End-to-End ASA to NGFW Migration

Migration Strategy and Best Practices

Ranil Fernando

Customer Success Specialist

BRKSEC-2639

This session is for you if:

- ✓ You have existing ASA Firewalls that you want to replace with Cisco FirePOWER

- ✓ You want to know about FTD architecture and where to start the migration process

- ✓ You want to understand how Cisco's migration solution works

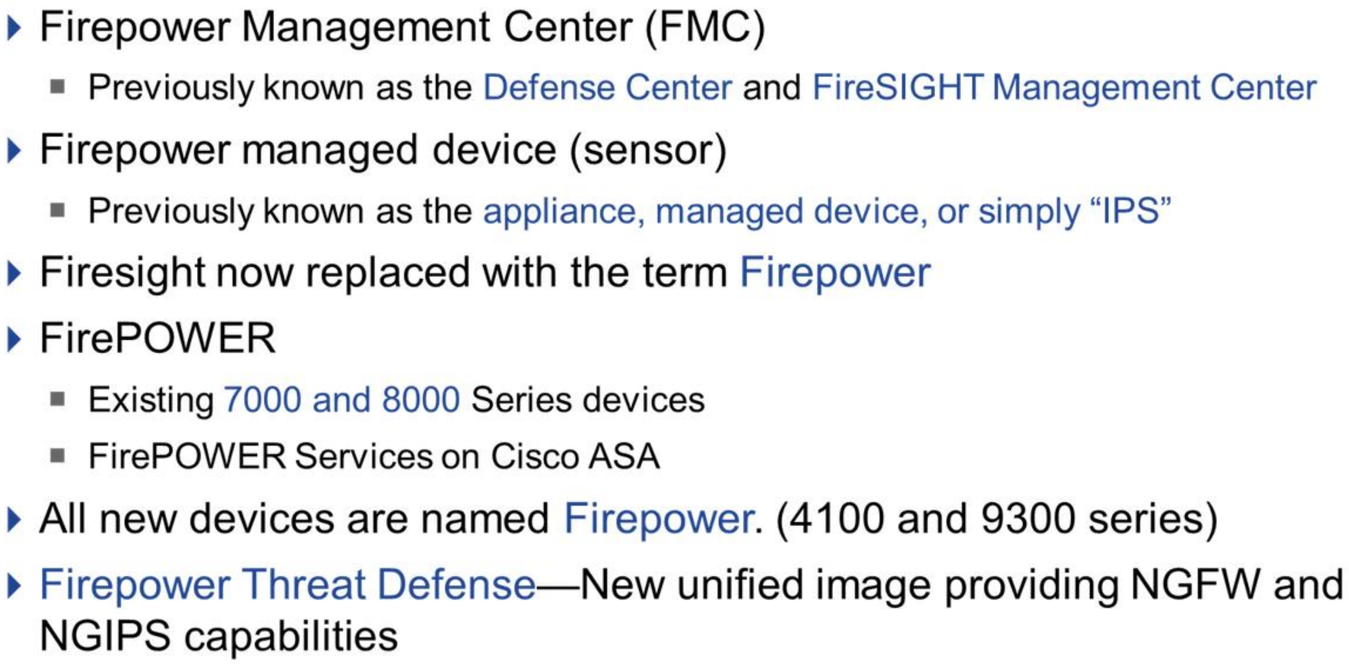
Agenda

- FirePOWER Architecture Overview
- Why Migrate
- Cisco FirePOWER Migration Tool (FMT)
- Migration Steps
- Customer Migration Scenario
- Best Practices & Troubleshooting
- DEMO

FirePOWER Architecture Overview

You make customer experience **possible**

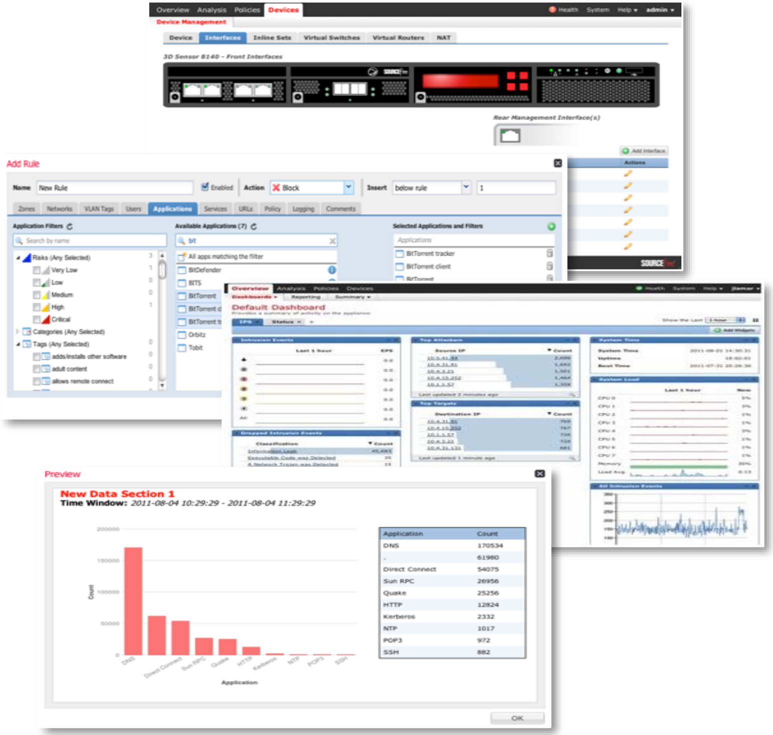
Firepower Product-Naming Progression



- Firepower Management Center (FMC)
  - Previously known as the Defense Center and FireSIGHT Management Center
- Firepower managed device (sensor)
  - Previously known as the appliance, managed device, or simply “IPS”
- Firesight now replaced with the term Firepower
- FirePOWER
  - Existing 7000 and 8000 Series devices
  - FirePOWER Services on Cisco ASA
- All new devices are named Firepower. (4100 and 9300 series)
- Firepower Threat Defense—New unified image providing NGFW and NGIPS capabilities

Firepower Management Center (FMC)

