Security Configuration Guide: Unified Threat Defense, Cisco IOS XE Fuji 16.7.x

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: https://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. (1721R)

CONTENTS

CHAPTER 2

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, and Intrusion Detection System (IDS)

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

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. 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:

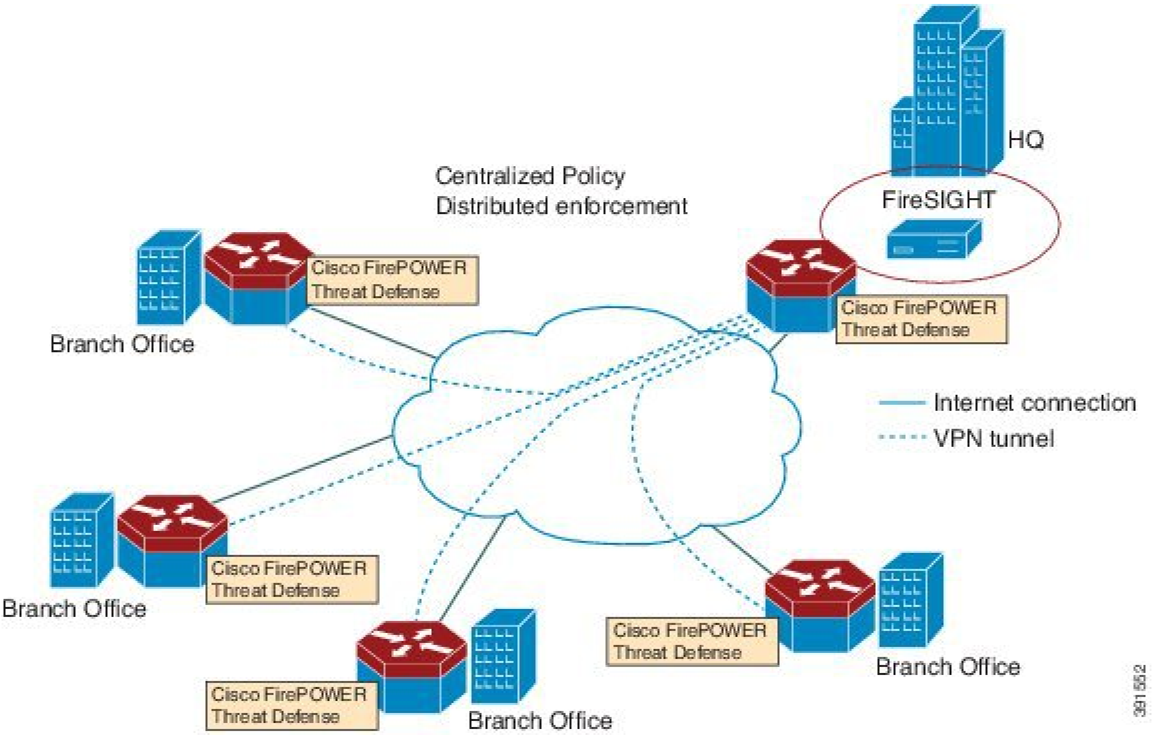
- Cisco FireSIGHT—A centralized policy and reporting entity that can run anywhere in the network. This can be the Cisco FireSIGHT appliance or a virtual installation on a server class machine.
- Virtual Firepower sensor—Security entities that implement policies, and send events and statistics back to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


HQ
FireSIGHT
Centralized Policy
Distributed enforcement
Cisco FirePOWER Threat Defense
Branch Office
Cisco FirePOWER Threat Defense
Internet connection
VPN tunnel
Cisco FirePOWER Threat Defense
Branch Office
Cisco FirePOWER Threat Defense
Branch Office
Cisco FirePOWER Threat Defense
Cisco FirePOWER Threat Defense
Branch Office
391552

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

	Command or Action	Purpose
Step 6	**switchport mode trunk** **Example:** `Router(config-if)# switchport mode trunk`	Specifies a trunking VLAN Layer 2 interface.
Step 7	**no mop enabled** **Example:** `Router(config-if)# no mop enabled`	Disables the Maintenance Operation Protocol (MOP) on an interface.
Step 8	**no mop sysid** **Example:** `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* **Example:** `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* **Example:** `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** **Example:** `Router(config-if-srv)# rewrite ingress tag pop 1 symmetric`	Specifies the encapsulation adjustment to be performed on a frame ingressing a service instance.
Step 12	**bridge domain** *bridge-ID* **Example:** `Router(config-if-srv)# bridge domain 10`	Binds a service instance or a MAC tunnel to a bridge domain instance.

Step 13	**end**
	Example:
	`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. • 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* **Example:** `Device# configure network ipv4 manual 10.66.152.137 255.255.255.0 10.66.152.1`	Configures network connectivity.
Step 3	**configure network dns servers** *dns-server* **Example:** `Device# configure network dns servers 192.10.26.10`	Configures domain name system (DNS) servers.
Step 4	**configure network dns searchdomains** *domain-name* **Example:** `Device# configure network dns searchdomains cisco.com`	Configures DNS search domains.
Step 5	**configure manager add** *dc-hostname registration-key* **Example:** `Device# configure manager sourcefire-dc.cisco.com cisco-sf`	Associates the sensor with the FireSIGHT. • 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**
4. **mode ids-global**
5. **ids redirect-interface** *interface interface-number*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**utd** **Example:** `Router(config)# utd`	Enters unified threat defense configuration mode.
Step 4	**mode ids-global** **Example:** `Router(config-utd)# mode ids-global`	Enables intrusion detection mode on all interfaces.
Step 5	**ids redirect-interface** *interface interface-number* **Example:** `Router(config-utd)# ids redirect-interface BDI 10`	Configures IDS traffic redirect on an interface.

Step 6	**end**
	Example:
	`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
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface gigabitethernet 0/1/1`	Configures an interface and enters interface configuration mode.
Step 4	**utd ids** **Example:** `Router(config-if)# utd ids`	Enables intrusion detection on an interface.
Step 5	**exit** **Example:** `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** **Example:** `Router(config)# utd`	Enters unified threat defense configuration mode.

	Command or Action	Purpose
Step 8	**ids redirect interface** *type number* **Example:** `Router(config-utd)# ids redirect interface BDI 10`	Configures IDS traffic redirect on an interface.

Step 9	**end**
	Example:
	`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	Cisco IOS Master Command List, All Releases
Security commands	• Cisco IOS Security Command Reference: Commands A to C • Cisco IOS Security Command Reference: Commands D to L • Cisco IOS Security Command Reference: Commands M to R • 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_Started_Guide.html

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. 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. 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

CHAPTER 2

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

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. 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 engine 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 engine 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.

  Note If you are downloading signature packages from a local server to hold the signature packages, only HTTP is supported.

