



CHAPTER 1

Overview

What Cisco Security Agent Does

Cisco Security Agents provides intrinsic, distributed security to your enterprise by deploying agents that defend against the proliferation of attacks across networks and systems. These Cisco Security Agents enforce a set of policies provided by Management Center for Cisco Security Agents and selectively applied to system nodes by the network administrator.

Operating under the direction of assigned policies, Cisco Security Agents provide strong system resource protection, tying together the auditing and control of multiple system and network resources.

This section contains the following topics.

- [The Lifecycle of an Attack, page 1-2](#)
- [How Cisco Security Agents Protect Against Attacks, page 1-3](#)
- [Deployment Overview, page 1-4](#)
- [Network Architecture, page 1-5](#)
- [Cisco Security Agent Architecture, page 1-6](#)
- [Preparing a Security Policy, page 1-9](#)
- [Configuring Rule Modules and Policies, page 1-9](#)
- [Communicating over Secure Channels, page 1-10](#)
- [Distributing Policy Updates, page 1-10](#)
- [Configuration Road Map, page 1-10](#)

The Lifecycle of an Attack

When your network is targeted for attack, an assault is typically launched in a series of steps. Each step of an attack often depends upon the previous step being successful. [Table 1-1](#) displays the common evolution of an attack.

Table 1-1 *Lifecycle of an Attack*

Attack Action	Network Manifestation
Probe	<ul style="list-style-type: none"> • ping server IP addresses • run traceroute on IP addresses • sniff passwords • impersonate mail users
Penetrate	<ul style="list-style-type: none"> • email attachments • Java applets and ActiveX controls • buffer overflows • backdoors and trojans
Persist	<ul style="list-style-type: none"> • weaken security settings • install new services
Propagate	<ul style="list-style-type: none"> • email • Internet connections • IRC • FTP • infected file shares
Paralyze	<ul style="list-style-type: none"> • reformat disks • destroy or corrupt data • drill security holes • crash computers • consume work cycles • steal confidential data

How Cisco Security Agents Protect Against Attacks

The Cisco Security Agent differs from anti-virus and network firewall software in that it doesn't prevent users from accessing technologies they require. It assumes that users are going to put their systems at risk by making use of a wide range of Internet resources. Keeping this in mind, Cisco Security Agents install and work at the kernel level, controlling network actions, local file systems, and other system components, maintaining an inventory of what actions may be performed on the system itself. This way, malicious system actions are immediately detected and disabled while other actions are permitted. Both actions take place transparently, without any interruption to the user.

If an encrypted piece of malicious code finds its way onto a system via email, for example, as it attempts to unexpectedly execute or alter Cisco Security Agent-protected system resources, it is immediately neutralized and a notification is sent to the network administrator.

Cisco Security Agents use policies which network administrators configure and deploy to protect systems. These policies can allow or deny specific system actions. Cisco Security Agents must determine whether an action is allowed or denied before any system resources are accessed and acted upon.

Specifically, rule policies enable administrators to control access to system resources based on the following parameters:

- What resource is being accessed.
- What operation is being invoked.
- Which application is invoking the action.

The resources in question may be either system resources or network resources such as mail servers.

When any system actions that are controlled by specific rules are attempted and allowed or denied accordingly, a system event is logged and sent to the administrator in the form of a configurable notification such as email, pager, or custom script.

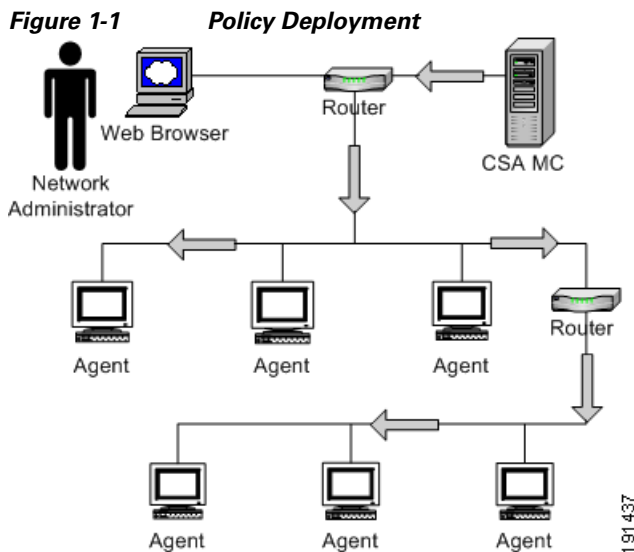
Deployment Overview

Management Center for Cisco Security Agents contains two components:

- CSA MC—installs on designated Windows 2003 systems and includes a configuration database server and a web-based user interface.
- Cisco Security Agent (the agent)—installs on server and desktop systems across your enterprise network.