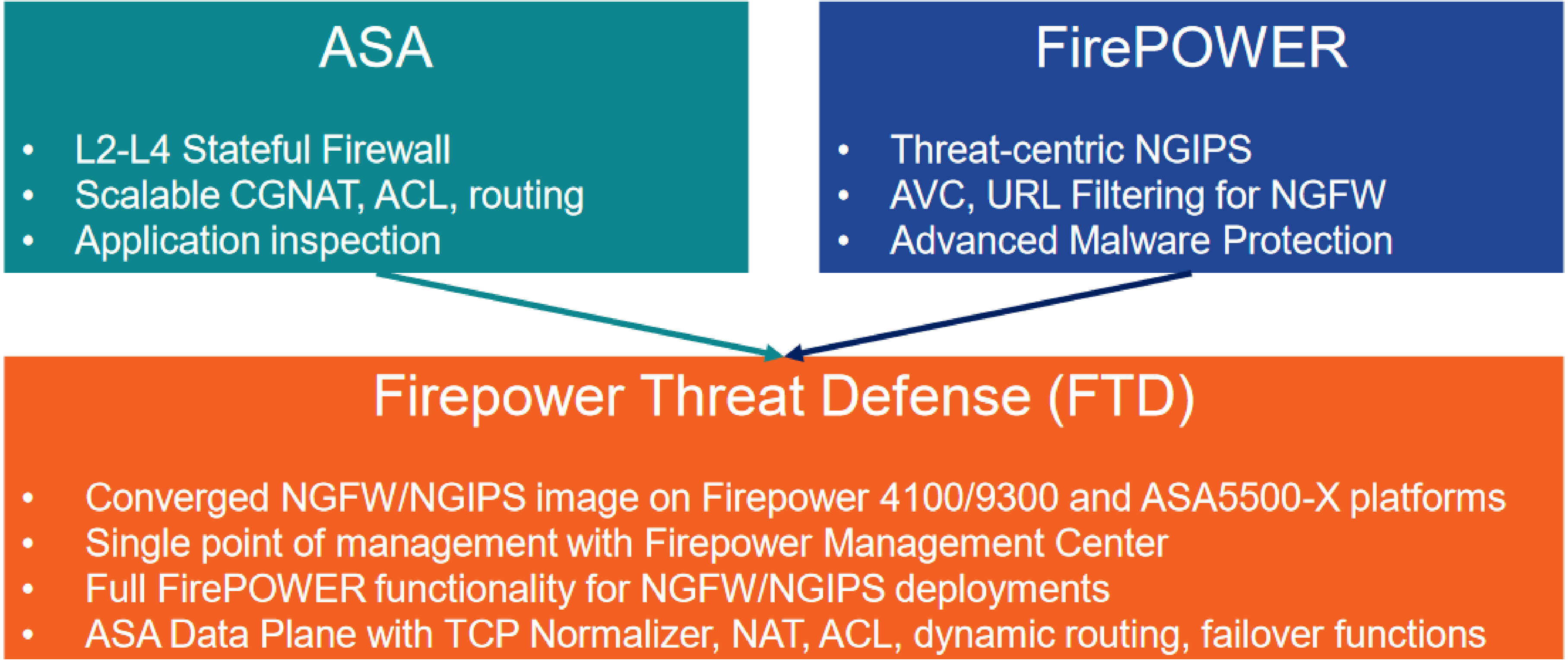
- Single console for event, policy, and configuration management
- Centralized analysis and management
- Customizable dashboard
- Comprehensive reports & alerts
- Centralized policy administration
- High availability
- Integrates with existing security



New Data Section 1
Time Window: 2011-08-04 10:29:29 - 2011-08-04 11:29:29

Application	Count
DNS	170534
-	61980
Direct Connect	54075
Sun RPC	26956
Quake	25256
HTTP	12824
Kerberos	2332
NTP	1017
POP3	972
SSH	882

Architecture of FTD Platform



ASA

- L2-L4 Stateful Firewall
- Scalable CGNAT, ACL, routing
- Application inspection

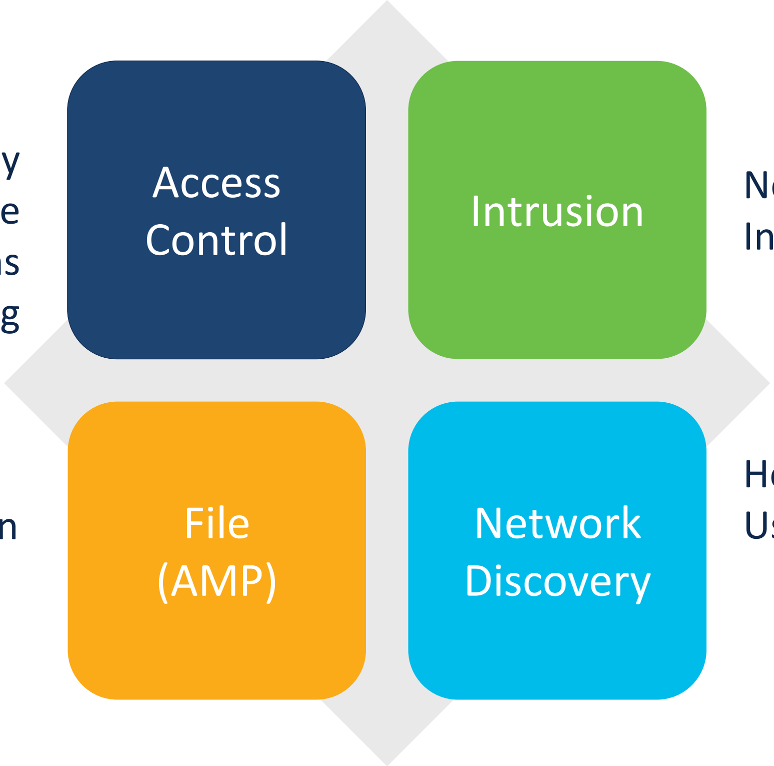
FirePOWER

- Threat-centric NGIPS
- AVC, URL Filtering for NGFW
- Advanced Malware Protection

Firepower Threat Defense (FTD)

- Converged NGFW/NGIPS image on Firepower 4100/9300 and ASA5500-X platforms
- Single point of management with Firepower Management Center
- Full FirePOWER functionality for NGFW/NGIPS deployments
- ASA Data Plane with TCP Normalizer, NAT, ACL, dynamic routing, failover functions

Advanced Security – Design Focused



Access Control

Intrusion

File (AMP)

Network Discovery

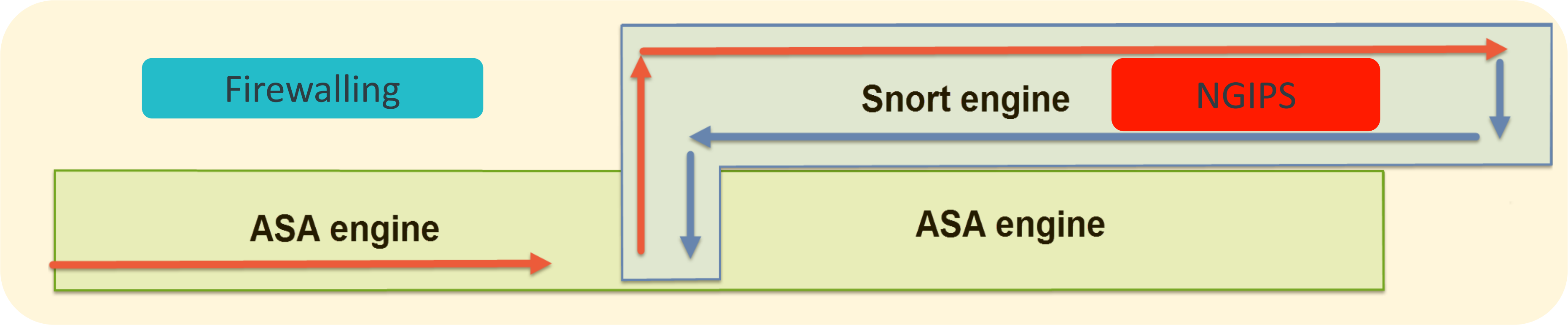
Firewall Capability
Security Intelligence
Applications
URL-Filtering

Network Analysis Policy
Intrusion Policy

Malware Inspection

Hosts, Applications, and Users

FTD Software Architecture



1. A packet enters the ingress interface and it is handled by the ASA engine
2. If the policy dictates so the packet is inspected by the Snort engine
3. Snort engine returns a verdict (whitelist or blacklist) for the packet
4. The ASA engine drops or forwards the packet based on Snort’s verdict