  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 performs a domain-name lookup (on the DNS server(s) configured on the router) to resolve the location for automatic signature updates from Cisco.com or on 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)

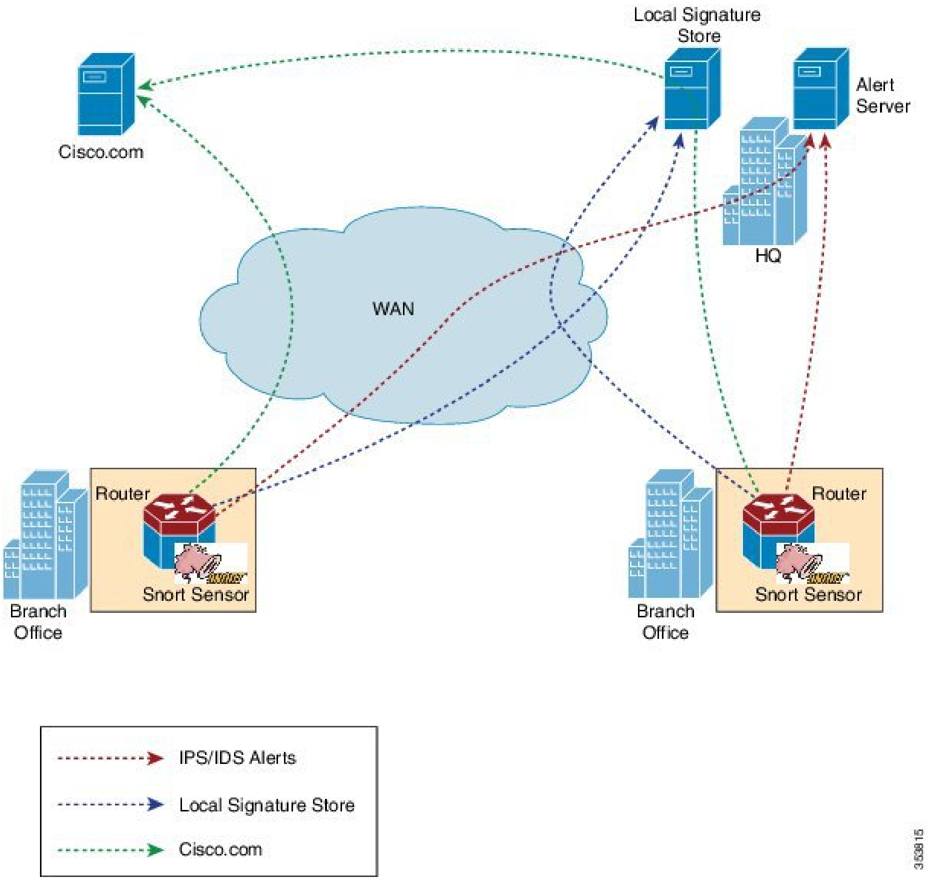
Platform	Profile	Virtual Service Resource Requirements		Platform Requirements
		System CPU	Memory	
Cisco 4331 ISR	Low (Default)	25%	Min: 1GB (RAM) Min: 750MB (Disk/Flash)	Min: 8GB (RAM) Min: 8GB(Disk/Flash)
	Medium	50%	Min: 2GB (RAM) Min: 1GB (Disk/Flash)	Min: 8GB (RAM) Min: 8GB(Disk/Flash)
	High	75%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

Platform	Profile	Virtual Service Resource Requirements		Platform Requirements
		System CPU	Memory	
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)
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.

Threat Inspection Alerts Visibility

From the Cisco IOS XE Fuji 16.8 release, you can get summarized details for the following threat-inspection alerts:

- The top 10 threat-inspection alerts (IDS/IPS) and counts are summarized for last 24 hours.

- For each signature-ID top 10 SIP, DIP, and VRF summary for the last 24 hours.

Note The last 24 hours period accounts for exact prior 24 hour duration from the time you request alert summary using CLI.

The visibility feature is available only on single tenancy and not on multi-tenancy.

Use **show utd engine standard logging threat-inspection statistics** *detail* command to view the alert summary.

Enabling and Disabling Logging of the Threat Inspection Alerts

To enable logging of the threat inspection alert statistics, perform the following steps:

```
config#utd eng standard
config-utd-eng-std#threat-inspection
config-utd-engstd-insp#logging statistics enable
config-utd-engstd-insp#exit
```

To disable logging of the threat inspection alert statistics, perform the following steps:

```
config#utd eng standard
config-utd-eng-std#threat-inspection
config-utd-engstd-insp#no logging statistics enable
config-utd-engstd-insp#exit
```

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
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**virtual-service install name** *virtual-service-name* **package** *file-url* **media** *file-system* **Example:** `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. • The length of the name is 20 characters. Hyphen (-) is not a valid character. • You must specify the complete path of the OVA package to be installed. **Note** OVA installation works on both hard disk and bootflash, the preferred filesystem to install the OVA will be hard disk.
Step 3	**show virtual-service list** **Example:** `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.

Note Before you change the Cisco IOS software image from any of the XE 3.x versions to XE 16.2.1, or from XE 16.2.1 to any of the XE 3.x versions, uninstall the virtual-service by using the **virtual-service uninstall name [name]** command for each virtual-service on the device. If one of the virtual-services is the ISR-WAAS service, which is installed with the **service waas enable** command, use the **service waas disable** command.

After the device is upgraded with the new version of Cisco IOS software image, re-install the virtual-services. For ISR-WAAS, use the **service wass enable** command, and for other virtual-services, use the **virtual-service install name [name] package [.ova file]** command.

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
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *VirtualPortGroup number* **Example:** `Device(config)# interface VirtualPortGroup 0`	Configures an interface and enters interface configuration mode. • Configure a VirtualPortGroup interface. This interface is used for management traffic when the management interface GigabitEthernet0 is not used.
Step 4	**ip address** *ip-address mask* **Example:** `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.
Step 5	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode and returns to global configuration mode.
Step 6	**interface** *type number* **Example:** `Device(config)# interface VirtualPortGroup 1`	Configures an interface and enters interface configuration mode. • Configure a VirtualPortGroup interface. • This interface is used for data traffic.
Step 7	**ip address** *ip-address mask* **Example:** `Device(config-if)# ip address 192.0.2.1 255.255.255.252`	Sets a primary IP address for an interface. • This IP address should not be routable to the outside network. • The IP address is assigned from the recommended 192.0.2.0/30 subnet.
Step 8	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode and returns to global configuration mode.
Step 9	**virtual-service** *name* **Example:** `Device(config)# virtual-service UTDIPS`	Configures a virtual container service and enters virtual service configuration mode. • The *name* argument is the logical name that is used to identify the virtual container service.

	Command or Action	Purpose

Step 10	**profile** *profile-name*
	Example:
	`Device(config-virt-serv)#profile high`
	Example:
	`Device(config-virt-serv)#profile multi-tenancy`
		(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, high, and multi-tenancy. (For multi-tenancy mode (Cisco CSR 1000v only), a `profile multi-tenancy` command must be configured.)

Step 11	**vnic gateway VirtualPortGroup** *interface-number* **Example:** `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. • 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.
Step 12	**guest ip address** *ip-address* **Example:** `Device(config-virt-serv-vnic)# guest ip address 10.1.1.2`	(Optional) Configures a guest vNIC address for the vNIC gateway interface. • **Note** Configure this command only if the **vnic management gigabitethernet0** command specified in Step 17 is not configured.
Step 13	**exit** **Example:** `Device(config-virt-serv-vnic)# exit`	Exits virtual-service vNIC configuration mode and returns to virtual service configuration mode.
Step 14	**vnic gateway VirtualPortGroup** *interface-number* **Example:** `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. • 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.
Step 15	**guest ip address** *ip-address* **Example:** `Device(config-virt-serv-vnic)# guest ip address 192.0.2.2`	Configures a guest vNIC address for the vNIC gateway interface.
Step 16	**exit** **Example:** `Device(config-virt-serv-vnic)# exit`	Exits virtual-service vNIC configuration mode and returns to virtual service configuration mode.

