Bereitstellung von Snort IPS auf Cisco Integrated Services Routern der Serie 4000

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie die Snort IPS- und Snort IDS-Funktion mithilfe der IOx-Methode auf den Cisco Integrated Services Routern (ISR) der Serie 4000 bereitstellen.

Voraussetzungen

Anforderungen

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

- Cisco Integrated Services Router der Serie 4000 mit mindestens 8 GB DRAM
- Grundlegende IOS-XE-Befehlserfahrung
- Grundlegendes Snort-Wissen.
- Ein Abonnement für 1 oder 3 Jahre ist erforderlich.
- IOS-XE 16.10.1a und höher

Verwendete Komponenten

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

- ISR4331/K9 mit Version 17.9.3a
- UTD Engine TAR für Version 17.9.3a.
- Security9-Lizenz für ISR4331/K9.

Die VMAN-Methode ist inzwischen veraltet.

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

möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Die Snort IPS-Funktion aktiviert Intrusion Prevention System (IPS) oder Intrusion Detection System (IDS) für Zweigstellen auf Cisco Integrated Services Routern der Serie 4000 und der Cisco Cloud Services Router der Serie 1000v. Diese Funktion verwendet Open-Source Snort, um IPS- und IDS-Funktionen zu aktivieren.

Snort ist ein Open-Source-IPS, das Datenverkehrsanalysen in Echtzeit durchführt und Warnmeldungen generiert, wenn in IP-Netzwerken Bedrohungen erkannt werden. Sie kann außerdem Protokollanalysen durchführen, Inhalte recherchieren oder marschieren und eine Vielzahl von Angriffen und Tests erkennen, z. B. Pufferüberläufe, Stealth-Port-Scans usw. Die Snort Engine wird als virtueller Container-Service auf den Cisco Integrated Services Routern der Serie 4000 und den Cloud Services Routern der Serie 1000v ausgeführt.

Die Snort IPS-Funktion dient als Erkennungs- oder Präventionsmodus für Netzwerkeingriffe und stellt IPS- oder IDS-Funktionen für die Cisco Integrated Services Router der Serie 4000 und die Cloud Services Router der Serie 1000v bereit.

- Überwacht den Netzwerkverkehr und analysiert ihn anhand eines definierten Regelsatzes.
- Führt Klassifizierung von Anhängen durch.
- Führt Aktionen für übereinstimmende Regeln auf.

Abhängig von den Netzwerkanforderungen Snort IPS kann als IPS oder IDS aktiviert werden. Im IDS-Modus prüft Snort den Datenverkehr und gibt Warnmeldungen aus, ergreift jedoch keine Maßnahmen zur Verhinderung von Angriffen. Im IPS-Modus wird der Datenverkehr geprüft und es werden wie bei IDS Warnmeldungen gemeldet, es werden jedoch Maßnahmen zur Verhinderung von Angriffen ergriffen.

Das Snort IPS wird als Service auf ISR-Routern ausgeführt. Servicecontainer nutzen Virtualisierungstechnologie, um eine Hosting-Umgebung für Anwendungen auf Cisco Geräten bereitzustellen. Snort Traffic Inspection ist entweder schnittstellenbasiert oder global auf allen unterstützten Schnittstellen aktiviert. Der Snort-Sensor erfordert zwei VirtualPortGroup-Schnittstellen. Die erste VirtualPortGroup wird für den Verwaltungsverkehr und die zweite für den Datenverkehr zwischen der Weiterleitungsebene und dem virtuellen Container-Service von Snort verwendet. Für diese VirtualPortGroup-Schnittstellen müssen wahrscheinlich IP-Adressen konfiguriert werden. Das der VirtualPortGroup Management-Schnittstelle zugewiesene IP-Subnetz muss mit dem Signatur- und Warnmeldungs-/Berichtsserver kommunizieren können.

