Developer Days
Automation

cisco
The bridge to possible

Building Automation For Firewall Policy Provisioning

Fatih Ayvaz
Software Architect, Cisco CX
12.05.2022

Agenda

- Automation challenges
- Solution design and building blocks
- Features
- Workflow and personas
- Limitations and future work
- Q&A

sound familiar?

I cannot access AAA server.

Can you configure firewall to allow my access?

Can you configure the FW-East-01 & FW-West-01 firewall to allow my access?

How many firewalls are there in my path to access AAA server?

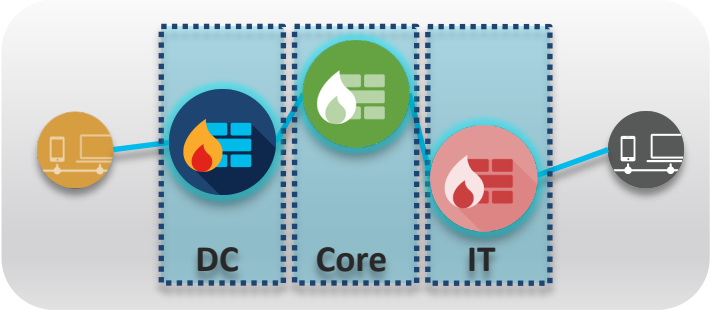
Which team can configure the firewalls in my path to access AAA server?

What vendor/type of firewalls are present in path? Who can configure? When?

Request

Allow HTTPS access from 10.0.0.10 to 20.0.0.20 starting from 12th May for one month.

Key Challenges



- Find the path and identify firewalls between source to destination
- Find the teams controlling the firewalls
- Multi-vendor firewalls
  - technology & skills
- Change Management & Approvals
  - Long & cumbersome approval process
- Implementation Challenges
  - Availability of skilled resources
  - Errors, rollback, dry-run, post-checks, reporting

Key Takeaways

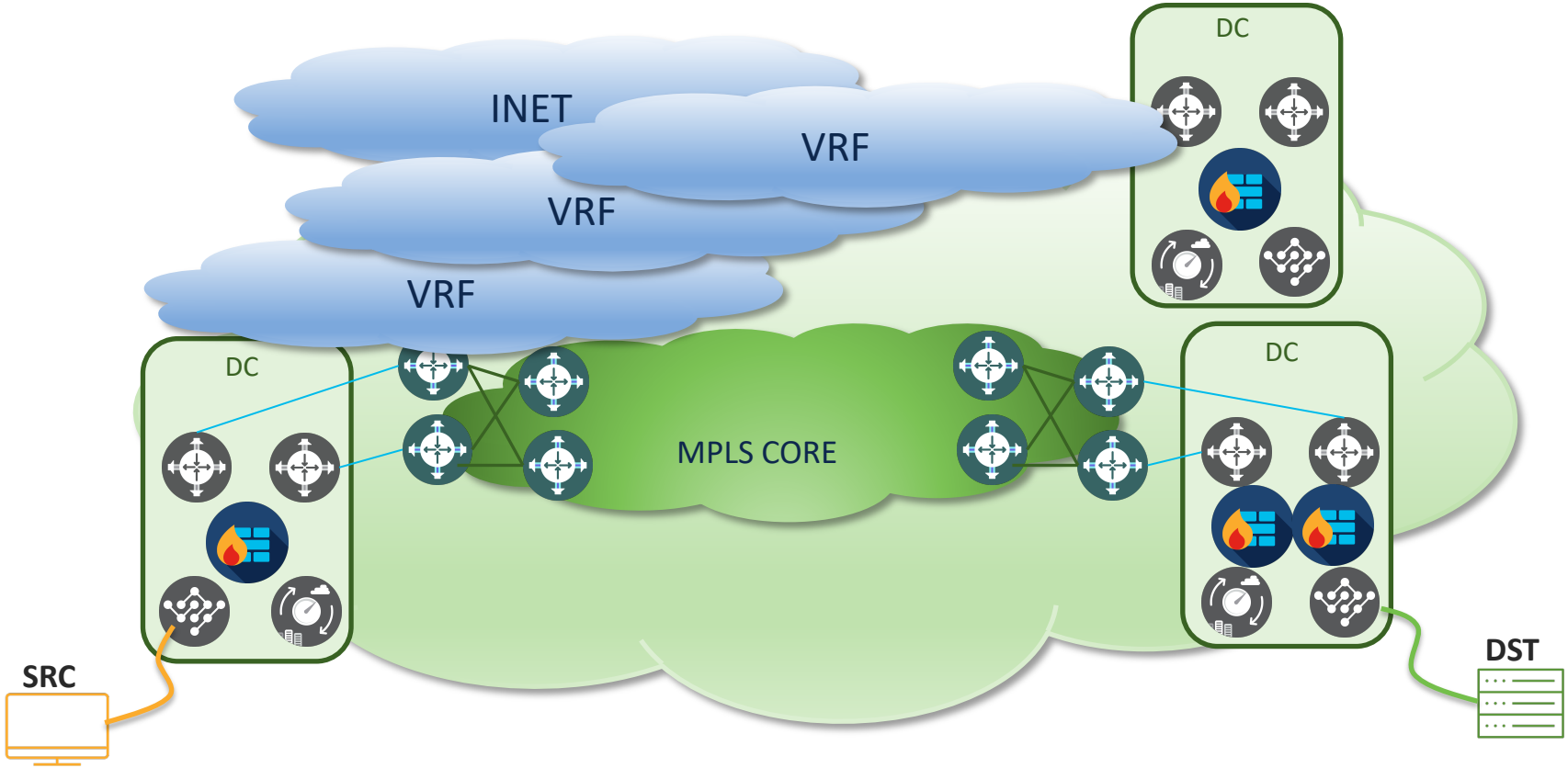
automate

simplify

Firewall Policy Intent

… things to consider

Firewall Policy Intent

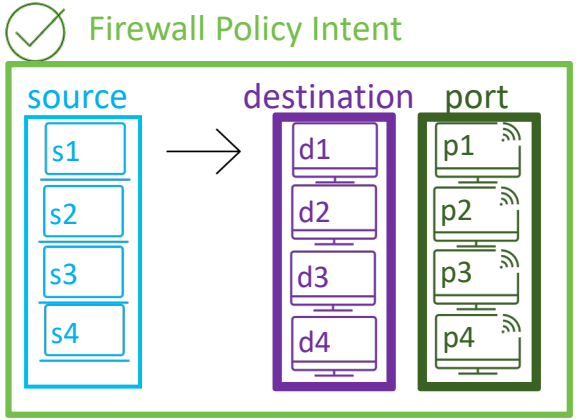


Firewall Policy Provisioning Intent

Allow HTTPS access from 10.0.0.10 to 20.0.0.20 and 30.0.0.30.

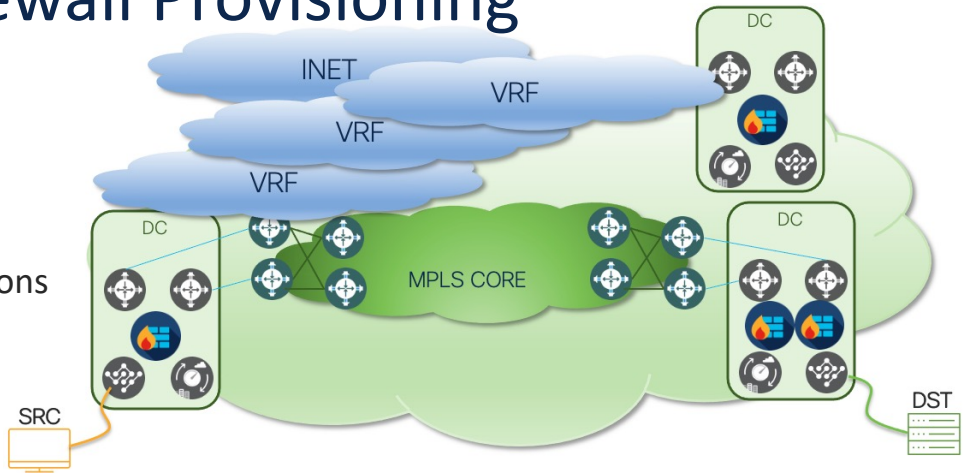
	Example	User	Automation
PARAMETERS			
Source IP Address	✓ 10.0.0.10/24	✓	
Destination IP Address	✓ 20.0.0.20;30.0.0.30	✓	
Protocol (UDP | TCP | ICMP | IP)	✓ TCP	✓	
Port	✓ 8080;8888	✓	
Firewall Device(s)			✓
Existing or New Policy			✓
Policy Name			✓
Source Interface(s)			✓
Destination Interface(s)			✓

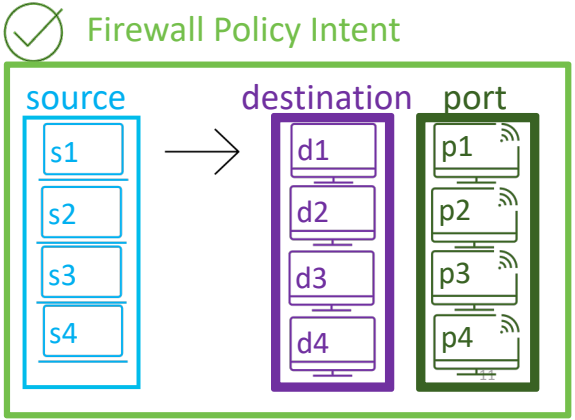
Firewall Policy Provisioning Intent



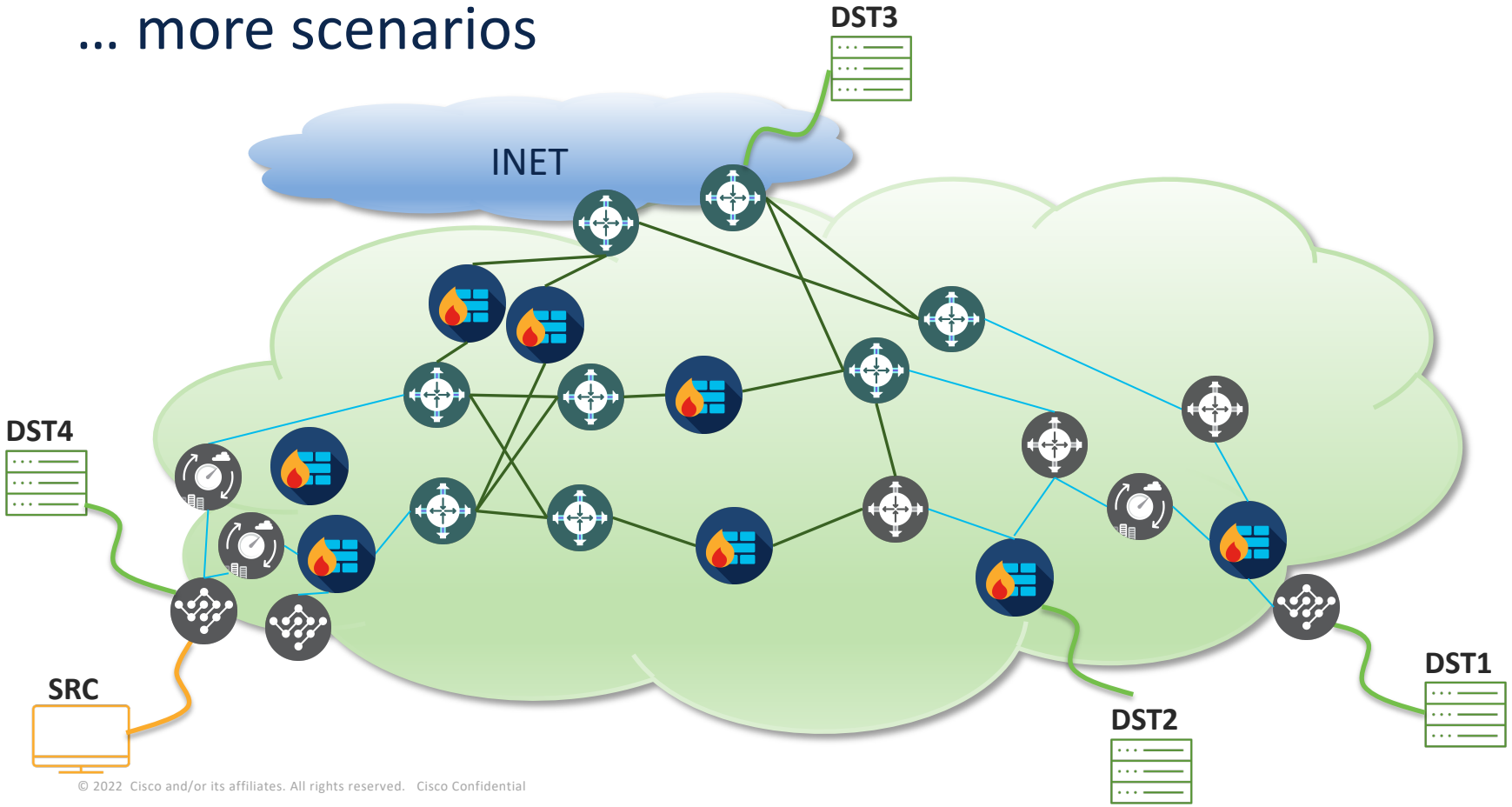
Building Automation for Firewall Provisioning

- How to identify the firewalls?
  - The path from a given source to a destination
    - asymmetric path?
  - The path(s) from multiple sources to multiple destinations
    - *source-address grouping & destination-address grouping
- The ingress and the egress interfaces
- What to configure: existing policy or new policy?
  - Use existing objects or create new ones
  - How to optimize the existing policy?
  - How to handle unknown sources or destinations?
- How to complete provisioning faster in runtime?
  - **asynchronous APIs
  - ***offline data stores



