FirePOWER Management Center displays some TCP connection events in the wrong direction

Contents

Introduction

This document describes the reasons and mitigation steps for FirePOWER Management Center(FMC) displaying TCP connection events in the reverse direction where the Initiator IP is the TCP connection's server IP and Responder IP is the TCP connection's client IP.

> **Note**: There are multiple reasons for occurrence of such events. This documents explains the most common cause of this symptom.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- FirePOWER technology
- Basic knowledge of Adaptive Security Appliance (ASA)
- Understanding of Transmission Control Protocol(TCP) timing mechanism

Components Used

The information in this document is based on these software and hardware versions:

- ASA Firepower Threat Defense (5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X) that runs Software Version 6.0.1 and later
- ASA Firepower Threat Defense (5512-X,5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X,FP9300,FP4100) that runs Software Version 6.0.1 and later

- ASA with Firepower modules (5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X,5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X) that runs Software versions 6.0.0 and later
- Firepower Management Center (FMC) Version 6.0.0 and later

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a clear (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Background

In a TCP connection, **client** refers to the IP which sends the initial packet. The FirePOWER Management Center generates a connection event when the managed device(sensor or FTD) sees the intial TCP packet of a connection.

Devices that track the state of a TCP connection have an **idle timeout** defined to make sure that connections that are erroneously not closed by endpoints do not consume the available memory for long periods of time. The default idle timeout for established TCP connections on FirePOWER is **three minutes**. A TCP connection that has stayed idle for three minutes or more, is not tracked by the FirePOWER IPS sensor.

The subsequent packet after the timeout is treated as a new TCP flow and the forwarding decision is taken as per the rule that matches this packet.When the packet is from the server, the server's IP is recorded as the initiator of this new flow. When logging is enabled for the rule, a connection event is generated on the FirePOWER Management Center.

> **Note**: As per configured policies, the forwarding decision for the packet that comes after the timeout is different from the decision for the initial TCP packet. If the configured default action is "Block", the packet is dropped.

An example of this symptom is as per the screenshot below:

First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code
2017-05-12 17:48:05		Block		10.32.38.30		192.168.38.30				443 (https) / tcp	44705 / tcp
2017-05-12 17:39:13		Allow		192.168.38.30		10.32.38.30				44705 / tcp	443 (https) / tcp

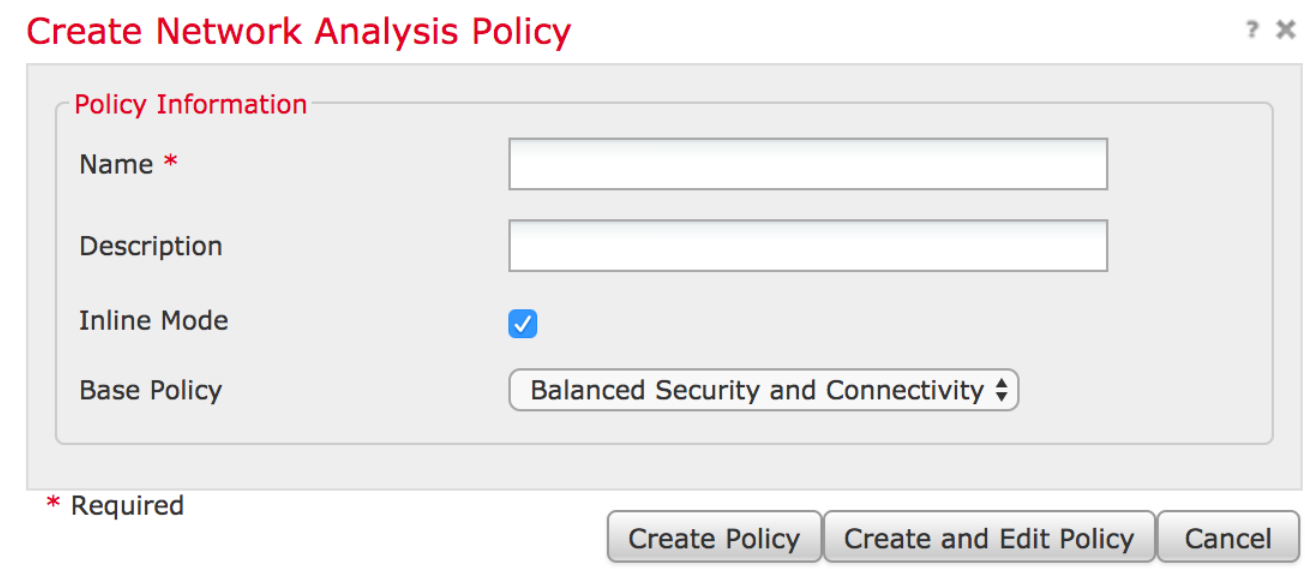
Solution

The above mentioned problem is mitigated by increasing the **Timeout** of TCP connections. In order change the timeout,

