نشر نظام منع التسلل (IPS) على موجهات الخدمات المتكاملة 1000 Series

المحتويات

المقدمة

يوضح هذا المستند كيفية نشر ميزة Snort IPS على سلسلة موجه الخدمات المدمجة (ISR) 1000 من Cisco.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- سلسلة موجهات الخدمات المدمجة الطراز 1k من Cisco
- أوامر XE-IOS الأساسية
- معرفة الشخ الأساسية

المكونات المستخدمة

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

- C1111X-8P يشغل الإصدار 17.03.03
- محرك UTD TAR الإصدار 17.3.3
- ترخيص Security K9 مطلوب على ISR1k
- يلزم الشراك في التوقيع لمدة سنة أو ثلاث سنوات
- الطراز XE 17.2.1r أو على
- طرز أجهزة ISR التي تدعم ذاكرة DRAM سعة 8 جيجابايت فقط

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 Snort IPS نظام منع التسلل (IPS) أو نظام اكتشاف الاقتحام (IDS) للمكاتب الفرعية على موجهات الخدمات المتكاملة (ISR) من السلسلة Cisco 4000 Series Integrated Services Routers (ISR) وموجهات الخدمات المتكاملة Cisco 1000 Series (X PIDs مثل 111X و 1121X و 1161X، وما إلى ذلك التي تدعم ذاكرة DRAM بسعة 8 جيجابايت فقط) وموجه خدمات السحابة 1000V من Cisco. تستخدم هذه الميزة محرك الشبكة لتوفير وظائف IPS و IDS.

SNORT هو بروتوكول IPS لشبكة مفتوحة المصدر يقوم بإجراء تحليل حركة مرور البيانات في الوقت الفعلي ويقوم بإنشاء تنبيهات عند اكتشاف التهديدات على شبكات IP. كما يمكنه إجراء تحليل للبروتوكول والبحث عن المحتوى أو مطابقة واكتشاف مجموعة متنوعة من الهجمات والتحقيقات، مثل تجاوز سعة التخزين المؤقت والمنافذ الخفية وما إلى ذلك. تعمل ميزة Snort IPS في نموذج اكتشاف ومنع إقتحام الشبكة الذي يوفر وظائف نظام منع التسلل (IPS) أو نظام اكتشاف الاقتحام (IDS). في وضع اكتشاف ومنع التطفل على الشبكة، يقوم Snort بالإجراءات التالية

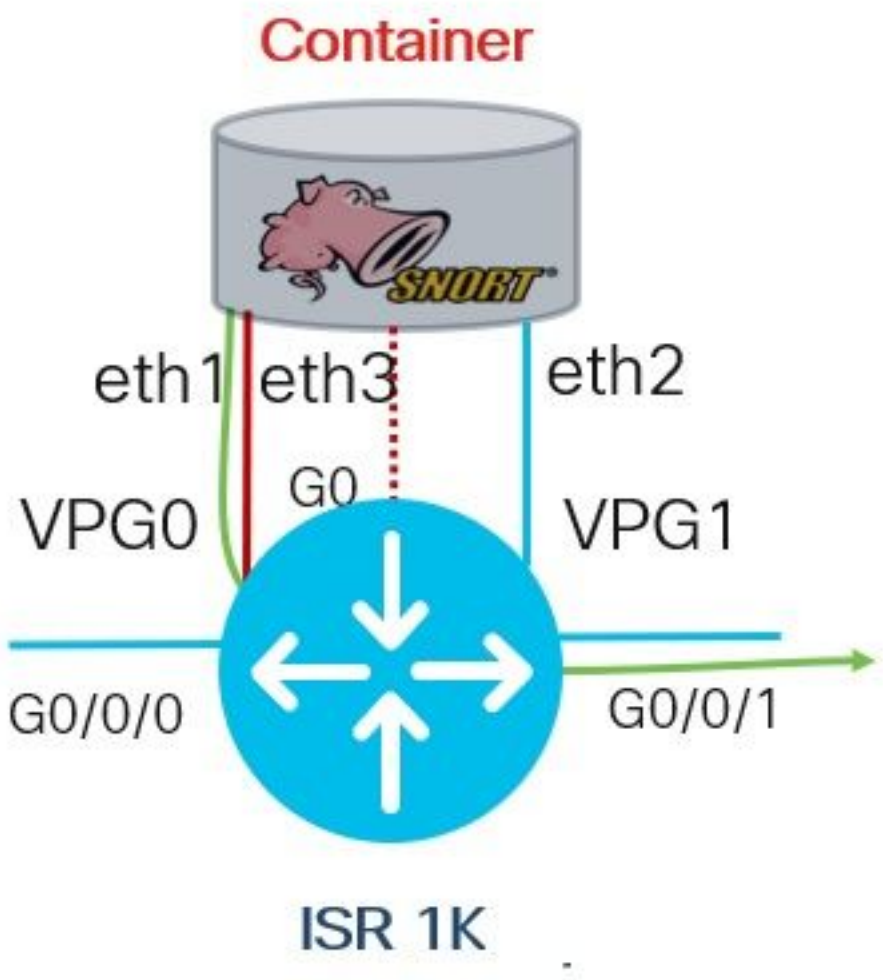
- مراقبة حركة مرور الشبكة وتحليلها مقابل قواعد محددة
- تصنيف الهجمات المنفذة
- إستدعاء الإجراءات مقابل القواعد المطابقة

