



## **Security Configuration Guide: Unified Threat Defense, Cisco IOS XE Release 3S**

### **Americas Headquarters**

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
<http://www.cisco.com>  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <http://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2015 Cisco Systems, Inc. All rights reserved.



## CONTENTS

---

### CHAPTER 1

#### Cisco Firepower Threat Defense for ISR 1

Finding Feature Information 1

Restrictions for Cisco Firepower Threat Defense for ISR 1

Information About Cisco Firepower Threat Defense for ISR 2

Cisco Firepower Threat Defense for ISR Overview 2

UCS-Based Hosting 3

IDS Packet Flow in Cisco Firepower Threat Defense 4

Firepower Sensor Interfaces 4

Cisco Firepower Threat Defense Interoperability 4

Hardware and Software Requirements for Cisco Firepower Threat Defense 5

Obtaining Cisco Firepower Threat Defense License 5

How to Deploy Cisco Firepower Threat Defense for ISR 6

Obtaining the Firepower Sensor Package 6

Installing the Firepower Sensor OVA File 6

Installing Firepower Sensor on a UCS E-Series Blade 6

Configuring Traffic Redirect on Cisco UCS E-Series Blade 8

Bootstrapping the Firepower Sensor 9

Enabling IDS Inspection Globally 11

Enabling IDS Inspection per Interface 12

Configuration Examples for Cisco Firepower Threat Defense on ISR 14

Example: Configuring Traffic Redirect on Cisco UCS E-Series Blade 14

Example: Bootstrapping the Firepower Sensor 14

Example: Enabling IDS Inspection Globally 15

Example: Enabling IDS Inspection per Interface 15

Verifying and Monitoring IDS Inspection 15

Additional References for Cisco Firepower Threat Defense for ISR 17

Feature Information for Cisco Firepower Threat Defense for ISR 18

---

**CHAPTER 2****Snort IPS 19**

Finding Feature Information	19
Restrictions for Snort IPS	20
Information About Snort IPS	20
Snort IPS Overview	20
Snort IPS Signature Package	20
Snort IPS Solution	21
Overview of Snort Virtual Service Interfaces	21
Virtual Service Resource Profile	22
Deploying Snort IPS	25
How to Deploy Snort IPS	25
Installing the Snort OVA File	26
Configuring VirtualPortGroup Interfaces and Virtual Service	27
Configuring Snort IPS Globally	31
Configuring Snort IDS Inspection Globally	35
Displaying the List of Active Signatures	38
Configuration Examples for Snort IPS	38
Example: Configuring VirtualPortGroup Interfaces and Virtual Service	38
Example: Configuring a Different Resource Profile	39
Example: Configuring UTD with Operation Mode IPS and Policy Security	39
Example: Configuring Snort IPS Globally	39
Example: Configuring Snort IPS Inspection per Interface	40
Example: Configuring UTD with VRF on both Inbound and Outbound Interface	40
Example: Configuring Logging IOS Syslog	41
Example: Configuring Logging to Centralized Log Server	42
Example: Configuring Signature Update from a Cisco Server	42
Example: Configuring Signature Update from a Local Server	42
Example: Configuring Automatic Signature Update	42
Example: Performing Manual Signature Update	43
Example: Configuring Signature Whitelist	43
Examples for Displaying Active Signatures	44
Example: Displaying Active Signatures List With Balanced Policy	44
Example: Displaying Active Signatures List With Security Policy	44
Example: Displaying Active Signatures List With Connectivity Policy	44

Verifying the Integrated Snort IPS Configuration	45
Deploying Snort IPS Using Cisco Prime CLI Templates	52
Troubleshooting Snort IPS	53
Traffic is not Diverted	53
Signature Update is not Working	56
Signature Update from the Local Server is not Working	57
Logging to IOSd Syslog is not Working	58
Logging to an External Server is not Working	58
UTD Conditional Debugging	59
Additional References for Snort IPS	59
Feature Information for Snort IPS	60





## CHAPTER

# 1

## Cisco Firepower Threat Defense for ISR

Cisco Firepower Threat Defense is Cisco's premier network security option. It provides a comprehensive suite of security features such as firewall capabilities, monitoring, alerts, Intrusion Detection System (IDS) and Intrusion Prevention System (IPS).

This module describes how to configure and deploy IDS on Cisco Integrated Services Routers (ISRs).

- [Finding Feature Information, page 1](#)
- [Restrictions for Cisco Firepower Threat Defense for ISR, page 1](#)
- [Information About Cisco Firepower Threat Defense for ISR, page 2](#)
- [How to Deploy Cisco Firepower Threat Defense for ISR, page 6](#)
- [Configuration Examples for Cisco Firepower Threat Defense on ISR, page 14](#)
- [Verifying and Monitoring IDS Inspection, page 15](#)
- [Additional References for Cisco Firepower Threat Defense for ISR, page 17](#)
- [Feature Information for Cisco Firepower Threat Defense for ISR, page 18](#)

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to [www.cisco.com/go/cfn](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

## Restrictions for Cisco Firepower Threat Defense for ISR

- Multicast traffic is not inspected.
- IPv6 traffic cannot be exported.

# Information About Cisco Firepower Threat Defense for ISR

## Cisco Firepower Threat Defense for ISR Overview

Cisco Firepower Threat Defense is a premier security solution that provides enhanced inspection for packet flows.

The Cisco Firepower Threat Defense solution consists of the following two entities:

- **Cisco FireSIGHT**—A centralized policy and reporting entity that can run anywhere in the network. This can be the Cisco FireSIGHT appliance or a virtual installation on a server class machine.
- **Virtual Firepower sensor**—Security entities that implement policies, and send events and statistics back to the defense center. The Firepower sensor is hosted on Cisco Unified Computing System (UCS) E-Series Blade. Both the FireSIGHT and sensor are distributed as virtual packages.

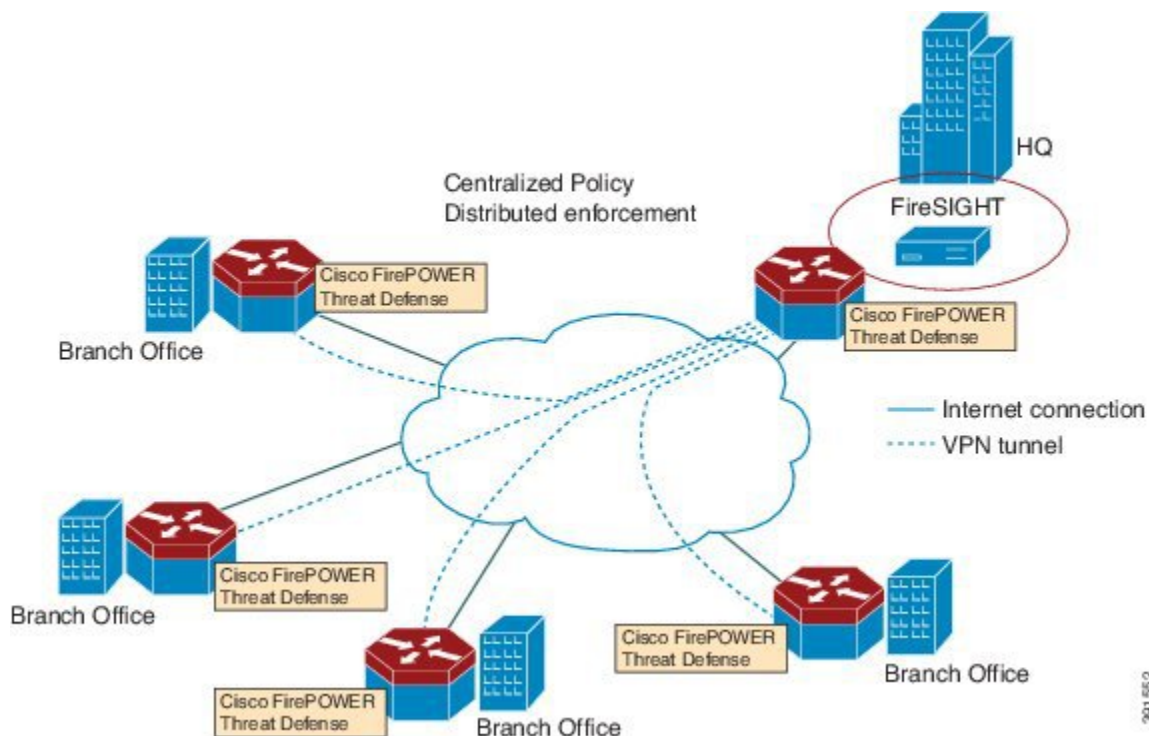
UCS E-Series Blades are general purpose blade servers that are housed within Cisco Integrated Services Routers (ISR) Generation 2 (G2) and Cisco ISR 4000 Series Integrated Services Routers. These blades can be deployed either as bare-metal on operating systems or as virtual machines on hypervisors. There are two internal interfaces that connect a router to an UCS E-Series Blade. On ISR G2, Slot0 is a Peripheral Component Interconnect Express (PCIe) internal interface, and UCS E-Series Slot1 is a switched interface connected to the backplane Multi Gigabit Fabric (MGF). In Cisco ISR 4000 Series Routers, both internal interfaces are connected to the MGF.

A hypervisor is installed on the UCS E-Series Blade, and Cisco Firepower Threat Defense runs as a virtual machine on it. The Cisco Firepower Threat Defense OVA file is directly installed on the UCS E-Series Blade using the hypervisor operating system. Cisco Firepower Threat Defense runs as an anonymous inline device with no additional communication with the router. Traffic is diverted from the ingress physical interface to the Cisco Firepower Threat Defense that runs on the UCS E-Series Blade.



The following figure shows a Cisco Firepower Threat Defense deployment scenario. In this figure, the traffic lines between sensors and FireSIGHT are control connections. Packets are routed through these connections using router forwarding rules.

**Figure 1: Cisco Firepower Threat Defense Deployment Scenario**



By default, the virtualized Cisco Firepower sensor comes with three interfaces, one for management, and two others for traffic analysis. These interfaces must be mapped to the UCS E-Series interfaces.

## UCS-Based Hosting

The Cisco Unified Computing System (UCS) E-Series Blade provides a generic server blade for hosting applications. This blade typically runs VMware ESXi hypervisor and is managed through vSphere like other VMWare deployments.

If the Firepower sensor is hosted on the Cisco UCS E-Series Blade, you must specify the Cisco IOS interfaces connected to Cisco Firepower Threat Defense. Applications running within the UCS E-Series Blade are only loosely coupled with Cisco IOS, and to determine the interfaces that are attached to appliances a mapping of the interfaces must be done. Interfaces to connect to the Cisco UCS E-Series Blade are Bridge Domain Interfaces (BDI).

The following Cisco UCS E-Series Blades are supported for hosting the Firepower sensor:

- UCS-E 120S
- UCS-E 140D
- UCS-E 140S

- UCS-E 160D
- UCS-E 180D

## IDS Packet Flow in Cisco Firepower Threat Defense

Cisco Firepower Threat Defense supports Intrusion Detection System (IDS). In IDS mode, traffic is copied to the sensor and is analyzed for threats. IDS mode cannot enforce policies; it can detect and report violations. In IDS mode, traffic is replicated from interfaces and redirected to Cisco Firepower Threat Defense that runs on the Cisco UCS E-Series blade.

IDS copies the traffic and analyzes them for threats. Enable the **utd** command to replicate packets to the Firepower sensor based on one of the following criteria:

- If global inspection is enabled, all packets that flow through a router are replicated to the sensor.
- If per interface inspection is enabled, packets are replicated only if the input or output interface has enabled the **utd** command for inspection.

To view the interfaces that have enabled packet inspection in IDS mode, use the **show platform software utd interfaces** command. The packet replication occurs as one of the first output features.

For general packet processing, features that are applied to a packet form an ordered sequence that is determined by the configuration of the device. In general, these features are grouped as either input or output features, with the routing function marking the boundary between the two. The IDS packet replication occurs as one of the first output features and so if any input feature drops the packet, it will not be replicated to the IDS engine.

## Firepower Sensor Interfaces

The Firepower sensor virtual appliance has three network interfaces—two for analyzing the traffic and one for management connectivity to FireSIGHT. The two traffic-bearing interfaces are represented as two virtual interfaces; Bridge Domain Interfaces (BDIs), in the configuration.

Although two interfaces are available for analyzing the traffic, only one traffic-bearing interface is used for Intrusion Detection System (IDS).

The Firepower sensor is connected to the management network and appears as another host on the LAN segment.

## Cisco Firepower Threat Defense Interoperability

Cisco Firepower Threat Defense supports Intrusion Detection System (IDS). In IDS mode, selected traffic is copied to the Firepower sensor for analysis.

Cisco Firepower Threat Defense interoperates with the following features:

- Zone-based firewall—Application layer gateways (ALGs), application inspection and controls (AICs), and policies configured between zones
- Network Address Translation (NAT)

**Note**

Cisco Firepower Threat Defense does not support outside address translation, because there is no mechanism to inform Firepower Threat Defense about outside global addresses. However, you can still enable address translation on outside interfaces. Intrusion Prevention System (IPS) or IDS is invoked after NAT on the ingress interface, and before NAT on the egress interface, always using inside addresses.

