Integrating Cisco Security Agent with Cisco Intrusion Prevention System

Cisco® Security Agent and Cisco Intrusion Prevention System (IPS) are two key components of Cisco's Threat Control and Containment strategy, a fundamental piece of the Cisco Self-Defending Network solution. The Cisco Security Agent provides unequal protection to mission-critical servers and desktops by identifying threats and preventing malicious endpoint behavior. Cisco IPS, implemented in a variety of platforms, offers significant protection to the network by detecting, classifying, and stopping threats in real time. Combined, the Cisco Security Agent and Cisco IPS build a true end-to-end threat control and containment solution, providing protection that spans from the core of the network infrastructure all the way to the endpoints.

Residing on servers and desktops, Cisco Security Agents have full visibility on the endpoints, which allows them to gather information that no other security component in the network has visibility to. The Cisco Security Agent software and Cisco IPS have been enhanced to allow the sensor to use this valuable endpoint information. This collaboration helps Cisco IPS increase its visibility on endpoints and global threats, extending as a result the overall threat control and containment.

The collaboration between Cisco Security Agent and Cisco IPS has a series of benefits:

- Ability to use Cisco Security Agent endpoint information to influence 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 and false negatives: Cisco Security Agent provides OS type and other endpoint posture information that helps Cisco IPS determine the relevancy of a threat, reducing the chances for false positives and false negatives.
- Enhanced attack mitigation: Cisco IPS can use the Watch List maintained by Cisco Security Agent. The Watch List helps Cisco IPS keep an eye on systems identified by Cisco Security Agent as suspicious or malicious, and helps highlight any events associated with these systems.
- Dynamic host quarantine: Cisco IPS ability to dynamically block hosts that have been identified by Cisco Security Agent as malicious. This extends the quarantine capabilities from Cisco Security Agent to the IPS.

This document is a technical overview of the integration between Cisco Security Agent and Cisco IPS. It describes how the collaborative architecture works, explains its benefits, and provides the necessary guidelines for a successful deployment.

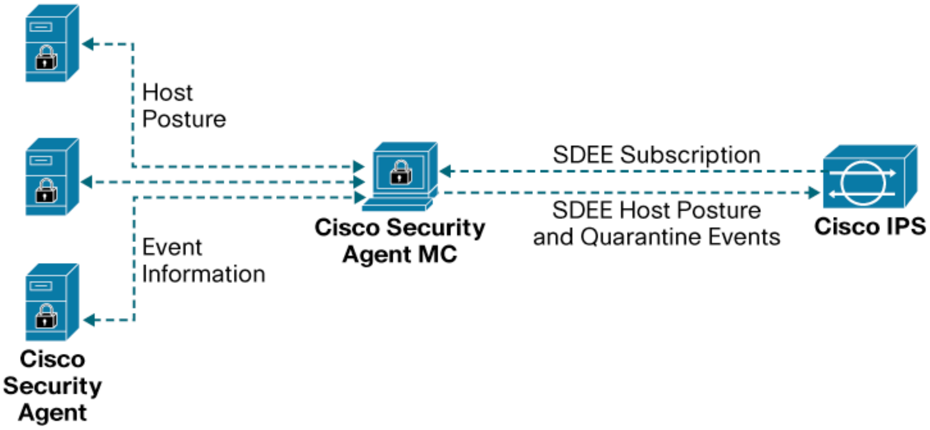
Cisco Security Agent/IPS Collaborative Architecture

The architecture integrating Cisco Security Agent and IPS relies on the interaction of three major components:

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

The components of the architecture and their interactions are depicted in Figure 1.

Figure 1. Cisco Security Agent/IPS Collaborative Architecture



Note: The minimum software versions required for integration are Cisco Security Agent MC 5.0 and Cisco IPS Sensor Software 6.0.

The Cisco Security Agent is a host-based agent that seats between the applications and OS kernel, gaining maximum endpoint visibility, and providing defense-in-depth protection to mission-critical servers and desktops. As part of their operation, Cisco Security Agents generate valuable event and posture information that is collected and correlated by Cisco Security Agent MC. The transfer of information between the agents and Cisco Security Agent MC is protected by the use of SSL.

In addition to the detailed endpoint information collected from agents, Cisco Security Agent MC global correlation generates threat data that can be valuable to Cisco IPS. When shared with Cisco IPS, this data helps increase the sensor visibility on endpoints and global threats. The Cisco IPS sensor accesses this information via Secure Device Event Exchange (SDEE), a protocol developed by a consortium (led by Cisco) designed for the secure exchange of network event information. Communications between Cisco Security Agent MC and IPS are protected with SSL/TLS encryption and HTTP authentication.

Note: Cisco Security Agent MC authenticates by providing X.509 certificates while the IPS sensor authenticates using a username and password.

To start receiving information, an IPS sensor needs to open a SDEE subscription with Cisco Security Agent MC. After the communication channels are authenticated and established, two types of messages are exchanged between Cisco Security Agent MC and IPS sensors:

- **Cisco Security Agent Posture Events:** Contains host posture information collected by Cisco Security Agent MC such as the IP address and the OS type of the hosts running Cisco Security Agent. To receive posture events an IPS has to open a subscription. After the subscription is open Cisco Security Agent MC sends an initial state message with the IP addresses and OS types of all known agents. After the initial state the Cisco Security Agent MC keeps the IPS informed through updates.
- **Quarantine Events:** Generated by Cisco Security Agent MC to communicate IPS sensors the list of hosts that are being quarantined. A host is quarantined either manually by a Cisco Security Agent MC administrator or rule-generated by global correlation. Quarantine events include the reason for the quarantine, the protocol associated with a rule violation (TCP, UDP, or ICMP), 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. IPS sensors must subscribe before they can start receiving quarantine events. Cisco Security Agent 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

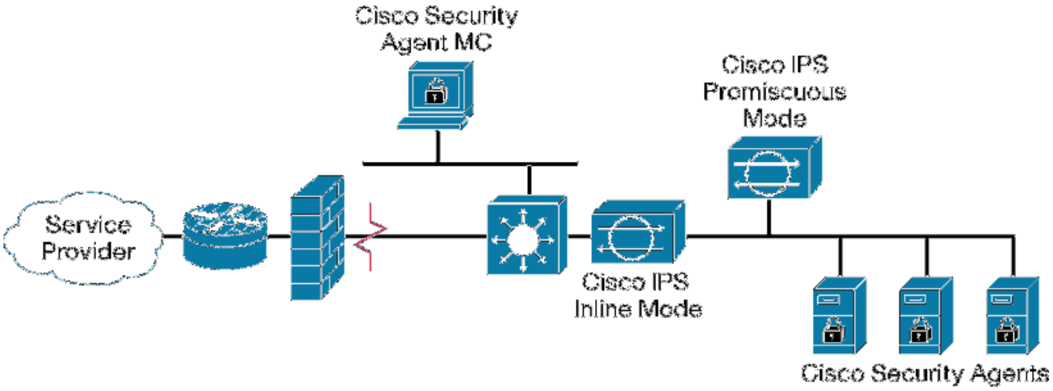
In general, the same best practices used to deploy Cisco Security Agent and Cisco IPS as standalone products apply when the two are implemented together in the same environment; therefore, it is always a good idea to follow those principles whenever possible. In addition to adopting the design best practices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

Inline Protection (IPS) and Promiscuous (IDS) Modes

Cisco Security Agent 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 may opt to deploy IPS in one mode or the other.