- Snort engine runs 6.x code
- ASA engine runs 9.6.x code

Threat Tornado – Design Focused

Prefilter

- Prefilter blocking
- Fast-path at layer 2-4

Basic Access Control

- Layer 1-4 Block
- Layer 1-4 Trust

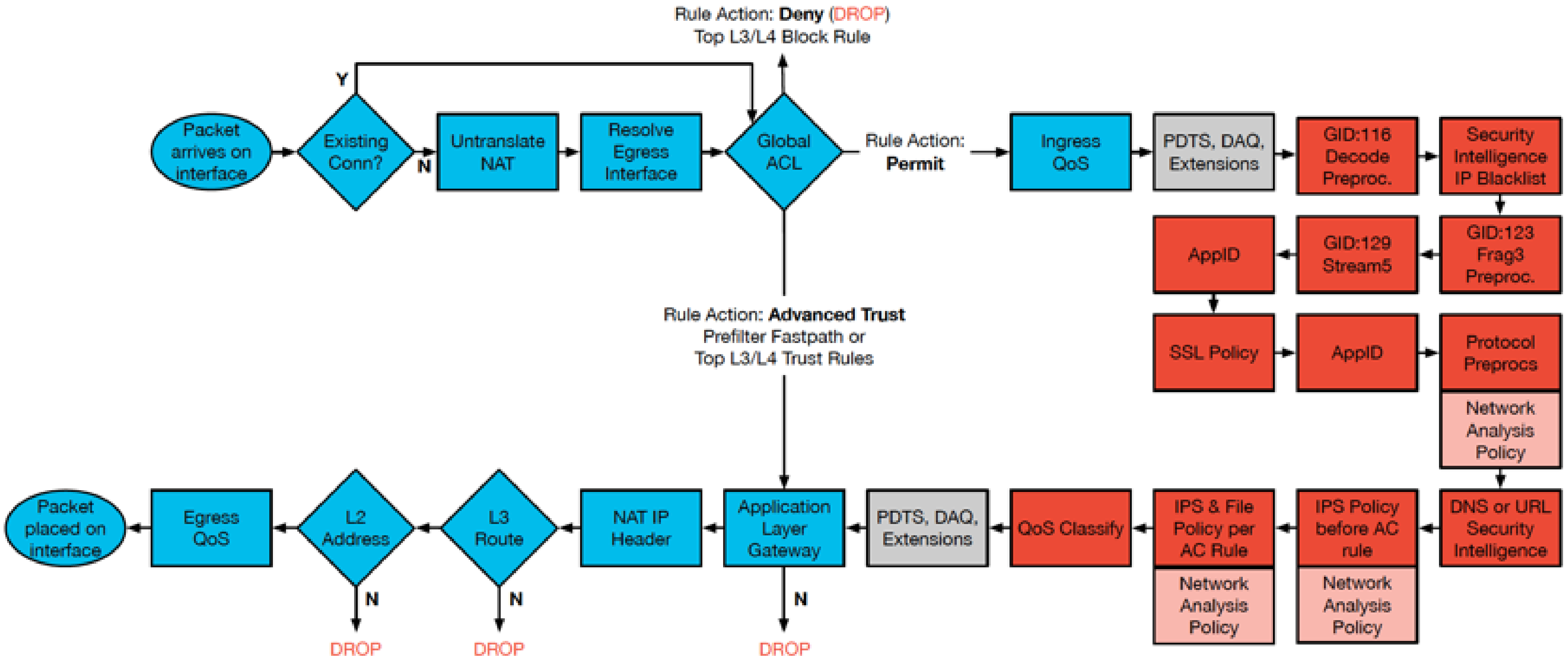
Access Control

- Layer 5 – 7 Block Rules
- Layer 5 – 7 Targeted Inspection and features

Generic Rules

- Generic inspection and features
- Default rule for non-matching traffic

FTD Packet Flow

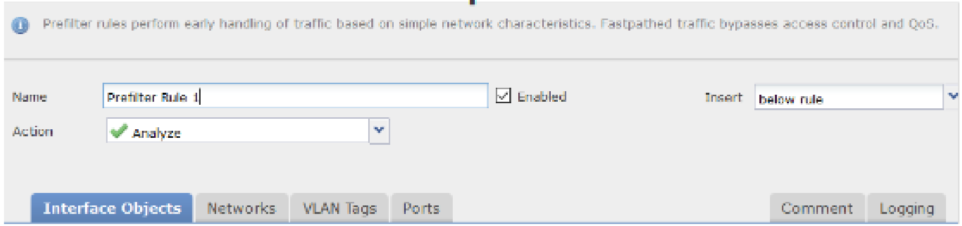


LINA ASA Engine = BLUE

Snort Engine = RED

Prefilter Policy

- First access control phase in Data Plane for each new flow
  - **Block**: Deny the flow without any further processing
  - **Fastpath**: Allow and process entirely in Data Plane, attempt Flow Offload
  - **Analyze**: Pass for evaluation in Main AP, optionally assign tunnel zone
- Not a “high performance” substitute to true NGFW policies
  - Non-NGFW traffic match criteria
  - Limited early IP blacklisting
  - Tunneled traffic inspection
  - Allowing high-bandwidth and low latency trusted flows (Flow Offload)



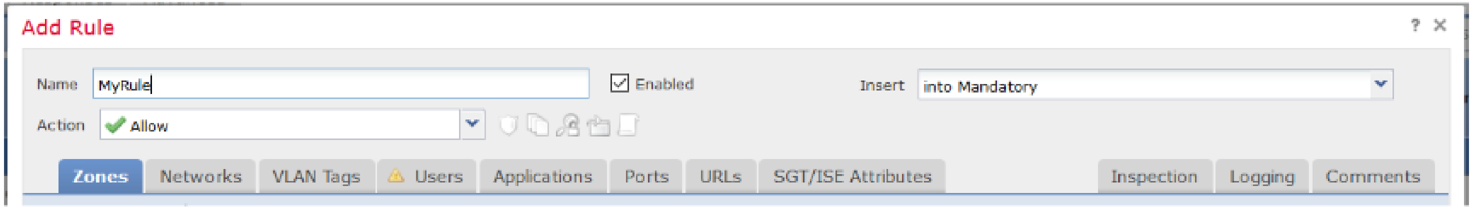
Prefilter rules perform early handling of traffic based on simple network characteristics. Fastpathed traffic bypasses access control and QoS.

Name: Prefilter Rule 1 ☑ Enabled Insert: below rule

Action: Analyze

Main Access Policy

- Second and final access control phase in Snort
  - **Block [with reset]**: Deny connection [and TCP RST]
  - **Interactive Block [with reset]**: Show HTTP(S) block page [and TCP RST]
  - **Monitor**: Log event and continue policy evaluation
  - **Trust**: Push all subsequent flow processing into Data Plane only
  - **Allow**: Permit connection to go through NGIPS/File inspection
- Appropriate place for implementing NGFW policy rules
  - Full NGFW traffic selection criteria



Add Rule

Name: MyRule

☑ Enabled

Insert: into Mandatory

Action: ✓ Allow

  - Decisions may need multiple packets

Why Migrate and Benefits

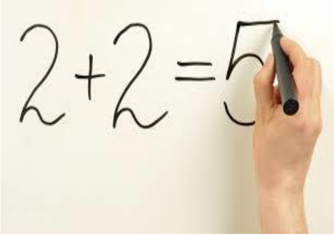
Why migrate?

