Inspectie van geaggregeerd verkeer door Sourcefire FirePOWER en virtuele applicaties

Inhoud

Inleiding

Link Aggregation is gestandaardiseerd door IEEE op 802.3ad 802.3ax. Gemeenschappelijke implementaties van Link Aggregation zijn EtherChannel, Link Aggregation Control Protocol (LACP), Port Aggregation Protocol (PAgP), enz. In dit artikel wordt beschreven hoe Sourcefire-apparaten omgaan met link tussen geaggregeerd verkeer.

Voorwaarden

Vereisten

Cisco raadt u aan kennis te hebben over Sourcefire FirePOWER-apparaatmodellen, virtuele apparaatmodellen, Link Aggregation Control Protocol (LACP), EtherChannel en Port Aggregation Protocol (PAgP).

Ondersteuning van linkaggregatie

Een Sourcefire-apparaat kan werken met alle standaardimplementaties voor link-aggregatie, omdat een protocol voor link-aggregatie geen extra gegevens aan het pakket zelf toevoegt. Er zijn geen problemen bekend tussen de implementatie van Sourcefire-apparaten en linkaggregatieprotocollen.

Te overwegen dingen

De volgende punten moeten in overweging worden genomen bij het inzetten van een Sourcefire-

apparaat in een link met geaggregeerde implementatie:

1. Als een Sourcefire-apparaat in passieve modus is en alle links van EtherChannel door dezelfde detectiemachine worden bewaakt, is de configuratie van de Link Aggregation niet belangrijk.
2. Als één enkele detectiemachine slechts een aantal van de verbindingen zal controleren of het apparaat als inline apparaat wordt ingezet, dan wordt aanbevolen, dat de Link Aggregation wordt geconfigureerd om zowel bron- als bestemming MAC-adressen te gebruiken. Dit zal de prestatiesproblemen met betrekking tot asynchrone routing vermijden.
3. Snort is in staat om geaggregeerd verkeer zonder probleem te verwerken. Snort kan echter niet de pakketten voor de aggregatie van de link decoderen die tussen de switches worden verzonden.
4. De taakverdelingsmethoden in EtherChannel zijn gebaseerd op elke verkeersstroom en niet op elk frame of pakket. De stromen zijn dus hetgene dat de lading gelijkmatig wordt verdeeld. De configuratie van "Bron IP en Bestemming IP" in EtherChannel kan de taakverdeling over Sourcefire-poortinstanties beïnvloeden. Dit is slechts als het hashing uitgevoerd resultaten in een beperktere reeks IP's heeft uitgevoerd om uit te kiezen. Het gebruik van "MAC-bron en MAC-bestemming" kan helpen bij de lastverdeling.

bekende probleem

Het volgende bekende probleem op LACP wordt gerapporteerd over alle versies voorafgaand aan en met 5.3.1.1:

In sommige gevallen veroorzaakt het toepassen van veranderingen in uw toegangsbeheerbeleid, inbraakbeleid, beleid voor netwerkontdekking, of de configuratie van het apparaat, of het installeren van een update van de inbraakregel of het bijwerken van de kwetsbaarheidsdatabase (VDB) het systeem om een verstoring in verkeer te ervaren die Link Aggregation Control Protocol (LACP) in snelle modus gebruikt. Als een bewerking, moet u de LACP-koppelingen in de modus langzaam configureren. (112070)

Verwante document

- FireSIGHT System versie 5.3.1.1 Releaseopmerkingen