Even though there are many possible designs, in a typical inline protection mode deployment the IPS will seat between the Cisco Security Agents and the rest of the network. In this way the IPS can block attacks dynamically as malicious packets move through the system. In a typical promiscuous mode deployment, the IDS will be connected to a switch port configured to capture traffic from and to the hosts protected with Cisco Security Agents. These designs are illustrated in Figure 2.

Figure 2. Typical IPS/IDS Deployment Designs



One Cisco Security Agent MC to Multiple IPS Sensors

A single Management Center for Cisco Security Agents can serve multiple IPS sensors simultaneously. In cases where IPS sensors are managed by different groups of administrators, their access to Cisco Security Agent MC can be separated by the use of different subscription credentials.

One Sensor to Two Cisco Security Agent MCs

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

Virtualization

Cisco Security Agent can be integrated with IPS systems configured with virtual sensors. When used with virtualization, all information provided by the Management Center for Cisco Security Agents is global to the IPS sensor, and as a result it can be used by all active virtual sensors.

IP Addressing

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

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

Cisco Security Agent/IPS Interface Configuration

Integrating Cisco Security Agent and IPS requires the configuration of both Cisco Security Agent MC and IPS sensors. For most scenarios configuration consists of the following three main activities:

1. Definition of a Cisco Security Agent MC administrative account to be used by IPS sensors in their SDEE subscriptions.
2. Addition of Cisco Security Agent MC as a trusted host in each IPS sensor.
3. Configuration of an External Product Interface in each IPS sensor.

Defining a Cisco Security Agent MC Administrative Account

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

Even though any of the existing administrative accounts in Cisco Security Agent MC with a minimum of view privileges could 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 Cisco Security Agent/IPS communication purposes. This account should be given no more than the minimum required privileges (monitor, view).

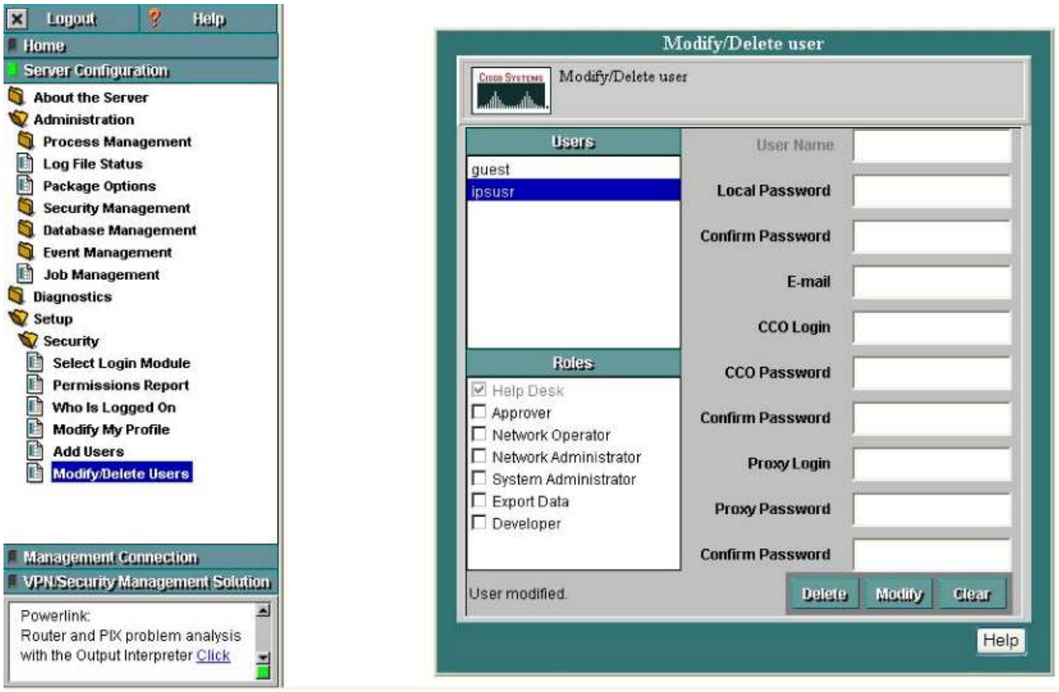
In environments with multiple IPS sensors under the same administration a single account can be shared by all the systems, while in environments where not all IPS sensors are administered by the same team, multiple accounts can be defined to help separate the administration.

In Cisco Security Agent MC 5.0 administrative accounts are defined in the CiscoWorks VPN/Security Management Solution (VMS). This is because in Cisco Security Agent MC 5.0 and prior versions of Cisco Security Agent MC are implemented as a component of CiscoWorks VMS. Cisco Security Agent MC 5.1 and later versions work standalone and do not require VMS. In these versions, the administrative accounts used for Cisco Security Agent/IPS communication are defined directly in Cisco Security Agent MC.

The account to be used for Cisco Security Agent/IPS communication should ideally be one configured with monitor privileges, which means the user has read access to the entire Cisco Security Agent MC database, but does not have write privileges. In the case of Cisco Security Agent MC 5.1 and later versions, the monitor role can be set in Cisco Security Agent MC as part of the user configuration. With Cisco Security Agent MC 5.0 and prior versions, administrative users are defined in VMS and not in Cisco Security Agent MC. In this case, the user can be associated to any of the predefined roles in CiscoWorks with read-only access. For example, Help Desk. Network Administrator, System Administrator, and Network Operator roles provide write access; hence, their use is not recommended for the purpose of Cisco Security Agent/IPS communication.

Figure 3 is a snapshot taken from Cisco Security Agent MC 5.0 showing the definition of “ipsusr”, an account defined for the exclusive use of Cisco Security Agent/IPS communication.

Figure 3. Cisco Security Agent MC Administrative Account



Users: guest, ipsusr

Roles:
☑ Help Desk
□ Approver
□ Network Operator
□ Network Administrator
□ System Administrator
□ Export Data
□ Developer

User modified.

For more information on managing administrative accounts please refer to your Cisco Security Agent MC documentation.

