The bridge to possible

Exploring FDM API Use Cases

Cesar Barrientos, Technical Leader, CX Americas
@i_am_csr

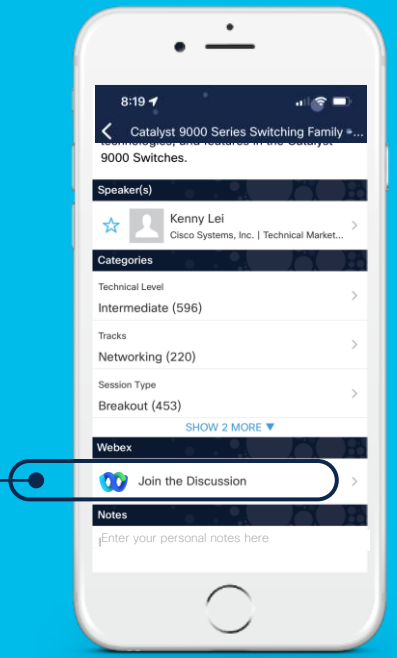
Cisco Webex App

Questions?

Use Cisco Webex App to chat
with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space



Webex spaces will be moderated until February 24, 2023.

About your presenter

Cesar Barrientos
Technical Leader, CX Security
Technical Leadership team in Mexico

In Cisco for 7 years.
5 years as TAC engineer
1 year as Consulting engineer
1 year as Technical Leader

