IPS 6.X and later/IDSM2: Inline Interface Pairs Mode using IDM Configuration Example

Document ID: 107540

Contents

Introduction
Prerequisites
Requirements
Components Used
Related Products
Conventions
Inline Interface Pairs Configuration
CLI Configuration
IDM Configuration
Configure the Switch for IDSM−2 in Inline Mode
Troubleshoot
Problem
Solution
Related Information

Introduction

Operating in Inline Interface Pair mode puts the Intrusion Prevention System (IPS) directly into the traffic flow and affects packet−forwarding rates, which makes them slower when latency is added. This allows the sensor to stop attacks so it drops malicious traffic before it reaches the intended target, thus it provides a protective service. Not only is the inline device processing information on Layers 3 and 4, but it also analyzes the contents and payload of the packets for more sophisticated embedded attacks (Layers 3 to 7). This deeper analysis lets the system identify and stop and/or block attacks that normally pass through a traditional firewall device.

In Inline Interface Pair mode, a packet comes in through the first interface of the pair on the sensor and out the second interface of the pair. The packet is sent to the second interface of the pair unless that packet is being denied or modified by a signature.

Note: You can configure AIM−IPS and AIP−SSM to operate inline even though these modules have only one sensing interface.

Note: If the paired interfaces are connected to the same switch, you should configure them on the switch as access ports with different access VLANs for the two ports. Otherwise, traffic does not flow through the inline interface.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on Cisco IPS Sensor that uses the Command Line Interface 6.0 and Intrusion Prevention System Device Manager (IDM) 6.0.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Related Products

The information in this document is also applicable to the Intrusion Detection System (IDSM−2) Services Module.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Inline Interface Pairs Configuration

Use the **inline−interfaces** *name* command in the service interface submode in order to create inline interface pairs.

Note: Use the Command Lookup Tool (registered customers only) in order to obtain more information on the commands used in this section.

Note: AIP−SSM is configured for inline interface mode from the Cisco ASA CLI and not from the Cisco IPS CLI.

These options apply:

- **inline−interfaces** *name* Name of the logical inline interface pair

  Note: On all backplane sensing interfaces on all modules (IDSM−2 NM−CIDS, and AIP−SSM), **admin−state** is set to enabled and is protected (you cannot change the setting). The **admin−state** has no effect (and is protected) on the command and control interface. It only affects sensing interfaces. The command and control interface does not need to be enabled because it cannot be monitored.
- **default** Sets the value back to the system default setting
- **description** Your description of the inline interface pair
- **interface1** *interface_name* The first interface in the inline interface pair
- **interface2** *interface_name* The second interface in the inline interface pair
- **no** Removes an entry or selection setting
- **admin−state {enabled | disabled}** The administrative link state of the interface, whether the interface is enabled or disabled.

CLI Configuration

Complete these steps in order to configure the inline VLAN pair settings on the sensor:

1. Log in to the CLI with an account that has administrator privileges.
2. Enter the interface submode:

```
sensor#configure terminal
```

```
sensor(config)#service interface
sensor(config-int)#
```

3. Verify if any inline interfaces exist. The subinterface type should read `none` if no inline interfaces have been configured:

```
sensor(config-int)#show settings
   physical-interfaces (min: 0, max: 999999999, current: 2)
   -----------------------------------------------
      <protected entry>
      name: GigabitEthernet0/0 <defaulted>
      -----------------------------------------------
         media-type: tx <protected>
         description: <defaulted>
         admin-state: disabled <protected>
         duplex: auto <defaulted>
         speed: auto <defaulted>
         alt-tcp-reset-interface
         -----------------------------------------------
            none
            -----------------------------------------------
            -----------------------------------------------
         -----------------------------------------------
         subinterface-type
         -----------------------------------------------
            none
            -----------------------------------------------
            -----------------------------------------------
         -----------------------------------------------
      -----------------------------------------------
<protected entry>
      name: GigabitEthernet0/1 <defaulted>
      -----------------------------------------------
         media-type: tx <protected>
         description: <defaulted>
         admin-state: disabled <defaulted>
         duplex: auto <defaulted>
         speed: auto <defaulted>
         alt-tcp-reset-interface
         -----------------------------------------------
            none
            -----------------------------------------------
            -----------------------------------------------
         -----------------------------------------------
         subinterface-type
         -----------------------------------------------
            none
            -----------------------------------------------
            -----------------------------------------------
         -----------------------------------------------
      -----------------------------------------------
      <protected entry>
      name: GigabitEthernet0/2 <defaulted>
      -----------------------------------------------
         media-type: tx <protected>
         description: <defaulted>
         admin-state: disabled <defaulted>
         duplex: auto <defaulted>
         speed: auto <defaulted>
         alt-tcp-reset-interface
         -----------------------------------------------
            none
            -----------------------------------------------
            -----------------------------------------------
         -----------------------------------------------
         subinterface-type
         -----------------------------------------------
```

```
            none
            -----------------------------------------------
            -----------------------------------------------
         -----------------------------------------------
      -----------------------------------------------
      <protected entry>
      name: GigabitEthernet0/3 <defaulted>
      -----------------------------------------------
         media-type: tx <protected>
         description: <defaulted>
         admin-state: disabled <defaulted>
         duplex: auto <defaulted>
         speed: auto <defaulted>
         alt-tcp-reset-interface
         -----------------------------------------------
            none
            -----------------------------------------------
            -----------------------------------------------
         -----------------------------------------------
         subinterface-type
         -----------------------------------------------
            none
            -----------------------------------------------
            -----------------------------------------------
         -----------------------------------------------
      -----------------------------------------------
      <protected entry>
      name: Management0/0 <defaulted>
      -----------------------------------------------
         media-type: tx <protected>
         description: <defaulted>
         admin-state: disabled <protected>
         duplex: auto <defaulted>
         speed: auto <defaulted>
         alt-tcp-reset-interface
         -----------------------------------------------
            none
            -----------------------------------------------
            -----------------------------------------------
         -----------------------------------------------
         subinterface-type
         -----------------------------------------------
            none
            -----------------------------------------------
            -----------------------------------------------
         -----------------------------------------------
      -----------------------------------------------
   -----------------------------------------------
   command-control: Management0/0 <protected>
   inline-interfaces (min: 0, max: 999999999, current: 0)
   -----------------------------------------------
   -----------------------------------------------
   bypass-mode: auto <defaulted>
   interface-notifications
   -----------------------------------------------
      missed-percentage-threshold: 0 percent <defaulted>
      notification-interval: 30 seconds <defaulted>
      idle-interface-delay: 30 seconds <defaulted>
   -----------------------------------------------
sensor(config-int)#
```

