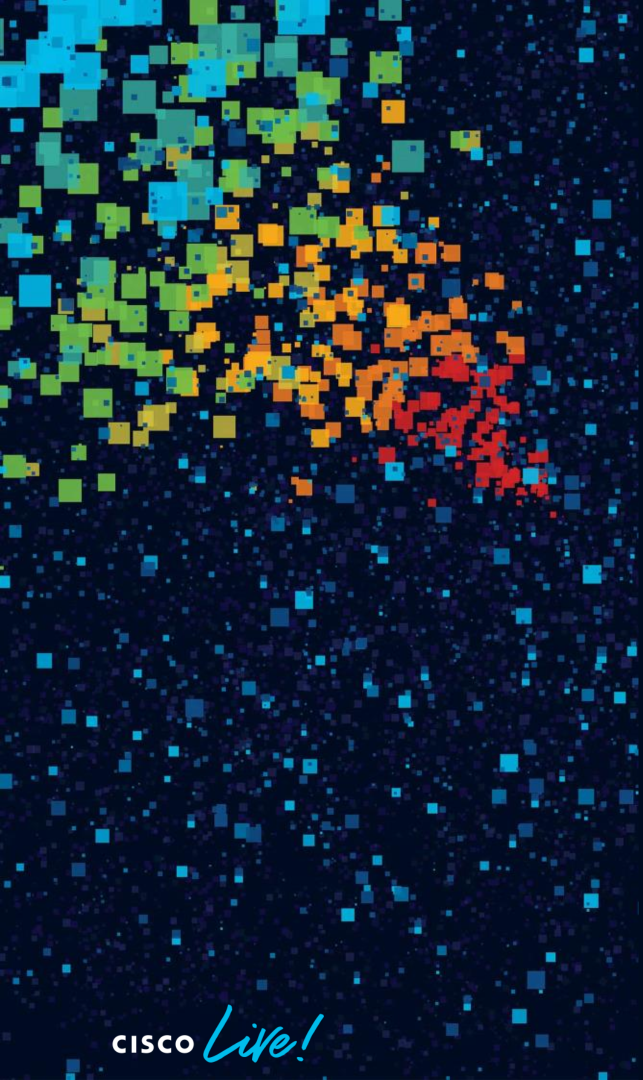
Possibilities

#CiscoLive

Deep Dive- Firepower Migration Tool

ADITYA GANJOO
Technical Marketing Engineer

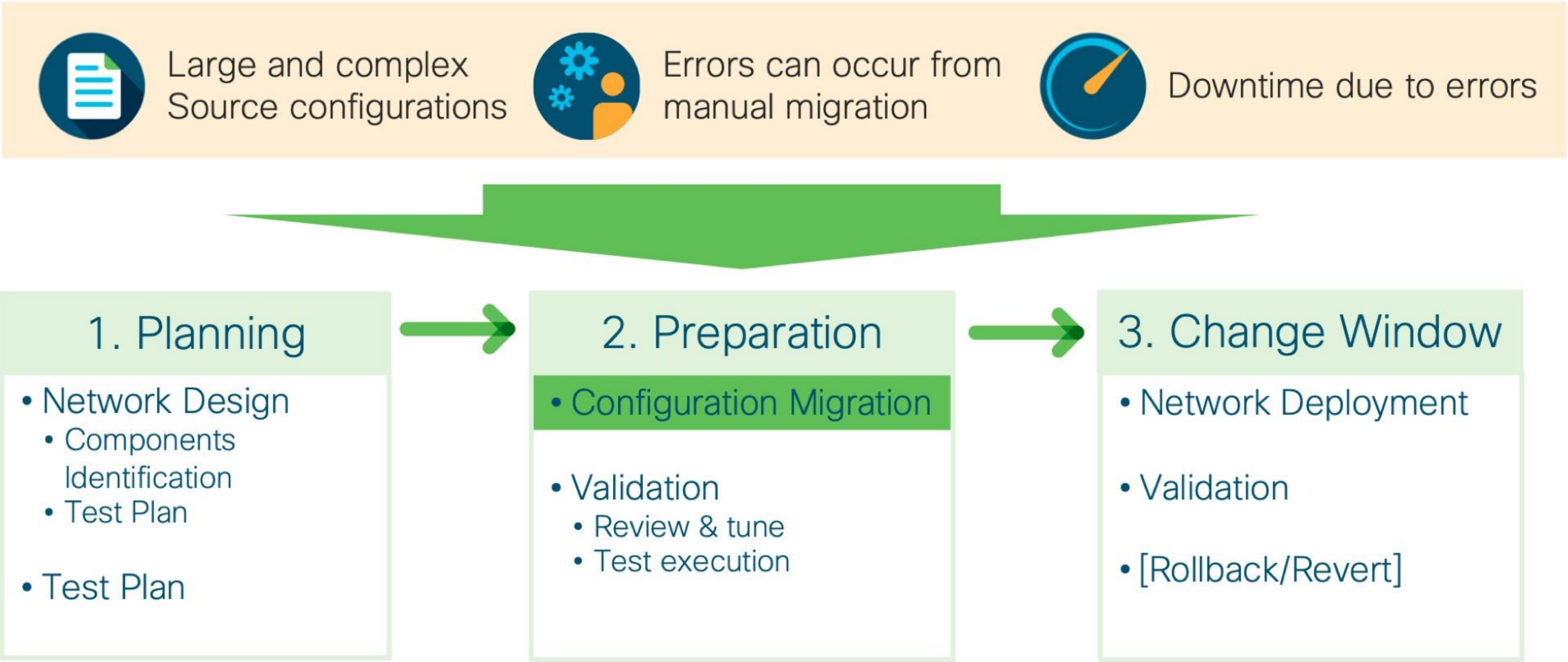
DGTL-BRKSEC-2101



Agenda

- Why Migration Tool?
- Supported Platforms
- What’s new (Roadmap)
- Best Practices
- Support and Troubleshooting
- Demo

Manual Migration is Complex



Large and complex Source configurations

Errors can occur from manual migration

Downtime due to errors

1. Planning

- Network Design
  - Components Identification
  - Test Plan
- Test Plan

2. Preparation

- Configuration Migration
- Validation
  - Review & tune
  - Test execution

3. Change Window

- Network Deployment
- Validation
- [Rollback/Revert]

Why Migration Tool?

Reporting

- Pre- and Post- Migration reports
- Ability to edit the configuration being migrated
- Live running logs, graceful error handling and resume from failure
- Object conflict detection and resolution

Automation

- ACL, NAT, Object, Interface, FQDN migration
- App DB support
- Multi Context to Multi Instance
- Selective migration and optimizations such as object re-use
- Auto-mapping of interfaces

