Implemente Snort IPS en los routers de servicios integrados serie 1000

Contenido

Introducción

Este documento describe cómo implementar la función Snort IPS en Cisco Integrated Services Router (ISR) serie 1000.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Routers de servicios integrados de Cisco serie 1k
- Comandos XE-IOS básicos
- Conocimiento básico de Snort

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- C1111X-8P que ejecuta la versión 17.03.03
- UTD Engine TAR para la versión 17.3.3
- La licencia de seguridad K9 es obligatoria en el ISR1k
- Se requiere una suscripción de firma de 1 año o 3 años
- XE 17.2.1r y superiores
- Modelos de hardware ISR compatibles solo con DRAM de 8 GB

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red

en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

La función Snort IPS habilita el sistema de prevención de intrusiones (IPS) o el sistema de detección de intrusiones (IDS) para sucursales en routers de servicios integrados (ISR) de la serie Cisco 4000, routers de servicios integrados de la serie Cisco 1000 (X PID como 1111X, 1121X, 1161GB, etc.) que admiten 8 Solo DRAM) y Cisco Cloud Services Router serie 1000v. Esta función utiliza el motor Snort para proporcionar funciones IPS e IDS.

Snort es un IPS de red de código abierto que realiza análisis de tráfico en tiempo real y genera alertas cuando se detectan amenazas en redes IP. También puede realizar análisis de protocolo, búsqueda o coincidencia de contenido, y detectar una variedad de ataques y sondas, como desbordamientos de búfer, exploraciones de puertos sigilosos, etc. La función Snort IPS funciona en el modelo de detección y prevención de intrusiones en la red que proporciona funciones IPS o IDS. En el modo de detección y prevención de intrusiones en la red, Snort realiza las siguientes acciones:

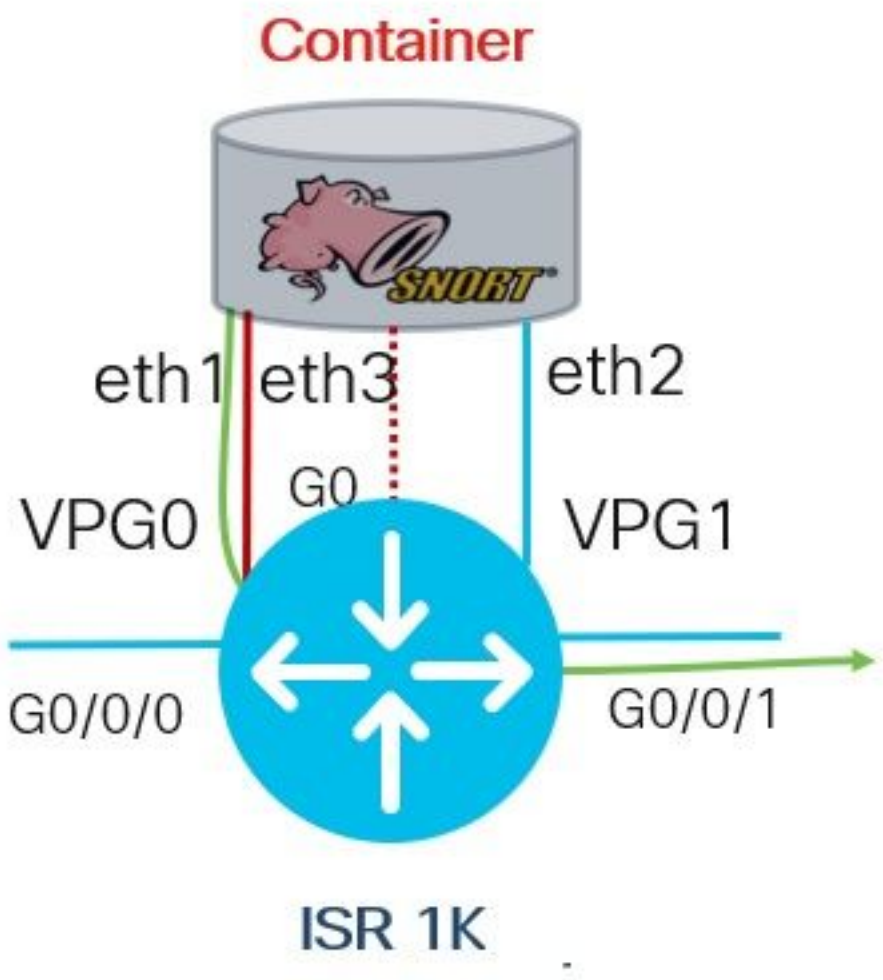
- Supervise el tráfico de red y analice un conjunto de reglas definido
- Clasificación de ataques realizados
- Invoca acciones contra reglas coincidentes

Según los requisitos, Snort se puede habilitar en modo IPS o IDS. En el modo IDS, Snort inspecciona el tráfico y notifica las alertas, pero no realiza ninguna acción para evitar ataques. En el modo IPS, además de la detección de intrusiones, se toman medidas para evitar ataques. El IPS de Snort monitorea el tráfico e informa los eventos a un servidor de registro externo o al Syslog del IOS. La habilitación del registro en el Syslog del IOS puede afectar el rendimiento debido al volumen potencial de mensajes de registro. Se pueden utilizar herramientas de supervisión externas de terceros, que admiten los registros de Snort, para la recopilación y el análisis de registros.

Hay dos formas principales de configurar Snort IPS en Cisco Integrated Services Routers (ISR), el método VMAN y el método IOx. El método VMAN utiliza un archivo utd.ova e IOx utiliza un archivo utd.tar. IOx es el método correcto y adecuado para la implementación de Snort IPS en Cisco Integrated Services Router (ISR) serie 1k.

Snort IPS se puede implementar en los routers de servicios integrados (ISR) de Cisco serie 1k con XE 17.2.1r y versiones posteriores.

Diagrama de la red



Configurar

Paso 1. Configurar grupos de puertos

```
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
```

Paso 2. Activar servicio virtual, configurar y registrar cambios

```
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
```

Paso 3. Configurar servicio virtual

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

Paso 4. Configuración de UTD (plano de servicio)

```
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
```

> **Nota:** Nota: *la protección contra amenazas* habilita Snort como IPS, *la detección de amenazas* habilita Snort como IDS.

Paso 5. Configuración de UTD (plano de datos)

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

> **Nota:** *fail open* es el valor predeterminado.

Verificación

Verifique la dirección IP de los grupos de puertos y el estado de la interfaz

```
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
```

Verificación de la configuración de los grupos de puertos

```
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
!
```

Verificar la configuración del servicio virtual

```
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
```

> **Nota:** Asegúrese de que el comando ***start*** esté presente; de lo contrario, la activación no se iniciará.

Verifique la activación del servicio virtual.

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

> **Nota:** ***iox*** activará el servicio virtual.

Verificar la configuración de UTD (plano de servicio y plano de datos)

```
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
```

Verificar el estado de alojamiento de aplicaciones

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

Verificar el estado del alojamiento de aplicaciones con detalles

```
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
```

Resolución de problemas

1. Asegúrese de que el router de servicios integrados (ISR) de Cisco ejecute XE 17.2.1r o posterior

2. Asegúrese de que el router de servicios integrados (ISR) de Cisco tiene licencia con Security K9

3. Verifique que el modelo de hardware ISR admita sólo 8 GB de DRAM

4. Confirmar la compatibilidad entre el software IOS XE y el archivo UTD Snort IPS Engine Software (archivo .tar) debe coincidir con el software IOS XE; la instalación puede fallar por incompatibilidad

> **Nota:** El software puede descargarse a través del enlace: https://software.cisco.com/download/home/286315006/type

5. Confirme para activar e iniciar servicios UTD usando los comandos **iox** e **start** que se muestran en el paso 2 bajo la sección ***Configure***

6. Validar los recursos asignados al servicio UTD utilizando '***show app-hosting resource***' después de la activación de 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. Después de la activación de Snort, confirme el uso de memoria y CPU de ISR. Puede utilizar el comando '***show app-hosting usage appid utd***' para supervisar la utilización de CPU, memoria y disco de UTD

```
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
```

Si es capaz de ver un uso elevado de memoria, CPU o disco, póngase en contacto con el TAC de Cisco.

8. Utilice los siguientes comandos para recopilar información de implementación de IPS de Snort en caso de que se produzca un error:

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

Información Relacionada

Los documentos adicionales relacionados con la implementación de Snort IPS se pueden encontrar aquí:

IPS de Snort

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 de Snort en ISR, ISRv y CSR: configuración paso a paso

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

Guía de implementación de Snort IPS

https://www.cisco.com/c/en/us/products/collateral/security/router-security/guide-c07-736629.html#_Toc442352480