Using CSA MC, you assemble your network machines into specified groups and then attach security policies to those groups. All configuration is done through the web-based user interface and then deployed to the agents.

The network example shown in [Figure 1-1](#) illustrates a basic deployment scenario. CSA MC software is installed on a system which maintains all policy and host groups. The administration user interface is accessed securely using SSL (Secure Sockets Layer) from any machine on the network that can connect to the server and run a web browser. Use the web-based interface to deploy your policies from CSA MC to agents across your network.



Network Architecture

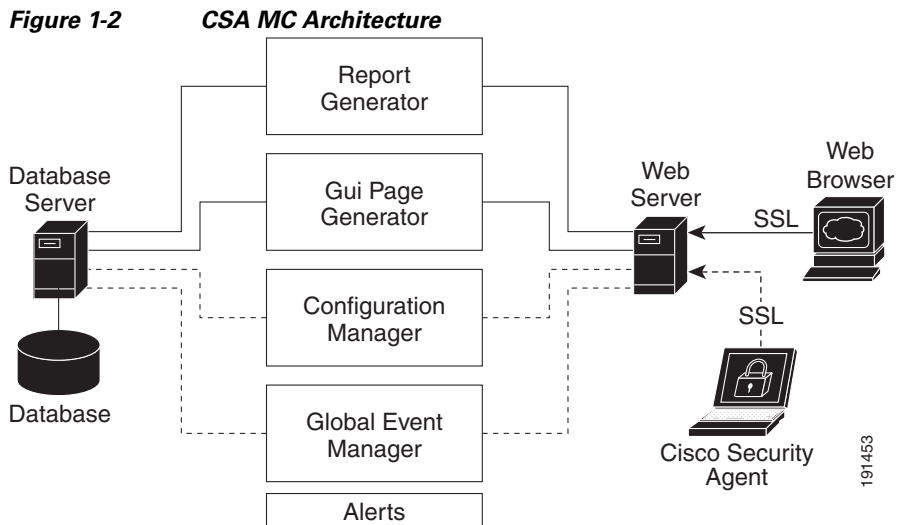
The CSA MC architecture model consists of a central management center which maintains a database of policies and system nodes, all of which have Cisco Security Agent software installed on their desktops and servers.

Agents register with CSA MC. CSA MC checks its configuration database for a record of the system. When the system is found and authenticated, CSA MC deploys a configured policy for that particular system or grouping of systems.

The Cisco Security Agent software now continually monitors local system activity and polls to the CSA MC at configurable intervals for policy updates. It also sends triggered event alerts to the CSA MC's global event manager. The global event manager examines system event logs and, based on that examination, may trigger an alert notification to the administrator or cause the agent to take a particular action.

**Note**

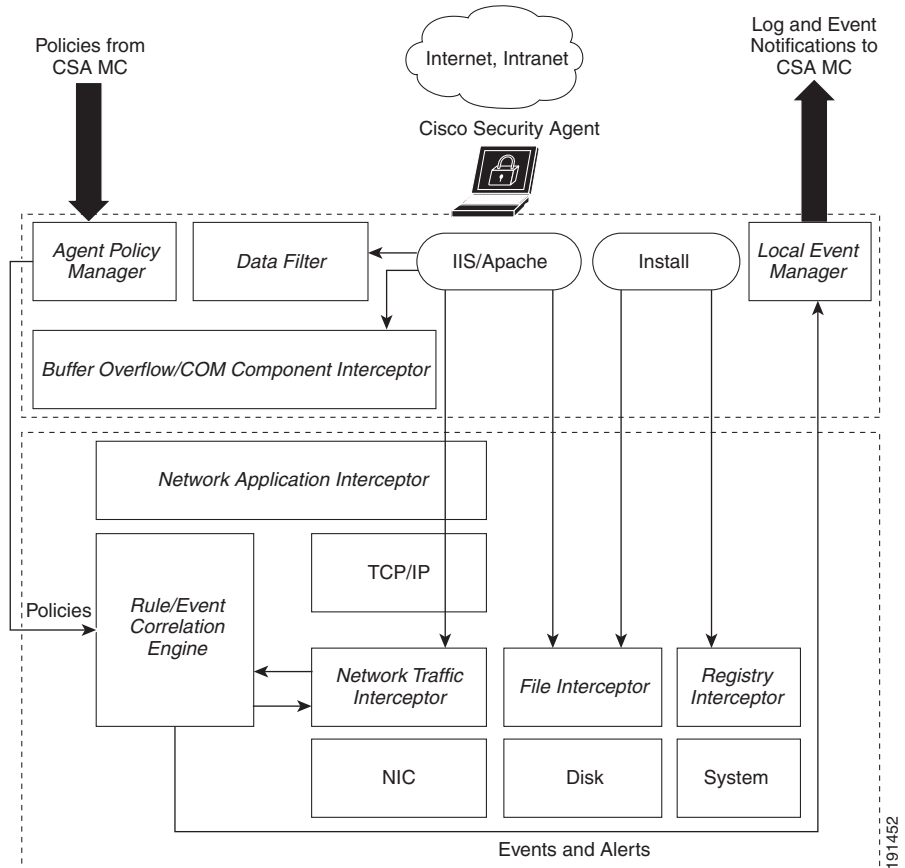
See [Appendix B, “System Components”](#) for detailed information on product architecture.