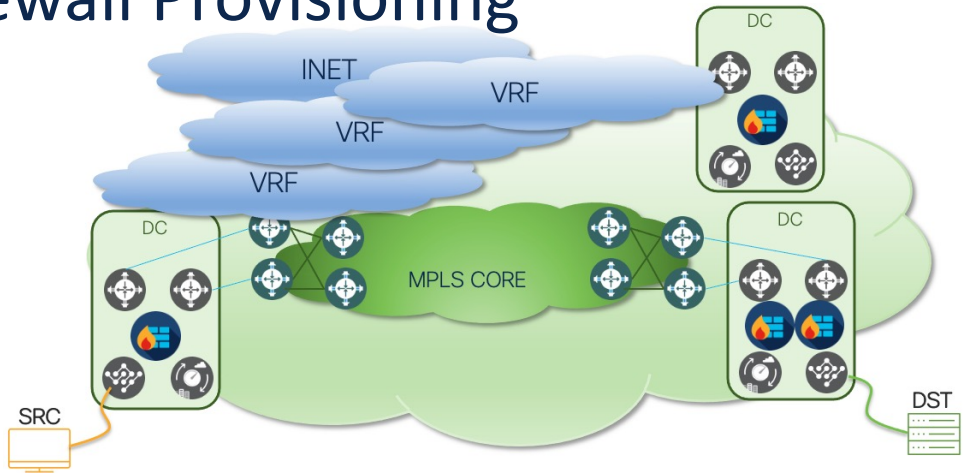


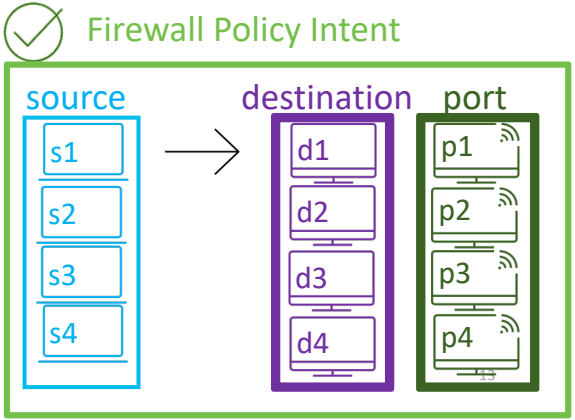
… more scenarios



Building Automation for Firewall Provisioning

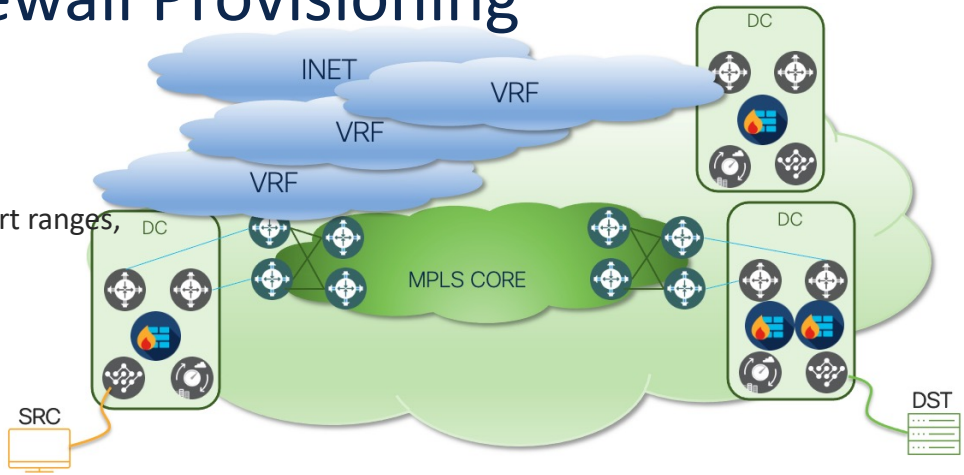
- Multi vendor
  - Firewalls
  - Routers
  - Load Balancers
  - DC Fabric & Controller
  - Cloud Controller
- Network devices: Routing scope vs provisioning scope
- User maintained data
  - Mapping data (NAT, ACI-to-PBR, etc)
  - Blacklisting
  - SLA (approve timer)
  - Excluded VRFs

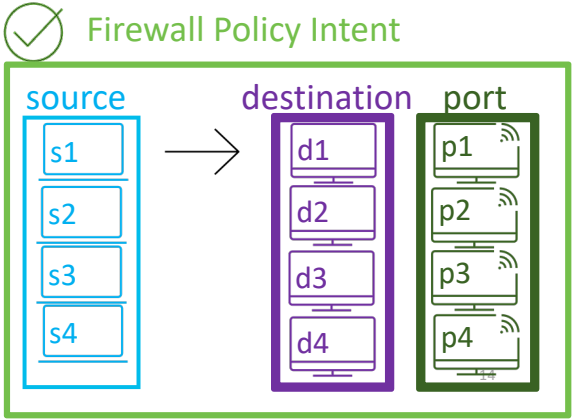




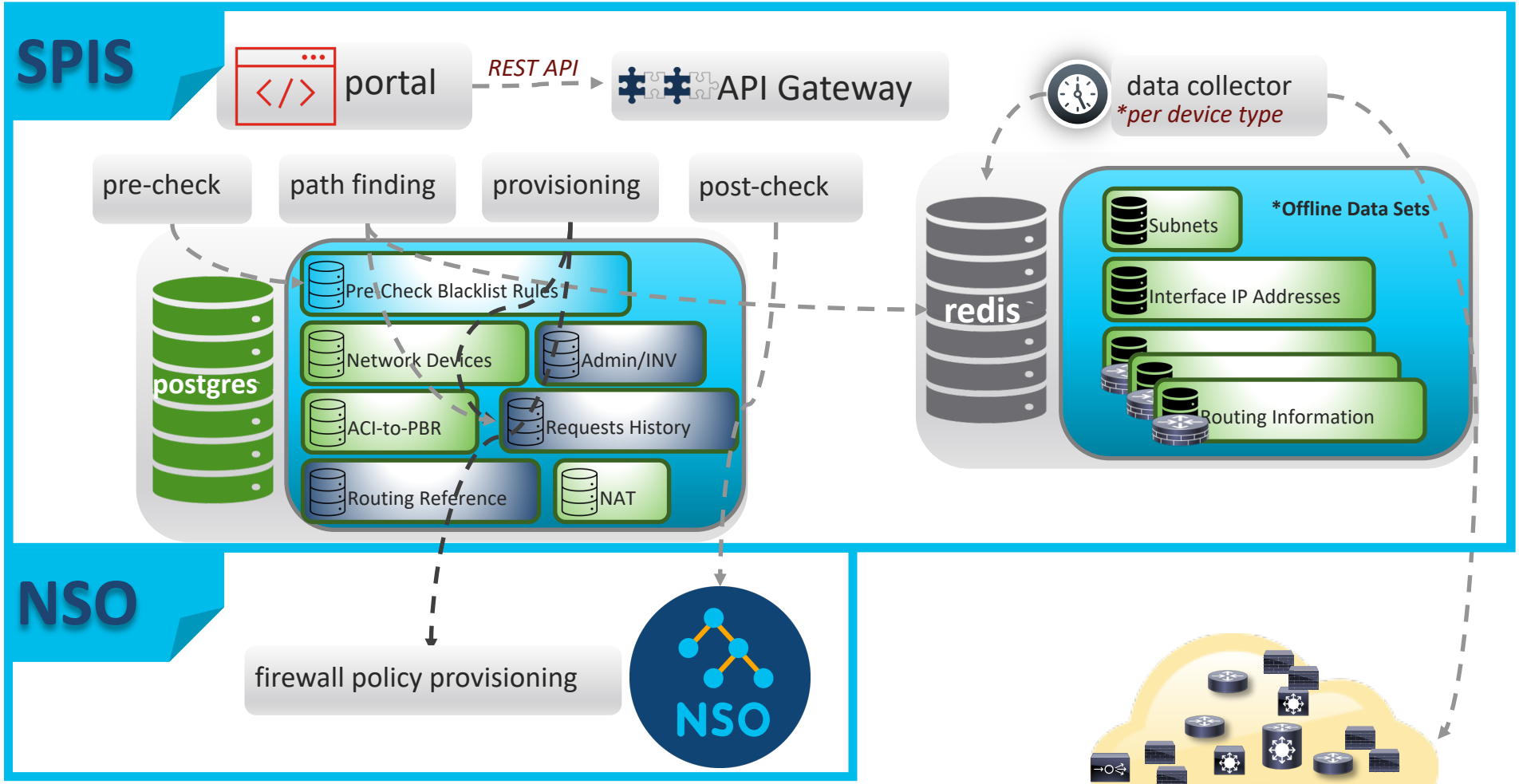
Building Automation for Firewall Provisioning

- Standardization of Communication Matrix (CM)
  - Mandatory vs optional fields
  - Field value constraints (chars, delimiters, regex, IP addresses, port ranges, etc.)
  - Protocol without port number
  - Same CM for different departments
  - Inline validations(int range, char limit, whitespace, etc)
  - Pre-check rules (blacklisting)
  - Compliance (insecure ports)
- Upload CSV file vs UI Form
  - Source of truth
  - Save the request form
- User roles and permissions
  - Request, approve, deploy





