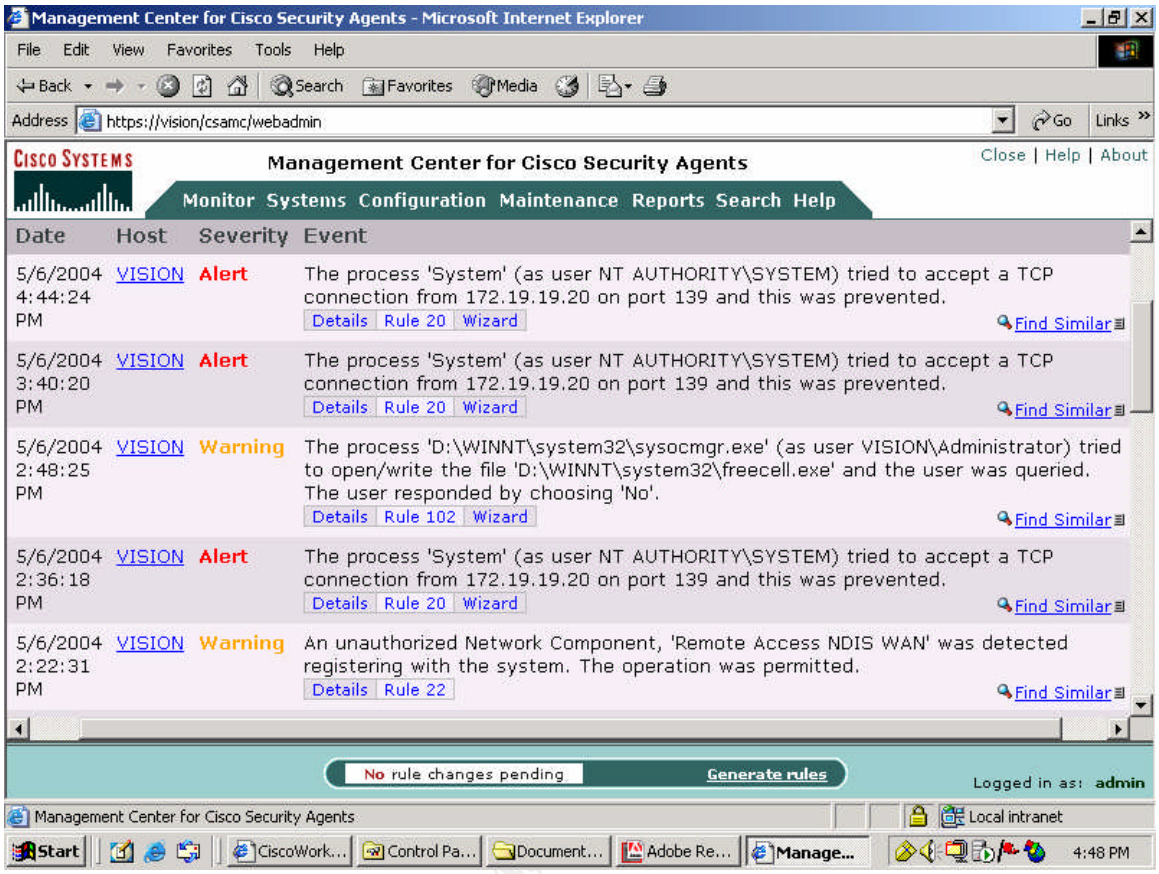

Figure 2 Severity levels recorded by Cisco Security Agent Management Center in the test lab environment.

SQL Database Engine

The SQL server database (or Microsoft SQL server Desktop Engine [MSDE]) collects information about the CSA Management system configuration. Details of groups of hosts/agents and individual clients belonging to the CSA network, logging, and event information provided to the central database by the clients, and relevant configuration information is stored on this server. Specific rules and policy settings pertinent to the file system, the network system, the registry, and COM configuration are recorded here as well.

The SQL server acquires the data used to produce extensive CSA reports.

Web browsers

Management of the CSA system is performed from a secure browser or similar web-based interface located on a local or remote device. The browser must accept cookies and Java and JavaScript. If Internet Explorer is utilized, it must be

version 5.5 or higher to allow the CSA MC to be fully functional. Netscape Navigator must be version 6.2 or higher. The CSA MC management interface requires a secure connection using SSL (HTTPS).

The use of a Web browser gives the CSA Management Center "'manage from anywhere' access [which] makes it easy for administrators to control thousands of agents per MC"[25].

There are two URLs to launch the CSA MC from a Web browser. The port numbers are configurable.

http://*server_name*:1741	a non-secure, limited function access
https://*server_name*:1742	secure, fully functional CiscoWorks Web page.

Access to the CSA MC through a Web browser provides simple remote access for the administrator.

SECTION VI. HOW CISCO SECURITY AGENT WORKS: INCORE[26]

Okena's StormWatch INCORE technology

At the heart of the Cisco Security Agent's intrusion prevention system is Okena's proprietary StormWatch INCORE architecture. INCORE is an acronym for **IN**tercept **CO**rrelate **R**ules **E**ngine technology.

"Okena's technology extends beyond conventional desktop and server security solutions. Rather than relying on signature-based techniques, Okena technology intercepts all operating system, file system, configuration, registry, and network requests, preventing malicious activity from occurring."[27]

In relation to the functional levels of the resident operating system, Cisco Security Agent is located next to the kernel. This proximity gives it access to application activity and the ability to monitor and intercept calls to files, the network, resource configuration and application execution space. The INCORE engine proactively examines system and application *behavior* on endpoint systems. It does not inspect packet content, and thus has little impact on system performance.

Policies and rules are managed by the CSA Management Center and are cataloged on the SQL server database. As endpoint devices are identified as clients or agents of the CSA system, Agent kits are installed on each device and appropriate policies are downloaded to the device. Modifications or updates to

the policies are also pushed to the clients. Alternatively, clients may pull updates from the Management Center through the CSA client GUI interface.

When requests are made by applications or system processes to files, network resources, the registry, or execution space, INCORE compares the action to the policies set for the client, looking for malicious behavior. The results of this comparison vary depending on the manner in which the policies are configured.

1. The activity is **allowed by the policies**:

   The requests are processed normally with no logging or alert. Anti-virus updates may be permitted by policy and therefore are processed without alerts.

2. The activity is **recognized as a questionable policy violation** and the administrator has allowed a user at the client to intervene with the resultant alert.

   A red flag is displayed in the system tray on the host. The flag waves and an alert message pops open on the monitor. The user chooses to continue with the current activity, as it is seen to be non-malicious, or the user chooses to prevent the unexpected activity as it is perceived to be tainted. In either case the event is recorded at the client and also sent to the Management Center's SQL database and/or other collection mechanism such as SNMP. An example of a user-permitted event is the addition of a Microsoft Windows XP update patch initiated by the user.

3. The activity is **seen as undesired malicious behavior, a strict policy violation***,* which requires immediate attention with no intervention needed, or perhaps allowed, by the user:

   The red flag may be configured to wave in the system tray. However, the user will not receive an alert message. In this case the request will be denied by the policy and an alert will be sent to the SQL database on the Management Center computer and/or other collection agencies. An example of a denied event that requires no user intervention is a read or write to the Windows Cmd shell.

A double-click on the red flag in the system tray opens the CSA agent window, as seen below. This screen capture was made during a laboratory test of the CSA system.

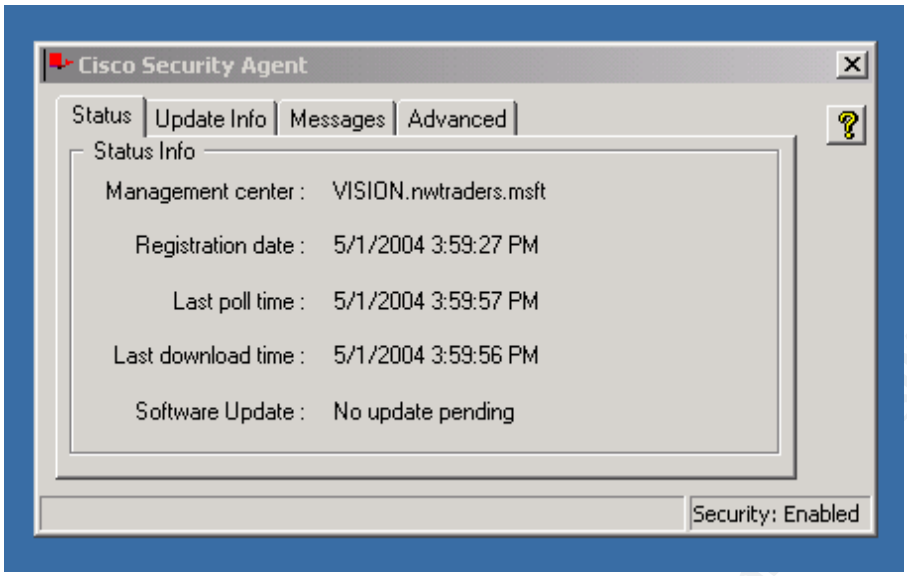

Figure 3 Client CSA dialog box: Status tab – test lab environment

The following screen shots are examples of user-permitted intervention alerts that popped open during a test of the CSA software described in another section of this report. Adobe Reader is attempting an update over the Internet. Notice that the default on this alert is “No”.

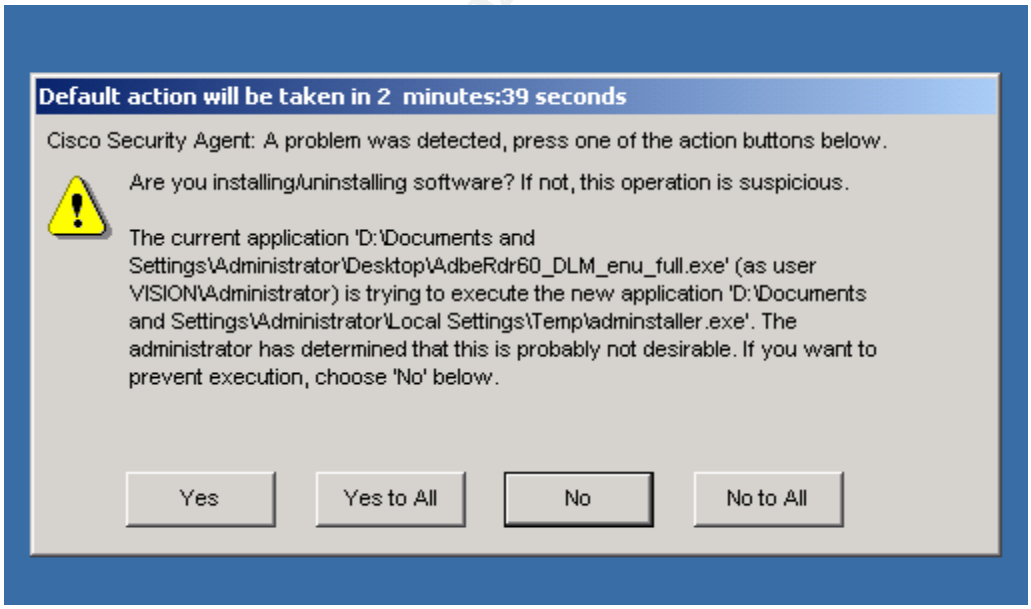

Figure 4 User-interactive CSA client alert – test lab environment

This alert has discovered a call to create a virtual machine as part of an installation. The default is “No” (do not permit this action).

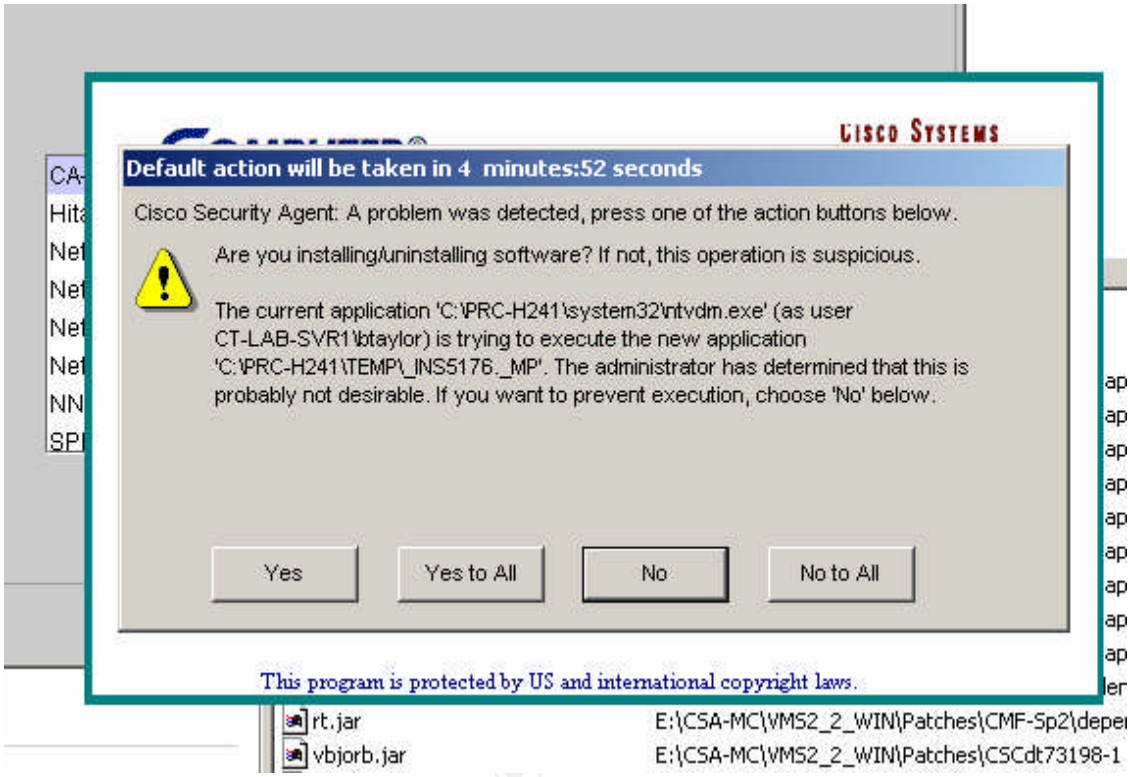

Figure 5 User-interactive CSA client alert – test lab environment

The local Cisco Security Agent kit shows a synopsis of alerts:

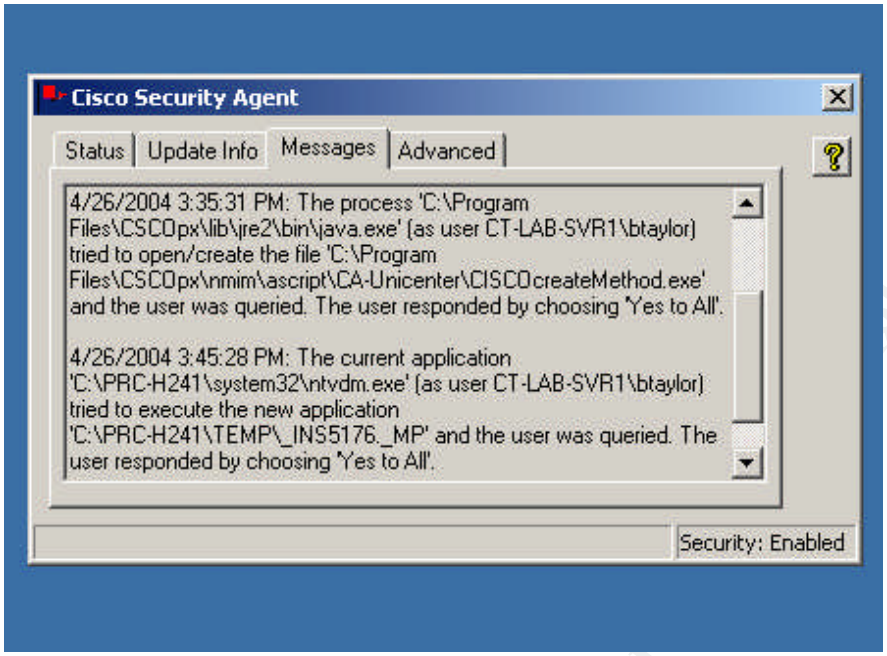

Figure 6 Client CSA dialog box: Messages tab – test lab environment

Managing endpoint security with StormWatch

There are two approaches to managing endpoint security:

- Everything that is not expressly permitted is denied
- Everything that is not expressly denied is permitted

The StormWatch system includes default desktop and server policies that monitor behavior based on the second approach. The undesired or malicious behavior is denied while all other “normal” activity is permitted. Administrators may modify the default policies or, preferably, create new policies. If, in rare cases, an application needs to be “locked down”, fine-tuning allows the Administrator to apply the first methodology: only those actions expressly permitted can occur and all else is denied.

Okena StormWatch Rules[28]

There are 124 pre-configured rules included in Okena's StormWatch 2.1, a 2001 version of StormWatch. The following list is a sampling of the types of rules.

- File Access and Version Control and Monitoring
- Network Access Control and Worm Protection
- Registry Access Control
- Application Access Control
- COM Component Access Control

  These rules allow configuration through selection of high priority deny, allow, query user (default = allow), query user (default = deny), or deny. The rules can be applied individually to applications, files, registry settings, etc., chosen by the administrator. Examples of rule configuration include: an application may not be permitted to execute, users may not be allowed to install applications, and a device may not be allowed to create shares.

- Portscan Detection
- Sniffer and Protocol Detection
- Syn Flood Protection
- Trojan Detection
- Service Restart Protection

  Several of these rules are either On or Off. Many allow granular configuration. For example, Trojan detection includes control of application trapping of keystrokes, code injection into other applications, attempts to share private or reserved application memory space and attempts to steal local passwords.

Desktop Policies

StormWatch Policies for Default Desktops Group[29] for Windows contains seven default policies to protect common applications and the standard working environment of a Windows-based desktop computer. These policies are combinations of the standard rules, configured per module requirements, and can be easily modified with the aid of a Wizard.

- Common Security Module
- Desktop Module
- Inbound Port Blocking Module
- Distributed Firewall Module
- Instant Messenger Module
- Microsoft Office Module
- Required Windows System Module

Server Policies

StormWatch Policies for the Default Servers Group[30] for Windows contains only three default policies for its expected environment and anticipated applications. Administrators are encouraged to create application-specific policies as needed for more restrictive control of vendor-specific applications.

- Common Security Module
- Required Window System Module
- Server Module

It is suggested by many sources that the default policies should not be modified. It is more efficient to create a new policy, based perhaps on a default policy. When upgrades or patches are made to the system, modifications of a default policy will not affect the configuration of a unique policy.

This screen shot was captured during a test of the CSA MC system.

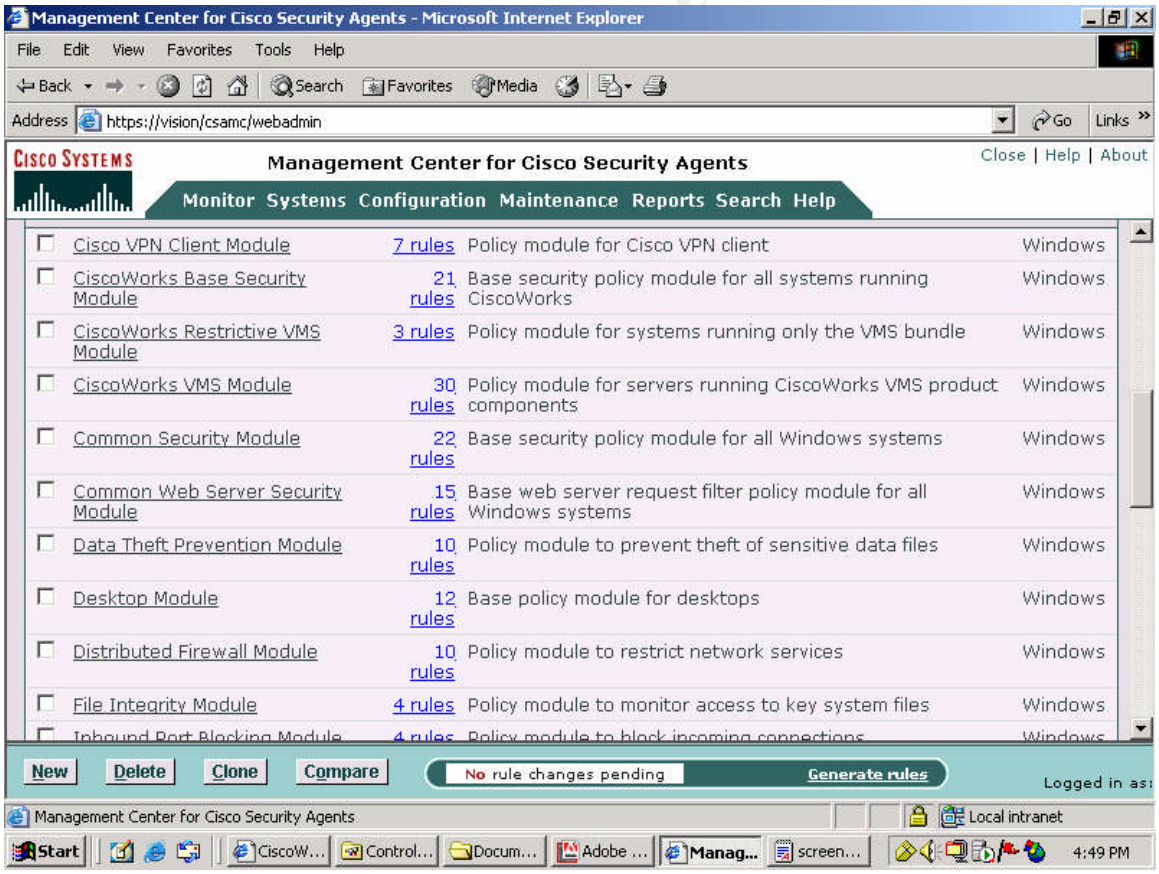

Figure 7 Default policies of Cisco Security Agent Management Center – test lab environment.

SECTION VII. CISCO SECURITY AGENT MANAGEMENT CENTER INSTALLATION

"The CiscoWorks Management Center for Cisco Security Agents is a featured component of CiscoWorks VPN/Security Management Solution (VMS)."[31] The current version is CSA MC v4.0. Although it is possible to upgrade version 3.1 of CSA MC to version 4.0, this involves a great deal of re-configuration. The new upgraded software will retain existing policies. However, the SQL database may also need to be upgraded, and the appropriate links between the database and the policies on agents may be broken. Therefore, Cisco recommends that CSA MC version 4.0 be installed from scratch. During the installation process a CSA security agent kit is automatically added to the MC server to protect that device. A web certificate is created and added to the MC server to add protection for the common components of CiscoWorks VMS.

Installation of Agent Kits on workstations or servers

One recommended method of installing an Agent kit is to pull the kit from the Management Center using a browser on the client. An HTTPS connection is required.

The three types of agents are:

1. The **local server** version installed automatically on the Management Center as a component of CiscoWorks VMS to protect the MC.

2. A **server version** installed on either a UNIX Solaris computer or a Windows server. The Windows version uses Microsoft's proprietary InstallShield.

3. A **workstation version** for Windows desktops.

A Personal Adventure: Installing Cisco Security Agent Management Center

There is a 90-day evaluation version of Cisco Security Agent and the CSA Management Center available from Cisco Connection Online (CCO). As it includes 3DES, to download the software I had to comply with security export restrictions through Cisco. The software downloads in four very large segments, including one .zip file. Much of the CSA installation and CSA management documentation located at http://Cisco.com is included with the CSA MC and Agent software.

To locate the evaluation version

- **login in to CCO**
- Select **Downloads** on the right side of the screen and login again
- Locate **CiscoWorks Software**
- Choose **VPN/Security Management Solutions (VMS)**
- Choose **Evaluation Software VMS 90-day Eval**

The URL is included in the reference section. However, there are multiple logins and forms to be submitted. The drill-down method takes you through the appropriate steps smoothly.

I chose a stand-alone non-production Windows 2000 Advanced Server on which to install Cisco Security Agent. It only had 512 MB of RAM, half the recommended memory component. I couldn't add memory (no spare RAM to add), but Windows Installer allowed me to continue the installation after a notification of this weakness. The hard drive had plenty of available space.

The Windows member server did not have Service Pack 3 (SP3) installed, which is required to complete the installation. SP4 was located and installed. After a required reboot, I was able to resume the installation. Of course, I should have confirmed the SP3 before I started, but I was pleased to see that the installation routine was well written, checking on required components as the installation progressed.

A screen shot of the opening dialog box shows the CiscoWorks VMS components included in the install. I chose to install only the Common Services and the Cisco Security Agent Management Center. InstallShield insisted that they be installed separately and each required a system reboot to complete the process.

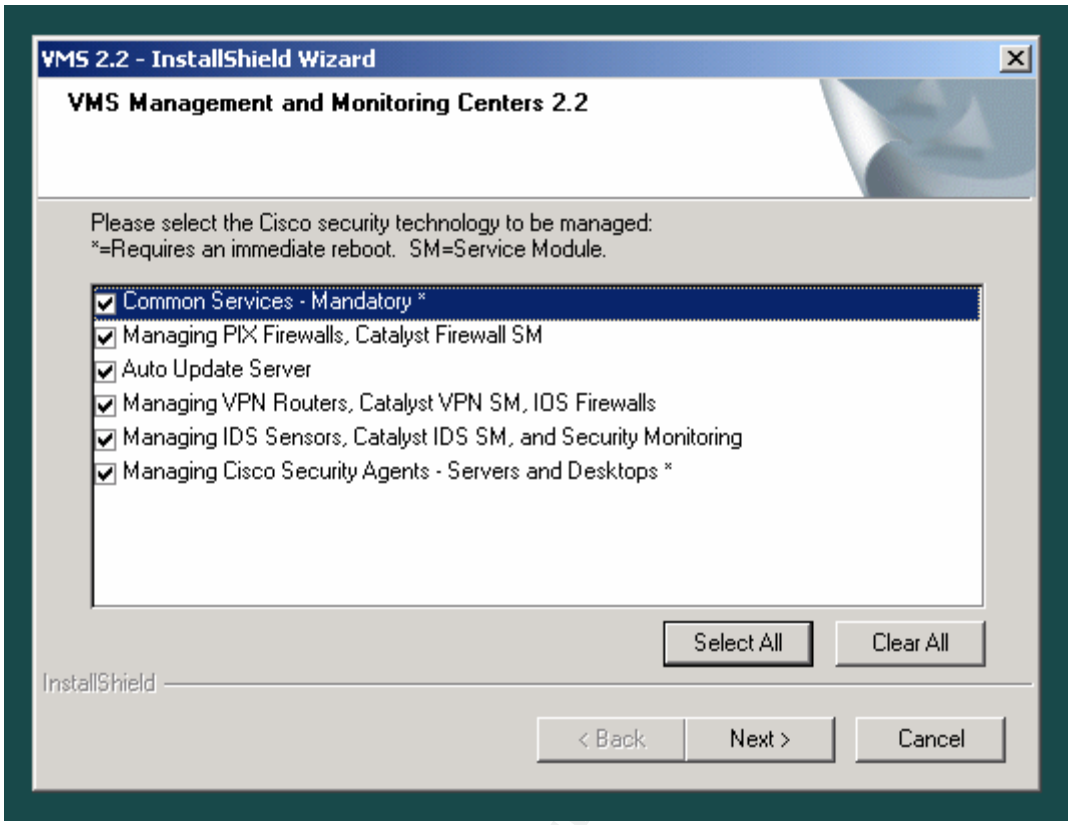

Figure 8 Cisco Security Agent installation selections – test lab environment

The installation routine enforces the primary installation of CiscoWorks Common Services v2.2. During this installation a subroutine checks the accuracy of the server's DNS configuration. There was a problem with my server's DNS configuration. The subroutine displayed an error message advising that I could correct the DNS error first or continue the installation and fix it later. I chose to continue and deal with the DNS issue(s) afterwards.

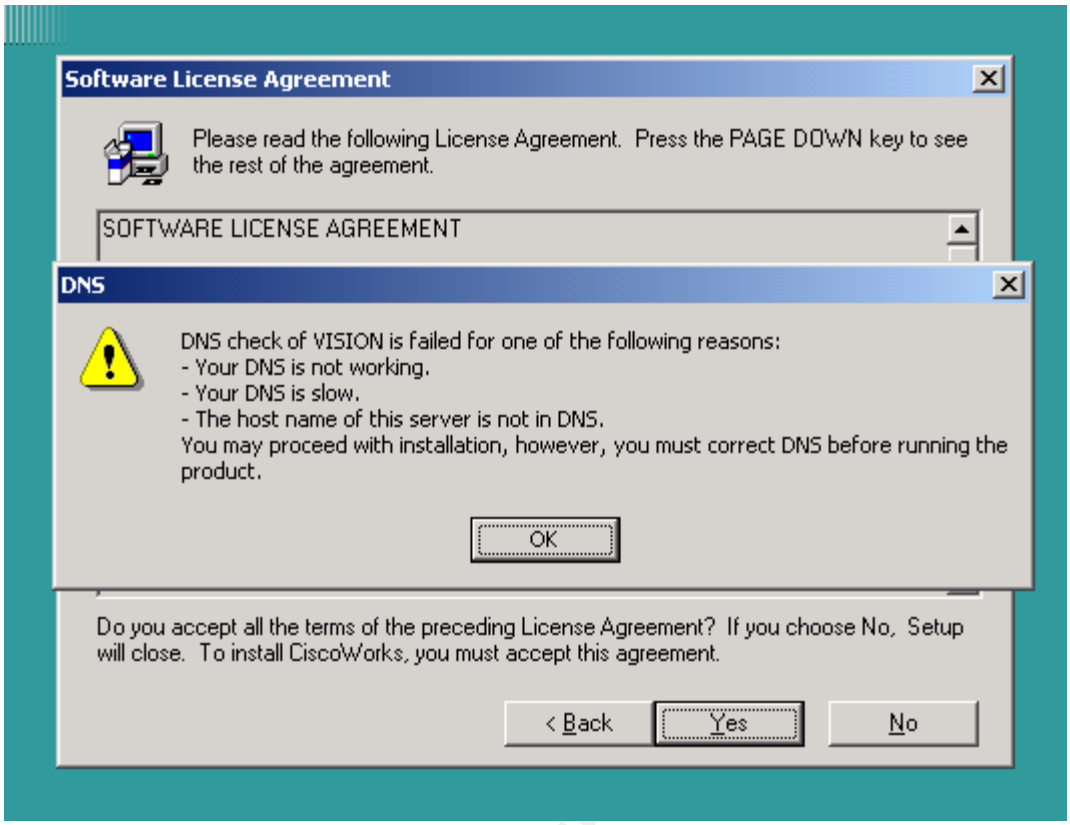

Figure 9 CSA installation: DNS error alert – test lab environment

In retrospect, to use the CSA Management Server Internet access must be "live". My DNS server was configured for a test environment and was not registered with Internet authorities. Therefore, the installation wizard could not resolve my DNS server with any DNS zones of authority. This may have caused the error condition. Once the installation was completed, I was able to experiment within my test environment.

SQL server was not installed on this server. The installation routine alerted me to that fact and requested that I choose to install the Microsoft SQL server Database Engine (MSDE) included with the Management Center software, which I did.

When the Cisco Security Agent Management Center installation concluded, two new entries appeared on the Programs list: Cisco Security Agent and CiscoWorks. The CSA Agent was the local intrusion detection and prevention agent software that is installed automatically on the Management Center. A red flag appeared in the system tray.

Opening the CiscoWorks program, the following window appeared:

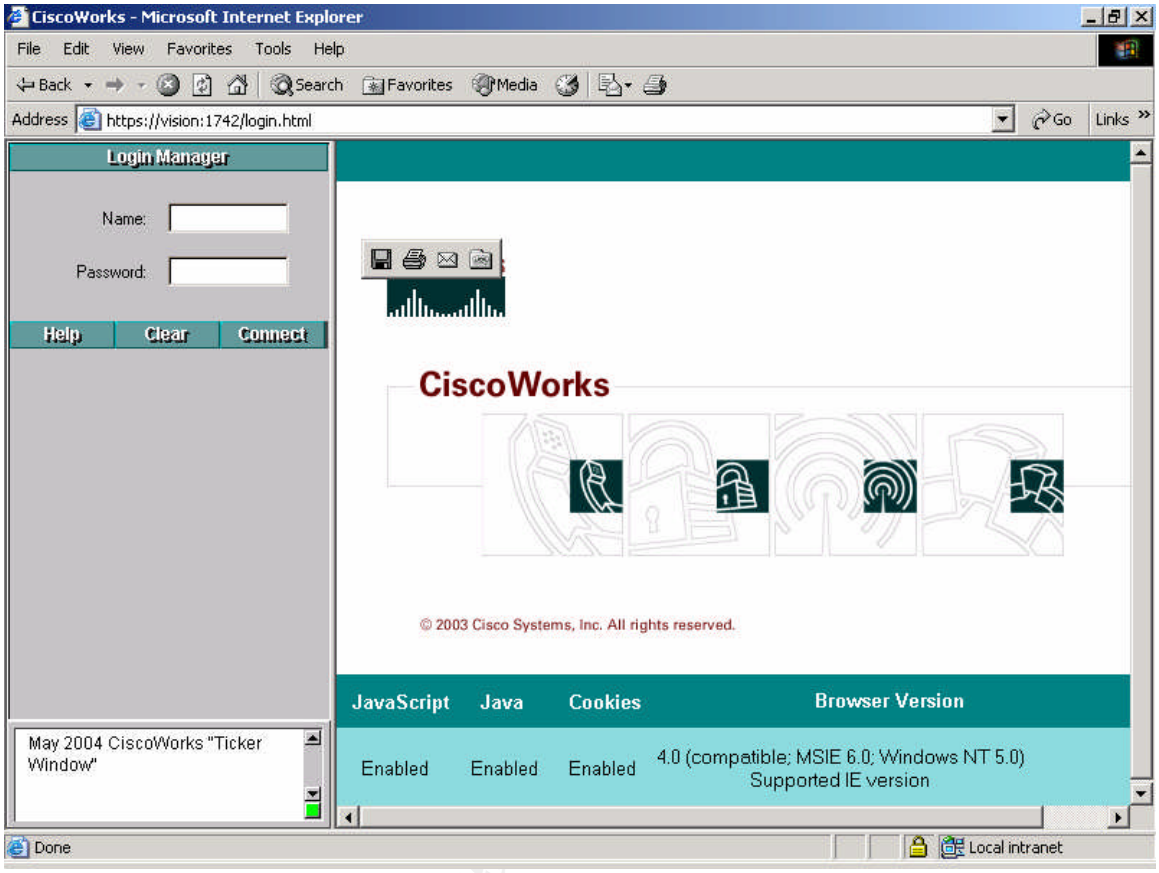

Figure 10 Launching CiscoWorks through Internet Explorer – test lab environment

The right panel shows Java, JavaScript and Cookies enabled. Also, an appropriate version of the IE browser was confirmed. Notice the URL uses SSL and a specified port number. “Vision” is the name of the server.

After the authenticated login the window changed to:

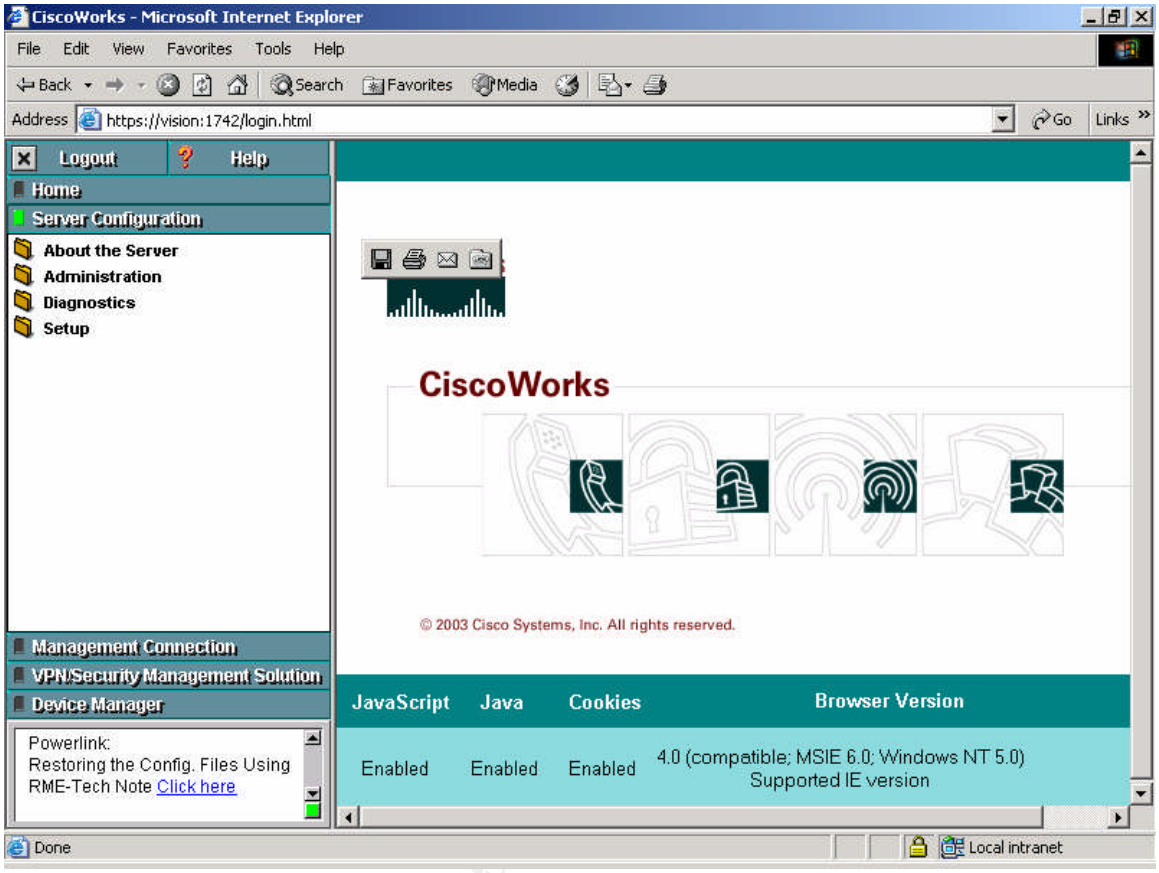

Figure 11 CiscoWorks with VPN/Security Management (CSA) components installed – test lab environment

The four drawers in the left pane control various configurations of the local CiscoWorks server and the CSA Management Center.

The VPN/Security Management Solution drawer manages the Agent kits:

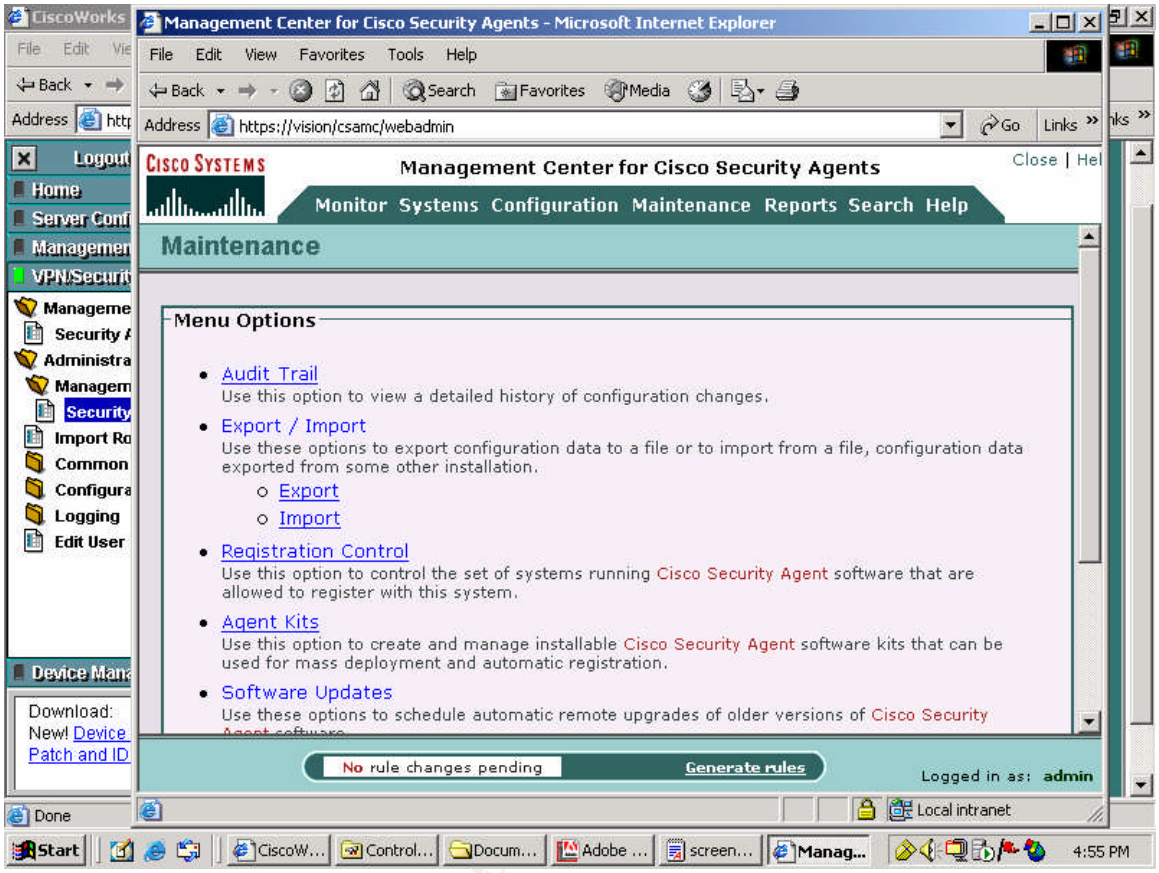

Figure 12 Create and manage Agent kits for CSA clients – test lab environment

Notice that this window also links to the controls, which register CSA-enabled network devices recognized by the Management Center (Registration Control).

Selecting the Agent kits link opens a window that lists the various agent kits for UNIX and Windows desktops and servers. Recall that the IDS Mode kits are only detection and notification applications, not intrusion prevention software.

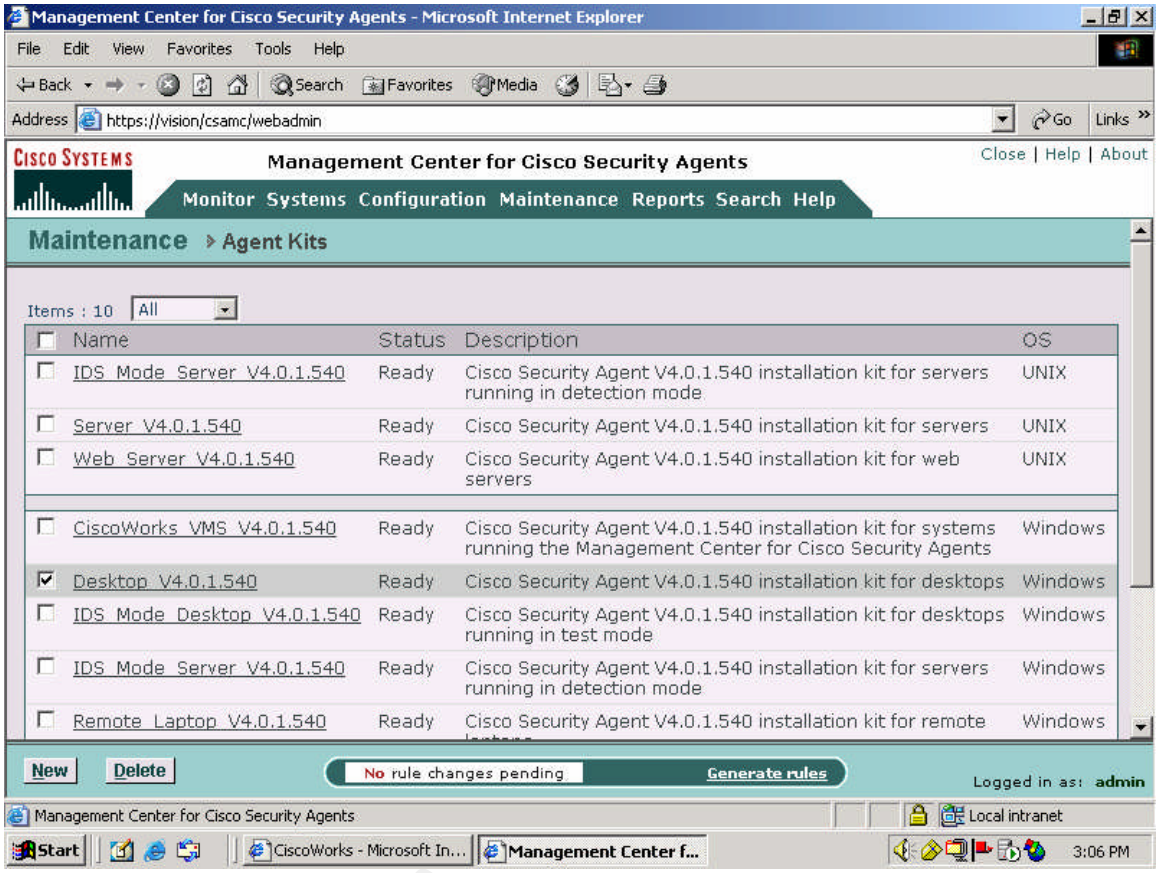

Figure 13 Default client Agent kits listed by OS type and client type – test lab environment

The default policies and rules, which are applied to servers, desktops and laptops through the kits, are designed to detect and prevent malicious behavior. Recall that the default policies require no initial configuration. Each policy set is configured to protect the specified hardware type, operating system, and typical installed applications.

SECTION VIII. CISCO SECURITY AGENT PROFILER

Some installed applications may be proprietary, programmed by the IT staff or purchased from a software design vendor for specific corporate use. In this case, the CSA administrator to protect the application can modify the default policies.

An alternate solution is to employ the Cisco Security Agent Profiler. "The Cisco Security Agent Profiler extends these security capabilities by automating analysis of the activities performed by particular applications and by building custom protective policies for these applications."[32]

An add-on to the CSA Management Center, the CSA Profiler is an analytical tool. It can be used to discover network information such as:

- Local and remote systems not protected by Cisco Security Agent software
- Which applications are resident on local and remote agent devices
- If these applications are approved applications or rogue applications
- Which of these applications have been run
- Any active reads or writes to registry keys
- What security protection systems are resident
- Which service packs, critical updates, or hot fixes have been applied

CSA Profiler can perform "forensics examination of any application on any computer."[33] Profiler thoroughly examines every aspect of the application's behavior, its interaction with the hardware, the network, the local operating system and the registry. It investigates alerts generated by the application and adds this information to the analysis. Profiler can then build a protection policy based on these observations.

The CSA MC can then apply this new policy to appropriate agent-enabled devices for intrusion protection and prevention.

SECTION IX. BEST PRACTICES

A search of the Internet produced only one White Paper targeting Best Practices for endpoint security, written by Cisco Systems, Inc. This paper observes that private data is commonly the target of malicious attack. As data is normally stored on servers and workstations within the core of the network, these endpoint devices require special attention for security protection.

Many factors contribute to the selection of a solution for endpoint security including corporate security requirements balanced by the need for ease of access to the data. Cisco Security Agent fulfills all the Best Practices.

The following factors are taken from Cisco's White Paper[34]. Paraphrased comments have been added as appropriate.

1. Real-time prevention decisions

   Policies deployed to the endpoints must detect and prevent malicious behavior immediately. A perceived attack must not be allowed to compromise the operating system or applications of the endpoint device.

2. Defense-in-depth protections from attacks

   Defense-in-depth is currently a common topic in network security discussions and papers. All five phases of the Lifecycle of Network System Attacks must be addressed in the design and implementation of a security policy. In a Windows-based network this includes prevention of anomalies caused by file system, network, registry, and COM component behavioral changes.

3. Real-time correlation at the agent and enterprise levels

   The ability to correlate events which appear to be benign by themselves but which aggregate to malicious activity is vital to behavior-based endpoint security.

4. Behavioral approach

   Policies deployed to network endpoints must be designed to detect abnormal behavior of applications and proactively prevent those effects on the device.

5. Flexibility to meet unique corporate needs

   Network security must be balanced by the needs of the corporation. An endpoint solution must be able to adapt to varying corporate network design.

6. Ease of deployment

   The endpoint security solution should contribute little overhead. Agents should generate alerts when appropriate but there should be minimal false positives. Web-based access allows ease of security management.

7. Centralized event management

   All endpoint alert logs should be collected centrally for ease of analysis. The solution should support standard collection mechanisms commonly integrated into corporate networks, e.g. SNMP.

8. Platform coverage

   Corporations often employ multiple hardware platforms with varying operating systems. Endpoint security must provide the flexibility to be deployed to workstations and servers as well as multiple operating systems on those devices.

9. Administration

   Many factors contribute to the selection of an endpoint security solution. Centralized management with access through a GUI interface is important

to many administrators. Remote management is also a favorable consideration. Ease of configuration and deployment of policies with low maintenance overhead are important factors as well. Corporate executives may consider the manpower investment, looking for solutions where a single IT manager might easily supervise thousands of devices.

SECTION X. CONCLUSION

The union of Cisco's endpoint security solution with Okena's StormWatch technology in May of 2003 gave birth to today's Cisco Security Agent and its Management Center. This behavior-based answer to anomalous attacks on endpoint servers and workstations provides ease of management and deployment through configurable policies.

The Cisco Security Agent Management Center is a component of CiscoWorks VPN/Security Management System (VMS) and resides on a Windows 2000 Server or Advanced Server. Agents reside on various Windows or Unix computers, servers or workstations. Configuration and management of the Agents is controlled through a secure Web browser and the Management Center.

Behavior-based rules are grouped into policies that are pulled by the Agent software from the Management Center's SQL database. These policies are designed to prevent persistence, propagation, and the paralysis of a corporate network through malicious attacks on endpoint devices.

IDS signatures are not required by CSA; there is no signature update race. Administrators can configure policies as newly discovered vulnerabilities warrant. Cisco Security Agent Profiler software can analyze application behavior and ancillary files to create appropriate mitigation policies.

When suspicious, anomalous behavior is detected, alerts are logged at the endpoint and the Management Center. The user may be notified of the alert and allowed to permit or deny the application activity. Malicious behavior is immediately denied.

Cisco Security Agent is designed to correlate seemingly random events, analyzing whether the pattern of activities produces abnormal behavior.

