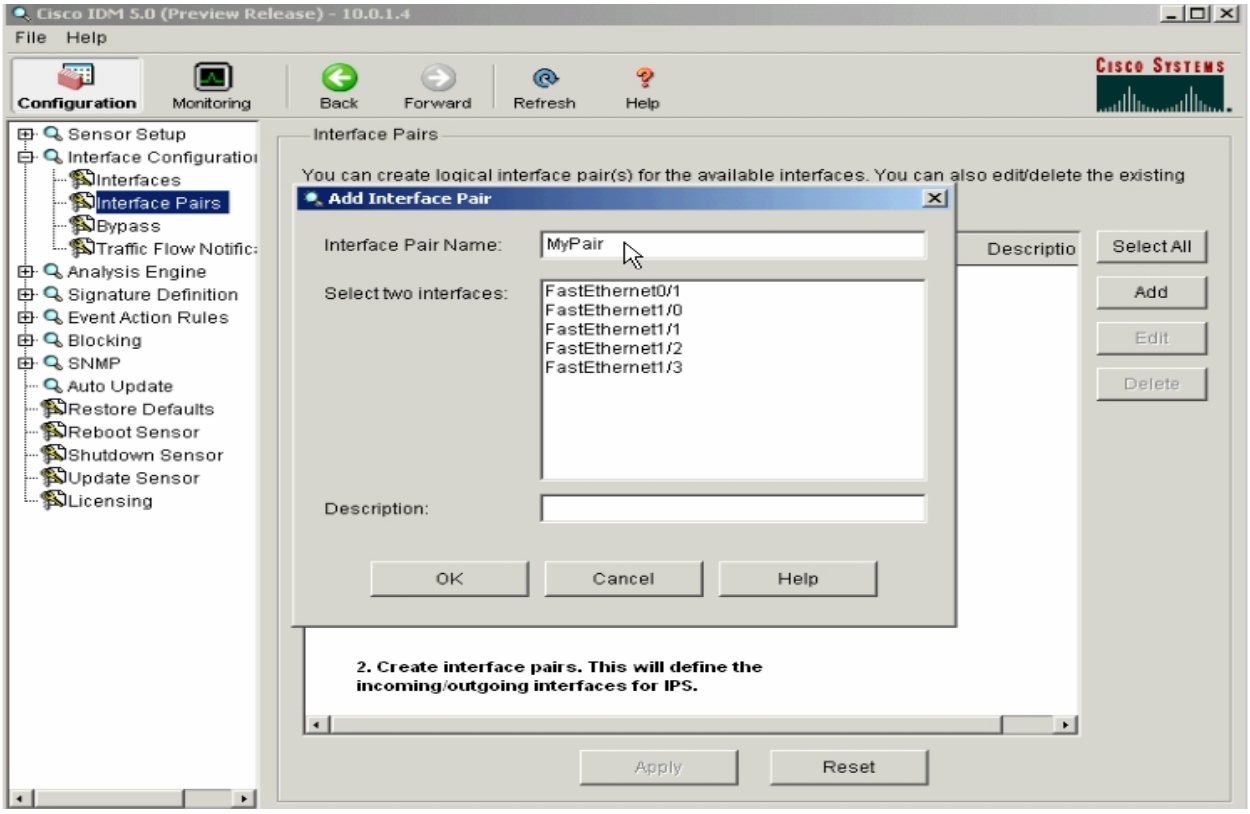
IPS BASIC CONFIGURATION:

