



WHITE PAPER

CISCO SECURITY AGENT DEPLOYMENT BEST PRACTICES GUIDE

INTRODUCTION

The Cisco® Security Agent (SA) provides endpoint server and desktop protection against new and emerging threats due to malicious network activity. Cisco SA identifies and prevents malicious behavior resulting in the elimination of known and unknown, or “Day Zero”, network threats. The Cisco Security Agent provides for the aggregation and extension of multiple endpoint security functions by providing intrusion prevention and distributed firewall capabilities in addition to malicious mobile code protection, system integrity assurance and audit log consolidation. All of these capabilities are based on a successful deployment of the Cisco Security Agent throughout the network as well as configuring and managing the agents through the Cisco SA Management Center (SAMC).

In order to achieve a successful enterprise-wide deployment of the Cisco Security Agent it is first necessary to have a solid background in the operational functions of Cisco SA. This information can be obtained by consulting the following documentation:

- Using Management Center for Cisco Security Agents
- Installing Management Center for Cisco Security Agents

In addition to the above documentation a successful deployment can be enhanced by one or both of the following:

- Attendance at a Cisco SA administrator training (a 2-day course offered by Cisco training partners)
- Consultation with your Cisco partner or Cisco Security Services group if your company does not have the internal technical resources for deployment (your Cisco partner must also have completed authorized training)

The focus of this document is to outline some of the best practices involved in an enterprise-wide deployment of the Cisco Security Agent. While this document will be useful in preparation for deployment, it does not replace the following requirements which are imperative to a successful agent implementation:

- Thorough reading of the Using Management Center for Cisco Security Agents and Installing Management Center for Cisco Security Agents (Product documentation that accompanies product media)

This document is broken into several sections:

- Overview of the deployment process
- Detailed deployment best practices using default policies (All customers should start their deployments using default policies in test mode; optionally, after the test mode period is complete a subset of the default policy can be used in a protection mode while the rest of the policy is still in test mode. While this leaves the systems vulnerable to some attacks it also provides for the ability to turn the full protection on at a moments notice while full testing in the production enterprise environment is completed)
- Detailed deployment best practices using customer built policies (Certain customers may wish to make their environments extremely restrictive. We recommend this only after successful implementation starting from default policies has been achieved)

DEPLOYMENT OVERVIEW

Every network environment provides its own challenges and pitfalls when deploying a new security tool suite. To overcome such challenges a sound implementation plan is necessary when first deploy a new security tool. Network and security best practice procedures stress that any new software or tool to be deployed across a network should be first deployed in a test network. Ideally this test network would include a sample of the systems available in the production network. This then provides the network engineers and security staff the ability to gauge the effects of the new software on the production systems without actually affecting those systems. While this may not prove feasible in many smaller networks it is still recommended, at some level, in order for the security and network staff to gain valuable training and experience with the new software or tool.

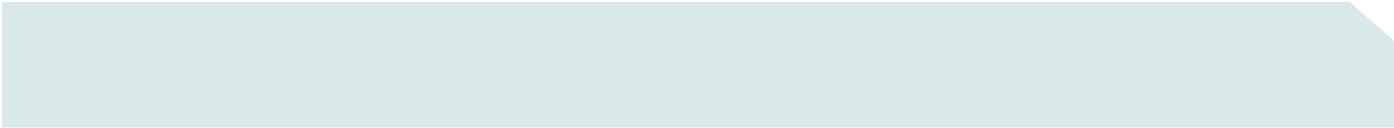
As in the case of deploying any new software product, software patch or system on a network the deployment of the Cisco Security Agent requires up-front planning, time, and a willingness to work through possibly several iterations before a final, satisfactory deployment can be implemented. The steps required to successfully deploy the Cisco SA software throughout a network include the following:

- Install the Cisco SA Management Center
- Identify the Cisco SA deployment model to be used:
 - Complete
 - Desktop Systems Only
 - Servers only
 - All servers plus select desktops/laptops
 - Select servers plus select desktops/laptops
 - Select servers only
- Identify the deployment stages
- Build a test deployment network and deploy Cisco SA in accordance with the deployment type
- Tune the Cisco SA deployment on the test network
- Deploy Cisco SA, in stages, in the production environment in accordance with the deployment model devised in the test environment
- Monitor the deployment stages and tune accordingly

The remainder of this document discusses each of the above stages in more detail. The reader should use this document as a guide in the deployment of the Cisco Security Agent software on the network.