Simply upgrading

Simplified management

Next-gen features

Why a Migration Tool is needed: The challenge



Benefit of Migration Tool

Derive faster value realization from Cisco's NGFW

Complementary to Partner driven services

Cisco Security Services

Our Security Services portfolio of people, tool, processes and technology helps you to do more, and many of our services are widely recognized by industry leaders and analysts as amongst the best capabilities in the market

Migration configuration validated by seasoned & skilled Security consultants

Provide you with design best practices based on Cisco's history of experience with variety of vertical industries

Provide support during migration to help mitigate risks during migration

Enhance your knowledge on Cisco's NGFW product features

Why is Cisco Firepower Migration Tool

Automation

- Easy and fast cloud based and stand-alone solutions
- Selective migration and optimizations such as object re-use
- Object conflict detection and resolution

Reporting

- Pre- and post-migration reports
- Ability to edit the configuration being migrated
- Live running logs, graceful error handling and resume from failure

Scale

- FMC REST API based, supports Windows or Mac
- CDO integration* to leverage orchestration benefits
- Programmability* through tool APIs

Migration Scenarios ASA to FirewPOWER Threat Defense (FTD)

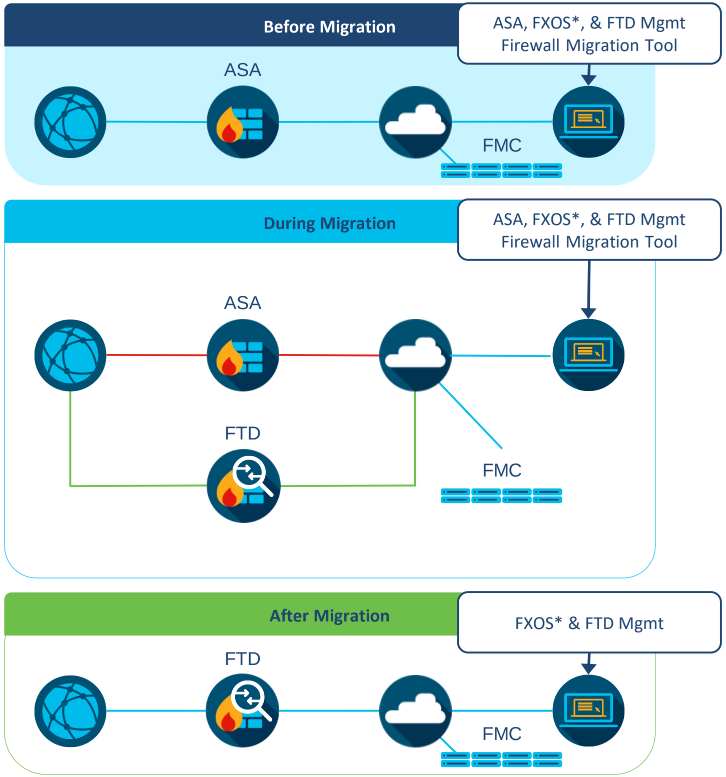
- Parallel System Install Method

Parallel System Install

- New platform introduced
- Configured and cabled parallel to production ASA
- Shorter outage window and rollback
- UAT, Migration and Rollback plans dependency

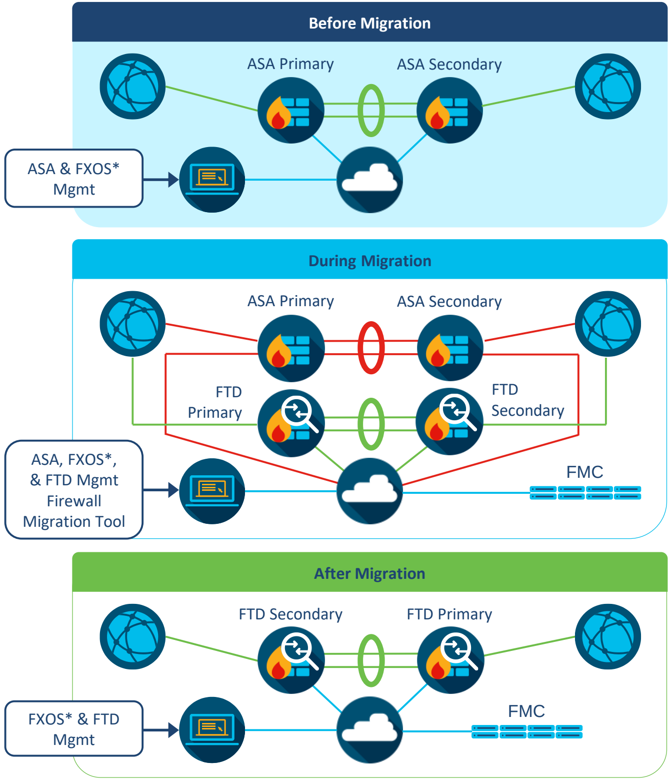
Adaptive Security Appliance (ASA) Standalone

