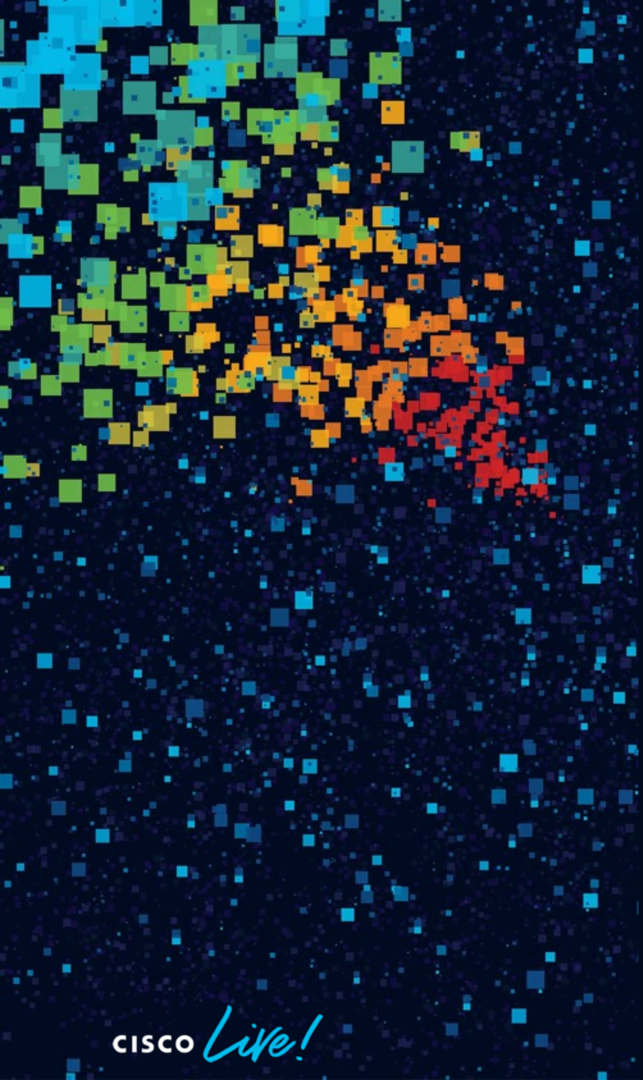
Firepower API and O365 Lightning Talk

Security Cisco Live Virtual DevNet Day

Christopher van der Made
@Chrisco_DevNet



Agenda

- Intro O365 networking best practices
- Intro Firepower API
- Flow of script
- Short demo
- Conclusion

Intro O365 networking best practices

Microsoft O365 Networking Best Practices

- All offices of your organization should have local Internet connections.
- Each local Internet connection should be using a regionally local DNS server for outbound Internet traffic from that location.
- Whenever possible, configure your edge routers to send trusted Microsoft O365 traffic directly, instead of proxying or tunneling through a gateway.
- Configure your edge devices to forward traffic without processing. This is known as traffic bypass.

Source: https://docs.microsoft.com/en-us/microsoft-365/enterprise/networking-provide-bandwidth-cloud-services

