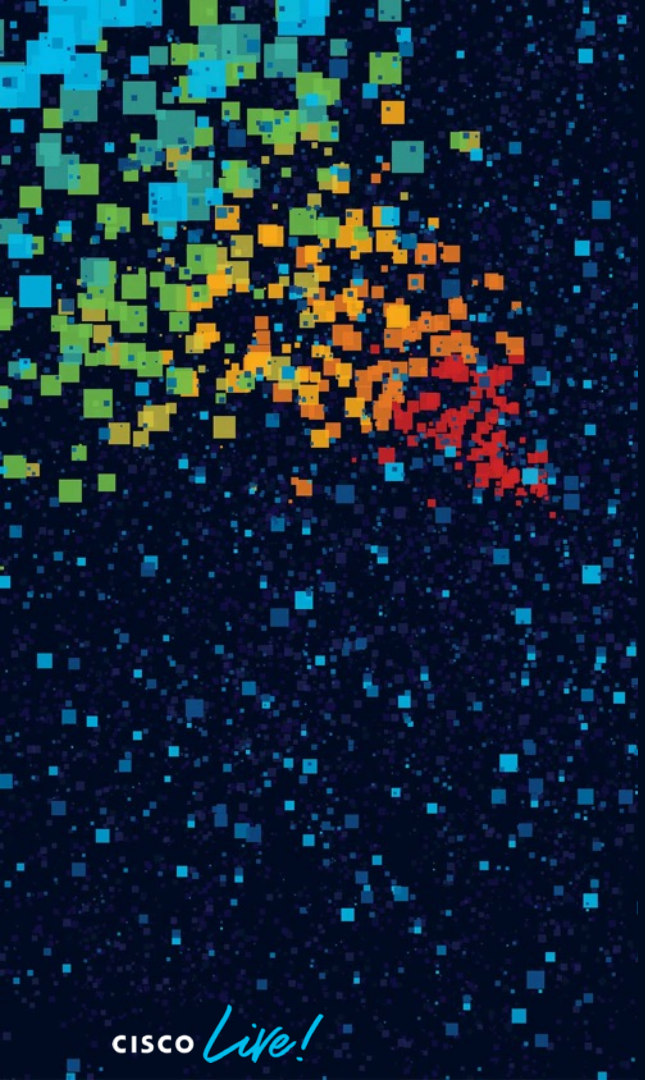
Firepower & Firepower APIs
Part1: FTD API

Security Cisco Live Virtual DevNet Day

Jared Smith – Principal Engineer

cisco Live!

cisco



Agenda

- Introduction Firepower Threat Defense
- Introduction to Firepower Threat Defense REST API
- Demo Ansible
- Demo Import/Export API

What is a Next Generation Firewall?

- Firepower Threat Defense (FTD) is our Next Generation Firewall (NGFW)

- Next Generational Functionality Includes:
  - Application Awareness
  - Decryption
  - Intrusion Prevention
  - Talos Intelligence
  - User Identity

Firepower Threat Defense API Use Cases

- Automated provisioning
- Scaling Configuration Updates
- Configuration Verification
- Object Definition Changes
- Configuration Cloning

Firepower Threat Defense REST API

- Direct to device API public since 6.2.3
- Used by Firepower Device Manager & Cisco Defense Orchestrator
- Internally Automated for Regression Test
- OAuth password authentication to obtain a token
- All features in FDM have an API
- The API is stable with good functionality coverage (SMB & Commercial)

Direct to Device API Options

{REST}

OpenAPI Specification

Bravado or other Libraries

Ansible

Firepower Threat Defense

What is Ansible?

- **Opensource** (free to use) tool supporting configuration management automation
- **No agent required** on the firewall
- **Declarative** configuration definition in YAML
- **Easy automation framework** – simple to use and learn (no programming required)
- **Idempotent** – Can replay playbook (checks current state and only does the required changes)

Import/Export API what is it for?

- Bulk Transactional addition and extraction of configuration from FTD
  - Faster than individual calls
- Performed as a background job (Asynchronous)
- Use Cases:
  - Cloning a device
  - Replicating objects
  - Replication of objects and policy
- Opensource tooling exists to get you started

API Demonstrations

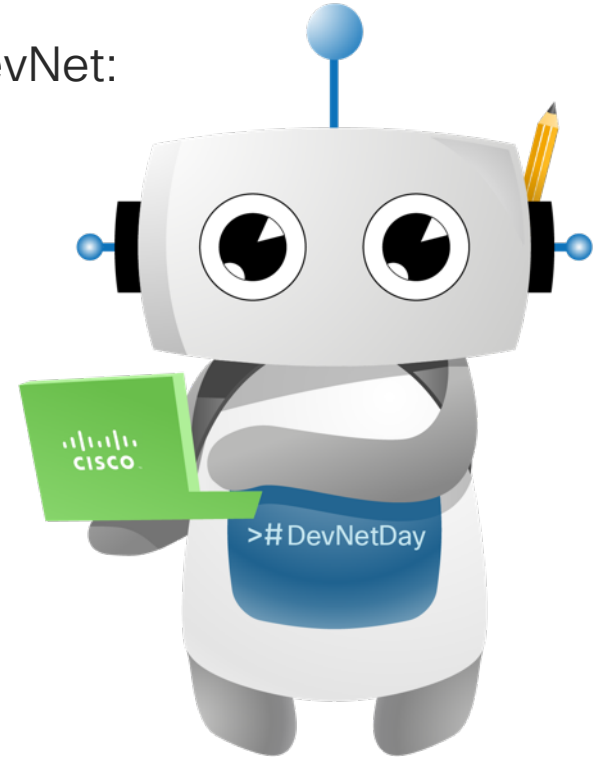
I will take you through two exercises leveraging a DevNet Sandbox:

- Ansible Demo
- Using Bulk Import Export API

Demo

Explore More

- General launch point for FTD-API resources on DevNet:
  - https://developer.cisco.com/firepower/threat-defense/
- Ansible Information:
  - https://developer.cisco.com/site/ftd-ansible/
  - https://github.com/CiscoDevNet/FTDAnsible
  - https://developer.cisco.com/learning/lab/fdm-api-103/step/1
- Import/Export API:
  - https://github.com/jaredtsmith/ftd_api
  - https://developer.cisco.com/learning/lab/fdm-api-104/step/1



Thank you

Possibilities

#CiscoLive | #DevNetDay