Déploiement de Snort IPS sur les routeurs à services intégrés Cisco 4000

Table des matières

Introduction

Ce document décrit comment déployer les fonctionnalités Snort IPS et Snort IDS sur les routeurs à services intégrés Cisco (ISR) 4000 à l'aide de la méthode IOx.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Routeurs à services intégrés Cisco série 4000 avec au moins 8 Go de DRAM.
- Expérience de base des commandes IOS-XE.
- Connaissances de base de Snort.
- Un abonnement signature d'un an ou de trois ans est requis
- IOS-XE 16.10.1a et versions ultérieures.

Composants utilisés

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

- ISR4331/K9 exécutant la version 17.9.3a.

- TAR du moteur UTD pour la version 17.9.3a.
- Licence SecurityTyk9 pour ISR4331/K9.

La méthode VMAN est maintenant déconseillée.

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 Snort IPS active le système de prévention des intrusions (IPS) ou le système de détection des intrusions (IDS) pour les filiales sur les routeurs à services intégrés Cisco 4000 et les routeurs à services cloud Cisco 1000v. Cette fonctionnalité utilise l'Open Source Snort pour activer les fonctionnalités IPS et IDS.

Snort est un système de prévention des intrusions open source qui effectue une analyse du trafic en temps réel et génère des alertes lorsque des menaces sont détectées sur des réseaux IP. Il peut également effectuer des analyses de protocole, des recherches de contenu ou des recherches en cours, et détecter une variété d'attaques et de sondes, telles que les dépassements de mémoire tampon, les analyses furtives de port, etc. Le moteur Snort fonctionne comme un service de conteneur virtuel sur les routeurs à services intégrés Cisco 4000 et les routeurs à services cloud 1000v.

La fonctionnalité Snort IPS fonctionne comme un mode de détection ou de prévention des intrusions sur le réseau et fournit des fonctionnalités IPS ou IDS sur les routeurs à services intégrés Cisco 4000 et les routeurs à services cloud 1000v.

- Surveille le trafic réseau et effectue des analyses par rapport à un ensemble de règles défini.
- Effectue la classification des pièces jointes.
- Appelle des actions par rapport aux règles correspondantes.

En fonction des besoins du réseau. Snort IPS peut être activé comme 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, inspecte le trafic et signale les alertes comme le fait le système IDS, mais des mesures sont prises pour empêcher les attaques.

Le Snort IPS fonctionne en tant que service sur les routeurs ISR. Les conteneurs de services utilisent la technologie de virtualisation pour fournir un environnement d'hébergement sur les périphériques Cisco pour les applications. L'inspection du trafic Snort est activée sur une base par interface ou globalement sur toutes les interfaces prises en charge. Le capteur Snort nécessite deux interfaces VirtualPortGroup. Le premier VirtualPortGroup est utilisé pour le trafic de gestion et le second pour le trafic de données entre le plan de transfert et le service de conteneur virtuel Snort. Des adresses IP d'estimation doivent être configurées pour ces interfaces VirtualPortGroup. Le sous-réseau IP affecté à l'interface de gestion VirtualPortGroup doit pouvoir communiquer avec le serveur de signatures et le serveur d'alertes/rapports.

Snort IPS surveille le trafic et signale les événements à un serveur de journalisation externe ou au