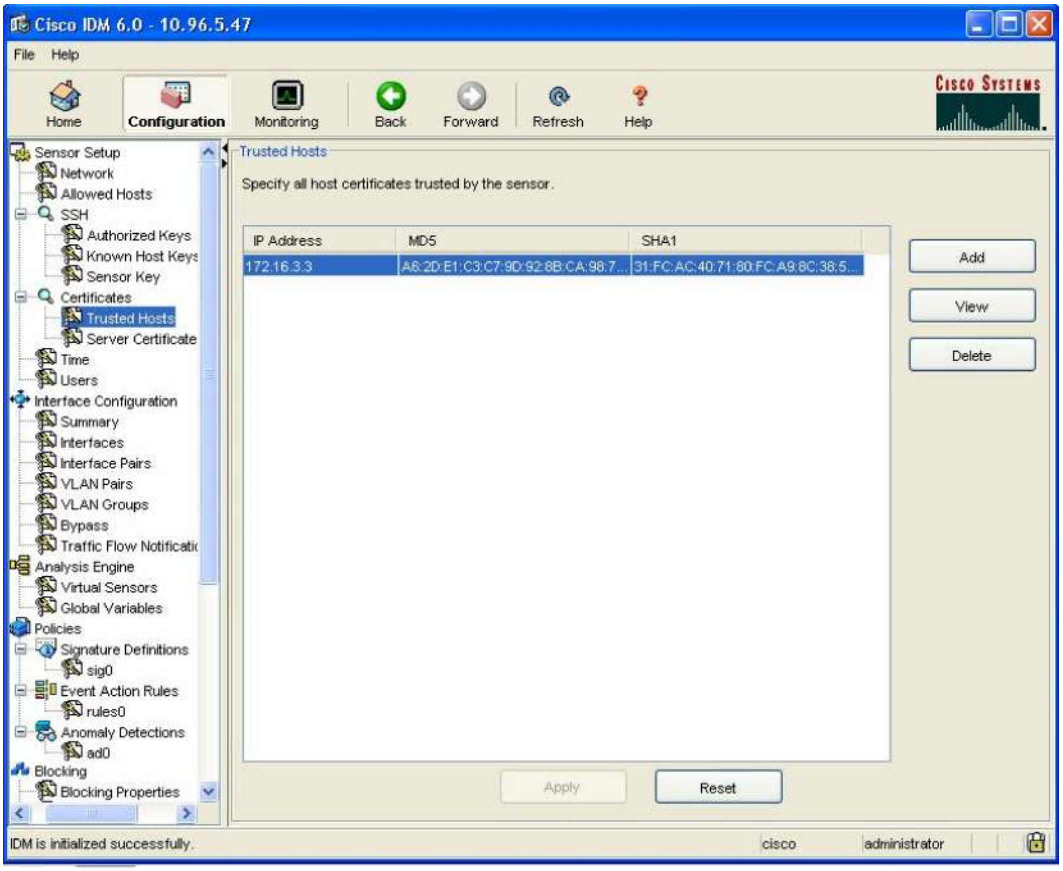
Configuring Cisco Security Agent MC System as a Trusted Host

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

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

Figure 4 is a snapshot of Cisco IPS Device Manager 6.0 (IDM) showing host 172.16.3.3 (system running Cisco Security Agent MC) listed as a trusted host.

Figure 4. IPS Trusted Hosts



Specify all host certificates trusted by the sensor.

IP Address	MD5	SHA1
172.16.3.3	A6:2D:E1:C3:C7:9D:92:8B:CA:98:7...	31:FC:AC:40:71:80:FC:A9:8C:38:5...

IDM is initialized successfully.

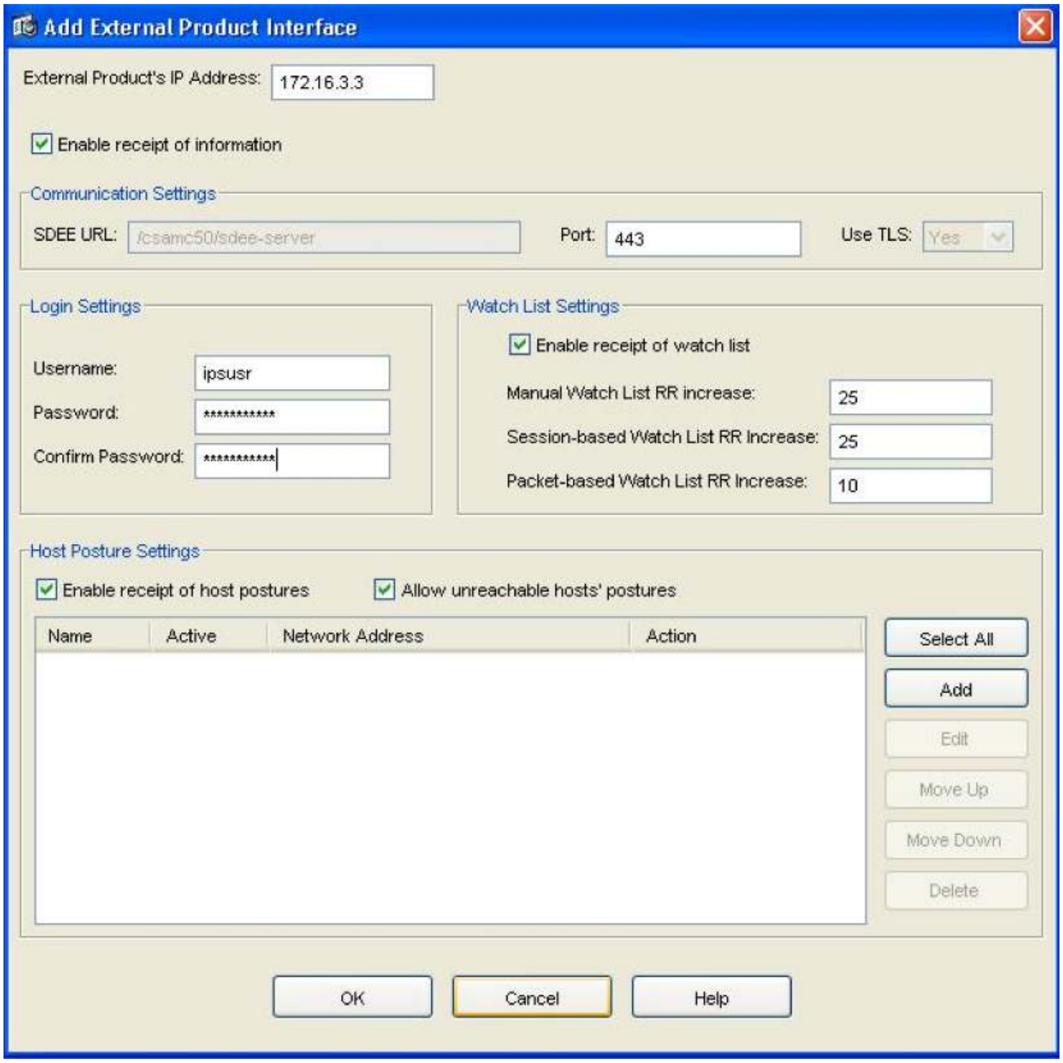
Configuring IPS External Product Interface

Cisco IPS sensors are equipped with an External Product Interface designed to handle communications with external security and management products like Cisco Security Agent MC. Thanks to this interface, the IPS sensors can take full advantage of useful host posture and threat context information maintained by Cisco Security Agent MC, including the OS type of the systems protected with Cisco Security Agent, and a list of IP addresses of systems suspected of causing malicious activity. This grade of collaboration increases the overall security effectiveness of Cisco Security Agent/IPS as an end-to-end security solution.