Email: cbarrien@cisco.com

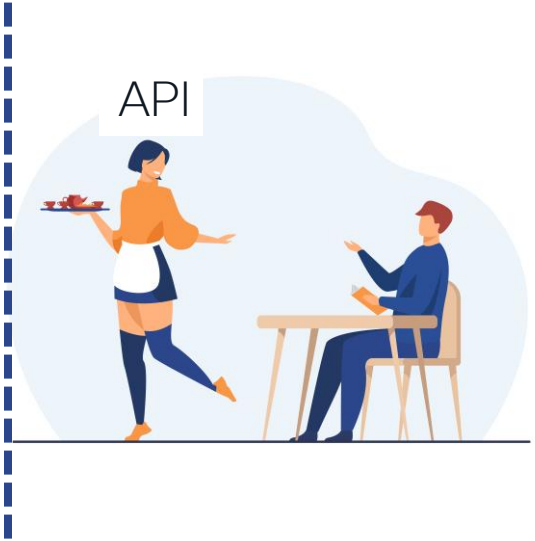
Agenda

- API Overview
- Firepower Programmability Journey
- Use Cases

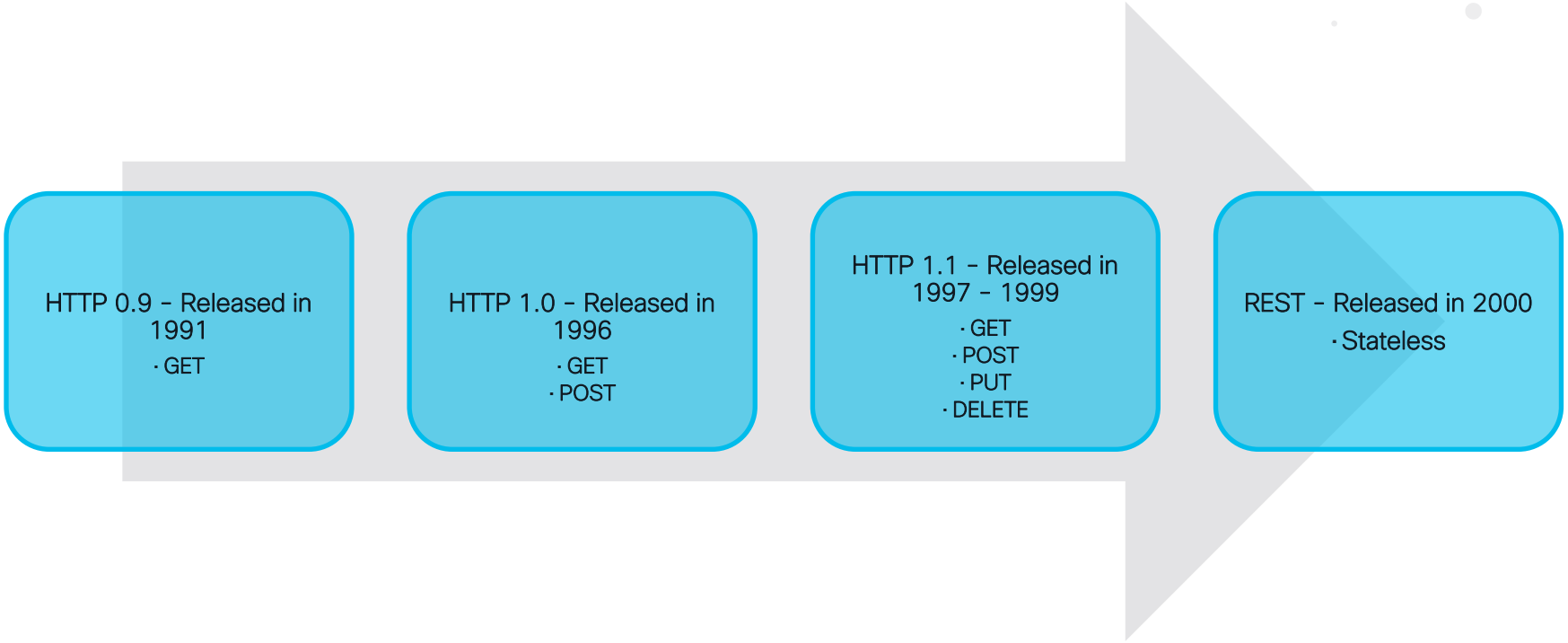
API Overview

What is an API?

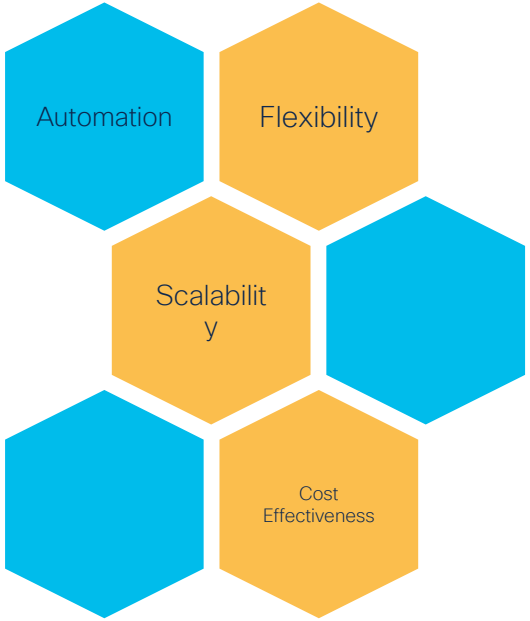
- Stands for **“Application Programming Interface”**
- Mechanism to allow communication between two different softwares



HTTP - REST over the time



Why API?



Data Serialization Languages

```
<devices>

  <hostname>MY_FDM</hostna
  me>

  <ipaddr>192.168.45.45</ipadd
  r>
 <port>443</port>
 <username>admin</username>
```

XML

```
{"devices": [
   {
     "hostname": "MY_FDM",
     "ipaddr": "192.168.45.45",
     "port": 443,
     "username": "admin",
     "password": "Admin123",
     "version": 4
   }
 ]}
```

JSON

```
---
devices:
  - hostname: MY_FDM
    ipaddr:   192.168.45.45
    port: 443
    username: admin
    password: Admin123
    version: 4
```

YAML

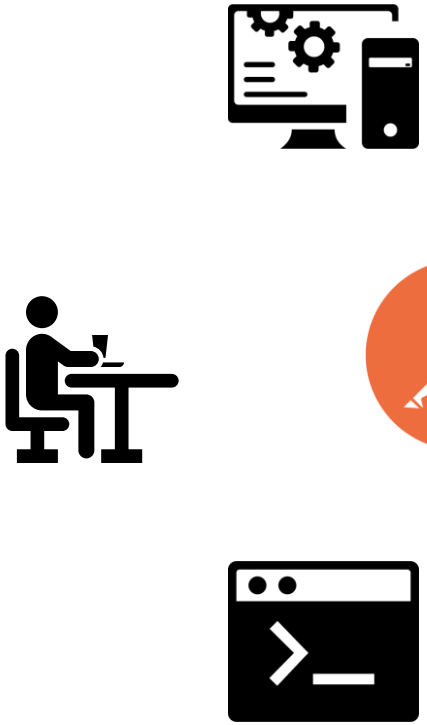
API Authentication methods

Basic Authentication	• Username and password
API Keys	• Unique generated value is assigned to each first time user

OAuth (2.0)	• Involves security tokens called bearer tokens
	  • access token
	  • refresh token

API Clients

- API Explorer
- Postman
- Curl/CMD
- Programming languages
- Others



Firepower Programmability Journey

Threat Defense REST API history

FMC started in 6.1 and it is still in v1

Initial Release

Get /api/versions

REST API v1 - Version 6.2.3

REST API v2 - Version 6.3

REST API v3 - Version 6.4

REST API v4 - Version 6.5

REST API v5 - Version 6.6

REST API v6 - Version 6.7

REST API v6 (6.1) - Version 7.0

REST API v6 (6.2) - Version 7.1

REST API v6 (6.3) - Version 7.2

REST API v6 (6.4) - Version 7.3

External Authorization wih RADIUS

ConfigurationImportExport
FileAndMalwarePolicies
Security Intelligence
LDAP attributes for VPN

From here URL does not change

Threat Defense API (FDM v7.3.0-69)

Firewall Device Manager | Monitoring | Policies | Objects | Device: **firepower** | admin *Administrator* | cisco SECURE

Threat Defense REST API

- API Explorer
- Error Catalog

that you use the API Explorer on a non-production device.