استنادا إلى المتطلبات، يمكن تمكين snort إما في وضع IPS أو IDS. في وضع IDS، يتفحص الشروع حركة المرور ويبلغ عن التنبيهات ولكنه لا يتخذ أي إجراء لمنع الهجمات. في وضع نظام منع الاختراقات (IPS)، يتم إتخاذ إجراءات لمنع الهجمات، بالإضافة إلى اكتشاف الاختراقات. يقوم ب snort IPS الحركة مرور ويبلغ حدث إلى سجل لدان خارجي أو ال ios syslog. قد يؤثر تمكين تسجيل الدخول إلى نظام IOS Syslog على الأداء بسبب الحجم المحتمل لرسائل السجل. يمكن إستخدام أدوات المراقبة الخارجية التابعة لجهة خارجية، والتي تدعم سجلات SNORT، لجمع السجلات وتحليلها.

هناك طريقتان رئيسيتان لتكوين IPS snort على موجهات الخدمات المدمجة (ISR) من Cisco، وطريقة VMAN وطريقة IOx. تستخدم طريقة VMAN ملف utd.ova ويستخدم IOx ملف utd.tar. يعد IOx الطريقة الصحيحة والسليمة لنشر Snort IPS على سلسلة موجه الخدمات المدمجة (ISR) 1k من Cisco.

يمكن نشر بروتوكول IPS على موجهات الخدمات المدمجة (ISR) من Cisco بسعة 1 آلاف لفة في الدقيقة باستخدام الطراز XE 17.2.1r والإصدارات الأحدث.

الرسم التخطيطي للشبكة



التكوين

الخطوة 1. تكوين مجموعات المنافذ

```
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
```

الخطوة 2. تنشيط الخدمة الظاهرية، وتكوين التغييرات وتنفيذها

```
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
```

الخطوة 3. تكوين الخدمة الظاهرية

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

الخطوة 4. تكوين UTD (مستوى الخدمة)

```
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
```

ملاحظة: ملاحظة: ***الحماية من التهديدات*** تمكن الشرخ كخدمة التبديل داخل الشاشة (IPS)، ***وتتيح ميزة اكتشاف التهديدات*** إمكانية التطفل كمعرفات.

الخطوة 5. تكوين UTD (مستوى البيانات)

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

ملاحظة: Note: ***Failed Open*** وه الإعداد الافتراضي.

التحقق من الصحة

التحقق من عنوان IP لمجموعات المنافذ وحالة الواجهة

```
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
```

التحقق من تكوين مجموعات المنافذ

```
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
!
```

التحقق من تكوين الخدمة الظاهرية

```
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
```

ملاحظة: تأكد من أن الأمر ***start*** موجود، وإلا فلن يبدأ التنشيط.

التحقق من تنشيط الخدمة الظاهرية.

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

ملاحظة: سيقوم ***IOX*** بتنشيط الخدمة الظاهرية.

التحقق من تكوين UTD (مستوى الخدمة ومستوى البيانات)

```
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
```

التحقق من حالة إستضافة التطبيقات

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

التحقق من حالة إستضافة التطبيقات مع التفاصيل

```
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
```

استكشاف الأخطاء وإصلاحها

1. تأكد من أن موجه الخدمات المدمجة (ISR) من Cisco يشغل الإصدار XE 17.2.1r أو إصدارا أعلى

2. تأكد من أن موجه الخدمات المدمجة (ISR) من Cisco مرخص مع الأمان K9

3. تحقق من أن طراز أجهزة ISR يدعم ذاكرة DRAM سعة 8 جيجابايت فقط

4. تأكيد التوافق بين برنامج IOS XE وبرنامج محرك UTD snort IPS (.tar) UTD يحتاج إلى التوافق مع برنامج IOS XE، قد يفشل التثبيت لعدم التوافق

> **ملاحظة**: يمكن تنزيل البرامج باستخدام الارتباط: https://software.cisco.com/download/home/286315006/type

5. تأكد من تنشيط خدمات UTD وبدئها باستخدام أوامر **ioX** و**start** الموضحة في الخطوة 2 ضمن قسم ***التكوين***

6. التحقق من صحة الموارد المعينة لخدمة UTD باستخدام ***عرض دورة استضافة التطبيقات***" بعد تنشيط Snort

```
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. بعد تنشيط الاتصال، تأكد من وحدة المعالجة المركزية ISR واستخدام الذاكرة. يمكنك إستخدام الأمر ***show appUTD "إستخدام إستخدام إستضافة التطبيقات"*** لمراقبة وحدة المعالجة المركزية UTD واستخدام القرص والذاكرة

```
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
```

إن يكون أنت يستطيع أن يرى high ذاكرة، cpu، أو قرص إستعمال، اتصل ب cisco TAC.

8. أستخدم الأوامر المدرجة أدناه لجمع معلومات نشر Snort IPS في حالة حدوث فشل:

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

معلومات ذات صلة

يمكن العثور على مستندات إضافية متعلقة بنشر Snort IPS هنا:

شورت آي بي إس

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

IPS على ISR و ISRv و CSR - التكوين بالتفصيل

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

دليل نشر Snort IPS

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

736629.html#_Toc442352480

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).