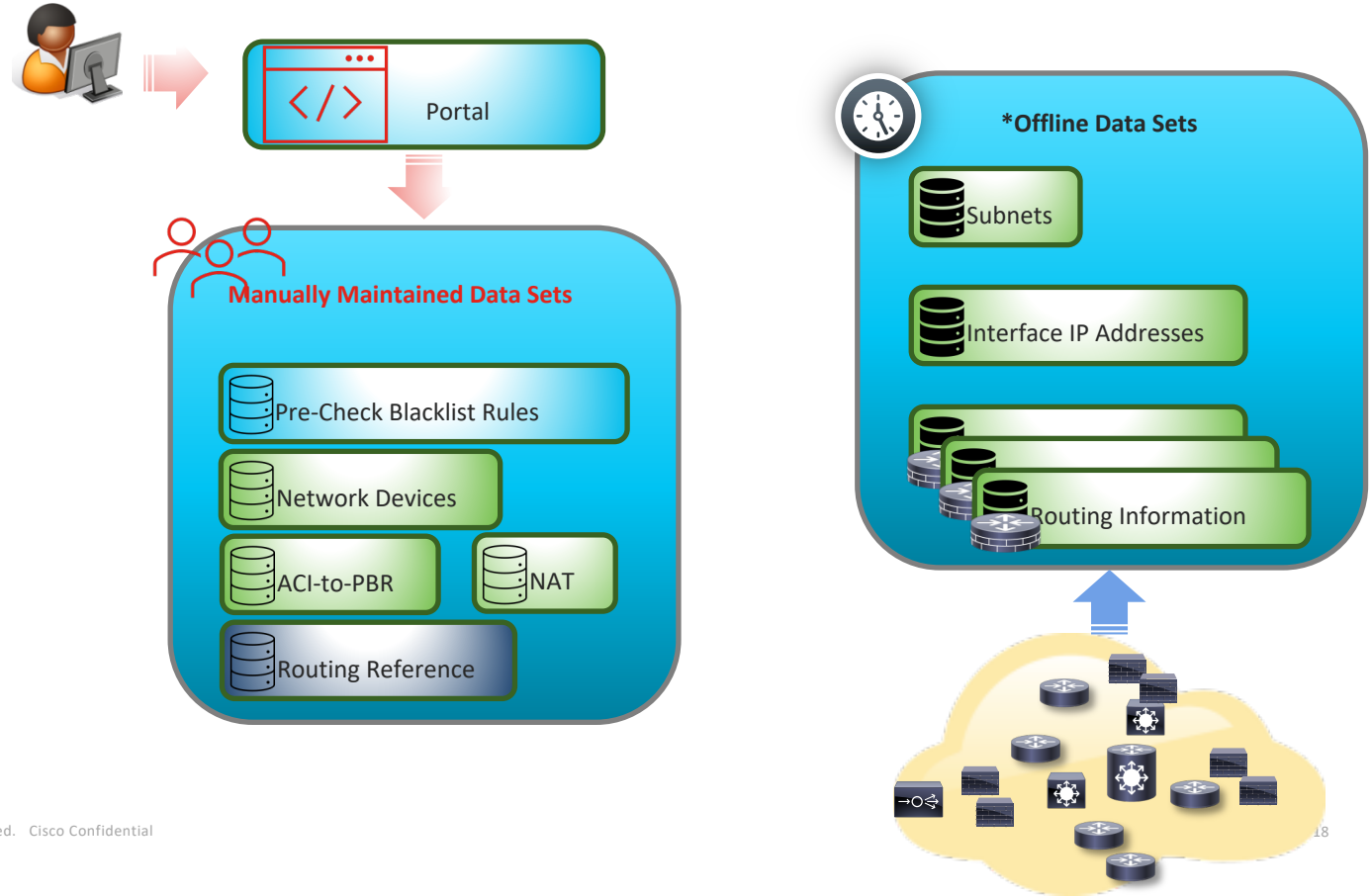
Solution & Architecture

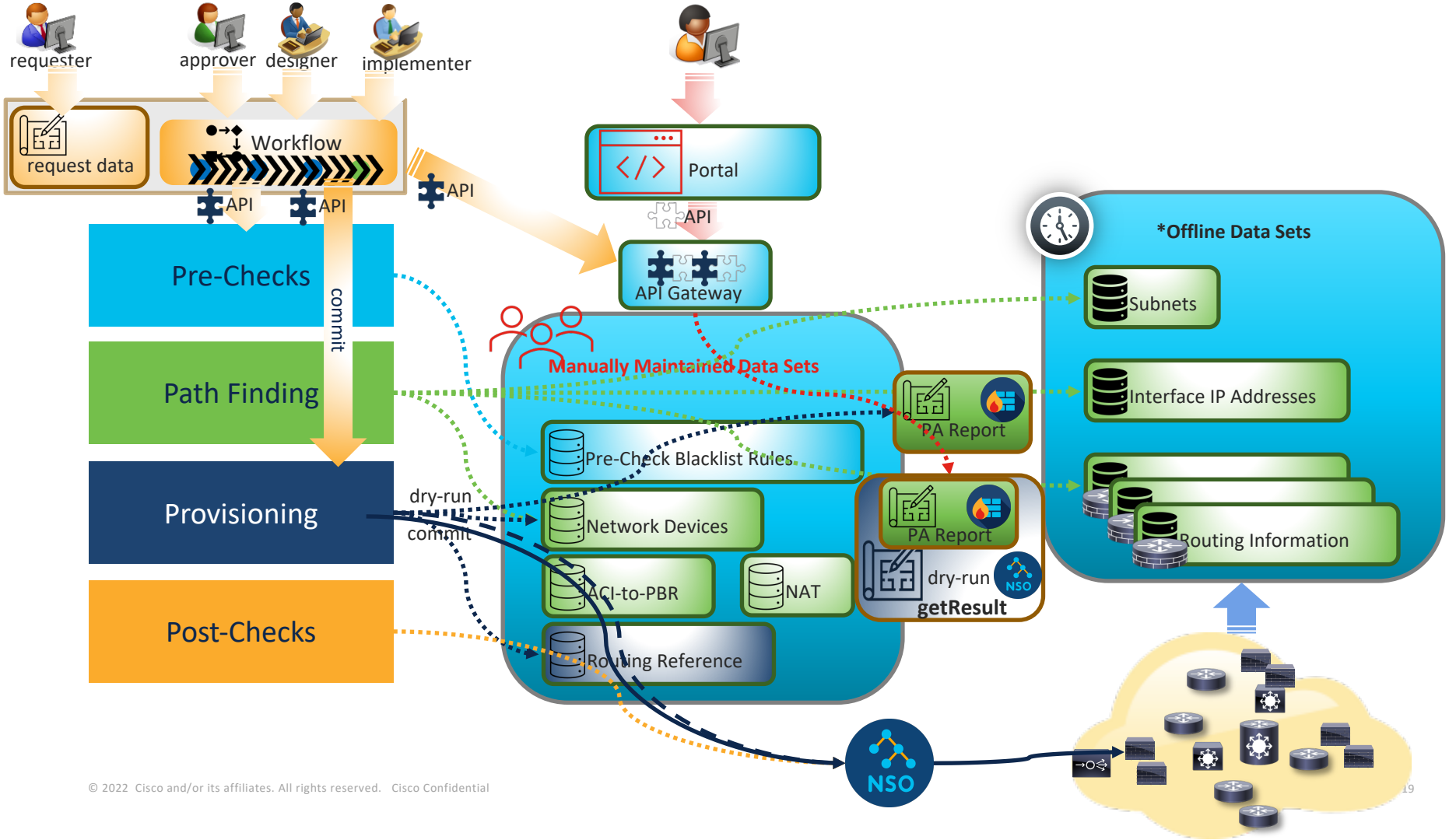


Software Solution - Process Stages

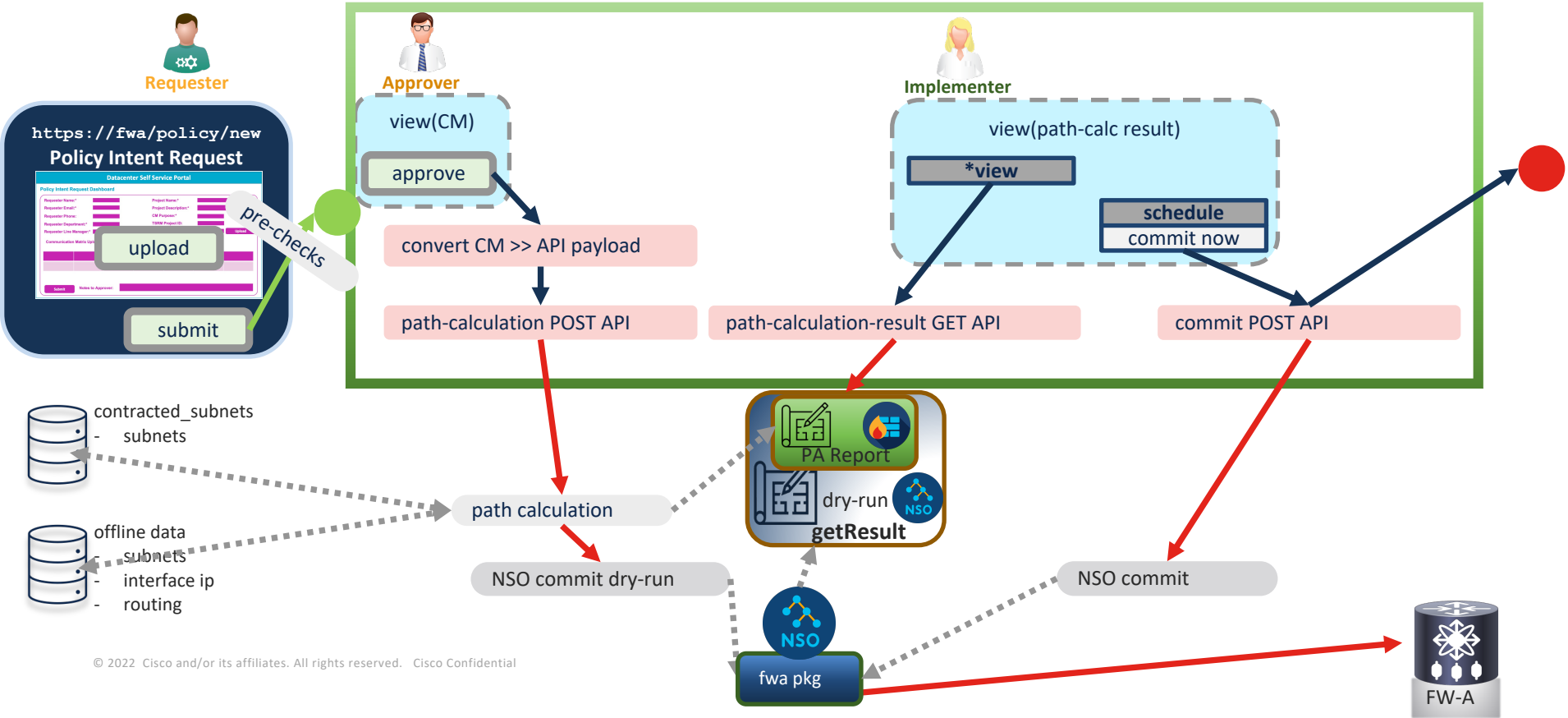
Pre-Checks	Blacklist rules
Path Finding	Find path from source to destination
Provisioning	Provision routes and access policies
Post-Checks	Device configs

Software Solution – Data Sets





With Portal



Roles and Interactions

Admin

SPIS

https://portal/auth

Admin

- Black List
  - Black List
- Device List
- Path Calculation History
- UOP Planning Action List
- DC - FW Automation - History

Pre-Checks BlackList

CREATE BLACKLIST

Rule	Enabled	Source IP Address	Destination IP Address	Destination Port No	Seq No	Description	Action
YM001	✓	150.1.1.0/24	120.1.1.0/24	200	2	OKKK	
lab test	✓	50.1.1.123	70.1.1.123	1234	4	test	
AnyALL-Word	✓	any	any	any	3		
Rule-A	✗	10.0.0.0/24	20.0.0.0/24	any	4		
Rule-BL-001	✓	any	20.99.0.0/24	any	5		
Rule-BL-002	✓	any	20.20.0.0/24	any	9		
Rule-BL-003	✓	10.99.0.0/24	any	any	6		
Rule-BL-004	✓	10.10.0.0/24	any	any	7		
Rule-BL-005	✓	any	any	760	8		
Rule-BL-007	✓	any	any	770	11		

1 2

Requester

SPIS

https://portal/auth

