Threat Gridアプライアンスクラスタでの外部ロードバランサの使用

内容

概要

このドキュメントでは、ThreatGridアプライアンスクラスタでの外部ロードバランサの使用に関する要件について説明します

前提条件

次の項目に関する知識があることが推奨されます。

- Cisco ThreatGridアプライアンス
- Cisco Firepower Management Center
- Cisco Eメール& Webセキュリティアプライアンス

コンフィギュレーション

Q. 2つ以上の個別のThreatGridアプライアンスを備えたロードバランサを使用して、高可用性/リソース共有を実現できますか。

A. ThreatGridアプライアンス(TGA)は、登録プロセス中に各デバイスのAPIユーザ名+固有キーを設定します。したがって、エンドデバイスはTGAアプライアンスの1つだけに登録されます。これにより、フェールオーバー/リソースバランシングオプションの可能性がなくなります。

ただし、2.4の時点で、TGAはクラスタリングをサポートしています。これにより、TGAリソースは複数の結合TGA間の負荷を管理し、ソフトウェア内でネイティブにリソース管理/HA機能を提供できます。クラスタは、使用可能な参加デバイスを介して要求を処理できるため、エンドデバイスは、複数のデバイス間でAPIキーが一致したり、外部のロードバランサタイプのデバイスを使用したりすることなく、プール内のすべてのリソースを参加および使用できます。ただし、外部ロードバランサをTGAの前に追加すると、よりプールのようなアーキテクチャを提供できます。

要約：

ロードバランサをTGクラスタの前に追加すると、デバイスが参加する単一のホスト名を容易にし、使用可能な任意のノードに転送できます。これはオプションの機能であり、必ずしもTGAソフトウェアが任意のクラスタメンバーに送信される要求に対してネイティブに実行する必要はありません。

– このセットアップでは、SAN証明書を使用する必要があります。CN名はロードバランサのホスト名で、SANエントリには各TGAアプライアンスのロードバランサのホスト名とエントリが含まれます。

ロードバランサの背後にある複数の個別のTGA**は警告で動作**

1. デバイス間で1対1の登録/キー交換が行われるため、LBはエンドデバイスを同じエンドデバイスに100 %の時間で渡す必要があります。デバイスが他のTGAデバイスの分析に到達し、ルックアップが失敗すると、カスケードの問題が発生します。
2. 1 to1キー交換が原因で、TGAデバイス障害のフェールオーバーが不可能になります。