Parallel System Install



Adaptive Security Appliance (ASA) High Availability

Parallel System Install



Cisco FirePOWER migration tool

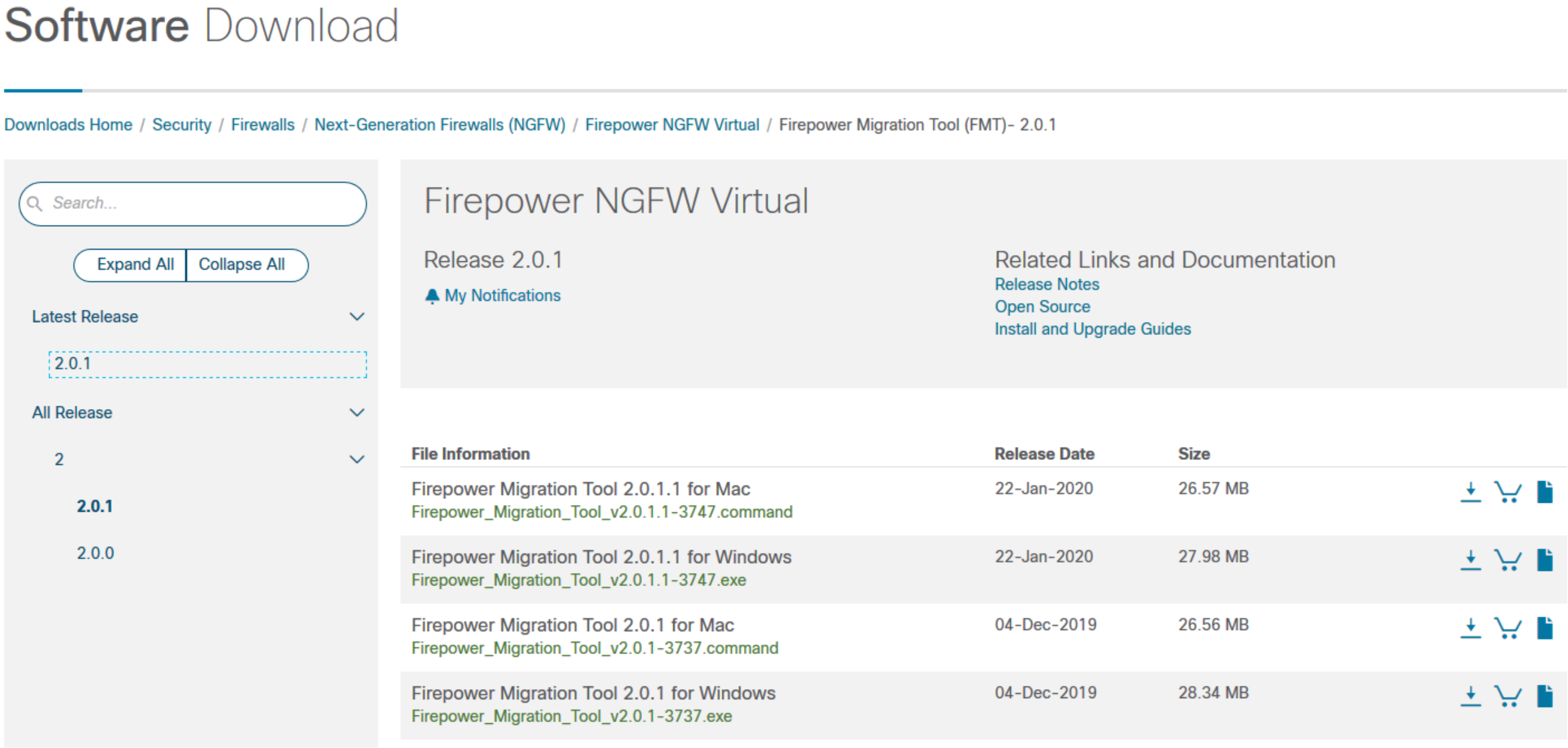
You make networking **possible**

History of FMT Versions

Versions
2.0
1.3
1.2
1.1
1.0

Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/migration-tool/migration-guide/ASA2FTD-with-FP-Migration-Tool/b_Migration_Guide_ASA2FTD_chapter_00.html

FMT Software Download



Software Download

Downloads Home / Security / Firewalls / Next-Generation Firewalls (NGFW) / Firepower NGFW Virtual / Firepower Migration Tool (FMT)- 2.0.1

Firepower NGFW Virtual

Release 2.0.1

My Notifications

Related Links and Documentation

Release Notes

Open Source

Install and Upgrade Guides

File Information	Release Date	Size
Firepower Migration Tool 2.0.1.1 for Mac Firepower_Migration_Tool_v2.0.1.1-3747.command	22-Jan-2020	26.57 MB
Firepower Migration Tool 2.0.1.1 for Windows Firepower_Migration_Tool_v2.0.1.1-3747.exe	22-Jan-2020	27.98 MB
Firepower Migration Tool 2.0.1 for Mac Firepower_Migration_Tool_v2.0.1-3737.command	04-Dec-2019	26.56 MB
Firepower Migration Tool 2.0.1 for Windows Firepower_Migration_Tool_v2.0.1-3737.exe	04-Dec-2019	28.34 MB

* The FMT application is free and does not require license

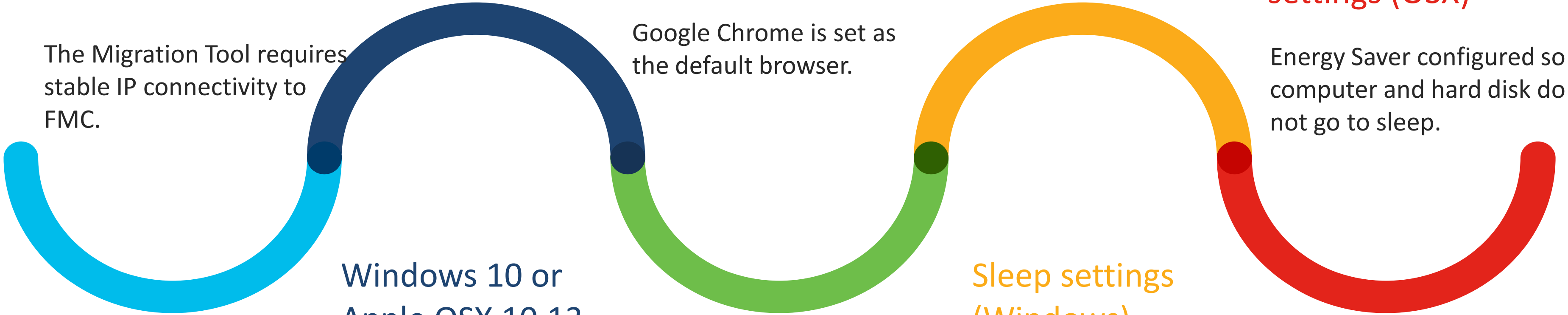
Feature support

What can be migrated:

- ✓ Access Control Rules
- ✓ Network Address Translation Policy
- ✓ Network and Port Objects
- ✓ Interface Configuration
- ✓ Static Routes

Prerequisites, Requirements and supported platforms

Platform requirements for migration tool



Stable connectivity

The Migration Tool requires stable IP connectivity to FMC.

Windows 10 or Apple OSX 10.13

These are OS minimums.

Google Chrome

Google Chrome is set as the default browser.

Sleep settings (Windows)

Power & Sleep set to ‘Never put the PC to Sleep’.

Energy Saver settings (OSX)

Energy Saver configured so computer and hard disk do not go to sleep.

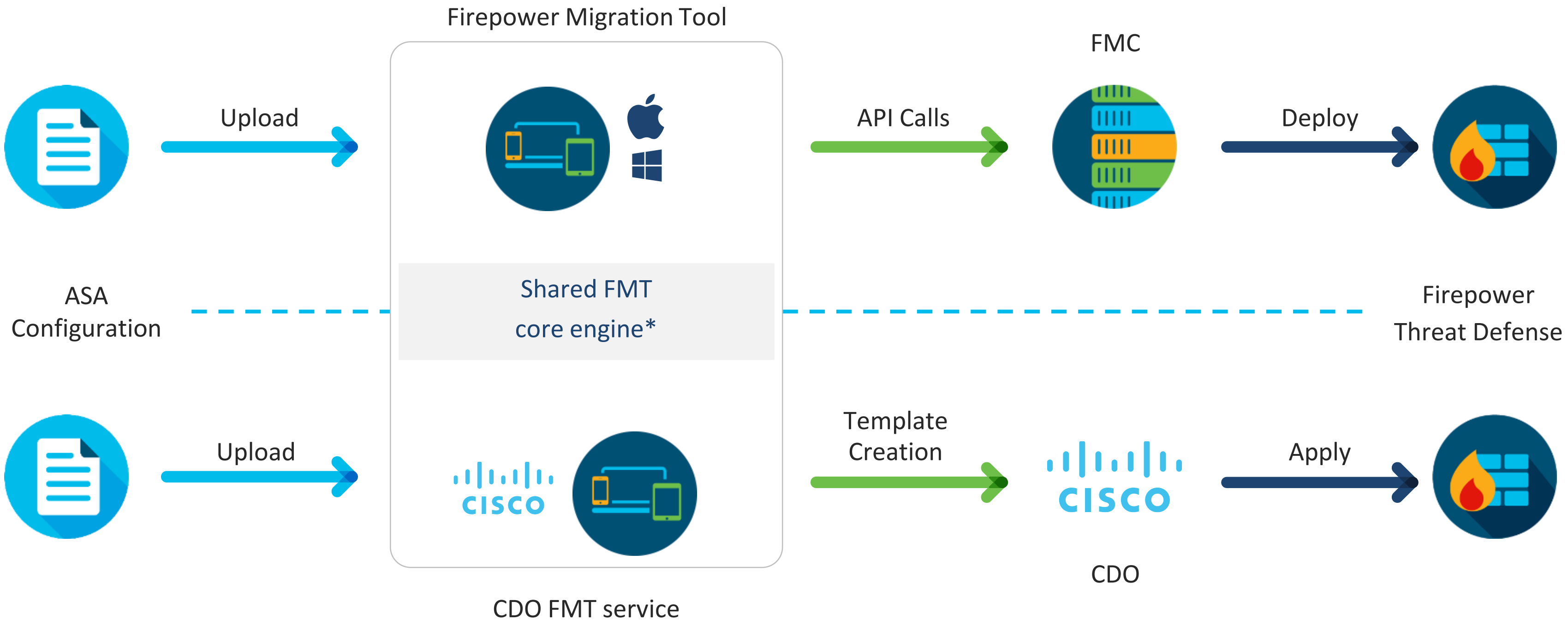
Supported software and hardware platform

