Deploy Snort IPS on Integrated Services Routers 1000 series

Contents

Introduction

This document describes how to deploy the Snort IPS feature on Cisco Integrated Services Router (ISR) 1000 series.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Integrated Services Routers 1k series
- Basic XE-IOS commands
- Basic Snort knowledge

Components Used

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

- C1111X-8P running 17.03.03 release
- UTD Engine TAR for 17.3.3 release
- Security K9 license is required on the ISR1k
- A signature subscription 1year or 3 years is required
- XE 17.2.1r and above
- ISR hardware models that support 8GB DRAM only

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

The Snort IPS feature enables Intrusion Prevention System (IPS) or Intrusion Detection System (IDS) for branch offices on Cisco 4000 Series Integrated Services Routers (ISR), Cisco 1000 Series Integrated Services Routers (X PIDs such as 1111X, 1121X, 1161X, etc that support 8GB DRAM only) 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 IPS feature works in the network intrusion detection and prevention model that provides IPS or IDS functionalities. In the network intrusion detection and prevention mode, Snort performs the following actions

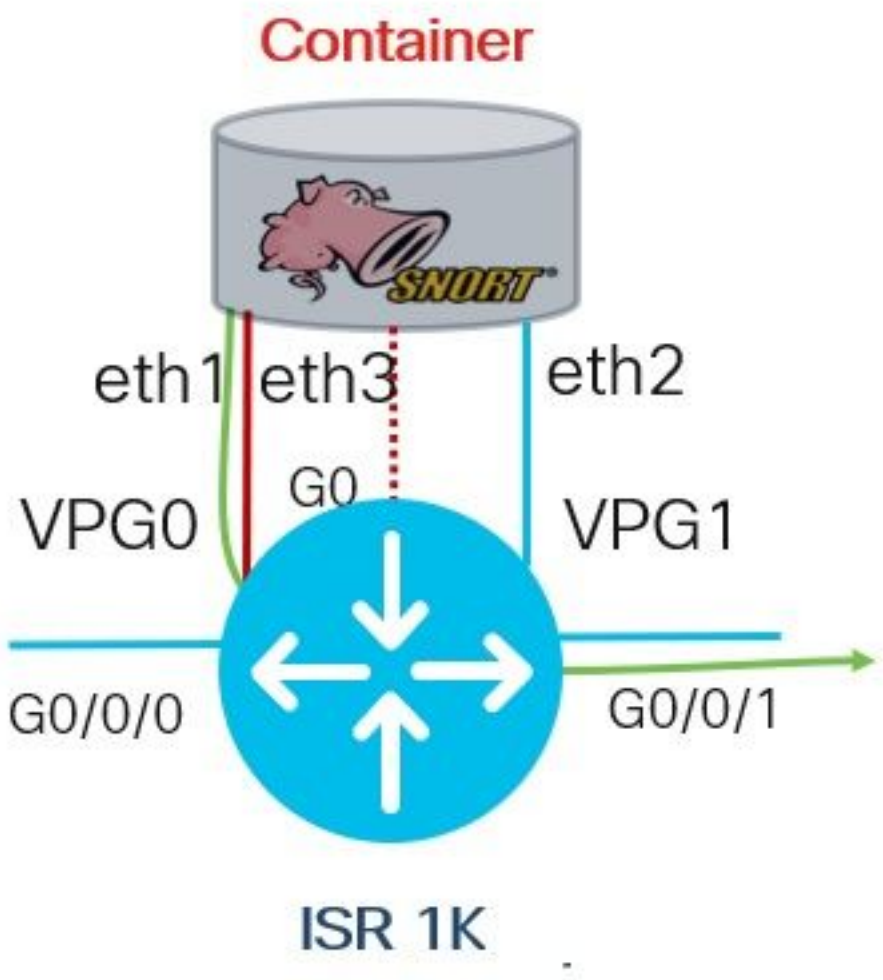
- Monitor network traffic and analyze against a defined ruleset
- Performed attacks classification
- Invokes actions against matched rules

Based on requirements, Snort can be enabled 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 support Snort logs, can be used for log collection and analysis.

There are two main ways to configure Snort IPS on Cisco Integrated Services Routers (ISR), the VMAN method and the IOx method. VMAN method uses a utd.ova file and IOx uses a utd.tar file. IOx is the correct and proper method for Snort IPS deployment on Cisco Integrated Services Router (ISR) 1k series.

Snort IPS can be deployed on Cisco Integrated Services Routers (ISR) 1k series with XE 17.2.1r and above.

