Implante o Snort IPS nos Cisco Integrated Services Routers 4000 Series

Contents

Introdução

Este documento descreve como implantar o recurso Snort IPS e Snort IDS nos Cisco Integrated Services Routers (ISR) 4000 Series usando o método IOx.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco Integrated Services Routers série 4000 com pelo menos 8 GB de DRAM.
- Experiência básica de comando do IOS-XE.
- Conhecimento básico do Snort.
- É necessária uma assinatura de assinatura de 1 ou 3 anos
- IOS-XE 16.10.1a e superior.

Componentes Utilizados

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

- ISR4331/K9 executando a versão 17.9.3a.
- UTD Engine TAR para a versão 17.9.3a.
- Licença do SecurityK9 para ISR4331/K9.

O método VMAN foi preterido agora.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer

comando.

Informações de Apoio

O recurso Snort IPS habilita o Sistema de Prevenção de Intrusão (IPS - Intrusion Prevention System) ou o Sistema de Detecção de Intrusão (IDS - Intrusion Detection System) para filiais em Cisco 4000 Series Integrated Services Routers e Cisco Cloud Services Router 1000v Series. Este recurso usa o Snort de código aberto para ativar os recursos de IPS e IDS.

O Snort é um IPS de código aberto que executa análise de tráfego em tempo real e gera alertas quando são detectadas ameaças em redes IP. Ele também pode executar análise de protocolo, pesquisa de conteúdo ou marcação e detectar uma variedade de ataques e testes, como estouros de buffer, varreduras de porta furtiva e assim por diante. O mecanismo Snort é executado como um serviço de contêiner virtual nos Cisco Integrated Services Routers série 4000 e Cloud Services Router série 1000v.

O recurso Snort IPS funciona como um modo de detecção ou prevenção de intrusão na rede e fornece recursos de IPS ou IDS nos Cisco Integrated Services Routers série 4000 e Cloud Services Router série 1000v.

- Monitora o tráfego de rede e o analisa em relação a um conjunto de regras definido.
- Executa a classificação de anexo.
- Invoca ações contra regras correspondentes.

Com base nos requisitos de rede. O Snort IPS pode ser ativado como IPS ou IDS. No modo IDS, o Snort inspeciona o tráfego e relata alertas, mas não toma nenhuma ação para evitar ataques. No modo IPS inspeciona o tráfego e relata alertas como faz o IDS, mas são tomadas ações para evitar ataques.

O Snort IPS é executado como um serviço em roteadores ISR. Os contêineres de serviço usam a tecnologia de virtualização para fornecer um ambiente de hospedagem em dispositivos Cisco para aplicativos. A inspeção de tráfego Snort é habilitada por interface ou globalmente em todas as interfaces suportadas. O sensor Snort requer duas interfaces VirtualPortGroup. O primeiro VirtualPortGroup é usado para tráfego de gerenciamento e o segundo para tráfego de dados entre o plano de encaminhamento e o serviço de contêiner virtual Snort. Adivinhe que os endereços IP devem ser configurados para essas interfaces VirtualPortGroup. A sub-rede IP atribuída à interface VirtualPortGroup de gerenciamento deve ser capaz de se comunicar com o servidor de assinatura e o servidor de alerta/relatório.

