Configuring External Product Interfaces

This chapter explains how to configure external product interfaces. It contains the following sections:

External Product Interface Notes and Caveats

The following notes and caveats apply to external product interfaces:

- In Cisco IPS, you can only add interfaces to the CSA MC.
- You can only enable two CSA MC interfaces.
- You must add the CSA MC as a trusted host so the sensor can communicate with it.

Understanding External Product Interfaces

Note In Cisco IPS, you can only add interfaces to the CSA MC.

The external product interface is designed to receive and process information from external security and management products. These external security and management products collect information that can be used to automatically enhance the sensor configuration information. For example, the types of information that can be received from external products include host profiles (the host OS configuration, application configuration, and security posture) and IP addresses that have been identified as causing malicious network activity.

Understanding the CSA MC

The CSA MC enforces a security policy on network hosts. It has two components:

- Agents that reside on and protect network hosts.
- Management Console (MC)—An application that manages agents. It downloads security policy updates to agents and uploads operational information from agents.

The CSA MC receives host posture information from the CSA agents it manages. It also maintains a watch list of IP addresses that it has determined should be quarantined from the network. The CSA MC sends two types of events to the sensor—host posture events and quarantined IP address events.

Host posture events (called imported OS identifications in IPS) contain the following information:

- Unique host ID assigned by the CSA MC
- CSA agent status
- Host system hostname
- Set of IP addresses enabled on the host
- CSA software version
- CSA polling status
- CSA test mode status
- NAC posture

For example, when an OS-specific signature fires whose target is running that OS, the attack is highly relevant and the response should be greater. If the target OS is different, then the attack is less relevant and the response may be less critical. The signature attack relevance rating is adjusted for this host.

The quarantined host events (called the watch list in IPS) contain the following information:

- IP address
- Reason for the quarantine
- Protocol associated with a rule violation (TCP, UDP, or ICMP)
- Indicator of whether a rule-based violation was associated with an established session or a UDP packet.

For example, if a signature fires that lists one of these hosts as the attacker, it is presumed to be that much more serious. The risk rating is increased for this host. The magnitude of the increase depends on what caused the host to be quarantined.

The sensor uses the information from these events to determine the risk rating increase based on the information in the event and the risk rating configuration settings for host postures and quarantined IP addresses.

Note The host posture and watch list IP address information is not associated with a virtual sensor, but is treated as global information.

Secure communications between the CSA MC and the IPS sensor are maintained through SSL/TLS. The sensor initiates SSL/TLS communications with the CSA MC. This communication is mutually authenticated. The CSA MC authenticates by providing X.509 certificates. The sensor uses username/password authentication.

Note You can only enable two CSA MC interfaces.

Caution You must add the CSA MC as a trusted host so the sensor can communicate with it.

For More Information

For the procedure for adding trusted hosts, see Adding TLS Trusted Hosts, page 4-53.

External Product Interface Issues

When the external product interface receives host posture and quarantine events, the following issues can arise:

- The sensor can store only a certain number of host records:
  - If the number of records exceeds 10,000, subsequent records are dropped.
  - If the 10,000 limit is reached and then it drops to below 9900, new records are no longer dropped.
- Hosts can change an IP address or appear to use another host IP address, for example, because of DHCP lease expiration or movement in a wireless network. In the case of an IP address conflict, the sensor presumes the most recent host posture event to be the most accurate.
- A network can include overlapping IP address ranges in different VLANs, but host postures do not include VLAN ID information. You can configure the sensor to ignore specified address ranges.
- A host can be unreachable from the CSA MC because it is behind a firewall. You can exclude unreachable hosts.
- The CSA MC event server allows up to ten open subscriptions by default. You can change this value. You must have an administrative account and password to open subscriptions.
- CSA data is not virtualized; it is treated globally by the sensor.
- Host posture OS and IP addresses are integrated into passive OS fingerprinting storage. You can view them as imported OS profiles.
- You cannot see the quarantined hosts.
- The sensor must recognize each CSA MC host X.509 certificate. You must add them as a trusted host.
- You can configure a maximum of two external product devices.

For More Information

- For more information on working with OS maps and identifications, see Adding, Editing, Deleting, and Moving Configured OS Maps, page 8-28 and Displaying and Clearing OS Identifications, page 8-32.
- For the procedure for adding trusted hosts, see Adding TLS Trusted Hosts, page 4-53.

Configuring the CSA MC to Support the IPS Interface

Note For more detailed information about host posture events and quarantined IP address events, refer to *Using Management Center for Cisco Security Agents 5.1*.

You must configure the CSA MC to send host posture events and quarantined IP address events to the sensor. To configure the CSA MC to support IPS interfaces, follow these steps:

Step 1 Choose **Events > Status Summary**.

