Ciscoサービス統合型ルータ4000シリーズでのSnort IPSの導入

内容

はじめに

このドキュメントでは、IOx方式を使用してCiscoサービス統合型ルータ(ISR)4000シリーズにSnort IPSおよびSnort IDS機能を導入する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- 8 GB以上のDRAMを搭載したCiscoサービス統合型ルータ(ISR)4000シリーズ
- 基本的なIOS-XEコマンドエクスペリエンス。
- Snortの基礎知識。
- 1年または3年のシグニチャサブスクリプションが必要です
- IOS-XE 16.10.1a以降。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- 17.9.3aリリースを実行するISR4331/K9。
- 17.9.3aリリース用UTDエンジンTAR。

- ISR4331/K9用Securityk9ライセンス。

VMANメソッドは廃止されました。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

Snort IPS機能は、Cisco 4000シリーズサービス統合型ルータおよびCiscoクラウドサービスルータ1000vシリーズ上のブランチオフィスで侵入防御システム(IPS)または侵入検知システム(IDS)を有効にします。この機能は、オープンソースのSnortを使用してIPSおよびIDS機能を有効にします。

Snortは、リアルタイムのトラフィック分析を実行し、IPネットワークで脅威が検出されたときにアラートを生成するオープンソースのIPSです。また、プロトコル分析、コンテンツの調査やマーチングを実行し、バッファオーバーフローやステルスポートスキャンなど、さまざまな攻撃やプローブを検出できます。Snortエンジンは、Ciscoサービス統合型ルータ(ISR)4000シリーズおよびCloud Services Router 1000vシリーズの仮想コンテナサービスとして動作します。

Snort IPS機能は、ネットワーク侵入検知または防御モードとして機能し、Ciscoサービス統合型ルータ(ISR)4000シリーズおよびクラウドサービスルータ1000vシリーズでIPSまたはIDS機能を提供します。

- ネットワークトラフィックを監視し、定義済みのルールセットに対して分析します。
- アタッチ分類を実行します。
- 一致したルールに対するアクションを呼び出します。

ネットワーク要件に基づく。Snort IPSはIPSまたはIDSとして有効にできます。IDSモードでは、Snortはトラフィックを検査してアラートを報告しますが、攻撃を防ぐためのアクションは実行しません。IPSモードでは、トラフィックを検査し、IDSと同様にアラートを報告しますが、攻撃を防ぐためにアクションが実行されます。

Snort IPSは、ISRルータ上でサービスとして動作します。サービスコンテナは、仮想化テクノロジーを使用して、アプリケーション用のシスコデバイス上にホスティング環境を提供します。Snortトラフィックインスペクションは、インターフェイス単位またはサポートされているすべてのインターフェイスに対してグローバルに有効になります。Snortセンサーには2つのVirtualPortGroupインターフェイスが必要です。1つ目のVirtualPortGroupは管理トラフィックに使用され、2つ目はフォワーディングプレーンとSnort仮想コンテナサービス間のデータトラフィックに使用されます。これらのVirtualPortGroupインターフェイスにIPアドレスを設定する必要があると推測します。管理VirtualPortGroupインターフェイスに割り当てられたIPサブネットは、シグニチャサーバおよびアラート/レポートサーバと通信できる必要があります。

Snort IPSはトラフィックを監視し、外部ログサーバまたはIOS syslogにイベントを報告します。IOSのsyslogへのロギングを有効にすると、ログメッセージの量が増える可能性があるため、パフォーマンスに影響を与える可能性があります。ログの収集と分析には、Snortログをサポートする