Das Snort IPS überwacht den Datenverkehr und meldet Ereignisse an einen externen Protokollserver oder das IOS-Syslog. Die Aktivierung der Protokollierung im IOS-Syslog kann sich auf die Leistung auswirken, da möglicherweise große Mengen von Protokollmeldungen vorhanden sind. Externe Überwachungstools von Drittanbietern, die Snort-Protokolle unterstützen, können zur Protokollsammlung und -analyse verwendet werden.

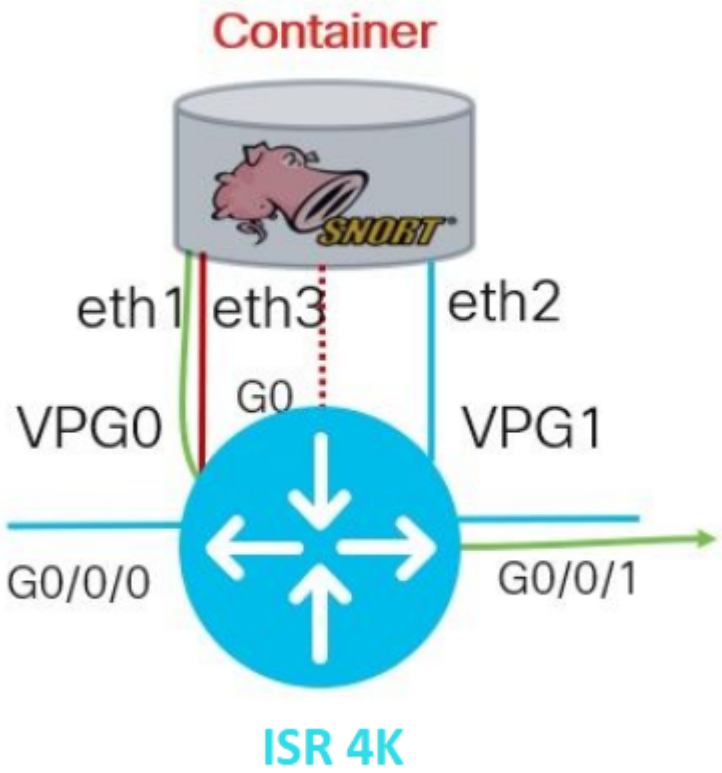
Snort IPS auf Cisco Integrated Services Routern der Serie 4000 und Cisco Cloud Services Routern der Serie 1000v basiert auf dem Download des Signaturpakets. Es gibt zwei Arten von Abonnements:

- Signaturpaket der Community.
- Abonnentenbasiertes Signaturpaket.

Der Regelsatz für das Community-Signaturpaket bietet eine begrenzte Abdeckung für Bedrohungen. Der Regelsatz für abonnentenbasierte Signaturpakete bietet den besten Schutz vor Bedrohungen. Sie deckt Exploits bereits im Voraus ab und bietet den schnellsten Zugriff auf aktualisierte Signaturen, wenn ein Sicherheitsvorfall eintritt oder eine neue Bedrohung proaktiv erkannt wird. Dieses Abonnement wird von

Cisco vollständig unterstützt, und das Paket wird unter Cisco.com aktualisiert. Das Signaturpaket kann unter software.cisco.com heruntergeladen werden. Informationen zur Snort-Signatur finden Sie unter snort.org.

Netzwerkdiagramm



Konfigurieren

Plattform-UTD-Konfiguration

Schritt 1: Konfigurieren Sie Virtual VirtualPortGroups-Schnittstellen.

```
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
```

Schritt 2: Aktivieren der IOx-Umgebung im globalen Konfigurationsmodus

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

Schritt 3: Konfigurieren Sie App-Hosting mithilfe der vNIC-Konfiguration.

```
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
```

Schritt 4 (optional). Ressourcenprofil konfigurieren.