Step 2 In the Network Status section, click **No** beside **Host history collection enabled**, and then click **Enable** in the popup window.

Note Host history collection is enabled globally for the system. This feature is disabled by default because the MC log file tends to fill quickly when it is turned on.

Step 3 Choose **Systems > Groups** to create a new group (with no hosts) to use in conjunction with administrator account you will next create.

Step 4 Choose **Maintenance > Administrators > Account Management** to create a new CSA MC administrator account to provide IPS access to the MC system.

Step 5 Create a new administrator account with the role of **Monitor**. This maintains the security of the MC by not allowing this new account to have configure privileges.

Note Remember the username and password for this administrator account because you need them to configure external product interfaces on the sensor.

Step 6 Choose **Maintenance > Administrators > Access Control** to further limit this administrator account.

Step 7 In the Access Control window, select the administrator you created and select the group you created.

Note When you save this configuration, you further limit the MC access of this new administrator account with the purpose of maintaining security on the CSA MC.

Adding External Product Interfaces and Posture ACLs

Caution In the Cisco IPS, the only external product interfaces you can add are CSA MC interfaces. The Cisco IPS supports two CSA MC interfaces.

Use the **cisco-security-agents-mc-settings** *ip-address* command in service external product interfaces submode to add the CSA MC as an external product interface.

The following commands apply:

- **enabled {yes | no}**—Enables/disables the receipt of information from the CSA MC.
- **host-posture-settings**—Specifies how host postures received from the CSA MC are handled:
  - **allow-unreachable-postures {yes | no}**—Allows postures for hosts that are not reachable by the CSA MC.

    A host is not reachable if the CSA MC cannot establish a connection with the host on any IP addresses in the posture of the host. 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. This filter is most applicable in network topologies where hosts that are not reachable by the CSA MC are also not reachable by the IPS, for example if the IPS and the CSA MC are on the same network segment.
  - **enabled** {**yes** | **no**}—Enables/disables receipt of host postures from the CSA MC.
  - **posture-acls** {**edit** | **insert** | **move**} **name1 {begin | end | inactive | before | after}**—Specifies the list of permitted or denied posture addresses. This command provides a mechanism for filtering postures that have IP addresses that may not be visible to the IPS or may be duplicated across the network.
  - **action {permit | deny}**—Specifies the permit or deny postures that match the specified network address.
  - **network-address** *address*—Specifies the network address, in the form x.x.x.x/nn, for postures to be permitted or denied.
- **password**—Specifies the password used to log in to the CSA MC.
- **port** —Specifies the TCP port to connect to on the CSA MC. The valid range is 1 to 65535. The default is 443.
- **username** —Specifies the username used to log in to the CSA MC.
- **watchlist-address-settings**—Specifies how watch listed addresses received from the CSA MC are handled:
  - **enabled {yes | no}**—Enables/disables receipt of watch list addresses from the CSA MC.
  - **manual-rr-increase**—Specifies the number added to an event RR because the attacker has been manually watch-listed by the CSA MC. The valid range is 0 to 35. The default is 25.
  - **packet-rr-increase**—Specifies the number added to an event risk rating because the attacker has been watch listed by the CSA MC because of a sessionless packet-based policy violation. The valid range is 0 to 35. The default is 10.
  - **session-rr-increase**—Specifies the number added to an event risk rating because the attacker has been watch-listed by the CSA MC because of a session-based policy violation. The valid range is 0 to 35. The default is 25.

Note Make sure you add the external product as a trusted host so the sensor can communicate with it.

Adding External Product Interfaces

To add external product interfaces, follow these steps:

Step 1 Log in to the CLI using an account with administrator privileges.

Step 2 Enter external product interfaces submode.

```
sensor# configure terminal
```

```
sensor(config)# service external-product-interface
```

Step 3 Add the CSA MC interface.

```
sensor(config-ext)# cisco-security-agents-mc-settings 209.165.200.225
sensor(config-ext-cis)#
```

Step 4 Enable receipt of information from the CSA MC.

```
sensor(config-ext-cis)# enabled yes
```

Step 5 Change the default port setting.

```
sensor(config-ext-cis)# port 80
```

Step 6 Configure the login settings:

a. Enter the username.

```
sensor(config-ext-cis)# username jsmith
```

b. Enter and confirm the password.

```
sensor(config-ext-cis)# password
Enter password[]: *******
Re-enter password: *******
sensor(config-ext-cis)#
```

Note Steps 7 through 10 are optional. If you do not perform Steps 7 though 10, the default values are used to receive all the CSA MC information with no filters applied.