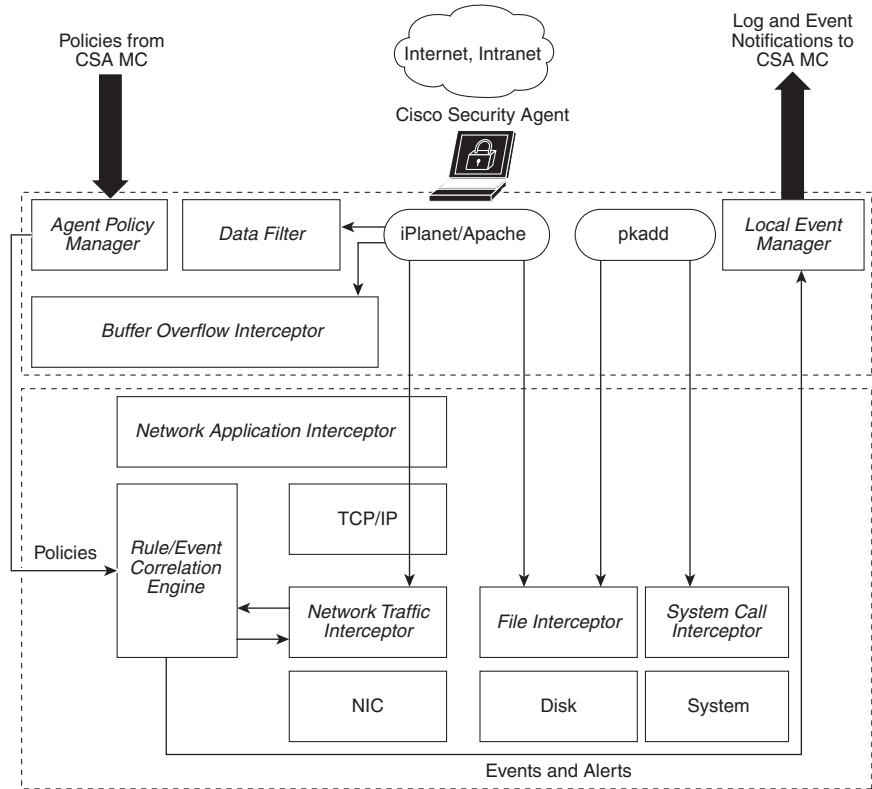
Cisco Security Agent Architecture

The Cisco Security Agent software installs locally on each system node and intercepts operations of that system. A network application interceptor sits at the application level and intercepts all application operations. Other Cisco Security Agent mechanisms intercept network traffic, file actions, and system registry actions while the rule/event correlation engine controls all agent mechanisms watching for any events that trigger an agent policy. See [Figure 1-3](#).

**Figure 1-3 Cisco Security Agent Software Architecture (Windows)
Cisco Security Agent Windows Architecture**



**Figure 1-4 Cisco Security Agent Software Architecture (UNIX)
Cisco Security Agent UNIX Architecture**



Preparing a Security Policy

You should have a carefully planned corporate security policy in place before you attempt to configure Management Center for Cisco Security Agents. You must understand exactly what network resources and services you want to protect in order to adequately scale a set of policies that safeguard those valuable organizational resources. A corporate security policy should allow the user community to easily access required resources, while protecting that community from the dangers those open resources can represent.

To help achieve this goal, CSA MC ships with a variety of rule templates and pre-configured security modules and policies. The policies you configure and deploy become the foundation of your security policy.

Configuring Rule Modules and Policies

A policy is a collection of rule modules. A rule module is a collection of rules. The rule module acts as the container for these rules while the policy serves as the unit of attachment to groups. Machines with similar security needs are grouped together and assigned one or more policies that specifically target the needs of the group.

When you are creating rules for your rule modules, targeting the needs of machine groupings is central to your overall security plan. You can base these security needs on various criteria. For example, the concerns you have for your web servers may require you to group them separately from your mail servers based on the types of policies each set of servers require. Therefore, you could place your web servers into a common group, create rules that protect those servers from having their cgi files and html files written to (for example), and then attach the policy that contains these rules to the web servers group.

