Impacto da inspeção da Camada 7 no tráfego multicamada: Revisão da implementação do Snort3

Contents

Problema

Depois de habilitar as regras DNS Sinkhole em uma Política de Controle de Acesso (ACP), o tráfego VXLAN encapsulado começou a ser descartado inesperadamente em dispositivos Firepower Threat Defense (FTD) executando versões do mecanismo Snort 3.

· O tráfego encapsulado de VXLAN cai após a habilitação da política DNS Sinkhole.

· Eventos de conexão mostrando endereços IP internos (por exemplo, 100.70.x.x) em vez de cabeçalhos VXLAN externos.

· Comportamento inesperado encontrado com a implementação do Snort 3 durante o teste de laboratório.

Ambiente

•Plataforma: Par de alta disponibilidade (HA) do FTD

•Versão afetada: 7.6.2.1 (Snort 3)

•Versão Fixa: 7.6.4+ (Snort 3)

Resolução

Solução no 7.6.2.1:

##########

Passo 1:

Política de pré-filtro (recomendada)

Crie uma regra Prefilter para ignorar inspeção Snort para tráfego VXLAN:

· Política de pré-filtragem

•Ação: Fastpath (regra de túnel)

•Fonte: <Outer_VXLAN_Source_IPs>

•Destino: <IPs_Destino_VXLAN_Externo>

•Protocolo: UDP

•Porta: 4789

Passo 2:

Limpar Conexões Existentes

· clear conn address <outer_ip_1> address <outer_ip_2>

Ajustar a Ordenação de Regras se não estiver usando a Política de pré-filtro

Coloque as regras L7 (DNS Sinkhole, App-ID) à frente das regras de permissão IP internas no ACP.

Solução de longo prazo:

##########

1. Atualizar para FTD 7.6.4 ou posterior

· Resolve CSCwo54753 (PSIRT DEFECT)

· Proporciona um comportamento consistente de inspeção multicamada.

2. Configure as Regras Internas e Externas para o Sinkhole DNS:

· Ao usar o DNS Sinkhole ou outros recursos de Inteligência de Segurança com tráfego encapsulado.

3. Para recursos da camada 7 não SI (filtragem de URL, controle de aplicativo):

· Somente as regras de cabeçalho interno são necessárias no ACP.

· As regras de cabeçalho externo não são necessárias.

Mais Detalhes sobre o Recurso de Inspeção de VXLAN Multicamada

##################################

O FTD inclui um recurso de inspeção multicamada para recursos de Inteligência de Segurança (SI) e Camada 7. Esse recurso determina se o Snort inspeciona os cabeçalhos de encapsulamento externo ou os cabeçalhos de payload interno com base nas políticas configuradas da camada 7.

Os Recursos Da Camada 7 Incluem:

· Sinkhole DNS

· Controle de aplicativos (App-ID)

•Filtragem de URL

· Localização geográfica

· Prevenção contra invasões

Comportamento-chave:

#########

Quando qualquer recurso da Camada 7 é habilitado no ACP, o Snort passa a inspecionar os cabeçalhos mais internos dos pacotes encapsulados (por exemplo, VXLAN, GRE, IP-em-IP).

Análise técnica:
##############
Snort 3 (7.6.2.1) - Comportamento com defeito

Sem regras da camada 7:

· O Snort depende dos metadados de conexão de Lina (mecanismo de caminho de dados ASA).

· O tráfego é permitido/negado apenas com base nas regras do cabeçalho externo.

· A inspeção do cabeçalho interno não é executada.

Com regras da camada 7:

· O Snort realiza verificações ACP e aplica a inspeção multicamada.

· Questões de ordem de regras (defeito no Snort 3).