	Command or Action	Purpose
Step 17	**vnic management GigabitEthernet0** **Example:** `Device(config-virt-serv)# vnic management GigabitEthernet0`	(Optional) Configures the GigabitEthernet interface as the vNIC management interface. • The management interface must either be a VirtualPortGroup interface or GibagitEthernet0 interface. • If you do not configure the **vnic management GigabitEthernet0** command, then you must configure the **guest ip address** command specified in Step 12.
Step 18	**guest ip address** *ip-address* **Example:** `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.
Step 19	**exit** **Example:** `Device(config-virt-serv-vnic)# exit`	Exits virtual-service vNIC configuration mode and returns to virtual service configuration mode.
Step 20	**activate** **Example:** `Device(config-virt-serv)# activate`	Activates an application installed in a virtual container service.

Step 21	**end**
	Example:
	`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** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter you password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**utd threat-inspection whitelist** **Example:** `Device(config)# utd threat-inspection whitelist`	(Optional) Enables the UTD whitelist configuration mode.
Step 4	**signature id** *signature-id* [**comment** *description*]	Configures signature IDs to be whitelisted.

	Command or Action	Purpose
	Example: `Device(config-utd-whitelist)# signature id 24245 comment traffic from branchoffice1`	- Signature IDs can be copied from alerts that needs to be suppressed. - You can configure multiple signature IDs. - Repeat this step for each signature ID that needs to be whitelisted.
Step 5	**exit** **Example:** `Device(config-utd-whitelist)# exit`	Exits UTD whitelist configuration mode and returns to global configuration mode.
Step 6	**utd engine standard** **Example:** `Device(config)# utd engine standard`	Configures the unified threat defense (UTD) standard engine and enters UTD standard engine configuration mode.

Step 7	**logging** {**server** *hostname* [**syslog**] | **syslog**}
	Example:
	`Device(config-utd-eng-std)# logging server syslog.yourcompany.com`
		Enables the logging of emergency messages to a server.

Step 8	**threat-inspection** **Example:** `Device(config-utd-eng-std)# threat-inspection`	Configures threat inspection for the Snort engine.

Step 9	**threat** {**detection** | **protection** }
	Example:
	`Device(config-utd-eng-std-insp)# threat protection`
		Configures threat detection or Intrusion Prevention System (IPS) as the operating mode for the Snort engine.
		- The default is **detection**.
		- Configure the **detection** keyword to configure Intrusion Detection System (IDS).

Step 10	**policy** {**balanced** | **connectivity** | **security**}
	Example:
	`Device(config-utd-eng-std-insp)# policy security`
		Configures the security policy for the Snort engine.
		- The default policy option is **balanced**.

Step 11	**whitelist** **Example:** `Device(config-utd-eng-std-insp)# whitelist`	(Optional) Enables whitelisting under the UTD engine.
Step 12	**signature update occur-at** {**daily** | **monthly** *day-of-month* | **weekly** *day-of-week*} *hour minute* **Example:** `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.

	Command or Action	Purpose
Step 13	**signature update server** {**cisco** | **url** *url* } [**username** *username* [**password** *password*]] **Example:** `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.

Step 14	**logging level** {**alert** | **crit** | **debug** | **emerg** | **err** | **info** | **notice** | **warning**}
	Example:
	`Device(config-utd-eng-std-insp)# logging level emerg`
		Enables the log level.

Step 15	**exit** **Example:** `Device(config-utd-eng-std-insp)# exit`	Exits UTD standard engine configuration mode and returns to global configuration mode.
Step 16	**utd** **Example:** `Device(config)# utd`	Enables unified threat defense (UTD) and enters UTD configuration mode.
Step 17	**redirect interface virtualPortGroup** *interface-number* **Example:** `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.
Step 18	**all-interfaces** **Example:** `Device(config-utd)# all-interfaces`	Configures UTD on all Layer 3 interfaces of the device.
Step 19	**engine standard** **Example:** `Device(config-utd)# engine standard`	Configures the Snort-based unified threat defense (UTD) engine and enters standard engine configuration mode.
Step 20	**fail close** **Example:** `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 21	**exit** **Example:** `Device(config-eng-std)# exit`	Exits standard engine configuration mode and returns to global configuration mode.

	Command or Action	Purpose

Step 22	**end**
	Example:
	`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
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter you password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config)# interface gigabitethernet 0/0/0`	Configures an interface and enters interface configuration mode.
Step 4	**utd enable** **Example:** `Device(config-if)# utd enable`	Enables unified threat defense (UTD).
Step 5	**exit** **Example:** `Device(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 inspection.	–
Step 7	**utd threat-inspection whitelist** **Example:** `Device(config)# utd threat-inspection whitelist`	(Optional) Enables the UTD whitelist configuration mode.
Step 8	**signature id** *signature-id* [**comment** *description*] **Example:** `Device(config-utd-whitelist)# signature id 24245 comment traffic from branchoffice1`	Configures signature IDs to be whitelisted. • Signature IDs can be copied from alerts that needs to be suppressed. • You can configure multiple signature IDs. • Repeat this step for each signature ID that needs to be whitelisted.
Step 9	**exit** **Example:** `Device(config-utd-whitelist)# exit`	Exits UTD whitelist configuration mode and returns to global configuration mode.

	Command or Action	Purpose
Step 10	**utd engine standard** **Example:** `Device(config)# utd engine standard`	Configures the unified threat defense (UTD) standard engine and enters UTD standard engine configuration mode.

Step 11	**logging** {**server** *hostname* [**syslog**] | **syslog**}
	Example:
	`Device(config-utd-eng-std)# logging syslog`
		Enables the logging of critical messages to the IOSd syslog.

Step 12	**threat-inspection** **Example:** `Device(config-utd-eng-std)# threat-inspection`	Configures threat inspection for the Snort engine.

Step 13	**threat** {**detection** | **protection** }
	Example:
	`Device(config-utd-eng-std-insp)# threat detection`
		Configures threat protection or Intrusion Detection System (IDS) as the operating mode for the Snort sensor.
		• Configure the **protection** keyword to configure Intrusion Prevention System (IPS).

Step 14	**policy** {**balanced** | **connectivity** | **security**}
	Example:
	`Device(config-utd-eng-std-insp)# policy balanced`
		Configures the security policy for the Snort sensor.

Step 15	**whitelist** **Example:** `Device(config-utd-eng-std-insp)# whitelist`	(Optional) Enables whitelisting of traffic.
Step 16	**signature update occur-at** {**daily** | **monthly** *day-of-month* | **weekly** *day-of-week*} *hour minute* **Example:** `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.
Step 17	**signature update server** {**cisco** | **url** *url*} [**username** *username* [**password** *password*]] **Example:** `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.

Step 18	**logging level** {**alert** | **crit** | **debug** | **emerg** | **err** | **info** | **notice** | **warning**}
	Example:
	`Device(config-utd-eng-std-insp)# logging level crit`
		Enables the log level.

	Command or Action	Purpose
Step 19	**exit** **Example:** `Device(config-utd-eng-std-insp)# exit`	Exits UTD standard engine configuration mode and returns to global configuration mode.
Step 20	**utd** **Example:** `Device(config)# utd`	Enables unified threat defense (UTD) and enters UTD configuration mode.
Step 21	**redirect interface virtualPortGroup** *interface-number* **Example:** `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.
Step 22	**engine standard** **Example:** `Device(config-utd)# engine standard`	Configures the Snort-based unified threat defense (UTD) engine and enters standard engine configuration mode.
Step 23	**exit** **Example:** `Device(config-eng-std)# exit`	Exits standard engine configuration mode and returns to global configuration mode.

