Installeer IPS op geïntegreerde services routers 1000 Series

Inhoud

Inleiding

Dit document beschrijft hoe u de functie Sort IPS op Cisco Geïntegreerde services router (ISR) 1000 Series kunt implementeren.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco 1000 geïntegreerde services routers uit de 1k-serie
- Basis XE-IOS-opdrachten
- Basiskennis van snaren

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- C111X-8P met 17.03.03 release
- UTD Engine TAR voor 17.3.3 release
- Security K9-licentie is vereist op ISR1k
- Een abonnement van 1 jaar of 3 jaar is vereist
- XE 17.2.1r en hoger
- ISR-hardwaremodellen die alleen 8 GB DRAM ondersteunen

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de

mogelijke impact van om het even welke opdracht begrijpt.

Achtergrondinformatie

Dankzij de functie Sort IPS (Inbraakpreventiesysteem) of Inbraakdetectiesysteem (IDS) voor bijkantoren op Cisco 4000 Series geïntegreerde services routers (ISR), Cisco 1000 Series geïntegreerde services routers (X PID's zoals 111X, 1121X, 1161X, enzovoort) ondersteuning voor ondersteuning (alleen DRAM) en Cisco Cloud Services router 1000v Series. Deze optie gebruikt de korte motor om IPS en IDS functies te bieden.

Snort is een opensource-netwerk IPS dat realtime-verkeersanalyse uitvoert en waarschuwingen genereert wanneer bedreigingen op IP-netwerken worden gedetecteerd. Het kan ook protocolanalyse uitvoeren, content zoeken of bijpassen, en een verscheidenheid aan aanvallen en sondes detecteren, zoals bufferoverstromen, stealth port scans, enzovoort. De functie van SNIJIPS werkt in het model van de detectie en preventie van het netwerkinbraaknetwerk dat IPS of IDS functies biedt. In de detectie- en preventiemodus van het netwerk voert de Snort de volgende acties uit

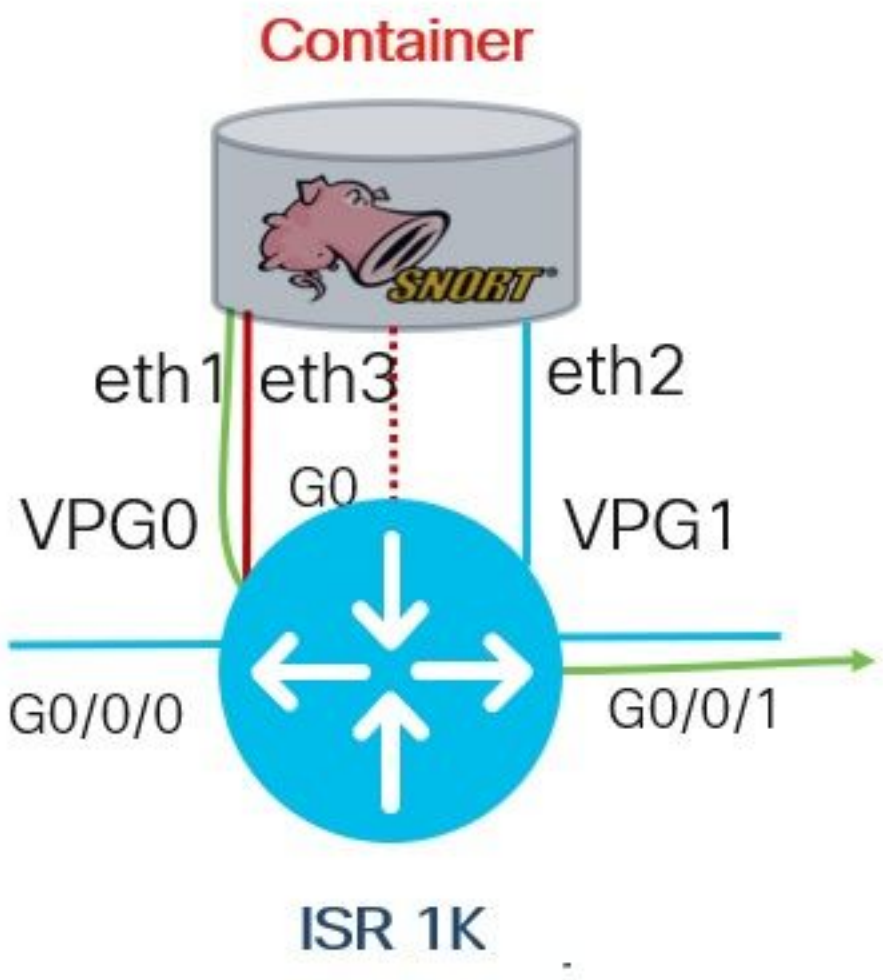
- Netwerkverkeer bewaken en analyseren op basis van een gedefinieerde regelgeving
- Classificatie van uitgevoerde aanvallen
- roept maatregelen op tegen afgedekte regels

