Implante o Snort IPS nos Integrated Services Routers série 1000

Contents

Introduction

Este documento descreve como implantar o recurso Snort IPS no Cisco Integrated Services Router (ISR) série 1000.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco Integrated Services Routers série 1k
- Comandos XE-IOS básicos
- Conhecimento básico do Snort

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- C1111X-8P executando a versão 17.03.03
- UTD Engine TAR para versão 17.3.3
- A licença de segurança K9 é necessária no ISR1k
- Énecessária uma assinatura de 1 ou 3 anos
- XE 17.2.1r e superior
- Modelos de hardware ISR que suportam somente DRAM de 8 GB

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

O recurso Snort IPS permite o Sistema de Prevenção de Intrusão (IPS - Intrusion Prevention System) ou o Sistema de Detecção de Intrusão (IDS - Intrusion Detection System) para filiais nos Cisco 4000 Series Integrated Services Routers (ISR - Integrated Services Routers), Cisco 1000 Series (X PIDs, como 1111X, 121X, 111, 1111111111111X, 111111111111X, 111116X, 168X, etc. GB DRAM apenas) e Cisco Cloud Services Router 1000v Series. Esse recurso usa o mecanismo Snort para fornecer funcionalidades de IPS e IDS.

O Snort é um IPS de rede de código aberto que executa análise de tráfego em tempo real e gera alertas quando ameaças são detectadas em redes IP. Ele também pode executar análise de protocolo, pesquisa ou correspondência de conteúdo e detectar uma variedade de ataques e testes, como estouros de buffer, verificações de porta ocultas e assim por diante. O recurso Snort IPS funciona no modelo de prevenção e detecção de intrusão na rede que fornece funcionalidades de IPS ou IDS. No modo de detecção e prevenção de intrusão na rede, o Snort executa as seguintes ações

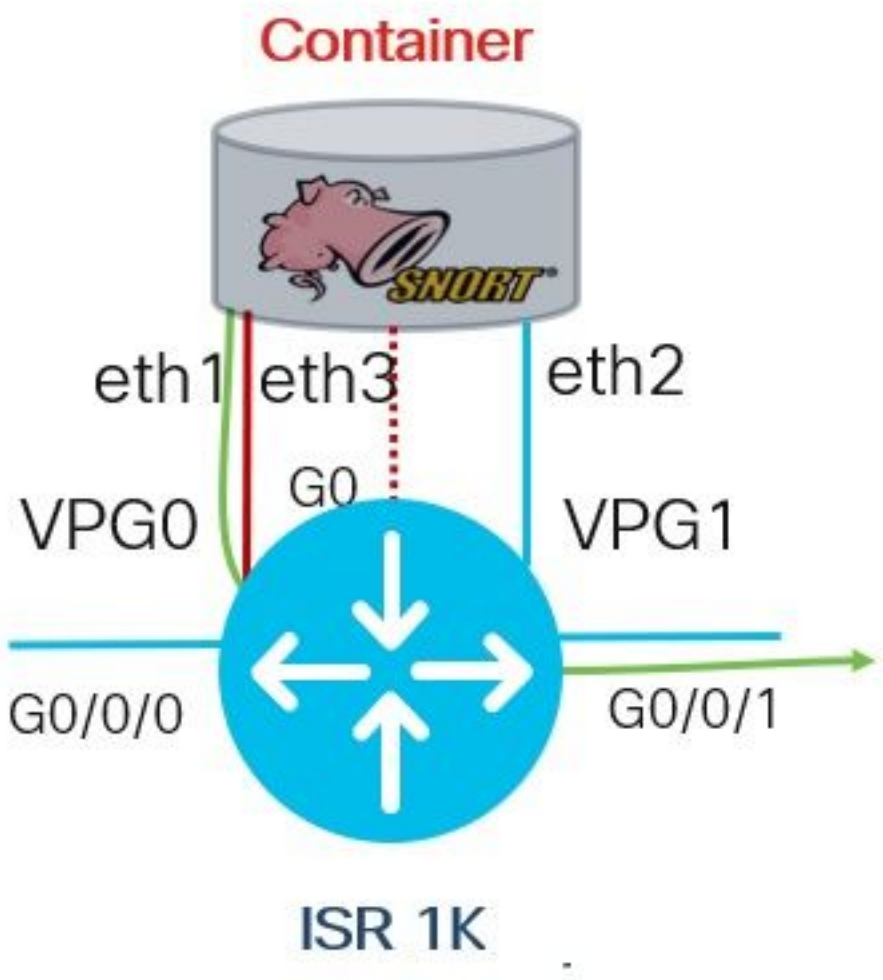
- Monitorar o tráfego de rede e analisar em relação a um conjunto de regras definido
- Classificação de ataques executados
- Invoca ações contra regras correspondentes

