Integrated Services Routers 1000 Series에 Snort IPS 구축

목차

소개

이 문서에서는 Cisco ISR(Integrated Services Router) 1000 시리즈에 Snort IPS 기능을 구축하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco Integrated Services Routers 1k 시리즈
- 기본 XE-IOS 명령
- 기본 Snort 지식

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- C1111X-8P(17.03.03 릴리스 실행)
- 17.3.3 릴리스용 UTD 엔진 TAR
- ISR1k에 보안 K9 라이센스가 필요합니다.
- 서명 서브스크립션 1년 또는 3년 필요
- XE 17.2.1r 이상
- 8GB DRAM만 지원하는 ISR 하드웨어 모델

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

배경 정보

Snort IPS 기능은 Cisco 4000 Series ISR(Integrated Services Router), Cisco 1000 Series Integrated Services Router(1111X, 1121X, 1161Gb 등 PID가 1111X, 1168Gb와 같은 지사의 지사를 위해 IPS(IPS) 또는 IDS)를 지원합니다. DRAM만 해당) 및 Cisco Cloud Services Router 1000v Series.이 기능은 Snort 엔진을 사용하여 IPS 및 IDS 기능을 제공합니다.

Snort는 실시간 트래픽 분석을 수행하고 IP 네트워크에서 위협이 탐지될 때 경고를 생성하는 오픈 소스 네트워크 IPS입니다.또한 프로토콜 분석, 콘텐츠 검색 또는 일치를 수행하고 버퍼 오버플로우, 스텔스 포트 스캔 등과 같은 다양한 공격 및 프로브를 탐지할 수 있습니다.Snort IPS 기능은 IPS 또는 IDS 기능을 제공하는 네트워크 침입 탐지 및 방지 모델에서 작동합니다.네트워크 침입 탐지 및 방지 모드에서 Snort는 다음 작업을 수행합니다

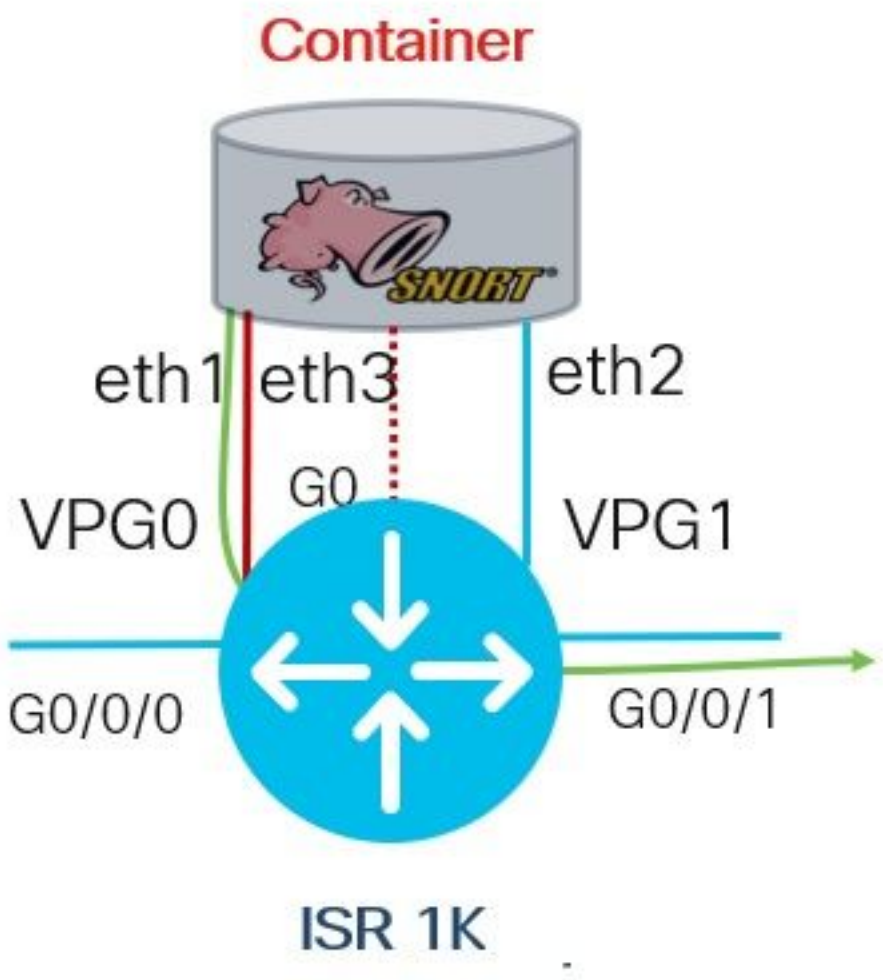
- 네트워크 트래픽을 모니터링하고 정의된 규칙 세트에 대해 분석
- 수행된 공격 분류
- 일치하는 규칙에 대한 작업 호출

