Sourcefire FirePOWER 및 가상 어플라이언스별 링크 집계 트래픽 검사

목차

소개

링크 집계는 802.3ad 802.3ax의 IEEE에 의해 표준화되었습니다.링크 집계의 일반적인 구현은 EtherChannel, LACP(Link Aggregation Control Protocol), PAgP(Port Aggregation Protocol) 등입니다.이 문서에서는 Sourcefire 어플라이언스가 링크 집계 트래픽을 처리하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 Sourcefire FirePOWER 디바이스 모델, 가상 디바이스 모델, LACP(Link Aggregation Control Protocol), EtherChannel 및 PAgP(Port Aggregation Protocol)에 대한 지식을 활용할 것을 권장합니다.

링크 어그리게이션 지원

링크 어그리게이션 프로토콜은 패킷 자체에 추가 데이터를 추가하지 않으므로 Sourcefire 어플라이언스는 모든 표준 링크 어그리게이션 구현에서 작업할 수 있습니다.Sourcefire 어플라이언스의 구현과 모든 링크 어그리게이션 프로토콜 간에는 알려진 문제가 없습니다.

고려해야 할 사항

링크 집계 구축에서 Sourcefire 어플라이언스를 구축할 때는 다음 사항을 고려해야 합니다.

1. Sourcefire 어플라이언스가 패시브 모드에 있고 EtherChannel의 모든 링크가 동일한 탐지 엔진에 의해 모니터링되는 경우 링크 어그리게이션 컨피그레이션은 중요하지 않습니다.
2. 단일 탐지 엔진이 일부 링크만 모니터링하거나 디바이스가 인라인 디바이스로 구축되는 경우 소스 및 대상 MAC 주소를 모두 사용하도록 링크 집계를 구성하는 것이 좋습니다.이렇게 하면 비동기 라우팅과 관련된 성능 문제가 발생하지 않습니다.
3. Snort는 링크 집계 트래픽을 문제 없이 처리할 수 있습니다. 그러나 Snort는 스위치 간에 전송된 링크 어그리게이션 제어 패킷을 디코딩할 수 없습니다.
4. EtherChannel의 로드 밸런싱 방법은 각 프레임이나 패킷이 아닌 각 트래픽 흐름을 기반으로 하므로 플로우는 로드 밸런싱을 수행합니다.EtherChannel에서 "Source IP and Destination IP(소스 IP 및 대상 IP)"를 구성하면 Sourcefire Snort 인스턴스 간의 로드 밸런싱에 영향을 줄 수 있습니다.해싱을 수행하면 선택할 수 있는 IP가 더 제한적으로 설정된 경우에만 가능합니다."Source MAC and Destination MAC(소스 MAC 및 대상 MAC)"을 사용하면 로드 분산을 지원할 수 있습니다.

알려진 문제

LACP에 대해 다음과 같은 알려진 문제가 5.3.1.1 이전 및 포함 모든 버전에서 보고됩니다.

경우에 따라 액세스 제어 정책, 침입 정책, 네트워크 검색 정책 또는 디바이스 컨피그레이션에 변경 사항을 적용하거나, 침입 규칙 업데이트 또는 VDB(취약성 데이터베이스 업데이트)를 설치하면 시스템이 빠른 모드에서 LACP(Link Aggregation Control Protocol)를 사용하는 트래픽의 중단을 경험하게 됩니다.이를 해결하려면 LACP 링크를 저속 모드로 구성합니다.(112070)

관련 문서

- FireSIGHT System 버전 5.3.1.1 릴리스 정보