Step 24	**end**
	Example:
	`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 examples show how to perform a manual signature update in different ways:

```
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: 2983.4.s
Current signature package name: UTD-STD-SIGNATURE-2983-4-S.pkg
Previous signature package version: 29.0.c
---------------------------------------
Last update status: Successful
---------------------------------------
Last successful update time: Mon Aug  7 02:02:32 2017 UTC
Last successful update method: Manual
Last successful update server: cisco
Last successful update speed: 3022328 bytes in 25 secs
---------------------------------------
Last failed update time: Mon Aug  7 01:53:21 2017 UTC
Last failed update method: Manual
Last failed update server: cisco
Last failed update reason: ('Connection aborted.', gaierror(-2, 'Name or service hnot
known'))
---------------------------------------
Last attempted update time: Mon Aug  7 02:02:32 2017 UTC
Last attempted update method: Manual
Last attempted update server: cisco
---------------------------------------
Total num of updates successful: 1
Num of attempts successful: 1
Num of attempts failed: 3
Total num of attempts: 4
---------------------------------------
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

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: 2983.4.s
Last update status: Successful
Last successful update time: Mon Aug  7 02:02:32 2017 UTC
Last failed update time: Mon Aug  7 01:53:21 2017 UTC
Last failed update reason: ('Connection aborted.', gaierror(-2, 'Name or service not known'))
Next update scheduled at: None
Current status: Idle
```

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: 2983.4.s
Current signature package name: UTD-STD-SIGNATURE-2983-4-S.pkg
Previous signature package version: 29.0.c
---------------------------------------
Last update status: Successful
---------------------------------------
Last successful update time: Mon Aug  7 02:02:32 2017 UTC
Last successful update method: Manual
Last successful update server: cisco
Last successful update speed: 3022328 bytes in 25 secs
---------------------------------------
Last failed update time: Mon Aug  7 01:53:21 2017 UTC
Last failed update method: Manual
Last failed update server: cisco
Last failed update reason: ('Connection aborted.', gaierror(-2, 'Name or service hnot known'))
---------------------------------------
Last attempted update time: Mon Aug  7 02:02:32 2017 UTC
Last attempted update method: Manual
Last attempted update server: cisco
---------------------------------------
Total num of updates successful: 1
Num of attempts successful: 1
Num of attempts failed: 3
Total num of attempts: 4
---------------------------------------
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} a000:0:0:0:0:0:0:10:59964 -> b000:0:0:0:0:0:0:10:53
```

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 techonlogy : 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 acquistion (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 Vitual-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 techonlogy : 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 eng standard threat-inspection signature update status
Current signature package version: 29.0.c
Current signature package name: default
Previous signature package version: None
---------------------------------------
Last update status: Failed
---------------------------------------
Last successful update time: None
Last successful update method: None
Last successful update server: None
Last successful update speed: None
---------------------------------------
Last failed update time: Thu Jan 11 13:34:36 2018 PST
Last failed update method: Manual
Last failed update server: http://172.27.57.252/UTD-STD-SIGNATURE-2983-1-S.pkg
Last failed update reason: [Errno 113] No route to host
---------------------------------------
Last attempted update time: Thu Jan 11 13:34:36 2018 PST
Last attempted update method: Manual
Last attempted update server: http://172.27.57.252/UTD-STD-SIGNATURE-2983-1-S.pkg
---------------------------------------
Total num of updates successful: 0
Num of attempts successful: 0
Num of attempts failed: 1
Total num of attempts: 1
---------------------------------------
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 Configutation:
  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} a000:0:0:0:0:0:0:10:59964 -> b000:0:0:0:0:0:0:10:53
```

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

Conditional debugging is supported by multi-tenancy for Unified Threat Defense. For further details about how to configure conditional debugging, see:

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	Cisco IOS Master Command List, All Releases
Security commands	• Cisco IOS Security Command Reference: Commands A to C • Cisco IOS Security Command Reference: Commands D to L • Cisco IOS Security Command Reference: Commands M to R • Cisco IOS Security Command Reference: Commands S to Z

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. 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. 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 Snort IPS

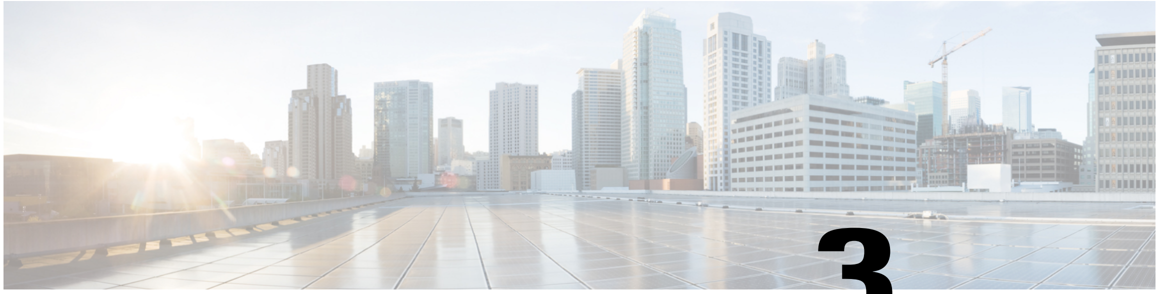
The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train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

Feature Name	Releases	Feature Information
Threat Inspection Alerts Visibility UTD Serviceability enhancements	Cisco IOS XE Fuji 16.8.1	This feature provides summary of threat inspection alerts. The following commands are introduced: • **show utd engine standard logging statistics threat-inspection** • **show utd engine standard logging statistics threat-inspection** *detail* Following commands are modified as part of UTD Serviceability Enahancement: • **show utd engine standard status** • **show utd engine standard threat-inspection signature update status**



CHAPTER 3

Web Filtering

The Web Filtering feature enables the user to provide controlled access to Internet websites or Interanet sites by configuring the domain-based or URL-based policies and filters on the device. The user can configure the web filtering profiles to manage the web access. The Web Filtering feature is implemented using the container service and it is similar to the Snort IPS solution.

Web Filtering can either allow or deny access to a specific domain or URL based on:

- Whitelist and Blacklist—These are static rules, which helps the user to either allow or deny domains or URLs. If the same pattern is configured under both whitelist and blacklist, the traffic will be whitelisted.
- Category—URLs can be classified into multiple categories such as News, Social Media, Education, Adult and so on. Based on the requirements, user has the option to block or allow one or more categories.
- Reputation—Each URL has a reputation score associated with it. The reputation score range is from 0-100, and it is categorized as: high-risk (reputation score (0-20), suspicious (0-40), moderate-risk (0-60), low-risk (0-80), and trustworthy (0-100). Based on the reputation score of a URL and the configuration, a URL is either blocked or allowed. If the user defines a reputation threshold through the CLI, all the URLs, with a reputation score lower than the user-defined threshold will be blocked.

Web Filtering

The Web Filtering feature enables the user to provide controlled access to Internet websites by configuring the domain-based or URL-based policies and filters on the device. Domain-based Filtering enables the user to control access to websites/servers at domain level, and URL-based Filtering enables the user to control access to websites at URL level. This section includes the following topics:

- Domain-based Filtering, on page 64
- URL-based Filtering, on page 65

Domain-based Filtering

Domain-based filtering allows the user to control access to a domain by permitting or denying access based on the domain-based policies and filters configured on the device. When the client sends a DNS request through the Cisco Cloud Services Router 1000V Series, the DNS traffic is inspected based on the domain-based policies (whitelist/blacklist). Domains that are whitelisted or blacklisted will not be subjected to URL-based filtering even if they are configured. Graylist traffic does not match both whitelist and blacklist, and it is subjected to URL-based filtering if it is configured.

