Deploy Snort IPS on Cisco Integrated Services Routers 4000 Series

Contents

Introduction

This document describes how to deploy the Snort IPS and Snort IDS feature on Cisco Integrated Services Routers (ISR) 4000 series using the IOx method.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Integrated Services Routers 4000 series with at least 8GB DRAM.
- Basic IOS-XE command experience.
- Basic Snort knowledge.
- A signature subscription for 1 year or 3 years is required
- IOS-XE 16.10.1a and above.

Components Used

The information in this document is based on these software and hardware versions:

- ISR4331/K9 running 17.9.3a release.
- UTD Engine TAR for 17.9.3a release.
- Securityk9 license for ISR4331/K9.

The VMAN method is now deprecated.

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

Background Information

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 to enable IPS and IDS capabilities.

Snort is an open-source IPS that performs real-time traffic analysis and generates alerts when threats are detected on IP networks. It can also perform protocol analysis, content researching or marching, 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 Integrated Services Routers 4000 series and Cloud Services Router 1000v Series.

The Snort IPS feature works as network intrusion detection or prevention mode and provides IPS or IDS capabilities on Cisco Integrated Services Routers 4000 series and Cloud Services Router 1000v Series.

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

Based on network requirements. Snort IPS can be enabled as IPS or IDS. In IDS mode, Snort inspects the traffic and reports alerts, but does not take any action to prevent attacks. In IPS mode inspects the traffic and reports alerts as IDS does but actions are taken to prevent attacks.

The Snort IPS runs as a service on ISR routers. Service containers use virtualization technology to provide a hosting environment on Cisco devices for applications. Snort traffic inspection is enabled either on a per-interface basis or globally on all supported interfaces. The Snort sensor requires two VirtualPortGroup interfaces. The first VirtualPortGroup is used for management traffic and the second for data traffic between the forwarding plane and the Snort virtual container service. Guess 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.

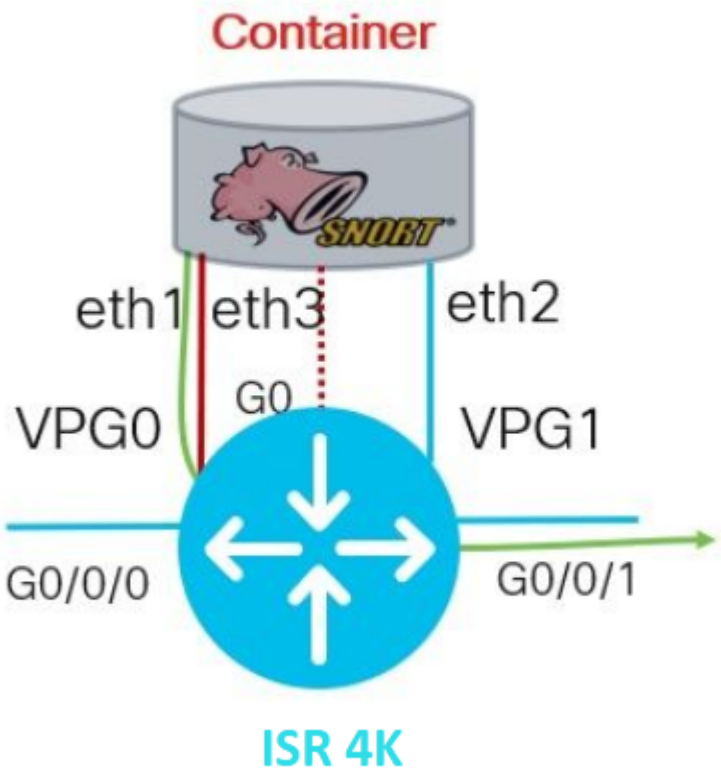
The Snort IPS monitors the traffic and reports events to an external log server or the IOS syslog. Enabling logging into the IOS syslog may impact performance due to the potential volume of log messages. External third-party monitoring tools, which support Snort logs, can be used for log collection and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

Snort IPS on Cisco 4000 Series Integrated Services Routers and Cisco Cloud Services Router 1000v Series is based on Signature package download. 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 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. The signature package can be downloaded from software.cisco.com. Snort signature information can be found on snort.org.