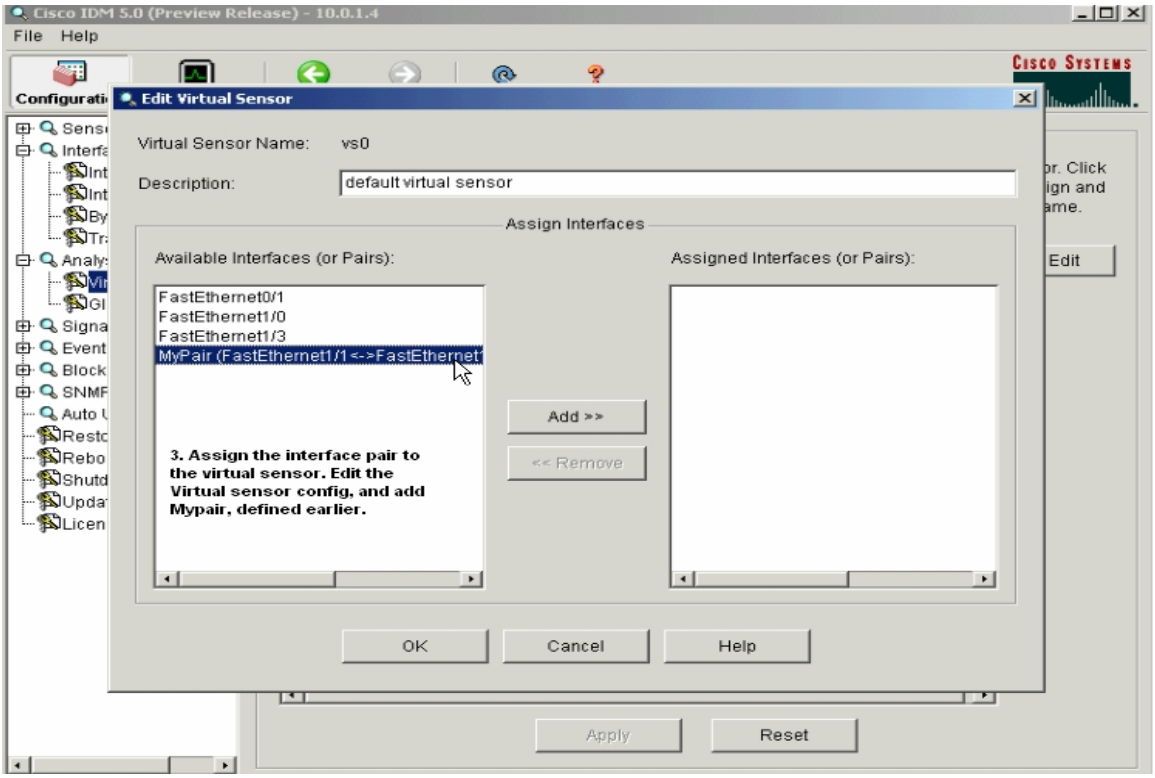
The following pages will show you how to complete all of the tasks necessary for configuring inline IPS.

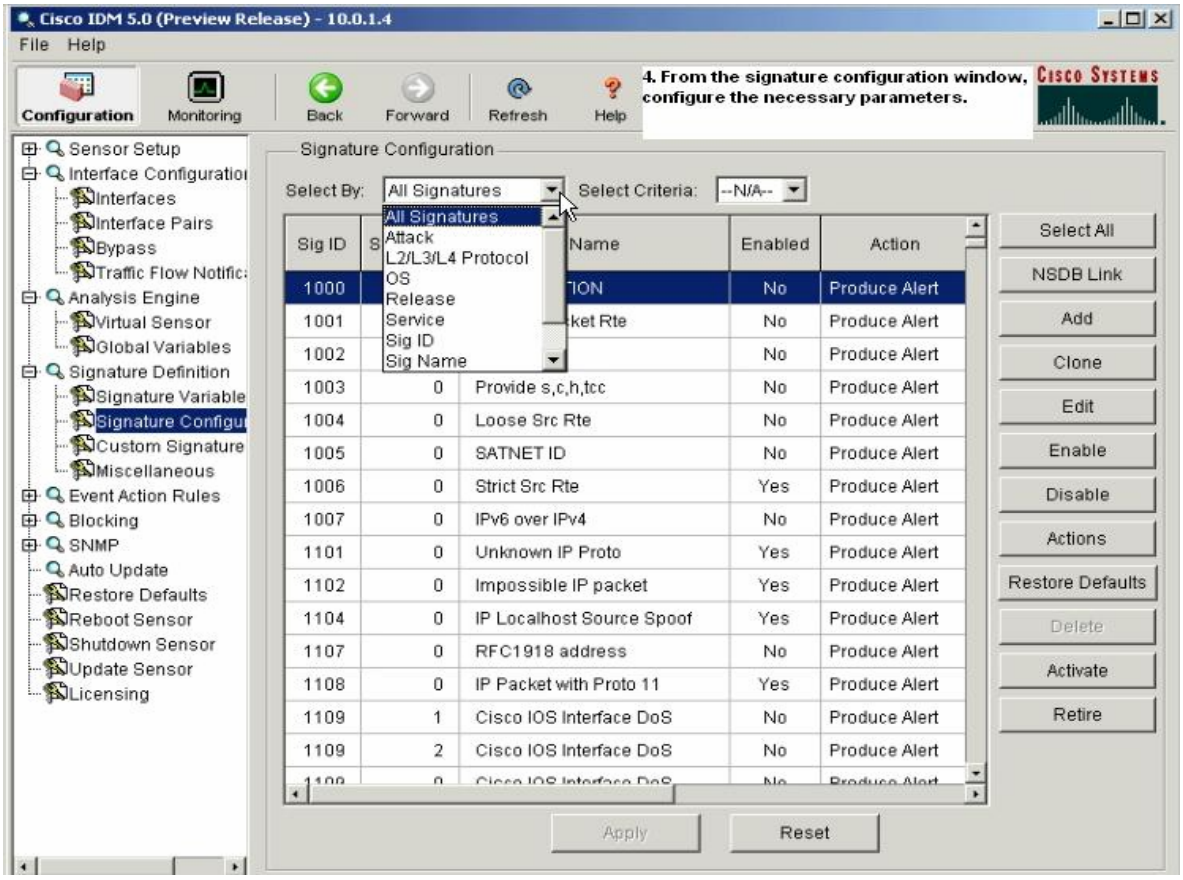
Configuring inline IPS consists of the tasks listed below:

