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 nenhum protocolo de transporte não demonstra 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 não pode consumir 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.

A potência de fogo presta serviços de manutenção ao Balanceamento de carga dos usos do tráfego a um número de processo diferente do Snort com o um processo do Snort que é executado em cada CPU no dispositivo. Idealmente, a carga de sistema equilibra o tráfego

uniformemente através de todos os processos do Snort. O Snort precisa de poder fornecer a análise do contexto apropriada para a inspeção NGFW, IPS, e ampère. Para assegurar o Snort é o mais eficaz, todo o tráfego de um fluxo único é carga equilibrada a um exemplo do snort. Se todo o tráfego de um fluxo único não foi equilibrado a um único exemplo do snort, o sistema poderia ser iludido rachando o tráfego de tal maneira que uma regra do Snort pode ser menos provável combinar ou as partes de um arquivo não são contíguas para a inspeção ampère. Consequentemente, o algoritmo do Balanceamento de carga é baseado na informação de conexão que pode excepcionalmente identificar uma conexão dada.

algoritmo 2-Tuple no ASA com serviços da potência de fogo e no NGIPS virtual

No ASA com potência de fogo preste serviços de manutenção à plataforma e NGIPS virtual, tráfego é carga balaned para roncar usando um algoritmo 2-tuple. Os datapoints para este algoritmo são:

- IP da fonte
- IP de Destino

o algoritmo 3-Tuple na versão de software 5.3 ou abaixa na potência de fogo e nos dispositivos FTD

Em todas as versões anterior (5.3 ou abaixam), o tráfego é carga balaned para roncar usando 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 potência de fogo e nos dispositivos FTD

Na versão 5.4, em 6.0 ou em maior, o tráfego é carga balaned para roncar usando 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 medida baseou no ritmo de tranferência agregado de todos os exemplos do snort que trabalham a sua capacidade mais plena. As práticas do padrão para indústria para a taxa de transferência de medição são para conexões de HTTP múltiplas usando vários tamanhos de objeto. Por exemplo, a metodologia de teste NS NGFW mede transferência de dados total do dispositivo usando os objetos 44k, 21k, 10k, 4.4k, e 1.7k. Estes traduzem a uma escala dos tamanhos médios do pacote em torno dos bytes 1k aos bytes 128 devido aos outros pacotes envolvidos na conexão de HTTP.

Você pode calcular a avaliação de desempenho de um exemplo individual do Snort tomando o throughput taxado do dispositivo e dividindo isso pelo número de exemplos do Snort que estão sendo executado. Por exemplo, se um dispositivo é avaliado em 10Gbps para o IPS com um tamanho médio do pacote dos bytes 1k, e esse dispositivo tem 20 exemplos do Snort, o throughput máximo aproximado para uma instância única seria 500 Mbps pelo Snort. Os tipos de tráfego diferentes, protocolos de rede, tamanhos dos pacotes junto com diferenças na política de segurança total podem todo o impacto a taxa de transferência observada do dispositivo.

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 frequentemente tráfego do valor da inspeção do uso alto ao baixo por exemplo, aos backup, à replicação de base de dados, etc. Muitos destes aplicativos não podem ser tirados proveito da inspeção. Para evitar edições com grandes fluxos, 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 aqueles fluxos passem uninspected, e não sejam limitados 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