Domain-based Filtering Using Whitelist Filter

To allow the complete domain (cisco.com) without subjecting to any filtering, use the whitelist option . When a user makes a request to access a website using a browser, the browser makes a DNS request to get the IP address of the website. Domain filtering applies the filter on the DNS traffic. If the website's domain name matches to one of the whitelisted patterns, domain filtering whitelists the website's address. The browser receives the IP address for the website and sends the HTTP(s) request to the IP address of the website. Domain filtering treats this traffic as whitelist traffic. This whitelist traffic is not further subjected to URL-based filtering even if it is configured. If the Snort IPS is configured, the traffic will be subjected to Snort IPS .

Domain-based Filtering Using Blacklist Filter

When a user want to block a complete domain (badsite.com), use the blacklist option. Domain filtering applies the filter on the DNS traffic. If the website's domain name matches to one of the blacklisted patterns, domain filtering will send the configured block server's IP address in the DNS response to the end user instead of the actual resolved IP address of the website. The browser receives the block server's IP address as the IP address for the website and sends the HTTP(s) request to this IP address. This traffic is not further subjected to URL filtering or Snort IPS even if they are configured.The block server receives the HTTP(s) request and serves a block page to the end user. Also, when the DNS request matches a blacklist, all application traffic to that domain will be blocked.

Domain filtering is applied to all the DNS traffic even if the DNS requests are made in the context of non-HTTP(S) requests such as FTP, telnet, and so on. The blacklisted non-HTTP(S) traffic (FTP, telnet, and so on.) will also be forwarded to the block server. It is block server's responsibility to serve a block page or deny the request. You can configure an internal or external block server. For configuration steps, see Configure Domain-based Web Filtering with an External Block Server, on page 69 and Configure Domain-based Web Filtering with a Local Block Server , on page 71.

If the traffic is not whitelisted or blacklisted by domain filtering, it will be subjected to URL filtering and Snort IPS if they are configured.

A user may consider using a combination of domain filtering whitelist and blacklist pattern list to design the filters. For an example, if a user want to whitelist *www\.foo\.com* but also wanted to blacklist other domains such as *www\.foo\.abc* and *www\.foo\.xyz*, configure the *www\.foo\.com* in the whitelist pattern list and *www\.foo\.* in the blacklist pattern list.

URL-based Filtering

URL-based filtering allows a user to control access to Internet websites by permitting or denying access to specific websites based on the whitelist/blacklist, category, or reputation configuration. For example, when a client sends a HTTP/HTTP(s) request through the Cisco CSR 1000V Cloud Services Router, the HTTP/HTTP(s) traffic is inspected based on the URL filtering policies (Whitelist/Blacklist, Category, and Reputation). If the HTTP/HTTP(s) request matches the blacklist, the HTTP(s) request is blocked either by inline block page response or redirects the URL to a block server. If the HTTP/HTTP(s) request matches the whitelist, the traffic is allowed without further URL filtering inspection.

For HTTPS traffic, the inline block page will not be displayed. URL-based filtering will not decode any encoded URL before peforming a lookup.

When there is no whitelist/blacklist configuration on the device, based on the category and reputation of the URL, traffic is allowed or blocked either using a block page or redirect URL for HTTP. For HTTP(s), there is no block page or redirect URL, the flow will be dropped.

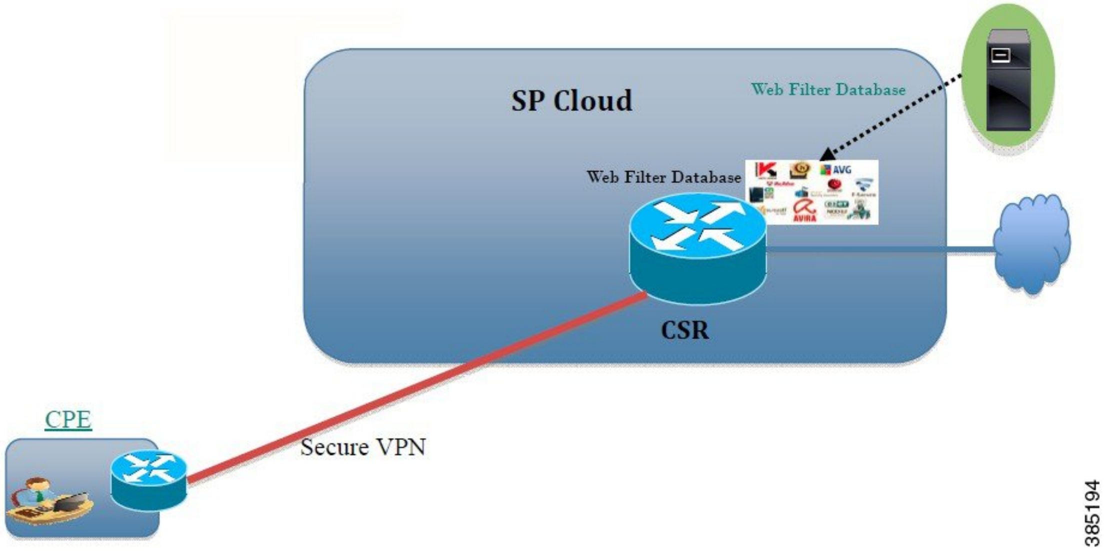
The URL database is downloaded from the cloud when the user configures the category/reputation-based URL filtering. The URL category/reputation database has only a few IP address based records and the category/reputation look up occurs only when the host portion of the URL has the domain name. After the full database is downloaded from the cloud, if there are any updates to the existing database, the incremental updates will be automatically downloaded in every 15 minutes. The complete database size is approximately 440 MB and the downloaded database should always synchronize with the cloud. The database will be invalid if the connection to the cloud is lost for more than 24 hours.

If the device does not get the database updates from the cloud, the fail-open option ensures that the traffic designated for URL filtering is not dropped. When you configure the fail-close option, all the traffic destined for URL filtering will be dropped when the cloud connectivity is lost.

Note The web filtering database is periodically updated from the cloud in every 15 minutes.

The figure illustrates the Web Filtering topology.

Figure 3: Web Filtering Network Topology



Benefits of Web Filtering

The web filtering feature allows a user to provide controlled access to the Internet by configuring domain and URL based policies and filters. It helps to secure the network by blocking malicious or unwanted websites.Web filtering comprises of URL-based filtering and the Domain-based filtering. Domain-based filtering helps control access to websites/servers at domain level and the URL-based filtering helps control access to websites at URLs level. A user can use web filtering to blacklist individual URL or domain names and configure whitelisting policies for the same. A user can also provision to allow or block a URL based on reputation or category.

Prerequisites for Web Filtering

Before you configure the web filtering feature on the Cisco CSR 1000V Cloud Services Router, ensure that you have the following:

- The Cisco CSR 1000V Cloud Services Router runs the Cisco IOS XE Denali 16.3 software image or later.
- The Cisco CSR 1000V Cloud Services Router requires 2 vCPU, 8GB memory, and 2GB extra disk space for deploying the container service.
- The Cisco CSR 1000V Cloud Service Router must have a security K9 license to enable the web filtering feature.

Restrictions for Web Filtering

The following restrictions apply to the web filtering feature:

- This feature is only supported on Cisco CSR 1000V Cloud Services Router and it is not supported on Cisco 4000 Series Integrated Services Routers.
- The blacklist/whitelist pattern supports only regex pattern, and currently 64 patterns are supported for blacklist/whitelist rules. For more information on regex pattern, see the Regular Expressions chapter.
- Domain filtering supports only the IPv4 domains resolved through DNS protocol using IPv4 UDP transport. Domain filtering alerts are sent only to IOS syslog.
- Domain filtering with OpenDNS is not supported.
- URL filtering with Virtual Routing and Forwarding (VRF) is not supported.
- Domain filtering with CWS is not supported.
- Domain filtering does not support category and reputation.
- Local block server does not support serving HTTPS block page.When the URL filter tries to inject block page or redirect message, it does not support HTTPS traffic.
- When there is a username and password in the URL, URL filter does not remove them from the URL before matching the whitelist/blacklist pattern. However, the category/reputation lookup does not have this limitation and removes the username and password from the URL before lookup.
- HTTPS inspection is limited. Web filtering uses server certificate to obtain the URL/domain information. It is not possible to inspect the full URL path.
- If the virtual-service profile *urlf-low* is configured after installing the virtual service, the activation will fail. You need to uninstall and install the virtual service again.
- UTD does not inter-operate with WCCP, and NBAR under inter-VRF scenario.
- Web filter profile names for URL, domain, block and sourcedb can have only alpha-numeric characters, dashes and underscores.