4. Name the inline pair:

```
sensor(config-int)#inline-interfaces PAIR1
```

5. Display the list of available interfaces:

```
sensor(config-int)#physical-interfaces ?
GigabitEthernet0/0     GigabitEthernet0/0 physical interface.
GigabitEthernet0/1     GigabitEthernet0/1 physical interface.
GigabitEthernet0/2     GigabitEthernet0/2 physical interface.
GigabitEthernet0/3     GigabitEthernet0/3 physical interface.
Management0/0          Management0/0 physical interface.
sensor(config-int)#physical-interfaces
```

6. Configure two interfaces into a pair:

```
sensor(config-int)#interface1 GigabitEthernet0/0

sensor(config-int-inl)#interface2 GigabitEthernet0/1
```

   You must assign the interface to a virtual sensor and enable it before it can monitor traffic. See step 10 for more information.

7. Add a description of this interface:

```
sensor(config-int-phy)#description PAIR1 Gig0/0 and Gig0/1
```

8. Repeat steps 4 through 7 for any other interfaces that you want to configure to inline interface pairs.
9. Verify the settings:

```
sensor(config-int-inl)#show settings
   name: PAIR1
   -----------------------------------------------
      description: PAIR1 Gig0/0 & Gig0/1 default:
      interface1: GigabitEthernet0/0
      interface2: GigabitEthernet0/1
   -----------------------------------------------
```

10. Enable the interfaces assigned to the interface pair:

```
sensor(config-int)#exit
sensor(config-int)#physical-interfaces GigabitEthernet0/0
sensor(config-int-phy)#admin-state enabled
sensor(config-int-phy)#exit
sensor(config-int)#physical-interfaces GigabitEthernet0/1
sensor(config-int-phy)#admin-state enabled
sensor(config-int-phy)#exit
sensor(config-int)#
```

11. Verify that the interfaces are enabled:

```
sensor(config-int)#show settings
   physical-interfaces (min: 0, max: 999999999, current: 5)
   -----------------------------------------------
      <protected entry>
      name: GigabitEthernet0/0
      -----------------------------------------------
         media-type: tx <protected>
         description: <defaulted>
         admin-state: enabled default: disabled
         duplex: auto <defaulted>
         speed: auto <defaulted>
         default-vlan: 0 <defaulted>
         alt-tcp-reset-interface
         -----------------------------------------------
            none
            -----------------------------------------------
            -----------------------------------------------
         -----------------------------------------------
         subinterface-type
         -----------------------------------------------
            none
            -----------------------------------------------
            -----------------------------------------------
         -----------------------------------------------
      -----------------------------------------------
      <protected entry>
      name: GigabitEthernet0/1
      -----------------------------------------------
         media-type: tx <protected>
         description: <defaulted>
         admin-state: enabled default: disabled
         duplex: auto <defaulted>
         speed: auto <defaulted>
         default-vlan: 0 <defaulted>
         alt-tcp-reset-interface
         -----------------------------------------------
            none
            -----------------------------------------------
            -----------------------------------------------
         -----------------------------------------------
         subinterface-type
         -----------------------------------------------
            none
            -----------------------------------------------
            -----------------------------------------------
         -----------------------------------------------
      -----------------------------------------------
      <protected entry>
      name: GigabitEthernet0/2 <defaulted>
      -----------------------------------------------
         media-type: tx <protected>
         description: <defaulted>
         admin-state: disabled <defaulted>
         duplex: auto <defaulted>
         speed: auto <defaulted>
         default-vlan: 0 <defaulted>
         alt-tcp-reset-interface
         -----------------------------------------------
            none
            -----------------------------------------------
            -----------------------------------------------
         -----------------------------------------------
         subinterface-type
         -----------------------------------------------
            none
            -----------------------------------------------
            -----------------------------------------------
         -----------------------------------------------
      -----------------------------------------------
      <protected entry>
      name: GigabitEthernet0/3 <defaulted>
      -----------------------------------------------
         media-type: tx <protected>
--MORE--
```

12. Issue this command in order to delete an inline interface pair and return the interfaces to promiscuous mode:

    ```
    sensor(config-int)#no inline-interfaces PAIR1
    ```

    You must also delete the inline interface pair from the virtual sensor to which it is assigned.
13. Verify the inline interface pair has been deleted:

    ```
    sensor(config-int)#show settings
      -----------------------------------------------
      command-control: Management0/0 <protected>
      inline-interfaces (min: 0, max: 999999999, current: 0)
      -----------------------------------------------
      -----------------------------------------------
    ```

```
bypass-mode: auto <defaulted>
interface-notifications
-----------------------------------------------
```

14. Exit interface configuration submode:

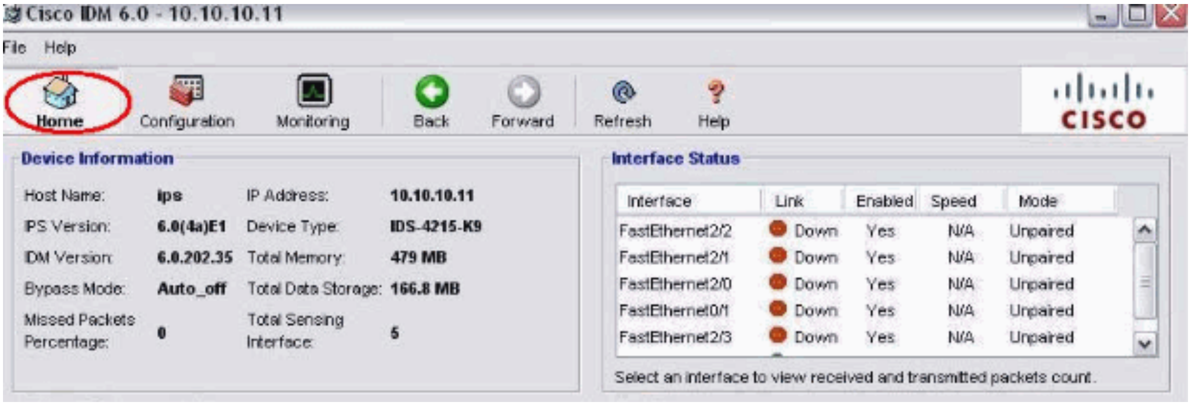
    ```
    sensor(config-int)#exit
    Apply Changes:?[yes]:
    ```

