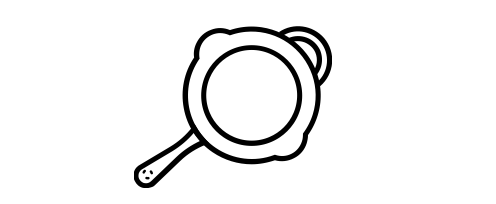
InitializeAndEnableGTPvulnerabilities

# 

# Brief Description

The Skillet initializes GGSN Tunnel Protocol (GTP) vulnerabilities checks, including floods’ attributes, by enabling them.

# 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**: <https://github.com/gpildush/GTPvulnerabilitiesSkillets/blob/master/InitializeAndEnableGTPvulnerabilities/initializeAndEnableGTPwithAttributes.xml>

**PAN-OS Supported**: 8.0 +

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

**Type of Skillet**: .xml

**Purpose**: Config

**Status**: semi-final, might need some tweaking.

# Detail Description

The Skillet enables and initializes all GTP flood attributes, while leaving the flood threshold values to their respective default values. This is advisable to do during the initial setup, unless a respective MNO provides the corresponding threshold values to deploy. In many instances, however, MNOs don’t have the attributes and rely on our expertise. It is, therefore, is a good idea to maintain the default threshold attributes for couple of weeks, while observing the corresponding GTP messages’ behavior on our platform, which is positioned within the MNO’s core network. Once established, Skillet named “AdjustfloodThreshold” may be used to adjust GTP flood attributes accordingly.

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.

By default, all GTP vulnerabilities attributes are disabled. GTP vulnerabilities are configured within the Security Profiles → Vulnerability Protection level of configuration.

The GTP vulnerabilities include the following threats:

39084 - GTPv1-C Create PDP Context Request Message

39085 - GTPv1-C Update PDP Context Request Message

39086 - GTPv1-C Delete PDP Context Request Message

39088 - GTPv1 Echo Request Message

39575 - GTPv2-C Create Session Request Message

39608 - GTPv2-C Delete Session Request Message

39609 - GTPv2-C Modify Bearer Request Message

39610 - GTPv2-C Release Access Bearer Request Message

39611 - GTPv2-C Echo Request Message

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 InitializeAndEnableGTPvulnerabilities Skillet, all aforementioned GTP vulnerabilities, including the flood ones with their respective threshold values, are enabled within the configuration of our firewall.