FMC 6.2 REST-APIs: Using FTD Device Package without APIC

Demo on youtube: https://youtu.be/GcCDxbFcchg

GitHub location: https://github.com/cisco-security/FMC-REST-API-scripts

Scripts: ftd-l2fw-apic.json ftd-l2fw-create.py ftd-l2fw-modify.py

The python scripts included here are stand-alone scripts that use/reference procedures build into FTD device package to configure FTD in Transparent (L2FW) Firewall mode, with two interfaces in a BVI. FTD device package should be unzipped and script copied into its directory.

Scripts include the device spec and device configuration sections that APIC would use to configure an FTD device in a managed service graph. In our case, we can use a stand-alone python script to apply the same configuration instead of using APIC.

The sample scripts are created by watching an APIC debug.log in FTD device package logs directory (/data/devicescript/CISCO.FTD_FI.1.0/logs/debug.log). Captured json device spec and device config sections (see ftd-l2fw-apic.json file included) are sanitized to create a script that can apply configuration stand-alone (see ftd-l2fw-create.py). Config creation script uses serviceAudit procedure built into device package.

To remove the configuration we have a second python script that uses serviceModify procedure with device and config sections ‘state’ arguments changed to value ‘3’.

FMC REST-API stand-alone script for FTD Transparent Firewall (BVI) configuration (No APIC)

Here is the diagram used in the yourtube demo where we use scripts to configure FTD inserted in ACI fabric with an unmanaged service graph: