CHAPTER 11

Threat Control and Containment

Cisco SAFE leverages the threat detection and mitigation capabilities available on Cisco firewalls, Cisco Cisco IPS, Cisco Security Agents (CSA), Cisco Network Admission Control (NAC), and web/E-mail security appliances. In addition, the alarm and event information generated by these devices is centrally collected and correlated by the Cisco Security Monitoring, Analysis, and Response System (CS-MARS) to identify the source of threats, visualize the attack paths, and to suggest and optionally enforce response actions. Cisco IPS visibility is enhanced with the endpoint posture information provided by CSA which reduces false-positives and allows for the dynamic quarantine of compromised hosts. Cisco SAFE also leverages the linkage between Cisco Security Manager (CSM) and CS-MARS to simplify management and to expedite troubleshooting and threat mitigation.

Following are some of the threat control and containment attributes of the Cisco SAFE design:

- *Complete visibility*—Infrastructure-wide intelligence provides an accurate vision of network topologies, attack paths, and extent of the damage.
- *Adaptive response to real-time threats*—Source threats are dynamically identified and blocked in real-time.
- *Consistent policy enforcement coverage*—Mitigation and containment actions may be enforced at different places in the network for defense-in-depth.
- *Minimize effects of attacks*—Response actions may be immediately triggered as soon as an attack is detected, thereby minimizing damage.
- *Common policy and security management*—A common policy and security management platform simplifies control and administration, and reduces operational expense.

Endpoint Threat Control

Network endpoints include servers, desktop computers, laptops, printers, IP phones, and any other systems that connect to the network. The great variety in hardware types, operating systems, and applications represents a clear challenge to security. In addition, portable devices such as laptops can be used at hotels and other places outside the corporate controls, further complicating the enforcement of security policies and controls. Common threats to these endpoints include malware, adware, spyware, viruses, worms, botnets, and E-Mail spam.

Properly securing the endpoints requires end-user awareness and the adoption of the appropriate technical controls. Cisco SAFE advocates for the continuous education of end-users on current threats and security measures. Furthermore, the Cisco SAFE design blueprints implement a range of security controls designed to protect the endpoints. These include host Cisco IPS, network-based intrusion prevention systems, and web and E-Mail traffic security.

As a host Cisco IPS, Cisco SAFE leverages CSA on end-user workstations and servers. CSA takes a proactive and preventative approach, using behavior-based security to focus on preventing malicious activity on the host. Malicious activity is detected and blocked, independent of the type of malware, spyware, adware, or virus affecting the host.

Once deployed on an endpoint, whenever an application attempts an operation, the agent checks the operation against the application's security policy—making a real-time *allow* or *deny* decision on the continuation of that operation and determining whether logging the operation request is appropriate. Security policies are collections of rules that IT or security administrators assign to protect servers and desktops, either individually or enterprise-wide. CSA provides defense-in-depth protection against spyware and adware by combining security policies that implement distributed firewall, operating system lockdown and integrity assurance, malicious mobile code protection, and audit-event collection capabilities in default policies for servers and desktops.

CSAs are centrally managed with the CSA Management Center (CSA-MC), which in the Cisco SAFE design is placed in a secure segment in the data center. The Management Center (MC) also provides centralized reporting and global correlation.

For complete details about deploying CSA in a network, refer to the *Rapid Deployment Guide for Cisco Security Agent 6.0 for Desktops* at the following URL:

http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5707/ps5057/deployment_guide_c07-501928.html

Network-Based Threat Control

Cisco SAFE leverages various forms of network-based threat control, including Cisco IPS sensors, Cisco firewalls, Cisco NAC and web/E-Mail security. Cisco NAC and web/E-Mail security are addressed in Chapter 5, "Enterprise Campus," and Chapter 6, "Enterprise Internet Edge," respectively.

Network-Based Cisco IPS

Cisco IPS modules and appliances are strategically deployed throughout the Cisco SAFE design blueprints. Cisco IPS provides signature and reputation-based threat detection and mitigation for threats such as worms, spyware, adware, network viruses, and application abuse.

The deployment mode and the platform selection in the Cisco SAFE design blueprints is driven by three key design aspects:

- Deployment Mode, page 11-3
- Scalability and Availability, page 11-3
- Maximum Threat Coverage, page 11-3
- Cisco IPS Blocking and Rate Limiting, page 11-4
- Cisco IPS Collaboration, page 11-4

Deployment Mode

Cisco IPS appliances and modules can be deployed in inline or promiscuous mode, typically referred to as Cisco IPS or IDS modes. When deployed in inline mode, the Cisco IPS is placed in the traffic path. This allows the sensor to stop attacks by dropping malicious traffic before it reaches the intended target, thus providing a protective service. Cisco IPS inline mode enables automatic threat detection and mitigation capabilities that offer some clear advantages in terms of timely threat mitigation. In addition, signature tuning enables the automated response actions to be tuned according to customer policy. Since the Cisco IPS is in the data path, it is critical to ensure that a deployment be well designed, architected, and tuned to ensure that it does not have a negative impact on network and service availability.

Cisco IPS can also be deployed in promiscuous mode. In this mode, the Cisco IPS performs passive monitoring, with traffic being passed to it through a monitoring port. The Cisco IPS sensor analyzes a copy of the monitored traffic rather than the actual forwarded packet. Upon detection of anomalous behavior, management systems are informed of an event and operational staff can subsequently decide what action, if any, to take in response to an incident. The time between threat detection and mitigation may thus be extended.

Scalability and Availability

For scalability, Cisco offers a range of IPS platforms with various levels of capacity and form factors that can be deployed according to particular customer needs. The Cisco SAFE designs implement Cisco IPS appliances on those *places in the network* (PINs) demanding the highest levels of throughout, such as the data center, campus, and the WAN edge. Cisco IPS modules are also viable options for environments where integrated security is preferred. At the branches, Cisco IPS modules are deployed on routers or firewalls.

For increased scalability and high availability, multiple Cisco IPS can be bundle together using a load-balancing mechanism. The Cisco SAFE campus design implements multiple appliances by connecting them to a switch and Ether Channel load-balancing (ECLB) feature of the switch to perform intelligent load balancing across the Cisco IPS devices. Multiple Cisco IPS sensors may also be deployed by using a load-balancing module or appliance as the Cisco Application Control Engine (ACE) module.

Maximum Threat Coverage

For maximum visibility, the Cisco IPS sensors must be able to see traffic in both directions. For this reason, it is important to ensure the symmetry of the traffic as traverses or reaches the Cisco IPS sensor.

Symmetrical traffic flows offer a number of important benefits, including enhanced threat detection, reduced vulnerability to Cisco IPS evasion techniques, and improved operations through reduced false positives and false negatives. Consequently, this is a key design element. For example, if more than one Cisco IPS exists in a single flow for availability and scalability purposes, maintaining symmetric flows requires some consideration of the Cisco IPS integration design. There are a number of options available to ensure symmetric traffic flows, including the following:

- *Copy traffic across Cisco IPS*—Use of SPAN, VLAN access control list (VACL) capture, or taps to duplicate traffic across all Cisco IPS, ensuring any single Cisco IPS sees all flows. This can become a challenge once more than two Cisco IPS are involved and results in all Cisco IPS being loaded with the active traffic flows.
- *Integration of an Cisco IPS switch*—Topological design to consolidate traffic into a single switch, thereby leveraging the switch to provide predictable and consistent forward and return paths through the same Cisco IPS. This is simple design, but introduces a single point-of-failure.

- *Routing manipulation*—Use of specific routing techniques, such as path cost metrics or policy-based routing (PBR), to provide predictable and consistent forward and return paths through the same switch and, consequently, the same Cisco IPS. This is a cost-effective design approach, but it introduces complexity and requires an agreement from network operations (NetOps).
- *Sticky load balancing*—Insertion of a sticky load-balancing device, such as the Cisco ACE module, to provide predictable and consistent forward and return paths through the same Cisco IPS. This is flexible design, but introduces additional equipment to deploy and manage.

Cisco IPS Blocking and Rate Limiting

Cisco IPS sensors can be used in conjunction with routers, switches, and firewalls to dynamically enforce blocking and rate limiting actions on those devices—and in response to suspicious events.

Blocking is configured at the signature level and, when triggered, the sensor updates the configuration of the managed devices to enforce the block action.

There are three types of blocks:

- *Host block*—Blocks all traffic from a given IP address.
- *Connection block*—Blocks traffic from a given source IP address to a given destination IP address and destination port.
- *Network block*—Blocks all traffic from a given network.

Caution Configuring a sensor to perform blocking at a very high rate, or to manage too many blocking devices and interfaces, might result in the sensor not being able to apply blocks in a timely manner—or not being able to apply blocks at all.

Cisco IPS sensors can also be configured to restrict the rate of specified traffic classes on network devices. Rate-limiting responses are supported for the Host Flood and Net Flood engines, and the TCP half-open SYN signature.

For more information on Cisco IPS capabilities, refer to the *Cisco IPS Configuration Guide* at the following URL:

http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/products_installation_and_configuration_guides_list.html

Cisco IPS Collaboration

In collaboration with other Cisco devices, the Cisco IPS provides enhanced visibility and control through system-wide intelligence. This includes host-based IPS collaboration with the CSA (explained later in this chapter), reputation-based filtering and global correlation using SensorBase, automated threat mitigation with the WLAN Controller (WLC), multi-vendor event correlation and attack path identification using CS-MARS, and common policy management using CSM.

Cisco IPS collaboration with the WLAN Controller is covered in detail in *the Secure Wireless Design Guide* at the following URL:

http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/secwlandg20/ch8_2_SPMb.html

Network-Based Firewalls

Cisco SAFE leverages the threat detection and mitigation capabilities available on Cisco firewalls. Firewall abilities include identifying and dropping packets due to denial by access list, invalid packet format, connection limits exceeded, protocol violations, and other abnormal conditions. Cisco firewalls are also equipped with application-layer protocol inspection to allow the identification and automatic mitigation of attacks based on protocol violation or manipulation. Other control mechanisms include the enforcement of timeouts and connection limits which helps mitigate flood-based denial of service (DoS) attacks.

For a detailed description of the deployment options and platforms implemented in each SAFE module, refer to the applicable module chapter.

Cisco IOS Embedded Event Manager

Cisco IOS Embedded Event Manager (EEM) is a powerful and flexible subsystem in Cisco IOS that provides real-time network event detection and on-board automation. Using EEM, customers can adapt the behavior of network devices to align with business needs.

EEM is available on a wide range of Cisco platforms and customers can benefit from the capabilities of EEM without upgrading to a new Cisco IOS version.

EEM supports more than 20 event detectors that are highly integrated with different Cisco IOS components to trigger actions in response to network events. Customer business logic can be injected into operations using EEM policies. These policies are programmed using either a simple CLI-based interface or using Tool Command Language (Tcl) scripting language. EEM harnesses the significant intelligence within Cisco devices to enable creative solutions including automated troubleshooting, automatic fault detection and troubleshooting, and device configuration automation.

For more information about EEM, refer to the *Cisco IOS Software Embedded Event Manager, Harnesses Network Intelligence to Increase Availability* at the following URL:

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6550/prod_white_paper0900aecd803a4dad_ps6815_Products_White_Paper.html

Global Threat Mitigation

As described in the previous section, CS-MARS develops network intelligence by understanding the network topology and device configurations and by profiling network traffic. CS-MARS uses this network intelligence to identify and mitigate threats *before* they affect other systems or PINs.

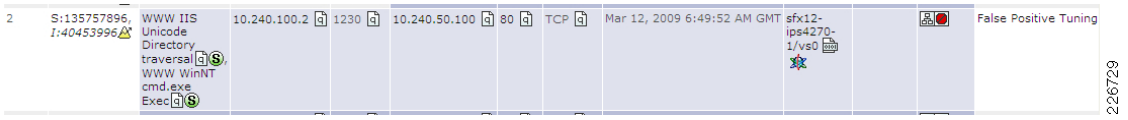
Upon identification of a legitimate network attack, CS-MARS is capable can visualize the attack path and identify possible mitigation enforcement devices along the path. Attack paths can be visualized by the user at both Layer2 and Layer 3. CS-MARS also provides the appropriate device commands that the user can employ to mitigate the threat on the possible mitigation devices.

Possible mitigation enforcement devices are devices that can deny the attack traffic flow and that are in the attack path. CS-MARS provides mitigation support in two forms:

- For supported Layer-3 devices based on the Open Systems Interconnection (OSI), CS-MARS provides the user with a suggested device and set of commands that can be used to halt an ongoing, detected attack. This information can be used to manually block the attack.
- For supported Layer-2 devices, CS-MARS recommends a device and a set of commands to halt the ongoing, detected attack, and provides a method for making the configuration changes on behalf of the user.

As an example, Figure 11-1 illustrates an attack launched from the main campus.

Figure 11-1 incident Detail



The attack paths and the recommended action (ACL enforcement) determined by CS-MARS are illustrated in Figure 11-2 and Figure 11-3.