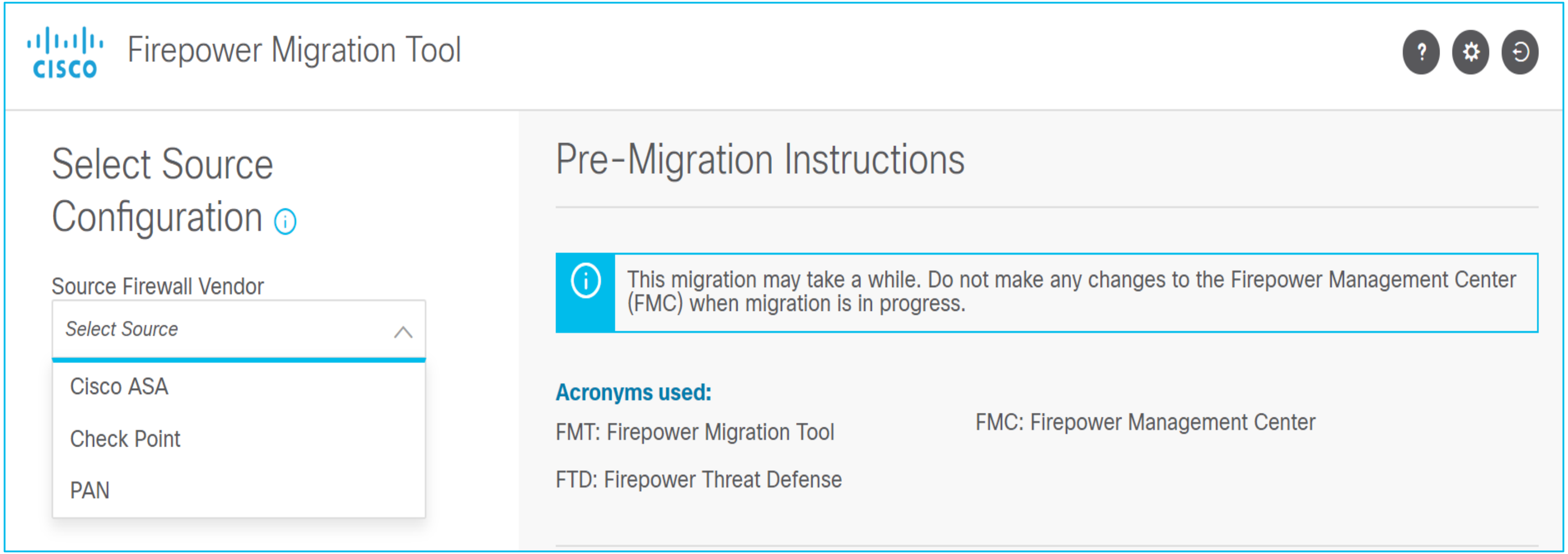
Scale

- Supports migration of features supported in FMC REST API
- Runs on Windows or Mac through Chrome browser
- CDO integration* to leverage orchestration benefits
- Programmability* through tool APIs

Supported Firewalls

- ASA
- Checkpoint
- Palo Alto Networks
- Fortinet* (Rule Book)