INSTALL THE CISCO SA MANAGEMENT CENTER

The Cisco SA Management Center (SAMC) is part of the CiscoWorks VPN and Security Management Solution (VMS) software bundle. The Cisco SAMC can be installed on a Windows 2000 Server or Windows 2000 Advanced Server only at the time of this writing. In brief, the Cisco SAMC provides a central distribution location of the Cisco SA agent kits to endpoint systems as well as a policy update site and an alarm console. The Cisco SAMC host should ideally be located in the management module of the network with other management hosts such as the authentication servers, syslog servers, and other designated management hosts. Communication between the Cisco SAMC and the agents is done over HTTP and HTTPS. The agents communicate with the MC over port TCP/5401 with a fallback to TCP/443 if TCP/5401 is not available. The Cisco SA Profiler uses port TCP/5401 to communicate with the SAMC. The Cisco SAMC uses either a Microsoft SQL Server database (for large installations) or the Microsoft SQL Server Desktop Engine (MSDE, for smaller installations) as the central repository of the various policies that can be applied to different agents across an enterprise as well as a central location where alarms are aggregated and information correlated and displayed. In addition to the Cisco SAMC, the alarms can also be sent to the CiscoWorks Security Information



Management Solutions (SIM) console. Additionally the MC is a central point where endpoint clients can download the agent installation kits. The Cisco SA Management Console system hardware must be sized appropriately to the deployment considered. An underpowered system can become a bottleneck in the deployment and operation of the Cisco Security Agent software. This host represents a nexus in the deployment model of the CSA software. It should be reachable by all hosts running Cisco SA. The current version of Cisco SAMC is capable of managing up to 10,000 agents deployed across an enterprise. If there are more agents than this then additional MCs will be required to handle to additional agents.

IDENTIFY THE CISCO SA DEPLOYMENT MODEL

The Cisco SA software can be deployed across both user desktop systems as well as servers. This results in several possible deployment models across a network. The following sections will detail these deployment models as well as provide the pros and cons of the models. It is up to the network administration personnel as well as management to determine which model is best for the network under consideration.

Select Servers Only

In the Select Servers Only model the Cisco SA software is deployed on selected servers such as Internet-facing web servers, DNS servers, database systems and other “critical” systems. This provides endpoint protection on systems deemed to provide essential, network-related services.

Servers Only

This model provides for the deployment of Cisco SA on all servers both inside the corporate LAN as well as those in a DMZ. This model calls for the deployment of Cisco SA on both business-critical as well as non-critical systems. The primary advantage to this model is the coverage provided on all server systems that Cisco SA can be deployed.

Select Servers plus Select Desktop Systems

In this deployment model the Cisco SA server is deployed on selected servers such as Internet-facing web servers, DNS hosts, database systems, and other “critical” systems. Additionally Cisco SA is deployed on a select group of desktop systems. These could be systems such as those hosts that are used by employees in the corporate finance department, Human Resources, or other departmental employees who handle sensitive and potentially confidential data. Another possible group of desktop systems that Cisco SA could be deployed on is the laptops of the account managers and other individuals who transit from the internal corporate LAN to other computing environments.

Servers plus Select Desktop Systems

This deployment model provides for the installment of Cisco SA across all corporate servers, not just business-critical ones, as well as a group of desktop systems as discussed in the Select Servers plus Select Desktop Systems deployment model above.

Desktop Systems Only

In this model, Cisco SA is deployed on all end-user system platforms. Servers are not included due to the fact that they are directly under the control of the IT/Infosec staff, they are much fewer in number and they are closely monitored, maintained and patched. The end-user desktops are more numerous and provide a variety of uses for the end-users. Additionally viruses typically require the interaction of a user and may be the primary threat that requires mitigation on these systems. Other threats could be Trojan programs that an attacker could use to gather user account information. The primary advantage to this model is the level of coverage that it provides.

Complete

In this model, Cisco SA is deployed on all supported platforms. All supported servers and desktops have a Cisco SA agent installed to protect it. The primary advantage to this model includes the level of coverage.

