Bereitstellung von Snort IPS auf Integrated Services Routern der Serie 1000

Inhalt

Einführung

Dieses Dokument beschreibt die Bereitstellung der Snort IPS-Funktion auf der Cisco Integrated Services Router (ISR) 1000-Serie.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco Integrated Services Router der Serie 1000
- Grundlegende XE-IOS-Befehle
- Grundlegendes Snort-Wissen

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- C111X-8P mit 17.03.03-Version
- UTD-Engine-TAR für Version 17.3.3
- Für den ISR1k ist die Security K9-Lizenz erforderlich.
- Ein Signaturabonnement für ein oder drei Jahre ist erforderlich.
- XE 17.2.1r und höher
- ISR-Hardwaremodelle, die nur 8 GB DRAM unterstützen

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer

gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Die Snort IPS-Funktion ermöglicht Intrusion Prevention System (IPS) oder Intrusion Detection System (IDS) für Zweigstellen auf Cisco Integrated Services Routern der Serie 4000 (ISR), Cisco Integrated Services Routern der Serie 100 (X PIDs wie 111X, 1121X, 1161X usw., die Unterstützung bieten Nur 8 GB DRAM) und Cisco Cloud Services Router der Serie 1000v. Diese Funktion verwendet die Snort-Engine, um IPS- und IDS-Funktionen bereitzustellen.

Snort ist ein Open-Source-Netzwerk-IPS, das Datenverkehrsanalysen in Echtzeit durchführt und Warnmeldungen ausgibt, wenn Bedrohungen in IP-Netzwerken erkannt werden. Darüber hinaus können Protokollanalysen durchgeführt, Content-Suchvorgänge oder -Matches durchgeführt und eine Vielzahl von Angriffen und Tests erkannt werden, z. B. Pufferüberläufe, Stealth-Port-Scans usw. Die Snort IPS-Funktion arbeitet im Netzwerk-Intrusion Detection and Prevention-Modell, das IPS- oder IDS-Funktionen bereitstellt. Im Netzwerk-Intrusion Detection and Prevention-Modus führt Snort die folgenden Aktionen aus

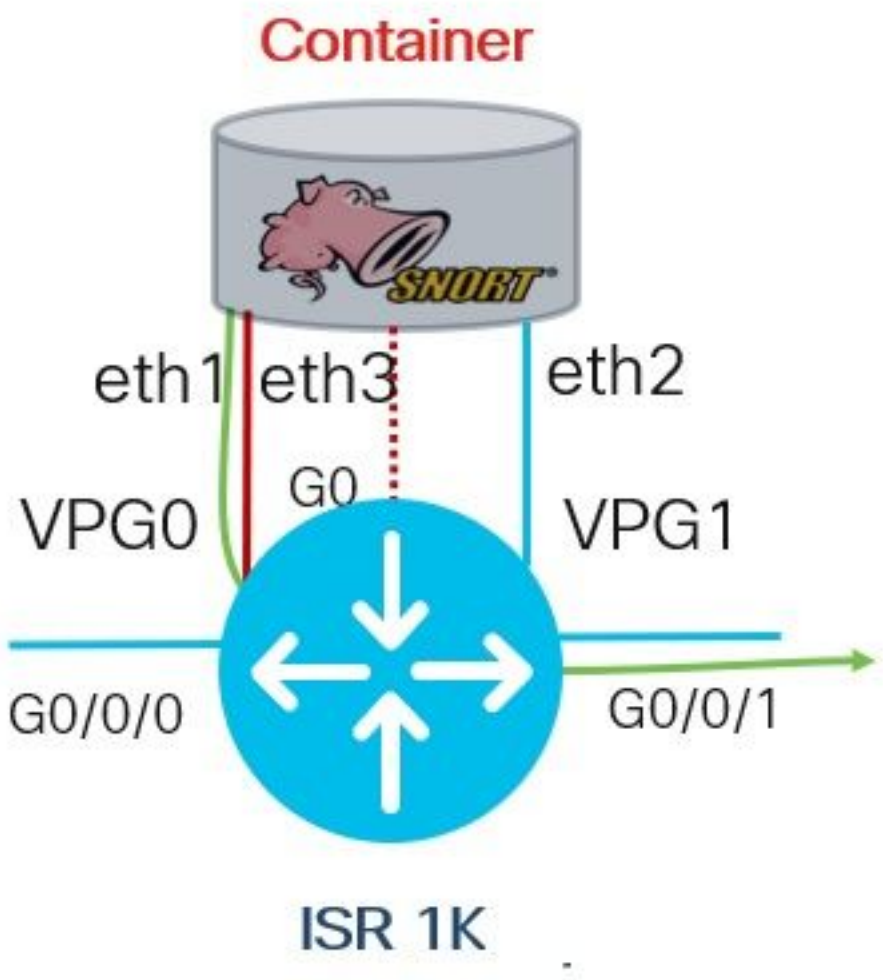
- Überwachung des Netzwerkverkehrs und Analyse anhand eines definierten Regelsatzes
- Klassifizierung durchgeführter Angriffe
- Ruft Aktionen gegen übereinstimmende Regeln auf