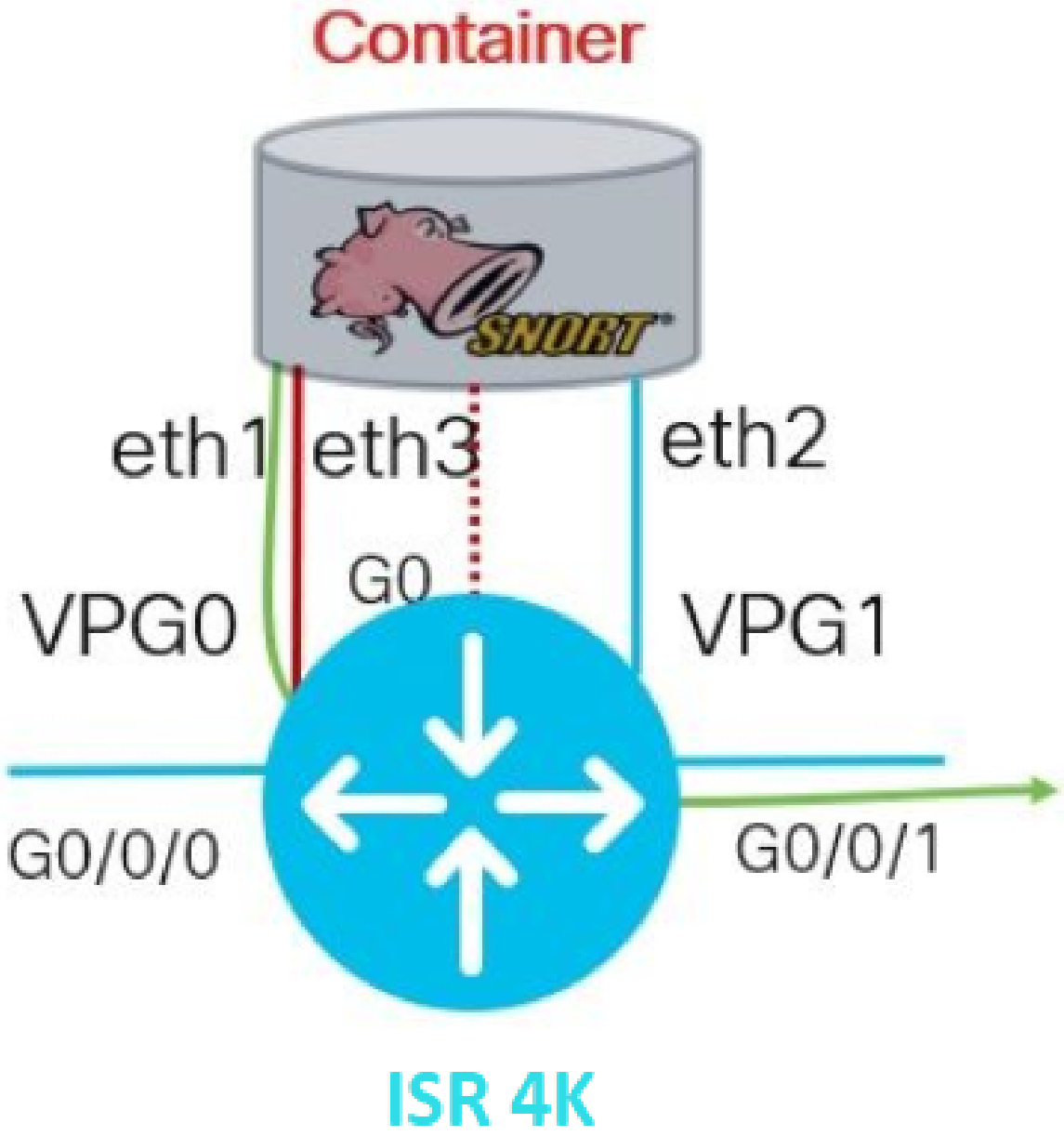
外部のサードパーティ製モニタリングツールを使用できます。

Cisco 4000シリーズサービス統合型ルータおよびCisco Cloud Services Router 1000vシリーズのSnort IPSは、シグニチャパッケージのダウンロードに基づいています。サブスクリプションには2つのタイプがあります。

- コミュニティシグニチャパッケージ。
- 加入者ベースのシグニチャパッケージ。

コミュニティシグニチャパッケージのルールセットでは、脅威に対するカバレッジが制限されています。加入者ベースのシグニチャパッケージのルールセットは、脅威に対する最適な保護を提供します。 また、セキュリティインシデントや新しい脅威の予防的な検出に対応して、更新されたシグニチャへの迅速なアクセスを提供します。このサブスクリプションはシスコによって完全にサポートされ、パッケージはCisco.comで更新されます。シグニチャパッケージは、software.cisco.comからダウンロードできます。Snortシグニチャ情報は、snort.orgで確認できます。

ネットワーク図



設定

プラットフォームUTDの設定

ステップ 1：Virtual VirtualPortGroupsインターフェイスを設定します。

```
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
```

ステップ2：グローバルコンフィギュレーションモードでIOx環境を有効にします。

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

ステップ 3：VNIC設定を使用してアプリケーションホスティングを設定します。

```
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
```

ステップ 4 (任意) ：リソースプロファイルを設定します。

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

注： これが定義されていない場合、システムはデフォルトのapp-resource config(Low)を使用します。デフォルトのプロファイル設定を変更する場合は、ISRで十分なリソースを使用できることを確認します。

ステップ 5：UTD.tarファイルを使用してアプリケーションホスティングをインストールします。

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

注：ブートフラッシュに正しいUTD.tarファイルを保存し、インストールに進みます。UTDファイル名にSnortバージョンが指定されています。

次に、UTDサービスが正しくインストールされたことを示すsyslogが表示されます。

```
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
```

注:「show app-hosting list」を使用すると、ステータスは「Deployed」になります。

手順 6：アプリケーションホスティングサービスを開始します。

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

注：アプリケーションホスティングサービスを開始した後、アプリケーションホスティングのステータスは「実行中」になります。詳細を表示するには、「show app-hosting list」または「show app-hosting detail」を使用してください。

UTDサービスが正しくインストールされたことを示す次のsyslogメッセージが表示されます。

```
*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
```

サービスプレーンとデータプレーンの設定。

インストールが成功したら、サービスプレーンを設定する必要があります。Snort IPSは、インスペクションのために侵入防御システム(IPS)または侵入検知システム(IDS)として設定できます。