Cisco makes no guarantee that the API version included on this Firepower Threat Device (the "API") will be compatible with future releases. Cisco, at any time in its sole discretion, may modify, enhance or otherwise improve the API based on user feedback.

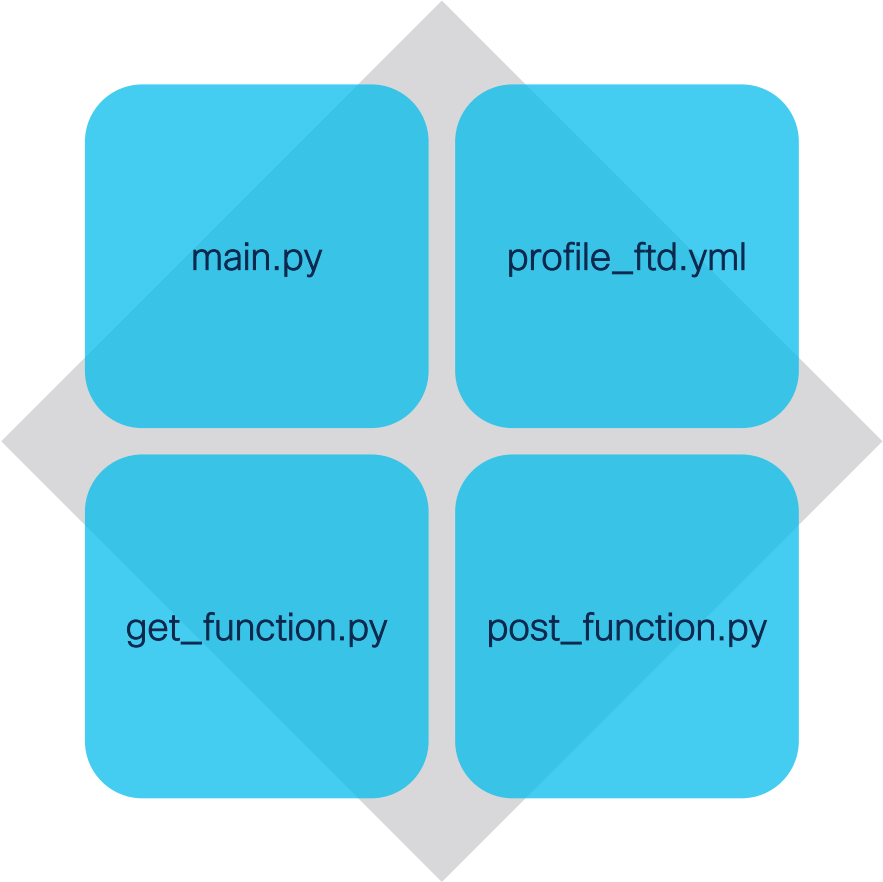
AAASetting	Show/Hide | List Operations | Expand Operations
ASPathList	Show/Hide | List Operations | Expand Operations
AccessPolicy	Show/Hide | List Operations | Expand Operations
ActiveDirectoryRealm	Show/Hide | List Operations | Expand Operations
ActiveUserSessions	Show/Hide | List Operations | Expand Operations
AnyConnectClientProfile	Show/Hide | List Operations | Expand Operations
AnyConnectPackageFile	Show/Hide | List Operations | Expand Operations
ApiVersions	Show/Hide | List Operations | Expand Operations
Application	Show/Hide | List Operations | Expand Operations
ArchivedBackup	Show/Hide | List Operations | Expand Operations
AuditEntityChange	Show/Hide | List Operations | Expand Operations
AuditEvent	Show/Hide | List Operations | Expand Operations
BGP	Show/Hide | List Operations | Expand Operations
BGPGeneralSettings	Show/Hide | List Operations | Expand Operations
BackupImmediate	Show/Hide | List Operations | Expand Operations