Je nach Anforderungen kann Snort entweder im IPS- oder im IDS-Modus aktiviert werden. Im IDS-Modus prüft Snort den Datenverkehr und meldet Warnungen, unternimmt jedoch keine Maßnahmen, um Angriffe zu verhindern. Im IPS-Modus werden neben der Identifizierung von Sicherheitsrisiken auch Maßnahmen ergriffen, um Angriffe zu verhindern. Das Snort IPS überwacht den Datenverkehr und meldet Ereignisse an einen externen Protokollserver oder das IOS-Syslog. Die Aktivierung der Protokollierung für das IOS-Syslog kann aufgrund des potenziellen Volumens der Protokollmeldungen die Leistung beeinträchtigen. Externe Überwachungstools von Drittanbietern, die Snort-Protokolle unterstützen, können für die Protokollerfassung und -analyse verwendet werden.

Es gibt zwei Hauptmethoden, Snort IPS auf Cisco Integrated Services Routern (ISR) zu konfigurieren: die VMAN-Methode und die IOx-Methode. Die VMAN-Methode verwendet eine Datei utd.ova und IOx eine Datei utd.tar. IOx ist die richtige und korrekte Methode für die Snort IPS-Bereitstellung auf der Cisco Integrated Services Router (ISR) 1000-Serie.

Snort IPS kann auf Cisco Integrated Services Routers (ISR) der Serie 1000 mit XE 17.2.1r und höher bereitgestellt werden.

Netzwerkdiagramm



Konfiguration

Schritt 1: Konfigurieren von Port-Gruppen

```
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
```

Schritt 2: Aktivieren des virtuellen Service, Konfigurieren und Übertragen von Änderungen

```
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
```

Schritt 3: Konfigurieren des virtuellen 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
```

Schritt 4: UTD konfigurieren (Service-Ebene)

```
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
```

> **Hinweis:** Hinweis: *Bedrohungsschutz* aktiviert Snort als IPS, *Bedrohungserkennung* aktiviert Snort als IDS.

Schritt 5: UTD konfigurieren (Datenebene)

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

> **Hinweis**: Hinweis: *Fail Open* ist die Standardeinstellung.

Überprüfung

IP-Adresse und Schnittstellenstatus für Portgruppen überprüfen

```
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
```

Konfiguration der Portgruppen überprüfen

```
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
!
```

Überprüfen der Konfiguration virtueller Services

```
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
```

> **Hinweis:** Vergewissern Sie sich, dass der ***Start***-Befehl vorhanden ist. Andernfalls wird die Aktivierung nicht gestartet.

Überprüfung der Aktivierung des virtuellen Dienstes

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

> **Hinweis:** *iox* aktiviert Virtual Service.

UTD-Konfiguration überprüfen (Service-Ebene und Datenebene)

```
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
```

Überprüfen des Anwendungshoststatus

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

Überprüfen Sie den Status des Anwendungshosts mit Details.

```
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
```

Fehlerbehebung

1. Sicherstellen, dass der Cisco Integrated Services Router (ISR) XE 17.2.1r oder höher ausführt

2. Vergewissern Sie sich, dass der Cisco Integrated Services Router (ISR) mit Security K9 lizenziert ist

3. Überprüfen Sie, ob das ISR-Hardwaremodell nur 8 GB DRAM unterstützt.

4. Kompatibilität zwischen IOS XE-Software und UTD Snort IPS Engine Software (TAR-Datei)-UTD-Datei muss mit der IOS XE-Software übereinstimmen. Die Installation kann aufgrund der Inkompatibilität scheitern.

> **Hinweis:** Software kann über folgenden Link heruntergeladen werden: https://software.cisco.com/download/home/286315006/type

5. Aktivieren und Starten von UTD-Diensten mit **iox** und **start**-Befehlen bestätigen, wie in Schritt 2 im Abschnitt ***Konfigurieren*** gezeigt

6. Validieren Sie die Ressourcen, die dem UTD-Service zugewiesen sind, mithilfe von "***show app-hosting resource***" nach der Snort-Aktivierung.

```
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. Überprüfen Sie nach der Snort-Aktivierung die CPU- und Speichernutzung des ISR. Sie können den Befehl "***show app-hosting use appid utd***" verwenden, um die CPU-, Arbeitsspeicher- und Festplattenauslastung von UTD zu überwachen.

```
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
```

Wenn Sie eine hohe Arbeitsspeicher-, CPU- oder Festplattenauslastung sehen können, wenden Sie sich an das Cisco TAC.

8. Verwenden Sie die unten aufgeführten Befehle, um Informationen zur IPS-Bereitstellung von Snort zu sammeln, falls ein Fehler auftritt:

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

Zugehörige Informationen

Weitere Dokumente zur Snort IPS-Bereitstellung finden Sie hier:

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

Snort IPS auf ISR, ISRv und CSR - schrittweise Konfiguration

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

configuration/ta-p/3369186

Implementierungsleitfaden für Snort IPS

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