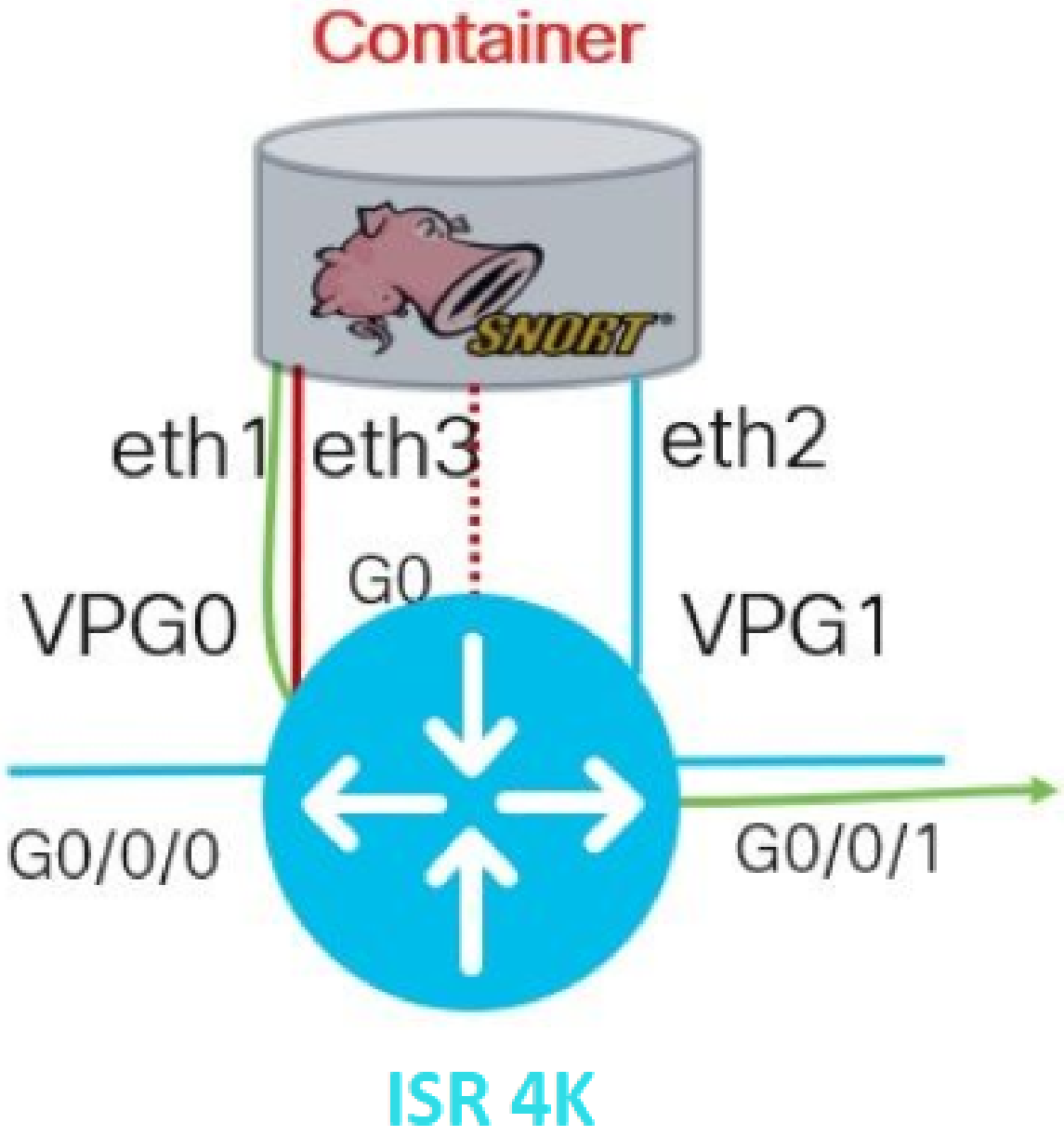
syslog IOS. L’activation de la journalisation dans le syslog IOS peut avoir un impact sur les performances en raison du volume potentiel de messages de journalisation. Des outils de surveillance tiers externes, qui prennent en charge les journaux Snort, peuvent être utilisés pour la collecte et l'analyse des journaux.

Snort IPS sur les routeurs à services intégrés Cisco 4000 et les routeurs à services cloud Cisco 1000v repose sur le téléchargement du package Signature. Il existe deux types d'abonnement :

- Package de signature communautaire.
- Package de signatures basé sur l'abonné.

L'ensemble de règles du package de signatures de la communauté offre une couverture limitée contre les menaces. L'ensemble de règles de package de signatures basé sur les abonnés offre la meilleure protection contre les menaces. Il inclut une couverture anticipée des exploits et fournit également l'accès le plus rapide aux signatures mises à jour en réponse à un incident de sécurité ou à la découverte proactive d'une nouvelle menace. Cet abonnement est entièrement pris en charge par Cisco et le package sera mis à jour sur Cisco.com. Le package de signature peut être téléchargé à l'adresse software.cisco.com. Les informations relatives à la signature Snort sont disponibles sur snort.org.

