نشر نظام منع التسلل (IPS) على سلسلة موجهات الخدمات المدمجة 4000 من Cisco

المحتويات

المقدمة

يوضح هذا المستند كيفية نشر ميزة Snort IPS و Snort IDS على سلسلة موجهات الخدمات المتكاملة (ISR) 4000 من Cisco باستخدام طريقة IOx.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- سلسلة موجهات الخدمات المدمجة طراز 4000 من Cisco مع ذاكرة DRAM سعة 8 جيجابايت على الأقل.
- تجربة أوامر IOS-XE الأساسية.
- معرفة الشخ الأساسية.
- يلزم اشتراك في التوقيع لمدة سنة أو ثلاث سنوات
- IOS-XE 16. 10. 1a أو أعلى.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- ISR4331/K9 يشغل الإصدار 17.9.3a.

- محرك UTD TAR لإصدار 17.9.3a.
- ترخيص SecurityTYK9 لـ ISR4331/K9.

أسلوب VMAN مهم لمآلا.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

تتيح ميزة نظام منع التسلل (IPS) أو نظام اكتشاف الاقتحام (IDS) للمكاتب الفرعية 1000V وموجه خدمات السحابة Cisco 4000 Series وموجهات الخدمات المتكاملة من السلسلة Cisco 4000 Series. تستخدم هذه الميزة الشنخ مفتوح المصدر لتمكين إمكانيات IPS و IDS.

SNORT هو برنامج IPS مفتوح المصدر يقوم بإجراء تحليل حركة مرور البيانات في الوقت الفعلي وإنشاء تنبيهات عند اكتشاف التهديدات على شبكات IP. كما يمكنه إجراء تحليل للبروتوكول والبحث عن المحتوى أو مسيرته واكتشاف مجموعة متنوعة من الهجمات والمستكشفات، مثل تجاوز سعة التخزين المؤقت وتصوير منافذ التخفي وما إلى ذلك. يعمل محرك الشبكة خدمة حاوية افتراضية على سلسلة موجهات الخدمات المدمجة 4000 من Cisco وموجه خدمات السحابة 1000V من Cisco.

تعمل ميزة نظام منع التسلل (IPS) على أنها وضع اكتشاف إقتحام الشبكة أو الوقاية من، كما توفر إمكانات نظام منع التسلل (IPS) أو نظام اكتشاف الاقتحام (IDS) على موجهات الخدمات المدمجة طراز 4000 من Cisco وموجه خدمات السحابة طراز 1000V من Cisco.

- يراقب حركة مرور الشبكة ويحلل مقابل مجموعة قواعد محددة.
- تنفيذ تصنيف الإرفاق.
- إستدعاء الإجراءات مقابل القواعد المتطابقة.

استنادا إلى متطلبات الشبكة. يمكن تمكين Snort IPS كمعرفات أو IPS. في وضع IDS، يتفحص الشوت حركة المرور ويبلغ عن التنبيهات، لكنه ال يتخذ أي إجراء لمنع الهجمات. في وضع IPS يقوم بفحص حركة المرور ويقدم تقارير عن التنبيهات كما تفعل المعرفات ولكن يتم إتخاذ إجراءات لمنع الهجمات.

يتم تشغيل Snort IPS كخدمة على موجهات ISR. تستخدم حاويات الخدمات تقنية المحاكاة الافتراضية لتوفير بيئة مضيفة على أجهزة Cisco للتطبيقات. يتم تمكين فحص حركة مرور البيانات إما على أساس كل واجهة أو بشكل عام على جميع الواجهات المدعومة. يتطلب مستشعر Snort واجهات VirtualPortGroup. يتم إستخدام مجموعة VirtualPort الأولى لحركة مرور البيانات الإدارية والثانية لحركة مرور البيانات بين مستوى إعادة التوجيه وخدمة الحاوية الظاهرية Snort. يجب تكوين عناوين IP التخمينية لواجهات VirtualPortGroup هذه. يجب أن تكون شبكة IP الفرعية التي تم تعيينها لواجهة VirtualPortGroup الخاصة بالإدارة قادرة على الاتصال بخادم التوقيع وخادم التنبيه/التقارير.