Step 7 (Optional) Configure the watch list settings:

a. Allow the watch list information to be passed from the external product to the sensor.

```
sensor(config-ext-cis-wat)# enabled yes
```

Note If you do not enable the watch list, the watch list information received from a CSA MC is deleted.

b. Change the percentage of the manual watch list RR from the default of 25.

```
sensor(config-ext-cis-wat)# manual-rr-increase 30
```

c. Change the percentage of the session-based watch list RR from the default of 25.

```
sensor(config-ext-cis-wat)# session-rr-increase 30
```

d. Change the percentage of the packet-based watch list RR from the default of 10.

```
sensor(config-ext-cis-wat)# packet-rr-increase 20
```

Step 8 (Optional) Allow the host posture information to be passed from the external product to the sensor.

```
sensor(config-ext-cis)# host-posture-settings
sensor(config-ext-cis-hos)# enabled yes
```

Note If you do not enable the host posture information, the host posture information received from a CSA MC is deleted.

Step 9 (Optional) Allow the host posture information from unreachable hosts to be passed from the external product to the sensor.

```
sensor(config-ext-cis-hos)# allow-unreachable-postures yes
```

Note A host is not reachable if the CSA MC cannot establish a connection with the host on any of the IP addresses in the host's posture. 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. This filter is most applicable in network topologies where hosts that are not reachable by the CSA MC are also not reachable by the IPS, for example if the IPS and the CSA MC are on the same network segment.

Step 10 Configure a posture ACL:

a. Add the posture ACL into the ACL list.

```
sensor(config-ext-cis-hos)# posture-acls insert name1 begin
sensor(config-ext-cis-hos-pos)#
```

Note Posture ACLs are network address ranges for which host postures are allowed or denied. Use posture ACLs to filter postures that have IP addresses that may not be visible to the IPS or may be duplicated across the network.

b. Enter the network address the posture ACL will use.

```
sensor(config-ext-cis-hos-pos)# network-address 192.0.2.0/24
```

c. Choose the action (deny or permit) the posture ACL will take.

```
sensor(config-ext-cis-hos-pos)# action permit
```

Step 11 Verify the settings.

```
sensor(config-ext-cis-hos-pos)# exit
sensor(config-ext-cis-hos)# exit
sensor(config-ext-cis)# exit
sensor(config-ext)# show settings
   cisco-security-agents-mc-settings (min: 0, max: 2, current: 1)
   ---------------------------------------------
      ip-address: 209.165.200.225

      ---------------------------------------------
         interface-type: extended-sdee <protected>
         enabled: yes default: yes
         url: /csamc50/sdee-server <protected>
         port: 80 default: 443
         use-ssl
         ---------------------------------------------
            always-yes: yes <protected>
         ---------------------------------------------
         username: jsmith
         password: <hidden>
         host-posture-settings
         ---------------------------------------------
            enabled: yes default: yes
            allow-unreachable-postures: yes default: yes
            posture-acls (ordered min: 0, max: 10, current: 1 - 1 active, 0 inactive)
            ---------------------------------------------
            ACTIVE list-contents
```

```
                  ------------------------------------------------
                     NAME: name1
                     ------------------------------------------------
                        network-address: 192.0.2.0/24
                        action: permit
                     ------------------------------------------------
                     ------------------------------------------------
                  ------------------------------------------------
               ------------------------------------------------
               watchlist-address-settings
               ------------------------------------------------
                  enabled: yes default: yes
                  manual-rr-increase: 30 default: 25
                  session-rr-increase: 30 default: 25
                  packet-rr-increase: 20 default: 10
               ------------------------------------------------
            ------------------------------------------------
         ------------------------------------------------
sensor(config-ext)#
```

Step 12 Exit external product interface submode.

```
sensor(config-ext)# exit
Apply Changes:?[yes]:
```

Step 13 Press **Enter** to apply the changes or enter **no** to discard them.

For More Information

For the procedure for adding trusted hosts, see Adding TLS Trusted Hosts, page 4-53.

Troubleshooting External Product Interfaces

To troubleshoot external product interfaces, check the following:

- Make sure the interface is active by checking the output from the **show statistics external-product-interface** command in the CLI, or choose **Monitoring > Sensor Monitoring > Support Information > Statistics** in the IDM and check the Interface state line in the response, or choose **Configuration > *sensor_name* > Sensor Monitoring > Support Information > Statistics** in the IME, and check the Interface state line in the response.
- Make sure you have added the CSA MC IP address to the trusted hosts. If you forgot to add it, add it, wait a few minutes and then check again.
- Confirm subscription login information by opening and closing a subscription on the CSA MC using the browser.
- Check the Event Store for the CSA MC subscription errors.

For More Information

- For the procedure for adding trusted hosts, see Adding TLS Trusted Hosts, page 4-53.
- For the procedure for displaying events, see Clearing Events from Event Store, page 8-42.