Supported FMC Version	Managed Devices	Supported ASA Version	Notes
6.2.3 and later	✓ Any platform capable of running the FTD code	8.4 and later	✗ ASA 5505 not supported

⚠ Migration tool does not migrate the configuration from the ASA FirePOWER module

✚ FDM support in future release

Firepower Migration Tool Paths (ASA to FTD)



*features shared in CDO depend on FTD-API and CDO support

Firepower Migration Tool Options

	FMT Desktop	FMT in CDO
FMT Client	Windows10 or Mac Chrome Browser No Internet Connectivity Required	CDO-Compatible Browser Internet Connectivity
FMT Authentication	Local or Cisco ID	CDO ID
Firepower Version	FP 6.2.3.0 ..FP 6.5	FP 6.4.0.x
FTD Manager	FMC	CDO (FDM)
ASA 8.4+ to FTD	Yes	Yes
Migration Target	Push to FMC for later deploy to FTD	Push to Live CDO managed FTD or create template in CDO for reuse
Reporting	Yes	Yes

Manual ASA configuration file requirements

Uploaded configuration requirements:

✓ Must include the version number

✓ Must be from an ASA in single mode configuration or specific context of a multiple context mode configuration

✓ Must have file extension as .cfg or .txt

✓ Must use a file encoding of UTF-8

✗ Cannot contain the "--More--" keyword as text

✗ Cannot contain syntax errors

ASA Requirements → **ASA Config Limitations** → FMC Requirements

ASA configuration file limitations

- ⚠ ASA enable password **cannot be blank**
- ⚠ Does not support migration of a single ACL policy applied to over 50 interfaces
- ⚠ Some ASA policies, such as dynamic routing and VPN cannot be migrated with the tool
- ⚠ ASA devices in routed mode with a bridge virtual interface, redundant interface or tunneled interface
- ⚠ Cannot migrate IPv6 objects and rules

ASA Requirements → ASA Config Limitations → FMC Requirements

Requirements for FMC

- ✓ Version 6.2.3 +
- ✓ The target platform (FTD) is registered to the FMC
- ✓ Smart licenses obtained and installed
- ✓ REST API enabled on the FMC
- ✓ Sufficient user privileges to make REST API calls to the FMC
- ✗ No changes should be performed on the FMC during configuration push phase

Migration Steps and Workflow

You make the power of data **possible**

Firewall Migration Strategy

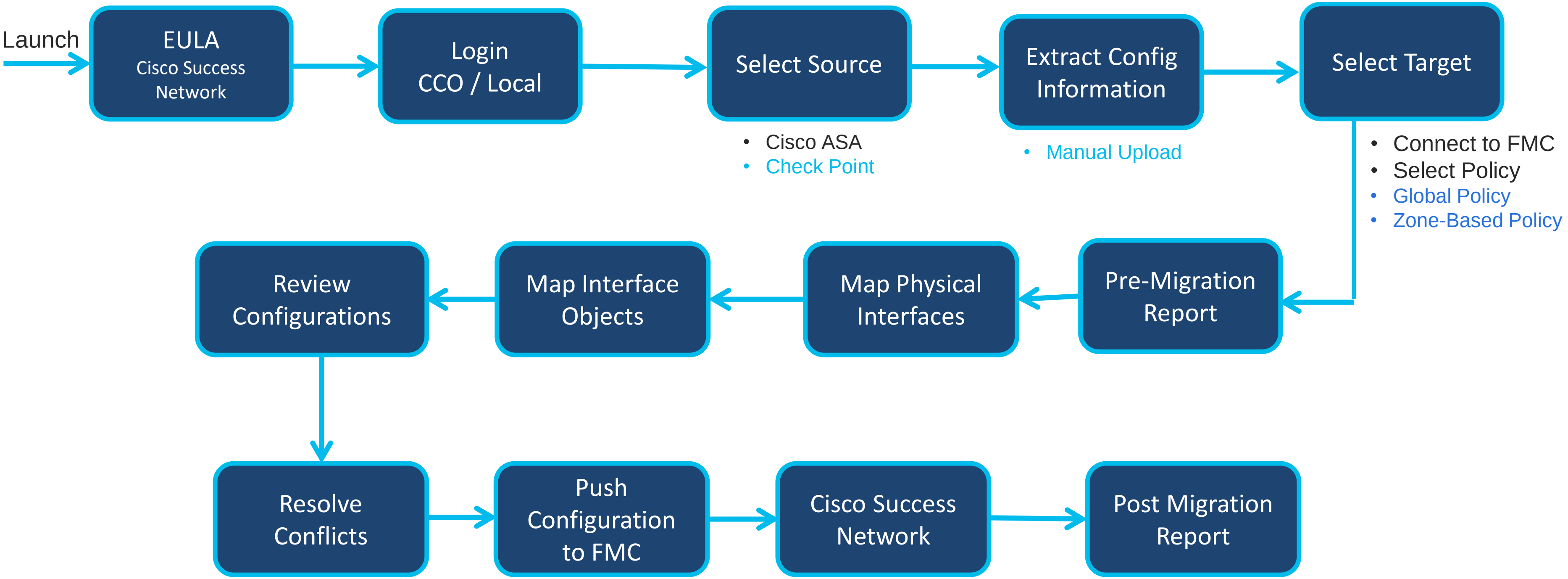
Days 0 – 5	Days 6 - 8	Days 9 - 11	Days 11- 13	Days 14-15
Discovery	Strategy	Execution	Support	TOKTEN
An assessment of your requirements and current configurations.	Conduct a review to finalize the migration design strategy and procedure, including testing, rollback, failure recovery, and risk mitigation	Execute the steps outlined in the migration and testing procedure plan and document results.	Review any outstanding technical issues related to application migration.	Provide Knowledge dump using best practices, what has been done.

Conversation Reports

- **Pre-Migration Report**
  - Feature Statistics of Source Configuration – ASA or CP.
  - Details on supported, partially supported and unsupported configuration.

- **Post-Migration Report**
  - Feature Statistics of migrated elements from ASA or CP configuration.
  - Any actions (Advanced Capabilities of FMT) taken during the course of conversion.
  - Details around migrated elements which are converted partially.

