在集成多业务路由器1000系列上部署Snort IPS

目录

简介

本文档介绍如何在思科集成多业务路由器(ISR)1000系列上部署Snort IPS功能。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科集成多业务路由器1000系列
- 基本XE-IOS命令
- 基本Snort知识

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行17.03.03版本的C111X-8P
- 用于17.3.3版本的UTD引擎TAR
- ISR1k上需要安全K9许可证
- 需要签名订用1年或3年
- XE 17.2.1r及以上版本
- 仅支持8GB DRAM的ISR硬件型号

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

Snort IPS功能可为Cisco 4000系列集成多业务路由器(ISR)、Cisco 1000系列集成多业务路由器（XPID，如1111X、11）上的分支机构启用入侵防御系统(IPS)或入侵检测系统(IDS)21X、1161X等，仅支持8GB DRAM)和思科云服务路由器1000v系列。此功能使用Snort引擎提供IPS和IDS功能。

Snort是一种开源网络IPS，可执行实时流量分析，并在IP网络上检测到威胁时生成警报。它还可以执行协议分析、内容搜索或匹配，并检测各种攻击和探测，如缓冲区溢出、隐藏端口扫描等。Snort IPS功能在提供IPS或IDS功能的网络入侵检测和防御模型中起作用。在网络入侵检测和防御模式下，Snort执行以下操作

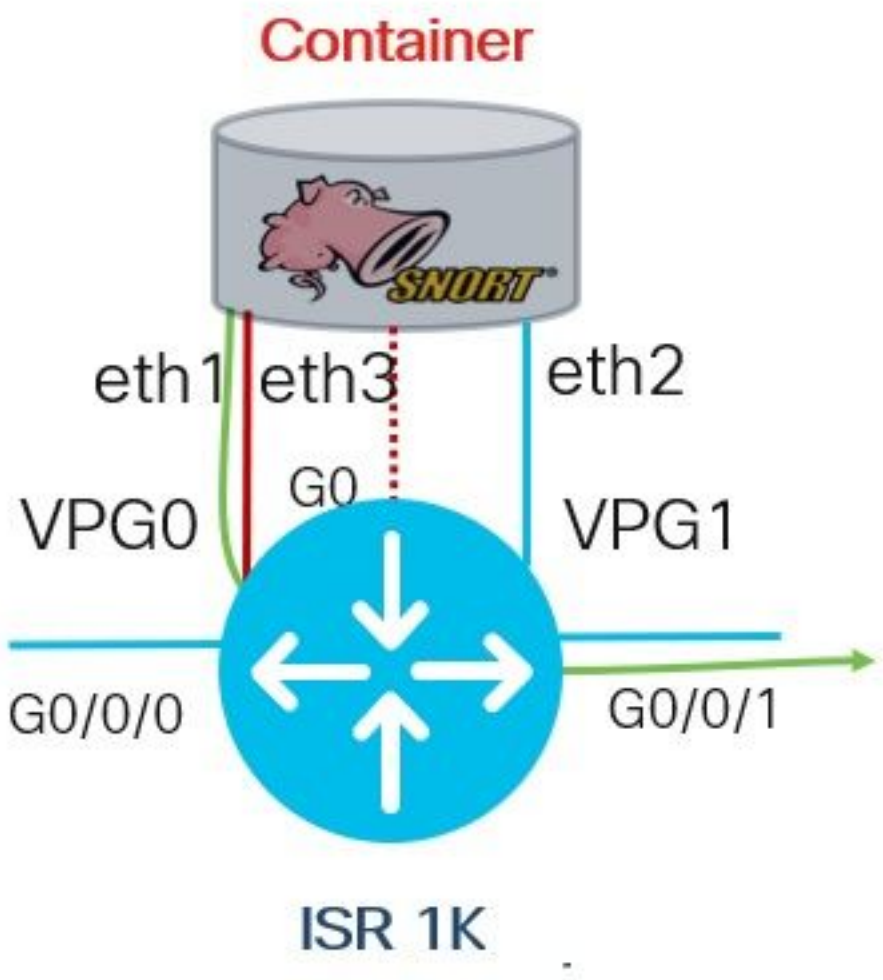
- 监控网络流量并根据定义的规则集进行分析
- 执行攻击分类
- 根据匹配的规则调用操作

根据要求，Snort可以在IPS或IDS模式下启用。在IDS模式下，Snort会检查流量并报告警报，但不会采取任何措施来防止攻击。在IPS模式下，除入侵检测外，还会采取措施防止攻击。Snort IPS监控流量，并向外部日志服务器或IOS系统日志报告事件。启用IOS系统日志记录可能会因日志消息的潜在数量而影响性能。支持Snort日志的外部第三方监控工具可用于日志收集和分析。

在思科集成多业务路由器(ISR)上配置Snort IPS的主要方法有两种：VMAN方法和IOx方法。VMAN方法使用utd.ova文件，而IOx使用utd.tar文件。IOx是在思科集成多业务路由器(ISR)1000系列上部署Snort IPS的正确方法。

Snort IPS可部署在带XE 17.2.1r及更高版本的思科集成多业务路由器(ISR)1k系列上。

网络图



配置

步骤1.配置端口组

```
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
```

步骤2.激活虚拟服务、配置和提交更改

```
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
```

步骤3.配置虚拟服务

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

步骤4.配置UTD（服务平面）

```
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
```

注意： 注意：***威胁防***护使Snort成为IPS，***威胁检***测使Snort成为IDS。

步骤5.配置UTD（数据平面）

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

注意:*fail open是默认设置。*

验证

检验端口组IP地址和接口状态

```
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
```

检验端口组配置

```
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
!
```

验证虚拟服务配置

```
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
```

注意：确保存*在*start命令，否则不会启动激活。

验证虚拟服务激活。

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

注意：*iox将*激活虚拟服务。

检验UTD配置（服务平面和数据平面）

```
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
```

验证应用托管状态

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

使用详细信息验证应用托管状态

```
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
```

故障排除

1.确保思科集成多业务路由器(ISR)运行XE 17.2.1r或更高版本

2.确保思科集成多业务路由器(ISR)已通过安全K9获得许可

3.验证ISR硬件型号是否仅支持8GB DRAM

4.确认IOS XE软件与UTD Snort IPS引擎软件（.tar文件）之间的兼容性UTD文件需要与IOS XE软件匹配，安装可能会因不兼容而失败

> **注意：**可使用以下链接下载软件：https://software.cisco.com/download/home/286315006/type

5.确认使用“配置”部分第2步中**显示的**iox和**start**命令激活和启动UTD***服务***

6.在Snort激活后，使用“show app-hosting resource”验***证分配给UTD服务***的资源

```
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.激活Snort后，确认ISR CPU和内存的使用情况。您可以使用命令***show app-hosting utilization appid utd***监控UTD CPU、内存和磁盘利用率

```
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
```

如果您能够看到内存、CPU或磁盘使用率较高，请联系Cisco TAC。

8.在发生故障时，使用下面列出的命令收集Snort IPS部署信息：

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

相关信息

有关Snort IPS部署的其他文档，请访问：

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

ISR、ISRv和CSR上的Snort IPS — 分步配置

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

Snort IPS部署指南

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