Supported Firewalls



Select Source Configuration

Source Firewall Vendor

Select Source

- Cisco ASA
- Check Point
- PAN

Pre-Migration Instructions

This migration may take a while. Do not make any changes to the Firepower Management Center (FMC) when migration is in progress.

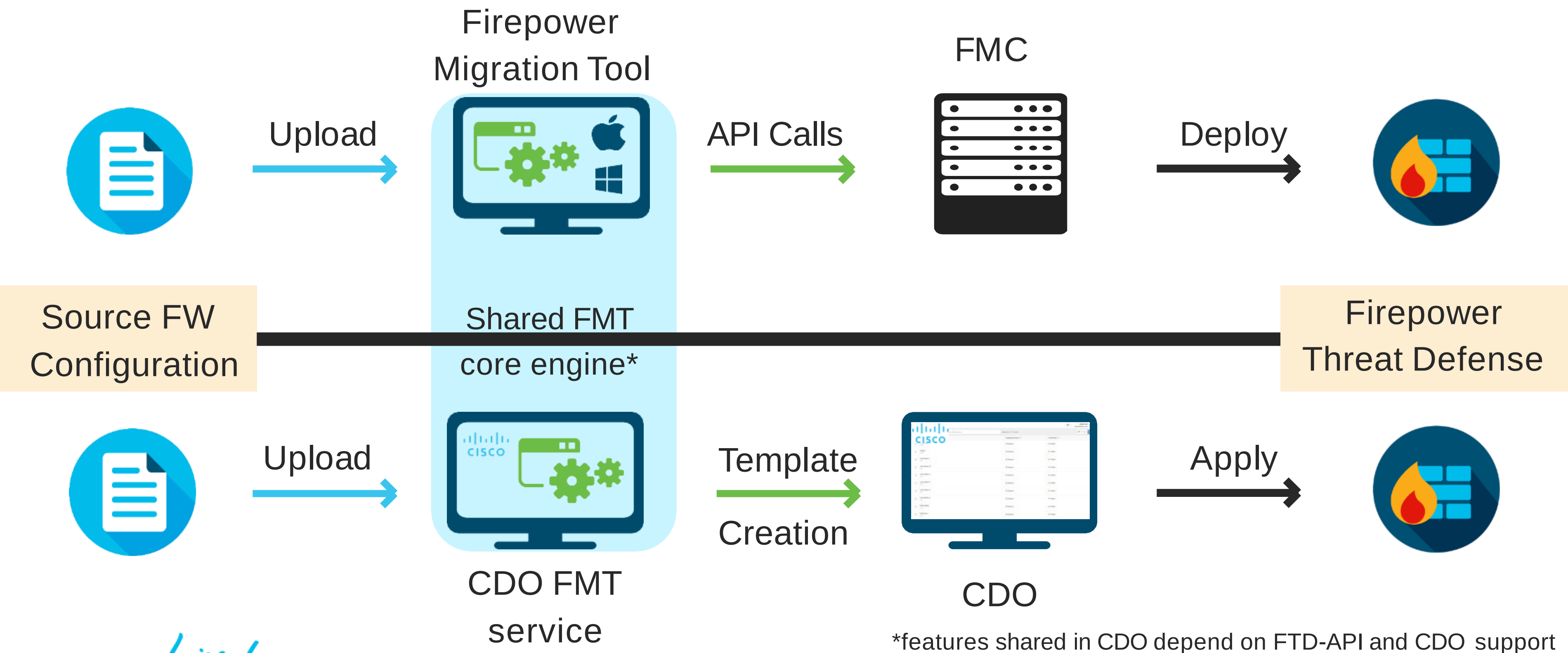
Acronyms used:

FMT: Firepower Migration Tool

FTD: Firepower Threat Defense

FMC: Firepower Management Center

Deployment Model



Firepower Migration Tool

FMC

Upload

API Calls

Deploy

Source FW Configuration

Shared FMT core engine*

Firepower Threat Defense

Upload

Template Creation

Apply

CDO FMT service

CDO

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

Roadmap & What’s New

CY19

Key Features

- Migrations in CDO
- Migrations from CP (r75-r77) to FTD

Usability

- Parsing & UI performance enhancements
- CSV download of review & validate tables
- Selective migration of ACL, NAT, object reuse

CY20*

Key Features

- Further 3rd party migrations (PAN, Fortinet,…)
- Version 2.1 released (PAN support)
- FMC to CDO migration

Usability

- Integration with Services
- Migration Versatility
- Layer 3 to Layer 7 mapping

Continued Support for:

- Multi-Context to Multi-Instance
- Enablement of L7 Firewalling capabilities
- Network, Service & FQDN objects and groups
- Access rules, CSM object grouping
- NAT, Static routes, IPv6
- Physical interface, port channels
- Bridge groups (transparent mode only)

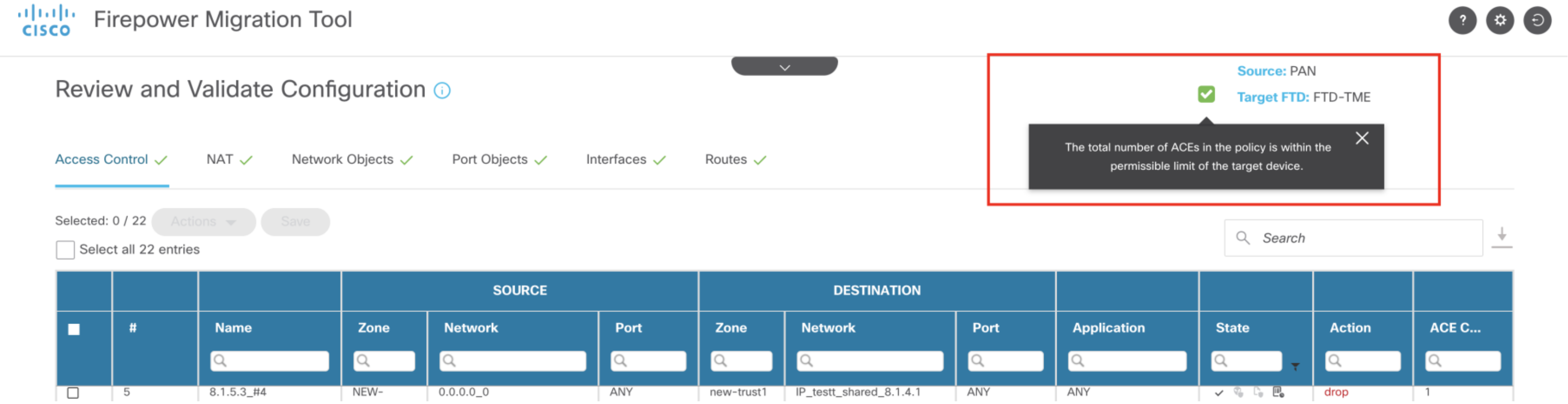
Support and Logs

Our goal is to make FMT user friendly and easier to troubleshoot issues

- Key-information right where you need it
- Link to detailed documentation
- Enhanced report storage in sub-folders
- Support Bundle to download logs, DB and configuration
- Telemetry improvements

Support and Logs

- ACE Platform Limit Warning



Review and Validate Configuration

Source: PAN

Target FTD: FTD-TME

The total number of ACEs in the policy is within the permissible limit of the target device.