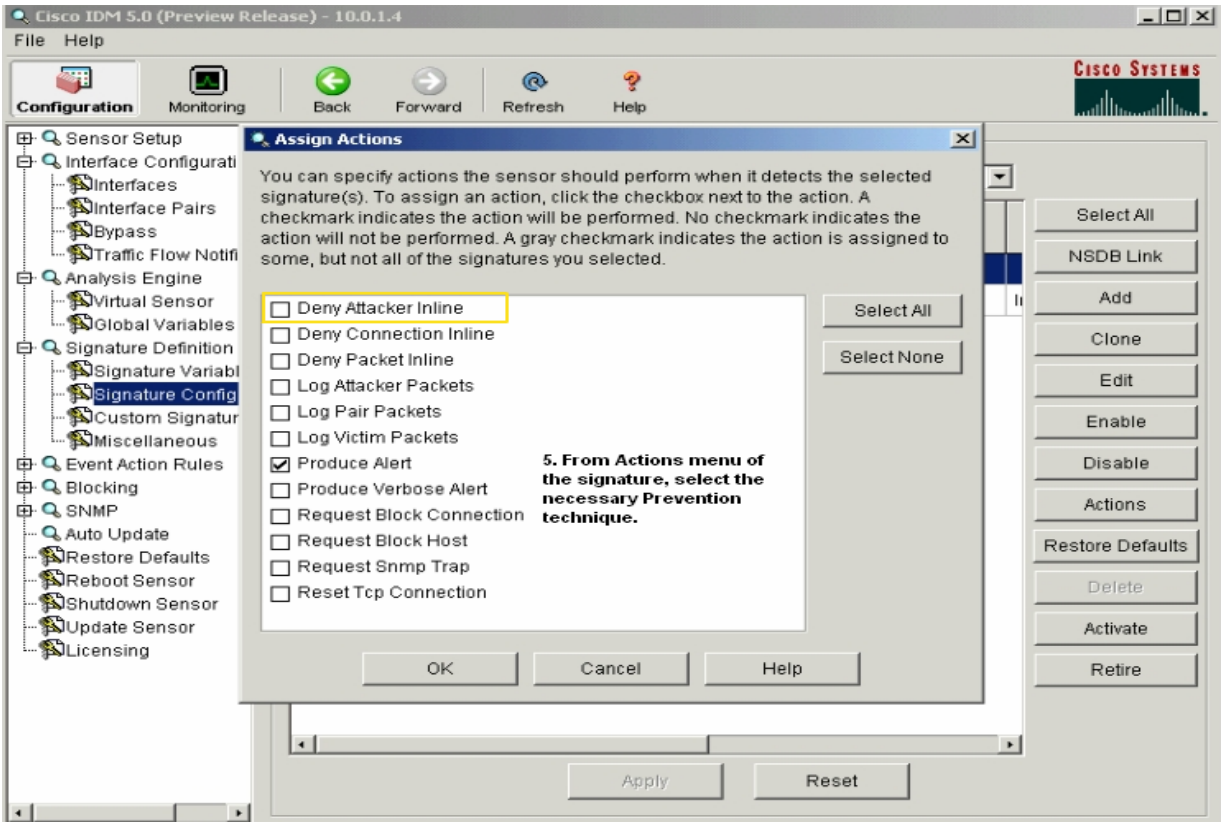
1. **Installing the sensor between two devices that have external network ports.**
   See the IPS Deployment guide for details.
2. **Enabling the interfaces.**
3. **Creating an interface pair.**
4. **Assigning the interfaces to the virtual sensor.**
5. **Configuring the desired signatures with inline drop actions.**

