Ispezione del traffico aggregato di collegamento da parte di Sourcefire FirePOWER e appliance virtuali

Sommario

Introduzione

L'aggregazione dei collegamenti è stata standardizzata da IEEE su 802.3ad 802.3ax. Implementazioni comuni dell'aggregazione di collegamenti sono EtherChannel, LACP (Link Aggregation Control Protocol), PAgP (Port Aggregation Protocol), ecc. In questo articolo viene descritto come gli accessori Sourcefire gestiscono il traffico aggregato dei collegamenti.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei modelli di dispositivi Sourcefire FirePOWER, dei modelli di dispositivi virtuali, del protocollo LACP (Link Aggregation Control Protocol), di EtherChannel e del protocollo PAgP (Port Aggregation Protocol).

Supporto dell'aggregazione dei collegamenti

Un accessorio Sourcefire è in grado di interagire con qualsiasi implementazione di aggregazione di collegamenti standard, in quanto un protocollo di aggregazione di collegamenti non aggiunge dati aggiuntivi al pacchetto stesso. Non vi sono problemi noti tra l'implementazione delle appliance Sourcefire e gli eventuali protocolli di aggregazione dei collegamenti.

Fattori da considerare

Quando si distribuisce un'appliance Sourcefire in una distribuzione aggregata con collegamenti, è necessario tenere in considerazione i punti seguenti:

1. Se un accessorio Sourcefire è in modalità passiva e tutti i collegamenti di EtherChannel sono monitorati dallo stesso motore di rilevamento, la configurazione dell'aggregazione dei collegamenti non è rilevante.
2. Se un singolo motore di rilevamento monitorerà solo alcuni collegamenti o se il dispositivo verrà distribuito come dispositivo in linea, è consigliabile configurare l'aggregazione dei collegamenti in modo da utilizzare sia gli indirizzi MAC di origine che quelli di destinazione. In questo modo si eviteranno i problemi di prestazioni relativi al routing asincrono.
3. Snort è in grado di elaborare il traffico aggregato del collegamento senza problemi. Tuttavia, Snort non sarà in grado di decodificare i pacchetti di controllo dell'aggregazione dei collegamenti inviati tra gli switch.
4. I metodi di bilanciamento del carico in EtherChannel sono basati su ciascun flusso di traffico e non su ciascun frame o pacchetto, quindi i flussi sono quelli che ottengono il bilanciamento del carico. La configurazione di "Source IP and Destination IP" in EtherChannel può influire sul bilanciamento del carico tra le istanze di Sourcefire Snort. Ciò è possibile solo se l'hashing eseguito genera un set più limitato di IP tra cui scegliere. L'uso di "MAC di origine e MAC di destinazione" può aiutare con la distribuzione del carico.

Problema noto

Il seguente problema noto relativo a LACP viene segnalato in tutte le versioni precedenti e inclusa la versione 5.3.1.1:

In alcuni casi, l'applicazione di modifiche ai criteri di controllo dell'accesso, ai criteri per le intrusioni, ai criteri di individuazione della rete o alla configurazione dei dispositivi, oppure l'installazione di un aggiornamento o di un aggiornamento delle regole di intrusione del database di vulnerabilità (VDB) provoca un'interruzione del traffico che utilizza il protocollo LACP (Link Aggregation Control Protocol) in modalità rapida. Per ovviare al problema, configurare i collegamenti LACP in modalità lenta. (112070)

Documenti correlati

- Note sulla release di FireSIGHT System versione 5.3.1.1