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

> **Anmerkung:** *Wenn dies nicht definiert ist, verwendet das System die Standard-App-Ressourcenkonfiguration (Niedrig). Vergewissern Sie sich, dass genügend Ressourcen auf dem ISR verfügbar sind, wenn die Standardprofilkonfiguration geändert wird.*

Schritt 5: Installieren Sie das App-Hosting mithilfe der Datei 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.
```

> **Hinweis**: Behalten Sie die richtige UTD.tar Datei beim Bootflash bei: um mit der Installation fortzufahren. Die Snort-Version ist für den UTD-Dateinamen angegeben.

Die nächsten Syslogs zeigen an, dass der UTD-Dienst ordnungsgemäß installiert wurde.

```
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
```

> **Hinweis**: Bei Verwendung von *'Show app-hosting list*' sollte der Status '*Deployed' lauten.*

Schritt 6: Starten Sie den App-Hosting-Dienst.

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

> **Hinweis**: Nach dem Start des App-Hosting-Dienstes sollte der App-Hosting-Status auf "*Running" (Wird ausgeführt) gesetzt werden.* Verwenden Sie *'Show app-hosting list' oder 'show app-hosting detail',* um weitere Details anzuzeigen.

Die nächsten Syslog-Meldungen zeigen an, dass der UTD-Dienst ordnungsgemäß installiert wurde.

```
*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
```

Konfiguration der Service- und Datenebene.

Nach der erfolgreichen Installation muss die Serviceebene konfiguriert werden. Snort IPS kann für die Inspektion als Intrusion Prevention System (IPS) oder Intrusion Detection System (IDS) konfiguriert werden.

> **Warnung:** Bestätigen Sie, dass die Lizenzfunktion *"securityk9"* aktiviert ist, um mit der Konfiguration der UTD-Serviceebene fortzufahren.

Schritt 1: Konfigurieren der Unified Threat Defense (UTD)-Standard-Engine (Serviceebene)

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

Schritt 2: Aktivieren Sie die Protokollierung von Notfallmeldungen an einen Remote-Server.

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

Schritt 3: Aktivieren Sie die Bedrohungsprüfung für die Snort-Engine.

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

Schritt 4: Konfigurieren Sie die Erkennung von Sicherheitsrisiken als Intrusion Prevention System (IPS) oder Intrusion Detection System (IDS).

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

Hinweis: *'Protection'* wird für IPS und *'Detection'* für IDS verwendet. *'Detection'* ist die Standardeinstellung.

Schritt 5: Konfigurieren der Sicherheitsrichtlinie

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

Hinweis: Die Standardrichtlinie ist *ausgeglichen.*

Schritt 6 (optional). Erstellen der Liste der zulässigen UTD-Adressen (Whitelist)

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

Schritt 7 (optional). Konfigurieren Sie Snort Signatures IDs so, dass sie in der Whitelist angezeigt werden.

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

Hinweis: Die ID *'40*' dient als Beispiel. Um die Informationen zur Snort-Signatur zu überprüfen, überprüfen Sie die offizielle Snort-Dokumentation.

Schritt 8 (optional). Aktiviert die Liste der zulässigen Bedrohungen in der Konfiguration für die Bedrohungsprüfung.

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

Schritt 9. Konfigurieren Sie das Aktualisierungsintervall für die Signatur so, dass Snort Signatures automatisch heruntergeladen wird.

```
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
```

Hinweis: Die erste Zahl definiert die Stunde im 24-Stunden-Format, die zweite Zahl steht für Minuten.

Warnung: UTD-Signatur-Updates führen zum Zeitpunkt der Aktualisierung zu einer kurzen Dienstunterbrechung.

Schritt 10. Konfigurieren Sie die Parameter des Signatur-Aktualisierungsservers.

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

Hinweis: Verwenden Sie "*cisco*", um den Cisco Server zu verwenden, oder *"url*", um einen benutzerdefinierten Pfad für den Update-Server zu definieren. Für den Cisco Server müssen Sie Ihren eigenen Benutzernamen und Ihr eigenes Kennwort eingeben.

Schritt 11. Aktivieren Sie die Protokollierungsebene.