Diagramme du réseau



Configurer

Configuration UTD de la plate-forme

Étape 1. Configurez les interfaces VirtualPortGroups.

```
Router#configure terminal
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 192.168.2.1 255.255.255.252
Router(config-if)#no shutdown
Router(config-if)#exit
```

Étape 2. Activer l'environnement IOx en mode de configuration globale

```
Router(config)#iox
```

Étape 3. Configurez l'hébergement d'applications avec la configuration vnic.

```
Router(config)#app-hosting appid UTD
Router(config-app-hosting)#app-vnic gateway0 virtualportgroup 0 guest-interface 0
Router(config-app-hosting-gateway0)#guest-ipaddress 192.168.1.2 netmask 255.255.255.252
Router(config-app-hosting-gateway0)#exit

Router(config-app-hosting)#app-vnic gateway1 virtualportgroup 1 guest-interface 1
Router(config-app-hosting-gateway0)#guest-ipaddress 192.168.2.2 netmask 255.255.255.252
Router(config-app-hosting-gateway0)#exit
```

Étape 4 (facultatif). Configurer le profil de ressources.

```
Router(config-app-hosting)#app-resource package-profile low [low,medium,high]
Router(config-app-hosting)#end
```

Remarque : Si ce paramètre n'est pas défini, le système utilise la configuration par défaut de la ressource d'application (Low). Assurez-vous de disposer de suffisamment de ressources sur le routeur de service intégré si la configuration de profil par défaut est modifiée.

Étape 5. Installez l'hébergement d'applications à l'aide du fichier UTD.tar.

```
Router#app-hosting install appid UTD package bootflash:iox-iosxe-utd.16.12.08.1.0.24_SV2.9.16.1_XE16.12
```

Remarque : conservez le fichier UTD.tar correct sur bootflash: pour continuer l'installation. La version Snort est spécifiée sur le nom de fichier UTD.

Les journaux système suivants indiquent que le service UTD a été installé correctement.

```
Installing package 'bootflash:iox-iosxe-utd.16.12.08.1.0.24_SV2.9.16.1_XE16.12
*Jun 26 19:25:35.975: %VMAN-5-PACKAGE_SIGNING_LEVEL_ON_INSTALL: R0/0: vman: Pa
*Jun 26 19:25:50.746: %VIRT_SERVICE-5-INSTALL_STATE: Successfully installed vi
*Jun 26 19:25:53.176: %IM-6-INSTALL_MSG: R0/0: ioxman: app-hosting: Install su
```

Remarque : avec 'show app-hosting list' l'état doit être 'Deployed'

Étape 6. Démarrez le service d'hébergement d'applications.

```
Router#configure terminal
Router(config)#app-hosting appid UTD
Router(config-app-hosting)#start
Router(config-app-hosting)#end
```

Remarque : après le démarrage du service d'hébergement d'applications, l'état de l'hébergement d'applications doit être « En cours d'exécution ». Utilisez 'show app-hosting list' ou 'show app-hosting detail' pour afficher plus de détails.

Les messages syslog suivants doivent s'afficher pour indiquer que le service UTD a été installé correctement.

```
*Jun 26 19:55:05.362: %VIRT_SERVICE-5-ACTIVATION_STATE: Successfully activated
*Jun 26 19:55:07.412: %IM-6-START_MSG: R0/0: ioxman: app-hosting: Start succee
```

Configuration du plan de service et du plan de données.

Une fois l'installation terminée, le plan de service doit être configuré. Snort IPS peut être configuré en tant que système de prévention des intrusions (IPS) ou système de détection des intrusions (IDS) pour inspection.

Avertissement : vérifiez que la fonction de licence 'securityk9' est activée pour poursuivre la configuration du plan de service UTD.