Firepower Migration Tool Workflow



- Cisco ASA
- Check Point

- Manual Upload

- Connect to FMC
- Select Policy
- Global Policy
- Zone-Based Policy

Logs and Other File Locations

File	Location
Log file	<*migration_tool_folder*>\logs
Pre-migration report	<*migration_tool_folder*>\resources
Post-migration report	<*migration_tool_folder*>\resources
unparsed file	<*migration_tool_folder*>\resources

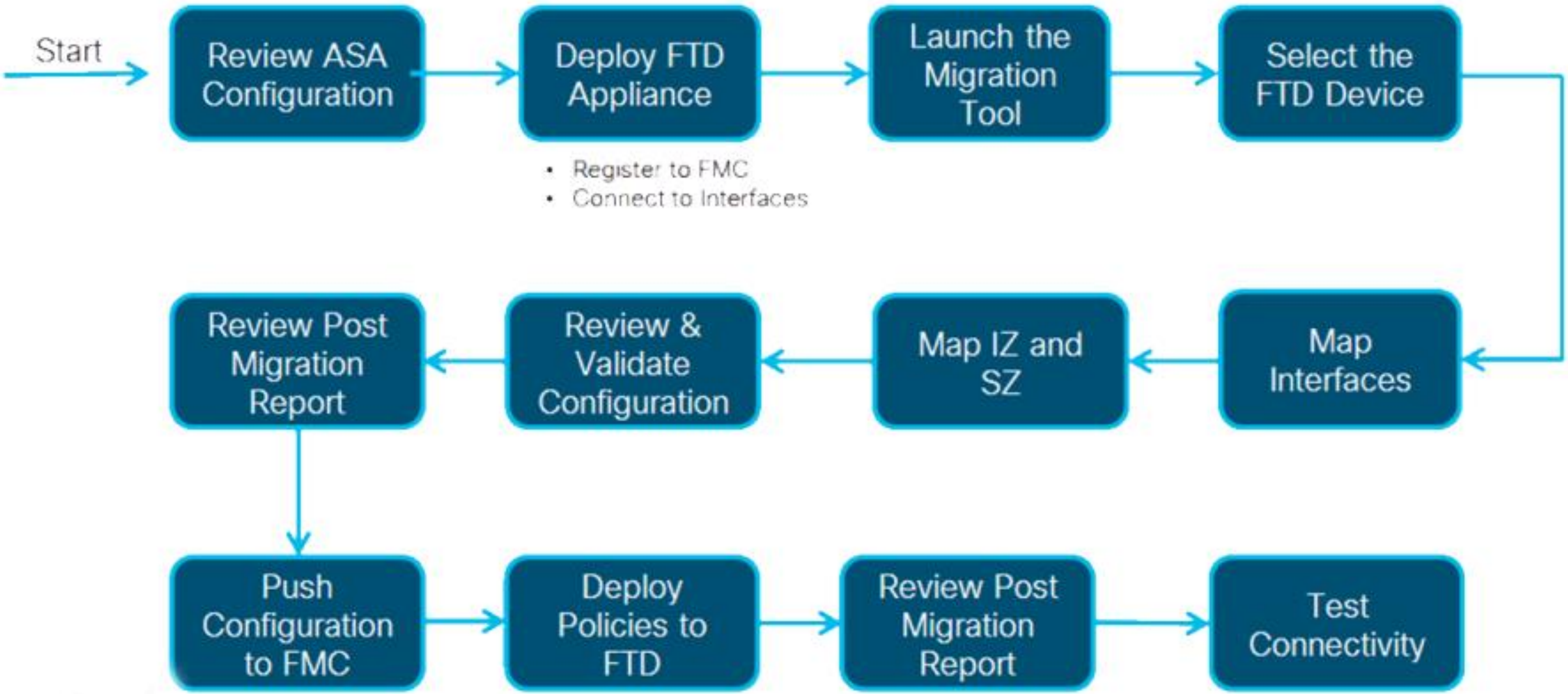
Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/migration-tool/migration-guide/ASA2FTD-with-FP-Migration-Tool/b_Migration_Guide_ASA2FTD_chapter_01110.html

Migration Tasks

You make customer experience **possible**

Migration Tasks

Task’s to be performed prior and post Migration to an FTD appliance



Start

Review ASA Configuration

Deploy FTD Appliance

- Register to FMC
- Connect to Interfaces

Launch the Migration Tool

Select the FTD Device

Map Interfaces

Map IZ and SZ

Review & Validate Configuration

Review Post Migration Report

Push Configuration to FMC

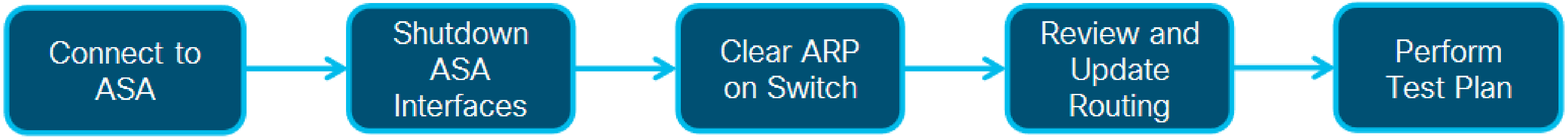
Deploy Policies to FTD

Review Post Migration Report

Test Connectivity

Migration Tasks – During Migration

Task's to be performed during Migrating to an FTD appliance



Connect to ASA → Shutdown ASA Interfaces → Clear ARP on Switch → Review and Update Routing → Perform Test Plan

