# 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, and Intrusion Detection System (IDS)

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



# 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:

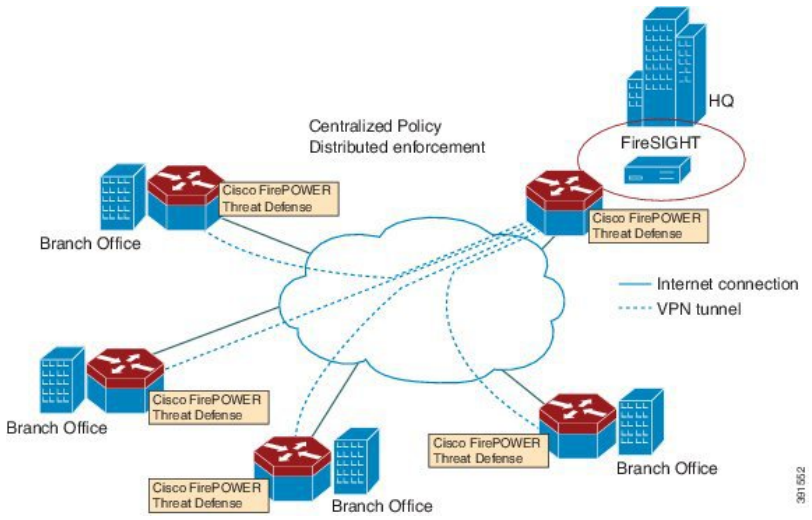
- Cisco FireSIGHT—A centralized policy and reporting entity that can run anywhere in the network. This can be the Cisco FireSIGHT appliance or a virtual installation on a server class machine.
- Virtual Firepower sensor—Security entities that implement policies, and send events and statistics back to 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 Interconnet 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.

**Note** To monitor VLAN traffic in your virtual environment, set the VLAN ID of the promiscuous port to 4095.

# 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           Technology-package
              Current       Type           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.

## 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 |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** *type number*<br>**Example:**<br>`Router(config)# interface ucse 1/0/0` | Configures an interface and enters interface configuration mode. |
| **Step 4** | **no ip address**<br>**Example:**<br>`Router(config-if)# no ip address` | Removes an IP address or disables IP processing on an interface. |
| **Step 5** | **no negotiation auto**<br>**Example:**<br>`Router(config-if)# no negotiation auto` | Disables advertisement of speed, duplex mode, and flow control on an interface. |
| **Step 6** | **switchport mode trunk**<br>**Example:**<br>`Router(config-if)# switchport mode trunk` | Specifies a trunking VLAN Layer 2 interface. |
| **Step 7** | **no mop enabled**<br>**Example:**<br>`Router(config-if)# no mop enabled` | Disables the Maintenance Operation Protocol (MOP) on an interface. |
| **Step 8** | **no mop sysid**<br>**Example:**<br>`Router(config-if)# no mop sysid` | Disables the sending of periodic MOP system identification messages from an interface. |
| **Step 9** | **service instance** *service-instance-number ethernet*<br>**Example:**<br>`Router(config-if)# service instance 10 ethernet` | Configures an Ethernet service instance on an interface and enters Ethernet service-instance configuration mode. |
| **Step 10** | **encapsulation dot1q** *vlan-id*<br>**Example:**<br>`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. |
| **Step 11** | **rewrite ingress tag pop** {**1** \| **2**} **symmetric**<br>**Example:** | Specifies the encapsulation adjustment to be performed on a frame ingressing a service instance. |

| | Command or Action | Purpose |
|---|---|---|
| | `Router(config-if-srv)# rewrite ingress tag pop 1 symmetric` | |
| **Step 12** | **bridge domain** *bridge-ID*<br>**Example:**<br>`Router(config-if-srv)# bridge domain 10` | Binds a service instance or a MAC tunnel to a bridge domain instance. |
| **Step 13** | **end**<br>**Example:**<br>`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 |
|---|---|---|
| **Step 1** | Provide the default username and password to login. | To configure the sensor, the default username and password are admin and Sourcefire, respectively.<br>• You must change the admin password after you login to the Firepower Sensor the first time. |
| **Step 2** | **configure network ipv4 manual** *ip-address network-mask default-gateway*<br>**Example:**<br>`Device# configure network ipv4 manual 10.66.152.137 255.255.255.0 10.66.152.1` | Configures network connectivity. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 3** | **configure network dns servers** *dns-server*<br>**Example:**<br>`Device# configure network dns servers 192.10.26.10` | Configures domain name system (DNS) servers. |
| **Step 4** | **configure network dns searchdomains** *domain-name*<br>**Example:**<br>`Device# configure network dns searchdomains cisco.com` | Configures DNS search domains. |
| **Step 5** | **configure manager add** *dc-hostname registration-key*<br>**Example:**<br>`Device# configure manager sourcefire-dc.cisco.com cisco-sf` | Associates the sensor with the FireSIGHT.<br>• The *registration key* is a string selected by the user that is later used to register the sensor with FireSIGHT. |