15. Press **Enter** in order to apply the changes or enter **no** in order to discard them.

IDM Configuration

Complete these steps in order to configure the inline VLAN pair settings on the sensor using the IDM:

1. Open your browser and enter **https://<Management_IP_Address_of_IPS>** to access the IDM on the IPS.
2. Click **Download IDM Launcher** and **Start IDM** to download the installer for the application.
3. Go to the Home page in order to view the device information such as Host Name, IP Address, version, and the model.



Device Information

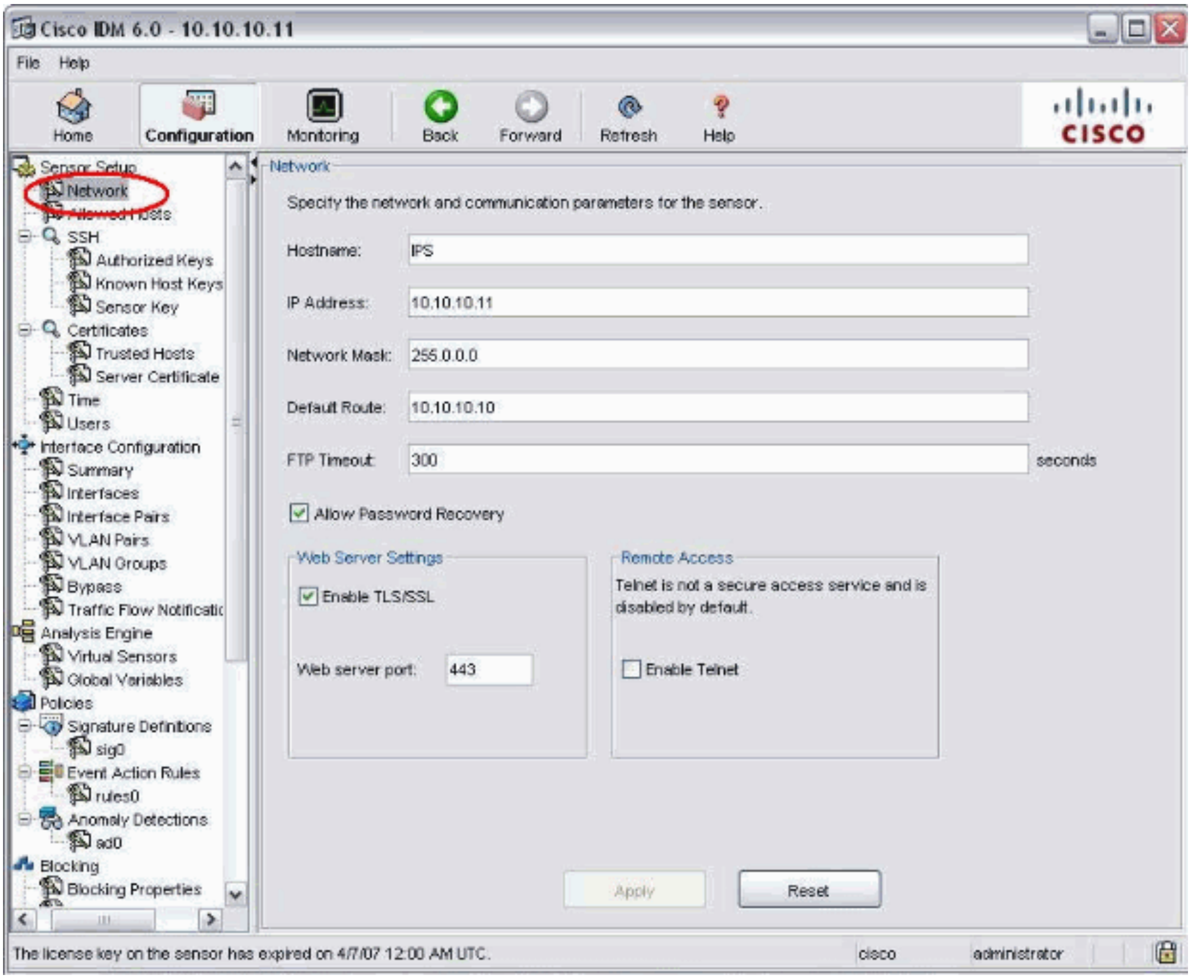
Host Name:	ips	IP Address:	10.10.10.11
IPS Version:	6.0(4a)E1	Device Type:	IDS-4215-K9
IDM Version:	6.0.202.35	Total Memory:	479 MB
Bypass Mode:	Auto_off	Total Data Storage:	166.8 MB
Missed Packets Percentage:	0	Total Sensing Interface:	5

Interface Status

Interface	Link	Enabled	Speed	Mode
FastEthernet2/2	● Down	Yes	N/A	Unpaired
FastEthernet2/1	● Down	Yes	N/A	Unpaired
FastEthernet2/0	● Down	Yes	N/A	Unpaired
FastEthernet0/1	● Down	Yes	N/A	Unpaired
FastEthernet2/3	● Down	Yes	N/A	Unpaired

Select an interface to view received and transmitted packets count.

4. Go to **Configuration > Sensor Setup** and click **Network**. Here you can specify the Hostname, IP Address and Default Route.



Specify the network and communication parameters for the sensor.

