Implementazione di Snort IPS su Integrated Services Router serie 1000

Sommario

[Introduzione](#)
[Prerequisiti](#)
[Requisiti](#)
[Componenti usati](#)
[Premesse](#)
[Esempio di rete](#)
[Configurazione](#)
[Verifica](#)
[Risoluzione dei problemi](#)
[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come implementare la funzionalità Snort IPS su Cisco Integrated Services Router (ISR) serie 1000.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Integrated Services Router serie 1k
- Comandi XE-IOS di base
- Conoscenze base di snort

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- C111X-8P con versione 17.03.03
- UTD Engine TAR per release 17.3.3
- Èrichiesta la licenza Security K9 sull'ISR1k
- Èrichiesta una sottoscrizione con firma di 1 anno o 3 anni
- XE 17.2.1r e superiori
- Modelli hardware ISR che supportano solo DRAM da 8 GB

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata

ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

La funzionalità Snort IPS consente di utilizzare Intrusion Prevention System (IPS) o Intrusion Detection System (IDS) per le filiali su Cisco serie 4000 Integrated Services Router (ISR), Cisco serie 1000 Integrated Services Router (X PID come 1111X, 1121X, 1161X, ecc. che supportano solo DRAM da 8 GB) e Cisco Cloud Services Router serie 1000v. Questa funzionalità utilizza il motore Snort per fornire funzionalità IPS e IDS.

Lo snort è un IPS di rete open-source che esegue analisi del traffico in tempo reale e genera avvisi quando vengono rilevate minacce sulle reti IP. Può inoltre eseguire l'analisi del protocollo, la ricerca di contenuti o la corrispondenza, e rilevare una varietà di attacchi e sonde, come overflow del buffer, scansioni di porte stealth e così via. La funzione Snort IPS funziona nel modello di rilevamento e prevenzione delle intrusioni in rete che fornisce funzionalità IPS o IDS. Nella modalità di rilevamento e prevenzione delle intrusioni nella rete, Snort esegue le azioni seguenti

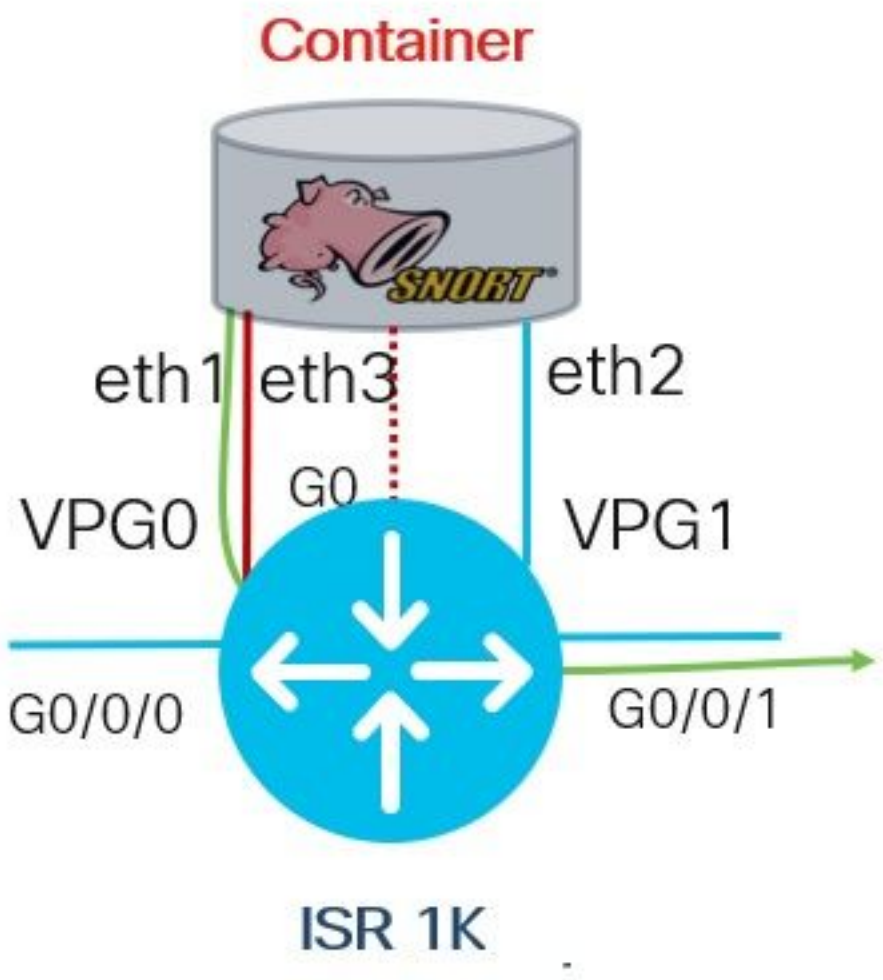
- Monitoraggio del traffico di rete e analisi in base a un set di regole definito
- Classificazione degli attacchi eseguiti
- Richiama azioni su regole corrispondenti

