

在思科集成多业务路由器4000系列上部署Snort IPS

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[网络图](#)

[配置](#)

[平台UTD配置](#)

[服务平面和数据平面配置。](#)

[验证](#)

[故障排除](#)

[调试](#)

[相关信息](#)

简介

本文档介绍如何使用IOx方法在Cisco集成多业务路由器(ISR)4000系列上部署Snort IPS和Snort IDS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4000系列，至少带8GB DRAM。
- 基本IOS-XE命令体验。
- Snort基础知识。
- 1年或3年的签名订用是必需的
- IOS-XE 16.10.1a及更高版本。

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17.9.3a版本的ISR4331/K9。
- 用于17.9.3a版本的UTD引擎TAR。

- Securityk9许可证，适用于ISR4331/K9。

VMAN方法现在已弃用。

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功能为思科4000系列集成多业务路由器和Cisco云服务路由器1000v系列上的分支机构启用入侵防御系统(IPS)或入侵检测系统(IDS)。此功能使用开源Snort启用IPS和IDS功能。

Snort是一个开源IPS，它会执行实时流量分析，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、内容研究或行进，并检测各种攻击和探测，例如缓冲区溢出、隐藏端口扫描等。

Snort引擎作为虚拟容器服务在思科集成多业务路由器4000系列和云服务路由器1000v系列上运行。

Snort IPS功能可作为网络入侵检测或防御模式，在思科集成服务路由器4000系列和云服务路由器1000v系列上提供IPS或IDS功能。

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

根据网络要求。Snort IPS可以作为IPS或IDS启用。在IDS模式下，Snort会检查流量并报告警报，但不会采取任何操作来防止攻击。在IPS模式下，检测流量并报告警报（与IDS一样），但会采取措施防止攻击。

Snort IPS作为ISR路由器上的服务运行。服务容器使用虚拟化技术在思科设备上为应用提供托管环境。Snort流量检测在每个接口上启用，或者在所有支持的接口上全局启用。Snort传感器需要两个VirtualPortGroup接口。第一个VirtualPortGroup用于管理流量，第二个VirtualPortGroup用于转发平面和Snort虚拟容器服务之间的数据流量。必须为这些VirtualPortGroup接口配置IP地址。分配给管理VirtualPortGroup接口的IP子网应该能够与签名服务器和警报/报告服务器通信。