警告:UTDサービスプレーンの設定に進むには、「securityk9」ライセンス機能が有効になっていることを確認してください。

ステップ 1：Unified Threat Defense(UTD)標準エンジン（サービスプレーン）の設定

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

ステップ 2：リモートサーバへの緊急メッセージのロギングを有効にします。

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

ステップ 3：Snortエンジンの脅威検査を有効にします。

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

ステップ 4：侵入防御システム(IPS)または侵入検知システム(IDS)としての脅威検出の設定

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

注:IPSには「Protection」（保護）、IDSには「Detection」（検出）が使用されます。「Detection」（検出）がデフォルトです。

ステップ 5：セキュリティポリシーを設定します。

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

注：デフォルトのポリシーは「balanced」

ステップ 6（オプション）：UTD許可リスト（ホワイトリスト）の作成

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

ステップ 7（オプション）：ホワイトリストに表示するSnortシグニチャIDを設定します。

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

```
Router(config-utd-whitelist)#end
```

注:ID '40'が例として使用されています。Snortシグニチャ情報を確認するには、Snortの公式ドキュメントを確認してください。

ステップ 8 (オプション) : 脅威検査の設定で許可リストを有効にします。

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

ステップ 9 : Snortシグニチャを自動的にダウンロードするようにシグニチャの更新間隔を設定します。

```
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
```

注：最初の数字は24時間形式の時間を定義し、2番目の数字は分を示します。

警告:UTDシグニチャのアップデートでは、アップデート時に短いサービス中断が生成されます。

ステップ 10 : シグニチャ更新サーバのパラメータを設定します。

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

注:「cisco」を使用してシスコサーバを使用するか、「url」を使用してアップデートサーバのカスタムパスを定義します。Ciscoサーバの場合は、独自のユーザ名とパスワードを入力する必要があります。

ステップ 11ログレベルを有効にします。

```
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
```

ステップ 12utdサービスを有効にします。

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

ステップ 13（オプション）：VirtualPortGroupインターフェイスからUTDサービスにデータトラフィックをリダイレクトします。

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

 注：リダイレクションが設定されていない場合は、自動的に検出されます。

ステップ 14：ISRのすべてのレイヤ3インターフェイスに対してUTDを有効にします。

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

ステップ 15：エンジン標準を有効にします。

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

次のsyslogメッセージは、UTDが正しくイネーブルにされたことを示します。

```
*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
```

ステップ 16（オプション）：UTDエンジンの障害に対するアクションの定義（UTDデータプレーン）

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

注:「Fail close」オプションは、UTDエンジンが故障したときに、すべてのIPS/IDSトラフィックをドロップします。Fail openオプションは、UTD障害時のすべてのIPS/IDSトラフィックを許可します。デフォルトのオプションは'fail open'です。

確認

VirtualPortGroups IPアドレスとインターフェイスステータスを確認します。

```
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
```

VirtualPortGroupの設定を確認します。

```
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
!
```

アプリケーションホスティングの設定を確認します。

```
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
```

ioxの有効化を確認します。

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

UTDサービスプレーンの設定を確認します。

```
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
```

アプリケーションホスティングの状態を確認します。

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

アプリケーションホスティングの詳細を確認します。

```
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
```

（「トラブルシューティング」）

1.シスコのサービス統合型ルータ(ISR)でXE 16.10.1a以降が稼働していることを確認する（IOx方式の場合）

2. Cisco Integrated Services Router(ISR)のSecurityk9機能のライセンスが有効になっていることを確認します。

3. ISRハードウェアモデルが最小リソースプロファイルに準拠していることを確認します。

4.ゾーンベースファイアウォールSYN-cookieおよびネットワークアドレス変換64(NAT64)と互換性のない機能

5.インストール後にUTDサービスが起動していることを確認します。

6.シグニチャパッケージの手動ダウンロード中に、パッケージのバージョンがSnort工ンジンのバージョンと同じであることを確認します。バージョンが一致しない場合、シグニチャパッケージのアップデートが失敗する可能性があります。

7.パフォーマンスの問題が発生した場合は、CPU/メモリ/ストレージの使用量を調べるには、show app-hosting resourceおよびshow app-hosting utilization appid "UTD-NAMEを使用します。

```
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
```

警告:CPU、メモリ、またはディスクの高使用率が確認できる場合は、Cisco TACにお問い合わせください。

デバッグ

障害発生時にSnort IPS情報を収集するには、次に示すdebugコマンドを使用します。

<#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
```

関連情報

Snort IPSの導入に関連するその他のドキュメントについては、次のサイトを参照してください。

Snort IPSセキュリティ設定ガイド

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

仮想サービスリソースプロファイル

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

ルータ上のSnort IPS：設定手順。

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

Snort IPSのトラブルシューティング

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

ハードウェアに十分なプラットフォームリソースがないため、ISR4K Snort IPSが導入されない

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

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。