Figure 11-2 Attack Paths Determined by CS-MARS

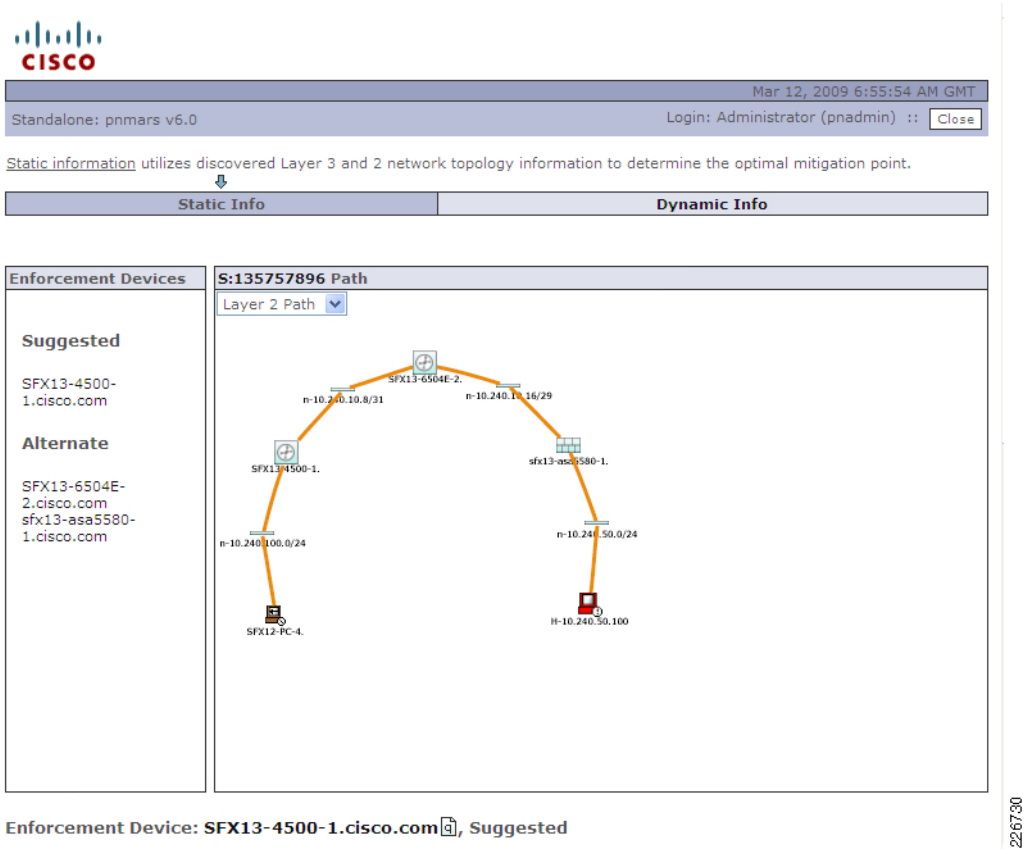
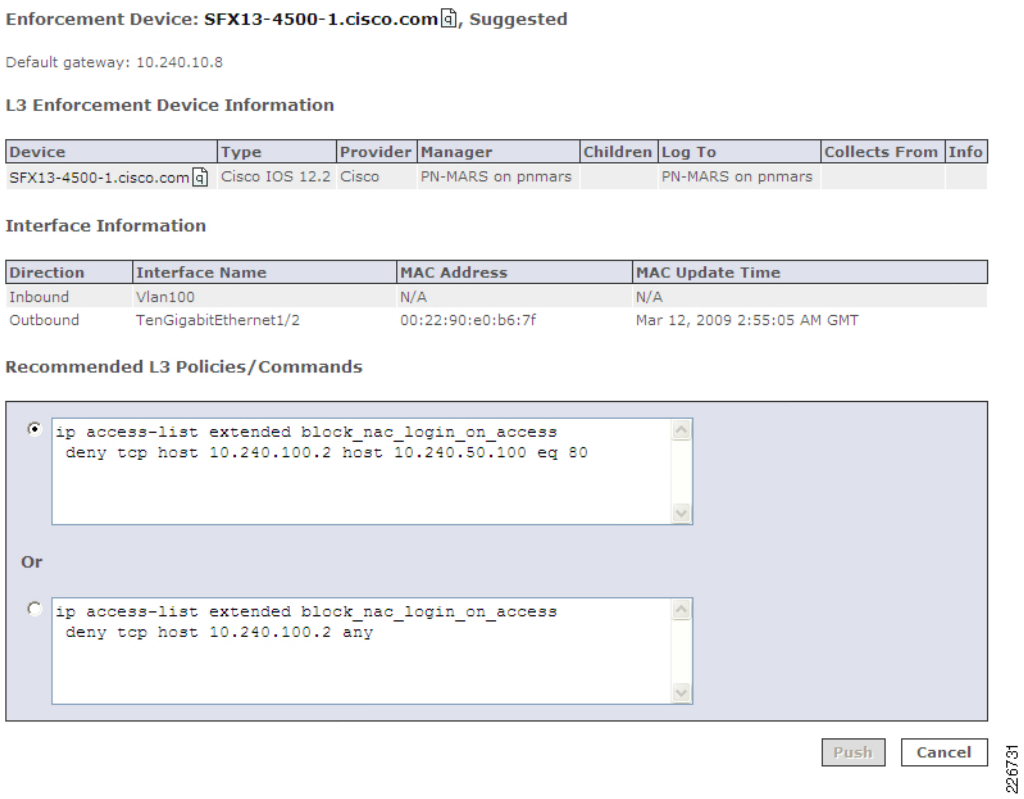


Figure 11-3 Suggested Mitigation Commands



Cisco IPS Enhanced Endpoint Visibility

Cisco SAFE leverages the integration between CSA and Cisco IPS as a key component of Cisco SAFE threat control and containment strategy. Residing on servers and desktops, CSAs have full visibility into endpoints which allows CSAs to gather information that is not available to any other security component on the network. The integration between CSA and Cisco IPS allows the sensor to use this valuable information and thereby increase its visibility into endpoints and global threats.

The collaboration between CSA and Cisco IPS has the following benefits:

- *Ability to use CSA endpoint information to influence Cisco IPS actions*—By using the endpoint contextual information, Cisco IPS determines the appropriate severity of a network threat and instructs the adequate response action.
- *Reduction of false positives*—CSA provides OS-type and other endpoint posture information that helps Cisco IPS determine the relevancy of a threat—reducing the chance of a false positive.
- *Enhanced attack mitigation*—Cisco IPS can use the *watch list* maintained by CSA. The watch list helps Cisco IPS monitor the systems identified by CSA as suspicious or malicious, and helps highlight any events associated with these systems.
- *Dynamic host quarantine*—The Cisco IPS has the ability to dynamically block hosts that have been identified by CSA as malicious. This extends the quarantine capabilities from CSA to the Cisco IPS.

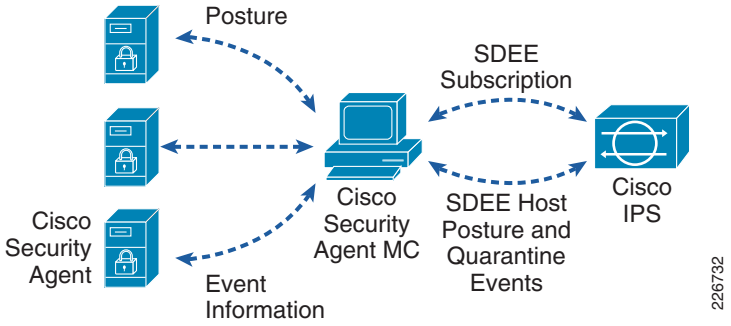
CSA and Cisco IPS Collaborative Architecture

The architecture integrating CSA and Cisco IPS relies on the interaction of the following major components:

- *Cisco IPS* —Any Cisco IPS platform running at minimum Cisco IPS Sensor Software Version 6.0, configured either in inline protection mode (IPS) or promiscuous mode (IDS).
- *CSAs*—Host-based Cisco IPS software running on servers and desktops to be protected and monitored.
- *CSA-MC*—A a standalone application that provides centralized security policy configuration, monitoring, and administration for CSAs. In addition, CSA-MC performs global correlation based on event and posture information generated by the CSAs. CSA-MC 5.0 or later is required to integrate with the Cisco IPS.

The components of the architecture and their interactions are depicted in Figure 11-4.

Figure 11-4 Cisco Secure Agent/Cisco IPS Collaborative Architecture



The Cisco IPS sensor accesses this information via Secure Device Event Exchange (SDEE), a protocol developed by a consortium (led by Cisco) that is designed for the secure exchange of network event information. Communications between CSA-MC and Cisco IPS are protected with Secure Socket Layer (SSL)/Transport Layer Security (TLS) encryption and Hypertext Transfer Protocol (HTTP) authentication.

Note CSA-MC authenticates by providing X.509 certificates while the Cisco IPS sensor authenticates using a username and password.

To start receiving information, a Cisco IPS sensor must open a SDEE subscription with CSA-MC. After the communication channels are authenticated and established, two types of messages are exchanged between CSA-MC and Cisco IPS sensors:

- *CSA Posture Events*—Contains host posture information collected by CSA- MC such as the IP address and the OS type of the hosts running CSA. To receive posture events a Cisco IPS must open a subscription. After the subscription is open, the CSA-MC sends an initial state message with the IP addresses and OS types of all known agents. After the initial state, the CSA-MC keeps the Cisco IPS informed through updates.
- *Quarantine Events*—Generated by CSA-MC to communicate the list of hosts that are being quarantined to Cisco IPS sensors. A host is quarantined either manually by a CSA-MC administrator or by rule-generated by global correlation. Quarantine events include the reason for the quarantine, the protocol—such as Transmission Control Protocol (TCP), User Datagram Protocol (UDP), or Internet Control Message Protocol (ICMP)—associated with a rule violation, an indicator on

whether a rule-based violation was associated with an established TCP connection or a UDP session, and the IP address of the host to be quarantined. Cisco IPS sensors must subscribe before they can start receiving quarantine events. The CSA-MC sends an initial state message containing the list of all the hosts under quarantine and reports any subsequent quarantine incidents via updates.

Deployment Considerations

In general, the same best practices used to deploy CSA and Cisco IPS as standalone products apply when the two are implemented together in the same environment; therefore, it is always a good idea to follow those principles whenever possible. In addition to adopting the design best practices for CSA and Cisco IPS, there are few important considerations that should be noted when integrating the two products. These are briefly summarized in the following sections:

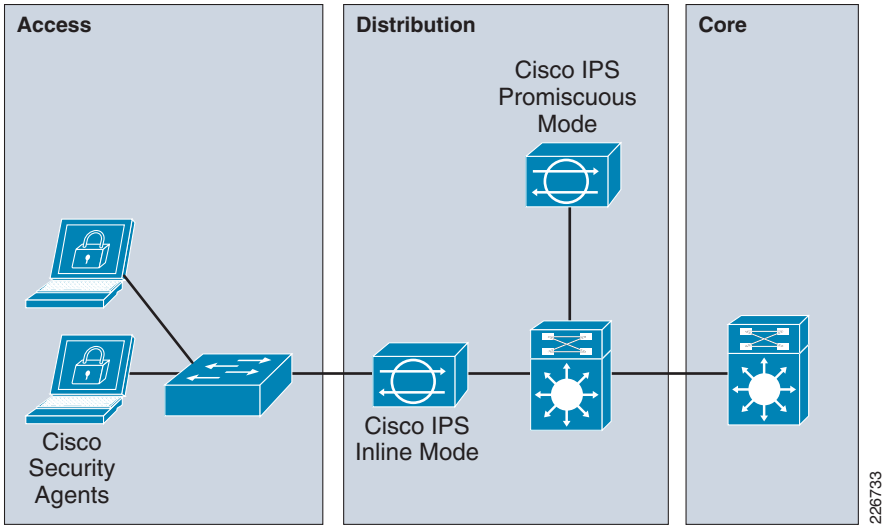
- Inline Protection (IPS) and Promiscuous (IDS) Modes, page 11-9
- One CSA-MC to Multiple Cisco IPS Sensors, page 11-10
- One Sensor to Two CSA-MCs, page 11-10
- Virtualization, page 11-10
- IP Addressing, page 11-10

Inline Protection (IPS) and Promiscuous (IDS) Modes

CSA can be integrated with Cisco IPS sensors that are configured either in inline protection (IPS) mode or promiscuous detection (IDS) mode. This results in greater flexibility because there are different valid reasons why a network administrator might opt to deploy Cisco IPS in one mode or the other.

The Cisco SAFE campus design is capable of integrating sensors in both inline protection mode and promiscuous detection mode. A sensor deployed inline at the distribution layer is capable of dynamically blocking malicious packets as they move through the system, When deployed in promiscuous mode, the sensor passively monitors traffic. These designs are illustrated in Figure 11-5.

Figure 11-5 Typical Cisco IPS/IDS Deployment Designs



One CSA-MC to Multiple Cisco IPS Sensors

A single CSA-MC can serve multiple Cisco IPS sensors simultaneously. In cases where Cisco IPS sensors are managed by different groups of administrators, their access to CSA-MC can be separated by the use of different subscription credentials.

One Sensor to Two CSA-MCs

A single Cisco IPS sensor can be configured to interface with up to two CSA-MCs simultaneously. Besides being crucial for redundancy purposes, this feature can be used to simplify the process of upgrading the version of CSA-MC.

Virtualization

The CSA can be integrated with Cisco IPS systems configured with virtual sensors. When used with virtualization, all information provided by the CSA-MC is global to the Cisco IPS sensor and, as a result, can be used by all active virtual sensors.