Network Diagram



Configure

Platform UTD configuration

Step 1. Configure Virtual VirtualPortGroups interfaces.

```
Router#configure terminal
Router(config)#interface VirtualPortGroup0
Router(config-if)#description Management Interface
Router(config-if)#ip address 192.168.1.1 255.255.255.252
Router(config-if)#no shutdown
Router(config-if)#exit

Router(config)#interface VirtualPortGroup1
Router(config-if)#description Data Interface
Router(config-if)#ip address 192.168.2.1 255.255.255.252
Router(config-if)#no shutdown
Router(config-if)#exit
```

Step 2. Enable the IOx environment in Global Configuration mode.

```
Router(config)#iox
```

Step 3. Configure app-hosting with vnic configuration.

```
Router(config)#app-hosting appid UTD
Router(config-app-hosting)#app-vnic gateway0 virtualportgroup 0 guest-interface 0
Router(config-app-hosting-gateway0)#guest-ipaddress 192.168.1.2 netmask 255.255.255.252
Router(config-app-hosting-gateway0)#exit

Router(config-app-hosting)#app-vnic gateway1 virtualportgroup 1 guest-interface 1
Router(config-app-hosting-gateway0)#guest-ipaddress 192.168.2.2 netmask 255.255.255.252
Router(config-app-hosting-gateway0)#exit
```

Step 4 (Optional). Configure Resource Profile.

```
Router(config-app-hosting)#app-resource package-profile low [low,medium,high]
Router(config-app-hosting)#end
```

Note: *If this is not defined, the system will use the default app-resource config (Low). Make sure to have enough available resources on ISR if the default profile config will be changed.*

Step 5. Install the app-hosting using the UTD.tar file.

```
Router#app-hosting install appid UTD package bootflash:iox-iosxe-utd.16.12.08.1.0.24_SV2.9.16.1_XE16.12.
```

Note: Keep the correct UTD.tar file on bootflash: to proceed to install it. Snort version is specified on UTD file name.

Next syslogs should be seen indicating UTD service was installed properly.

```
Installing package 'bootflash:iox-iosxe-utd.16.12.08.1.0.24_SV2.9.16.1_XE16.12
*Jun 26 19:25:35.975: %VMAN-5-PACKAGE_SIGNING_LEVEL_ON_INSTALL: R0/0: vman: Pa
*Jun 26 19:25:50.746: %VIRT_SERVICE-5-INSTALL_STATE: Successfully installed vi
*Jun 26 19:25:53.176: %IM-6-INSTALL_MSG: R0/0: ioxman: app-hosting: Install su
```

Note: Using *'show app-hosting list'* the status should be *'Deployed'*

Step 6. Start the app-hosting service.

```
Router#configure terminal
Router(config)#app-hosting appid UTD
```

```
Router(config-app-hosting)#start
Router(config-app-hosting)#end
```

> **Note**: After starting the app-hosting service, the app-hosting status should be *'Running'*. Use *'show app-hosting list' or 'show app-hosting detail'* to see more details.

Next syslog messages should be seen indicating UTD service was installed properly.

```
*Jun 26 19:55:05.362: %VIRT_SERVICE-5-ACTIVATION_STATE: Successfully activated
*Jun 26 19:55:07.412: %IM-6-START_MSG: R0/0: ioxman: app-hosting: Start succee
```

Service Plane and Data Plane Configuration.

After successful installation, the service plane must be configured. Snort IPS can be configured as Intrusion Prevention System (IPS) or Intrusion Detection System (IDS) for inspection.

> **Warning**: Confirm the *'securityk9'* license feature is enabled to proceed with UTD service plane configuration.