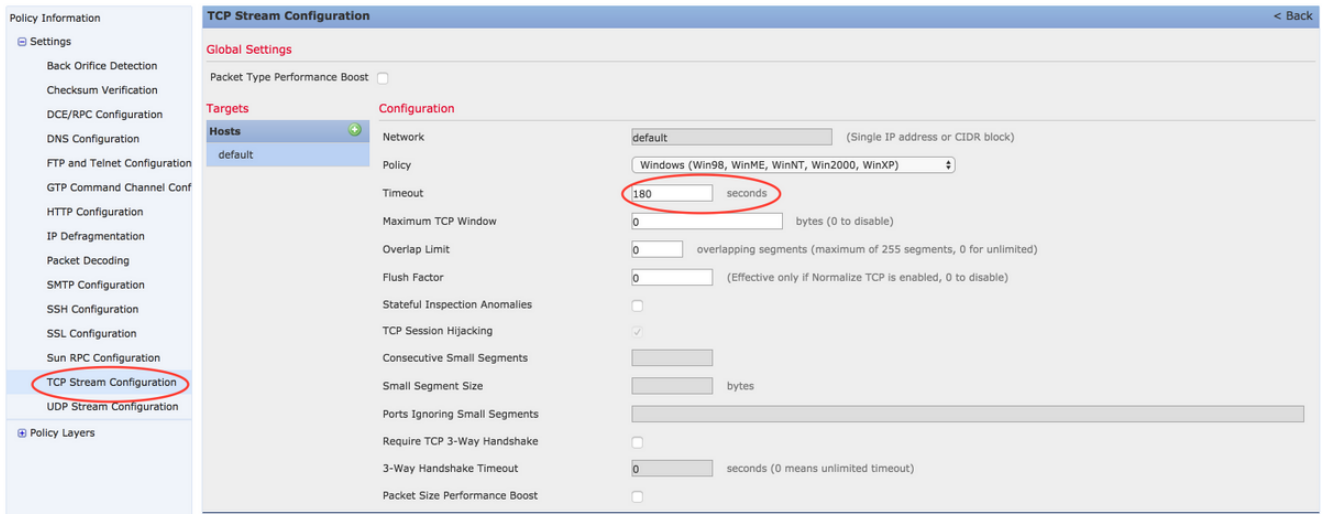
1. Navigate to **Policies > Access Control > Intrusion**.
2. Navigate to the top right corner and select **Network Access Policy**.

3. Select **Create Policy** ,choose a name and click on **Create and Edit Policy**. Do not modify

the **Base Policy.**

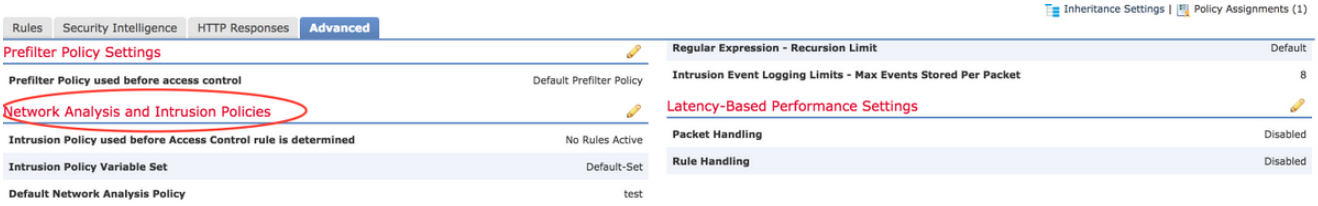


4. Expand the **Settings** option and choose **TCP Stream Configuration**.
5. Navigate to the configuration section and change the value of **Timeout** as desired.



6. Navigate to **Policies > Access Control > Access Control**.
7. Select the option **Edit** to edit the the policy applied to relevant managed device or create a new policy.

8. Select the **Advanced** tab in the Access policy.
9. Locate **Network Analysis and Intrusion Policies** section and click on **Edit** icon.



10. From the drop-down menu of **Default Network Analysis Policy**, choose the policy created in step 2.

11. Click **OK** and **Save** the changes.
12. Click on **Deploy** option to deploy the polices to relevant manged devices.

Caution: Increasing timeout is expected to cause higher memory utilization, FirePOWER has to track flows that are not closed by endpoints for a longer time. The actual increase in memory utilization is different for each unique network as it depends on how long the network applications keep TCP connections idle.

Conclusion

Every network's benchmark for idle timeout of TCP connections are different. It completely depends upon the applications that are in use. An optimum value must be established by observing how long network applications keep TCP connections idle. For issues that pertain to FirePOWER service module on a Cisco ASA, when an optimum value cannot be deduced, the timeout can be tuned by increasing it in steps upto ASA's timeout value.

Related Information

- **Cisco Firepower Threat Defense Quick Start Guide for the ASA**
- **Technical Support & Documentation - Cisco Systems**
- **ASA Firepower Quick Start Guide**