Note: In Cisco IPS Sensor Software 6.0, only two External Interfaces can be defined. Cisco Security Agent MC is the only external product supported at this time.

The configuration of the IPS External Product Interface consists in the definition of communication parameters, watch lists settings, and host posture settings (shown in Figure 5).

Figure 5. IPS External Product Interface Configuration



Add External Product Interface

External Product's IP Address: 172.16.3.3

☑ Enable receipt of information

Communication Settings

SDEE URL: /csamc50/sdee-server

Port: 443

Use TLS: Yes

Login Settings

Username: ipsusr

Password: ***********

Confirm Password: ***********

Watch List Settings

☑ Enable receipt of watch list

Manual Watch List RR increase: 25

Session-based Watch List RR Increase: 25

Packet-based Watch List RR Increase: 10

Host Posture Settings

☑ Enable receipt of host postures

☑ Allow unreachable hosts' postures

Name	Active	Network Address	Action

The following is the explanation of all the parameters configured in the External Product Interface.

General Parameters

External Product’s IP Address: IP address of the system hosting Cisco Security Agent 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 Cisco Security Agent MC. A default SDEE URL is provided. Be aware that the SDEE URL may have to be changed depending on the version of Cisco Security Agent MC.

Port: 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 Cisco Security Agent MC.

Username: Username of the administrative account used to communicate with Cisco Security Agent MC. This account is defined in Cisco Security Agent MC.

Password/Confirm Password: Password of the administrative account used to communicate with Cisco Security Agent 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. Later this document describes how watch lists work in detail.

Enable Receipt of Watch List: Enables/disables the reception of watch lists from Cisco Security Agent MC.

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, but it can be changed to any value in the 0 to 35 range.

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 Cisco Security Agent global correlation. By default the increase value is set to 25, but it can be changed to any value in the 0 to 35 range.

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 Cisco Security Agent global correlation. By default the increase value is set to 10, but it can be changed to any value in the 0 to 35 range.

Host Posture Settings

Defines how host posture information should be handled.

Enable Receipt of Host Postures: Enables/disables the reception of host posture information from Cisco Security Agent MC.

Allow Unreachable Hosts' Postures: Allows/denies the reception of host posture information for hosts not reachable by Cisco Security Agent MC. This option is useful in filtering the postures whose IP addresses may not be visible to the IPS or may be duplicated across the network.

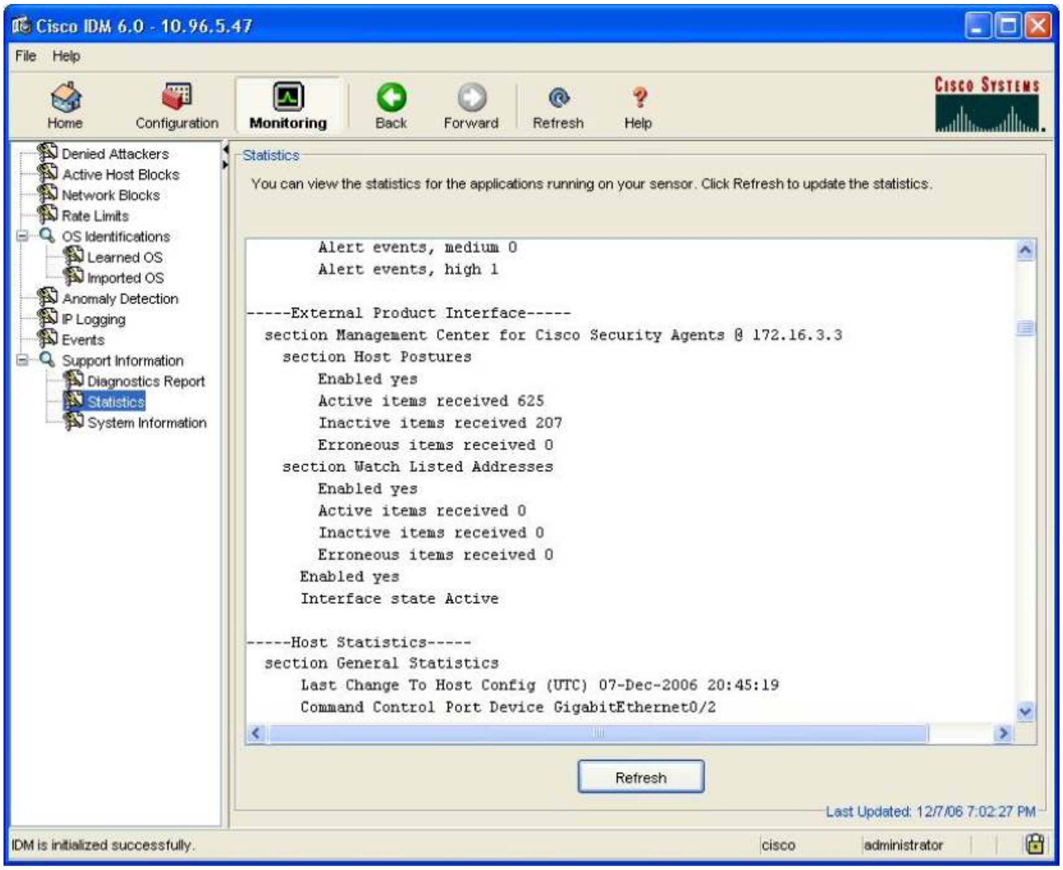
Posture ACLs: By default all host postures are processed by the IPS. Posture ACLs provide a mechanism to filter the network ranges from which host postures will be processed or ignored (permitted or denied). This option is useful in filtering the postures whose IP addresses may not be visible to the IPS or may be duplicated across the network.

Verifying the State of the External Product Interface

To verify the state of the External Product Interface in IDM you can access the Monitor/Statistics section as shown in Figure 6. Under normal operation the interface state should be *Active. A Communications Failed* state is likely caused due to an incorrect username or password, the user has no sufficient view privileges, or because the IPS sensor cannot reach Cisco Security Agent MC.

Figure 6 shows a snapshot of the statistics page of IDM 6.0. The figure shows that communication with the Management Center for Cisco Security Agents @ 172.16.3.3 is “Active”.

Figure 6. Verifying Status of External Product Interface



You can view the statistics for the applications running on your sensor. Click Refresh to update the statistics.

```
        Alert events, medium 0
        Alert events, high 1

-----External Product Interface-----
  section Management Center for Cisco Security Agents @ 172.16.3.3
    section Host Postures
        Enabled yes
        Active items received 625
        Inactive items received 207
        Erroneous items received 0
    section Watch Listed Addresses
        Enabled yes
        Active items received 0
        Inactive items received 0
        Erroneous items received 0
      Enabled yes
      Interface state Active

-----Host Statistics-----
  section General Statistics
      Last Change To Host Config (UTC) 07-Dec-2006 20:45:19
      Command Control Port Device GigabitEthernet0/2
```

Last Updated: 12/7/06 7:02:27 PM

IDM is initialized successfully.

