Sourcefire FirePOWER および仮想アプライアンスによるリンク集約トラフィックの検査

目次

概要

リンク アグリゲーションは IEEE により 802.3ad 802.3ax で標準化されました。 リンク アグリゲーションの一般的な実装には、EtherChannel、Link Aggregation Control Protocol（LACP）、Port Aggregation Protocol（PAgP）などがあります。 この記事では、Sourcefire アプライアンスによるリンク アグリゲーション トラフィックの処理方法について説明します。

前提条件

要件

Sourcefire FirePOWER デバイス モデル、仮想デバイス モデル、Link Aggregation Control Protocol（LACP）、EtherChannel、および Port Aggregation Protocol（PAgP）について十分に理解しておくことをお勧めします。

リンク アグリゲーションのサポート

リンク アグリゲーション プロトコルではパケット自体にデータが追加されないため、Sourcefire アプライアンスはすべての標準的なリンク アグリゲーション実装で機能します。 Sourcefire アプライアンスの実装とすべてのリンク アグリゲーション プロトコルの間では、既知の問題はありません。

考慮事項

Sourcefire アプライアンスをリンク アグリゲーション導入環境に導入する際には、次の点を考慮

する必要があります。

1. Sourcefire アプライアンスがパッシブ モードであり、すべての EtherChannel リンクが同一の検出エンジンによってモニタされる場合、リンク アグリゲーション設定は関係ありません。
2. 1 つの検出エンジンが一部のリンクだけをモニタしている場合、またはデバイスがインライン デバイスとして導入されている場合は、送信元 MAC アドレスと宛先 MAC アドレスの両方を使用するようにリンク アグリゲーションを設定することが推奨されます。 これにより、非同期ルーティングに関連するパフォーマンスの問題が回避されます。
3. Snort はリンク アグリゲーション トラフィックを問題なく処理できます。 ただし Snort は、スイッチ間で送信されるリンク アグリゲーション制御パケットを復号化できません。
4. EtherChannel のロード バランシング方式は、各フレームまたはパケットではなく各トラフィック フローに基づいているため、フローがロード バランシングされます。 EtherChannel の [Source IP and Destination IP] の設定は、Sourcefire snort インスタンス全体のロード バランシングに影響することがあります。 これは、実行されたハッシングの結果として、選択可能な IP が限定される場合だけです。 [Source MAC and Destination MAC] を使用するとロード分散に役立ちます。

既知の問題

5.3.1.1 およびそれ以前のすべてのバージョンで、LACP に関する次の既知の問題が報告されています。

場合によって、アクセス コントロール ポリシー、侵入ポリシー、ネットワーク ディスカバリ ポリシー、またはデバイス設定に変更を適用するか、侵入ルール更新または脆弱性データベース（VDB）の更新をインストールすると、システムで、Link Aggregation Control Protocol（LACP）を高速モードで使用するトラフィックが中断されることがあります。 回避策として、低速モードで LACP リンクを設定します。 (112070)

関連資料

- FireSIGHT システム バージョン 5.3.1.1 リリース ノート