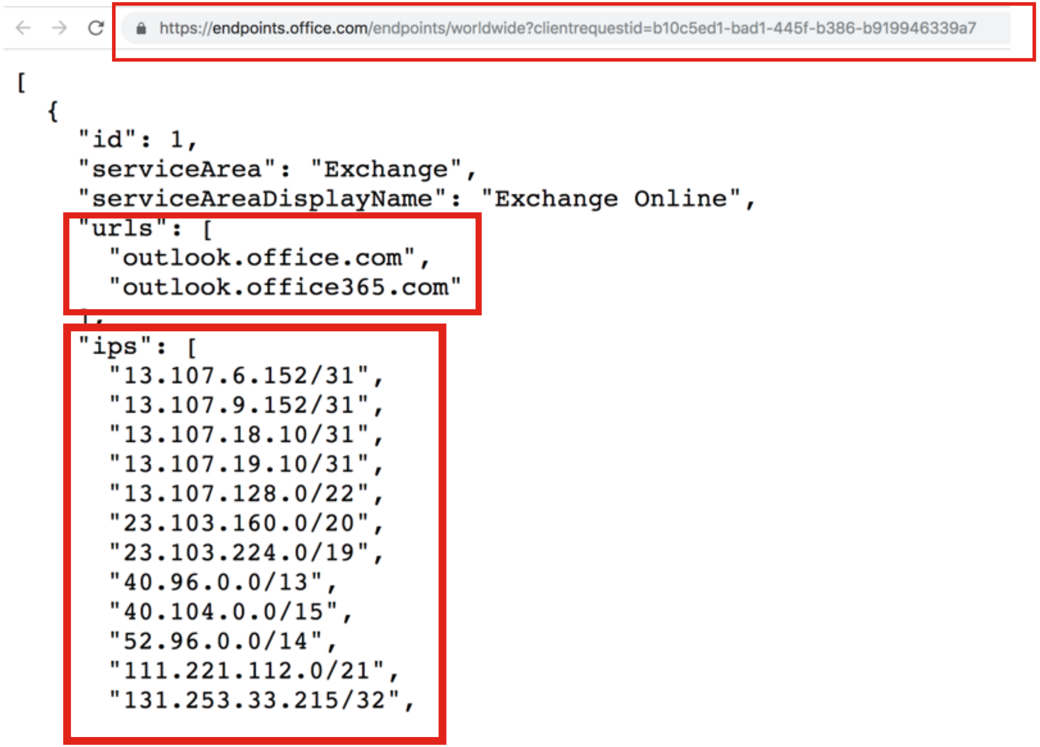
Microsoft O365 Networking Best Practices

“To configure and update the configurations of edge devices, you can use a script or a REST call to consume a structured list of endpoints from the Office 365 Endpoints web service. For more information, see Office 365 IP Address and URL Web service.”

Microsoft O365 Web Service API

- Service Areas:
  - *Exchange* Online and Exchange Online Protection
  - *SharePoint* Online and OneDrive for Business
  - *Skype* for Business Online and Microsoft Teams
  - *Common*, O365 Pro Plus, Office Online, Azure AD and others.
- Categories:
  - *Optimize*: bypass or whitelist on edge devices (75% of all O365 traffic)
  - *Allow*: bypass or whitelist on edge devices (less sensitive though to latency etc.)
  - *Default*: can be treated as “normal” traffic (not always hosted by MSFT)