Search

Requester

DC - FW Automation - Requester

DC - FW Automation - Requester

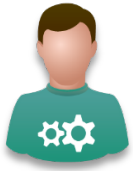
Requester Action List

Policy Intent Request Action List

Create Request

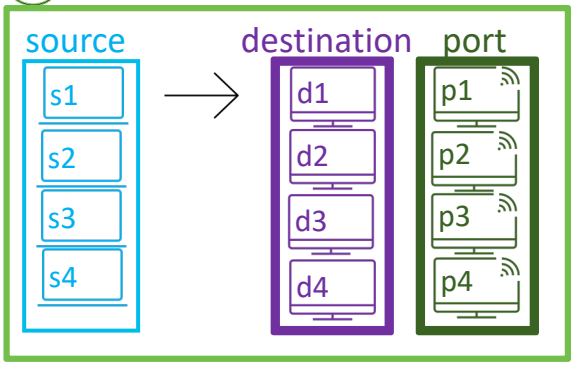
Request ID	Requester Name	Requester Email	Requester Phone	Requester Department	Requester Line Manager	Project Name	Project Description	CM Purpose	Status	Action
000165	requester	1		1	1	1	1	1	COMMIT_C...	
000164	requester	2		2	2	2	2	2	APPROVED	
000163	requester	1		1	1	1	1	1	APPROVED	
000162	requester	fa		cx	kenny	DE53132-BL_FA	DE53132-BL_FA	DE53132-BL_FA	REQUESTER_SU...	
000161	reques	DE53020-test-F...		DE53020-test-F...	DE53020-test-F...	DE53020-test-F...	DE53020-test-F...	DE53020-test-F...	REQUESTER_SU...	
000160	requester	faa		cisco	matt	dup-test	dup-test	dup-test	APPROVED	
000159	requester	faa		dup-test	dup-test	dup-test	dup-test	dup-test	_REJECT	
000158	requester	faa		faa	faa	DE53008-06-du...	DE53008-06-du...	DE53008-06	_REJECT	
000157	requester	faa		faa	ff	DE53008-06-dup	DE53008-06-dup	DE53008-06	_REJECT	
000156	requester	faa		faa	faa	DE53008-06	DE53008-06	DE53008-06	_COMMIT_C...	