Step 1. Configure the Unified Threat Defense (UTD) standard engine (Service Plane)

```
Router#configure terminal
Router(config)#utd engine standard
```

Step 2. Enable the logging of emergency messages to a remote server.

```
Router(config-utd-eng-std)#logging host 192.168.10.5
```

Step 3. Enable Threat Inspection for Snort Engine.

```
Router(config-utd-eng-std)#threat-inspection
```

Step 4. Configure Threat Detection as Intrusion Prevention System (IPS) or Intrusion Detection System (IDS)

```
Router(config-utd-engstd-insp)#threat [protection,detection]
```

Note: *'Protection'* is used for IPS and *'Detection'* for IDS. *'Detection'* is the default.

Step 5. Configure Security Policy.

```
Router(config-utd-engstd-insp)#policy [balanced, connectivity, security]
Router(config-utd-engstd-insp)#exit
Router(config-utd-eng-std)#exit
```

Note: Default Policy is *'balanced'*

Step 6 (Optional). Create the UTD-allowed list (Whitelist)

```
Router#configure terminal
Router(config)#utd threat-inspection whitelist
```

Step 7 (Optional). Configure Snort Signatures IDs to appear in the whitelist.

```
Router(config-utd-whitelist)#generator id 40 signature id 54621 comment FILE-OFFICE traffic from network
Router(config-utd-whitelist)#end
```

Note: ID *'40'* is used as an example. In order to check Snort Signature information, check Official Snort documentation.

Step 8 (Optional). Enable Allowed List on Threat Inspection config.

```
Router#config terminal
Router(config)#utd engine standard
Router(config-utd-eng-std)#threat-inspection
Router(config-utd-engstd-insp)#whitelist
```

Step 9. Configure the Signature update interval to download Snort Signatures automatically.

```
Router#config terminal
Router(config)#utd engine standard
Router(config-utd-eng-std)#threat-inspection
Router(config-utd-engstd-insp)#signature update occur-at [daily, monthly, weekly] 0 0
```

Note: The first number defines the hour in 24hr format, and the second number indicates minutes.

Warning: UTD Signature updates generate a brief service interruption at the time of update.

Step 10. Configure the signature update server parameters.

```
Router(config-utd-engstd-insp)#signature update server [cisco, url] username cisco password cisco12
```

Note: Use *'cisco'* to use the Cisco server or *'url'* to define a custom path for the update server. For the Cisco server, you must provide your own username and password.

Step 11. Enable logging level.

```
Router(config-utd-engstd-insp)#logging level [alert,crit,debug,emerg,info,notice,warning]
Router(config-utd-engstd-insp)#exit
Router(config-utd-eng-std)#exit
```

Step 12. Enable utd service.

```
Router#configure terminal
Router(config)#utd
```

Step 13 (Optional). Redirect data traffic from the VirtualPortGroup interface to the UTD service.

```
Router#configure terminal
Router(config)#utd
Router(config-utd)#redirect interface virtualPortGroup
```

Note: If the redirection is not configured, it is auto-detected.

Step 14. Enable UTD to all Layer 3 interfaces on ISR.

```
Router(config-utd)#all-interfaces
```

Step 15. Enable the engine standard.

```
Router(config-utd)#engine standard
```

Next syslog messages should be seen indicating UTD was enabled properly.

```
*Jun 27 23:41:03.062: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0,
*Jun 27 23:41:13.039: %IOSXE-2-PLATFORM: R0/0: cpp_cp: QFP:0.0 Thread:000 TS:0
*Jun 27 23:41:22.457: %IOSXE-5-PLATFORM: R0/0: cpp_cp: QFP:0.0 Thread:000 TS:0
```

Step 16 (Optional). Define the action for UTD engine failure (UTD Data Plane)

```
Router(config-engine-std)#fail close
Router(config-engine-std)#end
Router#copy running-config startup-config
Destination filename [startup-config]?
```

> **Note**: *'Fail close'* option drops all the IPS/IDS traffic when the UTD engine fails. *'Fail open'* option allows all the IPS/IDS traffic on UTD failures. The default option is *'fail open'*.