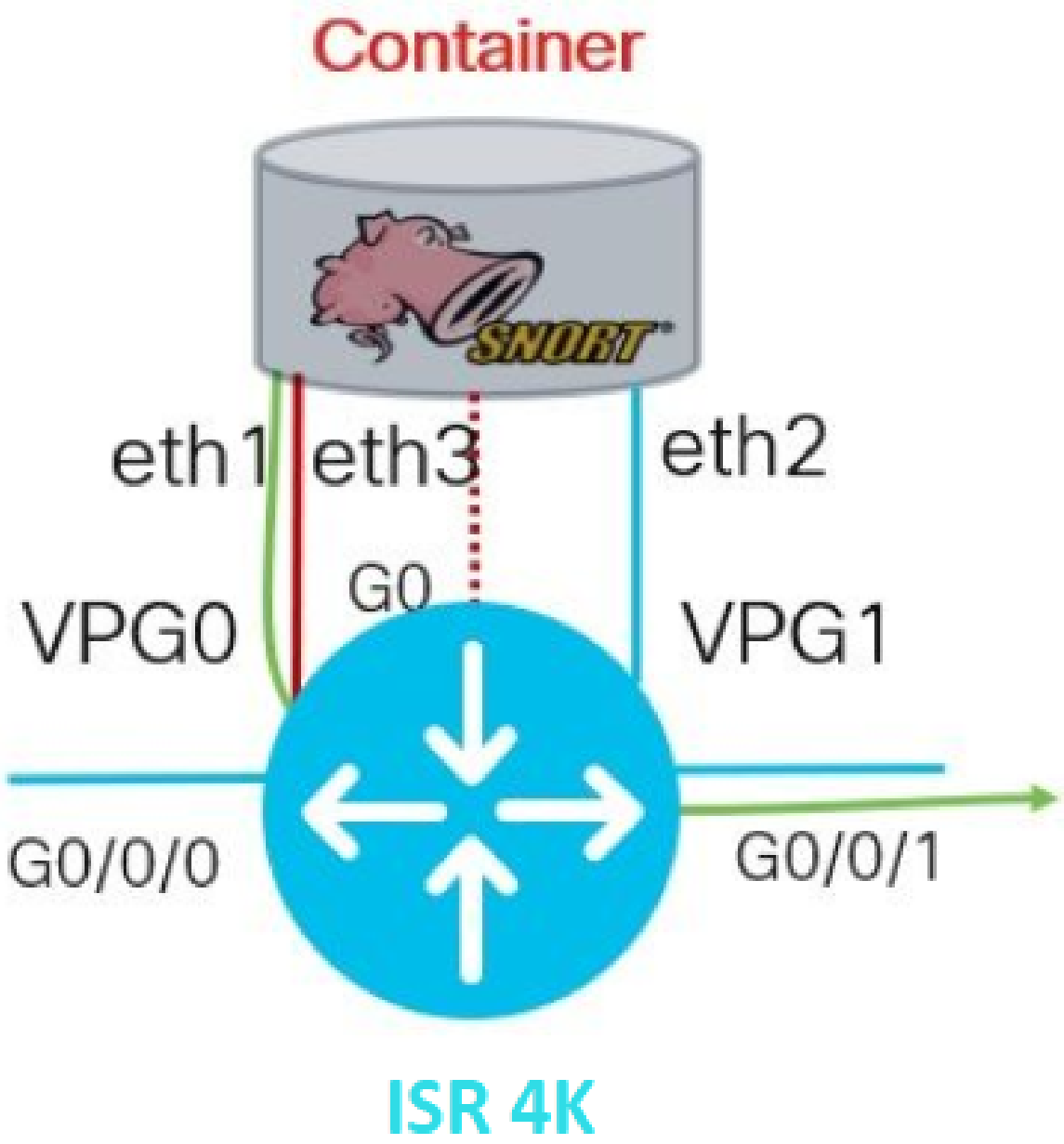
يراقب الـ snort IPS الحركة مرور ويبلغ حادث إلى خارجي سجل دان لـ أو الـ ios syslog. قد يؤثر تمكين تسجيل الدخول إلى نظام IOS على الأداء بسبب الحجم المحتمل لرسائل السجل. يمكن إستخدام أدوات المراقبة الخارجية التابعة لجهة خارجية، والتي تدعم سجالت SNORT، لجمع السجالت وتحليلها.

يعتمد IPS على موجهات الخدمات المتكاملة Cisco 4000 Series Integrated Services Router 1000V Series من Cisco Cloud Services Router على تنزيل حزمة التوقيع. هناك نوعان من الاشتراكات:

- حزمة توقيع المجتمع.
- حزمة التوقيع المستندة إلى المشترك.