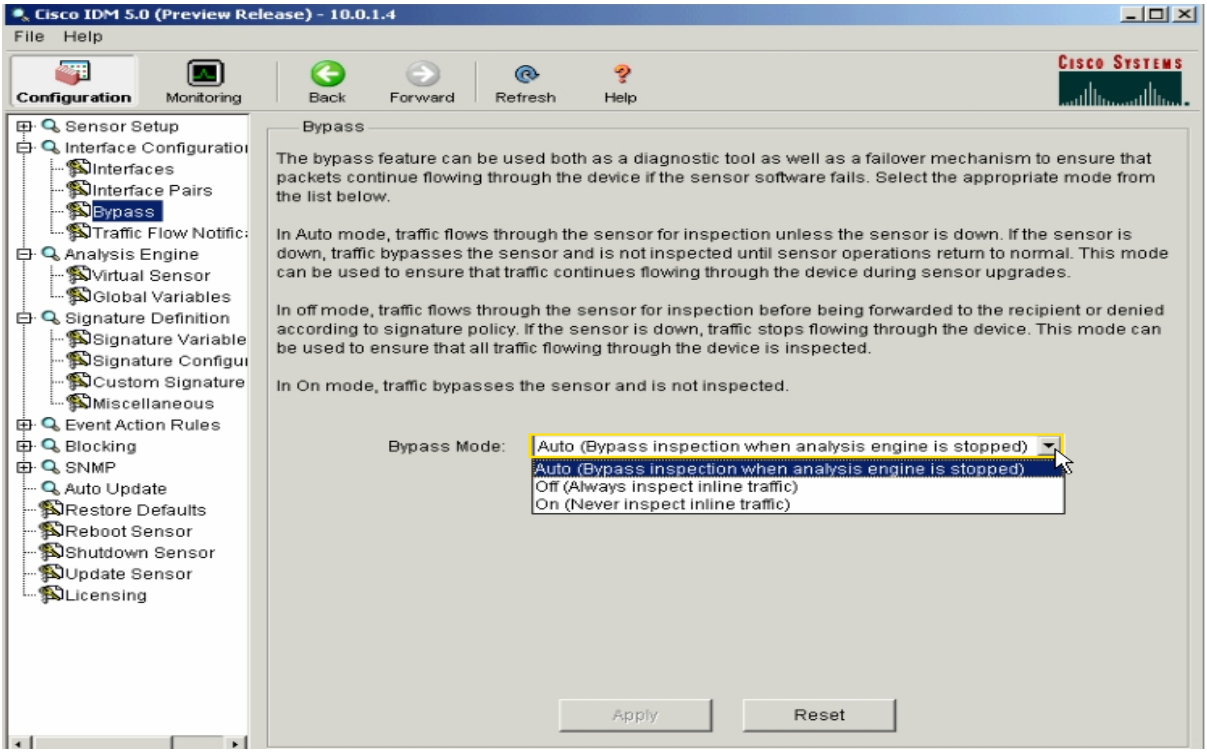
This module also shows you how to configure the software bypass mode. Software bypass mode can be used to enable traffic to continue to flow through inline pairs even when the sensor is not running. This function minimizes dataflow interruptions during reconfiguration, service pack installation, or software failure.




Cisco IDM 5.0 (Preview Release) - 10.0.1.4
File Help
Edit Virtual Sensor
Virtual Sensor Name: vs0
Description: default virtual sensor
Assign Interfaces
Available Interfaces (or Pairs):
Assigned Interfaces (or Pairs):
FastEthernet0/1
FastEthernet1/0
FastEthernet1/3
MyPair (FastEthernet1/1<->FastEthernet
Add >>
<< Remove
3. Assign the interface pair to the virtual sensor. Edit the Virtual sensor config, and add Mypair, defined earlier.
OK
Cancel
Help
Apply
Reset