Using Endpoint Information

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

A false positive is an event where the IPS triggers an alarm in response to an activity that is actually not malicious, or where the IPS triggers a response action that is out of proportion. Per contrary, a false negative is a situation where the IPS fails to alert or trigger an appropriate response action to a real malicious activity. The problem of false positives and false negatives often occurs when the IPS fails to interpret the risk level associated to the network event in question, typically due to the lack of context information. By using the OS type information provided by Cisco Security Agent, Cisco IPS can better determine the appropriate relative risk associated with a particular event, reducing the possibilities for false positives and false negatives.

Starting in Cisco IPS Sensor Software 5.0, IPS alerts are evaluated under a sophisticated Risk Rating mechanism. Each 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).

When integrated with Cisco Security Agent, Cisco IPS has the capacity to dynamically adjust the Risk Rating values based on the OS type information imported from Cisco Security Agent, helping it determine the right risk level of an event. In this way the 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.

The following section describes how Risk Rating is calculated and how it is influenced by the information available from Cisco Security Agent.

IPS Risk Rating Calculation

Introduced in Cisco IPS 5.0, Risk Rating is a mechanism that quantifies the risk associated with the alarms generated by the IPS sensor. The Risk Rating is represented with a numerical value between 0 and 100, and where the higher the value, the greater the risk associated with the triggering event. The calculation of Risk Rating takes into consideration a combination of factors, including the value of the network asset being attacked, the fidelity of the attack, the severity of the threat, and other important contextual factors. Starting in Cisco IPS Sensor Software 6.0 the calculation of Risk Rating has been enhanced to include two more factors: Promiscuous Delta, which takes into consideration the configuration mode of the sensor, and Watch List Rating, which uses the Cisco Security Agent watch lists.

Every time a network event triggers an alarm, the IPS sensor calculates the associated Risk Rating using the following formula:

$$\begin{array}{c}\text{Risk}\\\text{Rating}\end{array} = \frac{\text{Fidelity(SFR)} \star \text{Severity(ASR)} \star \begin{array}{c}\text{Target}\\\text{Value(TVR)}\end{array}}{100 \star 100 \star 100} + \text{Relevancy(ARR)} - \begin{array}{c}\text{Promiscuous}\\\text{Delta(PD)}\end{array} + \begin{array}{c}\text{Watch}\\\text{List(WLR)}\end{array}$$

Signature Fidelity Rating (SFR): Predefined by Cisco, and configurable on a per-signature basis. A weight associated with the accuracy of the signature. Signatures written with specific rules (specific regular expressions) have a higher SFR than signatures programmed with more generic rules. Acceptable values are between 0 and 100.

Alert Severity Rating (ASR): Predefined by Cisco, and configurable on a per-signature basis. A weight associated with the severity of a successful attack. Possible values are:

- **Information (25)**—An informational alert is based on commonly seen network traffic and has no particular security relevance when seen on most networks. It may be a violation of a policy on some networks, but it generally poses no immediate threat to network security.
- **Low (50)**—A low alert is also based on relatively benign network traffic, but is somewhat unusual on most networks. Also categorized as low would be overt scans, such as those commonly seen by network management devices. Although this type of scan could be a precursor to an attack, it is uncommon for an overt scan to be used for this purpose.
- **Medium (75)**—A medium alert is based on traffic that generally should not be seen on the network. It is usually assigned to midlevel reconnaissance traffic, denial of service (DoS)

attacks on self-healing services, and remote access of unexpected information or programs. This type of behavior warrants investigation or preventive actions, sometimes requiring policy decisions from the user.

- **High (100)**—A high alert is based on traffic that is indicative of an active attack or an obvious precursor to an attack. This traffic should never be seen in a normal network. This rating is reserved for attacks that could result in serious compromise of the target, or for specific network traffic that is only seen in covert reconnaissance traffic.

Target Value Rating (TVR): Configurable per target. A weight associated with the perceived value of the target. By default all targets are assigned a Medium value. This allows the user to increase the risk level of events associated with critical systems, and de-emphasize the risk level of events corresponding to low-value systems. Possible values are:

- Low Asset Value (75)
- Medium Asset value (100)
- High Asset Value (150)
- Mission-Critical Asset Value (200)

Attack Relevancy Rating (ARR): Internal weighted value derived from target and threat context information known by the IPS or imported from Cisco Security Agent. The value of ARR represents whether or not the target is believed to be vulnerable to the attack:

- ARR is set to 10 whenever the OS type of the target system is found to be vulnerable. This applies for both, promiscuous (IDS) and inline protection (IPS) modes.
- ARR is set to –10 when the OS type of the target system is known not to be vulnerable, and the IPS is configured in promiscuous mode (IDS).
- ARR is set to 0 when the OS type of the target system is known not to be vulnerable, and the IPS is configured in inline protection mode (IPS).

Note: The OS type of the target is either learned by the IPS via fingerprinting, or imported from Cisco Security Agent. Therefore, the endpoint information provided by Cisco Security Agent has a direct impact on the Attack Relevancy Rating.

Promiscuous Delta (PD): Introduced in Cisco IPS Sensor Software 6.0. Promiscuous Delta is a value predefined by Cisco on a signature basis, whose objective is to lower the Risk Rating of certain alerts generated in promiscuous mode. Possible values are from 0 to 30.

The Promiscuous Delta is subtracted from Risk Rating every time an alert is triggered when the system is deployed in promiscuous mode. In general, systems deployed in inline protection mode have a more definitive picture on the target hosts, and alerts are more accurate than those generated by systems in promiscuous mode.

Signatures that are not service, OS, or application-specific are by default set with no Promiscuous Delta (PD=0). Signatures specific to an OS, service, or application, are predefined with Promiscuous Delta of 5, 10, or 15 calculated from 5 points for each category.

Note: Even though PD can be reconfigured on a signature basis, it is not recommended that you change any of the predefined promiscuous-delta settings.