IP Addressing

Both the CSA-MC and the Cisco IPS sensors identify hosts based on their IP addresses; therefore, both should have a consistent view of the IP address space. Implementing the CSA-MC and Cisco IPS sensors in different sides of a Network Address Translation (NAT) can lead to an incompatible view of the address space. As a result, the Cisco IPS sensors might not be able to properly match the posture information provided by the CSA-MC; one host might be seen by the CSA-MC and the Cisco IPS sensors as two different systems—or two separate hosts might be confused as being a single host. In all cases, an incompatible view of the address space reduces the quality of the integration and can result in the enforcement of mitigation actions on the wrong hosts.

As a general best practice, avoid implementing NAT between CSA, CSA-MC, and the Cisco IPS sensors whenever it is possible. When NAT is required, ensure CSA-MC and the Cisco IPS sensors are placed on the same side of the translation—making sure they have the same IP address space visibility.

Deployment Best Practices

Integrating CSA and Cisco IPS requires the configuration of both CSA-MC and the Cisco IPS sensors. For most scenarios, configuration consists of the following activities:

- Defining a CSA-MC administrative account to be used by Cisco IPS sensors in their SDEE subscriptions.
- Enabling CSA host history collection.
- Adding CSA-MC as a trusted host in each Cisco IPS sensor.
- Configuring an external product interface in each Cisco IPS sensor.

The following sections describe the best practices that should be followed.

- Cisco Security Agent MC Administrative Account, page 11-11
- Cisco Security Agent Host History Collection, page 11-11
- Adding CSA-MC System as a Trusted Host, page 11-12
- Configuring Cisco IPS External Product Interface, page 11-13

- Leveraging Endpoint Posture Information, page 11-14
- Cisco Security Agent Watch Lists, page 11-16
- Cisco IPS Event Action Override, page 11-17
- Validating Cisco Secure Agent and Cisco IPS Integration, page 11-18

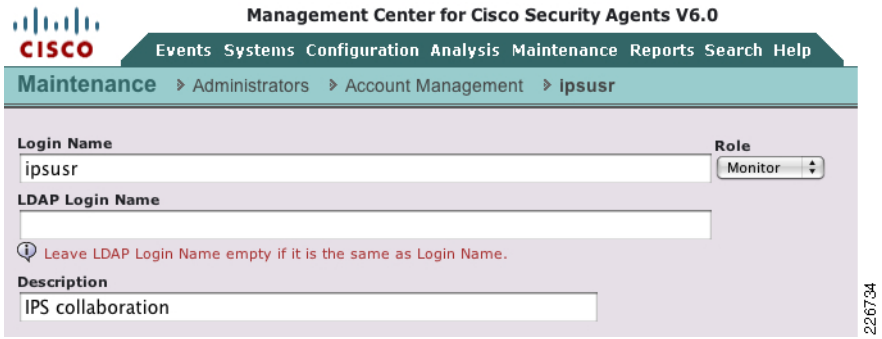
Cisco Security Agent MC Administrative Account

Communications between the CSA and Cisco IPS are authenticated. The CSA- MC will not accept a SDEE subscription for posture and quarantine information *unless* the requesting Cisco IPS sensor is successfully authenticated. To that end, every Cisco IPS sensor must be preconfigured with the username and password of a valid CSA-MC account granting a minimum of view privileges. The Cisco IPS sensor provides the CSA-MC with this information when subscribing and the CSA- MC accepts or denies the subscription based on the validity of the credentials.

Even though any of the existing administrative accounts in the CSA-MC with a minimum of view privileges can be used, it is not recommended. For obvious security reasons, it is always a good practice to create a new account to be used exclusively for CSA-to-Cisco IPS communications purposes. This account should be given no more than the minimum required privileges (that is, monitor and view).

Figure 11-6 shows a snapshot taken from CSA-MC 6.0 showing the definition of *Cisco IPSusr*, an account defined for the exclusive use of CSA/Cisco IPS communication.

Figure 11-6 Cisco Security Agent MC Administrative Account

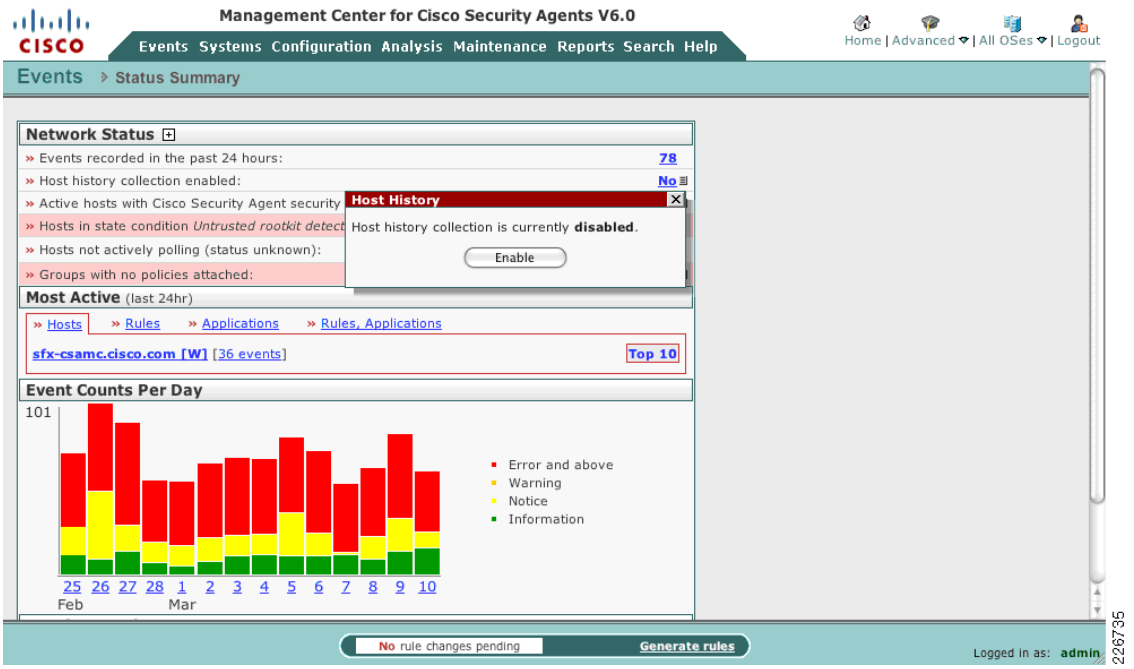


Cisco Security Agent Host History Collection

Host history collection is a feature required for the integration between CSA and Cisco IPS. When enabled, this feature maintains a two-week history of the previously listed host status changes which are maintained for every host registered with the MC. The information includes host registration, test-mode setting changes, learn-mode setting changes, IP address changes, Cisco Trust Agent (CTA) posture changes, CSA version changes, and host active/inactive status changes.

Host history collection is configured in CSA-MC via **Events > Status Summary**. Under the *Network Status* section, click **No** next to *host history collection enabled* and then click **Enable** in the popup window. See Figure 11-7.

Figure 11-7 Host History Collection



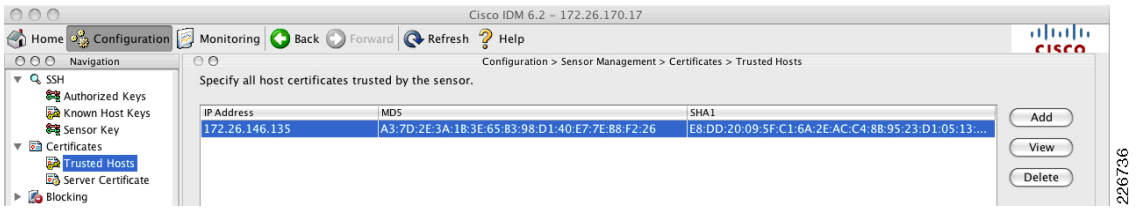
Adding CSA-MC System as a Trusted Host

Cisco IPS maintains a list of all the trusted hosts with which it communicates—including blocking devices, SSL/TLS servers, and external products, such as CSA-MC. This list contains the digital certificates of the trusted systems used by the Cisco IPS to establish secure connections.

As part of the CSA/Cisco IPS interface configuration, the system running CSA- MC must be added as a trusted host. In the process of adding the system, the Cisco IPS retrieves the digital certificate of the CSA-MC and displays its fingerprint—which is then presented to the administrator for approval. After the administrator approves the associated fingerprint, the CSA-MC system is added as a trusted host.

Figure 11-8 is a snapshot of Cisco IPS Device Manager 6.2 showing host 172.26.146.135 (system running CSA-MC) listed as a trusted host.

Figure 11-8 Cisco IPS Trusted Host



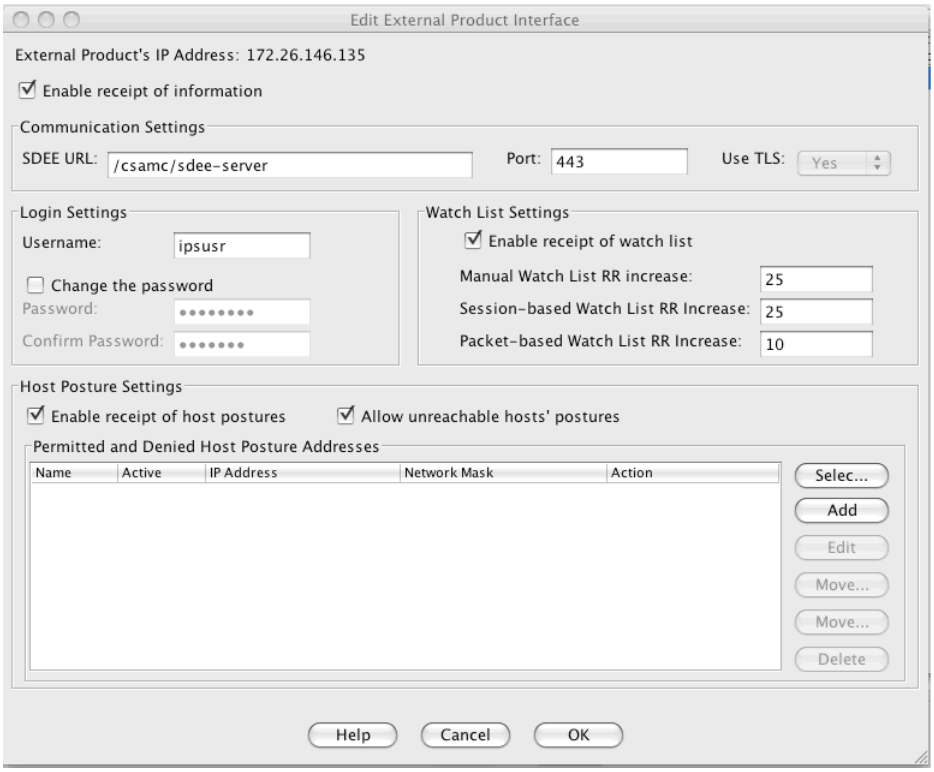
Configuring Cisco IPS External Product Interface

Cisco IPS sensors are equipped with an *external product interface* designed to handle communications with external security and management products such as the CSA-MC. This interface enables the Cisco IPS sensors to take full-advantage of useful host posture and threat context information maintained by CSA-MC—including the OS type of the systems protected with CSA and a list of IP addresses of systems suspected of causing malicious activity. This grade of collaboration increases the overall security effectiveness of the CSA/Cisco IPS combination as an end-to-end security solution.

Note With Cisco IPS Sensor Software 6.1, only two external interfaces can be defined. CSA-MC is the only external product supported at this time.

The configuration of the Cisco IPS external product interface consists in the definition of communication parameters, watch lists settings, and host posture settings (see Figure 11-9).

Figure 11-9 Cisco IPS External Product Interface



The following describe all the relevant parameters configured in the external product interface:

- *General parameters*
  - External Product IP Address—IP address of the system hosting CSA-MC.
  - Enable Receipt of Information—Enables/disables the external product interface.
- *Communication settings*—Defines the communication parameters.
  - SDEE URL—Specifies the URL used to communicate with CSA-MC. A default SDEE URL is provided.

  - Port—Used for communications. Default port is 443.
  - Use TLS—Indicates that secure TLS communication is enabled. Communication is always protected with TLS, this parameter cannot be changed.
- *Logging settings*—Sets the username and password used in the communication with CSA-MC.
  - Username—Username of the administrative account used to communicate with CSA-MC. This account is defined in the CSA-MC.
  - Password/Confirm Password—Password of the administrative account used to communicate with CSA-MC.
- *Watch list settings*—This section of the configuration is used to enable or disable the reception of watch lists. It also defines the values in which risk rating should be increased. Configuration is described in the next section.
- *Host posture settings*—Defines how host posture information should be handled. Configuration is described in the next section.

Leveraging Endpoint Posture Information

One of the key advantages of the CSA/Cisco IPS integration is that it gives the Cisco IPS sensor the ability to use the OS type information identified by the CSAs. This information extends the endpoint visibility of the Cisco IPS, helping it make smarter decisions and consequently reducing the chances for false-positives.

A false-positive is an event where the Cisco IPS triggers an alarm in response to an activity that is actually not malicious, or where the Cisco IPS triggers a response action that is out of proportion. The problem of false-positives often occurs when the Cisco IPS fails to interpret the risk level associated with the network event in question—typically due to the lack of context information. By using the OS type information provided by CSA, the Cisco IPS can better determine the appropriate relative risk associated with a particular event, thereby reducing the possibility of a false positive.

