Sessão do único córrego do processo grande (fluxo do elefante) por serviços de FirePOWER

Índice

Introdução

Este documento descreve porque um fluxo único não pode consumir o throughput taxado inteiro de um dispositivo de Cisco FirePOWER.

Informações de Apoio

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 puderam exibir a avaliação anunciada da taxa de transferência dos dispositivos de Cisco FirePOWER. Similarmente, transferência de um arquivo muito grande sobre nenhum protocolo de transporte não demonstra a avaliação anunciada da taxa de transferência de um dispositivo de FirePOWER. Ocorre porque o serviço de FirePOWER não usa um fluxo de rede única a fim determinar seu throughput máximo.

Tráfego do processo pelo Snort

A tecnologia subjacente da detecção do serviço de FirePOWER é Snort. A aplicação do Snort no dispositivo de Cisco FirePOWER é um único processo da linha a fim processar o tráfego. Um dispositivo é avaliado para uma avaliação específica baseada em transferência de dados total de todos os fluxos que atravessa 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.

Balanceamento de carga do uso dos serviços de FirePOWER do tráfego a um número de processo diferente do Snort com 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 o Firewall da próxima geração (NGFW), o Intrusion Prevention System (IPS) e inspeção avançada da proteção do malware (AMP). A fim 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 e o tráfego derramado de tal maneira que uma regra do Snort pôde ser menos provável combinar ou as partes de um arquivo não são contíguas para a inspeção AMP. 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 de FirePOWER e no NGIPS virtual

Na ferramenta de segurança adaptável (ASA) com a plataforma do serviço de FirePOWER e o sistema da prevenção de intrusão da próxima geração (NGIPS) virtuais, o tráfego é carga equilibrada a fim roncar com o uso de 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 em FirePOWER e em dispositivos FTD

Em todas as versões anterior (5.3 ou abaixam), o tráfego é a carga equilibrada para roncar que 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 em FirePOWER e em dispositivos FTD

Na versão 5.4, em 6.0 ou em maior, o tráfego é carga balaned para roncar com um algoritmo 5-tuple. Os datapoints que são levados em consideração são:

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

A finalidade 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. Pela adição das portas, as portas de origem efêmeras da alta ordem devem ser diferentes pelo fluxo, e devem adicionar a entropia adicional mais uniformemente que equilibra 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 trabalha a sua capacidade mais plena. As práticas do padrão para indústria a fim medir a taxa de transferência são para conexões de HTTP múltiplas com vários tamanhos de objeto. Por exemplo, a metodologia de teste NS NGFW mede transferência de dados total do dispositivo com objetos 44k, 21k, 10k, 4.4k, e 1.7k. Estes traduzem a uma escala dos tamanhos médios do pacote em torno de 1k & dos bytes 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. Tome o throughput taxado do dispositivo e divida isso pelo número de exemplos do Snort que são 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 da 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 IAB. Quando um dispositivo de FirePOWER alcança um limiar de desempenho predefinido, a característica IAB procura os fluxos que encontram critérios específicos a fim contornear inteligentemente que alivia a pressão nos motores da detecção.

> **Tip**: Mais informação na configuração do IAB pode ser encontrada aqui.

Identifique e confie 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. A fim 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.

Note: A fim identificar grandes fluxos para regras da confiança, contacte Cisco FirePOWER TAC.

Informações Relacionadas

- Controle de acesso usando o desvio inteligente do aplicativo
- **Suporte Técnico e Documentação - Cisco Systems**