توفر مجموعة قواعد حزمة توقيع المجتمع تغطية محدودة ضد التهديدات. توفر مجموعة قواعد حزمة التوقيع المستندة إلى المشترك أفضل حماية ضد التهديدات. كما يشمل تغطية عمليات التفجير قبل وقوعها، كما يوفر أسرع وصول إلى التوقيعات المحدثة در على حداث أمني وأ الاكتشاف الاستباقي لتهديد جديد. يدعم Cisco هذا الاشتراك بالكامل وسيتم تحديث الحزمة على Cisco.com. يمكن تنزيل حزمة التوقيع من software.cisco.com. يمكن العثور على معلومات توقيع Snort على snort.org.

الرسم التخطيطي للشبكة



التكوين

تكوين UTD للنظام الأساسي

الخطوة 1. تكوين واجهات VirtualPortGroups.

```
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
```

الخطوة 2. قم بتمكين بيئة IOx في وضع التكوين العام.

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

الخطوة 3. تكوين إستضافة التطبيقات باستخدام تكوين VNIC.

```
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
```

الخطوة 4 (اختيارية). تكوين ملف تعريف الموارد.

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

ملاحظة: إذا لم يتم تعريف هذا، سيستخدم النظام تكوين موارد التطبيق الافتراضي (منخفض). تأكد من وجود موارد كافية متاحة على ISR إذا كان تكوين ملف التعريف الافتراضي سيتم تغييره.

الخطوة 5. قم بتثبيت إستضافة التطبيقات باستخدام ملف UTD.tar.

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

ملاحظة: احتفظ بملف UTD.tar الصحيح على bootflash: لمتابعة تثبيته. تم تحديد إصدار SNORT على اسم ملف UTD.

يجب مراقبة syslog التالية التي تشير إلى تثبيت خدمة UTD بشكل صحيح.

```
Installing package 'bootflash:iox-iosxe-utd.16.12.08.1.0.24_SV2.9.16.1_XE16.12
*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 vi
*Jun 26 19:25:53.176: %IM-6-INSTALL_MSG: R0/0: ioxman: app-hosting: Install su
```

ملاحظة: استخدام 'show app-hosting list' يجب أن تكون الحالة 'نشر'

الخطوة 6. بدء تشغيل خدمة إستضافة التطبيقات.

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

ملاحظة: بعد بدء تشغيل خدمة إستضافة التطبيقات، يجب أن تكون حالة إستضافة التطبيقات 'قيد التشغيل'. أستخدم "إظهار قائمة إستضافة التطبيقات" أو "إظهار تفاصيل إستضافة التطبيقات" للاطلاع على مزيد من التفاصيل.

يجب مراقبة رسائل syslog التالية التي تشير إلى تثبيت خدمة UTD بشكل صحيح.

```
*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
```

تكوين مستوى الخدمة ومستوى البيانات.

بعد التثبيت الناجح، يجب تكوين مستوى الخدمة. يمكن تكوين نظام منع التسلل (IPS) على أنه نظام منع التسلل (IPS) أو نظام اكتشاف الاقتحام (IDS) للتفتيش.

تحذير: تأكد من تمكين ميزة الترخيص 'securityk9' لمتابعة تكوين مستوى خدمة UTD.

الخطوة 1. تكوين المحرك القياسي للدفاع عن التهديد الموحد (UTD) (مستوى الخدمة)

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

الخطوة 2. تمكين تسجيل رسائل الطوارئ إلى خادم بعيد.

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

الخطوة 3. قم بتمكين فحص التهديد لمحرك الشخير.

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

الخطوة 4. تكوين اكتشاف التهديد كنظام لمنع التسلل (IPS) أو نظام اكتشاف التسلل (IDS)

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

ملاحظة: يتم إستخدام "الحماية" لـ IPS و"الكشف" للمعرفات. 'الكشف' هو الإعداد الافتراضي.

الخطوة 5. تكوين نهج الأمان.

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

ملاحظة: النهج الافتراضي 'متوازن'

الخطوة 6 (اختيارية). إنشاء القائمة المسموح بها في UTD (Whitelist)

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

الخطوة 7 (اختيارية). قم بتكوين معرفات توقيعات الشخير لتظهر في العالم الأبيض.

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

```
Router(config-utd-whitelist)#end
```

ملاحظة: يتم إستخدام المعرف '40' كمثال. للتحقق من معلومات توقيع الشورت، راجع وثائق الشورت الرسمية.

الخطوة 8 (اختيارية). قم بتمكين القائمة المسموح بها في تكوين فحص التهديدات.