Starting with Cisco IPS Sensor Software 5.0, Cisco IPS alerts are evaluated under a sophisticated risk rating mechanism that takes into consideration attack relevancy. Under this mechanism, each Cisco IPS alarm is quantified with a numerical value between 0 and 100, called *risk rating*, which gives the user an idea of the relative risk associated with the event triggering the alarm. In practice, risk rating is used to either highlight events that require immediate attention when the sensor is configured in promiscuous mode (IDS), or trigger response actions when the sensor is configured in inline protection mode (IPS). Along all the variables used to calculate the risk rating, there is an *Attach Relevancy Rating* which represents whether or not the target is believed to be vulnerable to the attack.

For a detailed description on how risk rating is calculated, refer to the following documents:

- *Cisco IPS Configuration Guides*

  http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/products_installation_and_configuration_guides_list.html
- *Integrating Cisco Security Agent with Cisco Intrusion Prevention System*

  http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5729/ps5713/ps4077/prod_white_paper0900aecd805c389a_ns441_Networking_Solutions_White_Paper.html

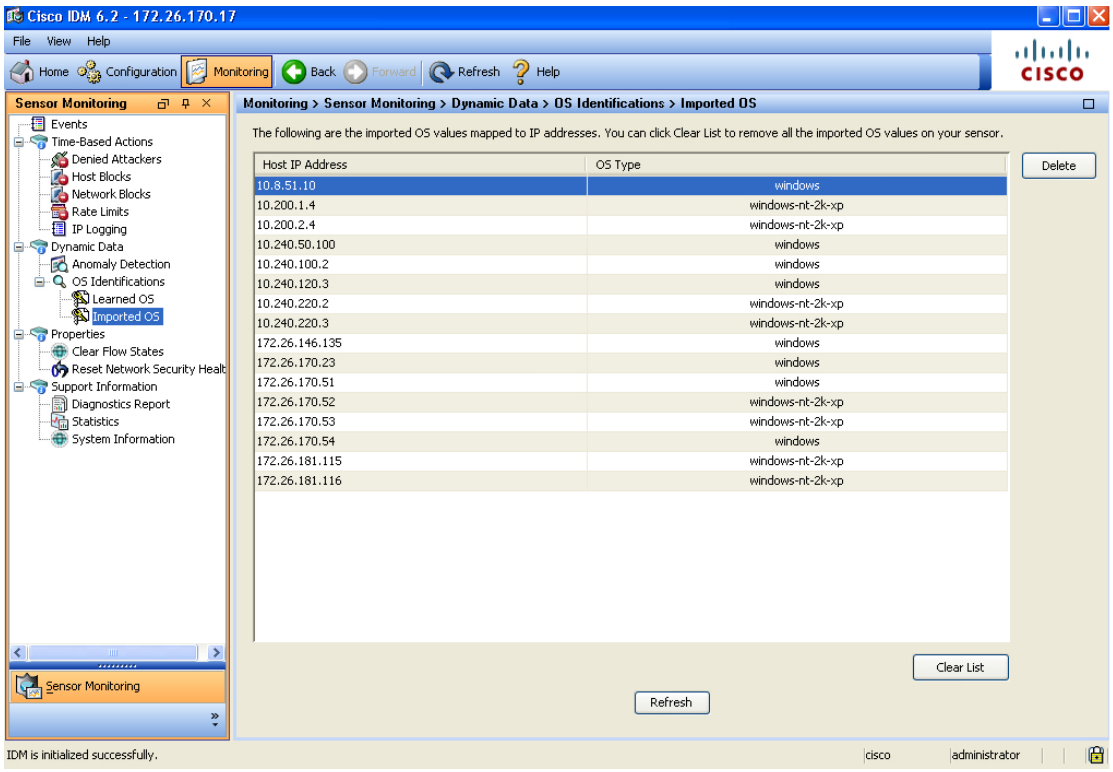
When integrated with CSA, Cisco IPS has the capacity to dynamically adjust the risk rating values based on the OS type information imported from CSA, thereby helping it to determine the right risk level of an event. This way, the Cisco IPS is capable of reducing the perceived severity of an attack when the target OS type is found not to be vulnerable and of increasing it when the target OS is known to be vulnerable.

To activate this functionality, the reception of endpoint posture information should be configured within Cisco IPS external product interface. Under the *Host Posture Settings* section, complete the following:

- *Enable Receipt of Host Postures*— Enables/disables the reception of host posture information from CSA-MC.
- *Allow Unreachable Hosts' Postures*—Allows/denies the reception of host posture information for hosts not reachable by CSA-MC. This option is useful in filtering the host postures with IP addresses that might not be visible to the Cisco IPS or that might be duplicated across the network.
- *Posture ACLs*—By default all host postures are processed by the Cisco IPS. Posture ACLs provide a mechanism to filter the network ranges from which host postures will be processed or ignored (permitted or denied). This option is useful in filtering the host postures with IP addresses that might not be visible to the Cisco IPS or that might be duplicated across the network.

Figure 11-10 is a snapshot of Cisco IPS Device Manager 6.2 that shows all the endpoint posture information imported from CSA-MC.

Figure 11-10 Cisco IPS OS Identification



The following output is the detailed event information from Cisco IPS Device Manager 6.2, corresponding to a Microsoft IIS 5.0 WebDav buffer overflow attack against system 10.240.50.100. Using the endpoint posture information learned from CSA-MC, the Cisco IPS sensor knows the system is Windows-based and, as a result, it determined to be relevant to the attack. Key information is highlighted.

```
vIdsAlert: eventId=1234240033910687083  vendor=Cisco  severity=high
  originator:
    hostId: sfx12-Cisco IPS4270-1
    appName: sensorApp
    appInstanceId: 434
  time: Mar 10, 2009 22:45:38 UTC  offset=0  timeZone=GMT00:00
```

```
  signature:   description=Long WebDAV Request  id=5365  version=S258  type=other
created=20041119
    subsigId: 0
    sigDetails: SEARCH /...\x3c40000+ chars>...
    marsCategory: Info/Misc
  interfaceGroup: vs0
  vlan: 15
  participants:
    attacker:
      addr: 10.240.100.2  locality=OUT
      port: 17185
    target:
      addr: 10.240.50.100  locality=OUT
      port: 80
      os:   idSource=imported  type=windows  relevance=relevant
  actions:
    droppedPacket: true
    deniedFlow: true
    tcpOneWayResetSent: true
  context:
    fromTarget:
000000  48 54 54 50 2F 31 2E 31  20 34 31 34 20 52 65 71  HTTP/1.1 414 Req
! <output omitted>

    fromAttacker:
000000  62 30 25 31 64 6D 25 31  66 57 25 38 39 25 31 32  b0%1dm%1fW%89%12
! <output omitted>

  riskRatingValue: 95  targetValueRating=medium  attackRelevanceRating=relevant
watchlist=25
  threatRatingValue: 60
  interface: ge3_1
  protocol: tcp
```

Cisco Security Agent Watch Lists

As part of its threat control function, the CSA has the ability to quarantine hosts that violate security rules or exhibit malicious behavior. The quarantine of a host occurs either dynamically as a result of the global correlation of events from multiple CSAs, or manually by configuration of an administrator. When quarantined, the IP address of the host is added to the *Quarantine IP list* and all systems running CSA are instructed to block any communication attempt with the affected host.

For improved threat visibility and overall control, the Cisco IPS external product interface can be configured to use the quarantine information generated by the CSA. This way, every time a host is quarantined, the CSA will send a quarantine event to each one of the Cisco IPS sensors subscribed for the reception of quarantine information. Quarantine events include the reason for the quarantine, the protocol associated with a rule violation (TCP, UDP or ICMP), and the IP address of the host to be quarantined.

With all the quarantine information provided by CSA, each Cisco IPS sensor builds and maintains a watch list. The purpose of the watch list is to help the Cisco IPS monitor systems identified by the CSA as suspicious or malicious and to highlight any events associated with these systems. The watch list identifies systems that the Cisco IPS must monitor closely and which risk ratings must be increased. The watch list does not extend the quarantine of the hosts in the list to the Cisco IPS. In fact, the Cisco IPS does not block a host solely because it is part of the list.

Note For a host, being on the watch list translates into being quarantined by the CSA and *watched* by the Cisco IPS. The Cisco IPS does not automatically quarantine systems in the watch list.

Every time a host in the watch list triggers an alert, the resulting risk rating is increased by the watch list rating. The watch list rating is configured as part of the external product interface and consists of the following three parameters (configurable in a range of integer values between 0 to 35):

- *Manual Watch List RR increase*—Indicates the value by which risk rating should be increased for events associated with hosts that were manually added to the watch list. By default, the increase value is set to 25.
- *Session-based Watch List RR increase*—Indicates the value by which risk rating should be increased for events associated with TCP connections added to the watch list as a result of CSA global correlation. By default the increase value is set to 25.
- *Packet-based Watch List RR increase*—Indicates the value by which risk rating should be increased for events associated with UDP-based sessions added to the watch list as a result of CSA global correlation. By default the increase value is set to 10.

A host can be added to the watch list either manually by a CSA administrator or as a result of CSA global correlation:

- Manual Configuration—A CSA administrator may chose to manually quarantine systems known to be compromised, or that need to be isolated from the network for any particular reason. To quarantine a host manually, the administrator must add the IP address of the host to the **Quarantined IP Addresses** list. This is done by accessing the dynamically quarantined IP addresses link within the Global Event Correlation section in CSA-MC, and by adding a new entry with the host IP address.
- Dynamic Global Correlation—CSA can be configured to quarantine hosts dynamically when they violate a security rule, communicate with an untrusted host, or exhibit malicious behavior. The configuration of dynamic quarantining requires the definition of a rule setting the offending host as globally untrusted, and to enable the global correlation of the event.

For information on how to define manually or dynamically quarantine systems, refer to I*ntegrating Cisco Security Agent with Cisco Intrusion Prevention System* at the following URL:

http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5729/ps5713/ps4077/prod_white_paper0900aecd805c389a.html

Cisco IPS Event Action Override

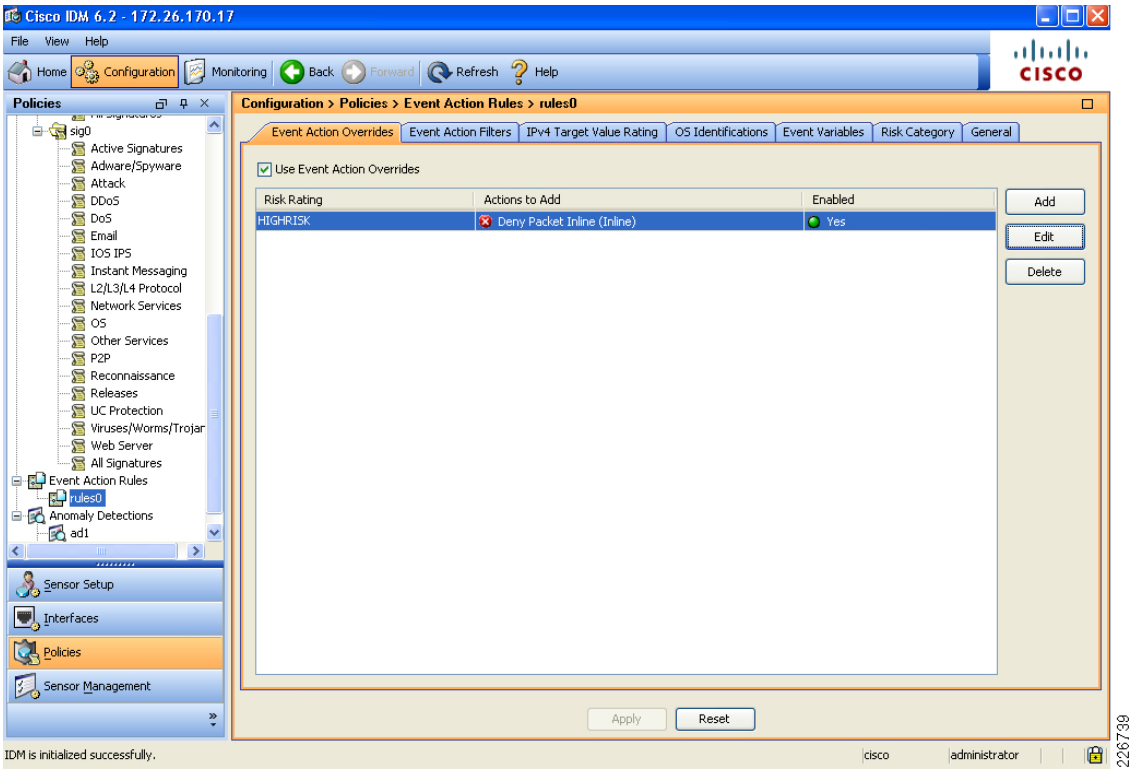
The Cisco IPS implements watch lists primarily to highlight the activity of suspicious systems and, while the CSA isolates the hosts in the list, the Cisco IPS does not enforce quarantine automatically—although it is possible to combine the watch list with one or more event action overrides to dynamically block hosts in the list.

An event action override is a general rule that sets response actions for events with risk ratings falling into specific ranges and that supersedes the actions defined at the signature level. As a result of a watch list, the Cisco IPS increases the risk rating of the events triggered by the systems in the list. An event action override can be configured to block the offending host once it triggers an event exceeding a predefined threshold.