How to Deploy Web Filtering

To deploy web filtering on supported devices, perform the following tasks:

Before You Begin

- **Provision the device:** Identify the device to install the Web Filtering feature. This feature is supported on Cisco CSR 1000V Cloud Services Router.

- **Obtain the license:** The web filtering functionality is available only in security packages which require a security license to enable the service. Contact Cisco Support to obtain the license.

Step 1 Install and activate the virtual container service—How to Install and Activate the Virtual Container Service , on page 68

Step 2 Configure the domain-based web filtering with an external block server—Configure Domain-based Web Filtering with an External Block Server, on page 69

Step 3 Configure the domain-based web filtering with local block server—Configure Domain-based Web Filtering with a Local Block Server , on page 71

Step 4 Configure the URL-based web filtering with a local block server—Configure URL-based Web Filtering with a Local Block Server, on page 72

Step 5 Configure the URL-based web filtering with an Inline block server—Configure URL-based Web Filtering with an Inline Block Page, on page 74

Step 6 Configure the Snort IPS/IDS—Configuring Domain/URL based Web Filtering and Snort IPS, on page 75

How to Install and Activate the Virtual Container Service

To install and activate the virtual container service, perform the following task:

Step 1 Install the UTD OVA file—Installing the UTD OVA File, on page 68.

Step 2 Configure the VirtualPortGroup interfaces and virtual-service—Configuring VirtualPortGroup Interfaces and Virtual Service, on page 69.

Step 3 Activate the Snort virtual container service.

Installing the UTD OVA File

An OVA file is an Open Virtualization Archive that contains a compressed, installable version of a virtual machine. 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.

This is the sample configuration:

```
Device> enable
Device# virtual-service install name UTDIPS package harddisk:utd-ips-v102.ova media harddisk:

Device# show virtual-service list
Virtual Service List:
Name Status Package Name
```

```
------------------------------------------------------------------------------
snort Installed utdsnort.1_2_2_SV2982_XE_main.20160
```

Configuring VirtualPortGroup Interfaces and Virtual Service

You must configure two VirtualPortGroup interfaces and configure guest IP addresses for both interfaces.

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.

This is the sample configuration:

```
Device# configure terminal
evice(config)# interface VirtualPortGroup0
Device(config-if)# ip address 192.0.2.0 255.255.255.252
Device(config-if)# exit
Device(config)# interface VirtualPortGroup 1
Device(config-if)# ip address 192.0.2.1 255.255.255.224
Device(config-if)# exit
Device(config)# virtual-service UTDIPS

Device(config-virt-serv)# profile urlf-low (This is minimum requirement for web filtering
to work.)

Device(config-virt-serv)# vnic gateway VirtualPortGroup 0 (The IP-address configured in
VPG0 interface should have access to Internet over http(s).If the VPG0 interface does not
have access to Internet, the web filter database will not be updated.)
Device(config-virt-serv-vnic)# guest ip address 10.0.0.2
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)# activate
Device(config-virt-serv)# end

Device# show virtual-service list
Virtual Service List:

Name                    Status            Package Name
------------------------------------------------------------------------------
snort                   Activated         utdsnort.1_2_2_SV2982_XE_main.20160
```

Configure Domain-based Web Filtering with an External Block Server

To configure domain-based web filtering with an external block server, perform these steps:

Step 1 Install and activate the virtual service. For more information, see Configuring VirtualPortGroup Interfaces and Virtual Service, on page 69.

Step 2 Configure the blacklist parameter-map:

```
parameter-map type regex domainfilter_blacklist_pmap1
    pattern “www\.examplebook\.com”
    pattern “www\.bitter\.com”
```

Step 3 Configure the whitelist parameter-map:

```
parameter-map type regex domainfilter_whitelist_pmap1
     pattern “www\.example\.com”
    pattern “www\.exmaplegogle\.com”
```

Step 4 Configure the domain profile and associate the blacklist and whitelist parameter-maps:

```
utd web-filter domain profile 1
 blacklist
  parameter-map regex domainfilter_blacklist_pmap1
 whitelist
  parameter-map regex domainfilter_whitelist_pmap1
```

Step 5 (Optional) By default the domain filtering alerts are not enabled. Configure the alerts for blacklist or whitelist, or both under the domain profile:

```
alert {all |blacklist | whitelist}
```

Step 6 Configure the external redirect-server under the domain profile:

```
redirect-server external x.x.x.x (This is the IP address that is used for serving block page when a
 page is blacklisted)
```

Step 7 Configure the UTD engine standard with domain profile:

```
utd engine standard
 web-filter
  domain-profile 1
```

Step 8 Configure the UTD with engine standard and enable it globally or on a specific interface:

```
utd
    all-interfaces
    engine standard
```

This example shows how to configure domain-based web filtering with an external block server:

```
parameter-map type regex domainfilter_blacklist_pmap1
 pattern “www\.examplebook\.com”
parameter-map type regex domainfilter_whitelist_pmap1
 pattern “www\.example\.com”
utd engine standard
 web-filter
  domain-profile 1
!utd web-filter domain profile 1
 alert all
 blacklist
  parameter-map regex domainfilter_blacklist_pmap1
 whitelist
  parameter-map regex domainfilter_whitelist_pmap1
redirect-server external 2 to x
!
utd
 all-interfaces
 engine standard
```

Configure Domain-based Web Filtering with a Local Block Server

To configure domain-based web filtering with a local block server, perform these steps:

Step 1 Install and activate the virtual service. For more information, see Configuring VirtualPortGroup Interfaces and Virtual Service, on page 69.

Step 2 Configure a loopback interface or use any existing interface that the client can access:

```
interface loopback 110
 ip address 10.1.1.1 255.255.255.255
exit
```

Step 3 Configure the UTD web filter with the local block server profile:

```
utd web-filter block local-server profile 1
 block-page-interface loopback 110
 http-ports 80
 content text "Blocked by Web-Filter"
```

Step 4 Configure the blacklist parameter-map:

```
parameter-map type regex domainfilter_blacklist_pmap1
      pattern “www\.bitter\.com”
```

Step 5 Configure the whitelist parameter-map:

```
parameter-map type regex domainfilter_whitelist_pmap1
       pattern “www\.exmaplegogle\.com”
```

Step 6 Configure the domain profile and associate the blacklist and whitelist parameter-maps:

```
utd web-filter domain profile1
 blacklist
  parameter-map regex domainfilter_blacklist_pmap1
 whitelist
  parameter-map regex domainfilter_whitelist_pmap1
```

Step 7 (Optional) By default the domain filtering alerts are not enabled. Configure the alerts for blacklist or whitelist, or both under the domain profile:

```
alert {all |blacklist | whitelist}
```

Step 8 Configure the redirect-server as local block server under the domain profile:

```
redirect-server local-block-server 1
```

Step 9 Configure the UTD engine standard with domain profile:

```
utd engine standard
 web-filter
  domain-profile 1
```

Step 10 Configure the UTD with engine standard and enable it globally or on a specific interface:

```
utd
    all-interfaces
    engine standard
```

This example shows how to configure a domain-based web filtering with a local block server:

```
interface loopback 110
 ip address 10.1.1.1 255.255.255.255
exit
utd engine standard
 web-filter
  domain-profile 1
  !
```

```
utd web-filter block local-server profile 1
 block-page-interface Loopback110
 content text "Blocked by Web-Filter"
 http-ports 80
!
utd web-filter domain profile 1
 alert all
 blacklist
  parameter-map regex df_blacklist_pmap1
 whitelist
  parameter-map regex df_whitelist_pmap1
 redirect-server local-block-server 1
!utd
all-interfaces
    engine standard
```

Configure URL-based Web Filtering with a Local Block Server

To configure URL-based web filtering with a local block server, perform these steps:

Step 1 Install and activate the virtual service. For more information, see Configuring VirtualPortGroup Interfaces and Virtual Service, on page 69.

