Überprüfung des Link-Aggregation-Datenverkehrs durch Sourcefire FirePOWER und virtuelle Appliances

Inhalt

Einführung

Link-Aggregation wurde von IEEE für 802.3ad 802.3ax standardisiert. Häufige Implementierungen von Link-Aggregation sind EtherChannel, Link Aggregation Control Protocol (LACP), Port Aggregation Protocol (PAgP) usw. In diesem Artikel wird beschrieben, wie Sourcefire-Appliances Link-Aggregation-Datenverkehr verarbeiten.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse zu Sourcefire FirePOWER-Gerätemodellen, virtuellen Gerätemodellen, Link Aggregation Control Protocol (LACP), EtherChannel und Port Aggregation Protocol (PAgP) verfügen.

Unterstützung von Link-Aggregation

Eine Sourcefire-Appliance kann mit allen Standard-Verbindungsaggregationsimplementierungen verwendet werden, da ein Link-Aggregation-Protokoll dem Paket selbst keine zusätzlichen Daten hinzufügt. Es sind keine Probleme zwischen der Implementierung von Sourcefire Appliances und Link Aggregation-Protokollen bekannt.

Wichtige Überlegungen

Die folgenden Punkte müssen bei der Bereitstellung einer Sourcefire-Appliance in einer Link-Aggregation-Bereitstellung berücksichtigt werden:

1. Wenn sich eine Sourcefire-Appliance im passiven Modus befindet und alle Verbindungen des EtherChannels von derselben Erkennungs-Engine überwacht werden, spielt die Konfiguration der Link-Aggregation keine Rolle.
2. Wenn eine Erkennungs-Engine nur einige der Verbindungen überwacht oder das Gerät als Inline-Gerät bereitgestellt wird, wird empfohlen, dass die Link-Aggregation so konfiguriert ist, dass sowohl Quell- als auch Ziel-MAC-Adressen verwendet werden. Dadurch werden Leistungsprobleme im Zusammenhang mit asynchronem Routing vermieden.
3. Snort kann problemlos Link-Aggregation-Datenverkehr verarbeiten. Snort kann jedoch die zwischen den Switches gesendeten Link-Aggregation-Steuerungspakete nicht dekodieren.
4. Die Load Balancing-Methoden im EtherChannel basieren auf jedem Datenverkehrsfluss und nicht auf jedem Frame oder Paket. Daher werden die Datenflüsse ausgeglichen. Die Konfiguration von "Quell-IP und Ziel-IP" im EtherChannel kann den Lastenausgleich zwischen Sourcefire-Snort-Instanzen beeinträchtigen. Dies ist nur der Fall, wenn durch Hashing ausgeführte Ergebnisse eine begrenztere Auswahl an IPs ergeben. Die Verwendung von "Quell-MAC und Ziel-MAC" kann bei der Lastverteilung helfen.

Bekanntes Problem

Das folgende bekannte Problem mit LACP wird für alle Versionen vor und einschließlich 5.3.1.1 gemeldet:

In einigen Fällen verursacht die Anwendung von Änderungen an Ihrer Zugriffskontrollrichtlinie, Ihrer Zugriffsrichtlinie, der Netzwerkerkennungsrichtlinie oder der Gerätekonfiguration oder die Installation einer Aktualisierung oder Aktualisierung einer Intrusion-Regel für die Schwachstellendatenbank (VDB) eine Unterbrechung des Datenverkehrs, bei der das Link Aggregation Control Protocol (LACP) im Schnellmodus verwendet wird. Konfigurieren Sie als Problemumgehung LACP-Verbindungen im langsameren Modus. (112070)

Verwandtes Dokument

- Versionshinweise für FireSIGHT-System Version 5.3.1.1