The event action override should be configured to block the attacker inline when the system is configured in inline protection mode (IPS) and to block the host with a shunning when the system is in promiscuous mode (IDS).

These concepts are illustrated in Figure 11-11.

Figure 11-11 Event Action Override



In Figure 11-11, one event action override is defined for a Cisco IPS configured in inline protection mode. Network events triggering alarms with a high risk rating (more than 90) will cause the source host to be blocked inline by the Cisco IPS. Other risk rating values are medium risk (from 70 but less than 90) and low risk (less than 70).

The implementation of event action overrides is a useful tool that extends the quarantine of hosts by the CSA to the Cisco IPS, thereby delivering a true end-to-end enforcement from the endpoint to the network. While the use of this practice yields clear benefits, there are some important aspects that should be considered prior to its adoption:

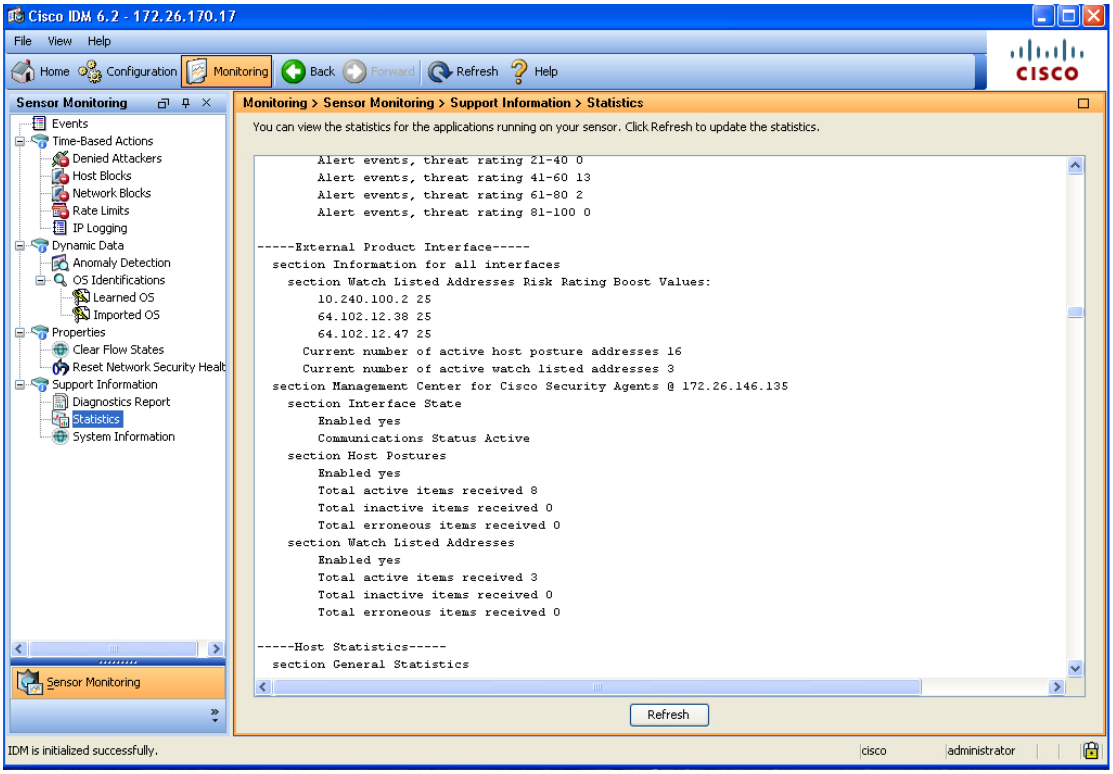
- After an event action override is set, it applies to all events with risk ratings falling in the range configured—not only those concerning hosts in the watch list.
- The Cisco IPS will not enforce any action until the host present in the watch list triggers an event with a resulting risk rating that falls in the range specified for the event action override. This means the Cisco IPS will not quarantine a host immediately after it receives a quarantine event from CSA-MC. An action on the host will be enforced only after the host triggers an event in the Cisco IPS.

Validating Cisco Secure Agent and Cisco IPS Integration

The statistics plane within the Cisco IPS Device Manager 6.2 provides valuable information that is useful for verifying the status of the external product interface, the reception of endpoint posture information, and CSA watch-lists. Within the Cisco IPS Device Manager 6.2, the statistics tab is accessible via **Monitoring > Sensor Monitoring > Support Information > Statistics**.

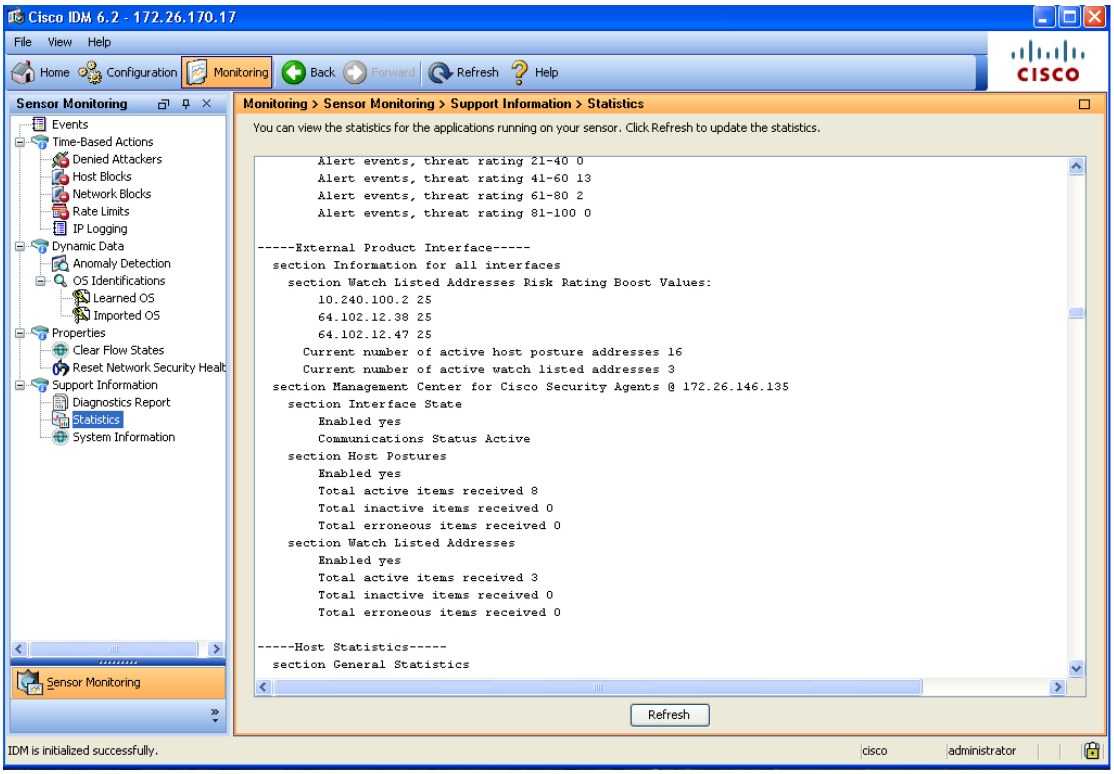
To verify the status of the external product interface, scroll-down to *External Product Interface* and look for *Communications Status*. The active status confirms the Cisco IPS sensor was able to open its subscription session with CSA-MC. The same section displays the list of systems in the CSA watch-list. See Figure 11-12.

Figure 11-12 External Product Interface Status



The *OS Identification Statistics* section displays the list of OS posture records imported from CSA-MC. The list can also been seen by accessing **Monitoring > Sensor Monitoring > Dynamic Data > OS Identifications > Imported OS**. This is illustrated in Figure 11-13.

Figure 11-13 Imported OS



Unified Management and Control

Cisco Security Manager (CSM) is a GUI-based, enterprise-class management application designed to enable scalable management of security policies on Cisco security devices by supporting integrated provisioning of firewall, Cisco IPS, and virtual private networking (VPN)—site-to-site, remote access, and SSL—services across Cisco IOS routers, Cisco Adaptive Security Appliances (ASA), Cisco Catalyst 6500/7600 security service modules, Cisco IPS appliances, and Cisco IPS modules. CSM efficiently manages a wide range of networks—from small networks consisting of a few devices to large networks with thousands of devices. Scalability is achieved through a rich feature set of shareable objects and policies and device grouping capabilities.

The primary benefits of using CSM are as follows:

- *Scalable network management*—Centrally administer security policies and device settings for either small networks or large scale networks consisting of thousands of devices. Define policies and settings once and then optionally assign them to individual devices, groups of devices, or all the devices in the enterprise.
- *Provisioning of multiple security technologies across different platforms*—Manage VPN, firewall, and Cisco IPS technologies on routers, security appliances, Cisco Catalyst devices and service modules, and Cisco IPS devices.
- *Provisioning of platform-specific settings and policies*—Manage platform-specific settings on specific device types. For example: Routing, 802.1x, Easy Secure Device Deployment (EzSDD), and NAC on routers; and, device access security, DHCP, AAA, and multicast on firewall devices.

- *VPN wizard*—Quickly and easily configure site-to-site, hub-and-spoke, and full-mesh VPNs across different VPN device types.
- *Multiple management views*—Device, policy, and map views enable you to manage your security in the environment that best suits your needs.
- *Reusable policy objects*—Create reusable objects to represent network addresses, device settings, VPN parameters, and so on, then use them instead of manually entering values.
- *Device grouping capabilities*—Create device groups to represent your organizational structure. Manage all devices in the groups concurrently.
- *Policy inheritance*—Centrally specify which policies are mandatory and enforced lower in the organization. New devices automatically acquire mandatory policies.
- *Role-based administration*—Enable appropriate access controls for different operators.
- *Workflow*—Optionally allow division of responsibility and workload between network operators and security operators and provide a change management approval and tracking mechanism.
- *Single, consistent user interface for managing common firewall features*—Single rule table for all platforms—including routers, Cisco PIX Security Appliances, Cisco ASAs, and Cisco Firewall Software Modules (FWSM).
- *Intelligent analysis of firewall policies*—The conflict detection feature analyzes and reports rules that overlap or conflict with other rules. The ACL hit count feature checks in real-time whether specific rules are being hit or triggered by packets.
- *Sophisticated rule table editing*—Inline editing, ability to cut, copy, and paste rules and to change rule order in the table.
- *Discover firewall policies from device*—Policies that exist on the device can be imported into CSM for future management.
- *Flexible deployment options*—Support for deployment of configurations directly to a device or to a configuration file. You can also use Auto-Update Server (AUS), Configuration Engine, or Token Management Server (TMS) for deployment.
- *Rollback*—Ability to roll back to a previous configuration if necessary.
- *FlexConfig (template manager)*—Intelligent CLI configlet editor to manage features that are available on a device, but that are not natively supported by CSM.

CSM works in conjunction with the CS-MARS. Used together, these two products provide a comprehensive security management solution that addresses configuration management, security monitoring, analysis, and mitigation. While CSM lets you centrally manage security policies and device settings in large-scale networks, CS-MARS is a separate application that monitors devices and collects event information, including Cisco IPS event information, Syslog messages and NetFlow traffic records. CS-MARS aggregates and presents massive amounts of network and security data in an easy-to-use format. Based on information derived from CS-MARS reports, you can edit device policies in CSM to counter security threats.

Specifically, if you use CSM to configure firewall access rules and Cisco IPS signatures, you can configure CS-MARS to collect information related to those policies and make it available to CSM users. By registering the CS-MARS servers with CSM, users can navigate directly from a specific access rule or Cisco IPS signature to a CS-MARS report window, pre-populated with query criteria for that rule or signature.

Similarly, CS-MARS users can view the CSM policies related to specific CS-MARS events. This bi-directional mapping of specific events to the policies that triggered them, combined with the ability to immediately modify the policies, can dramatically reduce the time spent configuring and troubleshooting large or complex networks.

CSM and CS-MARS Cross-Communication Deployment Considerations

To enable the cross-communication between CSM and CS-MARS, you must register the CSM servers with the CS-MARS servers and register the CS-MARS servers with the CSM servers. You must also register the specific devices with each application. Then, when working with firewall access rules or Cisco IPS signatures for a device, a CSM user can quickly view real-time and historical event information related to that rule or signature.

When deploying the CSM and CS-MARS cross-communication linkages, there are a few important considerations that should be noted when integrating the two products:

- Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS) is required for communication between the CSM server and CS-MARS.
- The clock on all devices must be in-sync, including CS-MARS, CSM, and the devices they monitor and manage.
- To query for CS-MARS events for Cisco FWSM, Cisco PIX, and Cisco ASA devices on which multiple independent security contexts exist, you must define a unique management IP address in the CSM for each security context. The host name and reporting IP address for each virtual context must be configured before adding it to CS-MARS—otherwise, event lookup from policies on these contexts fails.
- For all Cisco IPS device and service policies, a default signature policy is assigned to the device when you do not discover Cisco IPS policies, or when you remove the configured policies from the device. If you try to perform an event lookup from the default signature, a *Policy not found* error message is displayed. However, if you edit the default signature and save it, you can then navigate to events in CS-MARS.
- If object grouping (or rule optimization) is enabled for an access rule defined in CSM, and the associated access-list commands on the device do not match the optimized rules, no events are displayed in CS-MARS because of the mismatch between CSM and the device.
- If logging is not enabled for an access rule on the Cisco ASA, Cisco PIX, and Cisco FWSM devices, or if logging is not enabled on Cisco IOS routers for access rules, a warning message is displayed and you can only look up traffic-flow events for those rules.
- The CSM server that you add to CS-MARS can be used to perform policy lookup only for those devices that it manages and that publish events to CS-MARS.
- Each CS-MARS local controller can query only one CSM. You cannot define more than one CSM server per local controller. However, the same CSM server can be defined on multiple local controllers.
- CSM must be running version 3.2 or higher if you want to look up the policy table and modify matching rules or signatures. If you add a CSM server running 3.0.1, 3.0.2, or 3.1.x to a CS-MARS appliance running 4.3.2 through 4.3.4 or 5.3.2 through 5.3.4, you can query for policies in view mode only; you must open a CSM client instance separately to modify the policies.