```
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
```

Schritt 12: Aktivieren Sie den UTD-Dienst.

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

Schritt 13 (optional). Leiten Sie den Datenverkehr von der VirtualPortGroup-Schnittstelle an den UTD-Dienst um.

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

Hinweis: Wenn die Umleitung nicht konfiguriert ist, wird sie automatisch erkannt.

Schritt 14: Aktivieren Sie UTD für alle Layer-3-Schnittstellen des ISR.

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

Schritt 15: Aktivieren Sie den Motorstandard.

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

Die nächsten Syslog-Meldungen zeigen an, dass UTD ordnungsgemäß aktiviert wurde.

```
*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
```

Schritt 16 (optional). Aktion für Ausfall des UTD-Moduls definieren (UTD-Datenebene)

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

Hinweis: *Die* Option "*Fail close*" verwirft den gesamten IPS/IDS-Datenverkehr, wenn die UTD-Engine ausfällt. *Die* Option *'Fail open*' ermöglicht den gesamten IPS/IDS-Verkehr bei UTD-Ausfällen. Die Standardoption ist *"Fail Open"*.

Überprüfung

Überprüfen der VirtualPortGroups-IP-Adresse und des Schnittstellenstatus

```
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
```

Überprüfen der VirtualPortGroup-Konfiguration

```
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
!
```

Überprüfen der App-Hosting-Konfiguration

```
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
```

Überprüfen Sie die IoX-Aktivierung.

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

Überprüfen der Konfiguration der UTD-Serviceebene

```
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
```

Überprüfen des App-Hosting-Status

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

Überprüfen Sie die App-Hosting-Details.

```
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
```

Fehlerbehebung

1. Sicherstellen, dass auf dem Cisco Integrated Services Router (ISR) XE 16.10.1a und höher ausgeführt wird (für IOx-Methode)

2. Stellen Sie sicher, dass der Cisco Integrated Services Router (ISR) mit aktivierter Security900-Funktion lizenziert ist.

3. Überprüfen Sie, ob das ISR-Hardwaremodell mit dem minimalen Ressourcenprofil übereinstimmt.

4. Funktion nicht kompatibel mit Zone-Based Firewall SYN-Cookie und Network Address Translation 64 (NAT64)

5. Bestätigen Sie, dass der UTD-Dienst nach der Installation gestartet wird.

6. Stellen Sie beim manuellen Herunterladen des Signaturpakets sicher, dass das Paket die gleiche Version wie die Snort-Engine-Version hat. Die Aktualisierung des Signaturpakets schlägt möglicherweise fehl, wenn eine Versionskonflikt vorliegt.

7. Verwenden Sie bei Leistungsproblemen die ***App-Hosting-Ressource anzeigen*** und die ***App-Hosting-Nutzungsanwendung UTD-NAME anzeigen,*** um mehr über die CPU-/Speicher-/Speicherauslastung zu erfahren.

```
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
```

> **Warnung:** Wenn Sie eine hohe CPU-, Arbeitsspeicher- oder Festplattennutzung feststellen können, wenden Sie sich an das Cisco TAC.

Debuggen

Verwenden Sie die unten aufgeführten Debug-Befehle, um bei einem Fehler Informationen zu Snort IPS zu sammeln.

<#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
```

Zugehörige Informationen

Weitere Dokumente zur Snort IPS-Bereitstellung finden Sie hier:

Snort IPS Security - Konfigurationsleitfaden

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

Virtuelles Service-Ressourcenprofil

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 auf Routern - schrittweise Konfiguration.

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

Fehlerbehebung: 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 wird nicht bereitgestellt, da die HW nicht über ausreichende Plattformressourcen verfügt

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

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.