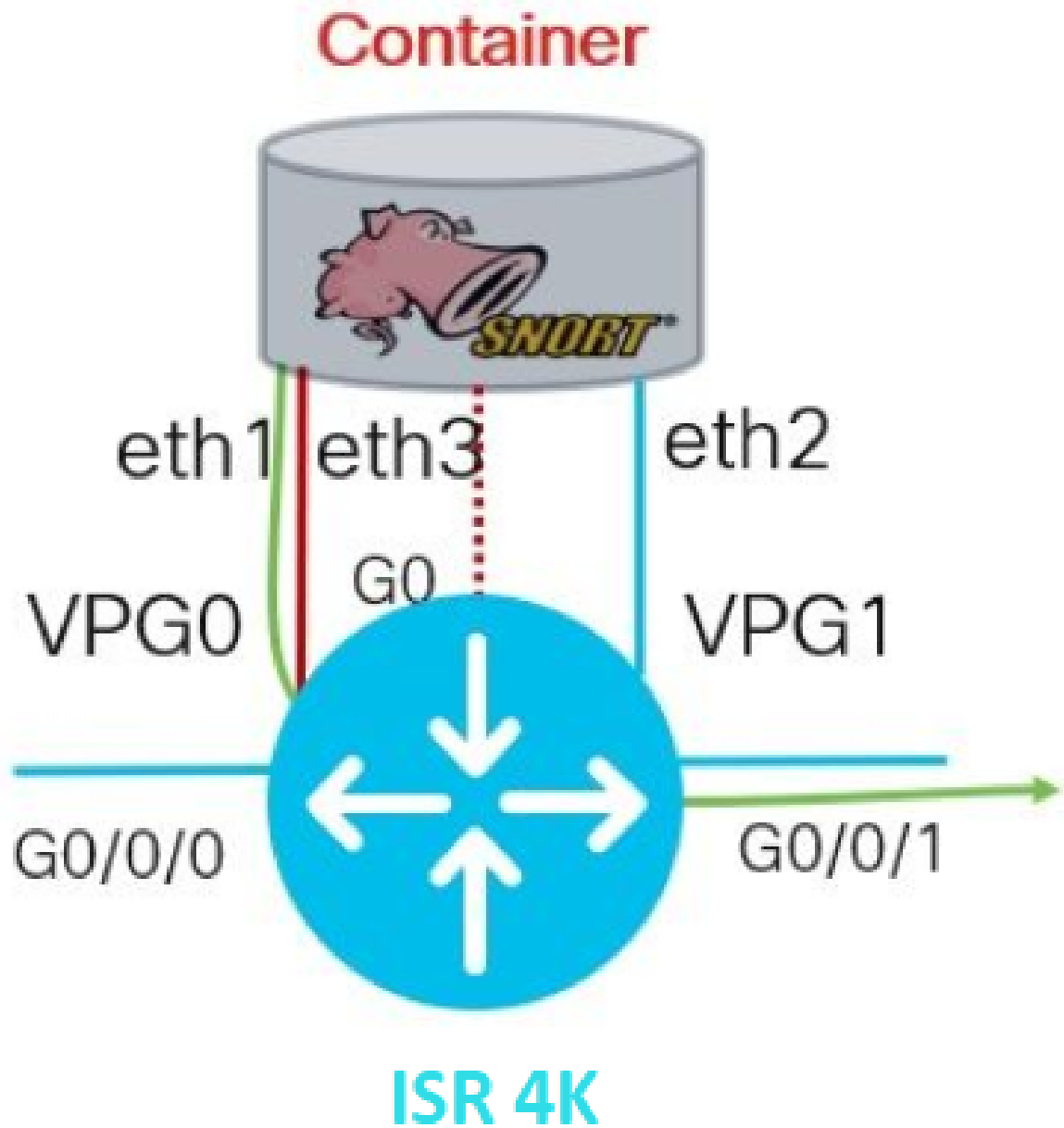
Snort IPS监控流量并向外部日志服务器或IOS系统日志报告事件。启用登录IOS系统日志可能会由于日志消息的数量而影响性能。支持Snort日志的外部第三方监控工具可用于日志收集和分析。

Cisco 4000系列集成多业务路由器和Cisco Cloud Services Router 1000v系列上的Snort IPS基于签名软件包下载。订用有两种类型：

- 社区签名包。
- 基于用户的签名包。

社区签名包规则集提供有限的威胁覆盖范围。基于用户的签名包规则集提供针对威胁的最佳保护。它包括在攻击发生之前提供保护，并且还提供对更新签名的快速访问，以响应安全事件或主动发现新威胁。思科完全支持此订用，并将在Cisco.com上更新该软件包。签名软件包可以从software.cisco.com下载。Snort签名信息可在snort.org上找到。

网络图



配置

平台UTD配置

步骤1:配置虚拟VirtualPortGroups接口。

```
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
```

步骤2.在全局配置模式下启用IOx环境。

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


第三步：使用vnic配置配置应用托管。

```
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
```


第 4 步 (可选) : 配置资源配置文件。

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

 注意：如果未定义此配置，系统将使用默认的应用资源配置（低）。如果要更改默认配置文件配置，请确保在ISR上有足够的可用资源。

第五步：使用UTD.tar文件安装应用托管。

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

 注意：在bootflash：上保留正确的UTD.tar文件，以继续安装。在UTD文件名上指定Snort版本。


应看到指示正确安装UTD服务的下一系统日志。

```
Installing package 'bootflash:iox-iosxe-utd.16.12.08.1.0.24_SV2.9.16.1_XE16.12.08.1.0.24'
*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 v
*Jun 26 19:25:53.176: %IM-6-INSTALL_MSG: R0/0: ioxman: app-hosting: Install su
```

 注意：使用“show app-hosting list”时，状态应为“Deployed”