In base ai requisiti, Snort può essere abilitato sia in modalità IPS che IDS. In modalità IDS, Snort controlla il traffico e segnala gli avvisi, ma non interviene per prevenirne gli attacchi. In modalità IPS, oltre al rilevamento delle intrusioni, vengono intraprese azioni per prevenire gli attacchi. Lo Snort IPS controlla il traffico e segnala gli eventi a un server di registro esterno o al Syslog IOS. L'abilitazione della registrazione nel syslog IOS può influire sulle prestazioni a causa del volume potenziale dei messaggi di log. Per la raccolta e l'analisi dei log è possibile utilizzare strumenti di monitoraggio esterni di terze parti, che supportano i log Snort.

Esistono due modi principali per configurare Snort IPS su Cisco Integrated Services Router (ISR), il metodo VMAN e il metodo IOx. Il metodo VMAN utilizza un file utd.ova e IOx un file utd.tar. IOx è il metodo corretto per la distribuzione di Snort IPS su Cisco Integrated Services Router (ISR) serie 1k.

Gli Snort IPS possono essere installati sui Cisco Integrated Services Router (ISR) serie 1k con XE 17.2.1r e versioni successive.

Esempio di rete



Configurazione

Passaggio 1. Configurazione dei gruppi di porte

```
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
```

Passaggio 2. Attivare il servizio virtuale, configurare ed eseguire il commit delle modifiche

```
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
```

Passaggio 3. Configurazione del servizio virtuale

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

Passo 4. Configurazione di UTD (Service Plane)

```
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 protezione dalle minacce* consente di eseguire Snort come IPS, il *rilevamento delle minacce* consente di eseguire Snort come IDS.

Passo 5. Configurazione di UTD (Data Plane)

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

> **Nota**: Nota: *fail-open* è l'impostazione predefinita.

Verifica

Verifica dell'indirizzo IP e dello stato dell'interfaccia dei gruppi di porte

```
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
```

Verifica della configurazione dei gruppi di porte

```
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
!
```

Verifica configurazione servizio virtuale

```
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: Verificare che il comando ***start*** sia presente, altrimenti l'attivazione non verrà avviata.

Verificare l'attivazione del servizio virtuale.

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

Nota: *iox* attiverà Servizio virtuale.

Verifica della configurazione UTD (piano di servizio e piano dati)

```
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
```

Verifica lo stato di hosting dell'app

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

Verifica lo stato di hosting dell'app con i dettagli

```
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
```

Risoluzione dei problemi

1. Verificare che Cisco Integrated Services Router (ISR) esegua XE 17.2.1r o versioni successive

2. Verificare che Cisco Integrated Services Router (ISR) sia concesso in licenza con Security K9

3. Verificare che il modello hardware ISR supporti solo DRAM da 8 GB

4. Confermare la compatibilità tra il software IOS XE e il software UTD Snort IPS Engine (file .tar) Il file UTD deve corrispondere al software IOS XE. L'installazione potrebbe non riuscire per incompatibilità

> **Nota:** Il software può essere scaricato dal seguente link: https://software.cisco.com/download/home/286315006/type

5. Confermare l'attivazione e l'avvio dei servizi UTD utilizzando i comandi **iox** e **start** mostrati nel passaggio 2 della sezione ***Configure***

6. Convalida le risorse assegnate al servizio UTD utilizzando '***show app-hosting resource***' dopo l'attivazione 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. Dopo l'attivazione di Snort, confermare l'utilizzo della CPU e della memoria ISR. È possibile usare il comando '***show app-hosting usage appid utd***' per monitorare l'utilizzo di CPU, memoria e disco 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
```

Se si rileva un utilizzo elevato della memoria, della CPU o del disco, contattare Cisco TAC.

8. Utilizzare i comandi elencati di seguito per raccogliere informazioni sulla distribuzione di Snort IPS in caso di errore:

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

Informazioni correlate

Ulteriori documenti relativi alla distribuzione di Snort IPS sono disponibili qui:

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

Avvio di IPS su ISR, ISRv e CSR - Configurazione dettagliata

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

Guida alla distribuzione di IPS Snort

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