Watch List Rating (WLR): Introduced in Cisco IPS Sensor Software 6.0, the Watch List Rating is a value that increases the RR of events associated with systems present in the Cisco Security Agent Watch List. The Watch List Rating is configured as part of the External Product Interface, and consists of three parameters configurable in the 0 to 35 range:

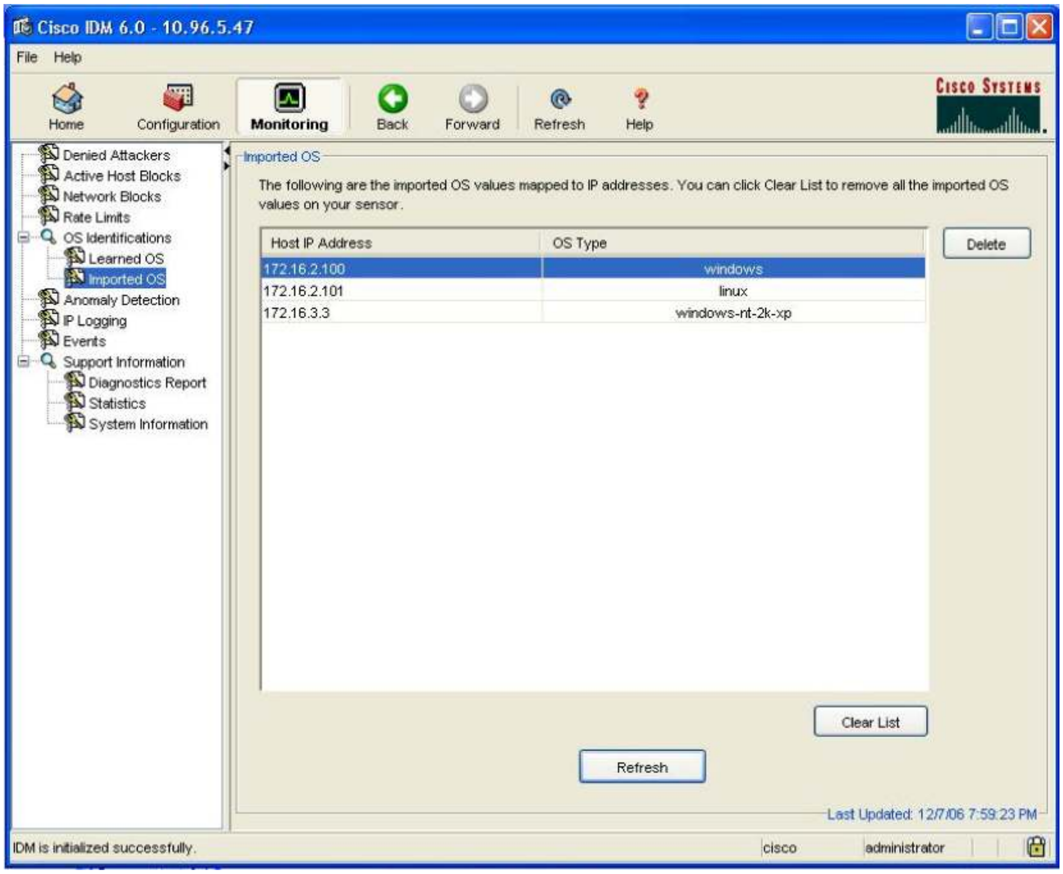
- Manual Watch List RR increase: Indicates the value by which Risk Rating should be increased for events associated with hosts that were manually added to the watch list. By default the increase value is set to 25.
- Session-based Watch List RR increase: Indicates the value by which Risk Rating should be increased for events associated with TCP connections added to the watch list as a result of Cisco Security Agent 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 Cisco Security Agent global correlation. By default the increase value is set to 10.

Verifying Imported OS Posture Information

As explained previously, the OS type information provided by Cisco Security Agent plays a crucial role in the calculation of Risk Rating. To verify that IPS has successfully imported the OS type information from Cisco Security Agent, access the “Imported OS” tab within the Monitoring section of IDM.

Figure 7 shows the table containing the list of the imported IP addresses mapped to the corresponding OS types.

Figure 7. Imported OS Information



The following are the imported OS values mapped to IP addresses. You can click Clear List to remove all the imported OS values on your sensor.

Host IP Address	OS Type
172.16.2.100	windows
172.16.2.101	linux
172.16.3.3	windows-nt-2k-xp

Last Updated: 12/7/06 7:59:23 PM

IDM is initialized successfully.

Using Cisco Security Agent Watch Lists

As part of its threat control function, Cisco Security Agent 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 Cisco Security Agents, 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 Cisco Security Agent are instructed to block any communication attempt with the affected host.

For improved threat visibility and overall control, the IPS External Product Interface can be configured to use the quarantine information generated by Cisco Security Agent. In this way, every time a host is quarantined the Cisco Security Agent will send a quarantine event to each one of the 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 Cisco Security Agent, each IPS sensors builds and maintains a Watch List. The purpose of the Watch List is to help the IPS monitor systems identified by Cisco Security Agent as suspicious or malicious, and to highlight any events associated with these systems. The Watch List tells the IPS what systems it needs to monitor closely and for which Risk Rating needs to be increased. The Watch List does not extend the quarantine of the hosts in the list to the IPS. In fact, the IPS does not block a host solely because it is part of the list.

Note: For a host, being in the Watch List means to be quarantined by Cisco Security Agent and "watched" by IPS. The IPS does not automatically quarantine systems in Watch List.

Every time a host in the Watch List triggers an alert, the resulting Risk Rating is increased by the Watch List Rating. As explained in the previous section, the Watch List rating is configured in the IPS External Product Interface. Three separate values can be defined to distinguish between manual and dynamic quarantine, and TCP- and UDP-based traffic. The IPS applies the Watch List Rating type that corresponds to the particular event.

As a result of the Watch List, the Risk Rating of events triggered by hosts in the list is automatically increased. Optionally, an override action can be configured to block the offending system when the resulting Risk Rating exceeds a predefined threshold. These concepts are explained in the following sections.

Adding Hosts to the Watch List

A host can be added to the Watch List either manually by a Cisco Security Agent administrator or as a result of Cisco Security Agent global correlation:

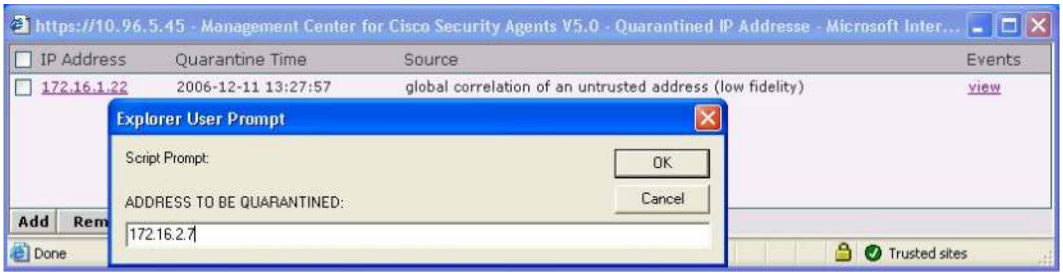
Manual Configuration

A Cisco Security Agent 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 Cisco Security Agent MC, and by adding a new entry with the host IP address.

Figure 8 illustrates this process. In this example, the system with IP address 172.16.2.7 is added to the quarantine list manually.

Figure 8. Manually Adding a Host to the Quarantine List



https://10.96.5.45 - Management Center for Cisco Security Agents V5.0 - Quarantined IP Addresse - Microsoft Inter...