JSON format O365 Web Service

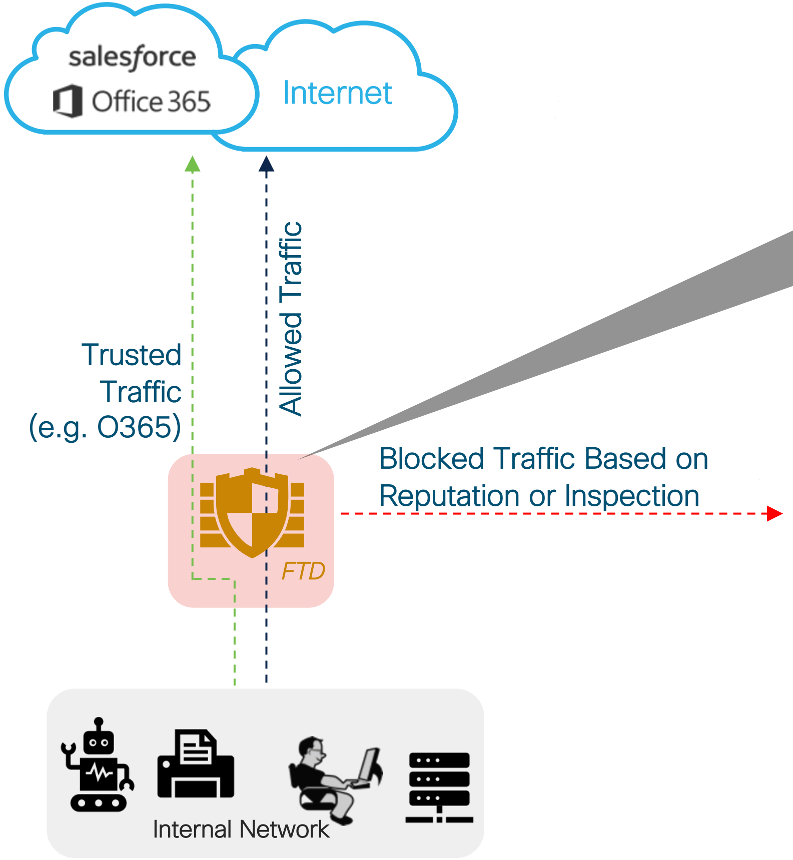


https://endpoints.office.com/endpoints/worldwide?clientrequestid=b10c5ed1-bad1-445f-b386-b919946339a7

```
[
  {
    "id": 1,
    "serviceArea": "Exchange",
    "serviceAreaDisplayName": "Exchange Online",
    "urls": [
      "outlook.office.com",
      "outlook.office365.com"
    ],
    "ips": [
      "13.107.6.152/31",
      "13.107.9.152/31",
      "13.107.18.10/31",
      "13.107.19.10/31",
      "13.107.128.0/22",
      "23.103.160.0/20",
      "23.103.224.0/19",
      "40.96.0.0/13",
      "40.104.0.0/15",
      "52.96.0.0/14",
      "111.221.112.0/21",
      "131.253.33.215/32",
```

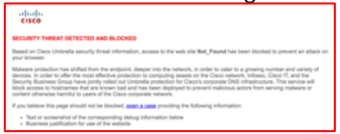
Intro Firepower API

Firepower Threat Defense Traffic Flow


salesforce
Office 365
Internet
Trusted Traffic (e.g. O365)
Allowed Traffic
FTD
Blocked Traffic Based on Reputation or Inspection
Internal Network

- Firewalling + NGIPS
- Application Control
- AMP and Threat Grid
- URL Filtering
- Security Intelligence
- Virtual Patching

Unified Block Page



SECURITY THREAT DETECTED AND BLOCKED

Based on Cisco Umbrella security threat information, access to the web site **Not_Found** has been blocked to prevent an attack on your browser.

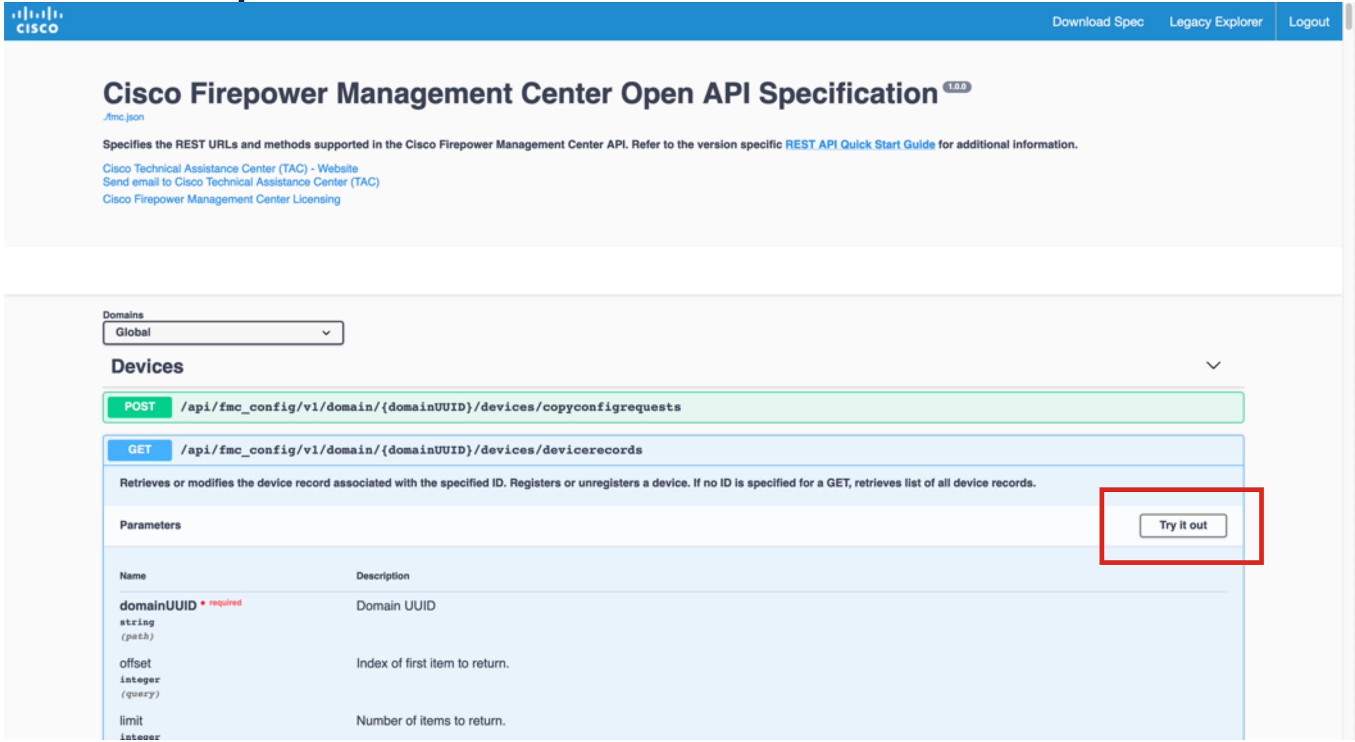
Malware protection has shifted from the endpoint, deeper into the network, in order to cater to a growing number and variety of devices. In order to offer the most effective protection to computing assets on the Cisco network, Infosec, Cisco IT, and the Security Business Group have jointly rolled out Umbrella protection for Cisco's corporate DNS infrastructure. This service will block access to hostnames that are known bad and has been deployed to prevent malicious actors from serving malware or content otherwise harmful to users of the Cisco corporate network.