Hostname: IPS

IP Address: 10.10.10.11

Network Mask: 255.0.0.0

Default Route: 10.10.10.10

FTP Timeout: 300 seconds

☑ Allow Password Recovery

Web Server Settings

☑ Enable TLS/SSL

Web server port: 443

Remote Access

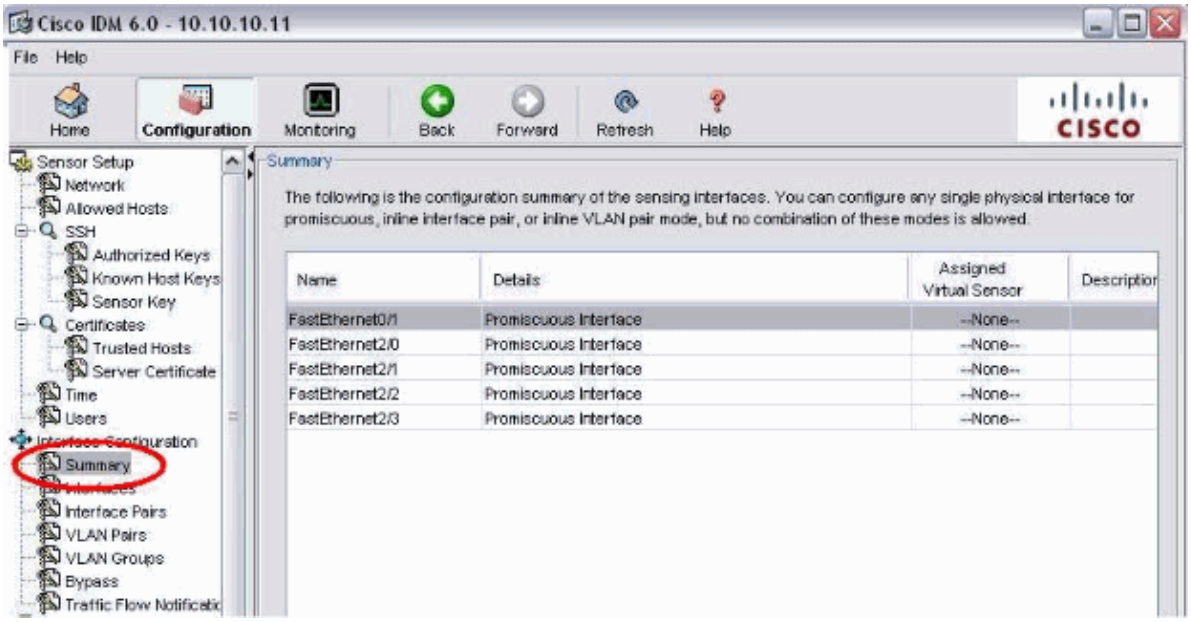
Telnet is not a secure access service and is disabled by default.

☐ Enable Telnet

The license key on the sensor has expired on 4/7/07 12:00 AM UTC. cisco administrator

5. Go to **Configuration** > **Interface Configuration** and click **Summary**.

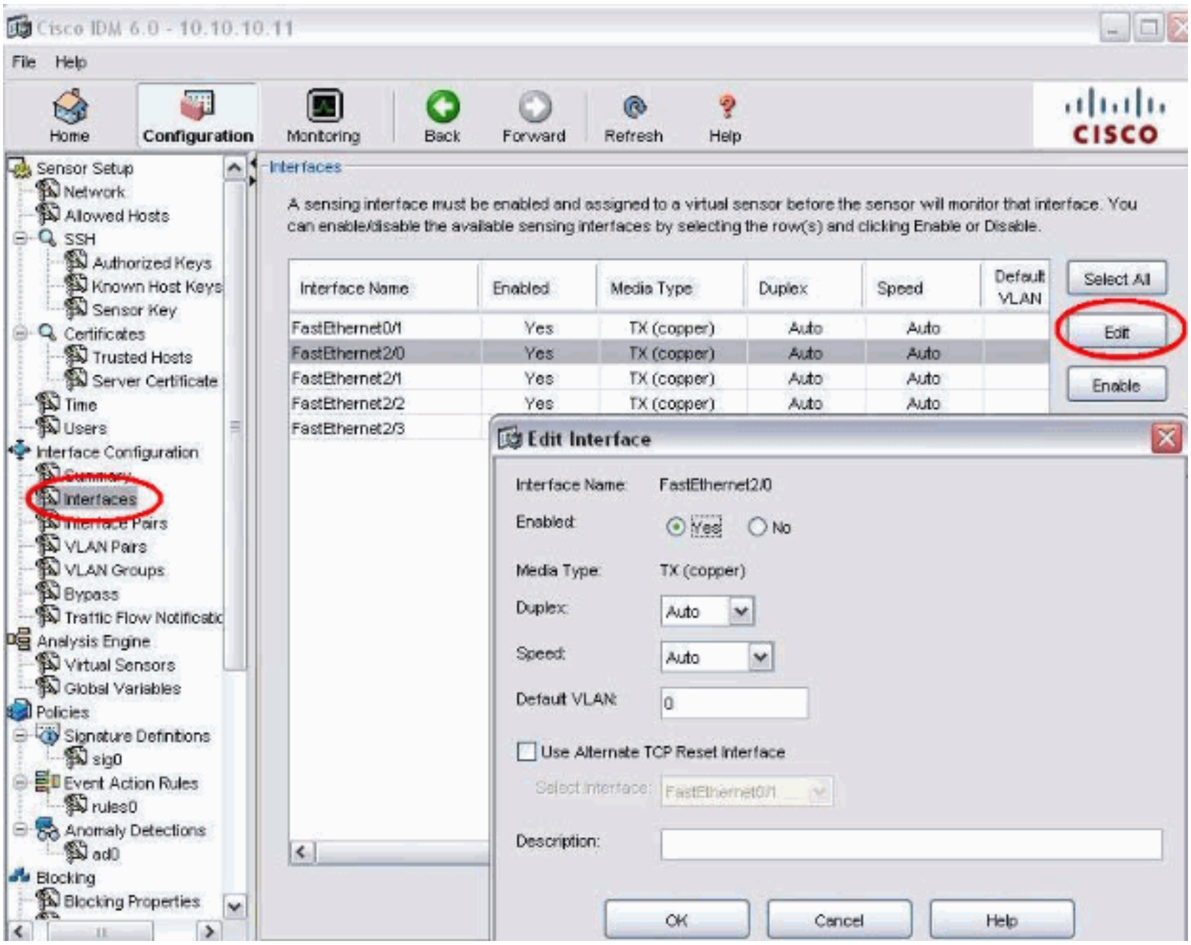
   This page shows the configuration summary of the sensing interface:



The following is the configuration summary of the sensing interfaces. You can configure any single physical interface for promiscuous, inline interface pair, or inline VLAN pair mode, but no combination of these modes is allowed.

