Déployer Snort IPS sur les routeurs à services intégrés de la gamme 1000

Contenu

Introduction

Ce document décrit comment déployer la fonctionnalité Snort IPS sur les routeurs à services intégrés Cisco ISR 1000.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Routeurs à services intégrés Cisco, série 100
- Commandes XE-IOS de base
- Connaissances de base du Snort

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- C111X-8P version 17.03.03
- Moteur UTD TAR pour version 17.3.3
- La licence Security K9 est requise sur le routeur ISR1k
- Un abonnement de signature d'un an ou de trois ans est requis
- XE 17.2.1r et versions ultérieures
- Modèles matériels ISR prenant en charge 8 Go de DRAM uniquement

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau

est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

La fonction IPS Snort active le système de prévention des intrusions (IPS) ou le système de détection des intrusions (IDS) pour les succursales sur les routeurs à services intégrés Cisco 4000 (ISR), les routeurs à services intégrés Cisco 1000 (X PID) tels que 1111X, 1121X, 1161X, etc. Go DRAM uniquement) et routeur de services cloud Cisco, série 1000v. Cette fonctionnalité utilise le moteur Snort pour fournir des fonctionnalités IPS et IDS.

Snort est un système de prévention des intrusions de réseau open source qui analyse le trafic en temps réel et génère des alertes lorsque des menaces sont détectées sur les réseaux IP. Il peut également effectuer des analyses de protocole, des recherches de contenu ou des correspondances, et détecter diverses attaques et sondes, telles que des dépassements de tampon, des analyses furtives de ports, etc. La fonctionnalité IPS Snort fonctionne dans le modèle de détection et de prévention des intrusions du réseau qui fournit des fonctionnalités IPS ou IDS. En mode de détection et de prévention des intrusions sur le réseau, Snort effectue les actions suivantes :

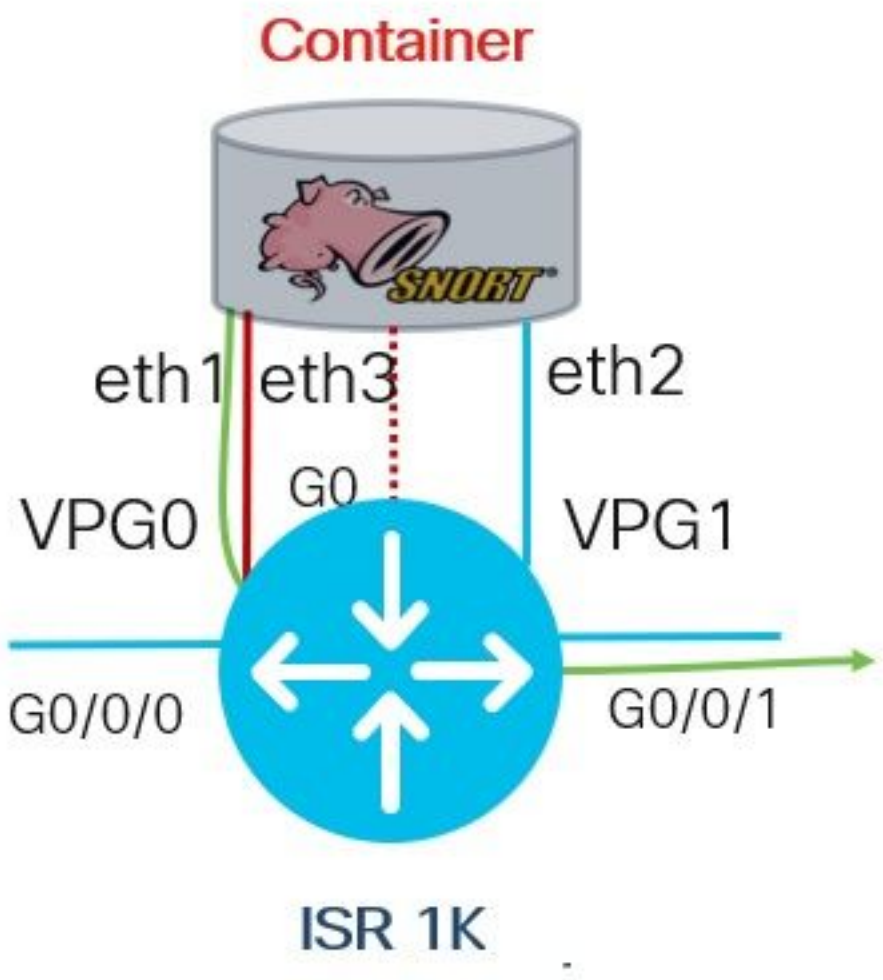
- Surveillez le trafic réseau et analysez-le par rapport à un ensemble de règles défini
- Classification des attaques effectuées
- Appelle les actions contre les règles correspondantes