Étape 1. Configurer le moteur standard Unified Threat Defense (UTD) (plan de service)

```
Router#configure terminal
Router(config)#utd engine standard
```

Étape 2. Activer la consignation des messages d'urgence sur un serveur distant.

```
Router(config-utd-eng-std)#logging host 192.168.10.5
```

Étape 3. Activez l'inspection des menaces pour Snort Engine.

```
Router(config-utd-eng-std)#threat-inspection
```

Étape 4. Configurer la détection des menaces comme système de prévention des intrusions (IPS) ou système de détection des intrusions (IDS)

```
Router(config-utd-engstd-insp)#threat [protection,detection]
```

Remarque : 'Protection' est utilisé pour IPS et 'Detection' pour IDS. 'Detection' est la valeur par défaut.

Étape 5. Configurer la stratégie de sécurité.

```
Router(config-utd-engstd-insp)#policy [balanced, connectivity, security]
Router(config-utd-engstd-insp)#exit
Router(config-utd-eng-std)#exit
```

Remarque : la stratégie par défaut est « équilibrée »

Étape 6 (facultatif). Créer la liste autorisée UTD (liste blanche)

```
Router#configure terminal
Router(config)#utd threat-inspection whitelist
```

Étape 7 (facultatif). Configurez les ID des signatures de sniffage pour qu'ils apparaissent dans la liste blanche.

```
Router(config-utd-whitelist)#generator id 40 signature id 54621 comment FILE-OFFICE traffic from networ
Router(config-utd-whitelist)#end
```

Remarque : l'ID'40' est utilisé à titre d'exemple. Afin de vérifier les informations de Snort Signature, consultez la documentation officielle de Snort.

Étape 8 (facultatif). Activer la liste autorisée dans la configuration d'inspection des menaces.

```
Router#config terminal
Router(config)#utd engine standard
Router(config-utd-eng-std)#threat-inspection
Router(config-utd-engstd-insp)#whitelist
```

Étape 9. Configurez l'intervalle de mise à jour des signatures pour télécharger automatiquement les signatures de sniffage.

```
Router#config terminal
Router(config)#utd engine standard
Router(config-utd-eng-std)#threat-inspection
Router(config-utd-engstd-insp)#signature update occur-at [daily, monthly, weekly] 0 0
```

Remarque : le premier nombre définit l'heure au format 24 heures et le second nombre indique les minutes.

Avertissement : les mises à jour des signatures UTD entraînent une brève interruption du service au moment de la mise à jour.

Étape 10. Configurez les paramètres du serveur de mise à jour des signatures.

```
Router(config-utd-engstd-insp)#signature update server [cisco, url] username cisco password cisco12
```

Remarque : utilisez 'cisco' pour utiliser le serveur Cisco ou 'url' pour définir un chemin d'accès personnalisé pour le serveur de mise à jour. Pour le serveur Cisco, vous devez

fournir vos propres nom d'utilisateur et mot de passe.

Étape 11. Activer le niveau de journalisation.

```
Router(config-utd-engstd-insp)#logging level [alert,crit,debug,emerg,info,notice,warning]
Router(config-utd-engstd-insp)#exit
Router(config-utd-eng-std)#exit
```

Étape 12. Activez le service UDT.

```
Router#configure terminal
Router(config)#utd
```

Étape 13 (facultatif). Rediriger le trafic de données de l'interface VirtualPortGroup vers le service UTD.

```
Router#configure terminal
Router(config)#utd
Router(config-utd)#redirect interface virtualPortGroup
```

Remarque : si la redirection n'est pas configurée, elle est automatiquement détectée.

Étape 14. Activez l'UTD pour toutes les interfaces de couche 3 sur ISR.

```
Router(config-utd)#all-interfaces
```

Étape 15. Activez la norme du moteur.

```
Router(config-utd)#engine standard
```

Les messages syslog suivants doivent s'afficher pour indiquer que le mode UTD a été activé correctement.

```
*Jun 27 23:41:03.062: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0,
*Jun 27 23:41:13.039: %IOSXE-2-PLATFORM: R0/0: cpp_cp: QFP:0.0 Thread:000 TS:0
*Jun 27 23:41:22.457: %IOSXE-5-PLATFORM: R0/0: cpp_cp: QFP:0.0 Thread:000 TS:0
```

Étape 16 (facultatif). Définir l'action pour la défaillance du moteur UTD (plan de données UTD)

```
Router(config-engine-std)#fail close
Router(config-engine-std)#end
Router#copy running-config startup-config
Destination filename [startup-config]?
```

Remarque : l'option « Fail close » supprime tout le trafic IPS/IDS lorsque le moteur UTD tombe en panne. L'option Fail open autorise tout le trafic IPS/IDS sur les pannes UTD. L'option par défaut est 'fail open'.