Name	Details	Assigned Virtual Sensor	Descriptior
FastEthernet0/1	Promiscuous Interface	--None--	
FastEthernet2/0	Promiscuous Interface	--None--	
FastEthernet2/1	Promiscuous Interface	--None--	
FastEthernet2/2	Promiscuous Interface	--None--	
FastEthernet2/3	Promiscuous Interface	--None--	

6. Go to **Configuration** > **Interface Configuration** > **Interfaces** and select the interface name. Then, click **Enable** in order to enable the sensing interface. Also, configure the Duplex, Speed and VLAN information.



Interfaces

A sensing interface must be enabled and assigned to a virtual sensor before the sensor will monitor that interface. You can enable/disable the available sensing interfaces by selecting the row(s) and clicking Enable or Disable.

Interface Name	Enabled	Media Type	Duplex	Speed	Default VLAN
FastEthernet0/1	Yes	TX (copper)	Auto	Auto	
FastEthernet2/0	Yes	TX (copper)	Auto	Auto	
FastEthernet2/1	Yes	TX (copper)	Auto	Auto	
FastEthernet2/2	Yes	TX (copper)	Auto	Auto	
FastEthernet2/3					

Edit Interface

Interface Name: FastEthernet2/0

Enabled: ● Yes ○ No

Media Type: TX (copper)

Duplex: Auto

Speed: Auto

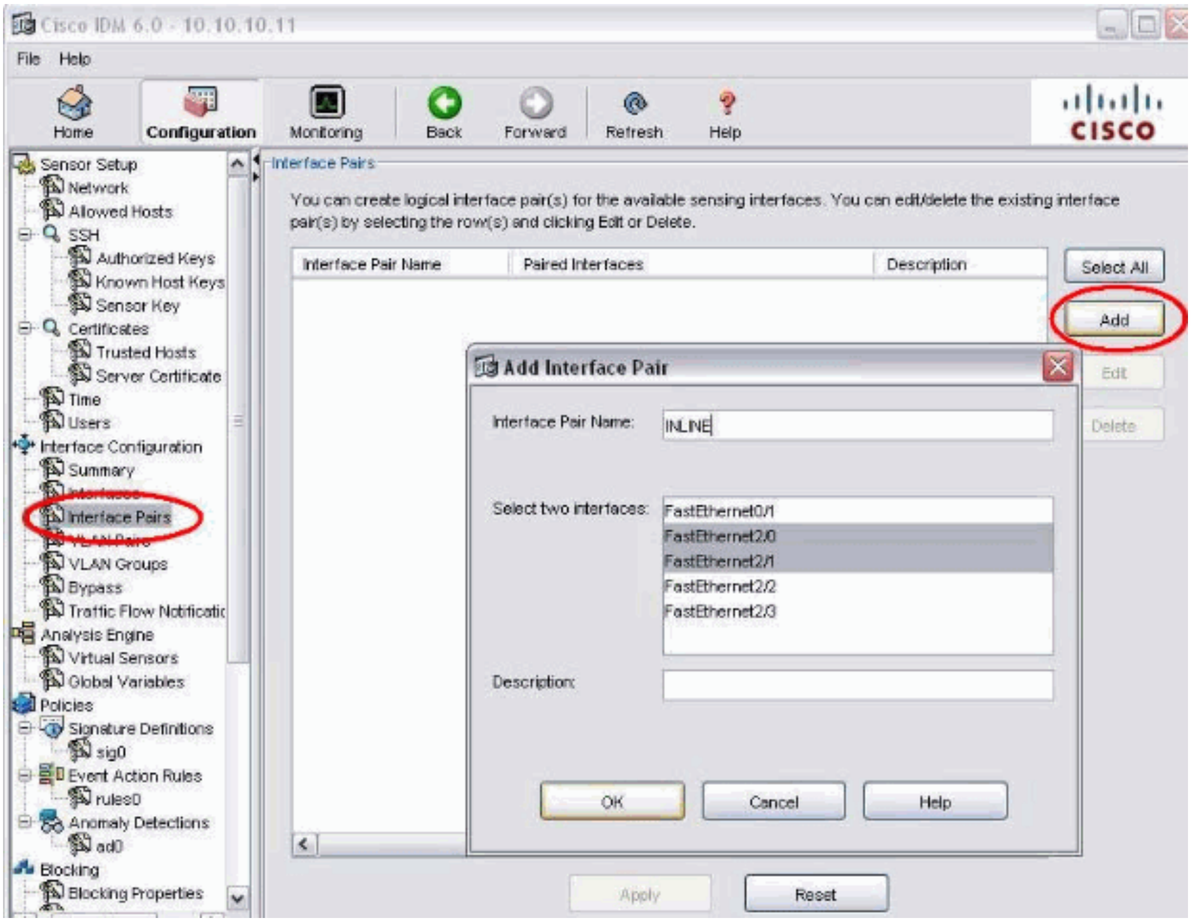
Default VLAN: 0

□ Use Alternate TCP Reset Interface

Select Interface: FastEthernet0/1

Description:

7. Go to **Configuration** > **Interface Configuration** > **Interface Pairs** and click **Add** in order to create the Inline Pair.