- Crypto
- Intelligent WAN (IWAN)
- Kernel-based Virtual Machine Wide-Area Application Services (kWAAS)

## Hardware and Software Requirements for Cisco Firepower Threat Defense

The following hardware is required to run the Cisco Firepower Threat Defense solution:

- Cisco Firepower Sensor version 5.4
- Cisco Integrated Services Routers (ISR) 4000 Series Routers
- Cisco Unified Computing System (UCS) E-Series Blade
- Cisco FireSIGHT

The following software is required to run the Cisco Firepower Threat Defense solution:

- UCS-E hypervisor
- ESXi 5.0.0, 5.1.0, or 5.5.0
- Cisco Firepower Sensor version Cisco IOS XE Release 3.14S and later releases
- Cisco FireSIGHT version 5.2, 5.3 or 5.4. FireSIGHT only supports the current version and is backward compatible with only the previous version. In case, your Cisco Firepower Sensor version is 5.4, then you have to use FireSIGHT version 5.4 or 5.3.

## Obtaining Cisco Firepower Threat Defense License

Cisco ISR 4000 Series Integrated Services Routers must have the security K9 license and Application Experience (AppX) license to enable the Cisco Firepower Threat Defense.

Technology Package License Information:

Technology	Technology-package Current	Type	Technology-package Next reboot
appx	appxk9	EvalRightToUse	appxk9
uc	uck9	EvalRightToUse	uck9
security	securityk9	EvalRightToUse	securityk9
ipbase	ipbasek9	Permanent	ipbasek9

# How to Deploy Cisco Firepower Threat Defense for ISR

To deploy Cisco Firepower Threat Defense Intrusion Detection System (IDS), perform the following tasks:

- 1 Obtain the Firepower sensor package.
- 2 Install the Firepower sensor package through a hypervisor, such as VMWare VSphere.
- 3 Configure router interfaces for traffic redirection.
  - Bridge-Domain interface (BDI) configuration for Cisco ISR 4000 Series Routers.
  - VLAN configuration for Cisco ISR Generation 2 routers.
- 4 Bootstrap the Firepower sensor.
- 5 Configure a policy in Cisco FireSIGHT.
  - The policy is configured through the FireSIGHT GUI.
- 6 Enable inspection.

## Obtaining the Firepower Sensor Package

To deploy the Firepower sensor on an Unified Computing System (UCS) E-Series Blade, download and save the OVA file. OVA is an Open Virtualization Archive that contains a compressed and installable version of a virtual machine. Download the OVA file from [https://support.sourcefire.com/sections/1/sub\\_sections/51#5-2-virtual-appliances](https://support.sourcefire.com/sections/1/sub_sections/51#5-2-virtual-appliances).

## Installing the Firepower Sensor OVA File

Install the Firepower Sensor OVA on a UCS E-Series Blade, using a hypervisor, such as VMWare VSphere.

### Installing Firepower Sensor on a UCS E-Series Blade

This section describes how to install the Firepower Sensor on a Unified Computing System (UCS) E-Series Blade that is installed on Cisco ISR 4000 Series Integrated Services Routers:

- 1 Install the UCS E-Series card.
- 2 Verify that the card is running by using the **show platform** command.
- 3 Configure the Cisco Integrated Management Controller (CIMC) port.

The CIMC GUI is a web-based management interface for E-Series Servers. You can launch the CIMC GUI to manage the server from any remote host that meets the following minimum requirements:

  - Java 1.6 or later
  - HTTP or HTTPS-enabled
  - Adobe Flash Player 10 or later

The CIMC runs on the port that is named management. The following example shows how to bootstrap the management port with an IP address:

```
ucse subslot 1/0
  imc access-port dedicated
  imc ip-address 10.66.152.158 255.255.255.0
!
```

Connect to the CIMC through the browser by using the default login and password, which are admin and password, respectively. Based on the configuration example, the browser address is https://10.66.152.158.

- 4 Install ESXi.  
Download the ESXi image for your Cisco UCS E-Series Blade from <https://my.vmware.com/web/vmware/details?downloadGroup=CISCO-ESXI-5.1.0-GA-25SEP2012&productId=284>.
- 5 Install Firepower Sensor by using VMWare VSphere on the Cisco UCS E-Series blade.
- 6 Configure traffic redirect. For more information, see the section “Configuring Traffic Redirect on Cisco UCS E-Series Blade”.
- 7 Configure the VMWare vSwitch. The Virtual Machine Network Interface Card (VMNIC) mapping on ISR 4000 Series Routers is as follows:
  - VMNIC0—Mapped to UCS E-Series interface x/0/0 on the router backplane
  - VMNIC1—Mapped to UCS E-Series interface x/0/1 on the router backplane
  - VMNIC2—Mapped to UCS E-Series frontplane GigabitEthernet 2 interface.
  - VMNIC3—Mapped to UCS E-Series frontplane GigabitEthernet 3 interface.



---

**Note** VMNIC3 is only available on UCS E-Series 140D, 160Dm and 180D.

---

UCS E-Series 120S and 140S have 3 network adaptors and one management port. UCS E-Series 140D, 160Dm and 180D have 4 network adaptors.

# Configuring Traffic Redirect on Cisco UCS E-Series Blade

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **no ip address**
5. **no negotiation auto**
6. **switchport mode trunk**
7. **no mop enabled**
8. **no mop sysid**
9. **service instance** *service-instance-number ethernet*
10. **encapsulation dot1q** *vlan-id*
11. **rewrite ingress tag pop** {1 | 2} **symmetric**
12. **bridge domain** *bridge-ID*
13. **end**

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode.  • Enter your password if prompted.
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>interface</b> <i>type number</i>  <b>Example:</b> Router(config)# interface ucse 1/0/0	Configures an interface and enters interface configuration mode.
<b>Step 4</b>	<b>no ip address</b>  <b>Example:</b> Router(config-if)# no ip address	Removes an IP address or disables IP processing on an interface.
<b>Step 5</b>	<b>no negotiation auto</b>  <b>Example:</b> Router(config-if)# no negotiation auto	Disables advertisement of speed, duplex mode, and flow control on an interface.

	Command or Action	Purpose
<b>Step 6</b>	<b>switchport mode trunk</b>  <b>Example:</b> Router(config-if)# switchport mode trunk	Specifies a trunking VLAN Layer 2 interface.
<b>Step 7</b>	<b>no mop enabled</b>  <b>Example:</b> Router(config-if)# no mop enabled	Disables the Maintenance Operation Protocol (MOP) on an interface.
<b>Step 8</b>	<b>no mop sysid</b>  <b>Example:</b> Router(config-if)# no mop sysid	Disables the sending of periodic MOP system identification messages from an interface.
<b>Step 9</b>	<b>service instance <i>service-instance-number</i> ethernet</b>  <b>Example:</b> Router(config-if)# service instance 10 ethernet	Configures an Ethernet service instance on an interface and enters Ethernet service-instance configuration mode.
<b>Step 10</b>	<b>encapsulation dot1q <i>vlan-id</i></b>  <b>Example:</b> Router(config-if-srv)# encapsulation dot1q 10	Defines the matching criteria to map 802.1Q frames ingress on an interface to the appropriate service instance.
<b>Step 11</b>	<b>rewrite ingress tag pop {1   2} symmetric</b>  <b>Example:</b> Router(config-if-srv)# rewrite ingress tag pop 1 symmetric	Specifies the encapsulation adjustment to be performed on a frame ingressing a service instance.
<b>Step 12</b>	<b>bridge domain <i>bridge-ID</i></b>  <b>Example:</b> Router(config-if-srv)# bridge domain 10	Binds a service instance or a MAC tunnel to a bridge domain instance.
<b>Step 13</b>	<b>end</b>  <b>Example:</b> Router(config-if)# end	Exits Ethernet service-instance configuration mode and returns to privileged EXEC configuration mode.

## Bootstrapping the Firepower Sensor

You must configure the Firepower Sensor manually. Perform this task to configure a Firepower sensor to communicate with FireSIGHT. For more information, see <https://support.sourcefire.com/sections/10>.

A sensor running on a Cisco Unified Computing System (UCS) E-Series Blade is bootstrapped by logging into the console of the Firepower Sensor virtual machine through VSphere.

**Note**

Firepower Sensor must be installed and deployed before bootstrapping it.

**SUMMARY STEPS**

1. Provide the default username and password to login.
2. **configure network ipv4 manual** *ip-address network-mask default-gateway*
3. **configure network dns servers** *dns-server*
4. **configure network dns searchdomains** *domain-name*
5. **configure manager add** *dc-hostname registration-key*

**DETAILED STEPS**

	Command or Action	Purpose
<b>Step 1</b>	Provide the default username and password to login.	To configure the sensor, the default username and password are admin and Sourcefire, respectively. <ul style="list-style-type: none"> <li>• You must change the admin password after you login to the Firepower Sensor the first time.</li> </ul>
<b>Step 2</b>	<b>configure network ipv4 manual</b> <i>ip-address network-mask default-gateway</i>  <b>Example:</b> Device# configure network ipv4 manual 10.66.152.137 255.255.255.0 10.66.152.1	Configures network connectivity.
<b>Step 3</b>	<b>configure network dns servers</b> <i>dns-server</i>  <b>Example:</b> Device# configure network dns servers 192.10.26.10	Configures domain name system (DNS) servers.
<b>Step 4</b>	<b>configure network dns searchdomains</b> <i>domain-name</i>  <b>Example:</b> Device# configure network dns searchdomains cisco.com	Configures DNS search domains.
<b>Step 5</b>	<b>configure manager add</b> <i>dc-hostname registration-key</i>  <b>Example:</b> Device# configure manager sourcefire-dc.cisco.com cisco-sf	Associates the sensor with the FireSIGHT. <ul style="list-style-type: none"> <li>• The <i>registration key</i> is a string selected by the user that is later used to register the sensor with FireSIGHT.</li> </ul>



### Example

The following is sample output from the **show network** command that displays the configured network settings of the Firepower Sensor:

```
Device# show network
```

```
-----  
IPv4  
Configuration      : manual  
Address            : 10.66.152.137  
Netmask            : 255.255.255.0  
Gateway            : 10.66.152.1  
MAC Address        : 44:03:A7:43:05:AD  
Management port    : 8305  
-----  
IPv6  
Configuration      : disabled  
Management port    : 8305  
-----
```

The following is sample output from the **show dns** command that displays the configured DNS settings:

```
Device# show dns
```

```
search cisco.com  
nameserver 192.10.26.10
```

The following is sample output from the **show managers** command that displays the configured management settings:

```
Device# show managers
```

```
Host                : sourcefire-dc.cisco.com  
Registration Key    : cisco-sf  
Registration        : pending  
RPC Status          :
```

## Enabling IDS Inspection Globally

Based on your requirements, you can configure the Intrusion Detection System (IDS) inspection at a global level or at an interface level.

You cannot enable IDS inspection on dedicated management interfaces.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **utd**
4. **mode ids-global**
5. **ids redirect-interface** *interface interface-number*
6. **end**

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode.  <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>utd</b>  <b>Example:</b> Router(config)# utd	Enters unified threat defense configuration mode.
<b>Step 4</b>	<b>mode ids-global</b>  <b>Example:</b> Router(config-utd)# mode ids-global	Enables intrusion detection mode on all interfaces.
<b>Step 5</b>	<b>ids redirect-interface</b> <i>interface interface-number</i>  <b>Example:</b> Router(config-utd)# ids redirect-interface BDI 10	Configures IDS traffic redirect on an interface.
<b>Step 6</b>	<b>end</b>  <b>Example:</b> Router(config-utd)# end	Exits unified threat defense configuration mode and returns to privileged EXEC mode.

## Enabling IDS Inspection per Interface

Based on your requirements, you can configure the Intrusion Detection System (IDS) inspection at a global level or at an interface level.

You cannot enable IDS inspection on dedicated management interfaces.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **utd ids**
5. **exit**
6. Repeat Steps 3 to 5, on all interfaces that require IDS inspection. Do not configure inspection on management interfaces.
7. **utd**
8. **ids redirect interface** *type number*
9. **end**

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode.  <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>interface</b> <i>type number</i>  <b>Example:</b> Router(config)# interface gigabitethernet 0/1/1	Configures an interface and enters interface configuration mode.
<b>Step 4</b>	<b>utd ids</b>  <b>Example:</b> Router(config-if)# utd ids	Enables intrusion detection on an interface.
<b>Step 5</b>	<b>exit</b>  <b>Example:</b> Router(config-if)# exit	Exits interface configuration mode and returns to global configuration mode.
<b>Step 6</b>	Repeat Steps 3 to 5, on all interfaces that require IDS inspection. Do not configure inspection on management interfaces.	-
<b>Step 7</b>	<b>utd</b>  <b>Example:</b> Router(config)# utd	Enters unified threat defense configuration mode.

	Command or Action	Purpose
<b>Step 8</b>	<b>ids redirect interface</b> <i>type number</i>  <b>Example:</b> Router(config-utd)# ids redirect interface BDI 10	Configures IDS traffic redirect on an interface.
<b>Step 9</b>	<b>end</b>  <b>Example:</b> Router(config-utd)# end	Exits unified threat defense configuration mode and returns to privileged EXEC mode.