Access Control ✓ | NAT ✓ | Network Objects ✓ | Port Objects ✓ | Interfaces ✓ | Routes ✓
Actions
Save
Search

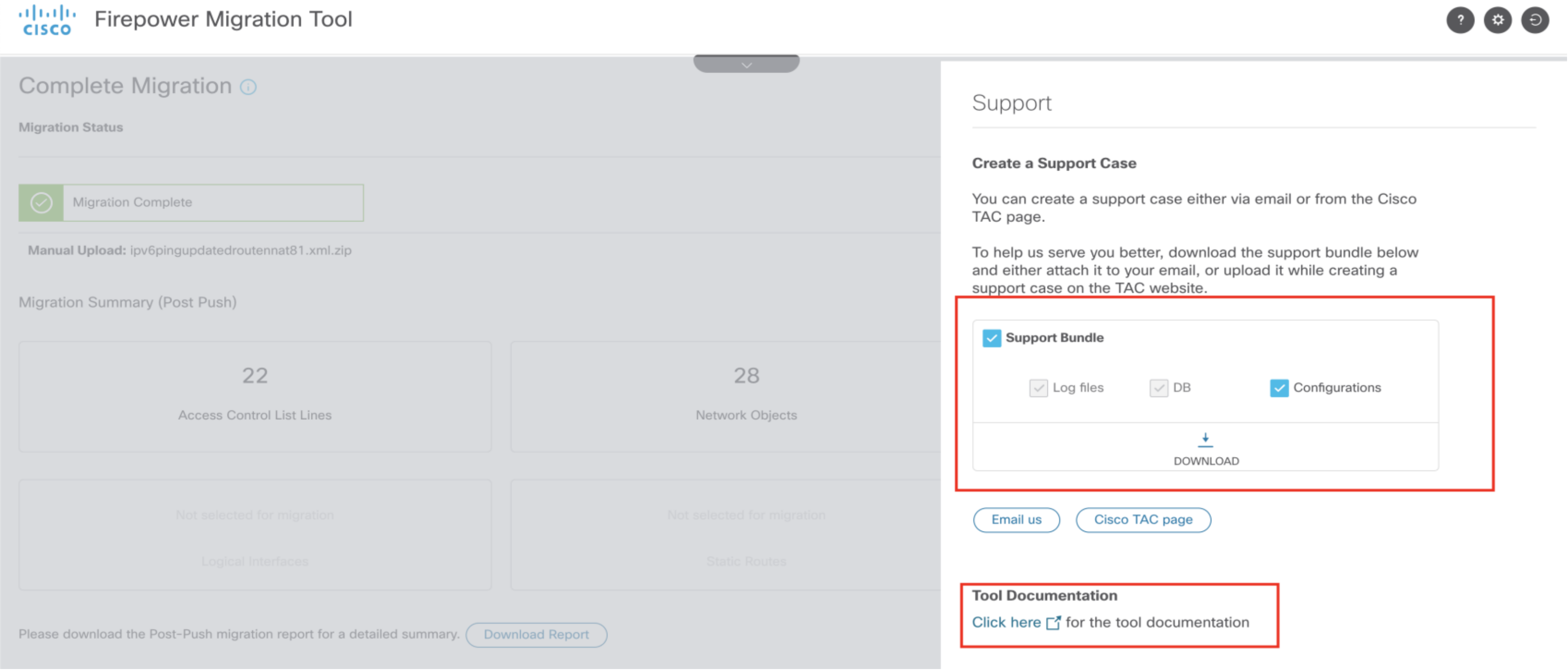
Selected: 0 / 22

□ Select all 22 entries

			SOURCE			DESTINATION						
□	#	Name	Zone	Network	Port	Zone	Network	Port	Application	State	Action	ACE C...
□	5	8.1.5.3_#4	NEW-	0.0.0.0_0	ANY	new-trust1	IP_testt_shared_8.1.4.1	ANY	ANY	✓	drop	1

Support and Logs

➢ Support Bundle and Documentation Help



Firepower Migration Tool

Complete Migration

Migration Status

Migration Complete

Manual Upload: ipv6pingupdatedroutennat81.xml.zip

Migration Summary (Post Push)

22
Access Control List Lines

28
Network Objects

Not selected for migration
Logical Interfaces

Not selected for migration
Static Routes

Please download the Post-Push migration report for a detailed summary. Download Report

Support

Create a Support Case

You can create a support case either via email or from the Cisco TAC page.

To help us serve you better, download the support bundle below and either attach it to your email, or upload it while creating a support case on the TAC website.