When first configuring and deploying policies, you should put them into Test Mode (from the Group or Rule Module pages). In Test Mode, the policies are not "live." The Cisco Security Agent will not deny any action or operation even if an associated policy says it should be denied. Instead, the agent will permit the action but log an event when a deny or query rule is triggered and when an allow rule with logging enabled is triggered. This helps you to understand the impact of deploying a policy on a host before enforcing it.

Communicating over Secure Channels

All communications between the Management Center for Cisco Security Agents server system and systems accessing the browser-based user interface are protected using SSL (Secure Sockets Layer). Administrator authentication is also provided via the required entry of a username and password to authenticate and initiate each management session. Additionally, communications between the management server and the agents are passed over SSL.

See the Installation Guide for information on importing certificates and connecting securely over SSL.

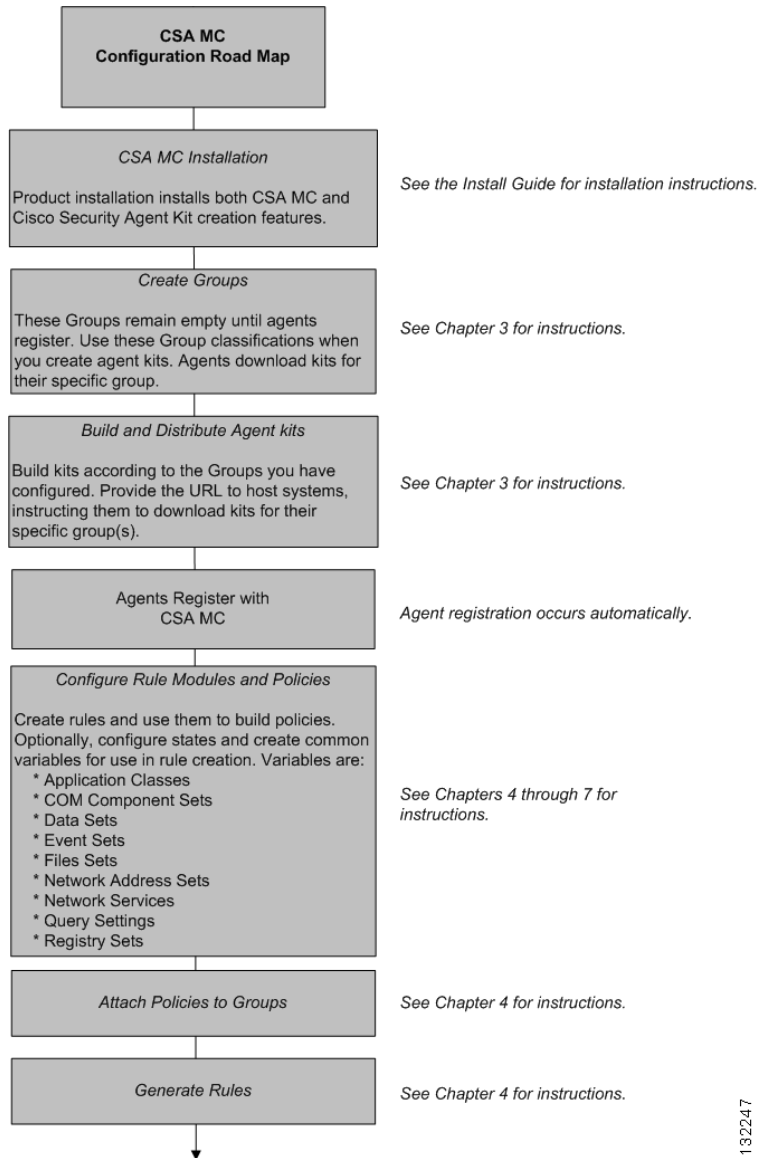
Distributing Policy Updates

At configurable time intervals, Cisco Security Agents on the network poll in to CSA MC to check for updated rule sets. See [Chapter 3, “Configuring Groups and Managing Hosts”](#) for details.

When a rule is triggered on a system, the agent sends its event notifications to CSA MC. CSA MC identifies the agent, examines the event notifications presented by the agent and correlates this information.

Configuration Road Map

There are several elements you must configure to create policies that are distributed to the agents. First, you must configure host groups and create Cisco Security Agent kits. After the agents are installed on systems throughout your network, they register with CSA MC. Then, they are automatically placed into their assigned groups. When you generate rules, agents receive the policies intended for them. Refer to the following CSA MC configuration roadmap in [Figure 1-5](#).

Figure 1-5 CSA MC Configuration Road Map

132247