## Configuration Examples for Cisco Firepower Threat Defense on ISR

### Example: Configuring Traffic Redirect on Cisco UCS E-Series Blade

This example shows how to configure ingress and egress interfaces for traffic redirect:

```
Router# configure terminal
Router(config)# interface ucse 1/0/0
Router(config-if)# no ip address
Router(config-if)# no negotiation auto
Router(config-if)# switchport mode trunk
Router(config-if)# no mop enabled
Router(config-if)# no mop sysid
Router(config-if)# exit
Router(config)# interface ucse 1/0/1
Router(config-if)# no ip address
Router(config-if)# no negotiation auto
Router(config-if)# switchport mode trunk
Router(config-if)# no mop enabled
Router(config-if)# no mop sysid
Router(config-if)# service instance 10 ethernet
Router(config-if-srv)# encapsulation dot1q 10
Router(config-if-srv)# rewrite ingress tag pop 1 symmetric
Router(config-if-srv)# bridge domain 10
Router(config-if-srv)# exit
Router(config-if)# exit
Router(config)# interface BDI 10
Router(config-if)# no shutdown
Router(config-if)# ip address 10.1.1.1 255.255.255.0
Router(config-if-srv)# end
```

### Example: Bootstrapping the Firepower Sensor

The following example shows how to bootstrap the Firepower Threat Defense sensor:

```
Sourcefire3D login: admin
Password: Sourcefire
```

```

Last login: Tue Nov 12 11:15:03 UTC 2013 on tty1

Copyright 2001-2013, Sourcefire, Inc. All rights reserved. Sourcefire is
a registered trademark of Sourcefire, Inc. All other trademarks are
property of their respective owners.

Sourcefire Linux OS v5.2.0 (build 135)
Sourcefire Virtual Device 64bit v5.2.0 (build 838)

> configure password
Enter current password:
Enter new password:
Confirm new password:

> configure network ipv4 manual 10.66.152.137 255.255.255.0 10.66.152.1
Setting IPv4 network configuration.
ADDRCONF(NETDEV_UP): eth0: link is not ready
e1000: eth0: e1000_phy_read_status: Error reading PHY register
e1000: eth0: e1000_watchdog_task: NIC Link is Up
1000 Mbps Full Duplex, Flow Control: None
ADDRCONF(NETDEV_CHANGE): eth0: link becomes ready

Network settings changed.

> configure network dns servers 192.10.26.10

> configure network dns searchdomains cisco.com

configure manager add sourcefire-dc.cisco.com cisco-sf
Manager successfully configured.

```

## Example: Enabling IDS Inspection Globally

```

Router# configure terminal
Router(config)# utd
Router(config-utd)# mode ids-global
Router(config-utd)# ids redirect-interface BDI 10
Router(config-utd)# end

```

## Example: Enabling IDS Inspection per Interface

```

Device# configure terminal
Device(config)# interface gigabitethernet 0/1/1
Device(config-if)# utd ids
Device(config-if)# end

```

## Verifying and Monitoring IDS Inspection

Use the following commands to verify and monitor your Intrusion Detection System (IDS) deployment:

### SUMMARY STEPS

1. enable
2. debug platform condition feature utd controlplane
3. debug platform condition feature utd dataplane submode
4. show platform hardware qfp active utd {config | status [all] [clear] [drop] [general]}

## DETAILED STEPS

- Step 1**      **enable**  
Enables privileged EXEC mode.
- Enter your password if prompted.

**Example:**

```
Router> enable
```

- Step 2**      **debug platform condition feature utd controlplane**  
Enables the debugging of the IDS configuration and status information.

**Example:**

```
Router# debug platform condition feature utd controlplane
```

```
network RF:
  network-rf idb-sync-history events debugging is on
IOSXE Conditional Debug Configs:
```

```
Conditional Debug Global State: Stop
```

Feature	Type	Submode	Level
UTD	controlplane		info

```
IOSXE Packet Tracing Configs:
```

```
Packet Infra debugs:
```

Ip Address	Port

- Step 3**      **debug platform condition feature utd dataplane submode**  
Enables the debugging of IDS packet flow information.

**Example:**

```
Router# debug platform condition feature utd dataplane submode
```

```
network RF:
  network-rf idb-sync-history events debugging is on
IOSXE Conditional Debug Configs:
```

```
Conditional Debug Global State: Stop
```

Feature	Type	Submode	Level
UTD	controlplane		info
UTD	dataplane	fia proxy punt	info

```
IOSXE Packet Tracing Configs:
```

```
Packet Infra debugs:
```

Ip Address	Port

- Step 4**      **show platform hardware qfp active utd {config | status [all] [clear] [drop] [general]}**  
Displays information about the IDS inspection in the Cisco Quantum Flow Processor (QFP).

**Example:**

```
Router# show platform hardware qfp active utd config
```

```
Global flags: 0x40004
Num divert interfaces: 1
Divert UIDBs: 65521 0
FIB information
[0][0] 0x309e3c30
[0][1] 0x0
[1][0] 0x309e4040
[1][1] 0x0
```

## Additional References for Cisco Firepower Threat Defense for ISR

### Related Documents

Related Topic	Document Title
IOS commands	<a href="#">Cisco IOS Master Command List, All Releases</a>
Security commands	<ul style="list-style-type: none"> <li>• <a href="#">Cisco IOS Security Command Reference: Commands A to C</a></li> <li>• <a href="#">Cisco IOS Security Command Reference: Commands D to L</a></li> <li>• <a href="#">Cisco IOS Security Command Reference: Commands M to R</a></li> <li>• <a href="#">Cisco IOS Security Command Reference: Commands S to Z</a></li> </ul>
UCS E-Series Servers	<a href="http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/e/2-0/guide/b_2_0_Getting_Started_Guide.html">http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/e/2-0/guide/b_2_0_Getting_Started_Guide.html</a>

**Technical Assistance**

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<a href="http://www.cisco.com/support">http://www.cisco.com/support</a>

## Feature Information for Cisco Firepower Threat Defense for ISR

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to [www.cisco.com/go/cfn](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

**Table 1: Feature Information for Cisco Firepower Threat Defense for ISR**

Feature Name	Releases	Feature Information
Cisco Firepower Threat Defense for ISR	Cisco IOS XE Release 3.14S	<p>Cisco Firepower Threat Defense is a premier network security option. It provides a comprehensive suite of Security features such as firewall capabilities, monitoring, alerts, Intrusion Detection System (IDS) and Intrusion Prevention System (IPS).</p> <p>This feature is introduced on Cisco ISR 4000 Series Integrated Services Routers.</p> <p>The following command was introduced or modified: <b>debug platform condition feature utd controlplane, debug platform condition feature utd dataplane submode, ids, mode (utd), show platform hardware qfp active feature utd, service utd, utd, utd ids.</b></p>





## Snort IPS

The Snort IPS feature enables Intrusion Prevention System (IPS) or Intrusion Detection System (IDS) for branch offices on Cisco 4000 Series Integrated Services Routers and Cisco Cloud Services Router 1000v Series. This feature uses the open source Snort solution to enable IPS and IDS. The [Snort IPS](#) feature is available in Cisco IOS XE Release 3.16.1S, 3.17S, and later releases.



### Note

The Virtual Routing and Forwarding (VRF) feature is supported on Snort IPS configuration from Cisco IOS XE Denali Release 16.3.1 and later releases.

This module explains the feature and how it works.

- [Finding Feature Information](#), page 19
- [Restrictions for Snort IPS](#), page 20
- [Information About Snort IPS](#), page 20
- [How to Deploy Snort IPS](#), page 25
- [Configuration Examples for Snort IPS](#), page 38
- [Examples for Displaying Active Signatures](#), page 44
- [Verifying the Integrated Snort IPS Configuration](#), page 45
- [Deploying Snort IPS Using Cisco Prime CLI Templates](#), page 52
- [Troubleshooting Snort IPS](#), page 53
- [Additional References for Snort IPS](#), page 59
- [Feature Information for Snort IPS](#), page 60

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to [www.cisco.com/go/cfn](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

## Restrictions for Snort IPS

The following restrictions apply to the Snort IPS feature:

- Incompatible with the Zone-Based Firewall SYN-cookie feature.
- Network Address Translation 64 (NAT64) is not supported.
- IOS syslog is rate limited and as a result, all alerts generated by Snort may not be visible via the IOS Syslog. However, you can view all Syslog messages if you export them to an external log server.

## Information About Snort IPS

### Snort IPS Overview

The Snort IPS feature enables Intrusion Prevention System (IPS) or Intrusion Detection System (IDS) for branch offices on Cisco 4000 Series Integrated Services Routers and Cisco Cloud Services Router 1000v Series. This feature uses the Snort sensor to provide IPS and IDS functionalities.

Snort is an open source network IPS that performs real-time traffic analysis and generates alerts when threats are detected on IP networks. It can also perform protocol analysis, content searching or matching, and detect a variety of attacks and probes, such as buffer overflows, stealth port scans, and so on. The Snort sensor runs as a virtual container service on Cisco 4000 Series Integrated Services Routers and Cisco Cloud Services Router 1000v Series.

The Snort IPS feature works in the network intrusion detection and prevention mode that provides IPS or IDS functionalities. In the network intrusion detection and prevention mode, Snort performs the following actions:

- Monitors network traffic and analyzes against a defined rule set.
- Performs attack classification.
- Invokes actions against matched rules.

Based on your requirements, you can enable Snort either in IPS or IDS mode. In IDS mode, Snort inspects the traffic and reports alerts, but does not take any action to prevent attacks. In IPS mode, in addition to intrusion detection, actions are taken to prevent attacks.

The Snort IPS monitors the traffic and reports events to an external log server or the IOS syslog. Enabling logging to the IOS syslog may impact performance due to the potential volume of log messages. External third-party monitoring tools, which supports Snort logs, can be used for log collection and analysis.

### Snort IPS Signature Package

The UTD OVA is included in the security license of the router. By default, the router is loaded only with community signature package. There are two types of subscriptions :

- Community Signature Package
- Subscriber-based Signature Package

The community signature package rule set offers limited coverage against threats. The subscriber-based signature package rule set offers the best protection against threats. It includes coverage in advance of exploits, and also provides the fastest access to the updated signatures in response to a security incident or the proactive discovery of a new threat. This subscription is fully supported by Cisco and the package will be updated on Cisco.com. You can download the subscriber-based signature package from the [Download Software](#) page.

If the user downloads the signature package manually from the download software page, then the user should ensure that the package has the same version as the Snort engine version. For example, if the Snort engine version is 2982, then the user should download the same version of the signature package. If there is a version mismatch, the signature package update will be rejected and it will fail.

**Note**

---

When the signature package is updated, the engine will be restarted and the traffic will be interrupted or bypass inspection for a short period depending on their data plane fail-open/fail-close configuration.

---

## Snort IPS Solution

The Snort IPS solution consists of the following entities:

- Snort sensor—Monitors the traffic to detect anomalies based on the configured security policies (that includes signatures, statistics, protocol analysis, and so on) and sends alert messages to the Alert/Reporting server. The Snort sensor is deployed as a virtual container service on the router.
- Signature store—Hosts the Cisco Signature packages that are updated periodically. These signature packages are downloaded to Snort sensors either periodically or on demand. Validated Signature packages are posted to Cisco.com. Based on the configuration, signature packages can be downloaded from Cisco.com or a local server.  
Signature packages must be manually downloaded from Cisco.com to the local server by using Cisco.com credentials before the Snort sensor can retrieve them.

The Snort container will perform a domain-name lookup to resolve the location for automatic signature updates from Cisco.com or the local server, if the URL is not specified as the IP address.

- Alert/Reporting server—Receives alert events from the Snort sensor. Alert events generated by the Snort sensor can either be sent to the IOS syslog or an external syslog server or to both IOS syslog and external syslog server. No external log servers are bundled with the Snort IPS solution.
- Management—Manages the Snort IPS solution. Management is configured using the IOS CLI. Snort Sensor cannot be accessed directly, and all configuration can only be done using the IOS CLI.

## Overview of Snort Virtual Service Interfaces

The Snort sensor runs as a service on routers. Service containers use virtualization technology to provide a hosting environment on Cisco devices for applications.

You can enable Snort traffic inspection either on a per interface basis or globally on all supported interfaces. The traffic to be inspected is diverted to the Snort sensor and injected back. In Intrusion Detection System

(IDS), identified threats are reported as log events and allowed. However, in Intrusion Prevention System (IPS), action is taken to prevent attacks along with log events.

The Snort sensor requires two VirtualPortGroup interfaces. The first VirtualPortGroup interface is used for management traffic and the second for data traffic between the forwarding plane and the Snort virtual container service. Guest IP addresses must be configured for these VirtualPortGroup interfaces. The IP subnet assigned to the management VirtualPortGroup interface should be able to communicate with the Signature server and Alert/Reporting server.

The IP subnet of the second VirtualPortGroup interface must not be routable on the customer network because the traffic on this interface is internal to the router. Exposing the internal subnet to the outside world is a security risk. We recommend the use of 192.0.2.0/30 IP address range for the second VirtualPortGroup subnet. The use of 192.0.2.0/24 subnet is defined in RFC 3330.

You can also use the management interface under the **virtual-service** command for management traffic. If you configure the management interface, you still need two VirtualPortGroup interfaces. However, do not configure the **guest ip address** for the first VirtualPortGroup interface.

You can assign the Snort virtual container service IP address on the same management network as the router on which the virtual service is running. This configuration helps if the syslog or update server is on the management network and is not accessible by any other interfaces.

## Virtual Service Resource Profile

The Snort IPS virtual service supports three resource profiles: Low, Medium, and High. These profiles indicate the CPU and memory resources required to run the virtual service. You can configure one of these resource profiles. The resource profile configuration is optional. If you do not configure a profile, the virtual service is activated with its default resource profile. This table provides the resource profiles details for Cisco 4000 Series ISR and Cisco Cloud Services Router 1000v Series.