1 2 3 4 5 ... 17



Requester

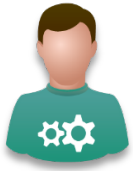
Firewall Policy Intent



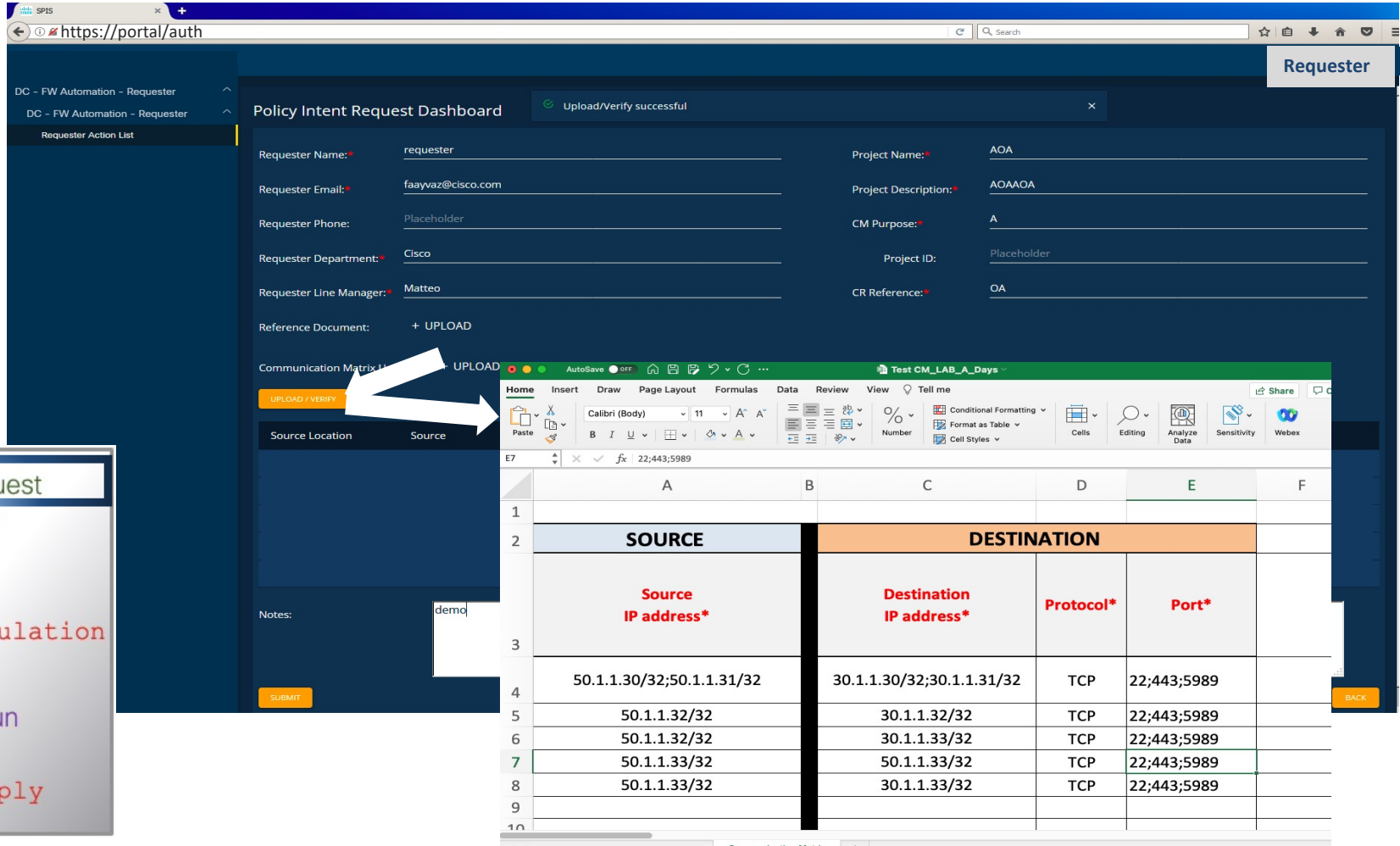
Test CM_LAB_A_Days

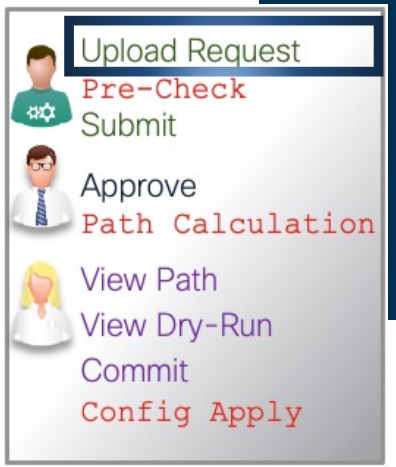
	A	B	C	D	E	F
1						
2	SOURCE		DESTINATION			
3	Source IP address*		Destination IP address*	Protocol*	Port*	
4	50.1.1.30/32;50.1.1.31/32		30.1.1.30/32;30.1.1.31/32	TCP	22;443;5989	
5	50.1.1.32/32		30.1.1.32/32	TCP	22;443;5989	
6	50.1.1.32/32		30.1.1.33/32	TCP	22;443;5989	
7	50.1.1.33/32		50.1.1.33/32	TCP	22;443;5989	
8	50.1.1.33/32		30.1.1.33/32	TCP	22;443;5989	
9						

Communication Matrix



Requester


SPIS
https://portal/auth
Requester
DC - FW Automation - Requester
DC - FW Automation - Requester
Requester Action List
Policy Intent Request Dashboard
Upload/Verify successful
Requester Name:*
requester
Requester Email:*
faayvaz@cisco.com
Requester Phone:
Placeholder
Requester Department:*
Cisco
Requester Line Manager:*
Matteo
Reference Document:
+ UPLOAD
Communication Matrix U
+ UPLOAD
UPLOAD / VERIFY
Source Location
Source
Notes:
demo
SUBMIT
Project Name:*
AOA
Project Description:*
AOAAOA
CM Purpose:*
A
Project ID:
Placeholder
CR Reference:*
OA
BACK
Test CM_LAB_A_Days
Home
Insert
Draw
Page Layout
Formulas
Data
Review
View
Tell me
Share
Paste
Calibri (Body)
11
Number
Conditional Formatting
Format as Table
Cell Styles
Cells
Editing
Analyze Data
Sensitivity
Webex
E7
22;443;5989
SOURCE
DESTINATION
Source IP address*
Destination IP address*
Protocol*
Port*
50.1.1.30/32;50.1.1.31/32
30.1.1.30/32;30.1.1.31/32
TCP
22;443;5989
50.1.1.32/32
30.1.1.32/32
TCP
22;443;5989
50.1.1.32/32
30.1.1.33/32
TCP
22;443;5989
50.1.1.33/32
50.1.1.33/32
TCP
22;443;5989
50.1.1.33/32
30.1.1.33/32
TCP
22;443;5989


Upload Request
Pre-Check
Submit
Approve
Path Calculation
View Path
View Dry-Run
Commit
Config Apply

Requester

SPIS

https://portal/auth

Requester

DC - FW Automation - Requester

DC - FW Automation - Requester

Requester Action List

Policy Intent Request Dashboard

Request has been Submitted, requestID is 000166

Requester Name:*	requester	Project Name:*	AOA
Requester Email:*	faayvaz@cisco.com	Project Description:*	AOAAOA
Requester Phone:	Placeholder	CM Purpose:*	A
Requester Department:*	Cisco	Project ID:	Placeholder
Requester Line Manager:*	Matteo	CR Reference:*	OA

Reference Document: + UPLOAD

Communication Matrix Upload: + UPLOAD Test CM_LAB.xlsx

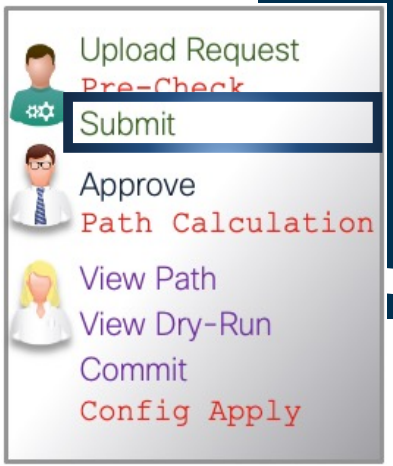
UPLOAD / VERIFY

Source Location	Source	Destination Location	Destination	Protocol	Port	Pre-Check Result	Notes
	50.1.1.30/32;50.1.1.31/32		30.1.1.30/32;30.1.1.31/32	TCP	22;443;5989	Pass	
	50.1.1.32/32		30.1.1.32/32	TCP	22;443;5989	Pass	
	50.1.1.32/32		30.1.1.33/32	TCP	22;443;5989	Pass	
	50.1.1.33/32		50.1.1.33/32	TCP	22;443;5989	Pass	
	50.1.1.33/32		30.1.1.33/32	TCP	22;443;5989	Pass	

Notes: demo

SUBMIT

BACK



Approver

SPIS

https://portal/auth

Approver Actions

Approver

The request has been approved and submitted to implementor.

