Índice

Introdução

Este documento descreve os recursos de tracking Inline da sessão de TCP do dispositivo do Intrusion Prevention System (IPS).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Dispositivos do 4200 Series IPS configurados com relações inline.
- Conhecimento do protocolo de TCP e dos fluxos de tráfego.

Componentes Utilizados

A informação neste documento é baseada sobre:

- IPS 4270 com Software Release 7.1(7)

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 sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

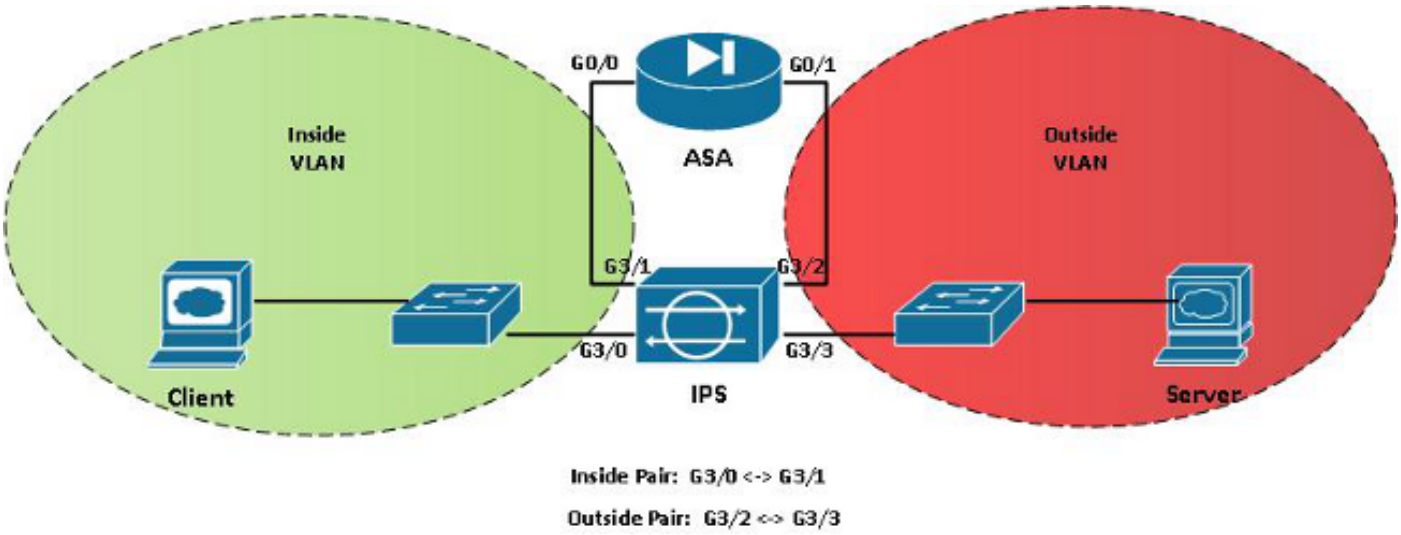
Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter informações sobre convenções de documentos.

Informações de Apoio

Em determinados cenários de distribuição inline IPS, os pacotes de um córrego TCP podem ser vistos duas vezes pelo motor do normalizador, que conduz às gotas devido ao seguimento impróprio do córrego. Esta situação está considerada tipicamente quando o tráfego está distribuído com as redes de área local virtual múltiplas (VLAN) ou os pares da relação que estão monitorados por um único sensor virtual. Esta edição está complicada mais pela necessidade para permitir que o tráfego assimétrico funda para o córrego apropriado que segue quando o tráfego para um ou outro sentido é recebido dos VLAN diferentes ou das relações.