Platform	Profile	Virtual Service Resource Requirements		Platform Requirements
		System CPU	Memory	
Cisco 4321 ISR	Default	50%	Min: 1GB (RAM) Min: 750MB (Disk/Flash)	Min: 8GB (RAM) Min: 8GB(Disk/Flash)
Cisco 4331 ISR	Low (Default)	25%	Min: 1GB (RAM) Min: 750MB (Disk/Flash)	Min: 8GB (RAM) Min: 8GB(Disk/Flash)
	Medium	50%	Min: 2GB (RAM) Min: 1GB (Disk/Flash)	Min: 8GB (RAM) Min: 8GB(Disk/Flash)
	High	75%	Min: 4GB (RAM) Min: 2GB (Disk/Flash)	Min: 8GB (RAM) Min: 8GB(Disk/Flash)

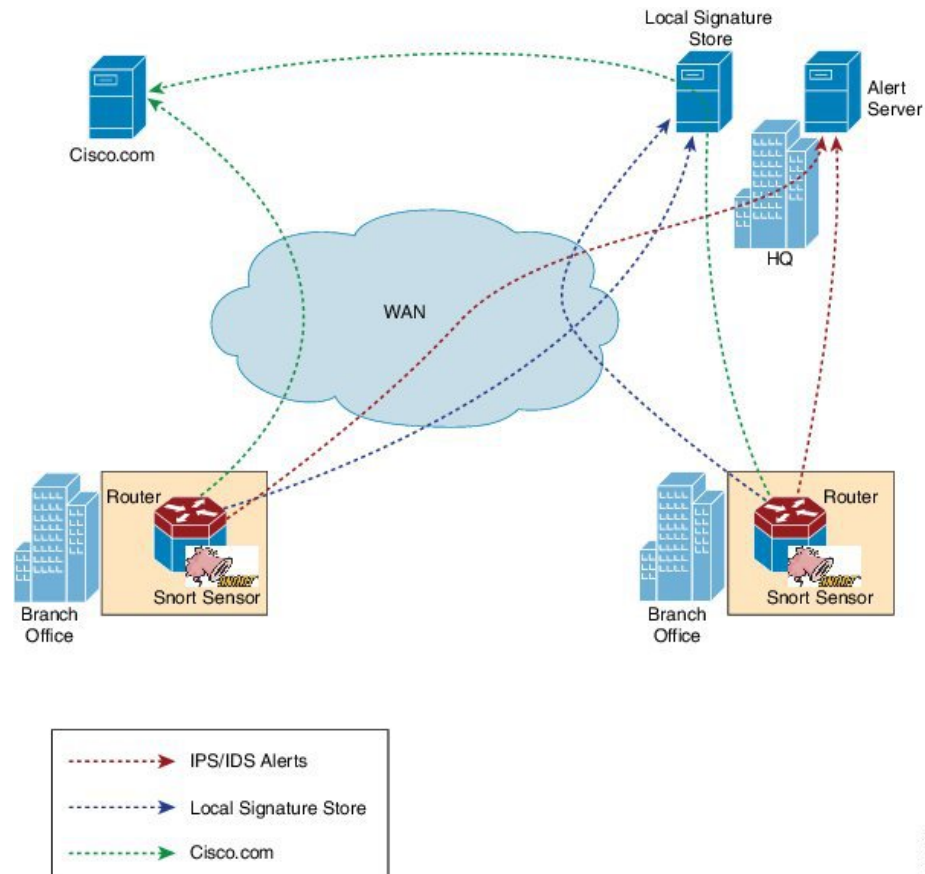
Platform	Profile	Virtual Service Resource Requirements		Platform Requirements
		System CPU	Memory	
Cisco 4351 ISR	Low (Default)	25%	Min: 1GB (RAM) Min: 750MB (Disk/Flash)	Min: 8GB (RAM) Min: 8GB(Disk/Flash)
	Medium	50%	Min: 2GB (RAM) Min: 1GB (Disk/Flash)	Min: 8GB (RAM) Min: 8GB(Disk/Flash)
	High	75%	Min: 4GB (RAM) Min: 2GB (Disk/Flash)	Min: 8GB (RAM) Min: 8GB(Disk/Flash)
Cisco 4431 ISR	Low (Default)	25%	Min: 1GB (RAM) Min: 750MB (Disk/Flash)	Min: 8GB (RAM) Min: 8GB(Disk/Flash)
	Medium	50%	Min: 2GB (RAM) Min: 1GB (Disk/Flash)	Min: 8GB (RAM) Min: 8GB(Disk/Flash)
	High	75%	Min: 4GB (RAM) Min: 2GB (Disk/Flash)	Min: 12GB (RAM) Min: 12GB(Disk/Flash)
Cisco 4451 ISR	Low (Default)	25%	Min: 1GB (RAM) Min: 750MB (Disk/Flash)	Min: 8GB (RAM) Min: 8GB(Disk/Flash)
	Medium	50%	Min: 2GB (RAM) Min: 1GB (Disk/Flash)	Min: 8GB (RAM) Min: 8GB(Disk/Flash)
	High	75%	Min: 4GB (RAM) Min: 2GB (Disk/Flash)	Min: 12GB (RAM) Min: 12GB(Disk/Flash)

Platform	Profile	Virtual Service Resource Requirements		Platform Requirements
		System CPU	Memory	
Cisco CSR 1000V	Low (Default)	25%	Min: 1GB (RAM) Min: 750MB (Disk/Flash)	Min: 8GB (RAM) Min: 8GB(Disk/Flash)
	Medium	50%	Min: 2GB (RAM) Min: 1GB (Disk/Flash)	Min: 8GB (RAM) Min: 8GB(Disk/Flash)
	High	75%	Min: 3GB (RAM) Min: 2GB (Disk/Flash)	Min: 12GB (RAM) Min: 12GB(Disk/Flash)

## Deploying Snort IPS

The figure illustrates a Snort IPS deployment scenario:

**Figure 2: Snort IPS Deployment Scenario**



The following steps describes the deployment of the Snort IPS solution:

- The Snort OVA file is copied to Cisco routers, installed, and then activated.
- Signature packages are downloaded either from Cisco.com or a configured local server to Cisco routers.
- Network intrusion detection or prevention functionality is configured.
- The Alert/Reporting server is configured to receive alerts from the Snort sensor.

## How to Deploy Snort IPS

To deploy Snort IPS on supported devices, perform the following tasks:

- 1 Provision the device.  
Identify the device to install the Snort IPS feature.

2 Obtain the license.

The Snort IPS functionality is available only in Security Packages which require a security license to enable the service. This feature is available in Cisco IOS XE Release 3.16.1S, 3.17S, and later releases.



**Note** Contact Cisco Support to obtain the license.

- 3 Install the Snort OVA file.
- 4 Configure VirtualPortGroup interfaces and virtual-service.
- 5 Activate the Snort virtual container service.
- 6 Configure Snort IPS or IDS mode and policy.
- 7 Configure the reporting of events to an external alert/log server or IOS syslog or both.
- 8 Configure the Signature update method.
- 9 Update the Signatures.
- 10 Enable IPS globally or on desired interfaces.

## Installing the Snort OVA File

An OVA file is an Open Virtualization Archive that contains a compressed, installable version of a virtual machine. The Snort IPS is available as a virtual container service. You must download this OVA file on to the router and use the **virtual-service install** CLI to install the service.

The service OVA file is not bundled with the Cisco IOS XE Release images that are installed on the router. However, the OVA files may be preinstalled in the flash of the router.

You must use a Cisco IOS XE image with security license. During the OVA file installation, the security license is checked and an error is reported if the license is not present.

### SUMMARY STEPS

1. **enable**
2. **virtual-service install name** *virtual-service-name* **package** *file-url* **media** *file-system*
3. **show virtual-service list**

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>virtual-service install name</b> <i>virtual-service-name</i> <b>package</b> <i>file-url</i> <b>media</b> <i>file-system</i>  <b>Example:</b> Device# virtual-service install name UTDIPS package harddisk:utd-ips-v102.ova media harddisk:	Installs an application on the virtual services container of a device. <ul style="list-style-type: none"> <li>• The length of the name is 20 characters. Hyphen (-) is not a valid character.</li> <li>• You must specify the complete path of the OVA package to be installed.</li> </ul>



	Command or Action	Purpose
		<b>Note</b> OVA installation works on both hard disk and bootflash, the preferred filesystem to install the OVA will be hard disk.
<b>Step 3</b>	<b>show virtual-service list</b>  <b>Example:</b> Device# show virtual-service list	Displays the status of the installation of all applications installed on the virtual service container.

## Configuring VirtualPortGroup Interfaces and Virtual Service

You must configure two VirtualPortGroup interfaces and configure guest IP addresses for both interfaces. However, if you configure a management interface by using the **vnic management GigabitEthernet0** command, then do not configure the guest IP address for the first VirtualPortGroup interface.

**Note**

The VirtualPortGroup interface for data traffic must use a private or nonroutable IP address. We recommend the use of 192.0.2.0/30 IP address range for this interface.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *VirtualPortGroup number*
4. **ip address** *ip-address mask*
5. **exit**
6. **interface** *type number*
7. **ip address** *ip-address mask*
8. **exit**
9. **virtual-service** *name*
10. **profile** *profile-name*
11. **vnic gateway** **VirtualPortGroup** *interface-number*
12. **guest ip address** *ip-address*
13. **exit**
14. **vnic gateway** **VirtualPortGroup** *interface-number*
15. **guest ip address** *ip-address*
16. **exit**
17. **vnic management** **GigabitEthernet0**
18. **guest ip address** *ip-address*
19. **exit**
20. **activate**
21. **end**

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode.  <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>interface</b> <i>VirtualPortGroup number</i>  <b>Example:</b> Device(config)# interface VirtualPortGroup 0	Configures an interface and enters interface configuration mode.  <ul style="list-style-type: none"> <li>• Configure a VirtualPortGroup interface. This interface is used for management traffic when the management interface GigabitEthernet0 is not used.</li> </ul>

	Command or Action	Purpose
<b>Step 4</b>	<b>ip address</b> <i>ip-address mask</i>  <b>Example:</b> Device(config-if)# ip address 10.1.1.1 255.255.255.252	Sets a primary IP address for an interface. This interface needs to be routable to the signature update server and external log server.
<b>Step 5</b>	<b>exit</b>  <b>Example:</b> Device(config-if)# exit	Exits interface configuration mode and returns to global configuration mode.
<b>Step 6</b>	<b>interface</b> <i>type number</i>  <b>Example:</b> Device(config)# interface VirtualPortGroup 1	Configures an interface and enters interface configuration mode. <ul style="list-style-type: none"> <li>• Configure a VirtualPortGroup interface.</li> <li>• This interface is used for data traffic.</li> </ul>
<b>Step 7</b>	<b>ip address</b> <i>ip-address mask</i>  <b>Example:</b> Device(config-if)# ip address 192.0.2.1 255.255.255.252	Sets a primary IP address for an interface. <ul style="list-style-type: none"> <li>• This IP address should not be routable to the outside network.</li> <li>• The IP address is assigned from the recommended 192.0.2.0/30 subnet.</li> </ul>
<b>Step 8</b>	<b>exit</b>  <b>Example:</b> Device(config-if)# exit	Exits interface configuration mode and returns to global configuration mode.
<b>Step 9</b>	<b>virtual-service</b> <i>name</i>  <b>Example:</b> Device(config)# virtual-service UTDIPS	Configures a virtual container service and enters virtual service configuration mode. <ul style="list-style-type: none"> <li>• The <i>name</i> argument is the logical name that is used to identify the virtual container service.</li> </ul>
<b>Step 10</b>	<b>profile</b> <i>profile-name</i>  <b>Example:</b> Device(config-virt-serv)#profile high	(Optional) Configures a resource profile. If you do not configure the resource profile, the virtual service is activated with its default resource profile. The options are: low, medium, and high.
<b>Step 11</b>	<b>vnic gateway</b> <b>VirtualPortGroup</b> <i>interface-number</i>  <b>Example:</b> Device(config-virt-serv)# vnic gateway VirtualPortGroup 0	Creates a virtual network interface card (vNIC) gateway interface for the virtual container service, maps the vNIC gateway interface to the virtual port group, and enters the virtual-service vNIC configuration mode. <ul style="list-style-type: none"> <li>• The interface referenced in this command must be the one configured in Step 3. This command maps the interface that is used for management purposes.</li> </ul>

	Command or Action	Purpose
<b>Step 12</b>	<b>guest ip address</b> <i>ip-address</i>  <b>Example:</b> Device(config-virt-serv-vnic)# guest ip address 10.1.1.2	(Optional) Configures a guest vNIC address for the vNIC gateway interface.  <ul style="list-style-type: none"> <li>• <b>Note</b> Configure this command only if the <b>vnic management gigabitethernet0</b> command specified in Step 17 is not configured.</li> </ul>
<b>Step 13</b>	<b>exit</b>  <b>Example:</b> Device(config-virt-serv-vnic)# exit	Exits virtual-service vNIC configuration mode and returns to virtual service configuration mode.
<b>Step 14</b>	<b>vnic gateway VirtualPortGroup</b> <i>interface-number</i>  <b>Example:</b> Device(config-virt-serv)# vnic gateway VirtualPortGroup 1	Creates a vNIC gateway interface for the virtual container service, maps the vNIC gateway interface to the virtual port group, and enters the virtual-service vNIC configuration mode.  <ul style="list-style-type: none"> <li>• This interface referenced in this command must be the one configured in Step 6. This command maps the interface in the virtual container service that is used by Snort for monitoring the user traffic.</li> </ul>
<b>Step 15</b>	<b>guest ip address</b> <i>ip-address</i>  <b>Example:</b> Device(config-virt-serv-vnic)# guest ip address 192.0.2.2	Configures a guest vNIC address for the vNIC gateway interface.
<b>Step 16</b>	<b>exit</b>  <b>Example:</b> Device(config-virt-serv-vnic)# exit	Exits virtual-service vNIC configuration mode and returns to virtual service configuration mode.
<b>Step 17</b>	<b>vnic management GigabitEthernet0</b>  <b>Example:</b> Device(config-virt-serv)# vnic management GigabitEthernet0	(Optional) Configures the GigabitEthernet interface as the vNIC management interface.  <ul style="list-style-type: none"> <li>• The management interface must either be a VirtualPortGroup interface or GigabitEthernet0 interface.</li> <li>• If you do not configure the <b>vnic management GigabitEthernet0</b> command, then you must configure the <b>guest ip address</b> command specified in Step 12.</li> </ul>
<b>Step 18</b>	<b>guest ip address</b> <i>ip-address</i>  <b>Example:</b> Device(config-virt-serv-vnic)# guest ip address 209.165.201.1	(Optional) Configures a guest vNIC address for the vNIC management interface and it must be in the same subnet as the management interface and GigabitEthernet0 configuration.
<b>Step 19</b>	<b>exit</b>  <b>Example:</b> Device(config-virt-serv-vnic)# exit	Exits virtual-service vNIC configuration mode and returns to virtual service configuration mode.