Verify

Verify VirtualPortGroups IP address and interface status.

```
Router#show ip interface brief | i VirtualPortGroup
VirtualPortGroup0 192.168.1.1 YES NVRAM up up
VirtualPortGroup1 192.168.2.1 YES NVRAM up up
```

Verify VirtualPortGroup configuration.

```
Router#show running-config | b interface
interface VirtualPortGroup0
description Management Interface
ip address 192.168.1.1 255.255.255.252
!
interface VirtualPortGroup1
description Data Interface
ip address 192.168.2.1 255.255.255.252
!
```

Verify app-hosting configuration.

```
Router#show running-config | b app-hosting
app-hosting appid UTD
app-vnic gateway0 virtualportgroup 0 guest-interface 0
guest-ipaddress 192.168.1.2 netmask 255.255.255.252
app-vnic gateway1 virtualportgroup 1 guest-interface 1
guest-ipaddress 192.168.2.2 netmask 255.255.255.252
start
end
```

Verify iox activation.

```
Router#show running-config | i iox
iox
```

Verify UTD service plane config.

```
Router#show running-config | b engine
utd engine standard
logging host 192.168.10.5
threat-inspection
threat protection
policy security
signature update server cisco username cisco password KcEDIO[gYafNZheBHBD`CC\g`_cSeFAAB
signature update occur-at daily 0 0
logging level info
whitelist
utd threat-inspection whitelist
generator id 40 signature id 54621 comment FILE-OFFICE traffic
utd
all-interfaces
redirect interface VirtualPortGroup1
engine standard
fail close
```

```
Router#show utd engine standard config
UTD Engine Standard Configuration:

IPS/IDS : Enabled

Operation Mode : Intrusion Prevention
Policy : Security

Signature Update:
Server : cisco
User Name : cisco
Password : KcEDIO[gYafNZheBHBD`CC\g`_cSeFAAB
Occurs-at : daily ; Hour: 0; Minute: 0

Logging:
Server : 192.168.10.5
Level : info
```

```
Statistics : Disabled
Hostname : router
System IP : Not set

Whitelist : Enabled
Whitelist Signature IDs:
54621, 40

 Port Scan : Disabled

Web-Filter : Disabled
```

Verify the app-hosting state.

```
Router#show app-hosting list
App id                                   State
---------------------------------------------------------
UTD                                      RUNNING
```

Verify app-hosting details.

```
Router#show app-hosting detail
App id : UTD
Owner : ioxm
State : RUNNING
Application
Type : LXC
Name : UTD-Snort-Feature
Version : 1.0.7_SV2.9.18.1_XE17.9
Description : Unified Threat Defense
Author :
Path : /bootflash/secapp-utd.17.09.03a.1.0.7_SV2.9.18.1_XE17.9.x86_64.tar
URL Path :
Multicast : yes
Activated profile name :

Resource reservation
Memory : 1024 MB
Disk : 752 MB
CPU :
CPU-percent : 25 %
VCPU : 0

Platform resource profiles
Profile Name CPU(unit) Memory(MB) Disk(MB)
----------------------------------------------------------------

Attached devices
Type Name Alias
---------------------------------------------
Disk /tmp/xml/UtdLogMappings-IOX
Disk /tmp/xml/UtdIpsAlert-IOX
Disk /tmp/xml/UtdDaqWcapi-IOX
Disk /tmp/xml/UtdUrlf-IOX
```

```
Disk /tmp/xml/UtdTls-IOX
Disk /tmp/xml/UtdDaq-IOX
Disk /tmp/xml/UtdAmp-IOX
Watchdog watchdog-503.0
Disk /tmp/binos-IOX
Disk /opt/var/core
Disk /tmp/HTX-IOX
Disk /opt/var
NIC ieobc_1 ieobc
Disk _rootfs
NIC mgmt_1 mgmt
NIC dp_1_1 net3
NIC dp_1_0 net2
Serial/Trace serial3

Network interfaces
---------------------------------------
eth0:
MAC address : 54:0e:00:0b:0c:02
IPv6 address : ::
Network name :
eth:
MAC address : 6c:41:0e:41:6b:08
IPv6 address : ::
Network name :
eth2:
MAC address : 6c:41:0e:41:6b:09
IPv6 address : ::
Network name :
eth1:
MAC address : 6c:41:0e:41:6b:0a
IPv4 address : 192.168.2.2
IPv6 address : ::
Network name :

------------------------------------------------------------------------
Process Status Uptime # of restarts
------------------------------------------------------------------------
climgr UP 0Y 0W 0D 21:45:29 2
logger UP 0Y 0W 0D 19:25:56 0
snort_1 UP 0Y 0W 0D 19:25:56 0

Network stats:
eth0: RX packets:162886, TX packets:163855
eth1: RX packets:46, TX packets:65

DNS server:
domain cisco.com
nameserver 192.168.90.92

Coredump file(s): core, lost+found

Interface: eth2
ip address: 192.168.2.2/30
Interface: eth1
ip address: 192.168.1.2/30

Address/Mask Next Hop Intf.
------------------------------------------------------------------------------
0.0.0.0/0 192.168.2.1 eth2
0.0.0.0/0 192.168.1.1 eth1
```

