

在思科整合多業務路由器4000系列上部署Snort IPS

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[網路圖表](#)

[設定](#)

[平台UTD配置](#)

[服務平面和資料平面配置。](#)

[驗證](#)

[疑難排解](#)

[調試](#)

[相關資訊](#)

簡介

本文說明如何使用IOx方法在Cisco整合多業務路由器(ISR)4000系列上部署Snort IPS和Snort IDS功能。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco Integrated Services Routers 4000系列，至少具有8GB DRAM。
- 基本IOS-XE命令體驗。
- 基本Snort知識。
- 1年或3年的簽名訂閱是必需的
- IOS-XE 16.10.1a及更高版本。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 運行17.9.3a版本的ISR4331/K9。
- 用於17.9.3a版的UTD引擎TAR。

- ISR4331/K9的SecurityK9許可證。

VMAN方法現在已棄用。

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功能為思科4000系列整合服務路由器和Cisco Cloud Services Router 1000v系列上的分支機構啟用入侵防禦系統(IPS)或入侵檢測系統(IDS)。此功能使用開源Snort啟用IPS和IDS功能。

Snort是一種開源IPS，它執行即時流量分析，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、內容搜尋或行進，並檢測各種攻擊和探測，如緩衝區溢位、隱藏埠掃描等。Snort引擎在思科整合多業務路由器4000系列和雲服務路由器1000v系列上作為虛擬容器服務運行。

Snort IPS功能可作為網路入侵檢測或防禦模式，在Cisco Integrated Services Routers 4000系列和Cloud Services Router 1000v系列上提供IPS或IDS功能。

- 監控網路流量並根據定義的規則集進行分析。
- 執行附加分類。
- 根據匹配的規則呼叫操作。

基於網路要求。Snort IPS可以作為IPS或IDS啟用。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，會像IDS一樣檢查流量並報告警報，但會採取措施來防止攻擊。

Snort IPS作為ISR路由器的服務運行。服務容器使用虛擬化技術為應用提供思科裝置上的託管環境。Snort流量檢測在每個介面上啟用，或在所有支援的介面上全域性啟用。Snort感測器需要兩個VirtualPortGroup介面。第一個VirtualPortGroup用於管理流量，第二個VirtualPortGroup用於轉發平面和Snort虛擬容器服務之間的資料流量。必須為這些VirtualPortGroup介面配置IP地址。分配給管理VirtualPortGroup介面的IP子網應能夠與特徵碼伺服器 and 警報/報告伺服器通訊。