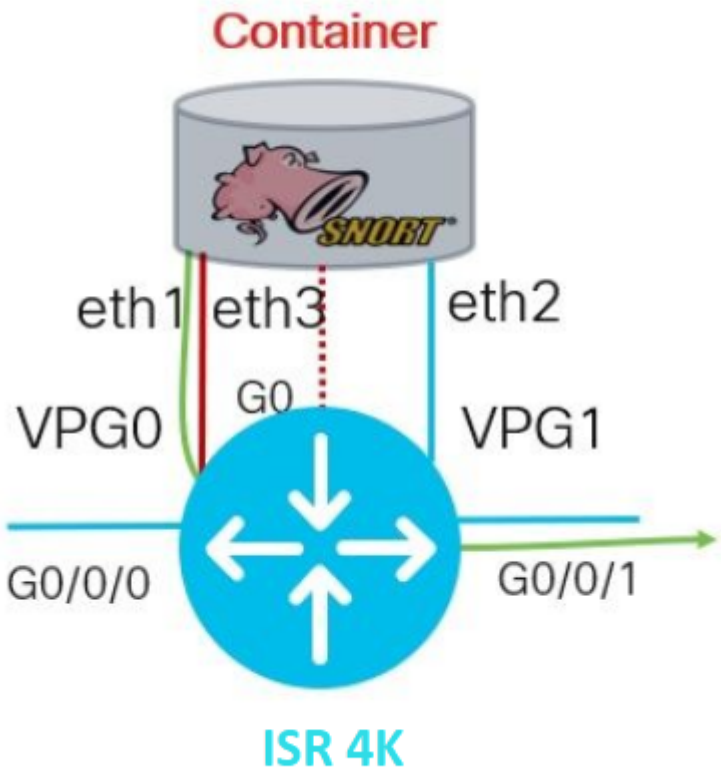
O Snort IPS monitora o tráfego e relata eventos para um servidor de registro externo ou para o syslog do IOS. Ativar o registro no registro de eventos do sistema IOS pode afetar o desempenho devido ao volume potencial de mensagens de registro. Ferramentas externas de monitoramento de terceiros, que oferecem suporte a logs do Snort, podem ser usadas para coleta e análise de logs.

O Snort IPS nos Cisco 4000 Series Integrated Services Routers e Cisco Cloud Services Router 1000v Series é baseado no download do pacote de assinatura. Há dois tipos de assinaturas:

- Pacote de Assinatura da Comunidade.
- Pacote de assinatura baseado em assinante.

O conjunto de regras do pacote de assinaturas da comunidade oferece cobertura limitada contra ameaças. O conjunto de regras do pacote de assinatura baseado em assinante oferece a melhor proteção contra ameaças. Ele inclui a cobertura antes das explorações e também oferece o acesso mais rápido a assinaturas atualizadas em resposta a um incidente de segurança ou à descoberta proativa de uma nova ameaça. Esta assinatura é totalmente suportada pela Cisco e o pacote será atualizado em Cisco.com. O pacote de assinatura pode ser baixado em software.cisco.com. As informações de assinatura do Snort podem ser encontradas em snort.org.

Diagrama de Rede



Configurar

Configuração UTD da plataforma

Etapa 1. Configure 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
```

Etapa 2. Ative o ambiente IOx no modo de configuração global.

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

Etapa 3. Configure a hospedagem de aplicativos com a configuração da 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
```

Etapa 4 (opcional). Configure o Perfil de Recurso.

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

> **Note**: *Se isso não for definido, o sistema usará a configuração de recurso de aplicativo padrão (Baixa). Certifique-se de ter recursos disponíveis suficientes no ISR se a configuração de perfil padrão for alterada.*

Etapa 5. Instale a hospedagem de aplicativos usando o arquivo 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.
```

> **Observação**: mantenha o arquivo UTD.tar correto no bootflash: para continuar a instalá-lo. A versão do Snort está especificada no nome do arquivo UTD.

Os próximos syslogs devem ser vistos indicando que o serviço UTD foi instalado corretamente.

```
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
```

> **Observação**: usando *'show app-hosting list'* o status deve ser *'Deployed'*

Etapa 6. Inicie o serviço de hospedagem de aplicativos.

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

> **Observação**: depois de iniciar o serviço de hospedagem de aplicativos, o status da hospedagem de aplicativos deve ser *'Em Execução'*. Use *'show app-hosting list' ou 'show app-hosting detail'* para ver mais detalhes.

As próximas mensagens de syslog devem ser vistas indicando que o serviço UTD foi instalado corretamente.

