Implemente Snort IPS en los routers de servicios integrados de Cisco serie 4000

Contenido

Introducción

Este documento describe cómo implementar la función Snort IPS e Snort IDS en los routers de servicios integrados (ISR) de Cisco serie 4000 mediante el método IOx.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Routers de servicios integrados de Cisco serie 4000 con al menos 8 GB de DRAM.
- Experiencia básica de comandos IOS-XE.
- Conocimiento básico de Snort.
- Se requiere una suscripción de firma por 1 año o 3 años
- IOS-XE 16.10.1a y superior.

Componentes Utilizados

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

- ISR4331/K9 que ejecuta la versión 17.9.3a.
- UTD Engine TAR para la versión 17.9.3a.
- Licencia de SecurityIK9 para ISR4331/K9.

El método VMAN está ahora obsoleto.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). 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 de la serie 4000 de Cisco y routers de servicios en la nube de la serie 1000v de Cisco. Esta función utiliza el Snort de código abierto para activar las funciones de IPS e IDS.

Snort es un IPS 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 protocolos, investigaciones de contenido o marchas, y detectar una variedad de ataques y sondeos, como desbordamientos de búfer, análisis de puertos sigilosos, etc. El motor Snort funciona como un servicio de contenedor virtual en los routers de servicios integrados de Cisco serie 4000 y los routers de servicios en la nube serie 1000v.

La función Snort IPS funciona como modo de detección o prevención de intrusiones en la red y proporciona capacidades IPS o IDS en los routers de servicios integrados de Cisco serie 4000 y los routers de servicios en la nube serie 1000v.

- Supervisa el tráfico de red y realiza análisis comparándolos con un conjunto de reglas definido.
- Realiza la clasificación de adición.
- Invoca acciones contra reglas coincidentes.

En función de los requisitos de red. Snort IPS se puede activar como IPS o IDS. En el modo IDS, Snort inspecciona el tráfico e informa de las alertas, pero no realiza ninguna acción para evitar ataques. En el modo IPS, inspecciona el tráfico e informa de las alertas como lo hace IDS, pero se toman medidas para evitar ataques.

Snort IPS se ejecuta como servicio en los routers ISR. Los contenedores de servicios utilizan tecnología de virtualización para proporcionar un entorno de alojamiento en dispositivos de Cisco para aplicaciones. La inspección del tráfico de Snort se habilita por interfaz o globalmente en todas las interfaces admitidas. El sensor de Snort requiere dos interfaces VirtualPortGroup. El primer VirtualPortGroup se utiliza para el tráfico de administración y el segundo para el tráfico de datos entre el plano de reenvío y el servicio de contenedor virtual de Snort. Se deben configurar direcciones IP para estas interfaces de VirtualPortGroup. La subred IP asignada a la interfaz de VirtualPortGroup de administración debe poder comunicarse con el servidor de firmas y el servidor de alertas/informes.

Snort IPS supervisa el tráfico e informa de 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. Las herramientas de supervisión externas de terceros, compatibles con los registros de Snort, se pueden utilizar para la recopilación y el análisis de registros.

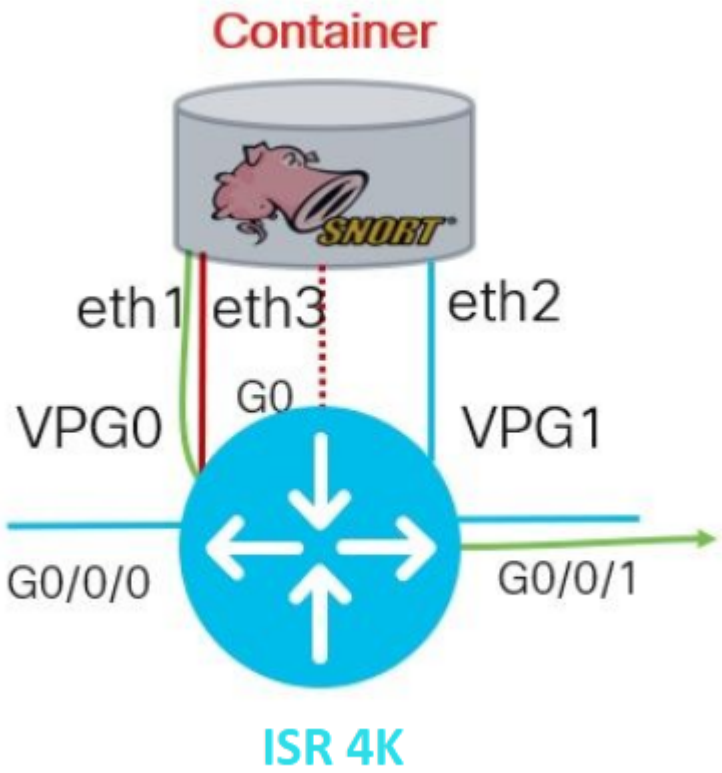
Snort IPS en los routers de servicios integrados de la serie 4000 de Cisco y en los routers de servicios en la nube de la serie 1000v de Cisco se basa en la descarga del paquete de firmas. Existen dos tipos de suscripciones:

- Paquete de firma de comunidad.
- Paquete de firma basado en suscriptor.

El conjunto de reglas del paquete de firmas de comunidad ofrece una cobertura limitada frente a amenazas. El conjunto de reglas del paquete de firmas basado en suscriptor ofrece la mejor protección contra amenazas. Incluye cobertura previa a las vulnerabilidades y también proporciona el acceso más rápido a las firmas actualizadas en respuesta a un incidente de seguridad o al descubrimiento proactivo de una nueva amenaza. Esta suscripción es totalmente compatible con Cisco y el paquete se actualizará en Cisco.com. El

paquete de firma se puede descargar de software.cisco.com. Puede encontrar información sobre la firma de Snort en snort.org.

Diagrama de la red



Configurar

Configuración de UTD de plataforma

Paso 1. Configure las interfaces 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
```

Paso 2. Habilite el entorno IOx en el modo de configuración global.

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

Paso 3. Configure el alojamiento de aplicaciones con la configuración de 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
```

Paso 4 (opcional). Configuración del perfil de recursos.

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

> **Nota:** *Si no se define, el sistema utilizará la configuración predeterminada app-resource (Baja). Asegúrese de tener suficientes recursos disponibles en ISR si se va a cambiar la configuración de perfil predeterminada.*

Paso 5. Instale el alojamiento de la aplicación mediante el archivo 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.
```

> **Nota**: Mantenga el archivo UTD.tar correcto en bootflash: para proceder a instalarlo. La versión de Snort se especifica en el nombre de archivo UTD.

Los registros del sistema siguientes deben aparecer para indicar que el servicio UTD se ha instalado correctamente.

```
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
```

> **Nota**: con *'show app-hosting list'* el estado debe ser *'Deployed'*

Paso 6. Inicie el servicio de alojamiento de aplicaciones.

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

> **Nota**: después de iniciar el servicio de alojamiento de aplicaciones, el estado de alojamiento de aplicaciones debe ser *'En ejecución'*. Utilice *'show app-hosting list' o 'show app-hosting detail'* para ver más detalles.

Los siguientes mensajes de syslog deben aparecer indicando que el servicio UTD se ha instalado correctamente.

```
*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
```

Configuración del plano de servicio y del plano de datos.

Después de una instalación correcta, se debe configurar el plano de servicio. Snort IPS se puede configurar como sistema de prevención de intrusiones (IPS) o sistema de detección de intrusiones (IDS) para su inspección.

> **Advertencia**: confirme que la función de licencia *'securityk9'* está habilitada para continuar con la configuración del plano de servicio UTD.

Paso 1. Configuración del motor estándar de Unified Threat Defence (UTD) (plano de servicio)

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

Paso 2. Habilite el registro de mensajes de emergencia en un servidor remoto.

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

Paso 3. Active la inspección de amenazas para el motor Snort.

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

Paso 4. Configuración de la detección de amenazas como sistema de prevención de intrusiones (IPS) o sistema de detección de intrusiones (IDS)

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

Nota: *'Protección'* se utiliza para IPS y *'Detección'* para IDS. *'Detección'* es el valor predeterminado.

Paso 5. Configuración de la política de seguridad.

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

Nota: la política predeterminada es *'equilibrada'*

Paso 6 (opcional). Crear la lista de UTD permitidos (Lista blanca)

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

Paso 7 (opcional). Configure los ID de firmas de Snort para que aparezcan en la lista blanca.

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

Nota: ID *'40'* se utiliza como ejemplo. Para comprobar la información de firma de Snort, consulte la documentación oficial de Snort.

Paso 8 (opcional). Habilitar lista de permitidos en configuración de inspección de amenazas.

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

Paso 9. Configure el intervalo de actualización de firmas para descargar firmas Snort automáticamente.