Cisco IDM 5.0 (Preview Release) - 10.0.1.4
File Help
Configuration
Monitoring
Back
Forward
Refresh
Help
4. From the signature configuration window, configure the necessary parameters.
Signature Configuration
Select By: All Signatures
Select Criteria: --N/A--
All Signatures
Attack
L2/L3/L4 Protocol
OS
Release
Service
Sig ID
Sig Name
Sig ID
Name
Enabled
Action
1000 No Produce Alert
1001 No Produce Alert
1002 No Produce Alert
1003 0 Provide s,c,h,tcc No Produce Alert
1004 0 Loose Src Rte No Produce Alert
1005 0 SATNET ID No Produce Alert
1006 0 Strict Src Rte Yes Produce Alert
1007 0 IPv6 over IPv4 No Produce Alert
1101 0 Unknown IP Proto Yes Produce Alert
1102 0 Impossible IP packet Yes Produce Alert
1104 0 IP Localhost Source Spoof Yes Produce Alert
1107 0 RFC1918 address No Produce Alert
1108 0 IP Packet with Proto 11 Yes Produce Alert
1109 1 Cisco IOS Interface DoS No Produce Alert
1109 2 Cisco IOS Interface DoS No Produce Alert
Select All
NSDB Link
Add
Clone
Edit
Enable
Disable
Actions
Restore Defaults
Delete
Activate
Retire
Apply
Reset
Sensor Setup
Interface Configuration
Interfaces
Interface Pairs
Bypass
Traffic Flow Notific
Analysis Engine
Virtual Sensor
Global Variables
Signature Definition
Signature Variable
Signature Configu
Custom Signature
Miscellaneous
Event Action Rules
Blocking
SNMP
Auto Update
Restore Defaults
Reboot Sensor
Shutdown Sensor
Update Sensor
Licensing


Cisco IDM 5.0 (Preview Release) - 10.0.1.4
File Help
Configuration
Monitoring
Back
Forward
Refresh
Help
Cisco Systems
Sensor Setup
Interface Configurati
Interfaces
Interface Pairs
Bypass
Traffic Flow Notifi
Analysis Engine
Virtual Sensor
Global Variables
Signature Definition
Signature Variabl
Signature Config
Custom Signatur
Miscellaneous
Event Action Rules
Blocking
SNMP
Auto Update
Restore Defaults
Reboot Sensor
Shutdown Sensor
Update Sensor
Licensing
Assign Actions
You can specify actions the sensor should perform when it detects the selected signature(s). To assign an action, click the checkbox next to the action. A checkmark indicates the action will be performed. No checkmark indicates the action will not be performed. A gray checkmark indicates the action is assigned to some, but not all of the signatures you selected.
Deny Attacker Inline
Deny Connection Inline
Deny Packet Inline
Log Attacker Packets
Log Pair Packets
Log Victim Packets
Produce Alert
Produce Verbose Alert
Request Block Connection
Request Block Host
Request Snmp Trap
Reset Tcp Connection
Select All
Select None
5. From Actions menu of the signature, select the necessary Prevention technique.
OK
Cancel
Help
Select All
NSDB Link
Add
Clone
Edit
Enable
Disable
Actions
Restore Defaults
Delete
Activate
Retire
Apply
Reset


Cisco IDM 5.0 (Preview Release) - 10.0.1.4
File Help
Configuration
Monitoring
Back
Forward
Refresh
Help
Cisco Systems
Sensor Setup
Interface Configuratio
Interfaces
Interface Pairs
Bypass
Traffic Flow Notific
Analysis Engine
Virtual Sensor
Global Variables
Signature Definition
Signature Variable
Signature Configu
Custom Signature
Miscellaneous
Event Action Rules
Blocking
SNMP
Auto Update
Restore Defaults
Reboot Sensor
Shutdown Sensor
Update Sensor
Licensing
Bypass
The bypass feature can be used both as a diagnostic tool as well as a failover mechanism to ensure that packets continue flowing through the device if the sensor software fails. Select the appropriate mode from the list below.
In Auto mode, traffic flows through the sensor for inspection unless the sensor is down. If the sensor is down, traffic bypasses the sensor and is not inspected until sensor operations return to normal. This mode can be used to ensure that traffic continues flowing through the device during sensor upgrades.
In off mode, traffic flows through the sensor for inspection before being forwarded to the recipient or denied according to signature policy. If the sensor is down, traffic stops flowing through the device. This mode can be used to ensure that all traffic flowing through the device is inspected.
In On mode, traffic bypasses the sensor and is not inspected.
Bypass Mode:
Auto (Bypass inspection when analysis engine is stopped)
Auto (Bypass inspection when analysis engine is stopped)
Off (Always inspect inline traffic)
On (Never inspect inline traffic)
Apply
Reset

BASIC CONFIGURATIONS DONE !!!!

IPS READY TO DO ITS FUNCTIONALITY !!!!