If you believe this page should not be blocked, open a case providing the following information:

- Text or screenshot of the corresponding debug information below
- Business justification for use of the website

Pro Tip

FMC API Explorer



Cisco Firepower Management Center Open API Specification 1.0.0

./fmc.json

Specifies the REST URLs and methods supported in the Cisco Firepower Management Center API. Refer to the version specific REST API Quick Start Guide for additional information.

Cisco Technical Assistance Center (TAC) - Website
Send email to Cisco Technical Assistance Center (TAC)
Cisco Firepower Management Center Licensing

Domains: Global

Devices

POST /api/fmc_config/v1/domain/{domainUUID}/devices/copyconfigrequests

GET /api/fmc_config/v1/domain/{domainUUID}/devices/devicerecords

Retrieves or modifies the device record associated with the specified ID. Registers or unregisters a device. If no ID is specified for a GET, retrieves list of all device records.

Parameters

Try it out

Name	Description
domainUUID * required string (path)	Domain UUID
offset integer (query)	Index of first item to return.
limit integer	Number of items to return.

https://<address-of-FMC>/api/api-explorer

Firepower API Use Cases

Augment firewall contextual data

Host discovery

Vulnerability analysis

More accurate IPS recommendations

Automate firewall configuration

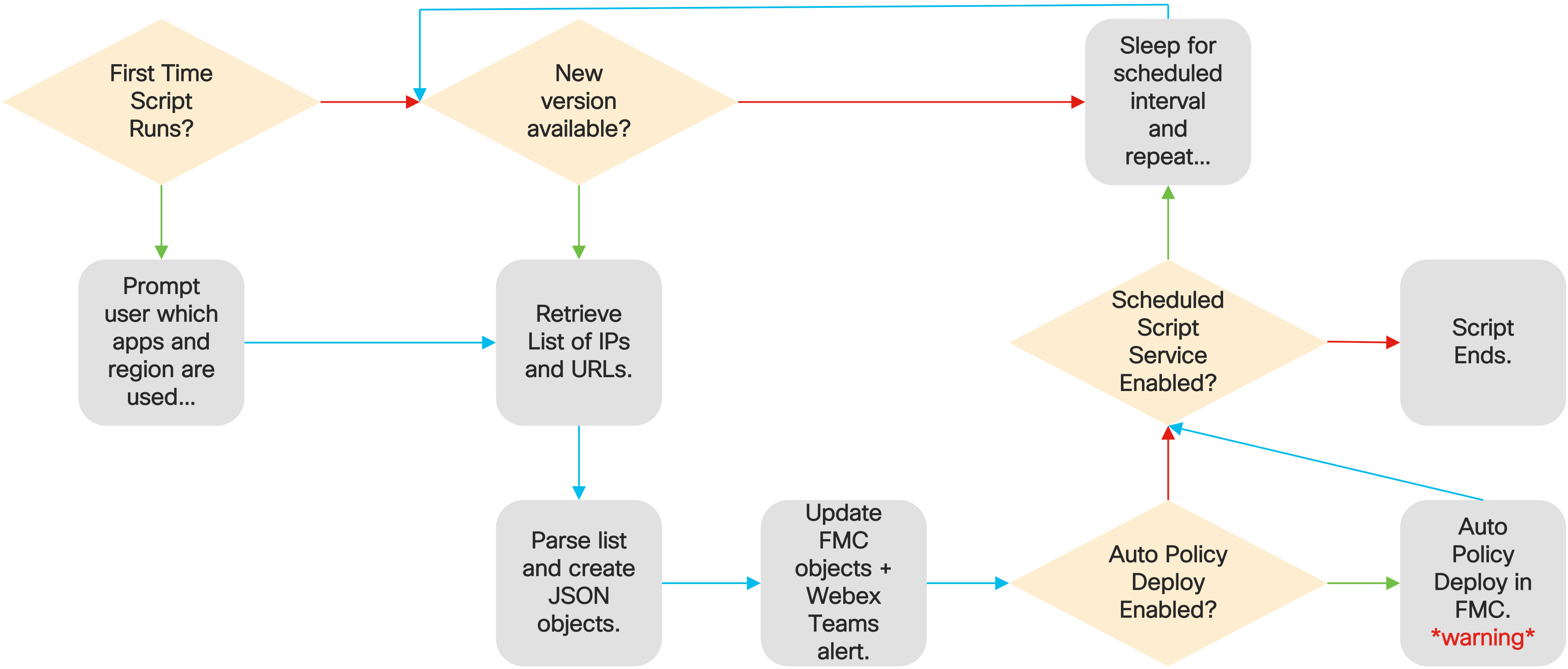
Manipulate objects

Change policy

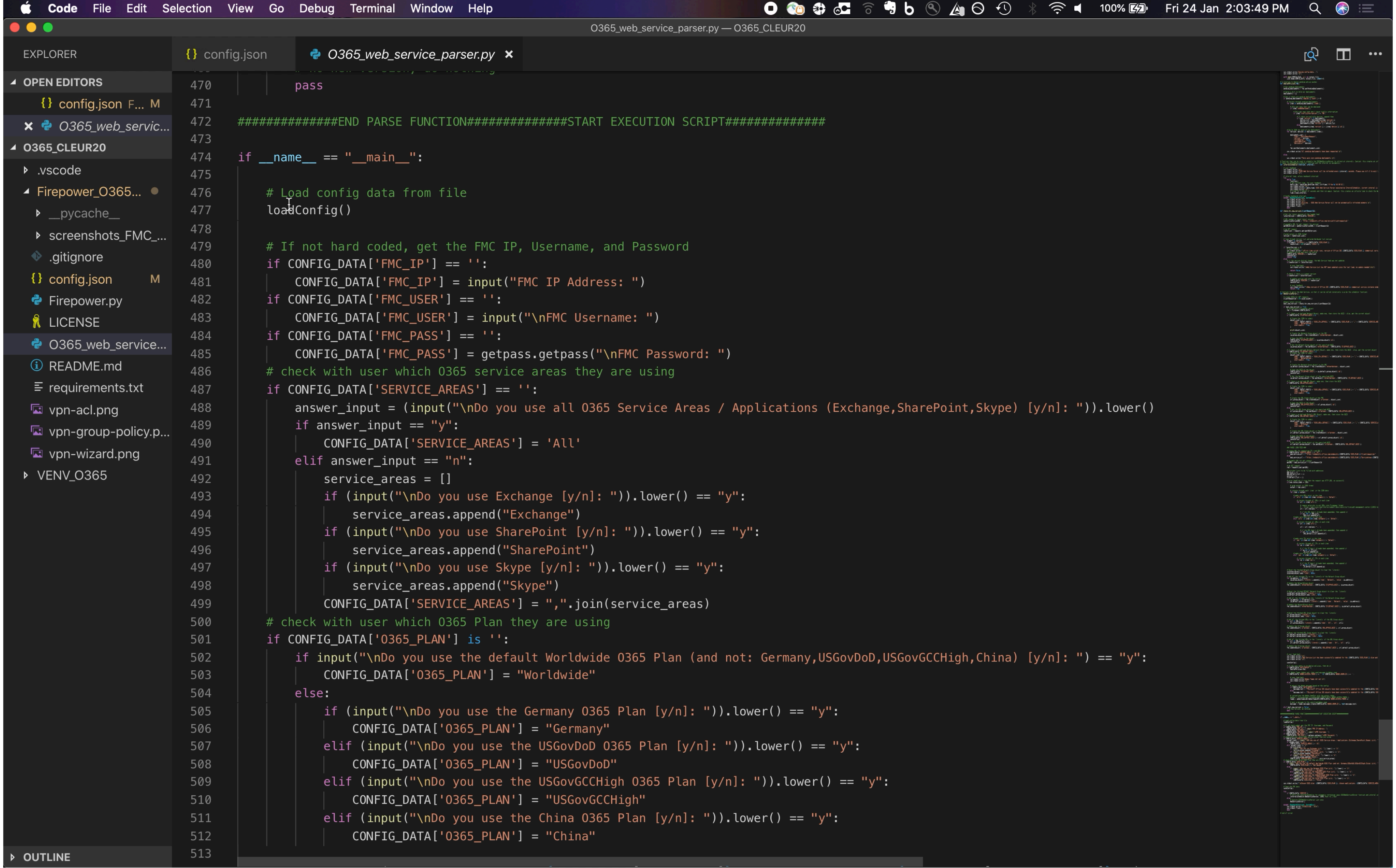
