サービス統合型ルータ1000シリーズへのSnort IPSの導入

内容

概要

このドキュメントでは、Ciscoサービス統合型ルータ(ISR)1000シリーズにSnort IPS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。

- シスコサービス統合型ルータ1kシリーズ
- 基本的なXE-IOSコマンド
- 基本的なSnortの知識

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。

- 17.03.03リリースを実行しているC1111X-8P
- 17.3.3リリース用UTDエンジンTAR
- ISR1kではセキュリティK9ライセンスが必要
- 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
- XE 17.2.1r以降
- 8 GB DRAMのみをサポートするISRハードウェアモデル

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、初期（デフォルト）設定の状態から起動しています。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(ISR)、Cisco 1000シリーズサービス統合型ルータ（111X、11などのX PID）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)を実現します8 GB DRAMのみをサポートする21X、1161Xなど)およびCisco Cloud Services Router 1000vシリーズこの機能は、Snortエンジンを使用してIPSおよびIDS機能を提供します。

Snortは、リアルタイム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ネットワークIPSです。また、プロトコル分析、コンテンツ検索またはマッチングを実行し、バッファオーバーフロー、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することもできます。Snort IPS機能は、IPSまたはIDS機能を提供するネットワーク侵入検知および防御モデルで動作します。ネットワーク侵入検知および防御モードでは、Snortは次のアクションを実行します

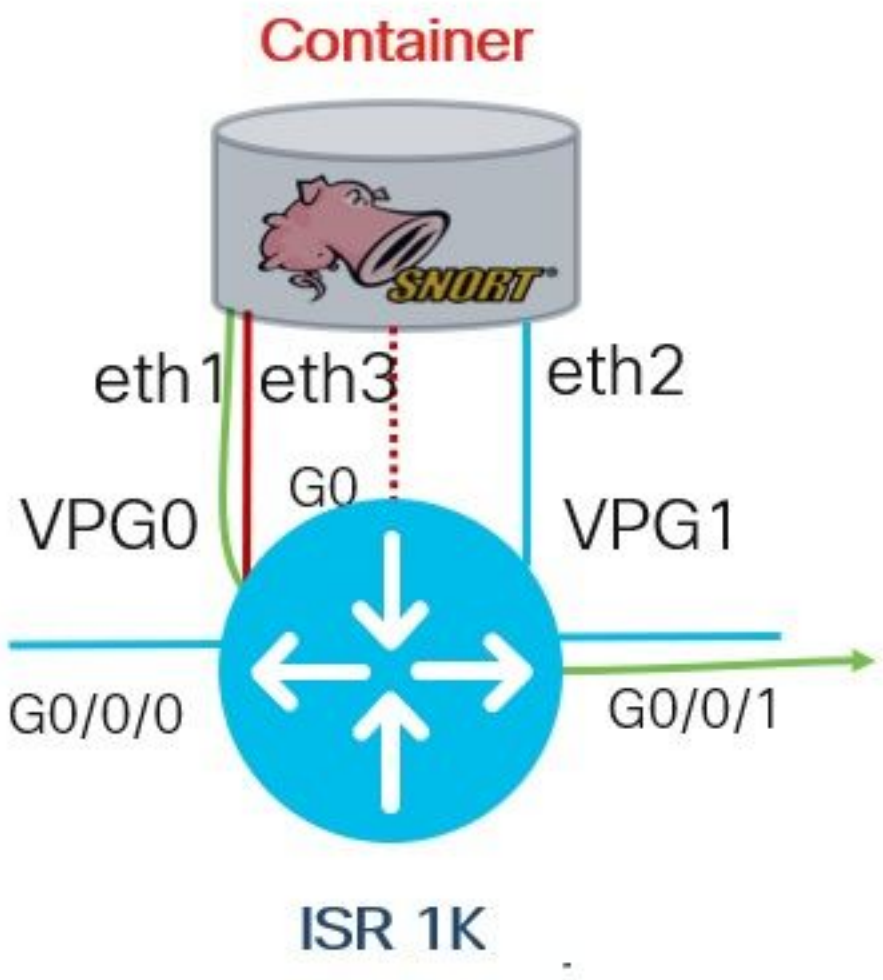
- ネットワークトラフィックを監視し、定義されたルールセットに対して分析する
- 実行された攻撃の分類
- 一致したルールに対するアクションの呼び出し