IDENTIFY THE DEPLOYMENT STAGES

In many cases the deployment stages are determined by the size of the network where the Cisco SA software will be used. Smaller networks may be deployed in one stage where the Cisco SA agent kits are downloaded and installed within a short period of time. Larger networks may be divided into multiple deployment stages where deployment is done based on departmental organization. This provides the network staff with the maximum amount of flexibility in deploying the Cisco SA software in a “limited” environment and then monitoring and adjusting the agents and the policies on a per-environment basis. In either case the deployment of the Cisco SA software should follow the general model below:

BUILD A TEST DEPLOYMENT

Once the deployment model has been chosen the next step is to build a test deployment. The test deployment provides for several objectives:

1. Providing the network and security staff with vital experience in the installation and operation of the Cisco SAMC
2. To provide a controlled environment with sample systems that can be used to test the deployment model
3. To provide a controlled environment wherein the Cisco SA software can be deployed on systems, tuned accordingly and any implementation issues resolved before full deployment in the production environment
4. To provide the network and security staff with valuable experience in the deployment and troubleshooting of the Cisco SA software system
5. Providing an environment to determine how to best manage event logs
6. Providing a controlled environment where the security staff can run network scanners and exploits on systems with Cisco SA to be able to gain experience in the types of alarms raised by the software and how to interpret them

While it is possible to completely bypass the test deployment stage, it is critical that Cisco SA be deployed in a test environment before being deployed in a production environment. This provides the network administration staff as well as the security staff the opportunity to gain experience with the installation and the operation of the software as well as potential problem areas. Additionally, it will help uncover possible conflicts between existing security measures and Cisco SA. By utilizing a test model first, the level of success of the Cisco SA deployment in the production environment is improved immensely.

If a test environment is not available it is still possible to test the effects of the Cisco SA software by using VMware. VMware provides for the creation of “Virtual Systems” on a single host by providing an abstraction layer wherein the operating system believes it is executing on dedicated hardware but is actually executing in a virtual environment. Utilizing VMware can significantly help in testing the effects of the Cisco Security Agent on various systems without incurring significant costs in physical hardware.

It is also possible to test the effects of the Cisco Security Agent on the selected target hosts in the network by choosing a group of systems representing a cross-section of application hosts on the network as pilot systems for the deployment. This subgroup of hosts can provide a test-production environment in which the Cisco SA software can be deployed and evaluated without impacting the overall production environment.

TUNING CISCO SA ON THE TEST DEPLOYMENT

Implementing the Default Policies of Cisco Security Agent

When deploying Cisco SA in the test deployment it is best to use default Cisco SA policies for operating system protection in order to develop a customized policy that provides basic operating system protection of servers. The default Cisco SA policies have stopped all new and unknown attacks like Nimda and Blaster.

Test deployment systems should be selected based on the following guidelines:

- At least one test system should be included per each application environment.
- The test systems should be a representative sample of the production systems.
- Whenever possible, include quality assurance servers as well as production servers. Use QA servers to ensure no negative impact from Cisco SA agent software installation.

Create one group, in test mode, for each type of application environment that needs to be protected. An application environment is comprised of a standard configuration of operating system plus a supporting suite of applications. Some examples could potentially include:

- Sales desktop configurations
- E-Business application servers
- Backend database servers

In test mode, the Cisco SA agent will not deny any action even if an associated policy indicates it should be denied, all actions will be logged instead. Test mode helps the engineers and administrators understand the impact of deploying a policy on a host before enforcing it. This is a critical step for ensuring no negative impact to the protected application environments.

Before proceeding with the test deployment it is recommended that the security staff reviews the default Cisco SA policies to determine which ones better meet the security requirements for the solution. The default operating system policy is the best starting point for policy development. In addition, Cisco SA comes with additional default policies tailored to specific application environments such as dedicated Microsoft IIS and SQL servers. These application specific policies are templates which should be used to secure servers that are dedicated to these applications.

When requirements are met by default policies, it is considered a best practice to apply both the operating system protection and the more specific default policy (for example, Dedicated IIS server) to the appropriate group(s). The default policies and groups that come with Cisco SA should never be modified. Always make a copy of default policies and groups and name the copy appropriately (for example, TEST-SALES-DESKTOPS for creating a group, in test-mode, which contains sales desktops).