### 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 enable**
4. **utd engine advanced**
5. **threat detection**
6. **exit**
7. **utd**
8. **all-interfaces**
9. **engine advanced**
10. **fail close**
11. **rate** *pps-rate*
12. **redirect-interface** *interface interface-number*
13. **end**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **utd enable**<br>**Example:**<br>`Router(config)# utd enable` | Enters unified threat defense configuration mode. |
| **Step 4** | **utd engine advanced**<br>**Example:**<br>`Router(config)# utd engine advanced` | Configures the unified threat defense (UTD) advanced engine and enters UTD advanced engine configuration.<br>mode. |
| **Step 5** | **threat detection**<br>**Example:**<br>`Router(config-utd-eng-adv)# threat detection` | Configures threat detection or Intrusion Prevention System (IPS) as the operating mode for the Snort engine. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 6** | **exit**<br>**Example:**<br>`Router(config-if)# exit` | Exits interface configuration mode and returns to global configuration mode. |
| **Step 7** | **utd**<br>**Example:**<br>`Router(config)# utd` | Enters unified threat defense configuration mode. |
| **Step 8** | **all-interfaces**<br>**Example:**<br>`Router(config-utd)# all-interfaces` | Configures UTD on all Layer 3 interfaces of the device |
| **Step 9** | **engine advanced**<br>**Example:**<br>`outer(config-utd)# engine advanced` | Configures the unified threat defense (UTD) advanced engine and enters UTD advaned engine configuration. |
| **Step 10** | **fail close**<br>**Example:**<br>`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. |
| **Step 11** | **rate** *pps-rate*<br>**Example:**<br>`Device(config-engine-std)# rate 2000000` | (Optional) Specify the pps rate to push to the sensor. The range is from 1000 to 4000000. |
| **Step 12** | **redirect-interface** *interface interface-number*<br>**Example:**<br>`Router(config-utd)# redirect-interface BDI 10` | Configures IDS traffic redirect on an interface. |
| **Step 13** | **end**<br>**Example:**<br>`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 enable**
5. **exit**
6. Repeat Steps 3 to 5, on all interfaces that require IDS inspection. Do not configure inspection on management interfaces.
7. **utd engine advanced**
8. **threat detection**
9. **utd**
10. **engine advanced**
11. **fail close**
12. **rate** *range*
13. **redirect interface** *type number*
14. **end**

**DETAILED STEPS**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** *type number*<br>**Example:**<br>`Router(config)# interface gigabitethernet 0/1/1` | Configures an interface and enters interface configuration mode. |
| **Step 4** | **utd enable**<br>**Example:**<br>`Router(config-if)# utd enable` | Enables intrusion detection on an interface. |
| **Step 5** | **exit**<br>**Example:**<br>`Router(config-if)# exit` | Exits interface configuration mode and returns to global configuration mode. |
| **Step 6** | Repeat Steps 3 to 5, on all interfaces that require IDS inspection. Do not configure inspection on management interfaces. | - |
| **Step 7** | **utd engine advanced**<br>**Example:**<br>`Router(config)# utd engine advanced` | Configures the unified threat defense (UTD) advanced engine and enters UTD advanced engine configuration.<br>mode. |
| **Step 8** | **threat detection**<br>**Example:** | Configures threat detection or Intrusion Prevention System (IPS) as the operating mode for the Snort engine. |

| | Command or Action | Purpose |
|---|---|---|
| | `Router(config-utd-eng-adv)# threat detection` | |
| **Step 9** | **utd**<br>**Example:**<br>`Router(config)# utd` | Enters unified threat defense configuration mode. |
| **Step 10** | **engine advanced**<br>**Example:**<br>`outer(config-utd)# engine advanced` | Configures the unified threat defense (UTD) advanced engine and enters UTD advaned engine configuration. |
| **Step 11** | **fail close**<br>**Example:**<br>`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. |
| **Step 12** | **rate** *range*<br>**Example:**<br>`Device(config-engine-std)# rate 1000` | (Optional) Specify the pps rate to push to the sensor. The range is 1000 to 4000000. |
| **Step 13** | **redirect interface** *type number*<br>**Example:**<br>`Router(config-utd)# redirect interface BDI 10` | Configures IDS traffic redirect on an interface. |
| **Step 14** | **end**<br>**Example:**<br>`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 enable
```

```
Router(config-utd)# utd engine advanced
Router(config-utd-adv)# threat detection
Router(config-utd-adv)# exit
Router(config)# utd
Router(config-utd)# all-interfaces
Router(config-utd)# engine advanced
Router(config-utd)# fail close
Router(config-utd)# rate 1000
Router(config-utd)# 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 enable
Router(config-utd)# utd engine advanced
Router(config-utd-adv)# threat detection
Router(config-utd-adv)# exit
Router(config)# utd
Router(config-utd)# engine advanced
Router(config-utd)# fail close
Router(config-utd)# rate 1000
Router(config-utd)# redirect-interface BDI 10
Router(config-utd)# 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 | Cisco IOS Master Command List, All Releases |
| Security commands | • Cisco IOS Security Command Reference: Commands A to C<br>• Cisco IOS Security Command Reference: Commands D to L<br>• Cisco IOS Security Command Reference: Commands M to R<br>• Cisco IOS Security Command Reference: Commands S to Z |
| UCS E-Series Servers | http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/e/2-0/gs/guide/b_2_0_Getting_S |

### Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.<br>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.<br>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. | http://www.cisco.com/support |

# 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. An account on Cisco.com is not required.

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

| Feature Name | Releases | Feature Information |
|---|---|---|
| | | |