A inspeção do link agregou o tráfego por Sourcefire FirePOWER e dispositivos virtuais

Índice

Introdução

A agregação do link foi estandardizada pela IEEE em 802.3ad 802.3ax. Os Implementação comum da agregação do link são EtherChannel, protocolo link aggregation control (LACP), Port Aggregation Protocol (PAgP), etc. Este artigo descreve como o link do punho dos dispositivos de Sourcefire agregou o tráfego.

Pré-requisitos

Requisitos

Cisco recomenda que você tem o conhecimento em modelos do dispositivo de Sourcefire FirePOWER, dispositivo virtual modela, o protocolo link aggregation control (LACP), o EtherChannel, e o Port Aggregation Protocol (PAgP).

Apoio da agregação do link

Um dispositivo de Sourcefire pode trabalhar com todas as aplicações padrão da agregação do link, porque um protocolo da agregação do link não adiciona nenhuns dados adicionais ao pacote próprios. Não há nenhum problema conhecido entre a aplicação de dispositivos de Sourcefire e algum liga protocolos da agregação.

Pontos a serem considerados

Os seguintes pontos precisam de ser considerados quando você distribui um dispositivo de

Sourcefire no desenvolvimento agregado link:

1. Se um dispositivo de Sourcefire reage do modo passivo e todos os links do EtherChannel estão sendo monitorados pelo mesmo motor da detecção, a seguir a configuração da agregação do link não importa.
2. Se um único motor da detecção somente estará monitorando alguns dos links ou o dispositivo está sendo distribuído como um dispositivo inline, a seguir recomenda-se que a agregação do link está configurada para usar ambos os endereços MAC de origem e de destino. Isto evitará os problemas de desempenho relativos ao roteamento assíncrono.
3. O Snort é capaz de processar o tráfego agregado link sem o problema. Contudo, o Snort não poderá descodificar os pacotes de controle da agregação do link enviados entre o Switches.
4. Os métodos do Balanceamento de carga no EtherChannel são baseados em cada fluxo de tráfego e não em cada quadro ou pacote, assim que os fluxos são o que obtém a carga equilibrada. A configuração da “do IP fonte e do IP de destino” no EtherChannel pode afetar o Balanceamento de carga através dos exemplos do snort de Sourcefire. Isto é somente se picando resultados executados em mais conjunto limitado de IPs para escolher de. O uso do “MAC de origem e do MAC de destino” pode ajudar com distribuição de carga.

Problema conhecido

O seguinte problema conhecido no LACP é relatado em todas as versões antes de e em incluir 5.3.1.1:

Em alguns casos, aplicar-se muda a sua política do controle de acesso, a política da intrusão, a política da descoberta da rede, ou a configuração de dispositivo, ou instalar uma atualização da regra da intrusão ou a atualização do base de dados da vulnerabilidade (VDB) faz com que o sistema experimente um rompimento no tráfego que usa o protocolo link aggregation control (LACP) no modo rápido. Como uma ação alternativa, configurar os links LACP no modo lento. (112070)

Documento relacionado

- Release Note de 5.3.1.1 da versão do sistema de FireSIGHT