	Command or Action	Purpose
Step 20	<b>activate</b>  <b>Example:</b> Device(config-virt-serv) # activate	Activates an application installed in a virtual container service.
Step 21	<b>end</b>  <b>Example:</b> Device(config-virt-serv) # end	Exits virtual service configuration mode and returns to privileged EXEC mode.

## Configuring Snort IPS Globally

Based on your requirements, configure the Intrusion Prevention System (IPS) or Intrusion Detection System (IDS) inspection at a global level or at an interface. Perform this task to configure IPS globally on a device.

**Note**

The term global refers to Snort IPS running on all supported interfaces.

## SUMMARY STEPS

1. enable
2. configure terminal
3. utd threat-inspection whitelist
4. signature id *signature-id* [**comment** *description*]
5. exit
6. utd engine standard
7. logging {server *hostname* [syslog] | syslog}
8. threat-inspection
9. threat {detection | protection }
10. policy {balanced | connectivity | security}
11. whitelist
12. signature update occur-at {daily | monthly *day-of-month* | weekly *day-of-week*} *hour minute*
13. signature update server {cisco | url *url* } [**username** *username* [**password** *password*]]
14. logging level {alert | crit | debug | emerg | err | info | notice | warning}
15. exit
16. utd
17. redirect interface **virtualPortGroup** *interface-number*
18. all-interfaces
19. engine standard
20. fail close
21. exit
22. end

## DETAILED STEPS

	Command or Action	Purpose
Step 1	enable  <b>Example:</b> Device> enable	Enables privileged EXEC mode.  • Enter your password if prompted.
Step 2	configure terminal  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
Step 3	utd threat-inspection whitelist  <b>Example:</b> Device(config)# utd threat-inspection whitelist	(Optional) Enables the UTD whitelist configuration mode.
Step 4	signature id <i>signature-id</i> [ <b>comment</b> <i>description</i> ]	Configures signature IDs to be whitelisted.

	Command or Action	Purpose
	<b>Example:</b> <pre>Device(config-utd-whitelist)# signature id 24245 comment traffic from branchoffice1</pre>	<ul style="list-style-type: none"> <li>Signature IDs can be copied from alerts that needs to be suppressed.</li> <li>You can configure multiple signature IDs.</li> <li>Repeat this step for each signature ID that needs to be whitelisted.</li> </ul>
<b>Step 5</b>	<b>exit</b>  <b>Example:</b> <pre>Device(config-utd-whitelist)# exit</pre>	Exits UTD whitelist configuration mode and returns to global configuration mode.
<b>Step 6</b>	<b>utd engine standard</b>  <b>Example:</b> <pre>Device(config)# utd engine standard</pre>	Configures the unified threat defense (UTD) standard engine and enters UTD standard engine configuration mode.
<b>Step 7</b>	<b>logging {server hostname [syslog]   syslog}</b>  <b>Example:</b> <pre>Device(config-utd-eng-std)# logging server syslog.yourcompany.com</pre>	Enables the logging of emergency messages to a server.
<b>Step 8</b>	<b>threat-inspection</b>  <b>Example:</b> <pre>Device(config-utd-eng-std)# threat-inspection</pre>	Configures threat inspection for the Snort engine.
<b>Step 9</b>	<b>threat {detection   protection }</b>  <b>Example:</b> <pre>Device(config-utd-eng-std-insp)# threat protection</pre>	Configures threat detection or Intrusion Prevention System (IPS) as the operating mode for the Snort engine. <ul style="list-style-type: none"> <li>The default is <b>detection</b>.</li> <li>Configure the <b>detection</b> keyword to configure Intrusion Detection System (IDS).</li> </ul>
<b>Step 10</b>	<b>policy {balanced   connectivity   security}</b>  <b>Example:</b> <pre>Device(config-utd-eng-std-insp)# policy security</pre>	Configures the security policy for the Snort engine. <ul style="list-style-type: none"> <li>The default policy option is <b>balanced</b>.</li> </ul>
<b>Step 11</b>	<b>whitelist</b>  <b>Example:</b> <pre>Device(config-utd-eng-std-insp)# whitelist</pre>	(Optional) Enables whitelisting under the UTD engine.
<b>Step 12</b>	<b>signature update occur-at {daily   monthly day-of-month   weekly day-of-week} hour minute</b>  <b>Example:</b> <pre>Device(config-utd-eng-std-insp)# signature update occur-at daily 0 0</pre>	Configures the signature update interval parameters. This configuration will trigger the signature update to occur at midnight.

	Command or Action	Purpose
<b>Step 13</b>	<b>signature update server</b> {cisco   url url } [username username [password password]]  <b>Example:</b> Device(config-utd-eng-std-insp)# signature update server cisco username abcd password cisco123	Configures the signature update server parameters. You must specify the signature update parameters with the server details. If you use Cisco.com for signature updates, you must provide the username and password. If you use local server for signature updates, based on the server settings you can provide the username and password.
<b>Step 14</b>	<b>logging level</b> {alert   crit   debug   emerg   err   info   notice   warning}  <b>Example:</b> Device(config-utd-eng-std-insp)# logging level emerg	Enables the log level.
<b>Step 15</b>	<b>exit</b>  <b>Example:</b> Device(config-utd-eng-std-insp)# exit	Exits UTD standard engine configuration mode and returns to global configuration mode.
<b>Step 16</b>	<b>utd</b>  <b>Example:</b> Device(config)# utd	Enables unified threat defense (UTD) and enters UTD configuration mode.
<b>Step 17</b>	<b>redirect interface virtualPortGroup</b> interface-number  <b>Example:</b> Device(config-utd)# redirect interface virtualPortGroup 1	(Optional) Redirects to a VirtualPortGroup interface. This is the data traffic interface. If you do not configure this interface, it is auto-detected.
<b>Step 18</b>	<b>all-interfaces</b>  <b>Example:</b> Device(config-utd)# all-interfaces	Configures UTD on all Layer 3 interfaces of the device.
<b>Step 19</b>	<b>engine standard</b>  <b>Example:</b> Device(config-utd)# engine standard	Configures the Snort-based unified threat defense (UTD) engine and enters standard engine configuration mode.
<b>Step 20</b>	<b>fail close</b>  <b>Example:</b> Device(config-engine-std)# fail close	(Optional) Defines the action when there is a UTD engine failure. Default option is fail-open. Fail-close option drops all the IPS/IDS traffic when there is an UTD engine failure. Fail-open option allows all the IPS/IDS traffic when there is an UTD engine failure.
<b>Step 21</b>	<b>exit</b>  <b>Example:</b> Device(config-eng-std)# exit	Exits standard engine configuration mode and returns to global configuration mode.



	Command or Action	Purpose
Step 22	<b>end</b>  <b>Example:</b> Device (config-utd) # end	Exits UTD configuration mode and returns to global configuration mode.

## Configuring Snort IDS Inspection Globally

Based on your requirements, configure either Intrusion Prevention System (IPS) or Intrusion Detection System (IDS) inspection at a global level or at an interface level. Perform this task to configure IDS on a per-interface basis.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **utd enable**
5. **exit**
6. Repeat Steps 3 to 5, on all interfaces that require inspection.
7. **utd threat-inspection whitelist**
8. **signature id** *signature-id* [**comment** *description*]
9. **exit**
10. **utd engine standard**
11. **logging** {**server** *hostname* [**syslog**] | **syslog**}
12. **threat-inspection**
13. **threat** {**detection** | **protection** }
14. **policy** {**balanced** | **connectivity** | **security**}
15. **whitelist**
16. **signature update occur-at** {**daily** | **monthly** *day-of-month* | **weekly** *day-of-week*} *hour minute*
17. **signature update server** {**cisco** | **url** *url*} [**username** *username* [**password** *password*]]
18. **logging level** {**alert** | **crit** | **debug** | **emerg** | **err** | **info** | **notice** | **warning**}
19. **exit**
20. **utd**
21. **redirect interface** **virtualPortGroup** *interface-number*
22. **engine standard**
23. **exit**
24. **end**

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode.  <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>interface <i>type number</i></b>  <b>Example:</b> Device(config)# interface gigabitethernet 0/0/0	Configures an interface and enters interface configuration mode.
<b>Step 4</b>	<b>utd enable</b>  <b>Example:</b> Device(config-if)# utd enable	Enables unified threat defense (UTD).
<b>Step 5</b>	<b>exit</b>  <b>Example:</b> Device(config-if)# exit	Exits interface configuration mode and returns to global configuration mode.
<b>Step 6</b>	Repeat Steps 3 to 5, on all interfaces that require inspection.	—
<b>Step 7</b>	<b>utd threat-inspection whitelist</b>  <b>Example:</b> Device(config)# utd threat-inspection whitelist	(Optional) Enables the UTD whitelist configuration mode.
<b>Step 8</b>	<b>signature id <i>signature-id</i> [<i>comment description</i>]</b>  <b>Example:</b> Device(config-utd-whitelist)# signature id 24245 comment traffic from branchoffice1	Configures signature IDs to be whitelisted.  <ul style="list-style-type: none"> <li>• Signature IDs can be copied from alerts that need to be suppressed.</li> <li>• You can configure multiple signature IDs.</li> <li>• Repeat this step for each signature ID that needs to be whitelisted.</li> </ul>
<b>Step 9</b>	<b>exit</b>  <b>Example:</b> Device(config-utd-whitelist)# exit	Exits UTD whitelist configuration mode and returns to global configuration mode.

	Command or Action	Purpose
<b>Step 10</b>	<b>utd engine standard</b>  <b>Example:</b> Device(config)# utd engine standard	Configures the unified threat defense (UTD) standard engine and enters UTD standard engine configuration mode.
<b>Step 11</b>	<b>logging {server hostname [syslog]   syslog}</b>  <b>Example:</b> Device(config-utd-eng-std)# logging syslog	Enables the logging of critical messages to the IOSd syslog.
<b>Step 12</b>	<b>threat-inspection</b>  <b>Example:</b> Device(config-utd-eng-std)# threat-inspection	Configures threat inspection for the Snort engine.
<b>Step 13</b>	<b>threat {detection   protection}</b>  <b>Example:</b> Device(config-utd-eng-std-insp)# threat detection	Configures threat protection or Intrusion Detection System (IDS) as the operating mode for the Snort sensor.  <ul style="list-style-type: none"> <li>Configure the <b>protection</b> keyword to configure Intrusion Prevention System (IPS).</li> </ul>
<b>Step 14</b>	<b>policy {balanced   connectivity   security}</b>  <b>Example:</b> Device(config-utd-eng-std-insp)# policy balanced	Configures the security policy for the Snort sensor.
<b>Step 15</b>	<b>whitelist</b>  <b>Example:</b> Device(config-utd-eng-std-insp)# whitelist	(Optional) Enables whitelisting of traffic.
<b>Step 16</b>	<b>signature update occur-at {daily   monthly day-of-month   weekly day-of-week} hour minute</b>  <b>Example:</b> Device(config-utd-eng-std-insp)# signature update occur-at daily 0 0	Configures the signature update interval parameters. This configuration will trigger the signature update to occur at midnight.
<b>Step 17</b>	<b>signature update server {cisco   url url} [username username [password password]]</b>  <b>Example:</b> Device(config-utd-eng-std-insp)# signature update server cisco username abcd password cisco123	Configures the signature update server parameters. You must specify the signature update parameters with the server details. If you use Cisco.com for signature updates, you must provide the username and password. If you use local server for signature updates, based on the server settings you can provide the username and password.
<b>Step 18</b>	<b>logging level {alert   crit   debug   emerg   err   info   notice   warning}</b>  <b>Example:</b> Device(config-utd-eng-std-insp)# logging level crit	Enables the log level.

	Command or Action	Purpose
<b>Step 19</b>	<b>exit</b>  <b>Example:</b> Device(config-utd-eng-std-insp)# exit	Exits UTD standard engine configuration mode and returns to global configuration mode.
<b>Step 20</b>	<b>utd</b>  <b>Example:</b> Device(config)# utd	Enables unified threat defense (UTD) and enters UTD configuration mode.
<b>Step 21</b>	<b>redirect interface virtualPortGroup interface-number</b>  <b>Example:</b> Device(config-utd)# redirect interface virtualPortGroup 1	(Optional) Redirects to a VirtualPortGroup interface. This is the data traffic interface. If you do not configure this interface, it is auto-detected.
<b>Step 22</b>	<b>engine standard</b>  <b>Example:</b> Device(config-utd)# engine standard	Configures the Snort-based unified threat defense (UTD) engine and enters standard engine configuration mode.
<b>Step 23</b>	<b>exit</b>  <b>Example:</b> Device(config-eng-std)# exit	Exits standard engine configuration mode and returns to global configuration mode.
<b>Step 24</b>	<b>end</b>  <b>Example:</b> Device(config-utd)# end	Exits UTD configuration mode and returns to global configuration mode.

