在整合多業務路由器1000系列上部署Snort IPS

目錄

簡介

本檔案介紹如何在思科整合式服務路由器(ISR)1000系列上部署Snort IPS功能。

必要條件

需求

思科建議您瞭解以下主題：

- 思科整合式服務路由器1000系列
- 基本XE-IOS命令
- 基本Snort知識

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 運行17.03.03版的C111X-8P
- 用於17.3.3版的UTD引擎TAR
- ISR1k上需要安全K9許可證
- 簽名訂用1年或3年
- XE 17.2.1r及更高版本
- 僅支援8 GB DRAM的ISR硬體型號

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

Snort IPS功能支援在Cisco 4000系列整合多業務路由器(ISR)、Cisco 1000系列整合多業務路由器（X PID，如1111X、1121X、1161X等，僅支援8 GB DRAM）和Cisco Cloud Services Router 1000v系列上為分支機構部署入侵防禦系統(IPS)或入侵檢測系統(IDS)。此功能使用Snort引擎提供IPS和IDS功能。

Snort是一種開源網路IPS，用於執行即時流量分析，並在IP網路上檢測到威脅時生成警報。它還可以執行協定分析、內容搜尋或匹配，並檢測各種攻擊和探測，如緩衝區溢位、隱身埠掃描等。Snort IPS功能可在提供IPS或IDS功能的網路入侵檢測和防禦模型中工作。在網路入侵檢測和防禦模式下，Snort執行以下操作

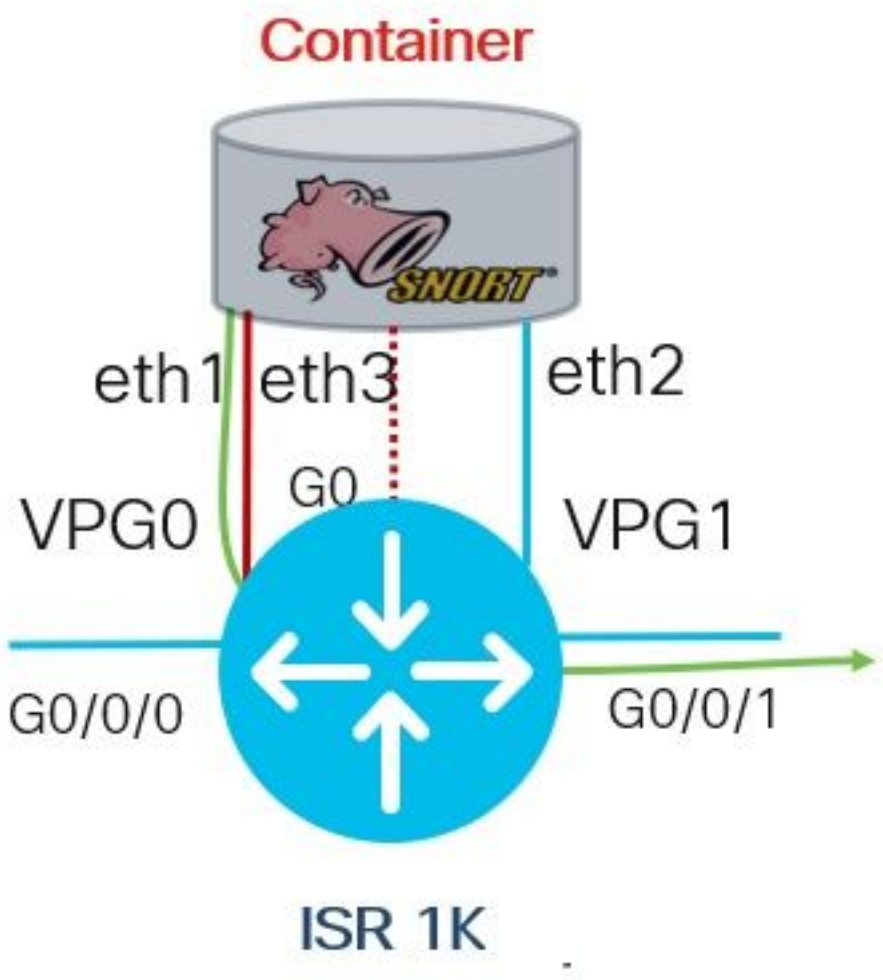
- 監控網路流量並根據定義的規則集進行分析
- 執行的攻擊分類
- 根據匹配的規則呼叫操作

根據要求，可在IPS或IDS模式下啟用Snort。在IDS模式下，Snort會檢查流量並報告警報，但不會採取任何操作來防止攻擊。在IPS模式中，除了入侵檢測，還要採取防範攻擊的措施。Snort IPS會監控流量並將事件報告給外部日誌伺服器或IOS系統日誌。啟用日誌記錄到IOS系統日誌可能會影響效能，因為日誌消息數量可能很大。支援Snort日誌的外部第三方監視工具可用於日誌收集和分析。

在Cisco整合多業務路由器(ISR)上配置Snort IPS主要有兩種方法，即VMAN方法和IOx方法。VMAN方法使用utd.ova檔案，而IOx使用utd.tar檔案。IOx是在思科整合多業務路由器(ISR)1000系列上部署Snort IPS的正確方法。

Snort IPS可以部署在Cisco Integrated Services Routers(ISR)1000系列和XE 17.2.1r及更高版本上。

網路圖表



設定

步驟1.配置埠組

```
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
```

步驟2.啟用虛擬服務，配置並提交更改

```
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
```

步驟3.配置虛擬服務

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

步驟4.設定UTD（服務平面）

```
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
```

附註： 附註：***威脅防護***將Snort啟用為IPS，威***脅檢測***將Snort啟用為IDS。

步驟5.設定UTD（資料平面）

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

附註:附註：***預設設置為失效開放。***

驗證

檢驗埠組IP地址和介面狀態

```
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
```

驗證埠組配置

```
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
!
```

驗證虛擬服務配置

```
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
```

附註：確保***start***命令存在，否則啟用不會啟動。

驗證虛擬服務啟用。

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

附註：***iox*** **將啟用虛擬服務。**

驗證UTD配置（服務平面和資料平面）

```
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
```

驗證應用託管狀態

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

使用詳細資訊驗證應用託管狀態

```
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
```

疑難排解

1.確保思科整合服務路由器(ISR)運行XE 17.2.1r或更高版本

2.確保思科整合多業務路由器(ISR)獲得安全許可K9

3.驗證ISR硬體型號僅支援8GB DRAM

4.確認IOS XE軟體與UTD Snort IPS引擎軟體（.tar檔案）之間的相容性UTD檔案需要與IOS XE軟體匹配，安裝可能會因不相容性而失敗

> **附註**：可以使用以下連結下載軟體
> ：https://software.cisco.com/download/home/286315006/type

5.確認使用**Configure**部分中步驟2中所示的**iox**和**start**命令啟用和啟動UTD服務

6.在Snort啟用後使用「***show app-hosting resource***」驗證***分配給UTD服***務的資源

```
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.啟用Snort後，請確認ISR CPU和記憶體使用情況。您可以使用命令***show app-hosting utilization appid utd***來監控UTD CPU、記憶體和磁碟利用率

```
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
```

如果您能看到高記憶體、CPU或磁碟利用率，請與Cisco TAC聯絡。

8.使用下列命令收集Snort IPS部署資訊，以防出現故障：

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

相關資訊

在以下位置可以找到與Snort IPS部署相關的其他文檔：

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 — 逐步配置

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