Diagrama de Rede



Problema

Nesta topologia de rede, um cliente na rede interna inicia uma conexão de HTTP ao server na rede externa. Ambos os segmentos de rede são separados por um Firewall adaptável da ferramenta de segurança (ASA). Neste projeto, um único dispositivo IPS é configurado para bater em ambos os VLAN internos e exteriores com dois grupos de pares inline da relação. Quando o cliente inicia a sessão ao server, o pacote TCP SYN (sincronizar) toma este trajeto (córrego de partida) com o IPS e o ASA:

Cliente > IPS G3/0 > *vs0* > IPS G3/1 > ASA G0/0 > ASA G0/1 > IPS G3/2 > *vs0* > IPS G3/3 > server

Após o córrego de partida, o TCP SYN enviado pelo cliente está visto pelo sensor **vs0** virtual enquanto o pacote atravessa os pares da interface interna para a interface interna do ASA e outra vez quando o pacote atravessa os pares da interface externa para o servidor de Web. Em uma encenação simétrica, a mesma situação ocorre no caminho de retorno com o SYN ACK (um

reconhecimento positivo) e pacotes subsequente do servidor de Web. Quando o IPS tenta combinar os córregos em uma única conexão de TCP, as duplicatas de cada pacote na conexão estão observadas, que conduz a um normalizador confuso e aos pacotes descartado. A fim confirmar se um IPS encontra esta situação, a saída do comando do **virt stat da mostra** mostra um grande número 1330 assinaturas do normalizador TCP que fogo, assim como um grande número pacotes e conexões alterados e negados.

Solução

A opção do modo de seguimento da sessão de TCP Inline pode ser usada para superar situações tais como esta. Há três modos possíveis que podem ser configurados:

1. **Sensor virtual (configuração padrão)** - Monitores em uma situação assimétrica do desenvolvimento onde os pacotes cliente sejam vistos em um par inline, quando os pacotes de servidor forem vistos em um segundo par da relação. Os dois pares da relação devem ser monitorados junto para considerar ambos os lados da conexão.
2. **Relação e VLAN** - Esta é uma ação alternativa à topologia de exemplo mostrada neste documento, em que os pares dois ou mais inline da relação são atribuídos ao mesmo sensor virtual. Com esta opção permitida, uma conexão de TCP pode atravessar mais de um par, que permite que o normalizador siga sessões de TCP independentemente para cada par inline.
3. **VLAN somente** - Esta é uma combinação muito rara das primeiras duas opções e é-lhe usada monitora redes assimétricas de uma combinação de múltiplo. **O VLAN1** à esquerda os pares da relação tem pacotes cliente e deve ser combinado com o **VLAN1 no** par direito da relação, que tem os pacotes de servidor. Neste caso, o tráfego é agregado através de todos os pares da relação, mas segregado pelo VLAN. Por exemplo, os pacotes VLAN1 através de todas as relações são colocados junto; Os pacotes VLAN2 de todas as relações são colocados junto, mas os pacotes VLAN1 e VLAN2 são colocados nunca junto para o seguimento da sessão de TCP.

Para a topologia de exemplo acima, há duas maneiras que o problema pode ser resolved:

Solução 1

Mova cada par inline da relação em seu próprio sensor virtual. Por exemplo, um par em **vs0** e um par em **vs1**. Este método é recomendado geralmente quando há menos de quatro pares inline (devido ao limite da plataforma de quatro sensores virtuais). O normalizador trata os córregos duplicados como duas conexões separadas.

Solução 2

Configurar o modo de seguimento da sessão de TCP inline **para conectar e o VLAN**. Este método está recomendado quando há mais de quatro pares inline, neste caso, você está forçado a colocar pares inline múltiplos em um único sensor virtual. O normalizador trata pacotes em pares inline diferentes como conexões completamente diferentes dentro do mesmo sensor virtual.

Configurar

Está aqui a configuração para separar o sensor virtual por pares inline da relação:

Está aqui a configuração para a relação e o VLAN:

Verificar

- Use o **virt stat da mostra | comando statistics** e revisão da **fase do normalizador b TCP** para **deixado cair**, a **duplicata**, **negado**, ou os **pacotes de SendAck enviaram** estatísticas diferente de zero no normalizador TCP.
- Use o **virt stat da mostra | comando count** e revisão de **SigEvent da Por-assinatura b** para 1330 assinaturas que atearam fogo conjuntamente com as estatísticas TCP Normalier do comando precedente.

Informações Relacionadas

- Guia de configuração de CLI do sensor de Sistema de prevenção de intrusões da Cisco para IPS 7.0 - modo de seguimento da sessão de TCP Inline
- Manual de configuração expresso do gerente do Sistema de prevenção de intrusões da Cisco para IPS 7.1 - modo de seguimento da sessão de TCP Inline
- Suporte Técnico e Documentação - Cisco Systems