요구 사항에 따라 IPS 또는 IDS 모드에서 Snort를 활성화할 수 있습니다.IDS 모드에서 Snort는 트래픽을 검사하고 알림을 보고하지만 공격을 방지하기 위한 어떤 조치도 취하지 않습니다.IPS 모드에서는 침입 탐지 외에도 공격을 방지하기 위한 조치가 취해집니다.Snort IPS는 트래픽을 모니터링하고 외부 로그 서버 또는 IOS Syslog에 이벤트를 보고합니다.IOS Syslog에 대한 로깅을 활성화하면 잠재적인 로그 메시지 볼륨 때문에 성능이 저하될 수 있습니다.Snort 로그를 지원하는 외부 서드파티 모니터링 툴을 로그 수집 및 분석에 사용할 수 있습니다.

Cisco ISR(Integrated Services Router)에서 Snort IPS를 구성하는 두 가지 주요 방법, VMAN 방법 및 IOx 방법이 있습니다.VMAN 메서드는 utd.ova 파일을 사용하며 IOx는 utd.tar 파일을 사용합니다.IOx는 Cisco ISR(Integrated Services Router) 1k Series에서 Snort IPS를 구축하는 올바른 방법입니다.

Snort IPS는 XE 17.2.1r 이상이 포함된 Cisco ISR(Integrated Services Router) 1k Series에 구축할 수 있습니다.

네트워크 다이어그램



구성

1단계. 포트 그룹 구성

```
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
```

2단계. 가상 서비스 활성화, 변경 사항 구성 및 커밋

```
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
```

3단계. 가상 서비스 구성

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

4단계. UTD(서비스 평면) 구성

```
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
```

> **참고:** 참고:*위협 차단*을 통해 Snort를 IPS로 지원하고 *위협 탐지를 통해* Snort를 IDS로 지원합니다.

5단계. UTD(데이터 플레인) 구성

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

> **참고**: 참고:*fail open은 기본 설정입니다.*

다음을 확인합니다.

포트 그룹 IP 주소 및 인터페이스 상태 확인

```
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
```

포트 그룹 구성 확인

```
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
!
```

가상 서비스 구성 확인

```
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
```

참고:*start* 명령이 ***있는지*** 확인하고 그렇지 않으면 활성화가 시작되지 않습니다.

가상 서비스 활성화를 확인합니다.

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

참고:*iox*가 가상 서비스를 활성화합니다.

UTD 컨피그레이션 확인(서비스 플레인 및 데이터 플레인)

```
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
```

앱 호스팅 상태 확인

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

세부 정보로 앱 호스팅 상태 확인

```
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
```

문제 해결

1. Cisco ISR(Integrated Services Router)이 XE 17.2.1r 이상을 실행하도록 보장

2. Cisco ISR(Integrated Services Router)에 보안 K9의 라이센스가 부여되었는지 확인

3. ISR 하드웨어 모델이 8GB DRAM만 지원하는지 확인합니다.

4. IOS XE Software와 UTD Snort IPS Engine Software(.tar 파일) 간의 호환성을 확인합니다. UTD 파일이 IOS XE 소프트웨어와 일치해야 합니다. 비호환성으로 인해 설치가 실패할 수 있습니다.

> **참고:**소프트웨어는 https://software.cisco.com/download/home/286315006/type 링크를 사용하여 다운로드할 수 있습니다.

5. Configure(구성) 섹션의 2단계에 표시된 **iox** 및 **start** 명령을 사용하여 UTD 서비스를 활성화하고 시작할지 확인합니다.

6. Snort 활성화 후 '***show app-hosting resource***'를 사용하여 UTD 서비스에 할당된 리소스를 검증합니다.

```
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. Snort 활성화 후 ISR CPU 및 메모리 사용량을 확인합니다.'show app-*hosting utilization appid* utd' 명령을 사용하여 UTD CPU, 메모리 및 디스크 사용률을 모니터링할 수 있습니다.

```
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
```

메모리, CPU 또는 디스크 사용률이 높을 경우 Cisco TAC에 문의하십시오.

8. 장애가 발생할 경우 아래 나열된 명령을 사용하여 Snort IPS 구축 정보를 수집합니다.

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

관련 정보

Snort IPS 구축과 관련된 추가 문서는 여기에서 찾을 수 있습니다.

Snort 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

ISR, ISRv 및 CSR에서 Snort IPS - 단계별 컨피그레이션

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

Snort IPS 구축 설명서

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