Build Cisco SA agent installation kits to support the data collection process that is required to fine-tune the Cisco SA default policies. The agent kits should only install the network shim on systems needing this functionality (for example, port scan detection, SYN flood protection, malformed packet detection, etc.). If the protected systems have VPN or firewall protection the network shim feature might not be needed. Once the agent kits are prepared for deployment in the test environment they can be distributed to the appropriate systems either by having those systems contact the Cisco SAMC over the network and downloading the kits or by being “pushed” through system management software to the target systems.

Once all of the agent kits are deployed the next step in the test deployment phase is to perform a full test of the application or host functionality in a test environment (if available). This will generate all the application-specific data needed to tune the default policies for each application environment.

In parallel with the test deployment effort, it is recommended that data be collected on all pilot systems that are in production environments. This will help identify rules that might have a negative impact on production as well as QA environments. Provide a *minimum* of two to four

weeks of data collection on production systems depending on the size of the deployment. Make sure the system administrator verifies that all the appropriate scripts and software—needed to support operations—run during the data collection period. This could potentially include:

- System Backups
- Network Management Software
- System Scheduler

After the data collection process is finalized on the QA server, analyze the data to identify policy rules that would have (if applied in protection mode) a negative impact to the application environment.

Once it is determined which rules would have a negative impact on the target systems, the tuning wizard can be used to modify the policy or policies applied by creating “allow rules” for the appropriate actions. The tuning wizard can be used to change the action of a rule that triggered a negative impact. The wizard will automatically generate an “exception” allow rule which takes the application class and resource information in the event and creates an allow rule to counteract the rule that caused the deny action.

It is important to organize the exception rules appropriately. Organize the exception rules as follows:

- Create an enterprise exception policy to include allow rules that are required on all protected systems. Add all enterprise-wide exception rules to this policy.
- Create one exception policy for each group. The group exception policy will include all allow rules that apply to that specific group.

Once all the appropriate exception policies are finalized, apply these policies to their respective groups and perform another round of data collection and tuning.

After the second round of Policy tuning, you should be confident about the non-intrusiveness (to legitimate behavior) of the rules. Enable protection mode on the pilot systems, one group at a time. Execute the additional components of the test plan (security testing, performance, operations) on each group to ensure the solution works as expected.

In summary, the following steps should be used for each Cisco SA group when deploying the agent kits in an application environment:

1. Deploy Cisco SA Agent in test-mode on all target systems
2. Perform data collection and policy tuning (as needed)
3. Enable protection mode
4. Work with security, operations, and engineering to ensure they are comfortable with the deployment

DEPLOYING CISCO SA IN A PRODUCTION ENVIRONMENT

Once the impact of the Cisco SA software can be determined in the test deployment (or the pilot deployment in the production environment), the next step is the deployment of the software across the entire production environment. This can be accomplished in one of two ways:

- A staged distribution in the production environment, or
- A single, full distribution

A staged distribution in the production environment is recommended as the better method of achieving the deployment as it provides for the capability of breaking the deployment into manageable parts. The production environment deployment can be done based on several characteristics (in order of preference):

- System network role (database servers, application servers, web servers, etc.)
- Network IP address blocks
- System physical location

The preferable method would be to deploy the Cisco SA across systems as a group based on their network roles. This allows for the ability to deploy the agent kits on similar systems and deal with similar issues that may arise unexpectedly at one time. The deployment of the Cisco SA software in each stage should be done with the appropriate policies set to the test mode as was done in the test or pilot environment. While this may appear to be unnecessarily duplicative it will allow for the ability to monitor any issues that may arise due to the deployment of the Cisco SA software in the production environment. Once each group of systems has been installed with the Cisco SA agent for a short period of time, deny actions can be activated where applicable in the policy.

CONSIDERATIONS FOR LARGE ENTERPRISE DEPLOYMENTS

Large scale enterprise deployments may require a scaling of the methods described in this document depending on the capabilities as well as the experience of the IT support staff in the enterprise. In some cases it may be required that the deployment of the agent in the production network be subdivided even further than the divisions described above. For example, instead of deploying the Cisco Security Agent across an entire departmental group such as Human Resources or Finance, it may be necessary to subdivide the deployment into smaller deployments across a subgroup. This is especially true if the deployment crosses geographic regions and affects remote users. This is to ensure that the deployment of the agents can be handled by the IT support staff levels. While this may result in a longer deployment, it helps ensure the most successful deployment possible.