The IBM Corporation was so impressed with the Cisco Security Agent solution that, in February of 2004, they committed to employing CSA as a part of their corporate security policy: "In order to provide better control over access to networks, Cisco's security policy management technology will be merged with IBM's Tivoli network management software, beginning in March."[35]

FOOTNOTES

[1] Overview of Attack Threats. CERT Coordination Center. Carnegie-Mellon University. (5 May 2004) http://www.cert.org/archive/pdf/attack_trends.pdf

[2] "Essentials of Security". Microsoft Security Summit. Dallas, Texas (30 April 2004) http://www.microsoft.com/seminar/securitysummit/ittracks.mspx

[3] "Security at the Endpoint: Cisco Acquires Okena." News@Cisco: News Release. (11 March 2004) http://newsroom.cisco.com/dlls/hd_012403.html

[4] Lemos, Robert. "Cisco's security agent guards desktops" ZDNet UK. 20 May 2003. (17 February 2004) http://news.zdnet.co.uk/business/0,39020645,2134926,00.htm
and
Lemos, Robert. "Cisco to unveil security products" CNET News.com 19 May 2003. (17 February 2004) http://news.com.com/2100-1009_3-1007952.html

[5] "Cisco Systems to Acquire Okena, Inc.: Acquisition Extends Cisco's Network Security Portfolio with Next-Generation Endpoint Security Solution." News@Cisco: News Release. 24 January 2003. (11 March 2004) http://newsroom.cisco.com/dlls/corp_012403.html

[6] "Cisco Extends Leadership in Integrated Network Security". GRID today Vol. 2 No. 21. 26 May 2003. (17 February 2004) http://www.gridtoday.com/03/0526/101459.html

[7] Vulnerability Note VU#980499: Certain MIME types can cause Internet Explorer to execute arbitrary code when rendering HTML. US-CERT. 29 March 2001. (1 June 2004) http://www.kb.cert.org/vuls/id/980499

[8] Cert Advisory CA-2001-26 Nimda Worm. CERT/CC. 18 September 2001. (1 June 2004) http://www.cert.org/advisories/CA-2001-26.html

[9] Vulnerability Note VU#484891: Microsoft SQL Server 2000 contains stack buffer overflow in SQL Server Resolution Service. 24 July 2002. (1 June 2004) http://www.kb.cert.org/vuls/id/484891

[10] Cert Advisory CA-2003-04 MS-SQL Server Worm. CERT/CC. 27 January 2003. (1 June 2004) http://www.cert.org/advisories/CA-2003-04.html

[11] Vulnerability Note VU#568148: Microsoft Windows RPC vulnerable to buffer overflow. US-CERT. 16 July 2003. (1 June 2004) http://www.kb.cert.org/vuls/id/568148

[12] Cert Advisory CA-2003-20 W32/Blaster worm. CERT/CC. 11 August 2003. (1 June 2004) http://www.cert.org/advisories/CA-2003-20.html

[13] Vulnerability Note VU#753212: Microsoft LSA Service contains buffer overflow in DsRoleInitializeLog() function. US-CERT. 13 April 2004. (1 June 2004) http://www.kb.cert.org/vuls/id/753212

[14] US-CERT Current Activity: W32/Sasser. 1 May 2004. (1 June 2004) http://www.us-cert.gov/current/#sasser

[15] Securing Network Endpoints Without Signatures: A Policy-Based Approach to Host Intrusion **Protection.** White Paper. p. 4 (16 March 2004) http://cisco.com/application/pdf/en/us/guest/products/ps5057/c1244/cdccont_0900aecd800ae55e.pdf

and

"Product Overview: What the Cisco Security Agent Does". Using Management Center for Cisco Security Agents. Chapter 1. p. 2 Cisco Systems, Inc. (16 March 2004) http://www.cisco.com/univercd/cc/td/doc/product/vpn/ciscosec/csa/40/vmsug.pdf

[16] Securing Network Endpoints Without Signatures: A Policy-Based Approach to Host Intrusion **Protection.** White Paper. (16 March 2004) http://cisco.com/application/pdf/en/us/guest/products/ps5057/c1244/cdccont_0900aecd800ae55e.pdf

[17] Security Products: Network Based Intrusion Prevention: Cisco IDS 4200 Series Sensors. The Northstar Group. (17 February 2004) http://www.nstargroup.com/security/security_products.htm

[18] Bosey, Jr., Teddy. Cisco HIPS: Cisco's Host-based Intrusion Prevention System (HIPS). DFW Cisco User's Group Meeting. 07/02/2003. (1 June 2004) http://cisco-users.org/past_meetings.htm

and

"Using System Correlation Rules". Using Management Center for Cisco Security Agents. Chapter 5. Cisco Systems, Inc. (16 March 2004) http://www.cisco.com/univercd/cc/td/doc/product/vpn/ciscosec/csa/40/vmsug.pdf

[19] "Preparing to Install: How the Cisco Security Agent Works". Installing Management Center for Cisco Security Agents. Chapter 1. p. 2 Cisco Systems, Inc. (16 March 2004) http://www.cisco.com/univercd/cc/td/doc/product/vpn/ciscosec/csa/40/index.htm

[20] CiscoWorks Management Center for Cisco Security Center. Cisco Systems, Inc. (11 March 2004) http://www.cisco.com/en/US/products/sw/cscowork/ps5212/index.html

[21] "Preparing to Install: How the Cisco Security Agent Works". Installing Management Center for Cisco Security Agents. Chapter 1. p. 3. Cisco Systems, Inc. (16 March 2004) http://www.cisco.com/univercd/cc/td/doc/product/vpn/ciscosec/csa/40/index.htm

[22] Cisco Security **Agent.** Data Sheet. p. 4. Cisco Systems, Inc. (15 March 2004) http://cisco.com/application/pdf/en/us/guest/products/ps5057/c1650/cdccont_0900aecd800ade37.pdf

[23] Cisco Security **Agent.** Data Sheet. p. 4. Cisco Systems, Inc. (15 March 2004) http://cisco.com/application/pdf/en/us/guest/products/ps5057/c1650/cdccont_0900aecd800ade37.pdf

[24] "Event Logging and Alerts". Using Management Center for Cisco Security Agents Chapter 8. Cisco Systems, Inc. (16 March 2004) http://www.cisco.com/univercd/cc/td/doc/product/vpn/ciscosec/csa/40/vmsug.pdf

[25] CiscoWorks Management Center for Cisco Security Center. Cisco Systems, Inc. (11 March 2004) http://www.cisco.com/en/US/products/sw/cscowork/ps5212/index.html

[26] Securing Network Endpoints Without Signatures: A Policy-Based Approach to Host Intrusion **Protection.** White Paper. (16 March 2004) http://cisco.com/application/pdf/en/us/guest/products/ps5057/c1244/cdccont_0900aecd800ae55e.pdf
and
Threat Management: Intrusion Protection Systems (IDS): Intrusion Prevention: Security Without Signatures. ConQwest, Inc. (17 February 2004) http://www.conqwest.com/solutions_cisco.asp
and
Bosey, Jr., Teddy. Cisco HIPS: Cisco's Host-based Intrusion Prevention System (HIPS). DFW Cisco User's Group Meeting. 07/02/2003. (1 June 2004) http://cisco-users.org/past_meetings.htm

[27] "Cisco Systems to Acquire Okena, Inc.: Acquisition Extends Cisco's Network Security Portfolio with Next-Generation Endpoint Security Solution." News@Cisco: News Release. 24 January 2003. (11 March 2004) http://newsroom.cisco.com/dlls/corp_012403.html

[28] Rules in Okena StormWatch. Cisco Systems, Inc. (15 March 2004) http://www.cisco.com/univercd/cc/td/doc/product/vpn/ciscosec/csa/21/rules.pdf

[29] StormWatch: Policies for the Default Desktops Group. Cisco Systems, Inc. (15 March 2004) http://www.cisco.com/univercd/cc/td/doc/product/vpn/ciscosec/csa/21/ddesk21.pdf

[30] StormWatch: Policies for the Default Servers Group. Cisco Systems, Inc. (15 March 2004) http://www.cisco.com/univercd/cc/td/doc/product/vpn/ciscosec/csa/21/dsrvr21.pdf

[31] CiscoWorks Management Center for Cisco Security Center. Cisco Systems, Inc. (11 March 2004) http://www.cisco.com/en/US/products/sw/cscowork/ps5212/index.html

[32] Cisco **Security** Agent Profiler. Data Sheet. Cisco Systems, Inc. (15 March 2004) http://cisco.com/application/pdf/en/us/guest/products/ps5057/c1650/cdccont_0900aecd800ade2a.pdf

[33] Cisco Security Agent with Intrusion **Protection** for Remote Corporate Users. White Paper. Cisco Systems, Inc. (16 March 2004) http://www.cisco.com/application/pdf/en/us/guest/products/ps5057/c1244/cdccont_0900aecd800ae54b.pdf

[34] Technology Best Practices for **Endpoint** Security. White Paper. Pp. 1-3. (16 March 2004) http://www.cisco.com/application/pdf/en/us/guest/products/ps5057/c1244/cdccont_0900aecd800ade42.pdf

[35] Reardon, Marguerite. "Cisco, IBM ally on security defenses" CNET News.com. 13 February 2004. (17 February 2004) http://zdnet.com.com/2100-1103_2-5158689.html?tag=tu.scblog.6584

REFERENCES

Bosey, Jr., Teddy. Cisco HIPS: Cisco's Host-based Intrusion Prevention System (HIPS). DFW Cisco User's Group Meeting. 07/02/2003. http://cisco-users.org/past_meetings.htm (1 June 2004).