```
*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
```

Configuração do plano de serviço e do plano de dados.

Após a instalação bem-sucedida, o plano de serviço deve ser configurado. O Snort IPS pode ser configurado como IPS (Sistema de prevenção de intrusão) ou IDS (Sistema de detecção de intrusão) para inspeção.

> **Aviso**: confirme se o recurso de licença *'securityk9'* está habilitado para continuar com a configuração do plano de serviço UTD.

Etapa 1. Configurar o mecanismo padrão (plano de serviço) do Unified Threat Defense (UTD)

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

Etapa 2. Ative o registro de mensagens de emergência em um servidor remoto.

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

Etapa 3. Ative a Inspeção de ameaças para o Snort Engine.

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

Etapa 4. Configurar a detecção de ameaças como sistema de prevenção de intrusão (IPS) ou sistema de detecção de intrusão (IDS)

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

Observação: *'Proteção'* é usada para IPS e *'Detecção'* para IDS. *'Detecção'* é o padrão.

Etapa 5. Configure a Política de Segurança.

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

Observação: a política padrão é *'equilibrada'*

Etapa 6 (opcional). Criar a lista permitida por UTD (Whitelist)

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

Etapa 7 (opcional). Configure IDs de assinaturas do Snort para que apareçam na lista branca.

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

Observação: a ID *'40'* é usada como exemplo. Para verificar as informações de assinatura do Snort, consulte a documentação oficial do Snort.

Etapa 8 (opcional). Habilitar lista de permitidos na configuração de Inspeção de ameaças.

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

Etapa 9. Configure o intervalo de atualização de Assinatura para fazer o download automático de Assinaturas Snort.

```
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
```

Observação: o primeiro número define a hora no formato de 24 horas e o segundo número indica minutos.

Aviso: as atualizações de Assinatura UTD geram uma breve interrupção de serviço no momento da atualização.

Etapa 10. Configure os parâmetros do servidor de atualização de assinatura.

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

Observação: use *'cisco'* para usar o servidor Cisco ou *'url'* para definir um caminho personalizado para o servidor de atualização. Para o servidor Cisco, você deve fornecer seu próprio nome de usuário e senha.

Etapa 11. Habilite o nível de log.

```
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
```

Etapa 12. Habilite o serviço utd.

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

Etapa 13 (opcional). Redirecione o tráfego de dados da interface VirtualPortGroup para o serviço UTD.

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

Observação: se o redirecionamento não estiver configurado, ele será detectado automaticamente.

Etapa 14. Ative o UTD para todas as interfaces de Camada 3 no ISR.

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

Etapa 15. Ative o padrão do mecanismo.

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

As próximas mensagens de syslog devem ser vistas indicando que o UTD foi habilitado corretamente.

```
*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
```

Etapa 16 (opcional). Definir a ação para falha de mecanismo UTD (Plano de Dados UTD)

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

> **Observação**: a opção *'Fail close'* descarta todo o tráfego de IPS/IDS quando o mecanismo UTD falha. A opção *'Fail open'* permite todo o tráfego IPS/IDS em falhas UTD. A opção padrão é *'fail open'*.

Verificar

Verifique o endereço IP e o status da interface do 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
```

Verifique a configuração do 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
!
```

Verifique a configuração de hospedagem de aplicativos.

```
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
```

Verifique a ativação do iox.

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

Verifique a configuração do plano de serviço 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
```

Verifique o estado de hospedagem do aplicativo.

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

Verifique os detalhes de hospedagem do aplicativo.

```
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
```

Troubleshooting

1. Verifique se o Cisco Integrated Services Router (ISR) executa o XE 16.10.1a e superior (para o método IOx)

2. Verifique se o Cisco Integrated Services Router (ISR) está licenciado com o recurso Securityk9 habilitado.

3. Verifique se o modelo de hardware do ISR está em conformidade com o perfil de recursos mínimos.

4. Recurso não compatível com o cookie SYN do firewall baseado em zona e o NAT64 (Network Address Translation 64)

5. Confirme se o serviço UTD foi iniciado após a instalação.

6. Durante o download manual do pacote Signature, certifique-se de que o pacote tenha a mesma versão que a versão do mecanismo Snort. A atualização do pacote de assinatura pode falhar se houver uma incompatibilidade de versão.

7. Em caso de problemas de desempenho, use ***'show app-hosting resource'*** e ***'show app-hosting usage appid''UTD-NAME'*** para aprender sobre o consumo de CPU/Memória/Armazenamento.

```
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
```

Aviso: se você puder ver alto uso de CPU, memória ou disco, entre em contato com o TAC da Cisco.

Depuração

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

<#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
```

Informações Relacionadas

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

Guia de configuração de segurança do 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

Perfil de Recurso de Serviço Virtual

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 on Routers - Configuração passo a passo.

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

Troubleshooting 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

O ISR4K Snort IPS não está implantado, pois o HW não tem recursos de plataforma suficientes

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

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.