☑ **Support Bundle**

☑ Log files ☑ DB ☑ Configurations

DOWNLOAD

Email us | Cisco TAC page

Tool Documentation

Click here for the tool documentation

Best Practices

Download and Run the latest migration tool.

Review the FMT pre-migration checklist.

Create Separate user accounts 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.

Run the connectivity test and monitor logs on FMC.

Cisco Success Network

CCO login to the tool after customer allows sharing statistics with Cisco Success Network

Use default login credentials for the tool if CCO is not reachable / if EULA is not agreed to / if the tool is offline

Data is sent automatically after migration succeeds or fails

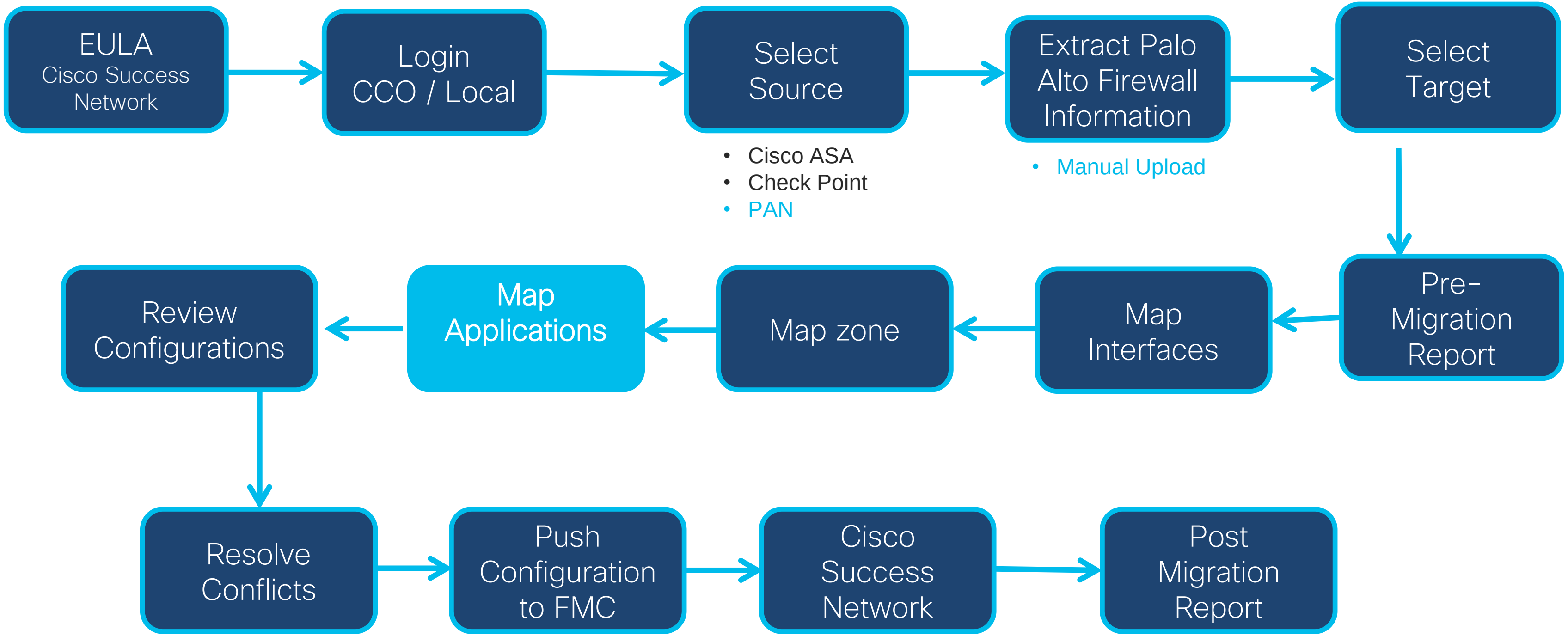
Internet connectivity is only needed for Cisco Success Network. Not having Internet access does not impact the migration

Improves the tool significantly

Troubleshooting Common Errors

- Error While Pushing Network Groups: No Data
- object not found when creating object-group network
- Error while validating: ‘NoneType’ object has no attribute ’name’
- access-list in bulk [1 - 1000] Another operation by another user prevented this operation. Please retry.
- Object with the same name already exists
- Source file type is wrong/File Upload Errors