Registering CSM with CS-MARS

In order to cross-launch CSM from within CS-MARS to view the firewall and Cisco IPS policies associated with triggered events, CSM must be registered with CS-MARS. The CSM server is registered in CS-MARS by defining a host with a software application residing on that host. In order to add CSM to CS-MARS, the user must be logged in with an administrative role and perform the following tasks:

Step 1 Add CSM as a SW security application in the *Security and Monitor device* section on the CS-MARS *Admin* window.

Step 2 Add the appropriate access and reporting IP (these addresses will typically be the same) and add the CSM interface IP address and subnet mask information

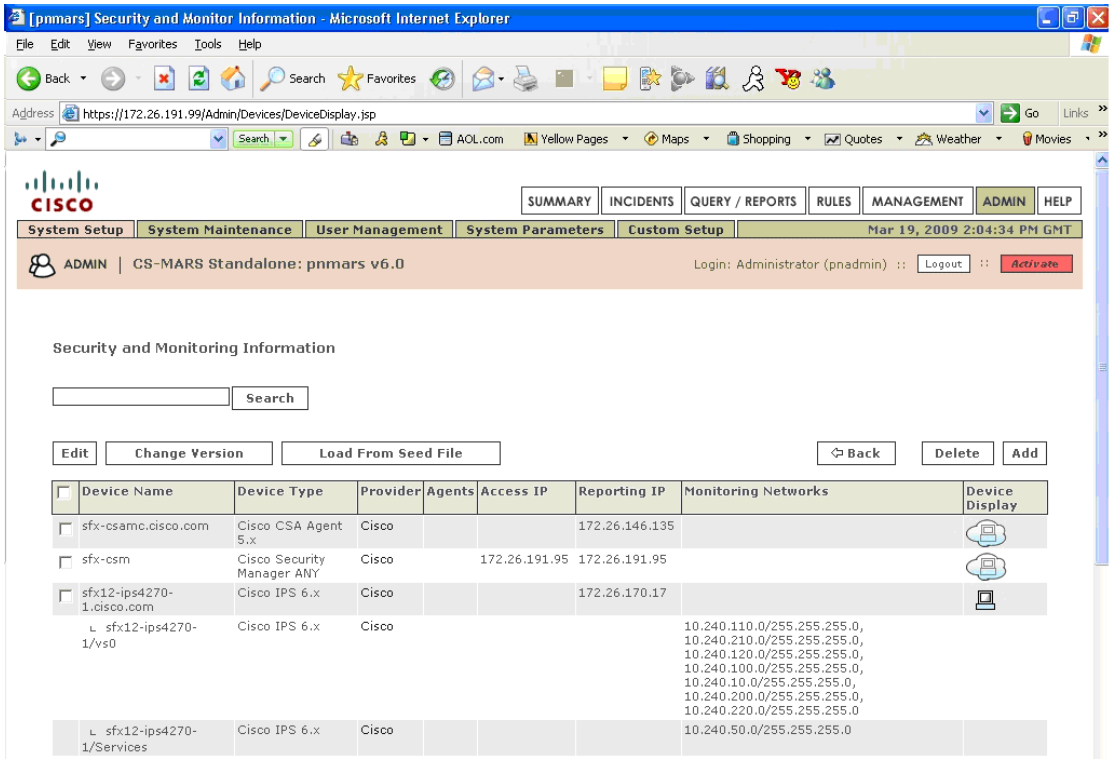
Step 3 In the reporting application section, select **Cisco Security Manager ANY**.

Step 4 Perform a connectivity test and select whether you want users to use a standard CS-MARS login ID or prompt users for separate login credentials when launching CSM.

Note It is recommended that users be prompted to enter their own login credentials when cross launching CSM from within CS-MARS. This will enable activity to be tracked and ensure that only authorized administrators can make changes to CSM managed devices.

Figure 11-14 shows CSM (*sfx-csm*) registered with CS-MARS.

Figure 11-14 CSM Registered with CS-MARS



Registering CS-MARS in CSM

In order to view real-time and historical event information related to firewall access rules and Cisco IPS signatures, CS-MARS must be registered with CSM. The specific CS-MARS must also be registered to the specific managed device within CSM. In order for the CSM server to be queried by CS-MARS, the CSM must have a user account that the CS-MARS can use to access it. If using AAA for authentication and authorization, the following actions can be performed with respect to the user accounts:

- If using Common Services AAA authentication on the CSM server—for example, Cisco Secure Access Control Server (CS-ACS), you must update the administrative access settings to ensure that the CS-MARS account has the necessary client access to the CSM server.

Note When you register a CSM server with CS-MARS, it is recommended that you select the option to prompt users for CSM credentials for policy table lookup. In this case, a separate CS-MARS account in Common Services might not be necessary for authentication purposes.

- If you are using local authentication and authorization, you must define a user account in CSM that CS-MARS can use to perform queries. Separate user accounts are recommended to provide a specific audit trail on the CSM server. These accounts must be assigned one of the following Common Services roles:
  - Approver
  - Network operator
  - Network administrator
  - System administrator

Users with the help desk security level can only view the policy lookup table in CS-MARS. They cannot cross-launch CSM to modify policies.

For more information on adding users and associating roles with them in Common Services, see the applicable *User Guide for CiscoWorks Common Services*, such as the following: http://www.cisco.com/en/US/docs/net_mgmt/ciscoworks_common_services_software/3.1.1/user/guide/cs311book.html

In order to register CS-MARS with CSM, you must be logged in as a user with an Admin role and perform the following tasks:

Step 1 Add CS-MARS from the *Security Manager Administration* page.

Step 2 Enter the *hostname/IP address*, *username*, and *password* information for accessing CS-MARS.

Step 3 Retrieve the certificate thumbprint from CS-MARS.

Step 4 Accept the certificate to register CS-MARS with CSM.

Step 5 Once CS-MARS is registered with CSM, you must map the specific CS-MARS to the individual managed devices within CSM. This is done by updating the device properties of each of the managed devices and discovering the specific CS-MARS from the list of CS-MARS devices which are registered with CSM.

The example CSM window in Figure 11-15 illustrates CS-MARS with the IP address of 172.26.191.99 is registered with CSM.

Figure 11-15 CS-MARS Registered with CSM

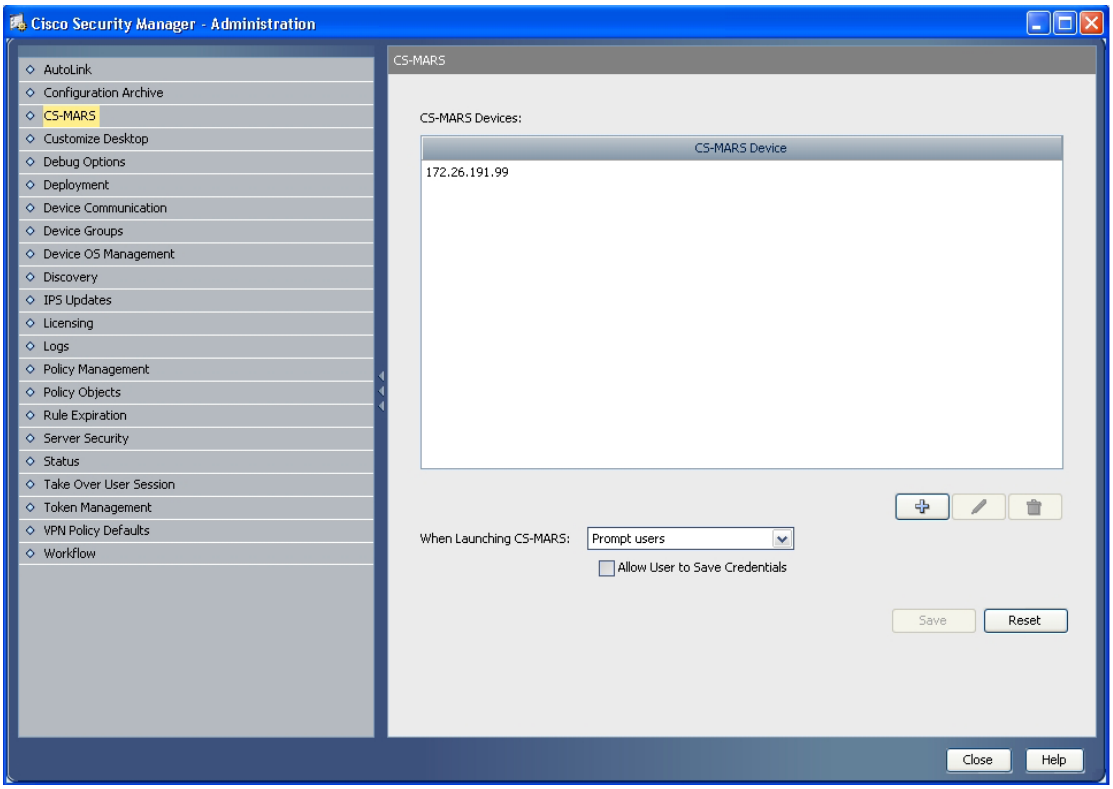
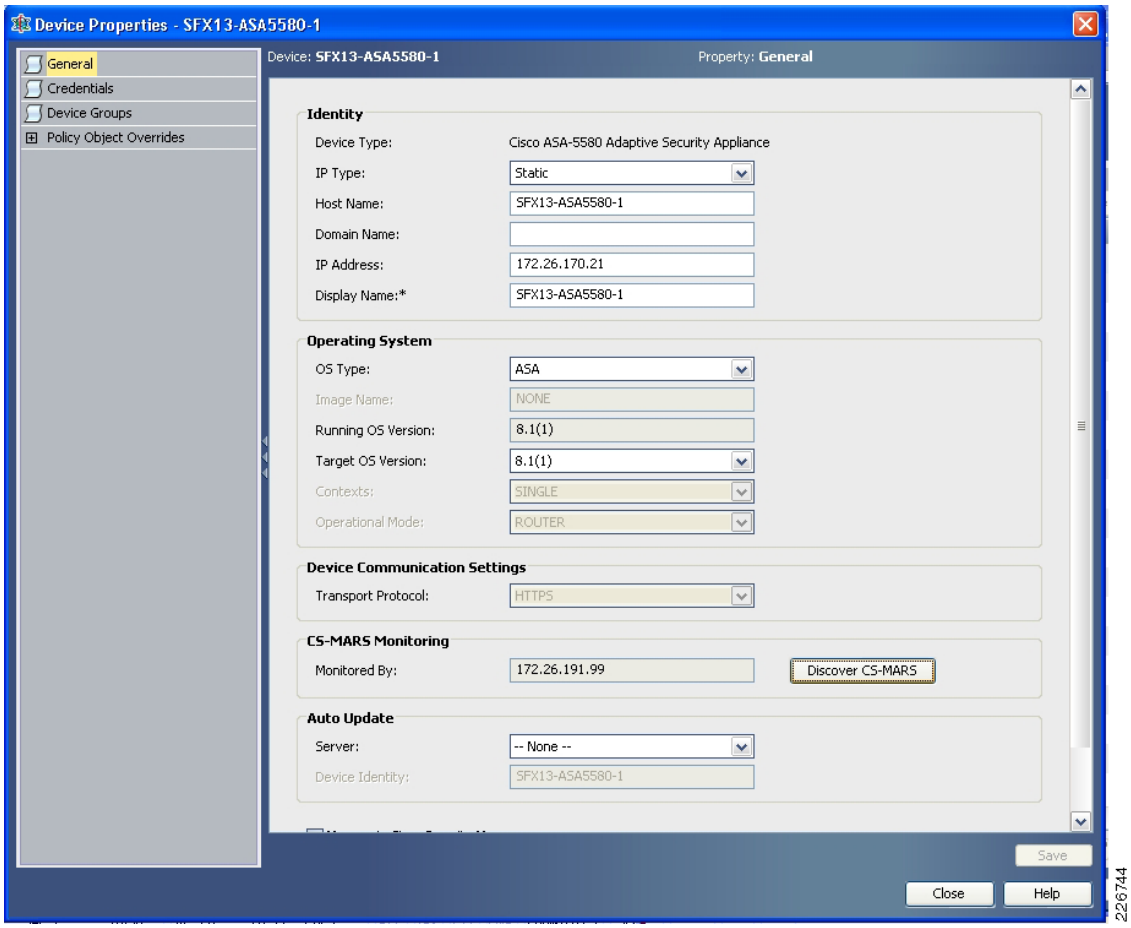