Requester Email:* faayvaz@cisco.com

Requester Phone: Placeholder

Requester Department:* Cisco

Requester Line Manager:* Matteo

Reference Document:

Notes: 2022-04-20 08:04:33 requester: demo

Project Description:* AOAAOA

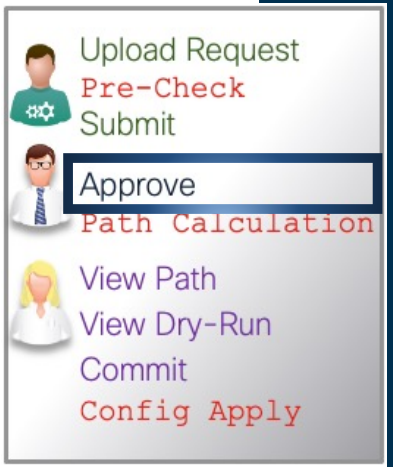
CM Purpose:* A

Project ID: Placeholder

Source Location	Source	Destination Location	Destination	Protocol	Port	Notes
	50.1.1.30/32;50.1.1.31/32		30.1.1.30/32;30.1.1.31/32	TCP	22;443;5989	Note ...
	50.1.1.32/32		30.1.1.32/32	TCP	22;443;5989	Note ...
	50.1.1.32/32		30.1.1.33/32	TCP	22;443;5989	Note ...
	50.1.1.33/32		50.1.1.33/32	TCP	22;443;5989	Note ...
	50.1.1.33/32		30.1.1.33/32	TCP	22;443;5989	Note ...

Notes: approve

REJECT APPROVE BACK



Implementer

Upload Request
Pre-Check
Submit

Approve
Path Calculation

View Path
View Dry-Run
Commit
Config Apply

SPIS

https://portal/auth

Implementer Actions

Policy Intent Requ

Request ID	Re Na
000166	rec
000165	rec
000164	rec
000163	rec
000160	rec
000156	rec
000154	rec
000153	rec
000148	TT
000147	log

Implementer

Request Action Page

Requester Name:* requester

Requester Email:* faayvaz@cisco.com

Requester Phone: Placeholder

Requester Department:* Cisco

Requester Line Manager:* Matteo

Reference Document:

Notes:

2022-04-20 08:04:33 **requester: demo**

2022-04-20 08:06:55 **approver: approve**

Project Name:* AOA

Project Description:* AOAAOA

CM Purpose:* A

Project ID: Placeholder

Source Location	Source	Destination Location	Destination	Protocol	Port	Notes
	50.1.1.30/32;50.1.1.31/32		30.1.1.30/32;30.1.1.31/32	TCP	22;443;5989	Note ...
	50.1.1.32/32		30.1.1.32/32	TCP	22;443;5989	Note ...
	50.1.1.32/32		30.1.1.33/32	TCP	22;443;5989	Note ...
	50.1.1.33/32		50.1.1.33/32	TCP	22;443;5989	Note ...
	50.1.1.33/32		30.1.1.33/32	TCP	22;443;5989	Note ...

Path Calculation Report CLICK TO REFRESH

Action

4 5 ... 14

Implementer

SPIS

https://portal/auth

Implementer Actions

Implementer

Rule ID: 000166_4

Source IPs: 50.1.1.33/32 Dest IPs: 50.1.1.33/32

Calculated Path

SRC IP:50.1.1.33/32, Dest IP: 50.1.1.33/32

ACI → Fortigate-FW-1 → ACI

PATHS:

Device	Context	VRF	Ingress Interface	Egress Interface	Device Type
ACI	Test	VRF-A	BD--FW-Service-1	node-101/vlan290	
Fortigate-FW-1	Test	Default	FW-APP	FW-WEB	FireWall
ACI	Test	VRF-Z	node-101/vlan290	BD--FW-Service-1	

DryRun Results

Device	Result
Fortigate-FW-1	config vdom edit 'Test' config firewall policy edit '452' set comments OA next end next end

Rule ID: 000166_5

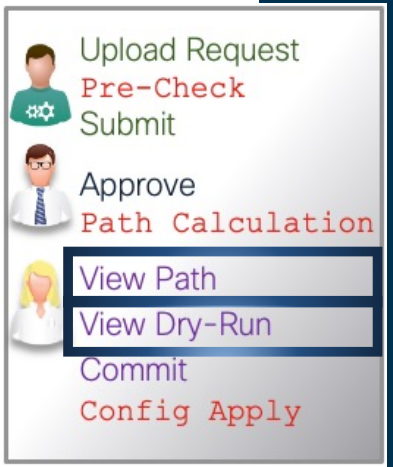
Source IPs: 50.1.1.33/32 Dest IPs: 30.1.1.33/32

Calculated Path

SRC IP:50.1.1.33/32, Dest IP: 30.1.1.33/32

Action

4 5 ... 14



Implementer

Upload Request
Pre-Check
Submit

Approve
Path Calculation

View Path
View Dry-Run
Commit
Config Apply

https://portal/auth

Implementer Actions

Implementer

Source IPs: 50.1.1.33/32 Dest IPs: 50.1.1.33/32

Rule ID: 800166_5

Source IPs: 50.1.1.33/32 Dest IPs: 30.1.1.33/32

Calculated Path

SRC IP:50.1.1.33/32, Dest IP: 30.1.1.33/32

ACI → Fortigate-FW-1 → 9010-DC-01

PATHS:

Device	Context	VRF	Ingress Interface	Egress Interface	Device Type
ACI	Test	VRF-A	BD-FW-Service-1	node-101/vlan290	
Fortigate-FW-1	Test	Default	FW-APP	FW-WEB	FireWall
ASR9010-DC-01	Test	VRF-Z	Bundle-Ether100.535	Bundle-Ether100.30	

DryRun Results

Device	Result
Fortigate-FW-1	config vdom edit "Test" config firewall policy edit '454' set comments OA next end next end

Notes:

REJECT COMMIT CLOSE

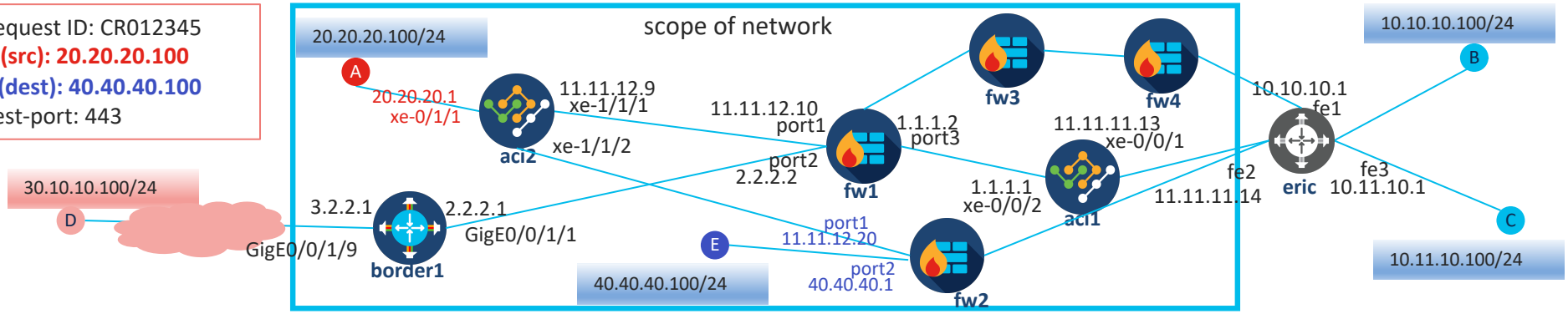
Action

5 ... 14

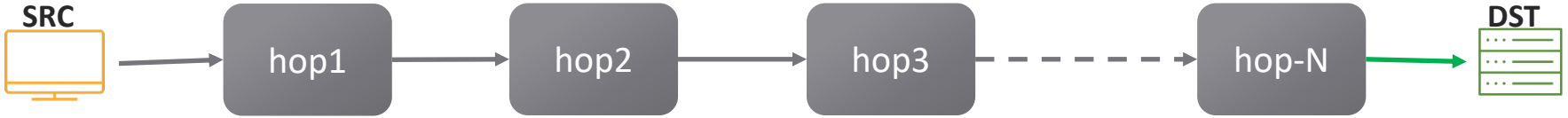
Path Finding

Firewall Policy Intent Request to give access for : A --> E

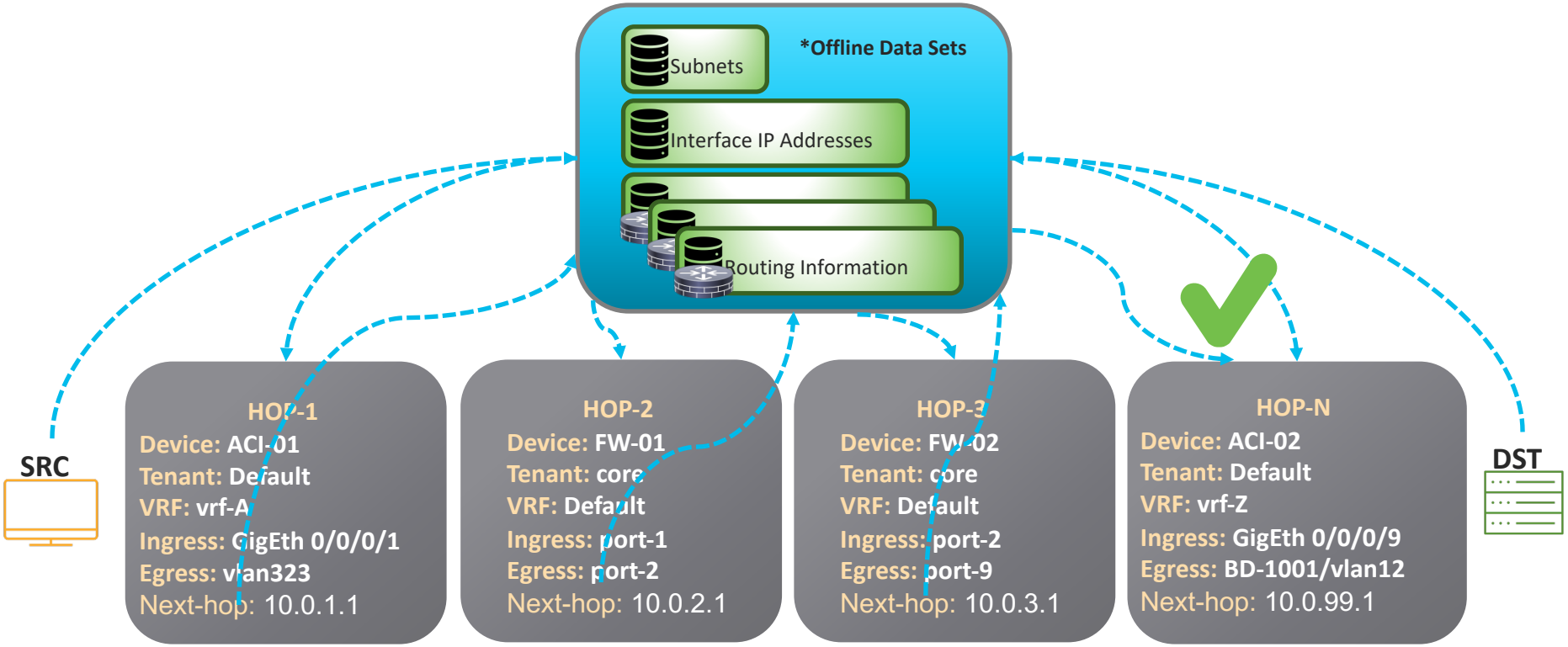
Request ID: CR012345
A (src): 20.20.20.100
E (dest): 40.40.40.100
dest-port: 443



What is the path from source to destination?



Path Finding



Q&A

Limitations and Future Work

- Uniqueness on data keys
- Improvement on offline data
  - move collection to CDB
  - collection through telemetry
  - data objects filtration (UI)
  - new vendors/device types
  - NRT data
  - automation of data validation
- Communication Matrix(CM) variations
- Path calculation performance
- Logging and monitoring

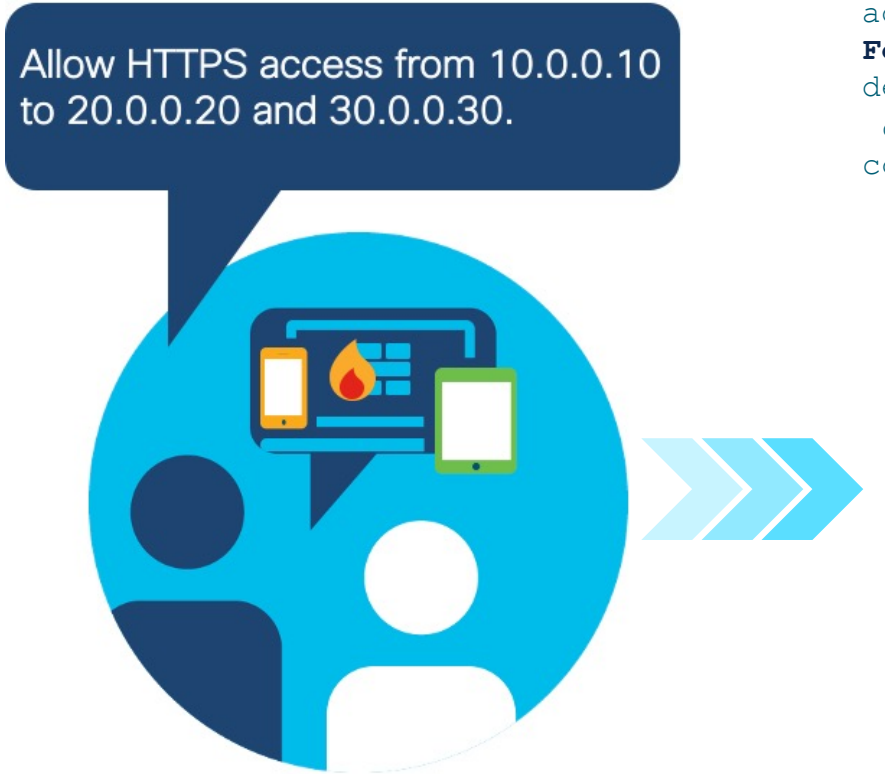
Limitations and Future Work

- Overlapping policy cases
  - Shadow policies
  - Duplicate policies
  - Conflicting policies
- Firewall missing routes
  - Route provisioning
- Post-checks
  - re-execute PC

The bridge to possible

Backup Slides

Firewall Policy Provisioning Intent




```
admin@ncs# show running-config devices device
FortiGate-FW-1 config vdom firewall policy 458
devices device FortiGate-FW-1
 config
config vdom
   edit vdom-core
    config firewall policy
     edit 458
      srcintf  FW-APP
      dstintf  FW-WEB
      srcaddr  10.0.0.10/24
      dstaddr  20.0.0.20/25 30.0.0.30/26
      action   accept
      schedule always
      service  TCP_8080_8888
      comments TEST-TEMPLATE
     exit
    exit
   exit
  !
 !
!
```

Northbound Integration APIs

A. **Path Analysis (PA) Functions API Set**
   1. calculate
   2. getResult (precheck + pathFound + dry-run)

B. **Configuration Functions API Set**
   1. Commit
   2. Dry-Run (embedded in getResult API above!)

C. **Request Management API Set**
   1. Cancel Request