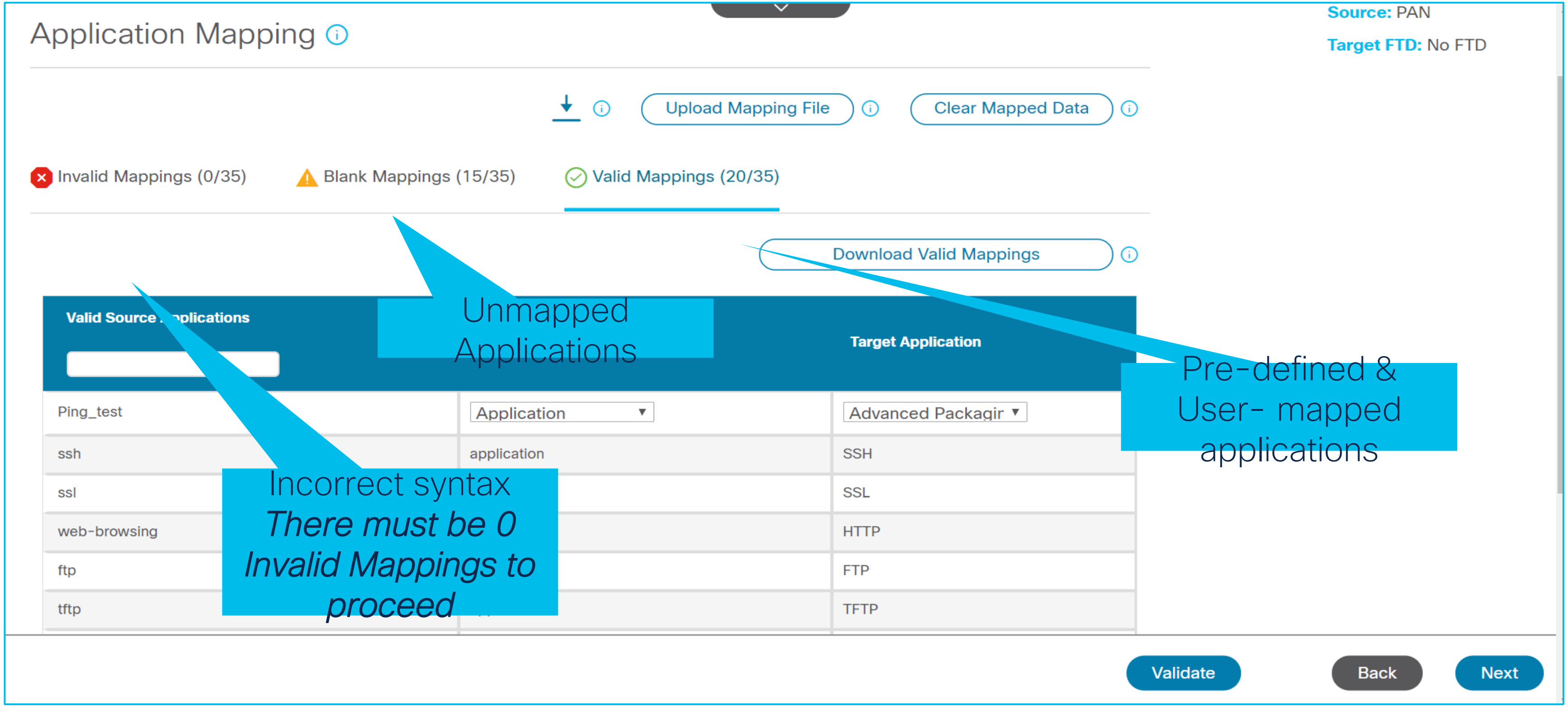
FMT Workflow of Migration from Palo Alto Networks Firewall



- Cisco ASA
- Check Point
- PAN

- Manual Upload

PAN to FTD Application Mapping



Application Mapping ⓘ

Source: PAN

Target FTD: No FTD

☒ Invalid Mappings (0/35)   ⚠ Blank Mappings (15/35)   ✓ Valid Mappings (20/35)

Valid Source Applications		Target Application
Ping_test	Application ▾	Advanced Packagir ▾
ssh	application	SSH
ssl		SSL
web-browsing		HTTP
ftp		FTP
tftp		TFTP

Unmapped Applications

Pre-defined & User- mapped applications

Incorrect syntax

There must be 0 Invalid Mappings to proceed

NGFW Migration Service

- ✓ Migration Verification
- Migration Support
- Knowledge Transfer
- Design Reviews

Demo

Thank you

Possibilities

#CiscoLive