Deploy configuration

Flow of script

How to Automate the Update Process


First Time Script Runs?
New version available?
Sleep for scheduled interval and repeat…
Prompt user which apps and region are used…
Retrieve List of IPs and URLs.
Scheduled Script Service Enabled?
Script Ends.
Parse list and create JSON objects.
Update FMC objects + Webex Teams alert.
Auto Policy Deploy Enabled?
Auto Policy Deploy in FMC.
warning

Short demo...



```python
        pass

##############END PARSE FUNCTION##############START EXECUTION SCRIPT##############

if __name__ == "__main__":

    # Load config data from file
    loadConfig()

    # If not hard coded, get the FMC IP, Username, and Password
    if CONFIG_DATA['FMC_IP'] == '':
        CONFIG_DATA['FMC_IP'] = input("FMC IP Address: ")
    if CONFIG_DATA['FMC_USER'] == '':
        CONFIG_DATA['FMC_USER'] = input("\nFMC Username: ")
    if CONFIG_DATA['FMC_PASS'] == '':
        CONFIG_DATA['FMC_PASS'] = getpass.getpass("\nFMC Password: ")
    # check with user which O365 service areas they are using
    if CONFIG_DATA['SERVICE_AREAS'] == '':
        answer_input = (input("\nDo you use all O365 Service Areas / Applications (Exchange,SharePoint,Skype) [y/n]: ")).lower()
        if answer_input == "y":
            CONFIG_DATA['SERVICE_AREAS'] = 'All'
        elif answer_input == "n":
            service_areas = []
            if (input("\nDo you use Exchange [y/n]: ")).lower() == "y":
                service_areas.append("Exchange")