Best Practices & Troubleshooting

You make multi-cloud **possible**

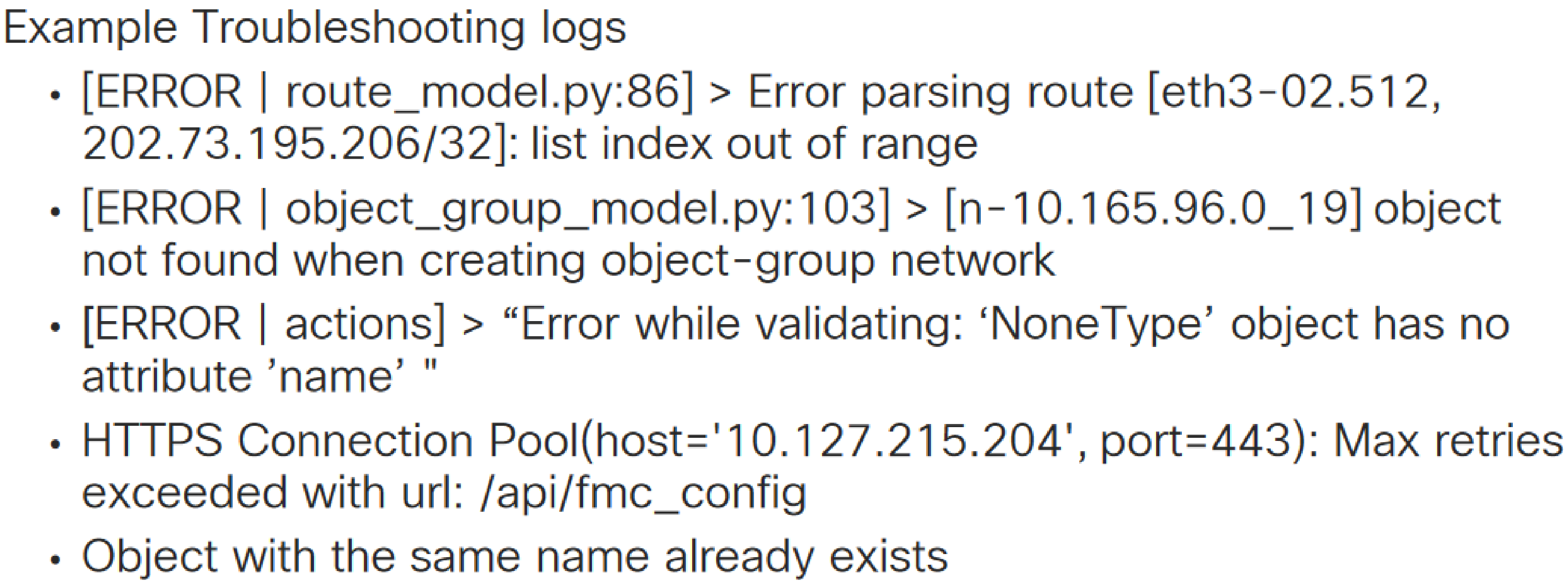
FMT Best Practices and Guidelines

Below is the high level list of steps to be considered during migration.

- Prior to Migration, Take the Show-Tech Output from ASA CLI and Save it as .txt or .cfg file
- Review the ASA configuration and do not use any Hand-Coded Config's.
- Download and Run the latest migration tool.
- Review the FMT pre-migration checklist.
- Create Separate user account on FMC for FMT tool usage with admin access.
- Map the interfaces and follow the on screen steps to review and validate config.
- Review the post migration report.
- Deploy the policies on FMC.

Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/migration-tool/migration-guide/ASA2FTD-with-FP-Migration-Tool/b_Migration_Guide_ASA2FTD_chapter_0111.html

Error Messages and Troubleshooting



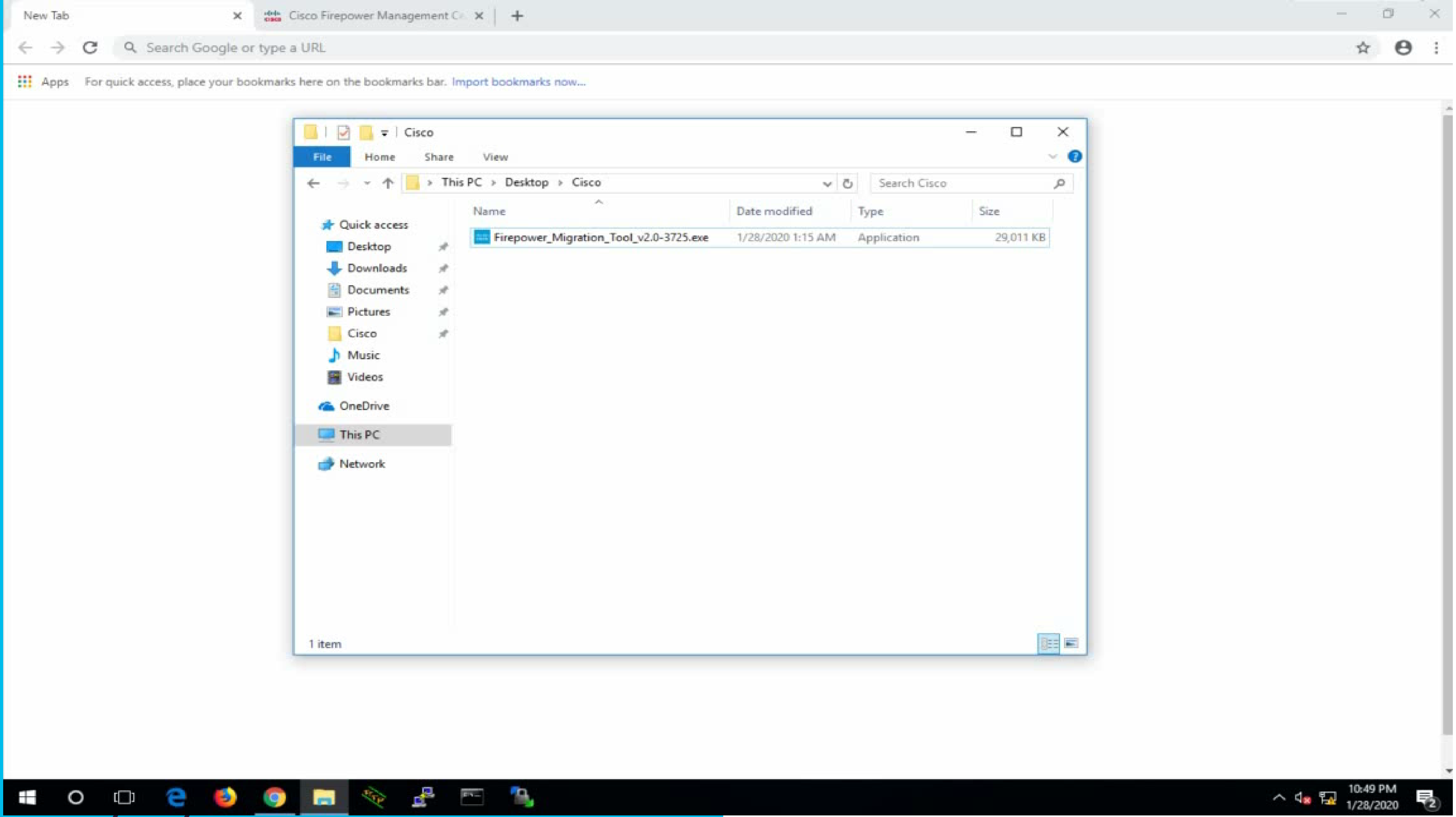
Example Troubleshooting logs

- [ERROR | route_model.py:86] > Error parsing route [eth3-02.512, 202.73.195.206/32]: list index out of range
- [ERROR | object_group_model.py:103] > [n-10.165.96.0_19] object not found when creating object-group network
- [ERROR | actions] > “Error while validating: ‘NoneType’ object has no attribute ’name’ "
- HTTPS Connection Pool(host='10.127.215.204', port=443): Max retries exceeded with url: /api/fmc_config
- Object with the same name already exists

Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/migration-tool/migration-guide/ASA2FTD-with-FP-Migration-Tool/b_Migration_Guide_ASA2FTD_chapter_01110.html

Demo

1. Extract info from the ASA configuration file
2. Select FTD target
3. Map FTD interfaces
4. Map zones and interface groups
5. Review and validate the configuration
6. Complete the migration



New Tab
Cisco Firepower Management C
Search Google or type a URL
Apps
For quick access, place your bookmarks here on the bookmarks bar. Import bookmarks now...
Cisco
File
Home
Share
View
This PC > Desktop > Cisco
Search Cisco
Quick access
Desktop
Downloads
Documents
Pictures
Cisco
Music
Videos
OneDrive
This PC
Network
1 item
10:49 PM
1/28/2020

Name	Date modified	Type	Size
Firepower_Migration_Tool_v2.0-3725.exe	1/28/2020 1:15 AM	Application	29,011 KB

Thank you

You make **possible**

#CiscoLiveAPJC