En fonction des besoins, Snort peut être activé en mode IPS ou IDS. En mode IDS, Snort inspecte le trafic et signale les alertes, mais ne prend aucune mesure pour empêcher les attaques. En mode IPS, outre la détection des intrusions, des actions sont prises pour empêcher les attaques. L'IPS Snort surveille le trafic et signale les événements à un serveur de journal externe ou au Syslog IOS. L'activation de la journalisation dans le Syslog IOS peut avoir un impact sur les performances en raison du volume potentiel de messages de journal. Des outils externes de surveillance tiers, qui prennent en charge les journaux Snort, peuvent être utilisés pour la collecte et l'analyse des journaux.

Il existe deux méthodes principales pour configurer Snort IPS sur les routeurs à services intégrés Cisco (ISR), la méthode VMAN et la méthode IOx. La méthode VMAN utilise un fichier utd.ova et IOx un fichier utd.tar. IOx est la méthode correcte et appropriée pour le déploiement de Snort IPS sur les routeurs à services intégrés (ISR) de la gamme 1K de Cisco.

Snort IPS peut être déployé sur les routeurs à services intégrés (ISR) de la gamme 1K avec XE 17.2.1r et versions ultérieures.

Diagramme du réseau



Configuration

Étape 1. Configurer les groupes de ports

```
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
```

Étape 2. Activer le service virtuel, configurer et valider les modifications

```
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
```

Étape 3. Configurer le service virtuel

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

Étape 4. Configuration de UTD (plan de service)

```
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
```

> Note: Note: *la protection contre les menaces* active Snort comme IPS, *la détection des menaces* active Snort comme IDS.

Étape 5. Configuration de UTD (plan de données)

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

> Note : Note : *fail open* est le paramètre par défaut.

Vérification

Vérifier l'adresse IP et l'état de l'interface des groupes de ports

```
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
```

Vérifier la configuration des groupes de ports

```
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
!
```

Vérifier la configuration du service virtuel

```
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
```

Note: Vérifiez que la commande ***start*** est présente, sinon l'activation ne démarrera pas.

Vérifiez l'activation du service virtuel.

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

Note: *iox* active le service virtuel.

Vérifier la configuration UTD (plan de service et plan de données)

```
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
```

Vérifier l'état de l'hébergement d'applications

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

Vérifier l'état de l'hébergement d'applications avec les détails

```
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
```

Dépannage

1. Garantir que le routeur de services intégrés Cisco (ISR) exécute XE 17.2.1r ou version ultérieure

2. Assurez-vous que le routeur à services intégrés Cisco (ISR) est sous licence Security K9

3. Vérifier que le modèle matériel ISR prend en charge 8 Go de DRAM uniquement

4. Confirmer la compatibilité entre le logiciel IOS XE et le logiciel UTD Snort IPS Engine (fichier .tar) Le fichier UTD doit correspondre au logiciel IOS XE, l'installation peut échouer en cas d'incompatibilité

> **Note**: Le logiciel peut être téléchargé à l'aide du lien suivant : https://software.cisco.com/download/home/286315006/type

5. Confirmer l'activation et le démarrage des services UTD à l'aide des commandes **iox** et **start** indiquées à l'étape 2 sous ***Configurer*** la section

6. Valider les ressources affectées au service UTD à l'aide de '***show app-hosting resource***' après

l'activation de 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. Après l'activation de Snort, confirmez l'utilisation du processeur ISR et de la mémoire. Vous pouvez utiliser la commande '***show app-hosting use appid utd***' pour surveiller l'utilisation du processeur UTD, de la mémoire et du disque

```
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
```

Si vous voyez une utilisation élevée de la mémoire, du processeur ou du disque, contactez le TAC de Cisco.

8. Utilisez les commandes répertoriées ci-dessous pour collecter les informations de déploiement Snort IPS en cas de défaillance :

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

Informations connexes

D'autres documents relatifs au déploiement de Snort IPS sont disponibles ici :

IPS Snort

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 sur ISR, ISRv et CSR - Configuration pas à pas

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

Guide de déploiement Snort IPS

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