Processamento da grande sessão do único córrego (fluxo do elefante) pelos serviços da potência de fogo

Índice

Introdução

O resultado de nenhum Web site dos testes de velocidade da largura de banda, ou a saída de nenhuma ferramenta da medida da largura de banda (por exemplo, *iperf*) não podem exibir a avaliação anunciada da taxa de transferência dos dispositivos da potência de fogo de Cisco. Similarmente, transferência de um arquivo muito grande sobre o FTP ou o protocolo HTTP não demonstram a avaliação anunciada da taxa de transferência de um dispositivo da potência de fogo. Ocorre porque o serviço da potência de fogo não usa um fluxo de rede única para determinar seu throughput máximo. Este documento descreve porque um fluxo único consome o throughput taxado inteiro de um dispositivo da potência de fogo de Cisco.

Contribuído por Nazmul Rajib, e por Lipkey adotivo, engenheiros de TAC da Cisco.

Processamento do tráfego pelo Snort

A tecnologia subjacente da detecção do serviço da potência de fogo é Snort. A aplicação do Snort no dispositivo da potência de fogo de Cisco é um único processo da linha para o processamento de tráfego. Um dispositivo é avaliado para uma avaliação específica baseada em transferência de dados total de todos os fluxos que atravessam o dispositivo. Espera-se que os dispositivos estão distribuídos em uma rede corporativa, geralmente perto da borda e dos trabalhos da beira com os milhares de conexões.

Os serviços da potência de fogo medem o throughput máximo de um dispositivo pelo tráfego do Balanceamento de carga a um número de processos running diferentes para o snort - um processo do snort para cada CPU no dispositivo. Contudo, o tráfego do equilíbrio da carga de serviços da potência de fogo uniformemente na por por pacote transversalmente todos os exemplos do Snort. O Snort precisa de poder remontar as conexões. Se o doesnot do Snort remonta estas sessões, um sistema da prevenção de intrusão poderia ser iludido

fragmentando os pacotes de tal maneira que uma regra do Snort pode ser menos provável combinar. Para que cada exemplo individual do Snort possa remontar o tráfego, o serviço da potência de fogo deve enviar todo o tráfego de todas as conexões ao mesmo exemplo do Snort. Consequentemente, o algoritmo do Balanceamento de carga é baseado na informação de conexão que pode excepcionalmente identificar uma conexão dada.

o algoritmo 3-Tuple na versão de software 5.3 ou abaixa

Em todas as versões anterior (5.3 ou abaixam), o Snort usa um algoritmo 3-tuple. Os datapoints para este algoritmo são:

- IP da fonte
- IP de Destino
- Protocolo IP

Todo o tráfego com a mesma fonte, o destino, e o protocolo IP são carga equilibrada à mesma instância do Snort.

algoritmo 5-Tuple na versão de software 5.4, 6.0, e maior

Na versão 5.4, em 6.0 ou em maior, a potência de fogo presta serviços de manutenção a usos um algoritmo 5-tuple. Os datapoints que são levados em consideração são mostrados abaixo:

- IP da fonte
- Porta de origem
- IP de Destino
- Porta de Destino
- Protocolo IP

A finalidade de adicionar portas ao algoritmo é equilibrar mais uniformemente o tráfego quando há os pares específicos da fonte e do destino que esclarecem grandes parcelas do tráfego. Adicionando as portas, as portas de origem efêmeras da alta ordem devem ser diferentes pelo fluxo, e devem adicionar a entropia adicional que equilibra mais uniformemente o tráfego aos exemplos diferentes do snort.

Transferência de dados total

Transferência de dados total de um dispositivo é baseada na capacidade combinada de todos os exemplos do snort que trabalham a sua capacidade mais plena. Você pode calcular a avaliação de desempenho de um exemplo individual do Snort tomando a avaliação do dispositivo e dividindo isso pelo número de exemplos do Snort que estão sendo executado.

Por exemplo, um dispositivo 8250 é avaliado no 10 Gbps para o IPS e tem 22 exemplos do corredor do Snort. Consequentemente, o único limiar de desempenho do Snort seria exemplo 10,000 Mbps/22 = 454 Mbps pelo exemplo do Snort. Agora alguns dos dispositivos podem subestimado levemente, consequentemente um único exemplo do Snort pode processar levemente mais do que este algoritmo o daria. O dispositivo 8250 é um deles, geralmente ele repica no 500 Mbps pelo exemplo do Snort.

Um outro exemplo seria um ASA 5516 com os serviços da potência de fogo. O ASA 5516 é avaliado em um throughput máximo do 450 Mbps com os 1500 pacotes de bytes para a visibilidade do aplicativo e o controle (AVC) e o IPS. O ASA 5516 tem 3 exemplos do corredor do

snort. O máximo pela taxa de transferência do exemplo seria aproximadamente 150 Mbps.

Resultado de teste de uma ferramenta da terceira parte

Quando você testa com todo o Web site dos testes de velocidade, ou qualquer ferramenta da medida da largura de banda, como, *iperf*, um grande único fluxo de TCP do córrego está gerado. Este tipo de grande fluxo de TCP é chamado um **fluxo do elefante**. Um fluxo do elefante é uma única sessão, a conexão de rede relativamente longa que consome uma grande ou quantidade desproporcional de largura de banda. Este tipo de fluxo é atribuído a um exemplo do Snort, consequentemente o resultado de teste indica a taxa de transferência de único exemplo do snort, não a avaliação do ritmo de tranferência agregado do dispositivo.

Remediações

Desvio inteligente do aplicativo (IAB)

A versão de software 6.0 introduz uns novos recursos chamados o **desvio de Inteligente Aplicativo** (IAB). Quando um dispositivo da potência de fogo alcança um limiar de desempenho predefinido, a característica IAB procura os fluxos que encontram critérios específicos para contornear inteligentemente que alivia a pressão nos motores da detecção.

> Dica: Mais informação em configurar o IAB pode ser encontrada aqui.

Identifique e confie os grandes fluxos

Os grandes fluxos são relacionados geralmente a grandes transferências de arquivo, por exemplo, aos backup, à replicação de base de dados, etc. Muitas destas transferências de arquivo não podem ser tiradas proveito da inspeção. Para evitar edições com grandes transferências de arquivo, você pode identificar os grandes fluxos e criar regras da confiança do controle de acesso para elas. Estas regras podem identificar excepcionalmente grandes fluxos, permitem que o Snort passe aqueles fluxos uninspected, e não seja limitado pelo único comportamento do exemplo do snort.

> Nota: Para identificar grandes fluxos para regras da confiança, contacte por favor a potência de fogo TAC de Cisco.

Documentos relacionados

- Controle de acesso usando o desvio inteligente do aplicativo