"Building Policies". Using Management Center for Cisco Security Agents. Chapter 4. Cisco Systems, Inc. http://www.cisco.com/univercd/cc/td/doc/product/vpn/ciscosec/csa/40/vmsug.pdf (16 March 2004).

Cert Advisory CA-2001-26 Nimda Worm. CERT/CC. 18 September 2001. http://www.cert.org/advisories/CA-2001-26.html (1 June 2004).

Cert Advisory CA-2003-04 MS-SQL Server Worm. CERT/CC. 27 January 2003. http://www.cert.org/advisories/CA-2003-04.html (1 June 2004).

Cert Advisory CA-2003-20 W32/Blaster worm. CERT/CC. 11 August 2003. http://www.cert.org/advisories/CA-2003-20.html (1 June 2004).

"Cisco Extends Leadership in Integrated Network Security" ITSecurity.com. 21 May 2003. http://itsecurity.com/tecsnews/may2003/may201.htm (17 February 2004).

"Cisco Extends Leadership in Integrated Network Security". GRID today Vol. 2 No. 21. 26 May 2003. http://www.gridtoday.com/03/0526/101459.html (17 February 2004).

"Cisco Extends Leadership in Integrated Network Security; New Management, Performance, and Scalability Extensions Enhance and Protect Business Productivity" News@Cisco: News Release. 20 May 2003. http://newsroom.cisco.com/dlls/prod_052003d.html (11 March 2004).

Cisco Security **Agent.** Data Sheet. Cisco Systems, Inc. http://cisco.com/application/pdf/en/us/guest/products/ps5057/c1650/cdccont_0900aecd800ade37.pdf (15 March 2004).

Cisco Security Agent Product Literature http://www.cisco.com/en/US/products/sw/secursw/ps5057/index.html (17 February 2004).

Cisco **Security** Agent Profiler. Data Sheet. Cisco Systems, Inc. http://cisco.com/application/pdf/en/us/guest/products/ps5057/c1650/cdccont_0900aecd800ade2a.pdf (15 March 2004).

Cisco Security Agent. Q & A. Cisco Systems, Inc. http://www.cisco.com/warp/public/cc/pd/nemnsw/callmn/prodlit/segag_qa.htm (10 April 2004).

Cisco Security Agent **ROI**: Deploying Intrusion Protection Agents on the Endpoint White Paper. Cisco Systems, Inc. http://cisco.com/application/pdf/en/us/guest/products/ps5057/c1244/cdccont_0900aecd800ae983.pdf (15 March 2004).

Cisco Security Agent **V4.0**. Evaluation Guide. Cisco Systems, Inc. http://cisco.com/application/pdf/en/us/guest/products/ps5057/c1031/cdccont_0900aecd800ae985.pdf (16 March 2004).

Cisco Security Agent with Intrusion **Protection** for Remote Corporate Users. White Paper. Cisco Systems, Inc. http://www.cisco.com/application/pdf/en/us/guest/products/ps5057/c1244/cdccont_0900aecd800ae54b.pdf (16 March 2004).

"Cisco Systems to Acquire Okena, Inc.: Acquisition Extends Cisco's Network Security Portfolio with Next-Generation Endpoint Security Solution." News@Cisco: News Release. 24 January 2003. http://newsroom.cisco.com/dlls/corp_012403.html (11 March 2004).

CiscoWorks VMS 90-day evaluation version. Cisco Systems, Inc. http://www.cisco.com/kobayashi/sw-center/cw2000/vms-planner.shtml (1 May 2004).

CiscoWorks Management Center for Cisco Security Agents. Cisco Systems, Inc. http://www.cisco.com/warp/public/cc/pd/wr2k/csav4/index.shtml (16 March 2004).

CiscoWorks Management Center for Cisco Security Center. Cisco Systems, Inc. http://www.cisco.com/en/US/products/sw/cscowork/ps5212/index.html (11 March 2004).

"Essentials of Security". Microsoft Security Summit. Dallas, Texas http://www.microsoft.com/seminar/securitysummit/ittracks.mspx (30 April 2004).

"Event Logging and Alerts". Using Management Center for Cisco Security Agents. Chapter 8. Cisco Systems, Inc. http://www.cisco.com/univercd/cc/td/doc/product/vpn/ciscosec/csa/40/vmsug.pdf (16 March 2004).

Lemos, Robert. "Cisco to unveil security products" CNET News.com 19 May 2003. http://news.com.com/2100-1009_3-1007952.html (17 February 2004).

Lemos, Robert. "Cisco's security agent guards desktops" ZDNet UK. 20 May 2003. http://news.zdnet.co.uk/business/0,39020645,2134926,00.htm (17 February 2004).

Otteson, Gail Meredith. "A Winning Game Plan: Best Practices for End-to-End Defense in Depth" Packet – Cisco Systems Users Magazine First Quarter 2004: 29-35.

Overview of Attack Threats. CERT Coordination Center. Carnegie-Mellon University. http://www.cert.org/archive/pdf/attack_trends.pdf (5 May 2004).

"Preparing to Install: How the Cisco Security Agent Works". Installing Management Center for Cisco Security Agents. Chapter 1. Cisco Systems, Inc. http://www.cisco.com/univercd/cc/td/doc/product/vpn/ciscosec/csa/40/index.htm (16 March 2004).

"Product Overview: What the Cisco Security Agent Does". Using Management Center for Cisco Security Agents. Chapter 1. Cisco Systems, Inc. http://www.cisco.com/univercd/cc/td/doc/product/vpn/ciscosec/csa/40/vmsug.pdf (16 March 2004).

Raider, Rhonda Heldman. "The Self-Defending Network: Faster Spreading, more malevolent network threats demand new security strategies and technologies" Packet – Cisco Systems Users Magazine First Quarter 2004: 24-28.

Reardon, Marguerite. "Cisco, IBM ally on security defenses" CNET News.com. 13 February 2004. http://zdnet.com.com/2100-1103_2-5158689.html?tag=tu.scblog.6584 (17 February 2004).

Rules in Okena StormWatch. Cisco Systems, Inc. http://www.cisco.com/univercd/cc/td/doc/product/vpn/ciscosec/csa/21/rules.pdf (15 March 2004).

Securing Network Endpoints Without Signatures: A Policy-Based Approach to Host Intrusion **Protection.** White Paper. http://cisco.com/application/pdf/en/us/guest/products/ps5057/c1244/cdccont_0900aecd800ae55e.pdf (16 March 2004).

"Security at the Endpoint: Cisco Acquires Okena." News@Cisco: News Release. http://newsroom.cisco.com/dlls/hd_012403.html (11 March 2004).

Security Products: Network Based Intrusion Prevention: Cisco IDS 4200 Series Sensors. The Northstar Group. http://www.nstargroup.com/security/security_products.htm (17 February 2004).

StormWatch: Policies for the Default Desktops Group. Cisco Systems, Inc. http://www.cisco.com/univercd/cc/td/doc/product/vpn/ciscosec/csa/21/ddesk21.pdf (15 March 2004).

StormWatch: Policies for the Default Servers Group. Cisco Systems, Inc. http://www.cisco.com/univercd/cc/td/doc/product/vpn/ciscosec/csa/21/dsrvr21.pdf (15 March 2004).

Technology Best Practices for **Endpoint** Security. White Paper. http://www.cisco.com/application/pdf/en/us/guest/products/ps5057/c1244/cdccont_0900aecd800ade42.pdf (16 March 2004).

Threat Management: Intrusion Protection Systems (IDS): Intrusion Prevention: Security Without Signatures. ConQwest, Inc. http://www.conqwest.com/solutions_cisco.asp (17 February 2004).

US-CERT Current Activity: W32/Sasser. 1 May 2004. http://www.us-cert.gov/current/#sasser (1 June 2004).

"Using System Correlation Rules". Using Management Center for Cisco Security Agents. Chapter 5. Cisco Systems, Inc. http://www.cisco.com/univercd/cc/td/doc/product/vpn/ciscosec/csa/40/vmsug.pdf (16 March 2004).

Vulnerability Note VU#484891: Microsoft SQL Server 2000 contains stack buffer overflow in SQL Server Resolution Service. 24 July 2002. http://www.kb.cert.org/vuls/id/484891 (1 June 2004).

Vulnerability Note VU#568148: Microsoft Windows RPC vulnerable to buffer overflow. US-CERT. 16 July 2003. http://www.kb.cert.org/vuls/id/568148 (1 June 2004).

Vulnerability Note VU#753212: Microsoft LSA Service contains buffer overflow in DsRoleInitializeLog() function. US-CERT. 13 April 2004. http://www.kb.cert.org/vuls/id/753212 (1 June 2004).

Vulnerability Note VU#980499: Certain MIME types can cause Internet Explorer to execute arbitrary code when rendering HTML. US-CERT. 29 March 2001. http://www.kb.cert.org/vuls/id/980499 (1 June 2004).