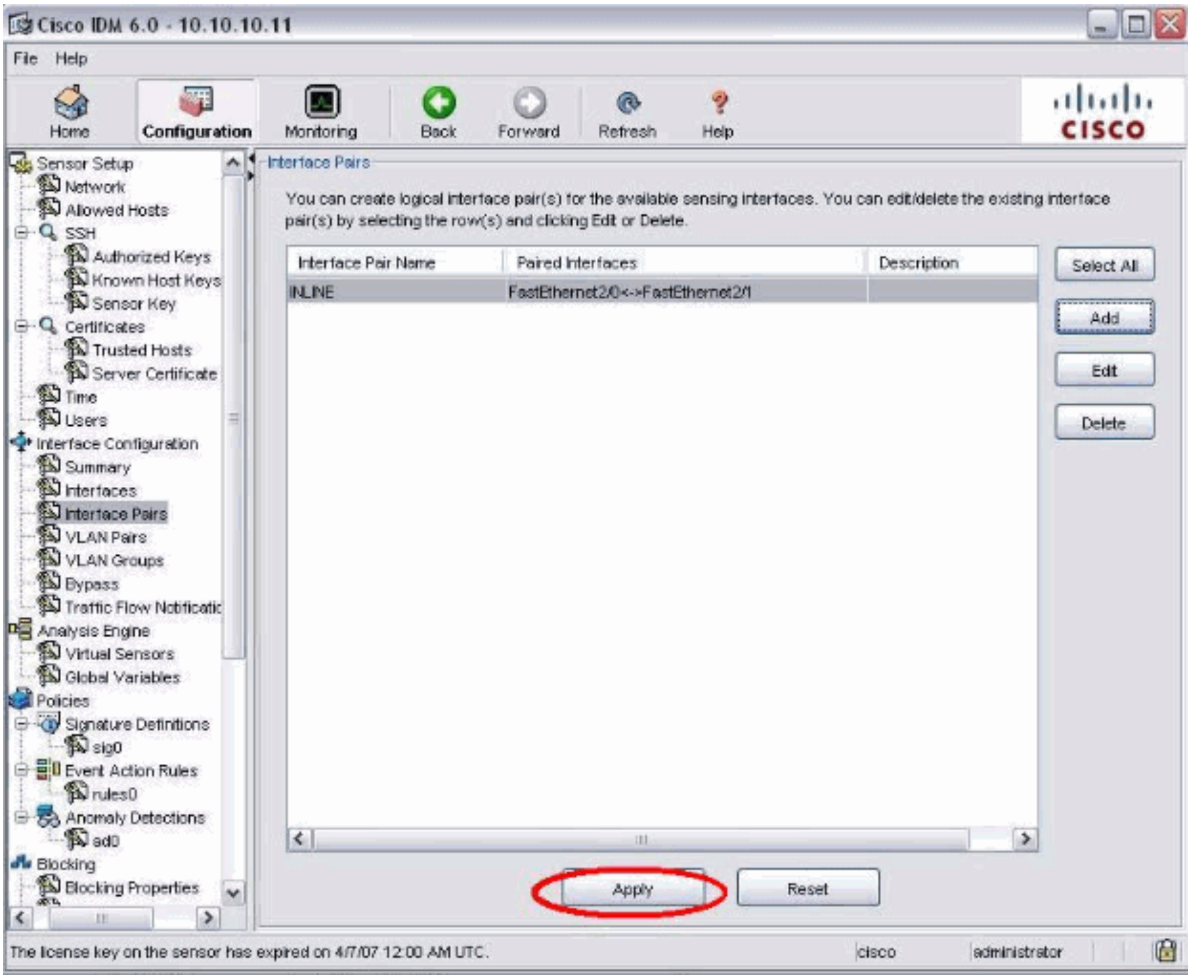
You can create logical interface pair(s) for the available sensing interfaces. You can edit/delete the existing interface pair(s) by selecting the row(s) and clicking Edit or Delete.

Interface Pair Name: INLINE

Select two interfaces:
FastEthernet0/1
FastEthernet2/0
FastEthernet2/1
FastEthernet2/2
FastEthernet2/3

Description:

8. View the summary of the Inline Pair Configuration and apply it.

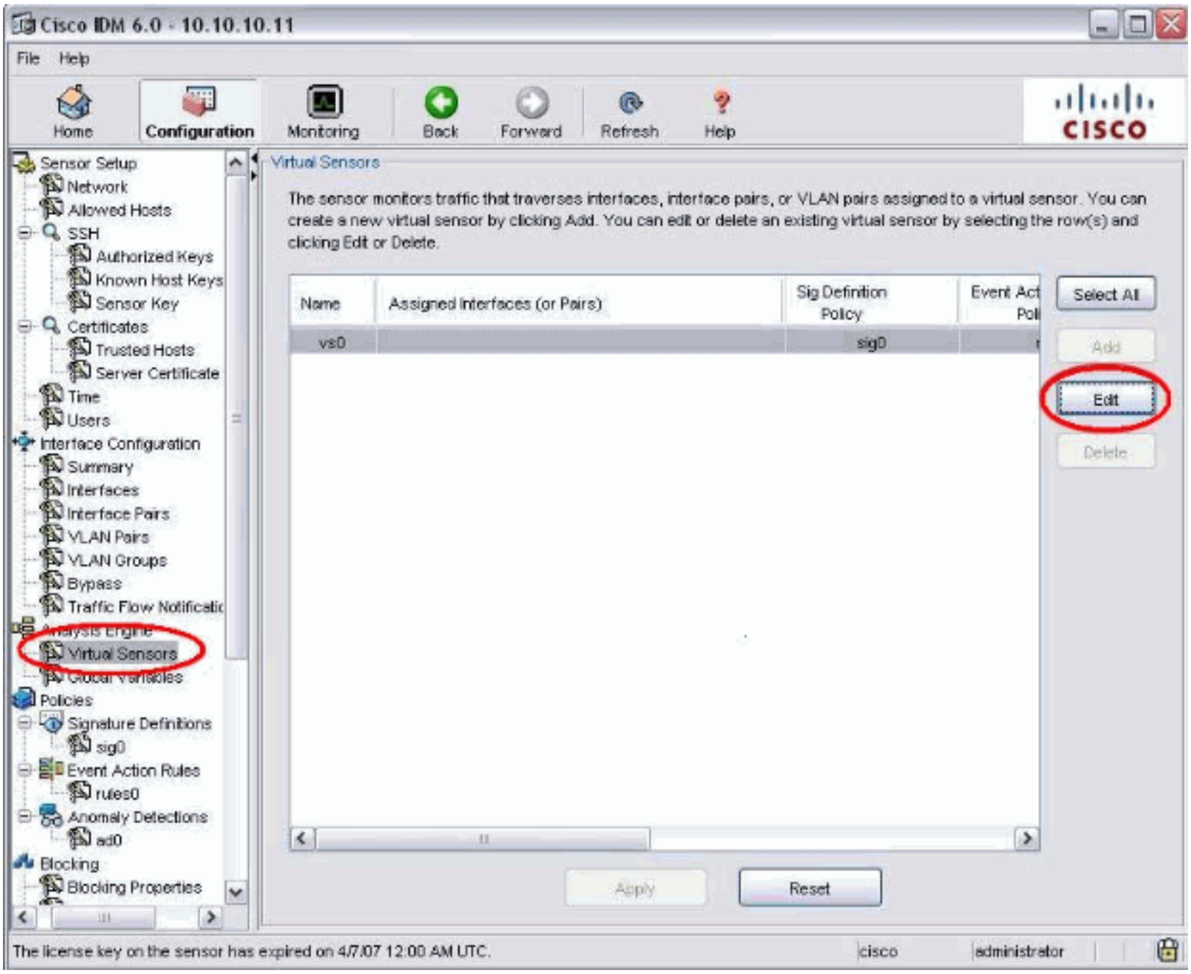


You can create logical interface pair(s) for the available sensing interfaces. You can edit/delete the existing interface pair(s) by selecting the row(s) and clicking Edit or Delete.

Interface Pair Name	Paired Interfaces	Description
INLINE	FastEthernet2/0<->FastEthernet2/1	

The license key on the sensor has expired on 4/7/07 12:00 AM UTC.

9. Go to **Configuration > Analysis Engine > Virtual Sensor** and click **Edit** in order to create the new virtual sensor.



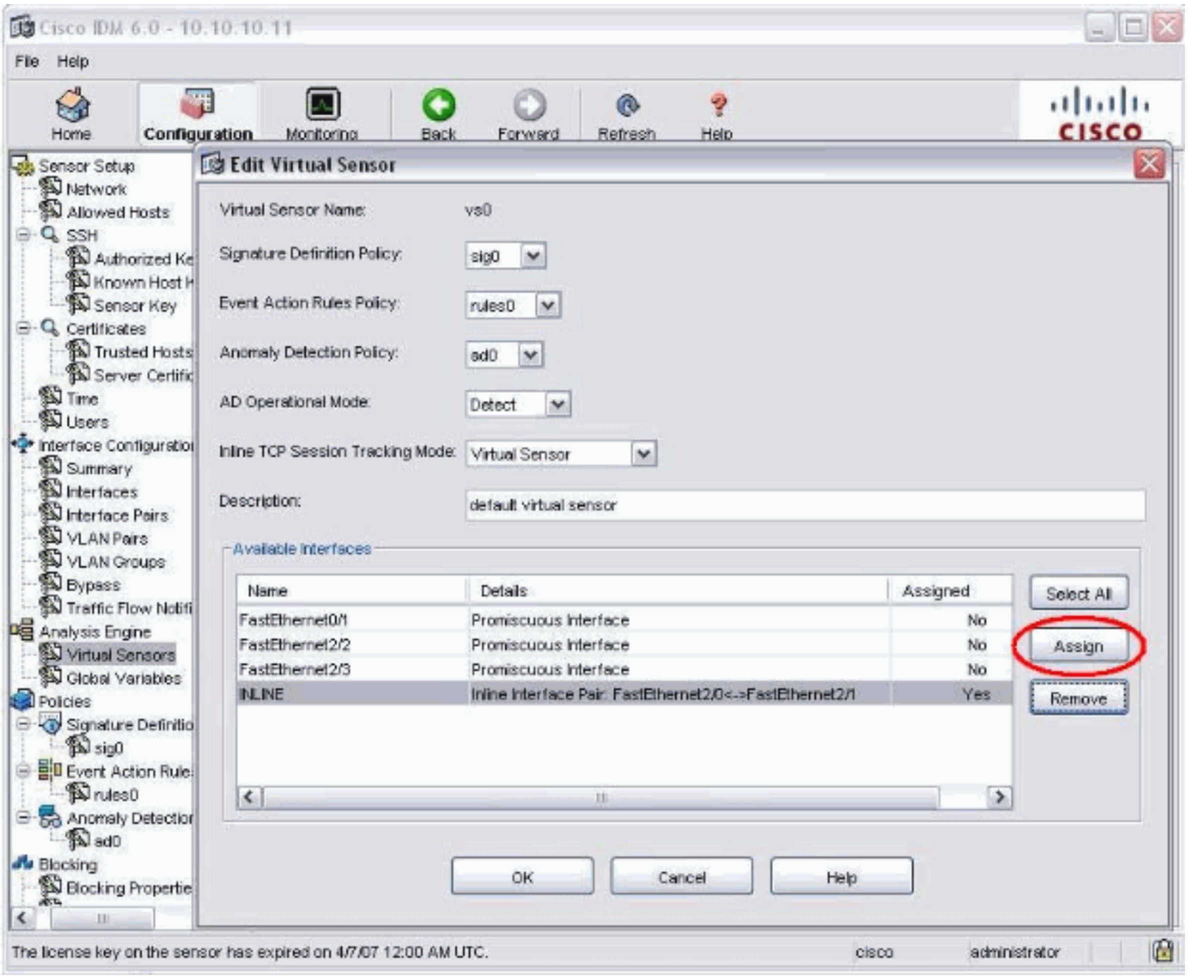
Virtual Sensors

The sensor monitors traffic that traverses interfaces, interface pairs, or VLAN pairs assigned to a virtual sensor. You can create a new virtual sensor by clicking Add. You can edit or delete an existing virtual sensor by selecting the row(s) and clicking Edit or Delete.