Network Diagram



Configure

Step 1. Configure Port Groups

```
Router#config-transaction
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 192.0.2.1 255.255.255.252
Router(config-if)# no shutdown
Router(config-if)# exit
```

Step 2. Activate virtual service, configure and commit changes

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

```
Router(config-app-hosting)# app-vnic gateway0 virtualportgroup 1 guest-interface 1
Router(config-app-hosting-gateway)# guest-ipaddress 192.0.2.2 netmask 255.255.255.252
Router(config-app-hosting-gateway)# exit

Router(config-app-hosting)# app-resource package-profile low
Router(config-app-hosting)# start
Router(config-app-hosting)# exit
Router(config)# exit
Uncommitted changes found, commit them? [yes/no/CANCEL] yes
```

Step 3. Configure Virtual Service

```
Router#app-hosting install appid utd package bootflash:secapp-
utd.17.03.03.1.0.13_SV2.9.16.1_XE17.3.aarch64.tar
```

Step 4. Configuring UTD (Service Plane)

```
Router(config)# utd engine standard
Router(config-utd-eng-std)# logging host 10.12.5.100
Router(config-utd-eng-std)# logging syslog
Router(config-utd-eng-std)# threat-inspection
Router(config-utd-engstd-insp)# threat protection [protection, detection]
Router(config-utd-engstd-insp)# policy security [security, balanced, connectivity]
Router(config-utd-engstd-insp)# logging level warning [warning, alert, crit, debug, emerg, err,
info, notice]
Router(config-utd-engstd-insp)# signature update server cisco username cisco password cisco
Router(config-utd-engstd-insp)# signature update occur-at daily 0 0
```

> **Note**: Note: ***threat protection*** enables Snort as IPS, ***threat detection*** enables Snort as IDS.

Step 5. Configuring UTD (Data Plane)

```
Router(config)# utd
Router(config-utd)# all-interfaces
Router(config-utd)# engine standard
Router(config-engine)# fail close
```

> **Note**: Note: ***fail open*** is the default setting.

Verify

Verify Port Groups IP address and interface state

```
Router#show ip int brief | i VirtualPortGroup
Interface IP-Address OK? Method Status Protocol
VirtualPortGroup0 192.168.1.1 YES other up up
VirtualPortGroup1 192.0.2.1 YES other up up
```

Verify Port Groups configuration

```
interface VirtualPortGroup0
description Management interface
ip address 192.168.1.1 255.255.255.252
no mop enabled
```

```
no mop sysid
!
interface VirtualPortGroup1
description Data interface
ip address 192.0.2.1 255.255.255.252
no mop enabled
no mop sysid
!
```

Verify Virtual Service 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 192.0.2.2 netmask 255.255.255.252
app-resource package-profile low
start
```

Note: Make sure the ***start*** command is present, otherwise activation won't start.

Verify Virtual Service activation.

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

Note: ***iox*** will activate Virtual Service.

Verify UTD configuration (service plane and data plane)

```
Router#show running-config | b utd
utd engine standard
logging host 10.12.5.55
logging syslog
threat-inspection
threat protection
policy security
signature update server cisco username cisco password BYaO\HCd\XYQXVRRfaabbDUGae]
signature update occur-at daily 0 0
logging level warning
utd
all-interfaces
engine standard
fail close
```

Verify app-hosting state

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

Verify app-hosting state with details

```
Router#show app-hosting detail
```

```
*May 29 16:05:48.129: VIRTUAL-SERVICE: Received status request message
*May 29 16:05:48.129: VIRTUAL-SERVICE: Received status request message for virtual service (utd)
*May 29 16:05:48.129: VIRTUAL-SERVICE [utd]: cs send request: Sending CSReq type 4 (1),
transid=12
*May 29 16:05:48.129: VIRTUAL-SERVICE [utd]: cs send request: Sending CSReq type 5 (3),
transid=13
*May 29 16:05:48.129: VIRTUAL-SERVICE [utd]: cs send request: Sending CSReq type 5 (4),
transid=14
*May 29 16:05:48.129: VIRTUAL-SERVICE: Delivered Virt-manager request message to virtual service
'utd'
*May 29 16:05:48.184: VIRTUAL-SERVICE [utd]: cs callback string info result: containerID=1,
tansid=12, type=4

*May 29 16:05:48.184: VIRTUAL-SERVICE [utd]: cs response callback for 1, error=0
*May 29 16:05:48.188: VIRTUAL-SERVICE: cs callback addr info result, TxID 13
*May 29 16:05:48.188: VIRTUAL-SERVICE: convert_csnet_to_ipaddrlist: count 2

*May 29 16:05:48.188: VIRTUAL-SERVICE: csnet_to_ipaddrlist: Num intf 2

*May 29 16:05:48.188: VIRTUAL-SERVICE [utd]: Calling callback
*May 29 16:05:48.188: VIRTUAL-SERVICE [utd]: cs response callback for 3, error=0
*May 29 16:05:48.193: VIRTUAL-SERVICE: cs callback addr info result, TxID 14
*May 29 16:05:48.193: VIRTUAL-SERVICE: convert csnet to rtlist: route count: 2
*May 29 16:05:48.194: VIRTUAL-SERVICE [utd]: Calling callbackApp id : utd