Figure 11-16 illustrates that the *SFX13-ASA5580-1* firewall is being monitored by the CS-MARS with the IP address 172.26.191.99:

Figure 11-16 Firewall Monitored by CS-MARS



CSM and CS-MARS Linkage Objectives

The following summarizes the objectives of the CSM and CS-MARS cross-communication linkages:

- Support for MARS to CSM cross launch
- Support for CS-MARS to CSM (event-to-policy) firewall cross linkages
- Support for CSM to CS-MARS (policy-to-event) firewall cross linkages
- Support for CS-MARS to CSM (event-to-policy) Cisco IPS cross linkages
- Support for CSM to CS-MARS (policy-to-event) Cisco IPS cross linkages
- Troubleshoot and diagnose network security incidents relating to Firewall and Cisco IPS policies in CSM
- Find reported events in CS-MARS with ***linking*** back to the triggering policy in CSM
- Find events in CS-MARS by clicking a policy of interest in CSM
- Enable quick policy collaboration between CS-MARS and CSM

Firewall Cross Linkages

CSM and CS-MARS cross-communication linkages for firewall policies and events include:

- Support for CS-MARS-to-CSM (event-to-policy) firewall cross-linkages
- Support for CSM-to-CS-MARS (policy-to-event) firewall cross linkages

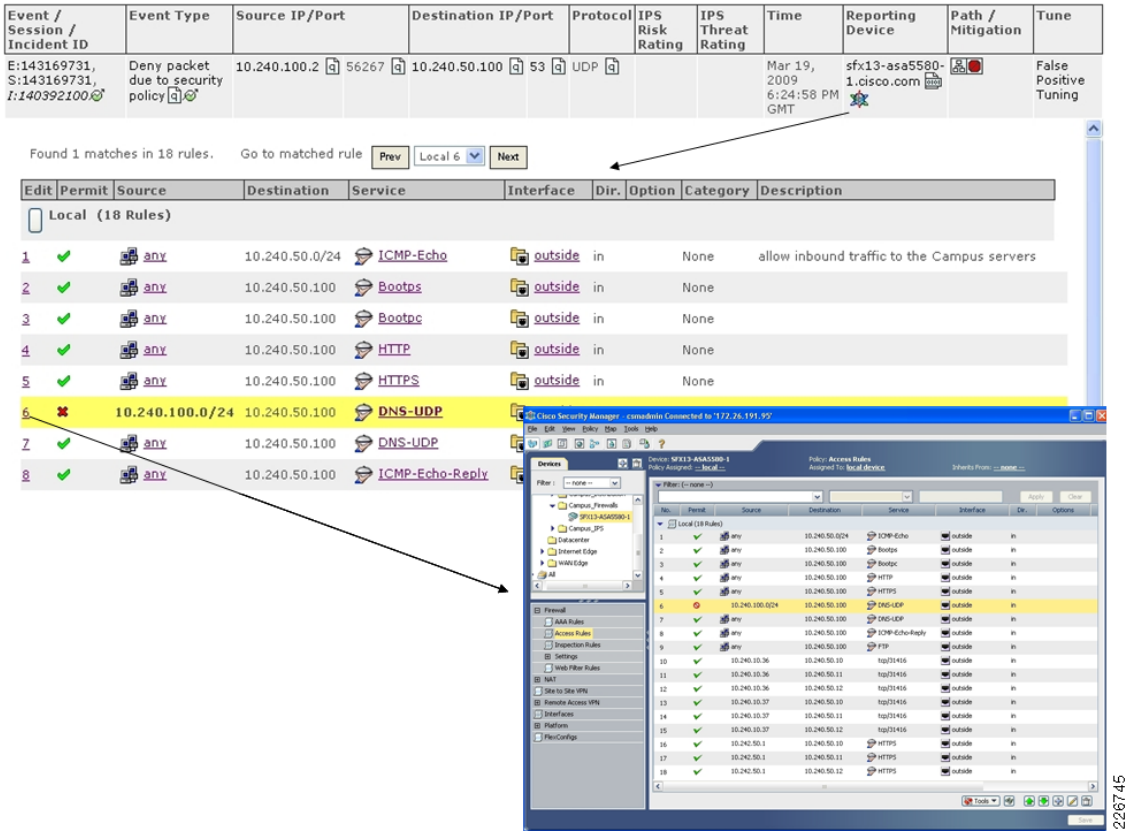
Firewall Cross Linkage: CS-MARS Event to CSM Policy

Firewall access rules filter network traffic by controlling whether routed packets are forwarded or blocked at the firewall's interfaces. After configuring and deploying access rules from the CSM to a firewall device and enabling logging on the device monitored by MARS, a log entry is created when an access rule matches the network traffic that the device is processing and the action defined in the rule is used to decide if traffic must be permitted or denied. An incident is generated in CS-MARS after the log associated with an access rule is received from the device.

Using CS-MARS, you can navigate from the event messages that are generated in CS-MARS to the configured access policy in CSM. You can then edit the access policy as needed to tune attributes of the rule or the action it takes on it.

Figure 11-17 illustrates the CSM/CS-MARS event-to-policy firewall cross linkage.

Figure 11-17 CSM and CS-MARS Event



Firewall Cross Linkage: CSM Policy to CS-MARS Event

Firewalls that are monitored by CS-MARS continually forward event information to CS-MARS. These events are stored in the CS-MARS database. Querying for historical events from CSM lets you view event information stored in the CS-MARS database. You also can navigate from policies in CSM to view events as they are forwarded to CS-MARS in nearly real-time.

From within the CSM, you can run an event query on the CS-MARS for managed access rules using the CSM and MARS cross linkage. The CSM requests specific event data by supplying the CS-MARS with relevant device details and event-identification information. The CS-MARS then creates a query based on the provided information and displays a query-related page. Real-time queries are run automatically and the results displayed. For historical queries, the *Query Criteria* window opens. You can either run the query or save the criteria as a report to run at a later time.

Because CSM and CS-MARS do not share a common device repository, the query created by CSM and sent to CS-MARS includes all the device details (management IP address, host name, domain name, and so on) available in the CSM database. CS-MARS compares this information to the device information in its database. Event lookup succeeds only if the relevant devices are recognized by both CSM and CS-MARS—and can be reached by CS-MARS using the specified IP address or fully qualified domain name.

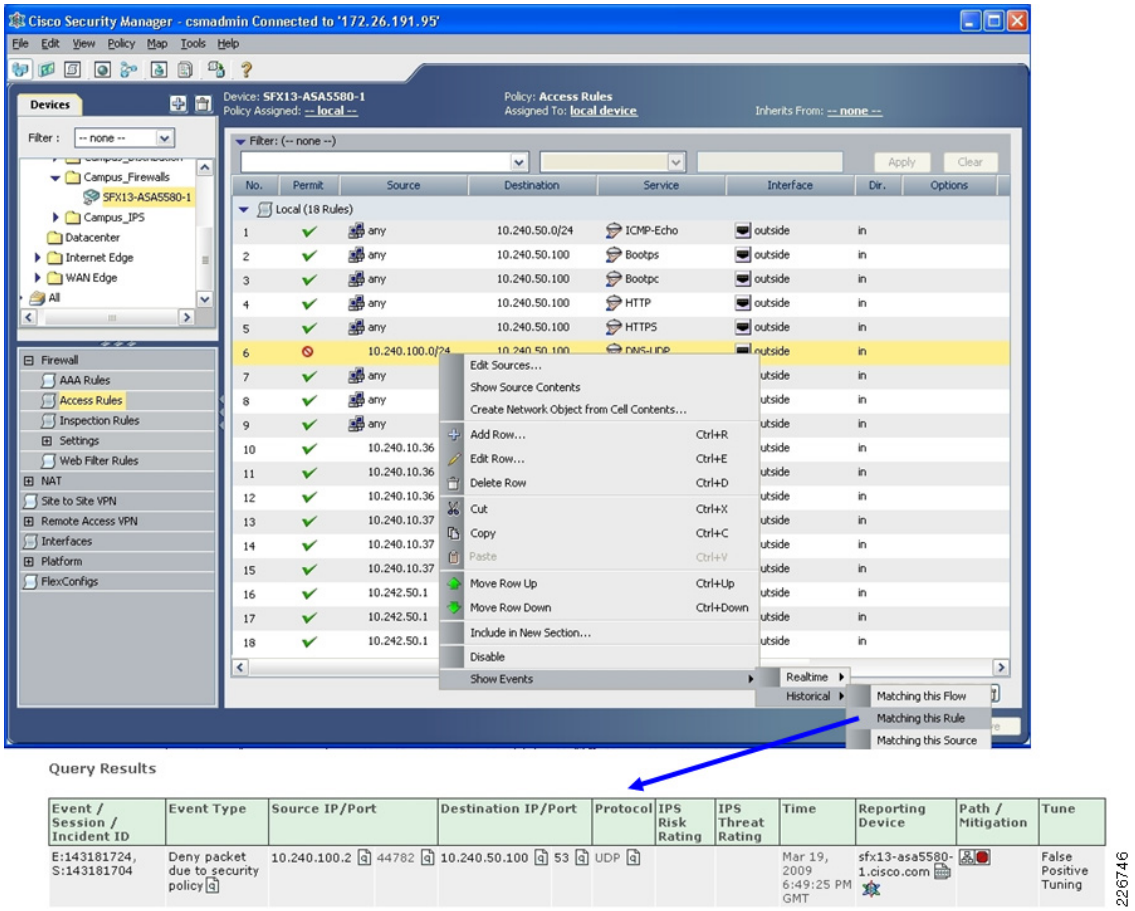
When querying for events on CS-MARS from within CSM, you can match the events based on five tuple flow information or match the rule using hash codes. Because the five tuple match is based on source IP, source port, destination IP, and timestamp, it might not be unique to the specific Cisco ACE and could produce unexpected results. If hash codes are available they can be used to match the flow to a specific Cisco ACE. This is a more granular than the five tuple match and is available on the Cisco ASA firewalls. A hash is created to uniquely identify individual Cisco ACEs within an access policy. If the CSM is used to deploy the Cisco ACE, then it knows the unique hashes associated with each Cisco ACE.

Note Large historical queries might need to run in batch mode. The CS-MARS system will automatically determine this and change the button from *Submit Inline* to *Submit Batch*.

Note Even though the query is pre-populated, the users still need to choose the time range through which they wish to search.

Figure 11-18 illustrates the CSM/CS-MARS policy-to-event firewall cross linkage for a historical query.

Figure 11-18 CSM/CS-MARS Policy-to-Event Firewall



Cisco IPS Cross Linkages

CSM and CS-MARS cross communication linkages for Cisco IPS policies and events include:

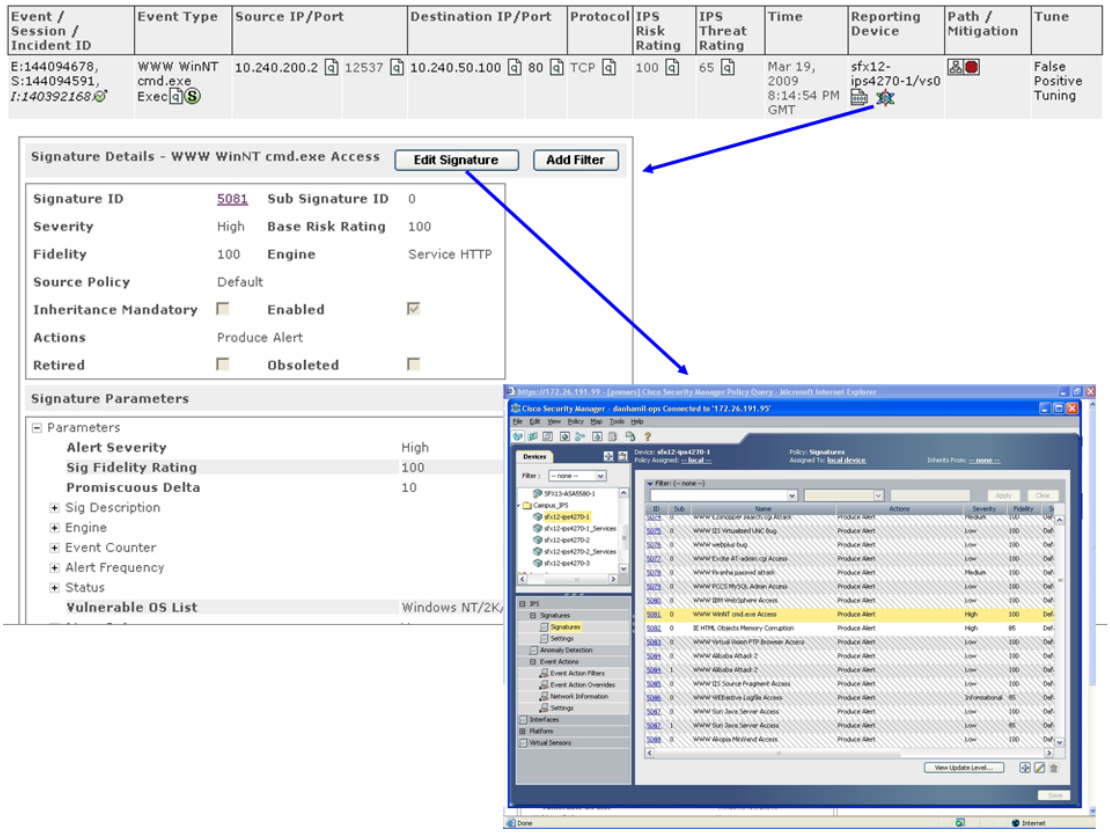
- Support for CS-MARS to CSM (event-to-policy) Cisco IPS cross linkages
- Support for CSM to CS-MARS (policy-to-event) Cisco IPS cross linkages

Cisco IPS Cross Linkage: CS-MARS Event to CSM Policy

The CSM and CS-MARS Cisco IPS event-to-policy cross linkage provides administrators with the ability to take an event within CS-MARS and link it back to the Cisco IPS signature and policy within the CSM that triggered the event. This provides the ability to quickly adjust signature policies as needed to fix problems in the network—such as false positives that create noise or that are blocking legitimate traffic.

