

AdjustfloodThreshold

# 

# 

# Brief Description

The Skillet provides the ability to adjust GGSN Tunnel Protocol (GTP) flood attributes.

# Target Audience

Target audiences include SEs, Mobile Network Operator (MNO) customers, and the corresponding partners. SEs include both - service provider and enterprise teams, whose customers are MNOs.

# Skillet Details

**Authoring Group**: Service Provider

**Documentation**: <to be provided>

**Github Location**: <to be adjusted>

<https://github.com/gpildush/GTPvulnerabilitiesSkillets/blob/master/AdjustfloodThreshold/adjustThresholdsGTP.xml>

**PAN-OS Supported**: 8.0 +

**Cloud Provider(s) Supported**: N/A

**Type of Skillet**: .xml

**Purpose**: Config

**Status**: draft

# Detail Description

This Skillet is a Stage 2 of the InitializeAndEnableGTPvulnerabilities one.

Once you observe GTP behavior for a period of time within an MNO’s production network, you may need to adjust the default GTP flood threshold attributes. Alternatively, you may adjust those attributes, as per MNO’s provided values.

This configuration is required for RAN/EPC and/or roaming security for MNOs or MVNOs. Specifically, it may be used while provisioning stateful GTP security for these interfaces → S11, S5, S8, Gn, Gp.

It is assumed that you’ve executed EnableGTPFloodAttributes Skillet first, which results in enabling GTP flood threats. GTP flood attributes are configured within the Security Profiles → Vulnerability Protection level of configuration.

The GTP flood attributes include the following threats:

40054 - GTPv1-C Create PDP Context Request Flood;

40055 - GTPv1-C Update PDP Context Request Flood;

40056 - GTPv1-C Delete PDP Context Request Flood;

40057 - GTPv1-C Echo Request Flood;

40063 - GTPv1-C Create Session Request Flood;

40064 - GTPv2-C Delete Session Request Flood;

40065 - GTPv2-C Modify Bearer Request Flood;

40066 - GTPv2-C Release Access Bearer Request Flood; and

40067 - GTPv2-C Echo Request Flood.

Upon the execution of the AdjustfloodThreshold Skillet, you will adjust one or more GTP flood attributes within the configuration of our firewall.