□ IP Address	Quarantine Time	Source	Events
□ 172.16.1.22	2006-12-11 13:27:57	global correlation of an untrusted address (low fidelity)	view

Explorer User Prompt

Script Prompt:

ADDRESS TO BE QUARANTINED:

172.16.2.7

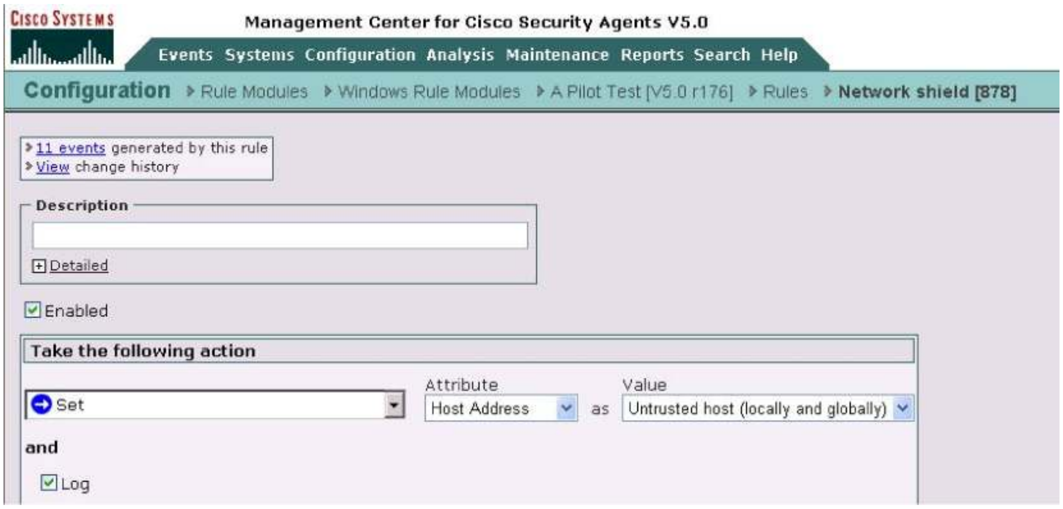
The manual addition of a host to the Quarantine IP Address list triggers a quarantine event to the IPS sensors. In addition to including the IP address of the affected system, the quarantine event indicates that the entry has been manually added to the list. As a result the IPS will use the Manual Watch List RR increase value when calculating Risk Rating.

Dynamic Global Correlation

Cisco Security Agent 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.

The rule triggering the quarantine must be configured to respond to a violation by setting the host address as an untrusted host (locally and globally). Being classified as untrusted host (locally and globally) makes the host a candidate for global event correlation. This is illustrated in Figure 9.

Figure 9. Rule Setting Offending Host as Globally Untrusted



Cisco Systems
Management Center for Cisco Security Agents V5.0
Events Systems Configuration Analysis Maintenance Reports Search Help

Configuration ▸ Rule Modules ▸ Windows Rule Modules ▸ A Pilot Test [V5.0 r176] ▸ Rules ▸ Network shield [878]

▸ 11 events generated by this rule
▸ View change history

Description

⊞ Detailed

☑ Enabled

Take the following action

Set — Attribute: Host Address as Value: Untrusted host (locally and globally)

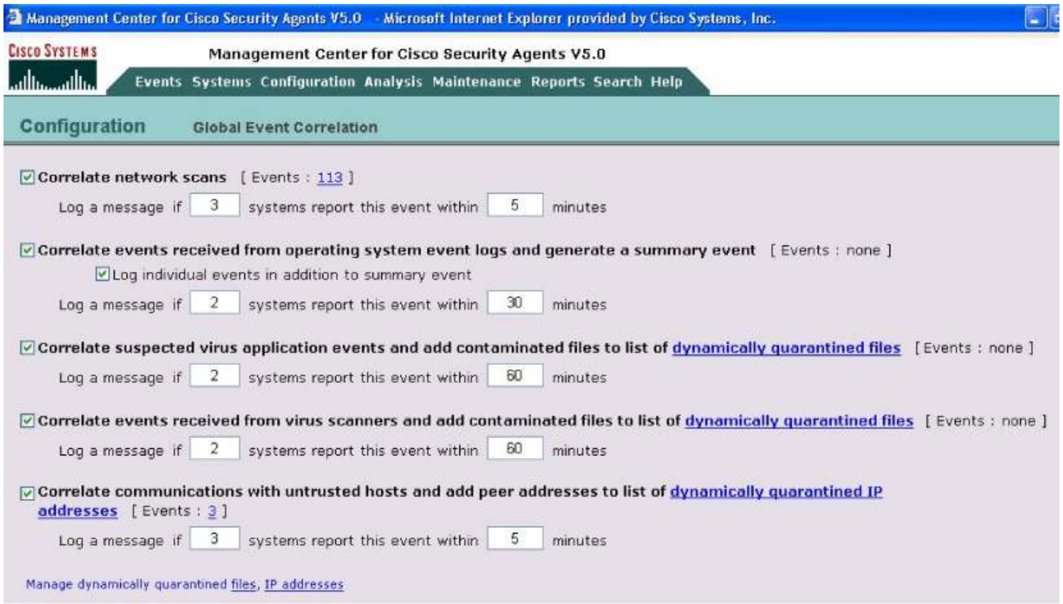
and

☑ Log

After the rule is set, Cisco Security Agent must be configured to correlate communications with untrusted hosts and to add the peer addresses to the list of dynamically quarantined IP addresses. This configuration includes the definition of an event threshold after which the host is automatically added to the global quarantine list on all systems running Cisco Security Agent.

Figure 10 shows the configuration of the Global Event Correlation.

Figure 10. Global Event Correlation Configuration


Management Center for Cisco Security Agents V5.0 - Microsoft Internet Explorer provided by Cisco Systems, Inc.
Cisco Systems
Management Center for Cisco Security Agents V5.0
Events Systems Configuration Analysis Maintenance Reports Search Help
Configuration
Global Event Correlation

☑ **Correlate network scans** [Events : 113]

Log a message if 3 systems report this event within 5 minutes

☑ **Correlate events received from operating system event logs and generate a summary event** [Events : none]

☑ Log individual events in addition to summary event

Log a message if 2 systems report this event within 30 minutes

☑ **Correlate suspected virus application events and add contaminated files to list of dynamically quarantined files** [Events : none]

Log a message if 2 systems report this event within 60 minutes

☑ **Correlate events received from virus scanners and add contaminated files to list of dynamically quarantined files** [Events : none]

Log a message if 2 systems report this event within 60 minutes

☑ **Correlate communications with untrusted hosts and add peer addresses to list of dynamically quarantined IP addresses** [Events : 3]

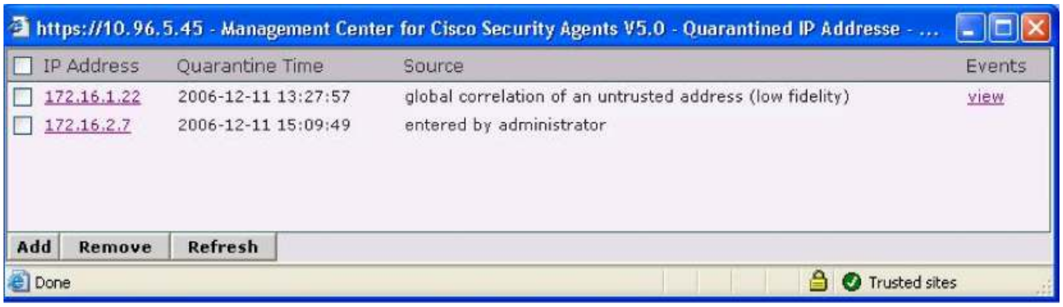
Log a message if 3 systems report this event within 5 minutes

Manage dynamically quarantined files, IP addresses

Every time a system is quarantined, a quarantine event is sent to the IPS sensors containing the IP address of the quarantined host, the protocol involved, and indicating the dynamic nature of the quarantine event. As a result, when calculating Risk Rating the IPS will use one of the two dynamic Watch List Rating values (session-based or packet-based).