Troubleshooting

1. Assure Cisco Integrated Services Router (ISR) runs XE 16.10.1a and above (For IOx method)

2. Assure Cisco Integrated Services Router (ISR) is licensed with the Securityk9 feature enabled.

3. Verify the ISR hardware model is in compliance with the minimum resource profile.

4. Feature not compatible with Zone-Based Firewall SYN-cookie and Network Address Translation 64 (NAT64)

5. Confirm UTD service is started after installation.

6. During the manual Signature package download, ensure the package has the same version as the Snort engine version. The signature package update may fail if there is a version mismatch.

7. In case of performance issues, use the ***'show app-hosting resource'*** and ***'show app-hosting utilization appid ''UTD-NAME'*** for learning about CPU/Memory/Storage consummation.

```
Router#show app-hosting resource
CPU:
Quota: 75(Percentage)
Available: 50(Percentage)
VCPU:
Count: 6
Memory:
Quota: 10240(MB)
Available: 9216(MB)
Storage device: bootflash
Quota: 4000(MB)
Available: 4000(MB)
Storage device: harddisk
Quota: 20000(MB)
Available: 19029(MB)
Storage device: volume-group
Quota: 190768(MB)
Available: 169536(MB)
Storage device: CAF persist-disk
Quota: 20159(MB)
Available: 18078(MB)
```

```
Router#show app-hosting utilization appid utd
Application: utd
CPU Utilization:
CPU Allocation: 33 %
CPU Used: 3 %
Memory Utilization:
Memory Allocation: 1024 MB
Memory Used: 117632 KB
Disk Utilization:
Disk Allocation: 711 MB
Disk Used: 451746 KB
```

Warning: If you are able to see high CPU, Memory, or Disk usage, contact Cisco TAC.

Debugging

Use the debug commands listed below to gather Snort IPS information in case of a failure.

<#root>

```
debug virtual-service all
```

```
debug virtual-service virtualPortGroup
```

```
debug virtual-service messaging
```

```
debug virtual-service timeout
```

```
debug utd config level error [error, info, warning]
debug utd engine standard all
```

Related Information

Additional documents related to Snort IPS deployment can be found here:

Snort IPS Security Configuration Guide

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_utd/configuration/xe-17/sec-data-utd-xe-17-book/snort-ips.html

Virtual Service Resource Profile

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_utd/configuration/xe-17/sec-data-utd-xe-17-book/snort-ips.html#id_31952

Snort IPS on Routers - Step-by-Step configuration.

https://community.cisco.com/t5/security-knowledge-base/router-security-snort-ips-on-routers-step-by-step-configuration/ta-p/3369186

Troubleshooting Snort IPS

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_utd/configuration/xe-17/sec-data-utd-xe-17-book/snort-ips.html#concept_C3C869E633A6475890475931DF83EBCC

ISR4K Snort IPS is not deployed since HW does not have enough platform resources

https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwf57595