Solucionar problemas de tráfego no CSF CLI

Contents

[Introdução](#)

[Pré-requisitos](#)

- [Requisitos](#)
- [Componentes Utilizados](#)
- [Produtos Relacionados](#)
- [Informações importantes](#)

[Informações de Apoio](#)

[Problema](#)

[Passo 1: Localizar a rota](#)

[Passo 2: Executar o Packet Tracer](#)

[Passo 3: Executar Capturas](#)

[Passo 4: Executar Rastreamento de Suporte do Sistema](#)

[Verificar](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve como usar a CLI do Cisco Secure Firewall para solucionar problemas de tráfego, validando o roteamento, o fluxo de pacotes e o comportamento Snort.

Pré-requisitos

Não existem requisitos específicos para este documento.

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Políticas e configuração de objetos do Firepower Management Center (FMC)
- Roteamento e lógica de interface do Cisco Secure Firewall (CSF)
- Conceitos de inspeção de pacotes e solução de problemas de firewall

Componentes Utilizados

Este documento não está restrito a versões específicas de software e hardware para CSF. O dispositivo usado no documento está executando o código 7.6.5.

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.

Produtos Relacionados

Este documento também pode ser usado com as seguintes versões de hardware e software:

- Centro de gerenciamento seguro de firewall (FMC)
- Cisco Secure Firewall (CSF)
- Ferramentas de CLI do Firepower Threat Defense

Informações importantes

Quando um dispositivo apresenta utilização elevada de CPU, memória ou E/S, a execução de comandos de solução de problemas pode exacerbar a degradação do desempenho. Recomenda-se investigar e resolver a condição de esgotamento de recursos primeiro e, em seguida, prosseguir com o diagnóstico de problema de tráfego. Os comandos de diagnóstico consomem recursos adicionais do sistema, o que pode degradar ainda mais a disponibilidade e prolongar o tempo de recuperação.

Informações de Apoio

A solução de problemas de tráfego no CSF geralmente começa confirmando o caminho lógico que um pacote deve seguir pelo firewall. Uma vez que a rota e o mapeamento de interface sejam entendidos, a próxima etapa é comparar o caminho esperado com o fluxo de pacote real. Isso pode ser realizado usando pesquisas de rota, simulação de rastreador de pacotes, capturas de pacotes e rastreamento de mecanismo Snort.

Cada ferramenta fornece uma camada diferente de visibilidade:

- show route confirma o caminho de roteamento do pacote e a identidade da interface.

- o packet-tracer simula o fluxo de tráfego e identifica as decisões de ACL, NAT e interface.
- as capturas de pacote inspecionam o tráfego em tempo real que atravessa o firewall.
- o rastreamento de suporte do sistema expõe a tomada de decisão do Snort para blocos ou eventos de inspeção relacionados à política.

Tip: Comece com a validação do roteamento e do packet-tracer antes de capturar o tráfego, para que você possa confirmar se as decisões esperadas de caminho e controle de acesso estão corretas antes de analisar o tráfego em tempo real.

Problema

Um fluxo de tráfego não está funcionando conforme esperado, e o administrador precisa determinar se o pacote está tomando o caminho correto, se o firewall está permitindo ou negando a conexão e se o Snort ou a inspeção de política está bloqueando o tráfego.

Passo 1: Localizar a rota

Identifique o caminho de roteamento e determine os nomes de interface lógica associados aos endereços IP origem e destino. Os nomes das interfaces lógicas são exigidos pela maioria dos comandos de identificação e solução de problemas, portanto, essa deve ser a primeira etapa no fluxo de trabalho de identificação e solução de problemas.

Execute o comando para o endereço IP origem e destino:

```
show route <IP>
```

O tráfego destinado à Internet que depende da rota padrão requer a identificação da interface de saída lógica. O nome da interface lógica pode ser determinado executando esta etapa:

```
show route 0.0.0.0
```

Saída de exemplo:

```
FTD1# show route 192.168.0.11
```

```
Routing entry for 192.168.0.0 255.255.255.0
Known via "connected", distance 0, metric 0 (connected, via interface)
Routing Descriptor Blocks:

    directly connected, via Inside
    Route metric is 0, traffic share count is 1
```

```
FTD1# show route 0.0.0.0

Routing entry for 0.0.0.0 0.0.0.0, supernet
Known via "static", distance 1, metric 0, candidate default path
Routing Descriptor Blocks:

    128.107.0.1, via Outside
    Route metric is 0, traffic share count is 1
```

Neste exemplo, a interface de entrada lógica é Inside e a interface de saída é Outside.

Caution: A conversão de endereço de rede (NAT) pode redirecionar o tráfego através de interfaces diferentes das que a tabela de roteamento indica quando as políticas de NAT correspondem ao fluxo de tráfego. Ao solucionar problemas de conectividade, verifique se a configuração de NAT está alinhada com o caminho de tráfego esperado.

Tip: Os nomes de interface lógica são usados em comandos de solução de problemas da CLI. Anote o nome lógico para referência futura.

Passo 2: Executar o Packet Tracer

Use o packet-tracer para simular como o firewall avalia um fluxo de tráfego específico. Essa ferramenta ajuda a confirmar quais interfaces são usadas, se uma política de NAT é aplicada e se uma ACL permite ou nega o tráfego.

