Using an external load balancer with a Threat Grid Appliance Cluster

Contents

Introduction

This document describes the requirements around using an external load balancer with a ThreatGrid Appliance Cluster

Prerequisites

Cisco recommends that you have knowledge of these topics:

- Cisco ThreatGrid Appliance
- Cisco Firepower Management Center
- Cisco Email and Web Security Appliances

Configuration

Q. Can use a Load Balancer with Two or More Separate ThreatGrid Appliances to provide High Availability / Resource Sharing?

A. ThreatGrid appliances (TGA) setup an API username + unique key for each device during the registration process; therefore the end device only registers with one of the TGA appliances. This removes any chance of failover/resource balancing options.

However, as of 2.4, TGA supports clustering which allows the TGA resources to manage the load across multiple joined TGAs to provide resource management/HA functionality natively within the software itself. As the cluster provides the ability to process a request through any available joined device, an end device be able to join and use all resources in the pool without the concerns of API key matches across multiple devices or through the use of an external Load Balancer type device.

Note however an external Load Balancer can be added in front of the TGAs to provide a more Pool like architecture.

Summary:

A Load balancer can be added in front of a TG cluster in order to facilitate a single hostname for devices to join and then be directed to any available node. This is an optional function and not necessarily needed as the TGA software do this natively for any request sent to any cluster member.

-This setup requires the use of a SAN cert in which the CN name is the load balancer hostname and SAN entries contain the load balancer hostname and entries for each of the TGA appliances.

Multiple separate TGAs behind a Load balancer **work with caveats**

1. The LB must pass the end device to the same end device 100% of the time due to the 1 to1 registration/key exchange that occurs between the devices. If a device reaches out to the other TGA device analysis and lookups fail which leads to cascading issues.
2. Failover for TGA device failure would not be possible due to the 1 to1 key exchange.