ENDPOINT INVESTIGATION—USING CISCO SA PROFILER

The Cisco SA Profiler is a tool that can be used to develop a *stringent* security policy for an application environment. The primary purpose of the Profiler is to allow the Cisco SA software to analyze endpoints to develop a profile of applications and behaviors in use. Profiler can also be used to automatically generate policies after analyzing the endpoints. The Profiler strategy is two-fold:

- Protect the application from the system
- Protect the system from the application

Profiler is a powerful tool that helps understand the endpoint environment based on applications and behaviors present. Using this information, policies can be created that satisfy very stringent security requirements for an application environment. The implementation process for a custom policy includes all the tasks executed in a default policy implementation plus the additional tasks listed below:

Use Cisco SA profiler to create custom policies when *all* of the following conditions apply:

- The security requirements for the application environment are extremely high
- Hosts are dedicated to the application environment (they are not shared with any other applications)
- Strict change control procedures exist over the application production servers. All changes are approved, tested, and deployed with close coordination with information security and IT management
- There is willingness to make a significant resource commitment of application experts and testing resources to support the Cisco SA implementation. These application experts and testing resources must be an integral part of the Analysis and Policy Tuning process
- There is a willingness to commit a significant budget for policy customization (custom policy development requires significant consulting resources and typically last a minimum of three months)

The first step in using the Cisco SA profiler is to identify application subject matter expert(s) and Quality Assurance resources for all major components of the application environment (for example, Web Servers, web application server, application source code, database, scheduling system, operating system, etc). It is critical that the subject matter experts (SMEs) are available to assist during the policy analysis, development, and tuning tasks. They must be an integral part of the Cisco SA implementation effort. Because custom policy analysis requires intimate knowledge of the application environment, the SMEs must be available to the Cisco SA implementation team.

Additional Implementation Tasks for Custom Policy Implementations Using Cisco SA Profiler

The application to be analyzed is designated through the Cisco SAMC. The MC is also where an agent host is selected on which the analysis is to take place. The process to create custom policy implementations with Cisco SA Profiler is described below:

- Select an agent host on which the analysis is to take place and a timeframe within which the analysis will be completed
- Create application classes to support the analysis of all the appropriate applications
- Create an Analysis Job for each application to be evaluated
- Select the appropriate operating system and application classes to monitor
- Select the host that will be used as a logging agent (where the application is running)

It is important to remember to analyze one application at a time. It is recommended that the selected host be a QA system with a similar configuration than the corresponding production system. Make sure the allocated timeframe is sufficient for the execution of all the application's functionality, for example, a full test cycle of the application.

When the analysis is completed there is an option to automatically create a customized policy from that job. The resulting policy can be imported into the Cisco SAMC. Once imported, the Profiler policy is added to the list of policies with the word "Job" appended to the original analysis job name. The application subject matter experts should then analyze the resulting policy and fine-tune its rules. Extensive knowledge of the application environment is needed to ensure the resulting rules are "general enough" to support—not only the previous execution of the application—but all subsequent runs under different situations. When the Profiler has completed its analysis of the application the rules can then be generated and distributed to the selected host(s). Depending on the selected parameters, the selected host(s) will begin the analysis job after it polls in to the Cisco SAMC and receive the new rules.

The default-policy implementation methodology described above can be used to further tune and apply applicable default policies, as well as the resulting policy generated by the Cisco SA Profiler, to the appropriate Cisco SA group.

SUMMARY

The Cisco SA software suite represents a powerful tool that can be used to protect a wide variety of hosts from attack. However, the deployment design as well as the testing and distribution of the software across a network must be done with care and consideration in order to minimize the impact of the Cisco SA software on network-based applications. The first step in implementing Cisco SA on a network is to define the model to be used in the deployment. Sufficient testing of the Cisco SA software, either through a test environment or in a pilot program using representative production systems, minimizes the potential impact and the learning curve of the network staff caused by the deployment.

**Corporate Headquarters**

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters

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

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters

Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

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

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

Copyright © 2004 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 United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0403R) RD/LW6532 06/04