Name	Assigned Interfaces (or Pairs)	Sig Definition Policy	Event Act Poli
vs0		sig0	r

The license key on the sensor has expired on 4/7/07 12:00 AM UTC. cisco administrator

10. Assign the Inline pair **INLINE** to the Virtual Sensor vs0.



Virtual Sensor Name: vs0

Signature Definition Policy: sig0

Event Action Rules Policy: rules0

Anomaly Detection Policy: ad0

AD Operational Mode: Detect

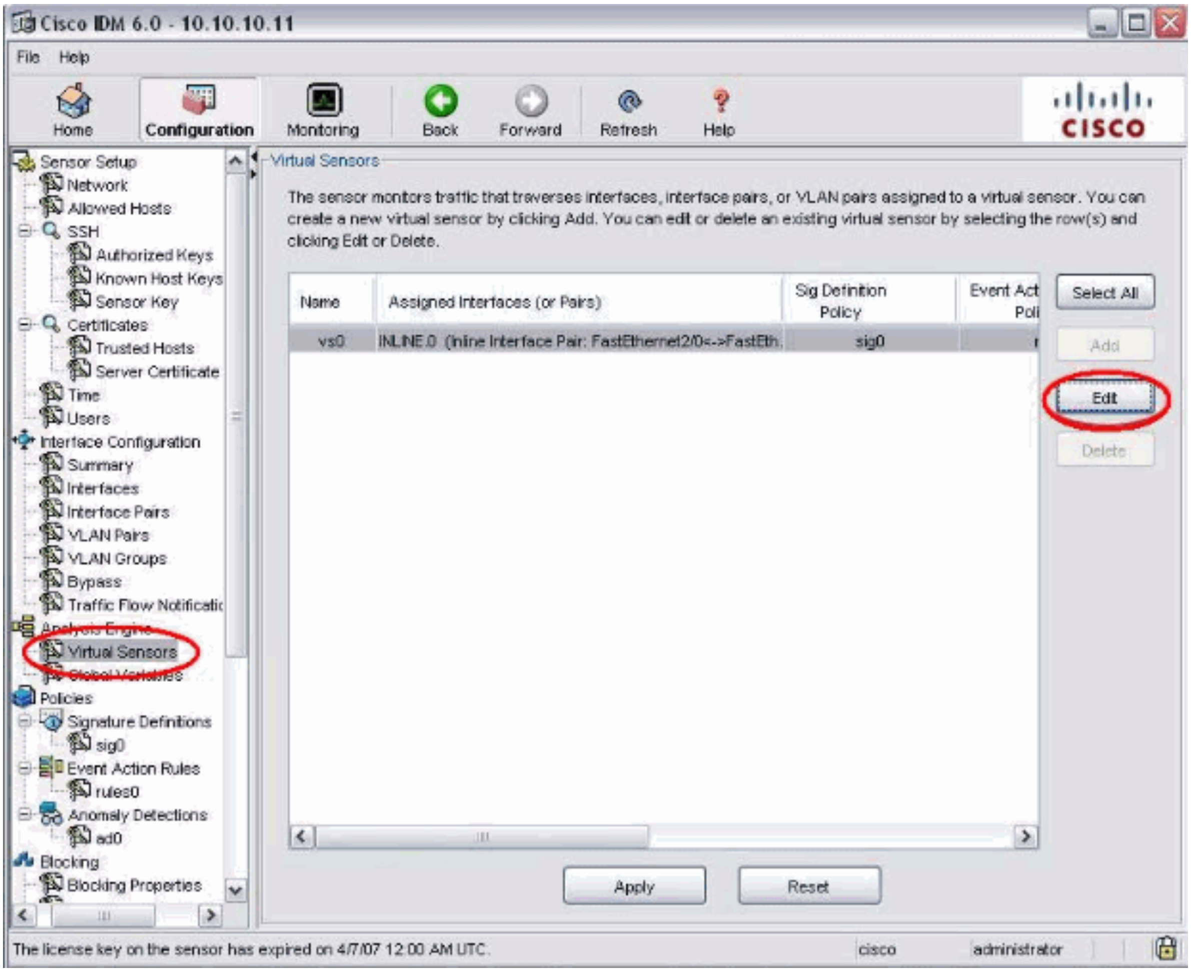
Inline TCP Session Tracking Mode: Virtual Sensor

Description: default virtual sensor

Name	Details	Assigned
FastEthernet0/1	Promiscuous Interface	No
FastEthernet2/2	Promiscuous Interface	No
FastEthernet2/3	Promiscuous Interface	No
INLINE	Inline Interface Pair: FastEthernet2/0<->FastEthernet2/1	Yes

The license key on the sensor has expired on 4/7/07 12:00 AM UTC. cisco administrator

11. View the summary of the assigned virtual sensor information.



The sensor monitors traffic that traverses interfaces, interface pairs, or VLAN pairs assigned to a virtual sensor. You can create a new virtual sensor by clicking Add. You can edit or delete an existing virtual sensor by selecting the row(s) and clicking Edit or Delete.

Name	Assigned Interfaces (or Pairs)	Sig Definition Policy	Event Act Poli
vs0	INLINE.0 (Inline Interface Pair: FastEthernet2/0<->FastEth	sig0	r

The license key on the sensor has expired on 4/7/07 12:00 AM UTC.

Configure the Switch for IDSM−2 in Inline Mode

Refer to the Configuring the Catalyst Series 6500 Switch for IDSM−2 in Inline Mode section of Configuring IDSM−2 in order to configure the switch for IDSM−2 inline mode.

Troubleshoot

Problem

If the IPS fails and it is configured inline, do the interfaces fail open (traffic continues to pass) or closed (traffic is dropped).

Solution

You can configure IPS in fail−open state. Thus, if the IPS fails it will continue to pass the traffic, but it will not monitor the traffic.

Related Information

- **Cisco ASA 5500 Series Adaptive Security Appliances**
- **Cisco Intrusion Prevention System**
- **Cisco IPS 4200 Series Sensors**
- **Technical Support & Documentation − Cisco Systems**