第六步：启动应用托管服务。

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


 注意：启动应用托管服务后，应用托管状态应为“Running”。使用“show app-hosting list”或“show app-hosting detail”查看更多详细信息。

应该看到下一条syslog消息，指示UTD服务已正确安装。

```
*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
```

服务平面和数据平面配置。

成功安装后，必须配置服务平面。Snort IPS可配置为用于检查的入侵防御系统(IPS)或入侵检测系统(IDS)。

 警告：确认已启用“securityk9”许可证功能，以继续执行UTD服务平面配置。

步骤1:配置统一威胁防御(UTD)标准引擎 (服务平面)

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

第二步：启用将紧急消息记录到远程服务器。

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

第三步：为Snort引擎启用威胁检测。

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

第四步：将威胁检测配置为入侵防御系统(IPS)或入侵检测系统(IDS)

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



注：“Protection”用于IPS，“Detection”用于IDS。“Detection”是默认设置。

第五步：配置安全策略。

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



注：默认策略为“balanced”

第6步（可选）：创建UTD允许的列表（白名单）

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

第7步（可选）：配置Snort签名ID以显示在白名单中。

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




注：以ID“40”为例。要检查Snort签名信息，请检查Snort官方文档。


第 8 步 (可选) : 在威胁检测配置上启用允许列表。

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

步骤 9配置签名更新间隔以自动下载Snort签名。


```
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
```

 注：第一个数字以24小时格式定义小时，第二个数字表示分钟。

 警告：UTD签名更新会在更新时生成短暂的服务中断。

步骤 10配置签名更新服务器参数。

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

 注意：使用“cisco”使用思科服务器或“url”定义更新服务器的自定义路径。对于Cisco服务器，您必须提供自己的用户名和密码。

步骤 11启用日志级别。


```
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
```

步骤 12启用utd服务。

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

第 13 步 (可选) : 将数据流量从VirtualPortGroup接口重定向到UTD服务。

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

 注：如果未配置重定向，则自动检测重定向。

步骤 14对ISR上的所有第3层接口启用UTD。

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

步骤 15启用引擎标准。


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

应该看到下一条syslog消息，指示UTD已正确启用。

```
*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
```

第 16 步 (可选) : 定义UTD引擎故障的操作 (UTD数据平面)

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

 注意:当UTD引擎发生故障时，“故障关闭”选项会丢弃所有IPS/IDS流量。“失效开放”选项允许在UTD故障时所有IPS/IDS流量。默认选项为“fail open”。

验证

检验VirtualPortGroups IP地址和接口状态。

```
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
```

验证VirtualPortGroup配置。

```
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
!
```

验证应用托管配置。

```
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 192.168.2.2 netmask 255.255.255.252
start
end
```

检验iox激活。

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

检验UTD服务平面配置。

```
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

验证应用托管状态。

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

验证应用托管详细信息。

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/UtdUr1f-IOX

Disk /tmp/xml/UtdT1s-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
```


故障排除

1. 确保思科集成多业务路由器(ISR)运行XE 16.10.1a及更高版本 (适用于IOx方法)
2. 确保思科集成多业务路由器(ISR)获得许可，并启用Securityk9功能。
3. 验证ISR硬件模式是否符合最低资源配置文件。
4. 与基于区域的防火墙SYN-cookie和网络地址转换64(NAT64)不兼容的功能
5. 确认安装后已启动UTD服务。
6. 在手动下载签名软件包期间，请确保软件包的版本与Snort引擎版本相同。如果版本不匹配，签名包更新可能会失败。
7. 如果出现性能问题，请使用show app-hosting resource和show app-hosting utilization appid "UTD-NAME"了解有关CPU/内存/存储完善的信息。

```
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
```

 **警告**：如果您能看到高CPU、内存或磁盘使用率，请联系思科TAC。

调试

使用下面列出的debug命令在出现故障时收集Snort IPS信息。

```
<#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
```

相关信息

有关Snort IPS部署的其他文档，请访问以下网址：

Snort IPS安全配置指南

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

虚拟服务资源配置文件

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

路由器上的Snort IPS — 逐步配置。

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

Snort IPS故障排除

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未部署，因为硬件没有足够的平台资源

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

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。