Step 2 Configure a loopback interface or use any existing interface that the client can access:

```
interface loopback 110
 ip address 10.1.1.1 255.255.255.255
exit
```

Step 3 Configure the UTD web filter with the local block server profile:

```
utd web-filter block local-server profile 1
 block-page-interface loopback 110
 http-ports 80
 content text "Blocked by Web-Filter"
```

Step 4 Configure the blacklist parameter-map:

```
parameter-map type regex urlf_blacklist_pmap1
 pattern www.exmplee.com/sports
```

Step 5 Configure the whitelist parameter-map:

```
parameter-map type regex urlf_whitelist_pmap1
 pattern www.examplehoo.com/finance
```

Step 6 Configure the URL profile and do the following:

```
utd web-filter url profile 1
```

a) Associate the blacklist and whitelist parameter-maps:

```
blacklist
  parameter-map regex urlf_blacklist_pmap1
whitelist
  parameter-map regex urlf_whitelist_pmap1
```

b) Configure the alerts for blacklist, whitelist or both under the local block-server profile:

```
alert {all |blacklist | whitelist}
```

c) Configure the categories to be allowed or blocked:

```
categories allow
  sports
```

d) Configure the reputation block threshold:

```
reputation
  block-threshold high-risk
```

e) Configure the URL source database with the fail option:

```
sourcedb fail close
```

f) Configure the log level. The default option is error. When you set the option to **info** or **detail**, the performance may impact:

```
log level error
```

g) Configure local block server:block

```
block local-server 1
```

Step 7 Configure the UTD engine standard with URL profile:

```
utd engine standard
 web-filter
 url-profile 1
```

Step 8 Configure the UTD engine standard and enable the UTD on a global or specific interface:

```
utd
all-interfaces
    engine standard
```

This example shows how to configuration a URL-based web filtering with a local block server:

```
parameter-map type regex urlf_blacklist_pmap1
    pattern www.goog.com/sprots
parameter-map type regex urlf_whitelist_pmap1
    pattern www.exmaplehoo.com/finance

!interface loopback 110
 ip address 10.1.1.1 255.255.255.255
exit
utd web-filter block local-server profile 1
 block-page-interface loopback 110
 http-ports 80
 content text "Blocked by Web-Filter"
utd web-filter url profile 1
    blacklist
        parameter-map regex urlf_blacklist_pmap1
    whitelist
        parameter-map regex urlf_whitelist_pmap1
    alert all
    categories allow
        sports
    reputation
     block-threshold high-risk
   sourcedb fail close
  log level error
  block local-server 1!
utd engine standard
```

```
    web-filter
        url-profile 1
!
utd
    all-interfaces
    engine standard
```

Configure URL-based Web Filtering with an Inline Block Page

To configure URL-based web filtering with an in-line block page, perform these steps:

Step 1 Install and activate the virtual service. For more information, see Configuring VirtualPortGroup Interfaces and Virtual Service, on page 69.

Step 2 Configure the blacklist parameter-map:

```
parameter-map type regex urlf_blacklist_pmap1
 pattern www.exmaplegogle.com/sports
```

Step 3 Configure the whitelist parameter-map:

```
parameter-map type regex urlf_whitelist_pmap1
 pattern www.exmaplehoo.com/finance
```

Step 4 Configure the UTD block page profile:

```
utd web-filter block page profile 1
 text "Blocked by Web-Filter URLF" (The other options are file and redirect-url)
```

Step 5 Configure the URL profile and do the following:

```
utd web-filter url profile 1
```

a) Associate the blacklist and whitelist parameter-maps:

```
blacklist
  parameter-map regex urlf_blacklist_pmap1
whitelist
  parameter-map regex urlf_whitelist_pmap1
```

b) Configure the alerts for blacklist, whitelist or both under the local block-server profile:

```
alert {all |blacklist | whitelist}
```

c) Configure the categories to be allowed or blocked:

```
categories allow
  sports
```

d) Configure the reputation block threshold:

```
reputation
  block-threshold high-risk
```

e) Configure the URL source database with the fail option:

```
sourcedb fail close
```

f) Configure the log level. The default option is error. When you set the option to **info** or **detail**, the performance may impact:

```
log level error
```

g) Configure local block server:block

```
block local-server 1
```

Step 6 Configure the UTD engine standard with URL profile:

```
utd engine standard
 web-filter
 url-profile 1
```

Step 7 Configure the UTD engine standard and enable the UTD on a global or specific interface:

```
utd
    engine standard
    all-interfaces
```

This example shows how to configuration an URL-based web filtering with an inline block server:

```
parameter-map type regex urlf_blacklist_pmap1
  pattern www.examplegogle.com/sprots
parameter-map type regex urlf_whitelist_pmap1
  pattern www.examplehoo.com/finance
!
utd web-filter block page profile 1
    text "Blocked by Web-Filter URLF"
!
utd web-filter url profile 1
  blacklist
 parameter-map regex urlf_blacklist_pmap1
  whitelist
 parameter-map regex urlf_whitelist_pmap1
  alert all
  categories  allow
 sports
  reputation
  block-threshold high-risk
sourcedb fail close
  log level error
!
utd engine standard
     web-filter
     url-profile 1
!
utd
    all-interfaces
    engine standard
```

Configuring Domain/URL based Web Filtering and Snort IPS

To configure Domain/URL based web filtering and Snort IPS, perform these steps:

Step 1 Configure the domain profile:

```
utd web-filter domain profile 1
```

Step 2 Configure the URL profile:

```
utd web-filter url profile 1
```

Step 3 Configure the threat-inspection under UTD engine standard:

```
utd engine standard
 threat-inspection
```

Step 4 Configure the web-filter under UTD engine standard with the domain and URL profiles:

```
utd engine standard
 logging syslog
 threat-inspection
  threat protection
  policy security
 signature update server cisco username xxx password QhLb]Z[ifMbFgLYgR]^KLDUZ
  signature update occur-at daily 0 0
  logging level error
 web-filter
  domain-profile 1
  url-profile 1
```

Step 5 Configure the UTD engine standard and enable it globally or on a specific interface:

```
utd
    engine standard
    all-interfaces
```

Verifying the Web Filter Configuration

You can verify the Web filtering configuration using the following commands:

```
Device# show utd engine standard config
IPS/IDS: Disabled


URL Filtering:
---------------
Status: Enabled

Whitelist:
==========
www.edition.cnn.com
16k.html

Blacklist:
==========
www.youtube.com

Categories(Allow):
==================
Sports

Block Profile:
Block text: "Blocked by URLF"

Reputation Threshold : High risk
Alerts : None
Debug level : Error

Device# show utd engine standard web-filter source status
Source DB Status:
        Process: Running
        Last known status: 2016-04-18 06:42:28  Current local database version 4-765
```

Troubleshooting Web Filtering

To collect the logs, use the virtual-service move name "CONTAINER_NAME" log to bootflash: command. You can troubleshoot issues that are related to enabling Web filtering feature using the following commands on the device:

- **debug utd engine standard all**
- **debug utd engine standard climgr**
- **debug utd engine standard daq**
- **debug utd engine standard internal**
- **debug utd engine standard onep**

For release 16.8.1, configuration error recovery on container is enhanced in order to apply configuration and signature updates to the container. With the improved error recovery, you can have:

- Greater robustness during configuration download to detect and act upon errors.
- Efficient way of handling signature and configuration updates occuring together.
- Early detect and recover from the loss of the oneP connection between IOSd and CLIMGR. For example, when CLIMGR crashes.
- Improved visibility to the detailed results of the (current or recent) configuration download, without requiring you to enable debugs.

