

Taxa de transferência do ASA e velocidade da conexão Solucionando problemas e analisando capturas de pacotes

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Metodologia de solução de problemas](#)

[Análise de dados](#)

[Problemas comuns](#)

[Valores de velocidade e duplex configurados incorretamente na interface que conecta o ASA ao dispositivo adjacente](#)

[Enviar tráfego para o módulo IPS](#)

[A modificação do ASA da opção TCP MSS causa uma ligeira redução no desempenho](#)

[Informações Relacionadas](#)

Introduction

Este documento descreve como resolver problemas de throughput do Cisco Adaptive Security Appliance (ASA) e problemas de velocidade de conexão.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas no Cisco Adaptive Security Appliance (ASA).

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. If your network is live, make sure that you understand the potential impact of any command.

Informações de Apoio

Alguns clientes podem ter um problema ao implantar um ASA pela primeira vez ou ao testar a nova conectividade. O problema é que o throughput do TCP para as conexões que fluem pelo ASA é muito menor do que quando o ASA não está no caminho da conexão (ou as conexões são

muito mais lentas do que antes do ASA ter sido implementado na rede).

Por exemplo, um cliente pode substituir um roteador D-Link low-end (ou outro dispositivo de roteamento) por um ASA 5505 ou um ASA 5510; no entanto, depois que o roteador é substituído, a velocidade da conexão é muito reduzida. O cliente pode levantar um caso no Cisco TAC porque acredita que o ASA causou a redução na velocidade da conexão.

Metodologia de solução de problemas

Os fluxos de TCP diminuem a velocidade quando há perda de pacotes ou atraso de pacotes na rede. Para entender a causa exata do problema, os dados devem mostrar os pacotes TCP reais no fio para essa conexão e como a rede pode afetá-los. Geralmente, um administrador de rede é alertado sobre o problema quando executa uma ação específica, como uma transferência de arquivo FTP ou um teste de velocidade on-line. Na maioria das vezes, o problema pode ser reproduzido. Portanto, o administrador pode coletar os dados necessários para encontrar a causa raiz.

Para coletar os dados necessários, o comando **show tech** deve ser executado do ASA antes e depois do teste. Esse comando mostra a configuração e as estatísticas de pacotes (principalmente do **show service-policy**) e também mostra se os erros de interface aumentam.

Capturas de pacotes simultâneas bidirecionais (retiradas das duas interfaces ASA afetadas pela conexão) são necessárias para diagnosticar totalmente a causa do problema.

Consulte estes documentos para obter exemplos de como aplicar capturas de pacotes ao ASA:

- [Troubleshooting de Conexões via PIX e ASA](#)
- [Episódio nº 1 do podcast de segurança do TAC - Uso do utilitário de captura de pacote ASA para solução de problemas](#)

Análise de dados

Depois de coletar os dados necessários, você pode usar as capturas de pacote para determinar qual desses problemas pode ter ocorrido:

- Os pacotes do host externo são descartados ou atrasados antes de chegarem à interface externa do ASA.
- Os pacotes são atrasados ou descartados pelo ASA.
- Os pacotes são atrasados ou descartados em algum lugar da rede interna.

Note: Essa análise pressupõe que os dados são enviados de um host na interface externa para um host na interface interna.

Este vídeo mostra um exemplo de como executar a análise em uma captura de pacote:

A *coalescência de fluxo TCP* é uma consideração técnica específica para esse problema porque, quando você envolve determinados recursos no ASA, o firewall coalesce totalmente o fluxo TCP que passa por ele.