Use esta sintaxe de comando:

```
packet-tracer input <source interface> <protocol> <source IP> <source port> <destination IP> <destinati
```

Comando de exemplo:

```
FTD1# packet-tracer input Inside tcp 192.168.0.11 55555 72.163.4.161 443
```

Revise a saída para confirmar se o pacote segue o caminho esperado e se é permitido durante a simulação. Isso é útil quando você precisa determinar se o problema está relacionado ao roteamento, à NAT ou à correspondência de políticas antes de realizar a análise de pacotes ativos.

A palavra-chave transmit no packet-tracer faz com que o pacote simulado seja injetado na interface de entrada, permitindo que ele passe por todas as fases de processamento do firewall em vez de permanecer como simulação.

Comando de exemplo:

```
FTD1# packet-tracer input Inside tcp 192.168.0.11 55555 72.163.4.161 443 transmit
```

Passo 3: Executar Capturas

Use capturas de pacotes para inspecionar o tráfego ao vivo à medida que ele passa pelo firewall. As capturas de pacotes são diferentes do packet-tracer porque capturam o tráfego real e, portanto, devem corresponder ao fluxo real que atravessa o firewall no momento em que a captura está ativa. As capturas de pacotes são bidirecionais, documentando os dois lados da conexão.

Para a maioria dos cenários de solução de problemas de tráfego, configure estas capturas:

- Captura de entrada — captura o tráfego que chega à interface de origem
- Captura de saída — captura o tráfego que sai da interface no lado do destino
- Captura de queda do ASP — captura pacotes que são descartados pelo firewall e correspondem aos critérios configurados

Sintaxe geral de captura:

```
capture <name> interface <interface name> trace match ip host <source IP> host <destination IP>
```

Exemplo de captura de ingresso:

```
FTD1# capture in interface trace Inside match ip host 192.168.0.11 host 72.163.4.161
```

Exemplo de captura de saída:

```
FTD1# capture out interface trace Outside match ip host 128.107.0.22 host 72.163.4.161
```

Exemplo de captura de queda ASP:

```
FTD1# cap asp type asp-drop match ip host 192.168.0.11 host 72.163.4.161
```

As capturas de pacotes são bidirecionais, o que significa que o tráfego de encaminhamento e de retorno pode ser capturado com base nos critérios de correspondência definidos. O recurso de rastreamento permite visualizar as decisões que o Firewall toma sobre o tráfego real.

⚠ Caution: Se o NAT estiver sendo executado, a captura de saída deverá usar o IP de origem convertido, e não o IP de origem original, para capturar o tráfego pós-NAT corretamente.

Passo 4: Executar Rastreamento de Suporte do Sistema

Use o rastreamento de suporte do sistema para visualizar o processo de inspeção Snort em tempo real para um fluxo de tráfego específico. Isso é especialmente útil quando o tráfego corresponde a uma regra de permissão da ACL, mas ainda é bloqueado pela inspeção de política. As capturas de pacote padrão mostram que um pacote foi bloqueado, mas o rastreamento de suporte do sistema fornece visibilidade do motivo pelo qual o pacote foi tratado dessa maneira. O rastreamento de suporte do sistema é bidirecional, o que significa que recebe tráfego de ambos os lados. Isso significa que a ordem em que os IPs são adicionados à ferramenta não importa.

Execute este comando e responda aos prompts:

```
> system support trace

Enable firewall-engine-debug too? [n]: y
```

```
Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.0.11
Please specify a client port:
Please specify a server IP address: 72.163.4.161
Please specify a server port: 443
```

Essa ferramenta é particularmente útil quando o ambiente está usando regras de aplicativo ou URL, regras baseadas em identidade, políticas de arquivo ou políticas de intrusão. Esses recursos são avaliados após a correspondência da ACL, portanto um pacote pode ser permitido pela política de controle de acesso, mas ainda ser bloqueado pela inspeção Snort.

Note: A porta do cliente pode ser deixada em branco se a porta de origem exata for desconhecida.

Verificar

Use a saída da pesquisa de rota, simulação de rastreador de pacotes, capturas de pacotes e rastreamento de suporte do sistema juntos para confirmar o comportamento do fluxo de tráfego. O objetivo é determinar se o pacote está tomando o caminho correto, se o firewall está permitindo ou negando-o e se o Snort está bloqueando-o com base em uma inspeção mais profunda.

Um fluxo completo de solução de problemas normalmente confirma:

- A pesquisa de rota mostra as interfaces lógicas de entrada e saída.
- O Packet Tracer confirma o caminho de encaminhamento pretendido e a avaliação da política.
- As capturas de pacote confirmam se o tráfego está chegando e saindo conforme esperado.
- O rastreamento de suporte do sistema confirma se o Snort ou a inspeção de política está causando o bloqueio.

Troubleshooting

Quando um problema de tráfego persistir, revise estas áreas:

- Verifique se a pesquisa de rota corresponde às interfaces de origem e destino esperadas.
- Verifique se a saída do packet-tracer mostra o tráfego sendo negado no estágio ACL ou NAT.
- Revise as capturas de pacotes de entrada e saída para confirmar se o tráfego está

chegando ao firewall e saindo na interface correta.
- Use capturas de queda de ASP para confirmar se o firewall está descartando o tráfego internamente.
- Use o rastreamento de suporte do sistema para determinar se o Snort está bloqueando o tráfego após a decisão de permissão da ACL.

Informações Relacionadas

- Analise as capturas de firewall do Firepower para solucionar problemas de rede
- Use as capturas do Firepower Threat Defense e o Packet Tracer

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.