Threat Defense Resources

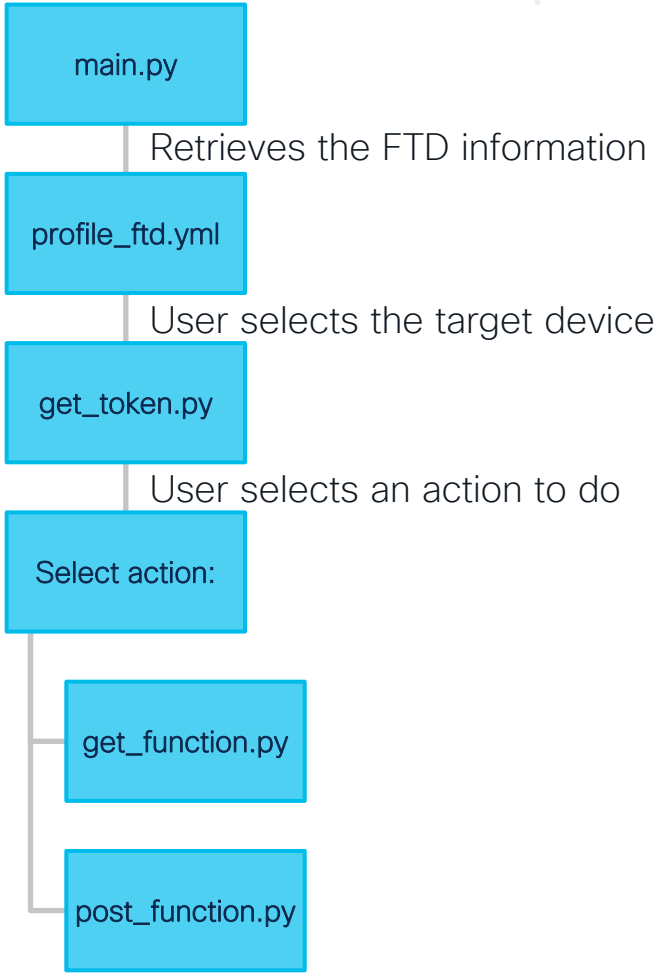
AAASetting
ASPathList
AccessPolicy
AnyConnectClientProfile
BGP
BackupImmediate
Command
CommandAutoComplete
Deployment
EIGRP
FlexConfigPolicy
GeoLocation
HAConfiguration
IPV4PrefixList
IPV6PrefixList
IdentityPolicy
IkevOnePolicy
IkevTwoPolicy
Interface
InterfacePresenceChange
IntrusionPolicy
Job
ManagementIP
NAT
NTP
NTPStatus
NetworkAnalysisPolicy
NetworkObject
OSPF
PendingChanges
PolicyList
PortObject
RaVpn
RouteMap
Routing
SNMP
SRUFileUpload
SSLPolicy
ScheduleTroubleshoot
SecurityGroupTag
SecurityZone
SmartLicensing
SystemInformation
URLCategory
URLObject
URLReputation
Upgrade
UrlCategoryInfo
VDBFileUpload
VDBUpdateImmediate
VDBUpdateSchedule
VirtualTunnelInterface
WebAnalyticsSetting
WebUICertificate

Use Cases

Code Design



App Workflow



Code Snippets

To read the FTD profile:

```
def read_ftd_profile(filename="profile_ftd.yml"):
    file = open(filename, "r")
    yaml_raw = file.read()
    ftd_info = yaml.load(yaml_raw, Loader=yaml.FullLoader)
    return ftd_info
```

Use Case 1: Read Network Resources

Code Snippets

Calling the module from the main file:

```
# * Collecting network objects and network groups
print("Collecting objects...")
objects = {}
objects['objects'], objects['network_groups'] = get_network_object.get(base_url, api_version,
                                                                        token.get("access_token"))
print("Done!")
```

Doing the API request:

```
api_path = url + f"/api/fdm/{api_version}/object/networks?offset={offset}&limit={limit}"

response = requests.request("GET", api_path, headers=headers, verify=False)
```

Use Case 2: Write configuration

Code Snippets

Calling the module from the main file:

```
# * Read information from CSV file
df = pd.read_csv('objects.csv')
print(green("Objects found..."))
print(yellow("Objects read..."))
# print(df.to_dict("record"))

# * Writing objects
for obj in df.to_dict("record"):
    print(blue(f"Writing object {obj['name']}"))
    post_network_object.post(base_url, api_version, token.get("access_token"), obj)
```

Bonus..

Complete your Session Survey

- Please complete your session survey after each session. Your feedback is important.
- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Session Catalog and clicking the "Attendee Dashboard" at https://www.ciscolive.com/emea/learn/sessions/session-catalog.html

Continue Your Education

Visit the Cisco Showcase for related demos.

Book your one-on-one Meet the Engineer meeting.

Attend any of the related sessions at the DevNet, Capture the Flag, and Walk-in Labs zones.

Visit the On-Demand Library for more sessions at ciscolive.com/on-demand.

The bridge to possible

Thank you

cisco Live!

CISCO Live!

ALL IN