Op basis van vereisten kan Snort in IPS of IDS-modus worden ingeschakeld. In de IDS-modus inspecteert Snort het verkeer en rapporteert u waarschuwingen, maar neemt u geen actie om aanvallen te voorkomen. In IPS-modus worden, naast inbraakdetectie, maatregelen genomen om aanvallen te voorkomen. Snoort IPS controleert het verkeer en rapporteert gebeurtenissen aan een externe logserver of het IOS systeem. Het in werking stellen van logging aan het IOS kan de prestaties beïnvloeden door het potentiële volume logberichten. Externe controle-instrumenten van derden, die Snort stammen ondersteunen, kunnen voor het verzamelen en analyseren van loggen worden gebruikt.

Er zijn twee belangrijke manieren om korte IPS op Cisco geïntegreerde services routers (ISR), de VMAN-methode en de IOx-methode te configureren. VMAN gebruikt een utd.ova-bestand en IOx gebruikt een utd.tar-bestand. IOx is de juiste methode voor de plaatsing van SNMP op Cisco Geïntegreerde Services Router (ISR) 1k serie.

Sorteer IPS kan worden gebruikt op Cisco geïntegreerde services routers (ISR) in 1k serie met XE 17.2.1r en hoger.

Netwerkdiagram



Configureren

Stap 1 Het configureren van poortgroepen

```
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
```

Stap 2 . Activeren de virtuele service, configureren en doorgeven van wijzigingen

```
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
```

Stap 3. Configuratie van de virtuele service

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

Stap 4 . UTD configureren (servicevlak)

```
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
```

> **Opmerking:** Opmerking: bedreigingsbescherming maakt snort als IPS mogelijk, *bedreigingsdetectie* maakt snort als IDS mogelijk.

Stap 5 . UTD configureren (datacenter)

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

> **Opmerking**: Opmerking: *Open* is de standaardinstelling *als* een *fout* wordt *gemaakt*.

Verifiëren

Controleer IP-adres en interfacestatus van poortgroepen

```
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
```

Controleer de configuratie van poortgroepen

```
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
!
```

Controleer de configuratie van de virtuele service

```
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
```

Opmerking: Zorg ervoor dat de opdracht ***starten*** aanwezig is, anders wordt de activering niet gestart.

Controleer de virtuele service.

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

Opmerking: ***iox*** activeert de virtuele service.

Controleer de UTD-configuratie (dienstvlak en gegevensvlak)

```
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
```

Controleer de app-hostingstaat

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

Controleer de app-hostingstatus met informatie

```
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
```

Probleemoplossing

1. Controleer of Cisco geïntegreerde services router (ISR) XE 17.2.1r of hoger werkt

2. Zorg ervoor dat Cisco geïntegreerde services router (ISR) gelicentieerd is met Security K9

3. Controleer of ISR-hardwaremodel alleen 8 GB DRAM ondersteunt

4. Controleer de compatibiliteit tussen IOS XE-software en UTD Snel IPS Engine Software (.tar-bestand) wanneer het UTD-bestand moet overeenkomen met IOS XE-software. Installatie kan falen voor incompatibiliteit

> **Opmerking:** U kunt software downloaden via de link: https://software.cisco.com/download/home/286315006/type

5. Bevestig dat u UTD-services kunt activeren en starten met **iox-** en **start-**opdrachten die in stap 2 zijn getoond onder ***Configureren*** sectie

6. Vestig de aan de UTD-service toegewezen middelen met behulp van '***show-app-host resource***'

na korte activering

```
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. Controleer na korte activering of u ISR CPU en geheugengebruik gebruikt. U kunt de opdracht '*app-host-toepassing tonen*' gebruiken *om* UTD CPU-, geheugen- en diskgebruik te bewaken

```
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
```

Als u veel geheugen, CPU of schijfgebruik kunt zien, neemt u contact op met Cisco TAC.

8. Gebruik de onderstaande opdrachten om informatie over de IPS-implementatie van snort te verzamelen in geval van een storing:

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

Gerelateerde informatie

Hier vindt u aanvullende documenten met betrekking tot de IPS-implementatie van snort:

SNELHEID IPS

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

SNELIPS op ISR, ISRv en CSR - stap voor stap configuratie

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

Intel IPS-implementatiehandleiding

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