            if (input("\nDo you use SharePoint [y/n]: ")).lower() == "y":
                service_areas.append("SharePoint")
            if (input("\nDo you use Skype [y/n]: ")).lower() == "y":
                service_areas.append("Skype")
            CONFIG_DATA['SERVICE_AREAS'] = ",".join(service_areas)
    # check with user which O365 Plan they are using
    if CONFIG_DATA['O365_PLAN'] is '':
        if input("\nDo you use the default Worldwide O365 Plan (and not: Germany,USGovDoD,USGovGCCHigh,China) [y/n]: ") == "y":
            CONFIG_DATA['O365_PLAN'] = "Worldwide"
        else:
            if (input("\nDo you use the Germany O365 Plan [y/n]: ")).lower() == "y":
                CONFIG_DATA['O365_PLAN'] = "Germany"
            elif (input("\nDo you use the USGovDoD O365 Plan [y/n]: ")).lower() == "y":
                CONFIG_DATA['O365_PLAN'] = "USGovDoD"
            elif (input("\nDo you use the USGovGCCHigh O365 Plan [y/n]: ")).lower() == "y":
                CONFIG_DATA['O365_PLAN'] = "USGovGCCHigh"
            elif (input("\nDo you use the China O365 Plan [y/n]: ")).lower() == "y":
                CONFIG_DATA['O365_PLAN'] = "China"

```

Conclusion

Endless possibilities with the Firepower API!

- Augment firewall contextual data
- Automate firewall configuration
- Host discovery
- Manipulate objects
- Vulnerability analysis
- Change policy
- More accurate IPS recommendations
- Deploy configuration

Thank you

CISCO

Possibilities

#CiscoLive | #DevNetDay