要件に基づいて、SnortはIPSモードまたはIDSモードで有効にできます。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、攻撃を防止するアクションは実行しません。IPSモードでは、侵入検知に加えて、攻撃を防止するためのアクションが実行されます。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 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ため、パフォーマンスに影響が出る可能性があります。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は、ログの収集と分析に使用できます。

Ciscoサービス統合型ルータ(ISR)にSnort IPSを設定する主な方法は、VMAN方式とIOx方式の2つです。VMANメソッドはutd.ovaファイルを使用し、IOxはutd.tarファイルを使用します。IOxは、Ciscoサービス統合型ルータ(ISR)1kシリーズでのSnort IPS導入に適した適切な方法です。

Snort IPSは、XE 17.2.1r以降を搭載したシスコサービス統合型ルータ(ISR)1kシリーズに導入できます。

ネットワーク図



設定

*ステップ1:*ポートグループの設定

```
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
```

*ステップ2:*仮想サービスのアクティブ化、設定、変更のコミット

```
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
```

ステップ3:仮想サービスの設定

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

ステップ4:UTD（サービスプレーン）の設定

```
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
```

> **注：** 注：***脅威の保護***によりSnort as IPSが、脅威の検出により*り*Snort as IDSが有効になります。

ステップ5:UTD（データプレーン）の設定

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

> **注：*fail openはデフォルト設定です。***

確認

ポートグループのIPアドレスとインターフェイスの状態の確認

```
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
```

ポートグループ設定の確認

```
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
!
```

仮想サービス設定の確認

```
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
```

> **注：*start*コマンドが存在すること*を確認し*てください。存在しない場合は、アクティブ化が成功し、起動しません。**

仮想サービスアクティベーションを確認します。

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

> **注：*ioxが仮想*サービスをアクティブにします。**

UTD設定（サービスプレーンおよびデータプレーン）の確認

```
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
```

アプリケーションホスティング状態の確認

```
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状態を詳細で確認します

```
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
```

トラブルシューティング

1.シスコサービス統合型ルータ(ISR)がXE 17.2.1r以上を実行していることを確認する

2.セキュリティK9でシスコサービス統合型ルータ(ISR)のライセンスを確実に取得する

3. ISRハードウェアモデルが8 GB DRAMのみをサポートしていることを確認します

4. IOS XEソフトウェアとUTD Snort IPS Engineソフトウェア（.tarファイル）のUTDファイルがIOS XEソフトウェアと一致する必要があることを確認します。インストールが失敗して互換性がない可能性があります

> **注**：ソフトウェアは、次のリンクを使用してダウンロードできます。 https://software.cisco.com/download/home/286315006/type

5. **ioxおよびstart**コマンドを使用してUTDサービスをアクティブ化および開始することを確認します。このコマンドは手順2の「***設定」セクション***の下に***表示さ***れます

6. Snortのアクティベーション後に[***show app-hosting resource***]を使用して、UTDサービスに割り

当てられたリソースを検証します

```
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. Snortのアクティベーション後、ISRのCPUおよびメモリ使用量を確認します。コマンド「*show app-hosting utilization appid utd*」を使用して、UTDのCPU、メモリ、およびディスク使用率を監視できます

```
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
```

メモリ、CPU、またはディスクの使用率が高い場合は、Cisco TACにお問い合わせください。

8.障害が発生した場合にSnort IPSの展開情報を収集するには、次のコマンドを使用します。

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

関連情報

Snort IPSの導入に関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

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

ISR、ISRv、およびCSR上のSnort IPS：段階的な設定

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

Snort IPS導入ガイド

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