Vérifier

Vérifiez l'adresse IP et l'état de l'interface VirtualPortGroups.

```
Router#show ip interface brief | i VirtualPortGroup
VirtualPortGroup0 192.168.1.1 YES NVRAM up up
VirtualPortGroup1 192.168.2.1 YES NVRAM up up
```

Vérifiez la configuration de VirtualPortGroup.

```
Router#show running-config | b interface
interface VirtualPortGroup0
description Management Interface
ip address 192.168.1.1 255.255.255.252
!
interface VirtualPortGroup1
description Data Interface
ip address 192.168.2.1 255.255.255.252
!
```

Vérifiez la configuration de l'hébergement des applications.

```
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 192.168.2.2 netmask 255.255.255.252
start
end
```

Vérifiez l'activation de iox.

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

Vérifiez la configuration du plan de service UTD.

```
Router#show running-config | b engine
utd engine standard
logging host 192.168.10.5
threat-inspection
threat protection
policy security
signature update server cisco username cisco password KcEDIO[gYafNZheBHBD`CC\g`_cSeFAAB
signature update occur-at daily 0 0
logging level info
whitelist
utd threat-inspection whitelist
generator id 40 signature id 54621 comment FILE-OFFICE traffic
utd
all-interfaces
redirect interface VirtualPortGroup1
engine standard
fail close
```

```
Router#show utd engine standard config
UTD Engine Standard Configuration:

IPS/IDS : Enabled

Operation Mode : Intrusion Prevention
Policy : Security

Signature Update:
Server : cisco
User Name : cisco
Password : KcEDIO[gYafNZheBHBD`CC\g`_cSeFAAB
Occurs-at : daily ; Hour: 0; Minute: 0

Logging:
Server : 192.168.10.5
Level : info
Statistics : Disabled
Hostname : router
```

```
System IP : Not set

Whitelist : Enabled
Whitelist Signature IDs:
54621, 40

 Port Scan : Disabled

Web-Filter : Disabled
```

Vérifiez l'état d'hébergement des applications.

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

Vérifiez les détails d'hébergement des applications.

```
Router#show app-hosting detail
App id : UTD
Owner : ioxm
State : RUNNING
Application
Type : LXC
Name : UTD-Snort-Feature
Version : 1.0.7_SV2.9.18.1_XE17.9
Description : Unified Threat Defense
Author :
Path : /bootflash/secapp-utd.17.09.03a.1.0.7_SV2.9.18.1_XE17.9.x86_64.tar
URL Path :
Multicast : yes
Activated profile name :

Resource reservation
Memory : 1024 MB
Disk : 752 MB
CPU :
CPU-percent : 25 %
VCPU : 0

Platform resource profiles
Profile Name CPU(unit) Memory(MB) Disk(MB)
----------------------------------------------------------------

Attached devices
Type Name Alias
---------------------------------------------
Disk /tmp/xml/UtdLogMappings-IOX
Disk /tmp/xml/UtdIpsAlert-IOX
Disk /tmp/xml/UtdDaqWcapi-IOX
Disk /tmp/xml/UtdUrlf-IOX
Disk /tmp/xml/UtdTls-IOX
```

```
Disk /tmp/xml/UtdDaq-IOX
Disk /tmp/xml/UtdAmp-IOX
Watchdog watchdog-503.0
Disk /tmp/binos-IOX
Disk /opt/var/core
Disk /tmp/HTX-IOX
Disk /opt/var
NIC ieobc_1 ieobc
Disk _rootfs
NIC mgmt_1 mgmt
NIC dp_1_1 net3
NIC dp_1_0 net2
Serial/Trace serial3

Network interfaces
---------------------------------------
eth0:
MAC address : 54:0e:00:0b:0c:02
IPv6 address : ::
Network name :
eth:
MAC address : 6c:41:0e:41:6b:08
IPv6 address : ::
Network name :
eth2:
MAC address : 6c:41:0e:41:6b:09
IPv6 address : ::
Network name :
eth1:
MAC address : 6c:41:0e:41:6b:0a
IPv4 address : 192.168.2.2
IPv6 address : ::
Network name :

-------------------------------------------------------------------------
Process Status Uptime # of restarts
-------------------------------------------------------------------------
climgr UP 0Y 0W 0D 21:45:29 2
logger UP 0Y 0W 0D 19:25:56 0
snort_1 UP 0Y 0W 0D 19:25:56 0

Network stats:
eth0: RX packets:162886, TX packets:163855
eth1: RX packets:46, TX packets:65

DNS server:
domain cisco.com
nameserver 192.168.90.92

Coredump file(s): core, lost+found

Interface: eth2
ip address: 192.168.2.2/30
Interface: eth1
ip address: 192.168.1.2/30

Address/Mask Next Hop Intf.
-------------------------------------------------------------------------------
0.0.0.0/0 192.168.2.1 eth2
0.0.0.0/0 192.168.1.1 eth1
```