· Se a regra de IP interno aparecer à frente da regra L7 → queda de tráfego Vxlan —> Comportamento com defeito

Resultado do LAB:
LABORATÓRIO FTD — 7.6.2.1 — snort3 — Regra do ACP do IP Interno seguida pela regra L7 — Descartar

Detalhes do Lab Packet Tracer:

17:46:48.773778 10.142.133.15:36066 > 10.126.133.15:4789 udp 80

Interno(vrfid:0)

OBJECT_GROUP_SEARCH

MODO NGIPS

| modo ngips

ACCESS-LIST

NGIPS-EGRESS-INTERFACE-LOOKUP

| Resolver interface de saída

CRIAÇÃO DE FLUXO

INSPEÇÃO EXTERNA

SNORT

Digite:

SNORT

Resultado:

SOLTAR

Config:

Tempo decorrido:

814472 ns

Informações adicionais

Resultado: queda

Interface de entrada:

Interno(vrfid:0)

Status de entrada:

up

Status da linha de entrada:

up

Interface de saída:

Externo(vrfid:0)

Status de saída:

up

Status da linha de saída:

up

Ação:

queda

Tempo Decorrido:

928908 ns

Motivo da queda:

(firewall) Bloqueado pelo pré-processador do firewall <— MOTIVO DA QUEDA

Detalhe da queda:

Local de destino: frame inspect_dp_snort_snp_drop_frame_wcaller:fluxo 58 (NA)/NA

Externo(vrfid:0)

· Se a regra L7 aparecer à frente da regra de IP interno → tráfego Vxlan permitido

Comportamento Específico do Sinkhole DNS (Snort 3):

· O DNS Sinkhole aciona a inspeção multicamada mesmo quando o ordenamento de regras permitiria tráfego.

Snort 3 (7.6.4+) - Comportamento fixo

Pós-correção (CSCwo54753):

· A inspeção multicamada é habilitada consistentemente quando recursos L7 estão presentes.

· A ordem das regras não afeta o comportamento.

· A inspeção de tráfego é baseada nos cabeçalhos mais internos, independentemente da posição da regra.

· Os cabeçalhos internos e externos devem ser permitidos no ACP para cenários de DNS Sinkhole.

Matriz de comparação de casos de teste

Cenário de teste	FTD 7.6.2.1 (Snort 3)	FTD 7.6.4+ (Snort 3)	Comportamento esperado
Regra L7 seguida pela Regra de IP Interno	Permitido	Permitido	Tráfego permitido
Regra de IP interno seguida da Regra L7	Ignorado (Defeito)	Permitido	Tráfego permitido
Somente Regra de IP Interno (Sem L7)	Bloqueado	Bloqueado	Bloqueado (Sem permissão interna)

Somente Regra de IP Externo (Sem L7)	Permitido	Bloqueado	O Snort 3 inspeciona o cabeçalho mais interno
Somente IP externo + DNS Sinkhole	Bloqueado	Bloqueado	Regra L7 reforça inspeção interna
Somente IP interno + Sinkhole DNS	Bloqueado	Bloqueado	Regra L7 reforça inspeção interna

Causa

Esse comportamento é causado pelo recurso de inspeção multicamada do Snort 3 para recursos de inteligência de segurança. Quando o DNS Sinkhole (parte da Inteligência de Segurança) está habilitado, o Snort 3 executa uma inspeção profunda de pacotes que detecta e avalia os endereços IP mais internos dentro de pacotes encapsulados, independentemente da camada de transporte.

O problema está documentado no bug da Cisco ID CSCwt12564, que afirma: "Se estiver usando a condição L7 (filtragem de url, id de aplicativo, geolocalização etc.) na regra ou em um recurso de inteligência de segurança no ACP, você precisará de uma regra ACP com cabeçalho interno para que as regras sejam correspondentes. Com o dns sinkhole, que faz parte da política de DNS no SI, os cabeçalhos interno e externo são necessários em um ACP para que as regras sejam correspondentes."

Esse comportamento difere da operação normal onde somente cabeçalhos externos são avaliados para tráfego VXLAN de trânsito quando nenhum recurso de Camada 7 ou Inteligência de segurança é configurado.

Conteúdo relacionado

- Guia de configuração do Snort 3
- Suporte técnico e downloads da Cisco
- ID de bug da Cisco CSCwt12564
- ID de bug da Cisco CSCwt07320

- ID de bug da Cisco CSCwu75396
- ID de bug da Cisco CSCwt58320

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.