Owner : ioxm
State : RUNNING
Application
Type : LXC
Name : UTD-Snort-Feature
Version : 1.0.13_SV2.9.16.1_XE17.3
Description : Unified Threat Defense
Path : /bootflash/secapp-utd.17.03.03.1.0.13_SV2.9.16.1_XE17.3.aarch64.tar
URL Path :
Activated profile name : low

Resource reservation
Memory : 1024 MB
Disk : 711 MB
CPU : 33 units
VCPU : 0

Attached devices
Type Name Alias
---------------------------------------------
Disk /tmp/xml/UtdIpsAlert-IOX
*May 29 16:05:48.194: VIRTUAL-SERVICE [utd]: cs response callback for 4, error=0
*May 29 16:05:48.194: VIRTUAL-SERVICE [utd]: Process status response message for virtual service
id (1)
*May 29 16:05:48.195: VIRTUAL-INSTANCE: Message sent for STATUS TDL response: Virtual service
name: u Disk /tmp/xml/UtdUrlf-IOX
Disk /tmp/xml/UtdTls-IOX
Disk /tmp/xml/UtdAmp-IOX
Watchdog watchdog-238.0
Disk /opt/var/core
Disk /tmp/HTX-IOX
Disk /opt/var
NIC ieobc_1 ieobc
Disk _rootfs
NIC dp_1_1 net3
NIC dp_1_0 net2
Serial/Trace serial3

Network interfaces
```

```
-------------------------------------
eth0:
MAC address : 54:e:0:b:c:2
Network name : ieobc_1
eth2:
MAC address : 78:c:f0:fc:88:6e
Network name : dp_1_0
eth1:
MAC address : 78:c:f0:fc:88:6f
IPv4 address : 192.0.2.2
Network name : dp_1_1

------------------------------------------------------------------------
Process Status Uptime # of restarts
------------------------------------------------------------------------
climgr UP 0Y 1W 3D 1:14:35 2
logger UP 0Y 1W 3D 1: 1:46 0
snort_1 UP 0Y 1W 3D 1: 1:46 0
Network stats:
eth0: RX packets:2352031, TX packets:2337575
eth1: RX packets:201, TX packets:236

DNS server:
nameserver 208.67.222.222
nameserver 208.67.220.220

Coredump file(s): lost+found

Interface: eth2
ip address: 192.0.2.2/30
Interface: eth1
ip address: 192.168.1.2/30

Address/Mask Next Hop Intf.
-------------------------------------------------------------------------------
0.0.0.0/0 192.0.2.1 eth2
0.0.0.0/0 192.168.1.1 eth1
```

Troubleshooting

1. Assure Cisco Integrated Services Router (ISR) runs XE 17.2.1r or above

2. Assure Cisco Integrated Services Router (ISR) is licensed with Security K9

3. Verify the ISR hardware model supports 8GB DRAM only

4. Confirm compatibility between IOS XE Software and UTD Snort IPS Engine Software (.tar file)
UTD file needs to match with IOS XE software, installation can fail for incompatibility

> **Note**: Software can be downloaded using the
> link: https://software.cisco.com/download/home/286315006/type

5. Confirm to activate and start UTD services using **iox** and **start** commands shown in step 2 under ***Configure*** section

6. Validate the resources assigned to UTD service using '***show app-hosting resource***' after Snort activation

```
Router#show app-hosting resource
CPU:
Quota: 33(Percentage)
Available: 0(Percentage)
VCPU:
Count: 2
Memory:
Quota: 3072(MB)
Available: 2048(MB)
Storage device: bootflash
Quota: 1500(MB)
Available: 742(MB)
```

7. After Snort activation, confirm ISR CPU and memory usage. You can use the command '***show app-hosting utilization appid utd***' to monitor UTD CPU, memory, and disk utilization

```
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
```

If you are able to see high memory, CPU, or Disk utilization, contact Cisco TAC.

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

```
debug virtual-service all
debug virtual-service virtualPortGroup
debug virtual-service messaging
debug virtual-service timeout
debug utd config level error [error, info, warning]
```

Related Information

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

Snort IPS

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_utd/configuration/xe-16-12/sec-data-utd-xe-16-12-book/snort-ips.pdf

Snort IPS on ISR, ISRv, and CSR - Step-By-Step Configuration

https://community.cisco.com/t5/security-documents/snort-ips-on-isr-isrv-and-csr-step-by-step-configuration/ta-p/3369186

Snort IPS Deployment Guide

https://www.cisco.com/c/en/us/products/collateral/security/router-security/guide-c07-736629.html#_Toc442352480