## Displaying the List of Active Signatures

Active signatures are the ones that prompt Snort IDS/IPS to take action against threats. If the traffic matches with any of the active signatures, Snort container triggers alert in the IDS mode, and drops the traffic in the IPS mode.

The **utd threat-inspection signature active-list write-to bootflash: file name** command provides a list of active signatures and a summary of the total number of active signatures, drop signatures, and alert signatures.

## Configuration Examples for Snort IPS

### Example: Configuring VirtualPortGroup Interfaces and Virtual Service

```
Device# configure terminal
Device(config)# interface VirtualPortGroup 0
```

```

Device(config-if)# ip address 10.1.1.1 255.255.255.252
Device(config-if)# exit
Device(config)# interface VirtualPortGroup 1
Device(config-if)# ip address 192.0.2.1 255.255.255.252
Device(config-if)# exit
Device(config)# virtual-service UTDIPS
Device(config-virt-serv)# vnic gateway VirtualPortGroup 0
Device(config-virt-serv-vnic)# exit
Device(config-virt-serv)# vnic gateway VirtualPortGroup 1
Device(config-virt-serv-vnic)# guest ip address 192.0.2.2
Device(config-virt-serv-vnic)# exit
Device(config-virt-serv)# vnic management GigabitEthernet0
Device(config-virt-serv-vnic)# guest ip address 209.165.201.1
Device(config-virt-serv-vnic)# exit
Device(config-virt-serv)# activate
Device(config-virt-serv-vnic)# end

```

## Example: Configuring a Different Resource Profile

```

Device# configure terminal
Device(config)# virtual-service UTDIPS
Device(config-virt-serv)# no activate
*Sep 7 13:57:04.660 IST: %VIRT_SERVICE-5-ACTIVATION_STATE: Successfully
deactivated virtual service UTDIPS
Device(config-virt-serv)# profile medium
Device(config-virt-serv)# activate
Device(config-virt-serv)# end

```

## Example: Configuring UTD with Operation Mode IPS and Policy Security

The following example shows how to configure the UTD with operation mode IPS and policy security:

```

Device# configure terminal
Device(config)# utd engine standard
Device(config-utd-eng-std)# threat-inspection
Device(config-utd-eng-std-insp)# threat protection
Device(config-utd-eng-std-insp)# policy security
Device(config-utd-eng-std)# end
Device#

```

## Example: Configuring Snort IPS Globally

The following example shows how to configure Intrusion Prevention System (IPS) globally on a device:

```

Device# configure terminal
Device(config)# utd engine standard
Device(config-utd-eng-std)# threat-inspection
Device(config-utd-eng-std-insp)# threat protection
Device(config-utd-eng-std-insp)# policy security
Device(config-utd-eng-std)# exit
Device(config)# utd
Device(config-utd)# all-interfaces
Device(config-utd)# engine standard
Device(config-utd-whitelist)# end
Device#

```

## Example: Configuring Snort IPS Inspection per Interface

The following example shows how to configure Snort Intrusion Detection System (IDS) on a per-interface basis:

```
Device# configure terminal
Device(config)# utd engine standard
Device(config-utd-eng-std)# threat-inspection
Device(config-utd-eng-std-insp)# threat detection
Device(config-utd-eng-std-insp)# policy security
Device(config-utd-eng-std)# exit
Device(config)# utd
Device(config-utd)# engine standard
Device(config-eng-std)# exit
Device(config)# interface gigabitethernet 0/0/0
Device(config-if)# utd enable
Device(config-if)# exit
```

## Example: Configuring UTD with VRF on both Inbound and Outbound Interface

```
Device# configure terminal
Device(config)# vrf definition VRF1
Device(config-vrf)# rd 100:1
Device(config-vrf)# route-target export 100:1
Device(config-vrf)# route-target import 100:1
Device(config-vrf)# route-target import 100:2
!
Device(config-vrf)# address-family ipv4
Device(config-vrf-af)# exit
!
Device(config-vrf)# address-family ipv6
Device(config-vrf-af)# exit
!
Device(config-vrf-af)# vrf definition VRF2
Device(config-vrf)# rd 100:2
Device(config-vrf)# route-target export 100:2
Device(config-vrf)# route-target import 100:2
Device(config-vrf)# route-target import 100:1
!
Device(config-vrf)# address-family ipv4
Device(config-vrf-af)# exit
!
Device(config-vrf)# address-family ipv6
Device(config-vrf-af)# exit
!
Device(config-vrf)# interface VirtualPortGroup0
Device(config-if)# ip address 192.0.0.1 255.255.255.0
Device(config-if)# no mop enabled
Device(config-if)# no mop sysid
!
Device(config-if)# interface VirtualPortGroup1
Device(config-if)# ip address 192.0.0.1 255.255.255.0
Device(config-if)# no mop enabled
Device(config-if)# no mop sysid
!
Device(config-if)# interface GigabitEthernet0/0/2
Device(config-if)# vrf forwarding VRF1
Device(config-if-vrf)# ip address 192.1.1.5 255.255.255.0
Device(config-if-vrf)# ipv6 address A000::1/64
!
Device(config-if)# interface GigabitEthernet0/0/3
Device(config-if)# vrf forwarding VRF2
Device(config-if-vrf)# ip address 192.1.1.5 255.255.255.0
Device(config-if-vrf)# ipv6 address B000::1/64
!
Device(config-if-vrf)# router bgp 100
```

```

Device(config-if-vrf)# bgp log-neighbor-changes
!
Device(config-vrf)# address-family ipv4 vrf VRF1
Device(config-vrf-af)# redistribute connected
Device(config-vrf-af)# redistribute static
Device(config-vrf-af)# exit
!
Device(config-vrf)# address-family ipv6 vrf VRF1
Device(config-vrf-af)# redistribute connected
Device(config-vrf-af)# redistribute static
Device(config-vrf-af)# exit
!
Device(config-vrf)# address-family ipv4 vrf VRF2
Device(config-vrf-af)# redistribute connected
Device(config-vrf-af)# redistribute static
Device(config-vrf-af)# exit
!
Device(config-vrf)# address-family ipv6 vrf VRF2
Device(config-vrf-af)# redistribute connected
Device(config-vrf-af)# redistribute static
Device(config-vrf-af)# exit
!
Device(config)# utd
Device(config-utd)# all-interfaces
Device(config-utd)# engine standard
!
Device(config)# utd engine standard
Device(config-utd-eng-std)# logging syslog
Device(config-utd-eng-std)# threat-inspection
Device(config-utd-engstd-insp)# threat protection
Device(config-utd-engstd-insp)# policy security

!
Device(config)# virtual-service utd
Device(config-virt-serv)# profile low
Device(config-virt-serv)# vnic gateway VirtualPortGroup0
Device(config-virt-serv-vnic)# guest ip address 47.0.0.2
Device(config-virt-serv-vnic)# exit
Device(config-virt-serv)# vnic gateway VirtualPortGroup1
Device(config-virt-serv-vnic)# guest ip address 48.0.0.2
Device(config-virt-serv-vnic)# exit
Device(config-virt-serv)# activate

UTD Snort IPS Drop Log
=====
2016/06/13-14:32:09.524475 IST [**] [Instance_ID: 1] [**] Drop [**]
[1:30561:1] BLACKLIST DNS request for known malware
domain domai.ddns2.biz - Win.Trojan.Beebone [**]
[Classification: A Network Trojan was Detected]
[Priority: 1] [VRF_ID: 2] {UDP} 11.1.1.10:58016 -> 21.1.1.10:53

```

## Example: Configuring Logging IOS Syslog

The following example shows how to configure logging IOS syslog with the log levels on a device:

```

Device# configure terminal
Device(config)# utd engine standard
Device(config-utd-eng-std)# logging syslog
Device(config-utd-eng-std)# threat-inspection
Device(config-utd-engstd-insp)# logging level debug
Device(config-utd-eng-std-insp)# end
Device#

```

## Example: Configuring Logging to Centralized Log Server

The following example shows how to configure logging to a centralized log server:

```
Device# configure terminal
Device(config)# utd engine standard
Device(config-utd-eng-std-insp)# logging server syslog.yourcompany.com
Device(config-utd-eng-std)# threat-inspection
Device(config-utd-eng-std-insp)# logging level info
Device(config-utd-eng-std-insp)# end
Device#
```

## Example: Configuring Signature Update from a Cisco Server

The following example shows how to configure the signature update from a Cisco server :

```
Device# configure terminal
Device(config)# utd engine standard
Device(config-utd-eng-std)# threat-inspection
Device(config-utd-eng-std-insp)# signature update server cisco username CCOuser password
passwd123
Device(config-utd-eng-std-insp)# end
Device#
```



### Note

Ensure that the DNS is configured to download signatures from the Cisco server.

## Example: Configuring Signature Update from a Local Server

The following example shows how to configure the signature update from a local server:

```
Device# configure terminal
Device(config)# utd engine standard
Device(config-utd-eng-std)# threat-inspection
Device(config-utd-eng-std-insp)# signature update server url http://192.168.1.2/sig-1.pkg
Device(config-utd-eng-std-insp)# end
Device#
```

## Example: Configuring Automatic Signature Update

The following example shows how to configure the automatic signature update on a server:

```
Device# configure terminal
Device(config)# utd engine standard
Device(config-utd-eng-std)# threat-inspection
Device(config-utd-eng-std-insp)# signature update occur-at daily 0 0
Device(config-utd-eng-std-insp)# signature update server cisco username abcd password
cisco123
Device(config-utd-eng-std-insp)# end
Device#
```



### Note

When the signature update is not in detail, you can get the signature update from the server.



## Example: Performing Manual Signature Update

The following example shows how to perform a manual signature update:

```
Device# utd threat-inspection signature update
```

It takes the existing server configuration to download from or the explicit server information configured with it.

These commands perform a manual signature update with the below settings:

```
Device#show utd engine standard threat-inspection signature update status
```

```
Current Signature package version: 2982.2.s
Current Signature package name: UTD-STD-SIGNATURE-2982-2-S.pkg
Previous Signature package version: 29.0.c
Last update status: Successful
Last failure Reason: None
Last successful update method: Auto
Last successful update server: cisco
Last successful update time: Fri Jul 1 05:15:43 2016 PDT
Last successful update speed: 2656201 bytes in 42 secs
Last failed update method: Manual
Last failed update server: cisco
Last failed update time: Fri Jul 1 16:51:23 2016 IST
Last attempted update method: Auto
Last attempted update server: cisco
Last attempted update time: Fri Jul 1 05:15:43 2016 PDT
Total num of updates successful: 1
Num of attempts successful: 1
Num of attempts failed: 5
Total num of attempts: 6
Next update scheduled at: None
Current Status: Idle
```

```
Device# utd threat-inspection signature update server cisco username ccouser password
passwd123
Device# utd threat-inspection signature update server url http://192.168.1.2/sig-1.pkg
```

## Example: Configuring Signature Whitelist

The following example shows how to configure signature whitelist:

```
Device# configure terminal
Device(config)# utd threat-inspection whitelist
Device(config-utd-whitelist)# signature id 23456 comment "traffic from client x"
Device(config-utd-whitelist)# exit
Device(config)# utd engine standard
Device(config-utd-eng-std)# whitelist
Device(config-utd-eng-std)# end
Device#
```



### Note

After the whitelist signature ID is configured, Snort will allow the flow to pass through the device without any alerts and drops.

# Examples for Displaying Active Signatures

## Example: Displaying Active Signatures List With Balanced Policy

```
Device# utd threat-inspection signature active-list write-to bootflash:siglist_balanced
Device# more bootflash:siglist_balanced
=====
Signature Package Version: 2982.1.s
Signature Ruleset: Balanced
Total no. of active signatures: 7884
Total no. of drop signatures: 7389
Total no. of alert signatures: 495

For more details of each signature please go to www.snort.org/rule_docs to lookup
=====

List of Active Signatures:
-----
<snipped>
```

## Example: Displaying Active Signatures List With Security Policy

```
Device# utd threat-inspection signature active-list write-to bootflash:siglist_security
Device# more bootflash:siglist_security
=====
Signature Package Version: 2982.1.s
Signature Ruleset: Security
Total no. of active signatures: 11224
Total no. of drop signatures: 10220
Total no. of alert signatures: 1004

For more details of each signature please go to www.snort.org/rule_docs to lookup
=====

List of Active Signatures:
-----
<snipped>
```

## Example: Displaying Active Signatures List With Connectivity Policy

```
Device# utd threat-inspection signature active-list write-to bootflash:siglist_connectivity
Device# more bootflash:siglist_connectivity
=====
Signature Package Version: 2982.1.s
Signature Ruleset: Connectivity
Total no. of active signatures: 581
Total no. of drop signatures: 452
Total no. of alert signatures: 129

For more details of each signature please go to www.snort.org/rule_docs to lookup
=====

List of Active Signatures:
-----
<snipped>
```

# Verifying the Integrated Snort IPS Configuration

Use the following commands to troubleshoot your configuration.