Com base nos requisitos, o Snort pode ser ativado no modo IPS ou IDS. No modo IDS, o Snort inspeciona o tráfego e relata alertas, mas não toma nenhuma ação para impedir ataques. No modo IPS, além da detecção de intrusão, são tomadas ações para evitar ataques. O Snort IPS monitora o tráfego e relata eventos a um servidor de log externo ou ao Syslog do IOS. A habilitação do registro no Syslog do IOS pode afetar o desempenho devido ao volume potencial de mensagens de log. Ferramentas externas de monitoramento de terceiros, que suportam logs Snort, podem ser usadas para coleta e análise de logs.

Há duas maneiras principais de configurar o Snort IPS em Cisco Integrated Services Routers (ISR), o método VMAN e o método IOx. O método VMAN usa um arquivo utd.ova e IOx usa um arquivo utd.tar. O IOx é o método correto e apropriado para a implantação do Snort IPS no Cisco Integrated Services Router (ISR) série 1k.

O Snort IPS pode ser implantado em Cisco Integrated Services Routers (ISR) série 1k com XE 17.2.1r e superior.

Diagrama de Rede



Configurar

Etapa 1. Configurar grupos de portas

```
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
```

Etapa 2. Ativar serviço virtual, configurar e confirmar alterações

```
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
```

Etapa 3. Configurar serviço virtual

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

Etapa 4. Configurando o UTD (plano de serviço)

```
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: *a proteção contra ameaças* permite o Snort como IPS, a *detecção de ameaças* permite o Snort como IDS.

Etapa 5. Configurando o UTD (plano de dados)

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

> **Observação:** Observação: *fail open* é a configuração padrão.

Verificar

Verificar o endereço IP e o estado da interface dos grupos de portas

```
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
```

Verificar a configuração dos grupos de portas

```
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
!
```

Verificar a configuração do serviço virtual

```
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**: Verifique se o comando ***start*** está presente, caso contrário a ativação não será iniciada.

Verifique a ativação do serviço virtual.

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

> **Note**: ***o iox*** ativará o Virtual Service.

Verificar a configuração do UTD (plano de serviço e plano de dados)

```
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
```

Verificar o estado de hospedagem do aplicativo

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

Verificar o estado de hospedagem do aplicativo com detalhes

```
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
```

Troubleshooting

1. Garantir que o Cisco Integrated Services Router (ISR) execute o XE 17.2.1r ou superior

2. Garanta que o Cisco Integrated Services Router (ISR) seja licenciado com Security K9

3. Verifique se o modelo de hardware do ISR suporta somente DRAM de 8 GB

4. Confirme a compatibilidade entre o software IOS XE e o arquivo UTD Snort IPS Engine (arquivo .tar) para corresponder ao software IOS XE; a instalação pode falhar por incompatibilidade

> **Note**: O software pode ser baixado usando o link: https://software.cisco.com/download/home/286315006/type

5. Confirme para ativar e iniciar serviços UTD usando os comandos **iox** e **start** mostrados na etapa 2 na ***seção*** Configurar

6. Validar os recursos atribuídos ao serviço UTD usando '***show app-host resource***' após a

ativação do 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. Após a ativação do Snort, confirme o uso da CPU ISR e da memória. Você pode usar o comando '***show app-host usage appid utd***' para monitorar a utilização de CPU UTD, memória e disco

```
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
```

Se você puder ver uma alta utilização de memória, CPU ou disco, entre em contato com o Cisco TAC.

8. Use os comandos listados abaixo para coletar informações de implantação do Snort IPS em caso de falha:

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

Informações Relacionadas

Documentos adicionais relacionados à implantação do Snort IPS podem ser encontrados aqui:

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

Snort IPS em ISR, ISRv e CSR - configuração passo a passo

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

Guia de implantação do Snort IPS

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