Configuration Examples

The following example shows how to enable domain filtering on CSR 1000V Cloud Services Router:

```
 Example: Configuring Parameter Map
The following example shows how to configure parameter map:
Device# enable
Device# configure terminal
Device(config)# parameter-map type regex wlist1
Device(config-profile)# pattern www.google.com
Device(config-profile)# pattern www.cisco.com
!
Device(config)# parameter-map type regex blist1
Device(config-profile)# pattern www.exmaplehoo.com
Device(config-profile)# pattern www.bing.com
exit
!
Device(config)# utd web-filter block local-server profile 1
Device(config--utd-webf-blk-srvr)# content file bootflash:test.utd.file
Device(config--utd-webf-blk-srvr)# exit


For the local block server to work, HTTP server should be running. Use the ip http server
command to configure the block server. The show ip http server status  command displays the
 server status as enabled.

Device(config)# show ip http server status
HTTP server status: Enabled
HTTP server port: 80
```

Example: Configuring Web Filter Domain Profile

The following example shows how to configure web filter domain profile:

```
Device(config)# utd web-filter domain profile 1
Device(config-utd-webfltr-domain)# blacklist
Device(config-utd-webf-dmn-bl)# parameter-map regex blist1
Device(config-utd-webf-dmn-bl)# whitelist
Device(config-utd-webf-dmn-wl)# parameter-map regex wlist1
Device(config-utd-webf-dmn-wl)# exit
Device(config-utd-webfltr-domain)# alert all
Device(config-utd-webfltr-domain)# redirect-server external 1.2.3.4
Device(config-utd-webfltr-domain)# exit
```

Configuring Web Filter URL Profile

The following example shows how to configure web filter URL profile:

```
Device(config)# utd web-filter url profile 1
Device(config-utd-webfltr-url)# blacklist
Device(config-utd-webf-url-bl)# parameter-map regex blist1
Device(config-utd-webf-url-bl)# whitelist
Device(config-utd-webf-url-wl)# parameter-map regex wlist1
Device(config-utd-webf-url-wl)# exit
Device(config-utd-webfltr-url)# categories allow
Device(config-utd-webf-url-cat)# news-and-media
Device(config-utd-webf-url-cat)# search-engines
Device(config-utd-webf-url-cat)# computer-and-internet-info
Device(config-utd-webf-url-cat)# computer-and-internet-security
Device(config-utd-webf-url-cat)# financial-services
Device(config-utd-webf-url-cat)# image-and-video-search
Device(config-utd-webf-url-cat)# job-search
Device(config-utd-webf-url-cat)#exit
Device(config-utd-webfltr-url)# alert all
Device(config-utd-webfltr-url)# reputation
Device(config-utd-webf-url-rep)# block-threshold suspicious
Device(config-utd-webf-url-rep)# exit
Device(config-utd-webfltr-url)# block local-server 1
Device(config-utd-webfltr-url)# exit
```

Configuring UTD Snort IPS/IDS Whitelist Signatures

The following example shows how to configure signature whitelist:

```
Device(config)# utd threat-inspection whitelist
Device(config-utd-whitelist)# signature id 1
Device(config-utd-whitelist)# signature id 2
evice(config-utd-whitelist)# exit
!
```

Example: Configuring Web Filter Profile

The following example shows how to configure web filter profile:

```
Device(config)# utd engine standard
Device(config-utd-eng-std)# logging server 1.2.3.4
Device(config-utd-eng-std)# threat-inspection
Device(config-utd-engstd-insp)#threat protection
Device(config-utd-engstd-insp)# policy security
Device(config-utd-engstd-insp)# logging level emerg
Device(config-utd-engstd-insp)# whitelist
Device(config-utd-engstd-insp)# web-filter
Device(config-utd-engstd-webf)# domain-profile 1
Device(config-utd-engstd-webf)# url-profile 1
Device(config-utd-engstd-webf)# exit
```

Example: Alert Messages for Web Filtering Events

The following example shows alert messages for web filtering events:

```
016/06/02-14:44:41.061501 IST [**] [Instance_ID: 1] [**] Drop [**] UTD WebFilter Blacklist
 [**] [URL: www.edition.cnn.com/2016/03/31/asia/kolkata-bridge-collapse/index.html]
[Initiator_VRF: 0] {TCP} 1.0.0.9:56608 -> 2.0.0.29:80

2016/06/02-14:48:06.636270 IST [**] [Instance_ID: 1] [**] Pass [**] UTD WebFilter Whitelist
 [**] [URL: www.ndtv.com/index.html] [Initiator_VRF: 0] {TCP} 1.0.0.9:56611 -> 2.0.0.23:80

Jun 2 14:37:57.856 IST: %IOSXE-6-PLATFORM: F0: cpp_cp: QFP:0.0 Thread:000
TS:00000618422205723793 %UTD-6-UTD_DF_BLACKLIST_MATCH: UTD WebFilter Domain Blacklist [**]
 [Domain: www.cricinfo.com] [Matched Pattern: www.cricinfo.com] {UDP} 2.0.0.10:53 ->
1.0.0.9:55184

Jun 2 14:39:22.653 IST: %IOSXE-6-PLATFORM: F0: cpp_cp: QFP:0.0 Thread:000
TS:00000618507002407540 %UTD-6-UTD_DF_WHITELIST_MATCH: UTD WebFilter Domain Whitelist [**]
 [Domain: www.cricinfo.com] [Matched Pattern: www.cricinfo.com] {UDP} 2.0.0.10:53 ->
1.0.0.9:55286
```

Additional References for Cisco Web Filtering

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 • Cisco IOS Security Command Reference: Commands D to L • Cisco IOS Security Command Reference: Commands M to R • 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_Started_Guide.html

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. 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. 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 Web Filtering

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 3: Feature Information for Cisco Web Filtering

Feature Name	Releases	Feature Information
Cisco Web Filtering	Cisco IOS XE Denali Release 16.3.1	The Web Filtering feature enables the user to provide controlled access to Internet websites by configuring the domain-based or URL-based policies and filters on the device. The user can configure the web filtering profiles to manage the web access.Web Filtering feature is implemented using the container service and it is similar to the Snort IPS solution.
UTD feature parity on ISRv UTD Serviceability Enhancements	Cisco IOS XE Fuji Release 16.8.1	Domain and URL filtering in both single-tenant and multi-tenant mode are supported for CSR. For ISRv, only single-tenant is supported. This feature is available on all models of the ENCS platforms. Error recovery feature in UTD is enhanced to allow the container to recover from internal error by initiating a bulk configuration download from IOS. The command **utd web-filter** *profile name* is modifed.