Entender o DNS Guard no Secure Firewall 7.7.0

Contents

Introdução

Este documento descreve o recurso DNS Guard no Secure Firewall 7.7.0, concentrando-se em sua funcionalidade e solução de problemas.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Entendendo o protocolo DNS e as sessões UDP
- Familiaridade com o Snort 3 e seu gerenciamento de sessão

Componentes Utilizados

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

- Secure Firewall Threat Defense (FTD) versão 7.7.0
- Firepower Management Center (FMC) versão 7.7.0
- Snort versão 3

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 DNS é um protocolo baseado em solicitação-resposta UDP com sessões de curta duração. Ao contrário de Lina, as sessões DNS no Snort 3 não são limpas imediatamente após a resposta DNS. Em vez disso, as sessões DNS são removidas com base em um tempo limite de fluxo de 120 segundos ou mais. Isso leva a um acúmulo desnecessário de sessões, que poderia ser usado para outras conexões TCP ou UDP.

Comparação com a versão anterior

In Secure Firewall 7.6 and Below		New to Secure Firewall 7.7
• The DNS session remains as a stale Snort 3 flow until it is pruned by the UDP timeout.		• DNS sessions in Snort 3 are released immediately after the DNS Response is inspected and handled.

Novo recurso no 7.7

Novos recursos

- Esse recurso "DNS Guard" limpa o fluxo de UDP imediatamente após o recebimento e a inspeção do pacote de resposta DNS.
- Este é um aprimoramento específico de protocolo sobre o projeto e a arquitetura atuais do Snort 3.

Conceitos básicos: Plataformas suportadas, licenciamento

Plataformas e gerentes de FTD

FTD Platforms	All
FMC on 7.7.0 FMC Rest API	Yes No
FTD Supported Versions *(lowest version FMC on 7.7.0 can manage is 7.2)*	7.7.0 only
Snort Support (Snort 3 is the only Snort version supported in 7.7)	Snort 3

Plataformas suportadas

Outros aspectos de suporte

FTD	
Licenses Required	Essentials, URL, Threat, Malware
Works in Evaluation Mode	Yes
IP Addressing	IPv4 IPv6
Multi-instances supported?	Yes
Supported with HA'd devices	Yes
Supported with clustered devices?	Yes
Other (only routed mode | transparent mode), etc.	No Special Notes

Licenciamento e compatibilidade

Problema

Em versões anteriores, especificamente o Secure Firewall 7.6 e anterior, a sessão DNS permanece como um fluxo antigo do Snort 3 até que seja cortada pelo tempo limite de UDP. Isso causa problemas com o gerenciamento de sessão e pode levar ao uso ineficiente de recursos à medida que as sessões de DNS se acumulam desnecessariamente.

Etapas para recriar o problema

Para observar o problema, execute o comando Lina para verificar as conexões DNS ativas do lado Lina:

```
show conn detail
```

No Secure Firewall 7.6 e abaixo, as sessões de DNS permanecem ativas até o tempo limite de UDP, levando à ineficiência de recursos.

Solução

O recurso DNS Guard no Secure Firewall 7.7.0 resolve esse problema limpando imediatamente o fluxo de UDP após receber e inspecionar o pacote de resposta DNS. Esse aprimoramento específico de protocolo garante que as sessões de DNS no Snort 3 sejam liberadas

imediatamente, evitando o acúmulo desnecessário de sessões e melhorando a eficiência de recursos.

Visão geral do recurso

O recurso DNS Guard limpa o fluxo de UDP imediatamente após o recebimento e a inspeção do pacote de resposta DNS. O fluxo Snort não precisa esperar até que o tempo limite de UDP ocorra.

- Quando há tráfego de DNS suficiente na caixa, esse recurso leva a menos fluxos ativos devido à limpeza oportuna dos fluxos Snort correspondentes.
- Mais conexões TCP/UDP podem ser manipuladas pela caixa sem remover as conexões ativas, o que melhora a eficácia geral da caixa.

Troubleshooting

Para verificar a funcionalidade do recurso DNS Guard, use o comando Lina para garantir que as sessões UDP sejam liberadas após o recebimento de uma resposta DNS:

<#root>

>

show snort counters | begin stream_udp

Exemplo de saída sem o recurso de proteção de DNS:

```
stream_udp sessions: 755
 max: 12
created: 755
released: 0
total_bytes: 124821
```

<#root>

>

show snort counters | begin stream_udp

Exemplo de saída com recurso de protetor de DNS:

```
stream_udp sessions: 899
max: 14
```

```
created: 899
released: 899
total_bytes: 135671
```

As saídas indicam que todas as sessões criadas são liberadas em tempo hábil, confirmando a operação correta do recurso DNS Guard.

Informações Relacionadas

- Suporte técnico e downloads da Cisco

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.