Por exemplo, se o ASA descobrir um pacote ausente na rede (já que ele não é recebido no ASA),

ele envia um ACK em nome do outro endpoint TCP para os dados ausentes. Esse cenário é mais comum. Se o ASA descobrir pacotes que chegam fora de ordem, ele reordena os pacotes e os passa para o receptor na ordem correta. Se não houver descartes de rede ou reordenação de pacotes, não haverá efeitos colaterais ao ativar esse recurso. Se todos os pacotes enviados por qualquer um dos pontos de extremidade TCP passassem com êxito pela rede e pelo ASA, você não saberia que esse recurso está ativado, já que ele não age nos fluxos de pacote. Somente quando há problemas com a conexão TCP na rede habilitará esse recurso para retardar ainda mais o tráfego da rede. O ato de coalescência do fluxo TCP exige muito recursos para o ASA. Para cada pacote descartado na rede, o ASA não deve apenas enviar uma solicitação de pacote TCP para a retransmissão desse pacote, mas também deve armazenar em buffer os pacotes que o remetente continuou a enviar depois que o pacote desapareceu.

Problemas comuns

Valores de velocidade e duplex configurados incorretamente na interface que conecta o ASA ao dispositivo adjacente

Esse problema frequentemente ocorre quando um dispositivo é substituído por um ASA. Se os valores de velocidade e duplex na interface do ASA não forem os mesmos que os valores no dispositivo adjacente, as quedas de pacote ocorrem nessa interface. Verifique os valores de velocidade e duplex na interface do ASA e na interface adjacente.

Verifique a saída **show interface** do ASA para saber se há erros óbvios que são sintomas desse problema:

```
Interface Ethernet0/0 "Outside", is up, line protocol is up
Hardware is i82546GB rev03, BW 100 Mbps
Auto-Duplex(Half-duplex), Auto-Speed(100 Mbps)
MAC address 0019.2f58.c324, MTU 1500
IP address 192.168.222.122, subnet mask 255.255.255.252
124047996 packets input, 35340918453 bytes, 0 no buffer
Received 3 broadcasts, 0 runts, 0 giants
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 L2 decode drops
156918660 packets output, 40931551514 bytes, 0 underruns
1 output errors, 4286634 collisions, 0 interface resets
0 babbles, 123332 late collisions, 4752834 deferred
0 lost carrier, 0 no carrier
input queue (curr/max blocks): hardware (0/0) software (0/0)
output queue (curr/max blocks): hardware (0/245) software (0/0)
Traffic Statistics for "Outside":
124047995 packets input, 33107957301 bytes
157041993 packets output, 38195084709 bytes
103480 packets dropped
1 minute input rate 2140 pkts/sec, 477200 bytes/sec
1 minute output rate 2630 pkts/sec, 396763 bytes/sec
1 minute drop rate, 0 pkts/sec
5 minute input rate 2152 pkts/sec, 525496 bytes/sec
5 minute output rate 2701 pkts/sec, 421215 bytes/sec
5 minute drop rate, 0 pkts/sec
```

Enviar tráfego para o módulo IPS

Quando o ASA é configurado para enviar tráfego para o módulo IPS, o recurso de coalescência de fluxo TCP é ativado no ASA. Consulte a seção *Análise de Dados* deste documento para obter

mais informações sobre o recurso de coalescência de fluxo TCP.

A modificação do ASA da opção TCP MSS causa uma ligeira redução no desempenho

Por padrão, o ASA define a opção TCP MSS nos pacotes SYN como 1380. Portanto, os pontos de extremidade TCP não devem transmitir um segmento TCP maior que 1380 bytes. Esse valor é inferior ao valor padrão de 1460 bytes, que representa uma queda de desempenho do TCP de cerca de 6% (6%). O desempenho pode melhorar se você aumentar a configuração máxima do MSS no ASA ou desativar o ajuste do MSS. Antes de modificar o comando padrão no ASA, entenda os riscos envolvidos com relação à fragmentação potencial se o pacote for encapsulado no caminho em algum lugar.

Para obter mais informações, consulte a seção [sysopt connection tcpmss](#) da *Referência de Comandos do Cisco ASA 5500 Series*.

Informações Relacionadas

- [Referência de comando do Cisco ASA 5500 Series, 8.2](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)