```
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
```

Nota: el primer número define la hora en formato de 24 horas y el segundo número indica minutos.

Advertencia: las actualizaciones de firmas de UTD generan una breve interrupción del servicio en el momento de la actualización.

Paso 10. Configure los parámetros del servidor de actualización de firmas.

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

Nota: Utilice *'cisco'* para utilizar el servidor de Cisco o *'url'* para definir una ruta personalizada para el servidor de actualización. Para el servidor de Cisco, debe proporcionar su propio nombre de usuario y contraseña.

Paso 11. Habilitar nivel de registro.

```
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
```

Paso 12. Habilitar servicio utd.

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

Paso 13 (opcional). Redireccione el tráfico de datos desde la interfaz de VirtualPortGroup al servicio UTD.

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

Nota: Si la redirección no está configurada, se detecta automáticamente.

Paso 14. Habilite UTD para todas las interfaces de capa 3 en ISR.

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

Paso 15. Active el estándar del motor.

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

Los siguientes mensajes de syslog deben ser vistos indicando que UTD fue habilitado correctamente.

```
*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
```

Paso 16 (opcional). Definir la acción para el fallo del motor UTD (plano de datos UTD)

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

> **Nota**: La opción *'Fail close'* descarta todo el tráfico IPS/IDS cuando falla el motor UTD. *La* opción *'Fail open'* permite todo el tráfico IPS/IDS en fallos UTD. La opción predeterminada es *'fallo al abrir'*.

Verificación

Verifique la dirección IP y el estado de la interfaz de VirtualPortGroups.

```
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
```

Verifique la configuración de VirtualPortGroup.

```
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
!
```

Verifique la configuración de alojamiento de aplicaciones.

```
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
```

Verifique la activación de iox.

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

Verifique la configuración del plano de servicio 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
```

Verifique el estado de alojamiento de la aplicación.

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

Verifique los detalles de alojamiento de aplicaciones.

```
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
```

Resolución de problemas

1. Asegúrese de que el router de servicios integrados (ISR) de Cisco ejecuta XE 16.10.1a y versiones posteriores (para el método IOx)

2. Asegúrese de que el router de servicios integrados (ISR) de Cisco tiene licencia con la función SecurityLink9 activada.

3. Compruebe que el modelo de hardware de ISR cumple con el perfil de recursos mínimo.

4. La función no es compatible con la cookie SYN de firewall basada en zona y la traducción de direcciones de red 64 (NAT64)

5. Confirme que el servicio UTD se ha iniciado después de la instalación.

6. Durante la descarga manual del paquete Signature, asegúrese de que el paquete tenga la misma versión que la versión del motor Snort. La actualización del paquete de firmas puede fallar si hay una discordancia de versión.

7. En caso de problemas de rendimiento, utilice ***'show app-hosting resource'*** y ***'show app-hosting utilization appid ''UTD-NAME'*** para conocer el consumo de CPU/Memoria/Almacenamiento.

```
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
```

> **Advertencia**: si puede ver un uso elevado de la CPU, la memoria o el disco, póngase en contacto con el TAC de Cisco.

Depuración

Utilice los comandos de depuración que se enumeran a continuación para recopilar información de Snort IPS en caso de fallo.

<#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
```

Información Relacionada

Puede encontrar documentos adicionales relacionados con la implementación de Snort IPS aquí:

Guía de configuración de seguridad de 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

Perfil de recursos de servicio virtual

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

Snort IPS en routers: configuración paso a paso.

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

Resolución de problemas de 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#concept_C3C869E633A6475890475931DF83EBCC

ISR4K Snort IPS no está implementado porque el hardware no tiene suficientes recursos de plataforma

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

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).