



APPENDIX **B**

System Components

Overview

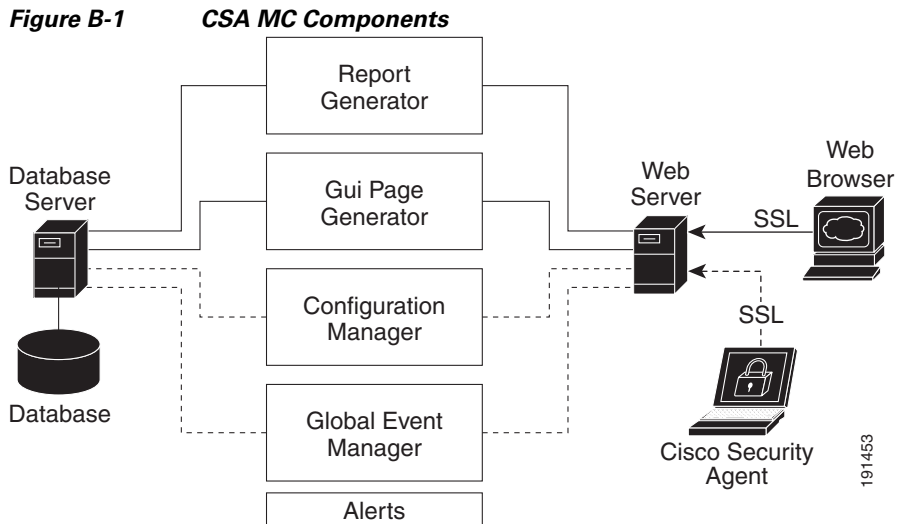
This appendix contains information on CSA MC and agent core components, explaining how these components relate to each other, including details on various CSA MC and agent services.

This section contains the following topics.

- [CSA MC Components, page B-2](#)
- [Agent Components, page B-4](#)

CSA MC Components

CSA MC architecture is displayed in this appendix. Note that although the agent is mentioned often here, it is only in terms of CSA MC's relation to the agent. Agent software does have its own system components which are described in this chapter. It is CSA MC that pushes security policies to the agents and coordinates the events it receives back from the agents. The mechanisms that are required to perform those tasks are described here as part of the CSA MC architecture.



The **web browser**, shown on the right in the diagram, represents any web browser on any system across an enterprise from which administrators can securely access the CSA MC web-based interface. Communications between the web browser and the web server occur over SSL, allowing administrators to securely access the database of rule configurations from any location.

The *web server* provides the means of communication between the web browser and all other CSA MC system components. The web server displays reporting information, configuration version data, and event logging data.

It is through the **web server** that the agents installed on systems across an enterprise can exchange data with the CSA MC **configuration manager** and the **global event manager**. When agents poll in to CSA MC for rule set updates, it is the configuration manager that pulls the rules from the database and distributes

them to the particular agents for which they are intended. Agents also send events to the global event manager which stores this information in the central SQL server database.

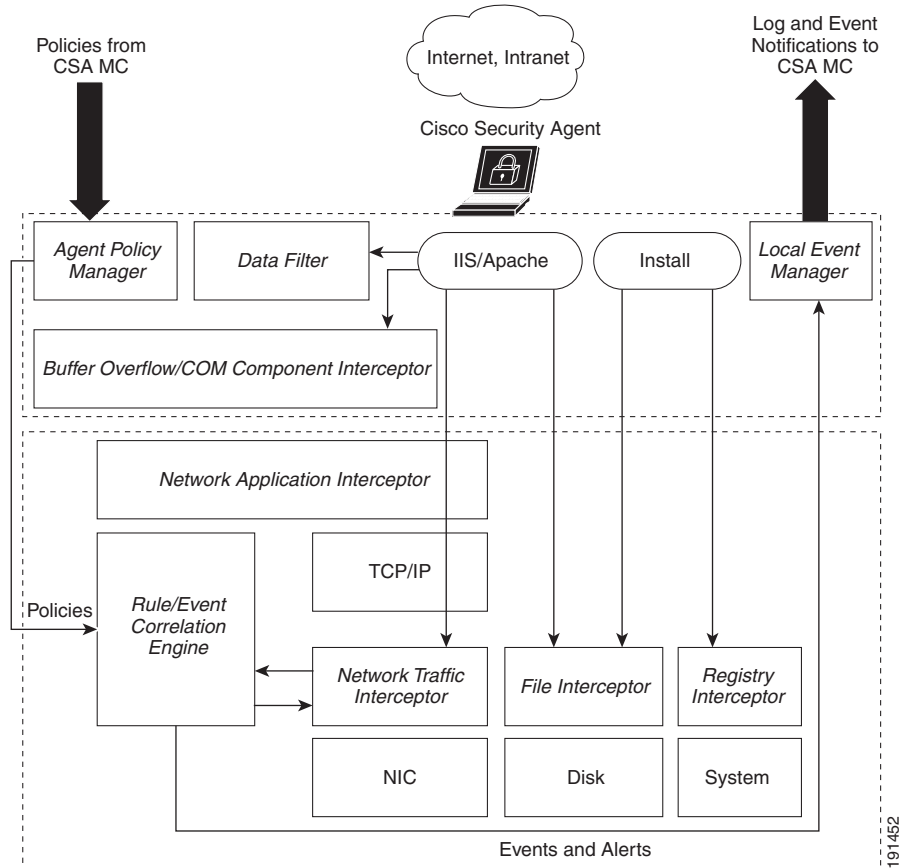
The **SQL server database** is the central repository for configuration data (host agents, groups, file rules, network rules, registry rules, etc.) created by the administrator and for the system event information provided by the agents. It is in this database that rules and information on system groupings are stored when the administrator generates rules and policies through the web-based interface. When reports are requested by the administrator, the **report generator** component gathers rule and event data kept in the database and produces reports using this information.

All information (rule configurations, event logs, etc.) passed between CSA MC and the agents distributed across your enterprise is encrypted providing a secure communication channel for the exchange of data.

Agent Components

Figure B-2 shows the agent in terms of its system components, displaying where those components operate in relation to general system functions. For example, the interceptors shown in the diagram install and work at the kernel level.

**Figure B-2 Cisco Security Agent Components (Windows)
Cisco Security Agent Windows Architecture**



Starting from the left side of the diagram, the agent **policy manager** receives the rules configured by the administrator from CSA MC. These rules are sent to the agent's **rule/event correlation** engine. If a rule set already exists there, those rules are updated or replaced with the newest rule set.

The **interceptors** do as their name indicates, they intercept key actions that are attempted on the system and check the action in question against the rule correlation engine to determine if a rule set allows or denies it. Based on the information the interceptors receive, they either allow the action to take place or they stop it cold.

Actions are stopped based on certain criteria that are part of each rule and consequently each interceptor acts based on a component-targeted set of criteria. For example, the **network application interceptor** controls which applications are allowed to communicate with the network, while the **network traffic interceptor** provides system hardening features such as SYN flood protection and port scan detection. The **file interceptor** controls which applications can read and/or write to specified system files and directories. The **registry interceptor** controls system behavior, preventing applications from writing to particular registry keys. All of these controls can be as broad or as granular as necessary.

As the interceptors are allowing or denying actions, they produce an event each time a rule set is triggered by a system action. These events are stored in the rule/event correlation engine which forwards them on to the **local event manager** and **global event manager**. Events are also stored in the NT event log or W2K event viewer on the agent system.

Figure B-3 Cisco Security Agent Components (UNIX)
Cisco Security Agent UNIX Architecture