Dépannage

1. Assurez-vous que le routeur à services intégrés (ISR) Cisco exécute XE 16.10.1a et versions ultérieures (pour la méthode IOx)

2. Assurez-vous que le routeur à services intégrés (ISR) Cisco est sous licence avec la fonction SecurityKit9 activée.

3. Vérifiez que le modèle matériel du routeur de service intégré est conforme au profil de ressources minimum.

4. Fonction non compatible avec le cookie SYN du pare-feu basé sur les zones et la traduction d'adresses réseau 64 (NAT64)

5. Confirmez que le service UTD est démarré après l'installation.

6. Lors du téléchargement manuel du package Signature, assurez-vous que la version du package est identique à celle du moteur Snort. La mise à jour du package de signatures peut échouer en cas de non-concordance de version.

7. En cas de problèmes de performances, utilisez les 'show app-hosting resource' et 'show app-hosting using appid"UTD-NAME' pour en savoir plus sur la consommation CPU/mémoire/stockage.

```
Router#show app-hosting resource
CPU:
Quota: 75(Percentage)
Available: 50(Percentage)
VCPU:
Count: 6
Memory:
Quota: 10240(MB)
Available: 9216(MB)
Storage device: bootflash
Quota: 4000(MB)
Available: 4000(MB)
Storage device: harddisk
Quota: 20000(MB)
Available: 19029(MB)
Storage device: volume-group
Quota: 190768(MB)
Available: 169536(MB)
Storage device: CAF persist-disk
Quota: 20159(MB)
Available: 18078(MB)
```

```
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
```

Avertissement : si vous constatez une utilisation élevée du processeur, de la mémoire ou du disque, contactez le centre d'assistance technique Cisco.

Débogage

Utilisez les commandes debug répertoriées ci-dessous pour collecter des informations sur Snort IPS en cas de défaillance.

<#root>

debug virtual-service all

debug virtual-service virtualPortGroup

debug virtual-service messaging

debug virtual-service timeout

debug utd config level error [error, info, warning]
debug utd engine standard all

Informations connexes

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

Guide de configuration de la sécurité Snort IPS

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_utd/configuration/xe-17/sec-data-utd-xe-17-book/snort-ips.html

Profil de ressource de service virtuel

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_utd/configuration/xe-17/sec-data-utd-

xe-17-book/snort-ips.html#id_31952

Snort IPS sur les routeurs - Configuration pas à pas.

https://community.cisco.com/t5/security-knowledge-base/router-security-snort-ips-on-routers-step-by-step-configuration/ta-p/3369186

Dépannage de Snort IPS

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_utd/configuration/xe-17/sec-data-utd-xe-17-book/snort-ips.html#concept_C3C869E633A6475890475931DF83EBCC

ISR4K Snort IPS n'est pas déployé car le matériel ne dispose pas de suffisamment de ressources de plate-forme

https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwf57595

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.