As an example, Figure 11 shows the list of quarantined IP addresses. The list includes a system quarantined by global correlation (172.16.1.22), and another one added manually by the administrator (17.16.2.7).

Figure 11. List of Quarantined IP Addresses


https://10.96.5.45 - Management Center for Cisco Security Agents V5.0 - Quarantined IP Addresse - ...
Add
Remove
Refresh
Done
Trusted sites

□ IP Address	Quarantine Time	Source	Events
□ 172.16.1.22	2006-12-11 13:27:57	global correlation of an untrusted address (low fidelity)	view
□ 172.16.2.7	2006-12-11 15:09:49	entered by administrator	

IPS Event Action Override

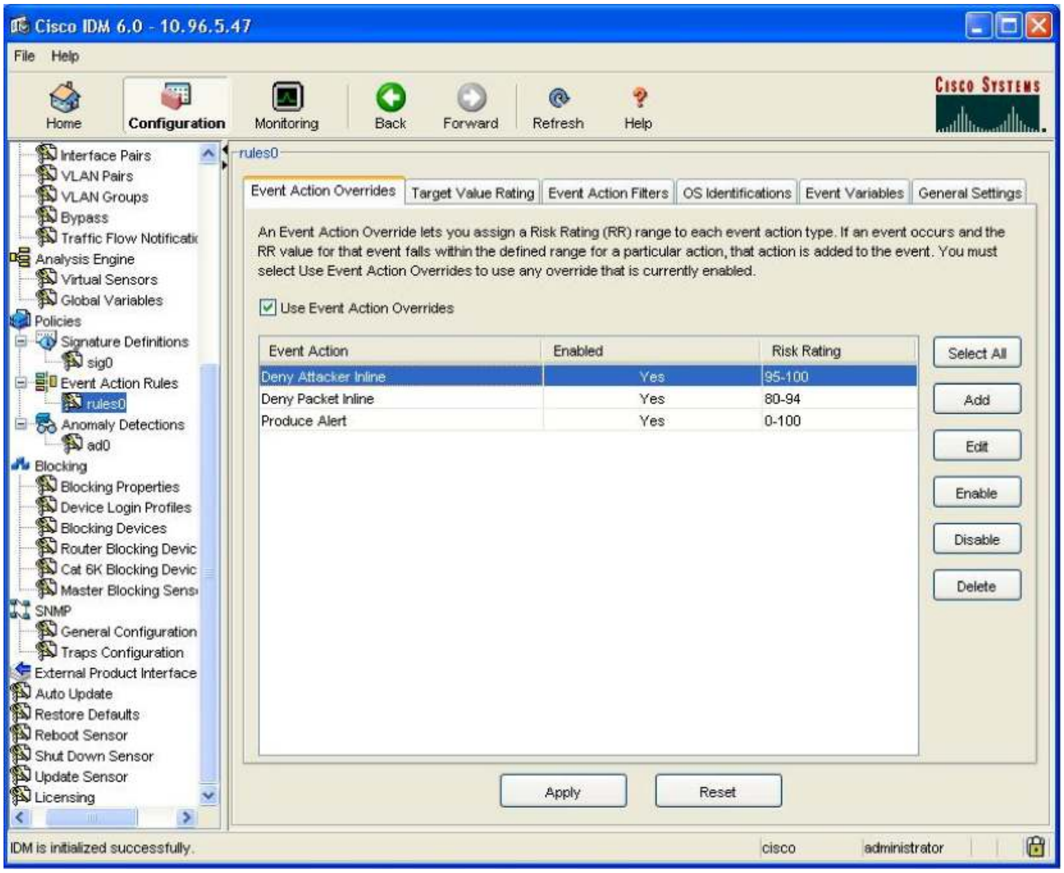
As explained in the previous sections of this document, Cisco IPS implements Watch Lists primarily to highlight the activity of suspicious systems; and while Cisco Security Agent isolates the hosts in the list the IPS does not enforce quarantine automatically. It is possible however to combine the Watch 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 Lists the 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 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 12.

Figure 12. Event Action Override Example



An Event Action Override lets you assign a Risk Rating (RR) range to each event action type. If an event occurs and the RR value for that event falls within the defined range for a particular action, that action is added to the event. You must select Use Event Action Overrides to use any override that is currently enabled.

☑ Use Event Action Overrides

Event Action	Enabled	Risk Rating
Deny Attacker Inline	Yes	95-100
Deny Packet Inline	Yes	80-94
Produce Alert	Yes	0-100

IDM is initialized successfully.

In Figure 12 three event action overrides are defined for an IPS configured in inline protection mode. Network events triggering alarms with Risk Rating equal to 95 and higher will cause the source host to be blocked inline by the IPS. Packets generating alarms with Risk Rating between

80 and 94 will be dynamically denied inline. Finally, events with any Risk Rating (between 0 and 100) will trigger an alert in the log.

The implementation of *event action overrides* is a useful tool that extends the quarantine of hosts by Cisco Security Agent to the IPS, 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 to hosts in the Watch List.
- The IPS will not enforce any action until the host present in the Watch List triggers an event with a resulting Risk Rating falling in the range specified for the *event action override*. This means the IPS will not quarantine a host immediately after it receives a quarantine event from Cisco Security Agent MC. An action on the host will be enforced only after the host triggers an event in the IPS.

Related Docs

Listed in alphabetical order:

- **Cisco IPS Risk Rating Explained:** http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5729/ps5713/ps4077/prod_white_paper0900aecd80191021.shtml
- **Installing and Using Cisco Intrusion Prevention System Device Manager 6.0:** http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/products_configuration_guide_book09186a00807a8a2a.html
- **Using Management Center for Cisco Security Agents 5.0:** http://www.cisco.com/en/US/products/sw/secursw/ps5057/products_configuration_guide_book09186a00805ae89c.html
- **Using Management Center for Cisco Security Agents 5.1:** http://www.cisco.com/en/US/products/sw/secursw/ps5057/products_configuration_guide_book09186a008067b6a5.html

Americas 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: 408 527-0883

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

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

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

Printed in USA C11-387679-01 08/07