Figure 11-19 illustrates this CSM/CS-MARS event-to-policy Cisco IPS cross linkage.

Figure 11-19 CSM/CS-MARS Event-to-Policy Cisco IPS Cross Link

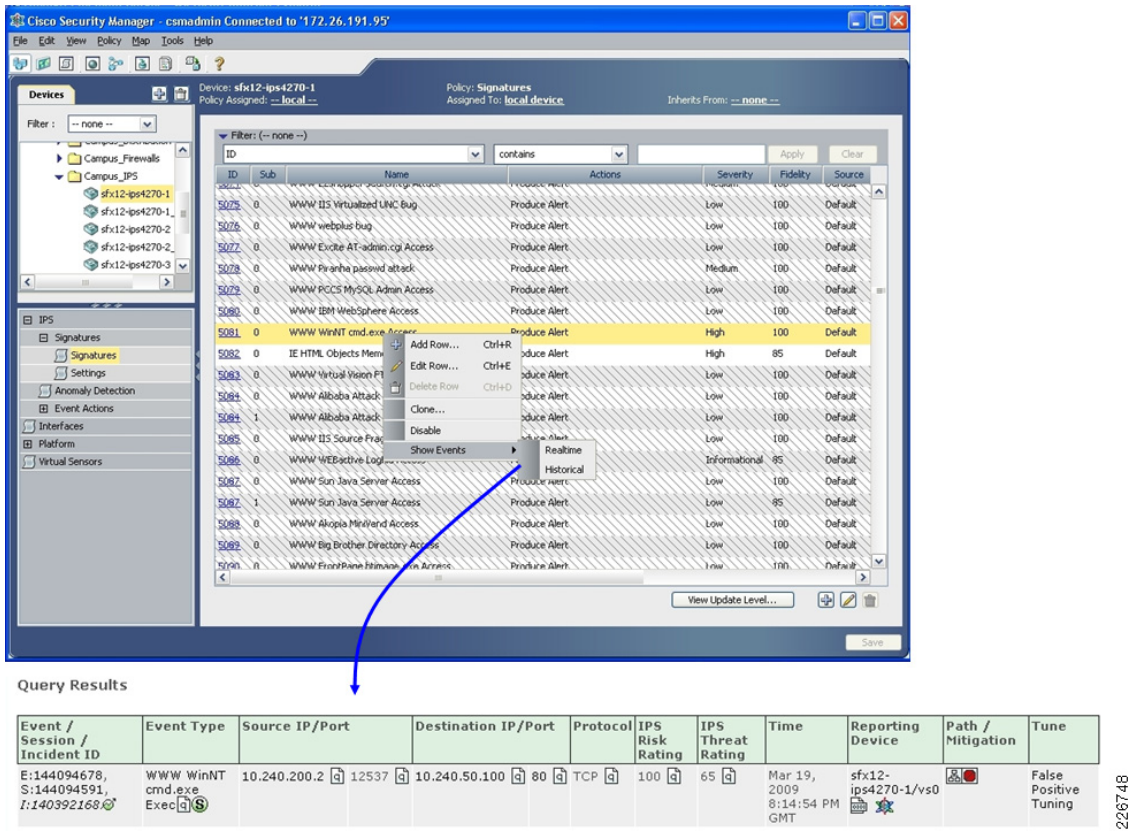


Cisco IPS Cross Linkage: CSM Policy to CS-MARS Event

The CSM and CS-MARS Cisco IPS policy-to-event cross linkage provides administrators with the ability to query events in CS-MARS from within CSM associated with Cisco IPS signatures. This provides administrators immediate insight into Cisco IPS effects on intrusions and instant verification about the effectiveness of updated policies. Event queries can be done for real-time events, as well as historical events stored on CS-MARS. When launching a CS-MARS query from within CSM, the query is automatically populated.

Figure 11-20 illustrates this CSM/CS-MARS policy-to-event cross linkage.

Figure 11-20 CSM/CS-MARS Policy-to-Event Cross Link

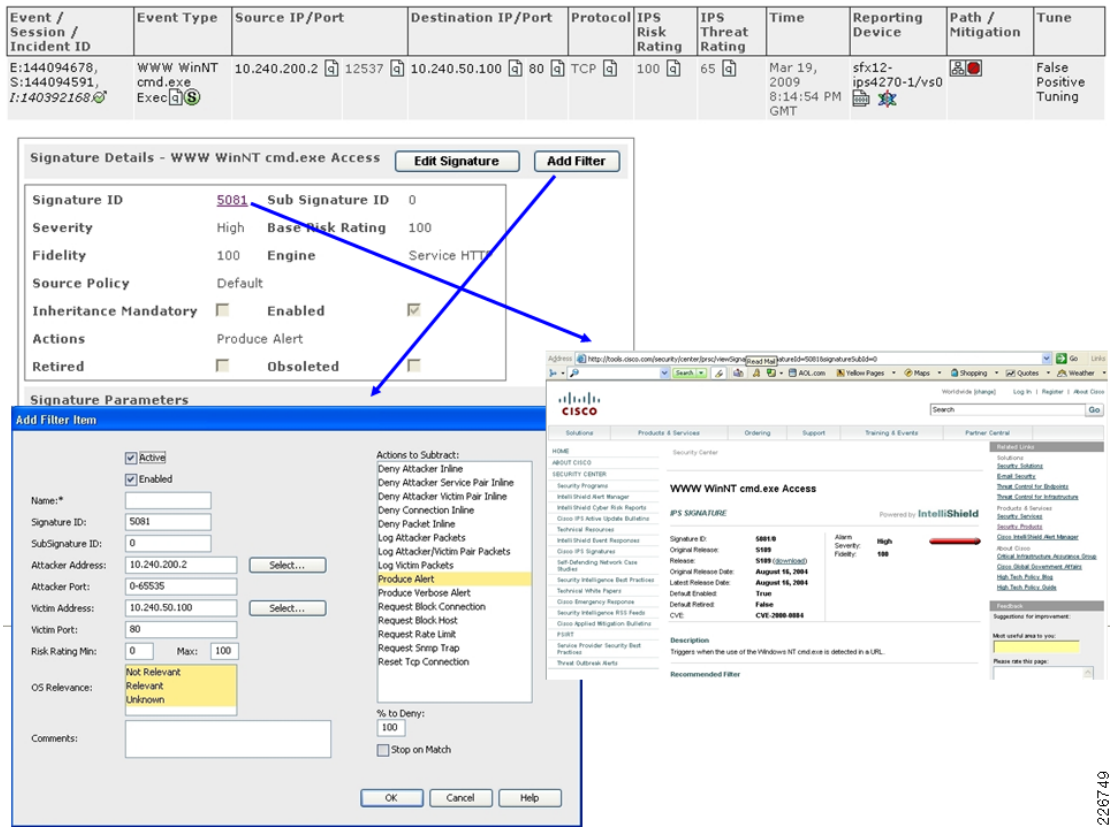


Cisco IPS Event Action Filter

Creating an event action filter (EAF) from an incident is a way to tune out false positives. When drilling down into the signature associated with a particular event, click the **Signature ID** link and to access the Cisco Security Center website. This site lists information on the Cisco IPS signatures, including known false triggers. This information can be used to quickly tune signatures in the customer environment. This collaborative Cisco IPS EAF creation enables administrators to trace events back to the triggering signature, investigate the signature, tune the signature on the fly, and rapidly deploy to a single sensor or all sensors throughout the network. EAFs can be created and enabled on a per-sensor or per-policy basis. Per-policy EAFs allows a user to change a single policy item then have that policy pushed out to all of the devices covered by that single policy.

Figure 11-21 illustrates the flow of this collaborative Cisco IPS EAF creation flow.

Figure 11-21 Collaborative Cisco IPS EAF Creation

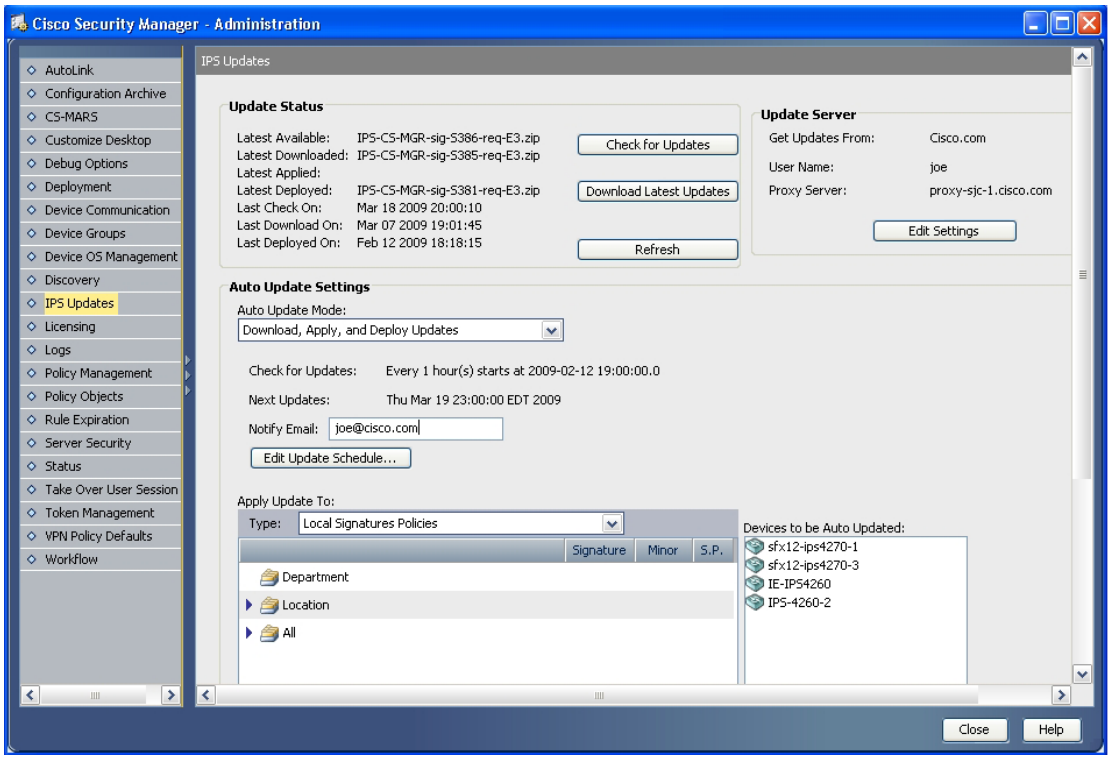


CSM Automatic Cisco IPS Updates

Another important feature that CSM provides for managed Cisco IPS devices is the Cisco IPS Automatic Update feature. This feature facilitates the automatic download and deployment of the latest Cisco IPS signatures available from Cisco on to Cisco IPS devices throughout the network. These updates can be applied to single sensors or multiple sensors. CSM is configured to poll Cisco's website for updated signatures on a configurable schedule and, if updated signatures are available, they can be automatically downloaded. Once they are downloaded, the CSM can be configured to notify you that an updated signature package is available or to automatically deploy the signatures on Cisco IPS sensors. This ensures Cisco IPS sensors are up-to-date to protect against the latest threats that might affect the network.

Figure 11-22 illustrates the Cisco IPS automatic update settings within CSM.

Figure 11-22 Cisco IPS Auto-Update Settings in CSM



Cisco IPS Threat Identification and Mitigation

The CSM and CS-MARS Cisco IPS linkages along with the Cisco IPS automatic update and event action features combine to provide a collaborative threat identification and mitigation solution that enables network administrators to rapidly respond and protect networks from new threats. The following timeline example illustrates how this collaborative solution is used to protect the network from a new potential threat:

- **10:07 AM** – MS Bulletin is published identifying a new potential threat.
- **10:20 AM** – Cisco Security team notified.
- **11:03 AM** – First Intellishield alert published.
- **12:40 PM** – Intellishield publishes a mitigation bulletin for new threat.
- **12:55 PM** – Cisco Security Center event response page for threat goes live.
- **1:19 PM** – New Cisco IPS signatures published.
- **1:30 PM** – CSM hourly automated signature updates checks and pushes latest updates.
- **2:03 PM** – Cisco IPS Signature update complete.
- **3:03 PM** – First CS-MARS correlated event is seen.
- **4:01 PM** – Cisco IPS event action filter is created based on insight from Cisco security event page.
- **4:30 PM** – CSM completes event action filter deployment throughout the network.

Note *IntelliShield* is a subscription-based service that gives advanced notification of problems and mitigation solutions. The Security Center response page is updated quickly, but is something that customers must manually check, whereas the IntelliShield service automatically sends notifications directly to subscribers.