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

الخطوة 9. قم بتكوين الفاصل الزمني لتحديث التوقيع لتنزيل توقيعات SNORT تلقائيا.

```
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
```

ملاحظة: يحدد الرقم الأول الساعة بتنسيق 24 ساعة، ويشير الرقم الثاني إلى دقائق.

تحذير: تعمل تحديثات توقيع UTD على توليد انقطاع قصير للخدمة عند إجراء التحديث.

الخطوة 10. قم بتكوين معلمات خادم تحديث التوقيع.

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

ملاحظة: أستخدم 'Cisco' لاستخدام خادم Cisco أو 'url' لتحديد مسار مخصص لخادم التحديث. بالنسبة لخادم Cisco، يجب عليك توفير اسم المستخدم وكلمة المرور الخاصين بك.

الخطوة 11. تمكين مستوى التسجيل.

```
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
```

الخطوة 12. تمكين خدمة التوقيت العالمي.

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

الخطوة 13 (اختيارية). قم بإعادة توجيه حركة مرور البيانات من واجهة VirtualPortGroup إلى خدمة UTD.

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

ملاحظة: إذا لم يتم تكوين إعادة التوجيه، يتم الكشف عنها تلقائيا.

الخطوة 14. تمكين UTD لجميع واجهات الطبقة 3 على ISR.

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

الخطوة 15. قم بتمكين معيار المحرك.

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

يجب ملاحظة رسائل syslog التالية التي تشير إلى تمكين UTD بشكل صحيح.

```
*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
```

الخطوة 16 (اختيارية). تحديد الإجراء الخاص بفشل محرك UTD (مستوى بيانات UTD)

```
Router(config-engine-std)#fail close
```

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

ملاحظة: يسقط خيار فشل الإغلاق لك حركة مرور IPS/IDS عند فشل محرك UTD. يسمح خيار 'فشل الفتح' لكل حركة مرور IPS/IDS على فشل UTD. الخيار الافتراضي هو 'فتح الفشل'.

التحقق من الصحة

تحقق من عنوان IP الخاص بـ VirtualPortGroups وحالة الواجهة.

```
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
```

التحقق من تكوين مجموعة VirtualPort.

```
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
!
```

تحقق من تكوين إستضافة التطبيقات.

```
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
```

التحقق من تنشيط IOx.

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

التحقق من تكوين مستوى خدمة UTD.

```
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
```

تحقق من حالة إستضافة التطبيقات.

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

تحقق من تفاصيل إستضافة التطبيقات.

```
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/UtdUrlf-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
------------------------------------------------------------------------
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
```

استكشاف الأخطاء وإصلاحها

1. تأكد من أن موجه الخدمات المدمجة (ISR) من Cisco يشغل الإصدار XE 16.10.1a والإصدارات الأعلى (طريقة IOx)

2. تأكد من ترخيص موجه الخدمات المتكاملة (ISR) (ISR) من Cisco مع تمكين ميزة SecurityTYK9.

3. تأكد من أن طراز أجهزة ISR متوافق مع الحد الأدنى لملف تعريف الموارد.

4. تأكد من أن بدء خدمة UTD بعد التثبيت.

5. أثناء تنزيل حزمة التوقيع اليدوي، تأكد من أن الحزمة لها نفس إصدار محرك snort. قد يفشل تحديث حزمة التوقيع في حالة عدم تطابق الإصدار.

6. في حالة حدوث مشاكل تتعلق بالأداء، أستخدم show app host resource" و'show app'utd-name' الخاص باستخدام إستضافة التطبيقات للتعرف على ملخص وحدة المعالجة المركزية (CPU)/الذاكرة/التخزين.

```
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
```

تحذير: إذا كنت قادرا على مشاهدة وحدة المعالجة المركزية (CPU) أو الذاكرة أو إستخدام القرص، فاتصل ب TAC من Cisco.

تصحيح الأخطاء

أستخدم أوامر تصحيح الأخطاء المدرجة أدناه لجمع معلومات Snort IPS في حالة حدوث فشل.

<#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
```

معلومات ذات صلة

يمكن العثور على مستندات إضافية متعلقة بنشر Snort IPS هنا:

دليل تكوين أمان Snort IPS

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

ملف تعريف مورد الخدمة الظاهرية

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

نظام منع التسلل (IPS) على الموجهات - التكوين بالتفصيل.

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

أستكشاف أخطاء IPS لدى برنامج Snort وإصلاحها

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

لم يتم نشر ISR4K Snort IPS نظرا لعدم توفر موارد كافية لمنصات العمل في الأجهزة

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

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).