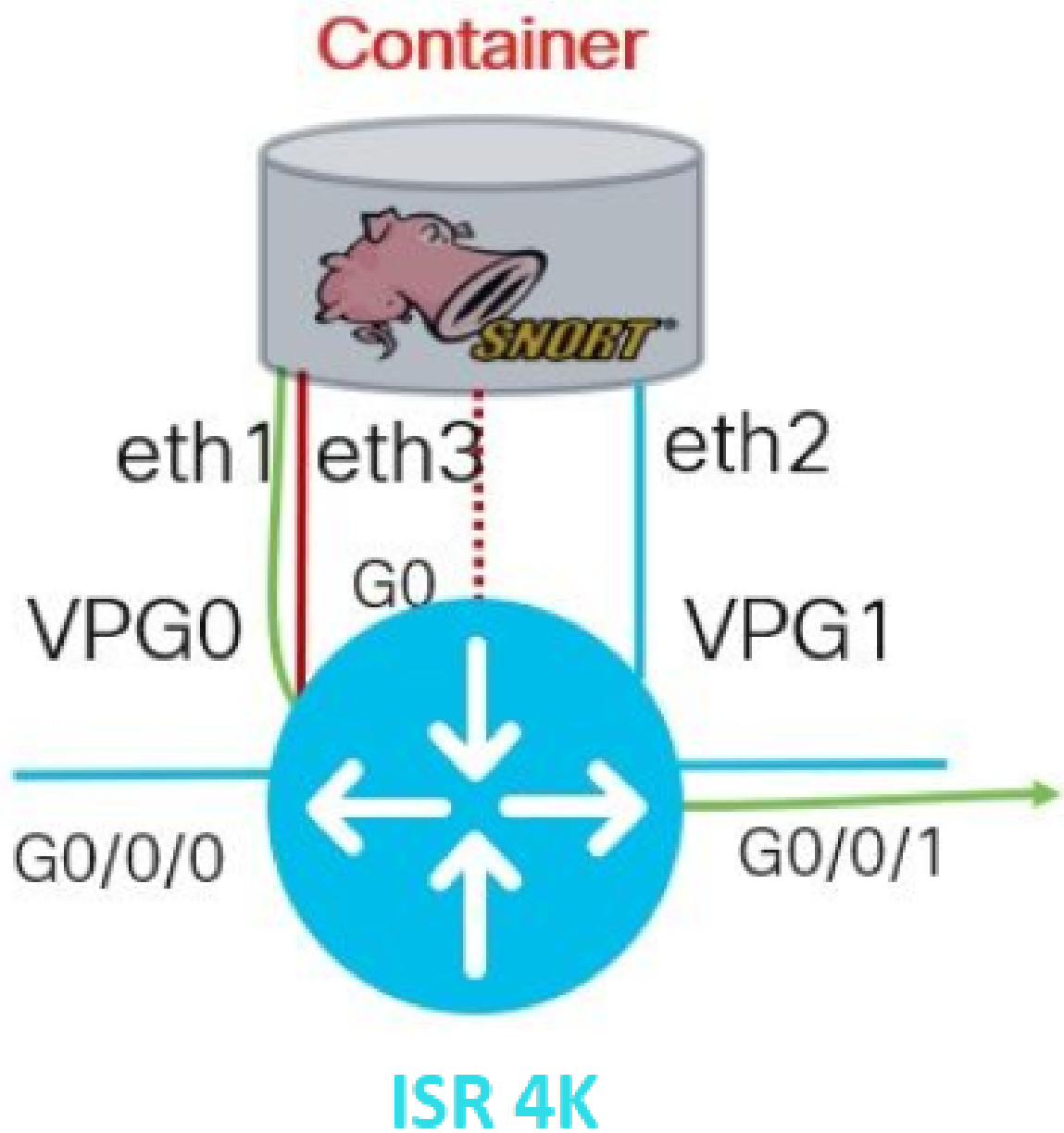
Snort IPS會監控流量並將事件報告給外部日誌伺服器或IOS系統日誌。啟用登入到IOS系統日誌可能會影響效能，因為日誌消息數量可能很大。支援Snort日誌的外部第三方監視工具可用於日誌收集和分析。

Cisco 4000系列整合服務路由器和Cisco Cloud Services Router 1000v系列上的Snort IPS基於特徵碼包下載。有兩種型別的預訂：

- 社群簽名包。
- 基於使用者的簽名包。

社群簽名包規則集提供有限的威脅覆蓋範圍。基於使用者的特徵碼包規則集提供了抵禦威脅的最佳保護。它包括在攻擊前提供保護，還可以為響應安全事件或主動發現新威脅提供最快的對更新特徵碼的訪問。思科完全支援此訂閱，並將在Cisco.com上更新該包。簽名包可以從software.cisco.com下載。Snort簽名資訊可在snort.org上找到。

網路圖表



設定

平台UTD配置

步驟 1. 配置虛擬VirtualPortGroups介面。

```
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
```

步驟2.在全域性配置模式下啟用IOx環境。

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


步驟 3.使用vnic配置配置應用託管。

```
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
```


步驟4 (可選)。配置資源配置檔案。

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

 附註：如果未定義該屬性，系統將使用預設的app-resource config(Low)。如果要更改預設配置檔案配置，請確保在ISR上有足夠的可用資源。

步驟 5.使用UTD.tar檔案安裝應用託管。

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

 註：在bootflash：中保留正確的UTD.tar檔案，以繼續安裝。在UTD檔名上指定了Snort版本。


應看到下一組系統日誌，指示UTD服務已正確安裝。

```
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」時狀態應為「Deployed」

步驟 6. 啟動應用託管服務。

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


 注意：啟動應用託管服務後，應用託管狀態應為「正在運行」。使用「show app-hosting list」或「show app-hosting detail」檢視更多詳細資訊。

應看到下一條syslog消息，指示UTD服務已正確安裝。