## SUMMARY STEPS

1. enable
2. show virtual-service list
3. show virtual-service detail
4. show service-insertion type utd service-node-group
5. show service-insertion type utd service-context
6. show utd engine standard config
7. show utd engine standard status
8. show utd engine standard threat-inspection signature update status
9. show utd engine standard logging events
10. clear utd engine standard logging events
11. show platform hardware qfp active feature utd config
12. show platform software utd global
13. show platform software utd interfaces
14. show platform hardware qfp active feature utd stats
15. show utd engine standard statistics daq all

## DETAILED STEPS

### Step 1 enable

**Example:**

```
Device> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

### Step 2 show virtual-service list

Displays the status of the installation of all applications on the virtual service container.

**Example:**

```
Device# show virtual-service list
```

Virtual Service List:

Name	Status	Package Name
UTDIPS	Activated	utdsnort.1_0_1_SV2982_XE_16_3.20160701_131509.ova

### Step 3 show virtual-service detail

Displays the resources used by applications installed in the virtual services container of a device.

### Example:

Device# **show virtual-service detail**

```
Device#show virtual-service detail
Virtual service UTDIPS detail
State           : Activated
Owner           : IOSd
Package information
  Name          : utdsnort.1_0_1_SV2982_XE_16_3.20160701_131509.ova
  Path          : bootflash:/utdsnort.1_0_1_SV2982_XE_16_3.20160701_131509.ova
  Application
    Name        : UTD-Snort-Feature
    Installed version : 1.0.1_SV2982_XE_16_3
    Description  : Unified Threat Defense
  Signing
    Key type    : Cisco development key
    Method      : SHA-1
  Licensing
    Name       : Not Available
    Version    : Not Available
```

Detailed guest status

Process	Status	Uptime	# of restarts
climgr	UP	0Y 0W 0D 0: 0:35	1
logger	UP	0Y 0W 0D 0: 0: 4	0
snort_1	UP	0Y 0W 0D 0: 0: 4	0

Network stats:

```
eth0: RX packets:43, TX packets:6
eth1: RX packets:8, TX packets:6
```

Coredump file(s): lost+found

Activated profile name: None

Resource reservation

```
Disk       : 736 MB
Memory     : 1024 MB
CPU        : 25% system CPU
```

Attached devices

Type	Name	Alias
NIC	ieobc_1	ieobc
NIC	dp_1_0	net2
NIC	dp_1_1	net3
NIC	mgmt_1	mgmt
Disk	_rootfs	
Disk	/opt/var	
Disk	/opt/var/c	
Serial/shell		serial0
Serial/aux		serial1
Serial/Syslog		serial2
Serial/Trace		serial3
Watchdog	watchdog-2	

Network interfaces

MAC address	Attached to interface
54:0E:00:0B:0C:02	ieobc_1
A4:4C:11:9E:13:8D	VirtualPortGroup0
A4:4C:11:9E:13:8C	VirtualPortGroup1
A4:4C:11:9E:13:8B	mgmt_1

Guest interface

```

---
Interface: eth2
ip address: 48.0.0.2/24
Interface: eth1
ip address: 47.0.0.2/24
---

Guest routes
---

```

Address/Mask	Next Hop	Intf.
0.0.0.0/0	48.0.0.1	eth2
0.0.0.0/0	47.0.0.1	eth1

```

---

Resource admission (without profile) : passed
Disk space      : 710MB
Memory         : 1024MB
CPU            : 25% system CPU
VCPUs          : Not specified

```

#### Step 4 **show service-insertion type utd service-node-group**

Displays the status of service node groups.

##### Example:

```
Device# show service-insertion type utd service-node-group
```

```

Service Node Group name : utd_sng_1
Service Context : utd/1
Member Service Node count : 1

Service Node (SN) : 30.30.30.2
Auto discovered : No
SN belongs to SNG : utd_sng_1
Current status of SN : Alive
Time current status was reached : Tue Jul 26 11:57:48 2016

Cluster protocol VPATH version : 1
Cluster protocol incarnation number : 1
Cluster protocol last sent sequence number : 1469514497
Cluster protocol last received sequence number: 1464
Cluster protocol last received ack number : 1469514496

```

#### Step 5 **show service-insertion type utd service-context**

Displays the AppNav and service node views.

##### Example:

```
Device# show service-insertion type utd service-context
```

```

Service Context : utd/1
Cluster protocol VPATH version : 1
Time service context was enabled : Tue Jul 26 11:57:47 2016
Current FSM state : Operational
Time FSM entered current state : Tue Jul 26 11:57:58 2016
Last FSM state : Converging
Time FSM entered last state : Tue Jul 26 11:57:47 2016
Cluster operational state : Operational

Stable AppNav controller View:
30.30.30.1

Stable SN View:

```

```
30.30.30.2
```

```
Current AppNav Controller View:
30.30.30.1
```

```
Current SN View:
30.30.30.2
```

**Step 6**      **show utd engine standard config**  
Displays the unified threat defense (UTD) configuration.

**Example:**

```
Device# show utd engine standard config
```

```
UTD Engine Standard Configuration:
  Operation Mode : Intrusion Prevention
  Policy         : Security

Signature Update:
  Server        : cisco
  User Name     : ccouser
  Password      : YEX^SH\fhdOeEGaOBiQAicOVLgaVGf
  Occurs-at     : weekly ; Days:0 ; Hour: 23; Minute: 50

Logging:
  Server        : IOS Syslog; 10.104.49.223
  Level         : debug

Whitelist Signature IDs:
28878
```

**Step 7**      **show utd engine standard status**  
Displays the status of the utd engine.

**Example:**

```
Device# show utd engine standard status
Engine version : 1.0.1_SV2982_XE_16_3
```

```
Profile : High
System memory :
Usage : 8.00 %
Status : Green
Number of engines : 4
```

```
Engine Running CFT flows Health Reason
=====
Engine(#1): Yes 0 Green None
Engine(#2): Yes 0 Green None
Engine(#3): Yes 0 Green None
Engine(#4): Yes 0 Green None
=====
```

```
Overall system status: Green
```

```
Signature update status:
=====
Current Signature package version: 29.0.c
Current Signature package name: default
Previous Signature package version: None
Last update status: None
Last failure Reason: None
```

**Step 8**      **show utd engine standard threat-inspection signature update status**

Displays the status of the signature update process.

**Example:**

```
Device# show utd engine standard threat-inspection signature update status
```

```
Current Signature package version: 2982.2.s
Current Signature package name: UTD-STD-SIGNATURE-2982-2-S.pkg
Previous Signature package version: 29.0.c
Last update status: Successful
Last failure Reason: None
Last successful update method: Auto
Last successful update server: cisco
Last successful update time: Fri Jul 1 05:15:43 2016 PDT
Last successful update speed: 2656201 bytes in 42 secs
Last failed update method: Manual
Last failed update server: cisco
Last failed update time: Fri Jul 1 16:51:23 2016 IST
Last attempted update method: Auto
Last attempted update server: cisco
Last attempted update time: Fri Jul 1 05:15:43 2016 PDT
Total num of updates successful: 1
Num of attempts successful: 1
Num of attempts failed: 5
Total num of attempts: 6
Next update scheduled at: None
Current Status: Idle
```

**Step 9 show utd engine standard logging events**

Displays log events from the Snort sensor.

**Example:**

```
Device# show utd engine standard logging events
```

```
2016/06/13-14:32:09.524475 IST [**] [Instance_ID: 1] [**] Drop [**] [1:30561:1]
BLACKLIST DNS request for known malware domain domai.ddns2.biz -
Win.Trojan.Beebone [**] [Classification: A Network Trojan was Detected] [Priority: 1]
[VRF_ID: 2] {UDP} 11.1.1.10:58016 -> 21.1.1.10:53
2016/06/13-14:32:21.524988 IST [**] [Instance_ID: 1] [**] Drop [**] [1:30561:1]
BLACKLIST DNS request for known malware domain domai.ddns2.biz -
Win.Trojan.Beebone [**] [Classification: A Network Trojan was Detected] [Priority: 1]
[VRF_ID: 2] {UDP} a000:0:0:0:0:0:10:59964 -> b000:0:0:0:0:0:10:53
```

**Step 10 clear utd engine standard logging events**

**Example:**

```
Device# clear utd engine standard logging events
```

Clears logged events from the Snort sensor.

**Step 11 show platform hardware qfp active feature utd config**

Displays information about the health of the service node.

**Example:**

```
Device# show platform hardware qfp active feature utd config
```

```
Global configuration
NAT64: disabled
SN threads: 12
CFT inst_id 0 feat id 1 fo id 1 chunk id 8
Context Id: 0, Name: Base Security Ctx
Ctx Flags: (0x60000)
Engine: Standard
```

```

SN Redirect Mode : Fail-open, Divert
Threat-inspection: Enabled, Mode: IDS
Domain Filtering : Not Enabled
URL Filtering : Not Enabled
SN Health: Green

```

**Step 12**     **show platform software utd global**  
 Displays the interfaces on which UTD is enabled.

**Example:**

```

Device# show platform software utd global

UTD Global state
Engine           : Standard
Global Inspection : Enabled
Operational Mode  : Intrusion Prevention
Fail Policy       : Fail-open
Container technology : LXC
Redirect interface : VirtualPortGroup1
UTD interfaces
All dataplane interfaces

```

**Step 13**     **show platform software utd interfaces**  
 Displays the information about all interfaces.

**Example:**

```

Device# show platform software utd interfaces

UTD interfaces
All dataplane interfaces

```

**Step 14**     **show platform hardware qfp active feature utd stats**  
 Displays dataplane UTD statistics.

**Example:**

```

Device# show platform hardware qfp active feature utd stats

Security Context:      Id:0      Name: Base Security Ctx

Summary Statistics:
Pkts entered policy feature          pkt      228
                                      byt      31083

Drop Statistics:

Service Node flagged flow for dropping          48
Service Node not healthy                      62

General Statistics:

Non Diverted Pkts to/from divert interface          32913
Inspection skipped - UTD policy not applicable      48892
Policy already inspected                          2226
Pkts Skipped - L2 adjacency glean                   1
Pkts Skipped - For Us                              67
Pkts Skipped - New pkt from RP                     102
Response Packet Seen                               891
Feature memory allocations                         891
Feature memory free                                891
Feature Object Delete                              863

```



```

Service Node Statistics:
SN Health: Green
SN down                                     85
SN health green                             47
SN health red                               13

Diversion Statistics
redirect                                   2226
encaps                                    2226
decaps                                    2298
reinject                                  2250
decaps: Could not locate flow               72
Redirect failed, SN unhealthy                62
Service Node requested flow bypass drop     48

```

**Step 15**    **show utd engine standard statistics daq all**  
 Displays serviceplane data acquisition (DAQ) statistics.

**Example:**

```
Device# show utd engine standard statistics daq all
```

```

IOS-XE DAQ Counters(Engine #1):
-----
Frames received                :0
Bytes received                 :0
RX frames released             :0
Packets after vPath decap      :0
Bytes after vPath decap        :0
Packets before vPath decap     :0
Bytes before vPath decap       :0
Frames transmitted             :0
Bytes transmitted              :0

Memory allocation              :2
Memory free                    :0
Merged packet buffer allocation :0
Merged packet buffer free      :0

VPL buffer allocation          :0
VPL buffer free                :0
VPL buffer expand              :0
VPL buffer merge               :0
VPL buffer split               :0
VPL packet incomplete          :0

VPL API error                  :0
CFT API error                  :0
Internal error                 :0
External error                 :0
Memory error                   :0
Timer error                    :0

Kernel frames received         :0
Kernel frames dropped          :0

FO cached via timer            :0
Cached fo used                 :0
Cached fo freed                :0
FO not found                   :0
CFT full packets               :0

```

```
VPL Stats(Engine #1):
-----
```

## Deploying Snort IPS Using Cisco Prime CLI Templates

You can use the Cisco Prime CLI templates to provision the Snort IPS deployment. The Cisco Prime CLI templates make provisioning Snort IPS deployment simple. To use the Cisco Prime CLI templates to provision the Snort IPS deployment, perform these steps:

- 
- Step 1** Download the Prime templates from the [Software Download](#) page, corresponding to the IOS XE version running on your system.
- Step 2** Unzip the file, if it is a zipped version.
- Step 3** From Prime, choose **Configuration > Templates > Features and Technologies**, select **CLI Templates**.
- Step 4** Click **Import**.
- Step 5** Select the folder where you want to import the templates to and click **Select Templates** and choose the templates that you just downloaded to import.
- The following Snort IPS CLI templates are available:
- **Copy OVA to Device**—Use this template to copy the Snort IPS OVA file to the router file system.
  - **Delete OVA**—Use this template to delete the copied Snort IPS OVA file from the router file system.
  - **Dynamic NAT**—Use this template if Dynamic NAT (Network Address Translation) is configured in your environment and an Access List is used to select the NAT translation that needs to be modified for Snort IPS Management Interface IP.
  - **Dynamic NAT Cleanup**—Use this template to delete the NAT configuration for Snort IPS.
  - **Dynamic PAT**—Use this template if Dynamic PAT (Port Address Translation) is configured in your environment and an Access List is used to select the PAT translation that needs to be modified for Snort IPS Management Interface IP.
  - **Dynamic PAT Cleanup**—Use this template to delete the PAT configuration for Snort IPS.
  - **IP Unnumbered**—Use this template to configure Snort IPS and required Virtual-Service for IP Unnumbered deployment.
  - **IP Unnumbered Cleanup**—Use this template to delete the configured Snort IPS Management interface with IP Unnumbered.
  - **Management Interface**—Use this template if you would like to use System Management interface (e.g. GigabitEthernet0) to route Snort IPS Management traffic.
  - **Management Interface Cleanup**—Use this template to delete the configured System Management interface (e.g. GigabitEthernet0) to route the Snort IPS Management traffic.
  - **Static NAT**—Use this template to configure Snort IPS and required Virtual-Service for existing Static NAT deployment.
  - **Static NAT Cleanup**—Use this template to delete the configured Snort IPS in a Static NAT deployment.
  - **Upgrade OVA**—Use this template to upgrade Snort IPS OVA file.

# Troubleshooting Snort IPS

## Traffic is not Diverted

**Problem** Traffic is not diverted.

**Possible Cause** Virtual-service may not be activated.

**Solution** Check whether the virtual-service is activated by using the **show virtual-service list** command. The following is sample output from the command:

```
Device# show virtual-service list
```

```
Virtual Service List:
```

```
Name Status Package Name
```

```
-----  
snort Activated utdsnort.1_0_1_SV2982_XE_16_3.20160701_131509.ova
```

**Possible Cause** Unified threat defense (UTD) may not be enabled for specified interface or interfaces.

**Solution** Use the **show platform software utd global** command to verify if UTD is enabled for the interface:

```
Device# show platform software utd global
```

```
UTD Global state  
Engine : Standard  
Global Inspection : Disabled  
Operational Mode : Intrusion Prevention  
Fail Policy : Fail-open  
Container technology : LXC  
Redirect interface : VirtualPortGroup1  
UTD interfaces  
GigabitEthernet0/0/0
```

**Possible Cause** The service node may not be working properly.

**Solution** Use the **show platform hardware qfp active feature utd config** command to verify if the health of the service node is green:

```
Device# show platform hardware qfp active feature utd config
```

```
Global configuration  
NAT64: disabled  
SN threads: 12  
CFT inst id 0 feat id 0 fo id 0 chunk id 4  
Context Id: 0, Name: Base Security Ctx  
Ctx Flags: (0x60000)  
Engine: Standard  
SN Redirect Mode : Fail-open, Divert  
Threat-inspection: Enabled, Mode: IDS  
Domain Filtering : Not Enabled  
URL Filtering : Not Enabled  
SN Health: Green
```

**Possible Cause** The Snort process may not be activated.

**Solution** Use the **show virtual-service detail** command to verify if the Snort process is up and running:

Device# **show virtual-service detail**

Virtual service UTDIPS detail

```

State          : Activated
Owner          : IOSd
Package information
  Name         : utdsnort.1_0_1_SV2982_XE_16_3.20160701_131509.ova
  Path         : bootflash:/utdsnort.1_0_1_SV2982_XE_16_3.20160701_131509.ova
Application
  Name         : UTD-Snort-Feature
  Installed version : 1.0.1_SV2982_XE_16_3
  Description    : Unified Threat Defense
Signing
  Key type     : Cisco development key
  Method       : SHA-1
Licensing
  Name         : Not Available
  Version      : Not Available

```

Detailed guest status

Process	Status	Uptime	# of restarts
climgr	UP	0Y 0W 0D 0: 0:35	1
logger	UP	0Y 0W 0D 0: 0: 4	0
snort_1	UP	0Y 0W 0D 0: 0: 4	0

Network stats:

```

eth0: RX packets:43, TX packets:6
eth1: RX packets:8, TX packets:6

```

Coredump file(s): lost+found

Activated profile name: None

Resource reservation

```

Disk       : 736 MB
Memory     : 1024 MB
CPU        : 25% system CPU

```

Attached devices

Type	Name	Alias
NIC	ieobc_1	ieobc
NIC	dp_1_0	net2
NIC	dp_1_1	net3
NIC	mgmt_1	mgmt
Disk	_rootfs	
Disk	/opt/var	
Disk	/opt/var/c	
Serial/shell		serial0
Serial/aux		serial1
Serial/Syslog		serial2
Serial/Trace		serial3
Watchdog	watchdog-2	

Network interfaces

MAC address	Attached to interface
54:0E:00:0B:0C:02	ieobc_1
A4:4C:11:9E:13:8D	VirtualPortGroup0
A4:4C:11:9E:13:8C	VirtualPortGroup1
A4:4C:11:9E:13:8B	mgmt_1

Guest interface

---

```

Interface: eth2
ip address: 48.0.0.2/24
Interface: eth1
ip address: 47.0.0.2/24

```

```

---
Guest routes
---
Address/Mask                Next Hop                Intf.
-----
0.0.0.0/0                   48.0.0.1                eth2
0.0.0.0/0                   47.0.0.1                eth1
---

Resource admission (without profile) : passed
Disk space      : 710MB
Memory         : 1024MB
CPU            : 25% system CPU
VCPUs          : Not specified

```

**Possible Cause** The AppNav tunnel may not be activated.

**Solution** Use the **show service-insertion type utd service-node-group** and **show service-insertion type utd service-context** commands to verify if the AppNav tunnel is activated.

**Solution** The following is sample output from the **show service-insertion type utd service-node-group** command:

```

Device# show service-insertion type utd service-node-group

Service Node Group name : utd_sng_1
Service Context : utd/1
Member Service Node count : 1

Service Node (SN) : 30.30.30.2
Auto discovered : No
SN belongs to SNG : utd_sng_1
Current status of SN : Alive
Time current status was reached : Tue Jul 26 11:57:48 2016

Cluster protocol VPATH version : 1
Cluster protocol incarnation number : 1
Cluster protocol last sent sequence number : 1469514497
Cluster protocol last received sequence number: 1464
Cluster protocol last received ack number : 1469514496

```

**Solution** The following is sample output from the **show service-insertion type utd service-context** command:

```

Device# show service-insertion type utd service-context

Service Context : utd/1
Cluster protocol VPATH version : 1
Time service context was enabled : Tue Jul 26 11:57:47 2016
Current FSM state : Operational
Time FSM entered current state : Tue Jul 26 11:57:58 2016
Last FSM state : Converging
Time FSM entered last state : Tue Jul 26 11:57:47 2016
Cluster operational state : Operational

Stable AppNav controller View:
30.30.30.1

Stable SN View:
30.30.30.2

Current AppNav Controller View:

```

```
30.30.30.1
```

```
Current SN View:
30.30.30.2
```

**Possible Cause** Check data plane UTD statistics for the status of the traffic. If the traffic is not diverted, the number of packets diverted and rejected will be zero. If the numbers are nonzero, then traffic diversion is happening, and the Snort sensor is resending packets back to the dataplane.

**Solution** Use the `show platform hardware qfp active feature utd stats` commands to verify the status of the traffic.

```
Device# show platform hardware qfp active feature utd stats
```

```
Security Context:      Id:0      Name: Base Security Ctx
```

```
Summary Statistics:
```

Active Connections		29
TCP Connections Created		712910
UDP Connections Created		80
Pkts entered policy feature	pkt	3537977
	byt	273232057
Pkts entered divert feature	pkt	3229148
	byt	249344841
Pkts slow path	pkt	712990
	byt	45391747
Pkts Diverted	pkt	3224752
	byt	249103697
Pkts Re-injected	pkt	3224746
	byt	249103373

```
....
```

## Signature Update is not Working

**Problem** Signature update from Cisco Borderless Software Distribution (BSD) server is not working.

**Possible Cause** Signature update may have failed due to various reasons. Check for the reason for the last failure to update the signatures.

**Solution** Use the `show utd engine standard threat-inspection signature update status` command to display the reason for the last failure to update the signatures:

```
Device# show utd engine standard threat-inspection signature update status
```

```
Current Signature package version: 2982.1.s
Current Signature package name: UTD-STD-SIGNATURE-2982-1-S.pkg
Previous Signature package version: 2982.2.s
Last update status: Successful
Last failure Reason: System error-fail to process username & password combination.
Last successful update method: Manual
Last successful update server: http://10.104.52.159/protected/UTD-STD-SIGNATURE-2982-1-S.pkg
Last successful update time: Fri Jul 8 14:21:49 2016 IST
Last successful update speed: 2631532 bytes in 6 secs
Last failed update method: Auto
Last failed update server: cisco
Last failed update time: Fri Jul 8 14:13:02 2016 IST
Last attempted update method: Manual
Last attempted update server: http://10.104.52.159/protected/UTD-STD-SIGNATURE-2982-1-S.pkg
Last attempted update time: Fri Jul 8 14:21:49 2016 IST
Total num of updates successful: 17
```

```
Num of attempts successful: 22
Num of attempts failed: 12
Total num of attempts: 34
Next update scheduled at: None
Current Status: Idle
```

**Possible Cause** Domain Name System (DNS) is not configured correctly.

**Solution** Use the **show running-config | i name-server** command to display the name server details:

```
Device# show run | i name-server
```

```
ip name-server 10.104.49.223
```

**Possible Cause** System error—Failed to process the username and password combination.

**Solution** Ensure that you have provided the correct credentials for signature package download.

## Signature Update from the Local Server is not Working

**Problem** Signature update from the local server not working.

**Possible Cause** Last failure Reason: Invalid scheme—only HTTP/HTTPS supported.

**Solution** Ensure that you have provided the HTTP or secure HTTP (HTTPS) as the local download method.

**Possible Cause** Last failure Reason: Name or service not known.

**Solution** Ensure that the hostname or IP address provided for the local server is correct.

**Possible Cause** Last failure Reason: Credentials not supplied.

**Solution** Ensure that you have provided the credentials for local HTTP/HTTPS server.

**Possible Cause** Last failure Reason: File not found.

**Solution** Ensure that the signature file name or URL that you have provided is correct.

**Possible Cause** Last failure Reason: Download corrupted.

**Solution**

- Verify whether the retry signature update is corrupted as the previous signature download.
- Ensure that the correct signature package is available.

## Logging to IOSd Syslog is not Working

**Problem** Logging to IOSd syslog is not working.

**Possible Cause** Logging to syslog may not be configured in the unified threat defense (UTD) configuration.

**Solution** Use the **show utd engine standard config** command to display the UTD configuration and to ensure that logging to syslog is configured.

```
Device# show utd engine standard config
```

```
UTD Engine Standard Configuration:
```

```
Operation Mode : Intrusion Prevention
Policy         : Security
```

```
Signature Update:
```

```
Server       : cisco
User Name    : ccouser
Password     : YEX^SH\fhdoeEGaOBIQAicOVLgaVGf
Occurs-at    : weekly ; Days:0 ; Hour: 23; Minute: 50
```

```
Logging:
```

```
Server       : IOS Syslog; 10.104.49.223
Level        : debug
```

```
Whitelist Signature IDs:
```

```
28878
```

**Solution** Use the following **show utd engine standard logging events** command to display the event logs for the UTD engine.

```
Device# show utd engine standard logging events
```

```
2016/06/13-14:32:09.524475 IST [**] [Instance_ID: 1] [**] Drop [**] [1:30561:1]
BLACKLIST DNS request for known malware domain domai.ddns2.biz -
Win.Trojan.Beebone [**] [Classification: A Network Trojan was Detected]
[Priority: 1] [VRF_ID: 2] {UDP} 11.1.1.10:58016 -> 21.1.1.10:53
2016/06/13-14:32:21.524988 IST [**] [Instance_ID: 1] [**] Drop [**] [1:30561:1]
BLACKLIST DNS request for known malware domain domai.ddns2.biz -
Win.Trojan.Beebone [**] [Classification: A Network Trojan was Detected] [Priority: 1]
[VRF_ID: 2] {UDP} a000:0:0:0:0:0:10:59964 -> b000:0:0:0:0:0:10:53
```

## Logging to an External Server is not Working

**Problem** Logging to an external server is not working.

**Possible Cause** Syslog may not be running on the external server.

**Solution** Verify whether syslog server is running on the external server. Configure the following command on the external server to view its status:

```
ps -eaf | grep syslog
```

```
root 2073 1 0 Apr12 ? 00:00:02 syslogd -r -m
```



**Possible Cause** Connectivity between unified threat defense (UTD) Linux Container (LXC) and external server may be lost.

**Solution** Verify the connectivity from the management interface to the external syslog server.

## UTD Conditional Debugging

The Snort IPS feature supports UTD conditional debugging. For details on how to configure conditional debugging, see the following URL:

[http://www.cisco.com/c/en/us/td/docs/routers/asr1000/troubleshooting/guide/Tblshooting-xe-3s-asr-1000-book.html#task\\_AC969BB06B414DCBBDEF7ADD29EF8131](http://www.cisco.com/c/en/us/td/docs/routers/asr1000/troubleshooting/guide/Tblshooting-xe-3s-asr-1000-book.html#task_AC969BB06B414DCBBDEF7ADD29EF8131)

## Additional References for Snort IPS

### Related Documents

Related Topic	Document Title
IOS commands	<a href="#">Cisco IOS Master Command List, All Releases</a>
Security commands	<ul style="list-style-type: none"><li>• <a href="#">Cisco IOS Security Command Reference: Commands A to C</a></li><li>• <a href="#">Cisco IOS Security Command Reference: Commands D to L</a></li><li>• <a href="#">Cisco IOS Security Command Reference: Commands M to R</a></li><li>• <a href="#">Cisco IOS Security Command Reference: Commands S to Z</a></li></ul>

**Technical Assistance**

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<a href="http://www.cisco.com/support">http://www.cisco.com/support</a>

## Feature Information for Snort IPS

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to [www.cisco.com/go/cfn](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

**Table 2: Feature Information for Snort IPS**

Feature Name	Releases	Feature Information
Snort IPS	Cisco IOS XE 3.16.1S, 3.17S and later releases	The Snort IPS feature, enables Intrusion Prevention System (IPS) and Intrusion Detection System (IDS) for branch offices on Cisco IOS XE-based platforms. This feature uses the open source Snort solution to enable IPS and IDS.
VRF support on Snort IPS	Cisco IOS XE Denali 16.3.1	Supports Virtual Fragmentation Reassembly (VFR) on Snort IPS configuration.
Snort IPS support on Cisco Cloud Services Router 1000v Series	Cisco IOS XE Denali 16.3.1	Cisco Cloud Services Router 1000v Series supports Snot IPS.
UTD Snort IPS Enhancements for 16.4 Release	Cisco IOS XE Everest 16.4.1	The UTD Snort IPS enhancements for 16.4 release adds a feature for displaying the list of active signatures.