```
*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
```

服務平面和資料平面配置。

成功安裝後，必須配置服務平面。Snort IPS可配置為用於檢查的入侵防禦系統(IPS)或入侵檢測系統(IDS)。

 警告：確認「securityk9」許可證功能已啟用，以繼續UTD服務平面配置。

步驟 1. 配置統一威脅防禦(UTD)標準引擎 (服務平面)

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

步驟 2. 啟用將緊急消息記錄到遠端伺服器。

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

步驟 3. 為Snort引擎啟用威脅檢測。

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


步驟 4. 將威脅檢測配置為入侵防禦系統(IPS)或入侵檢測系統(IDS)

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

 註: 「Protection」用於IPS, 「Detection」用於IDS。「Detection」是默認設定。

步驟 5. 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
```

 註: 預設策略為「balanced」

步驟6 (可選)。建立UTD允許的清單 (白名單)

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

第7步 (可選)。配置Snort簽名ID以顯示在白名單中。

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


 註：以ID「40」為例。要檢查Snort簽名資訊，請檢查Snort官方文檔。

第8步（可選）。啟用威脅檢測配置上的允許清單。

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

步驟 9. 配置特徵碼更新間隔以自動下載Snort特徵碼。


```
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
```

 註：第一個數字以24小時格式定義小時，第二個數字表示分鐘。

 警告：UTD簽名更新會在更新時生成一個短暫的服務中斷。

步驟 10. 配置簽名更新伺服器引數。

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

 注意：使用「cisco」使用Cisco伺服器，或「url」定義更新伺服器的自定義路徑。對於Cisco伺服器，您必須提供自己的使用者名稱和密碼。

步驟 11. 啟用日誌記錄級別。

```
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
```


步驟 12. 啟用utd服務。

```
Router#configure terminal
```

```
Router(config)#utd
```

步驟13 (可選)。將資料流量從VirtualPortGroup介面重定向到UTD服務。

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

 註：如果未配置重定向，則自動檢測到重定向。

步驟 14.對ISR上的所有第3層介面啟用UTD。

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

步驟 15.啟用引擎標準。


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

應看到下一條syslog消息，指示UTD已正確啟用。

```
*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 (可選)。定義UTD引擎故障的操作 (UTD資料平面)

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

 注意:當UTD引擎發生故障時，「失效關閉」選項將丟棄所有IPS/IDS流量。「失效開放」選項允許在UTD故障時所有IPS/IDS流量。預設選項為「fail open」。

驗證

驗證VirtualPortGroups IP地址和介面狀態。

```
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
```

驗證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
!
```

驗證應用託管配置。

```
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
```

驗證iox啟用。

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

驗證UTD服務平面配置。

```
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

驗證應用託管狀態。

```
Router#show app-hosting list
```

App id	State
-----	-----
UTD	RUNNING

驗證應用託管詳細資訊。

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/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
-----
```

```
c_limgr 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
```

疑難排解

1. 確保思科整合服務路由器(ISR)運行XE 16.10.1a及更高版本 (用於IOx方法)
2. 確保思科整合多業務路由器(ISR)在啟用SecurityK9功能的情況下獲得許可。
3. 驗證ISR硬體模型符合最低資源配置檔案。
4. 與基於區域的防火牆SYN-cookie和網路地址轉換不相容的功能64(NAT64)
5. 確認安裝後已啟動UTD服務。
6. 在手動下載特徵碼包期間，確保包與Snort引擎版本相同。如果版本不匹配，簽名包更新可能會失敗。
7. 如果出現效能問題，請使用「show app-hosting resource」和「show app-hosting utilization appid "UTD-NAME"」瞭解有關CPU/記憶體/儲存完善的資訊。

```
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**：如果您能夠看到高CPU、記憶體或磁碟使用率，請與Cisco TAC聯絡。

調試

使用下面列出的debug命令在出現故障時收集Snort IPS資訊。

```
<#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安全配置指南

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

虛擬服務資源配置檔案

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_utd/configuration/xs-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>

疑難排解Snort IPS

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

ISR4K Snort IPS未部署，因為硬體沒有足夠的平台資源

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

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。