

CISCO *Live!*



#CiscoLive



The bridge to possible

# Automation Concepts in Firewall Policy Provisioning

Fatih Ayvaz, Software Architect, Cisco CX  
Maciej Malysz, Software Architect, Cisco CX  
BRKOPS-2290

# 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 by the speaker until June 17, 2022.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKOPS-2290>



# Agenda

- Concepts
  - Firewall policy provisioning intent
  - Automation challenges
  - Design and architecture
  - Limitations and future work
- Demo
  - User interface
  - Workflow and roles
- Q&A

# Do they sound familiar?

I cannot access AAA server.

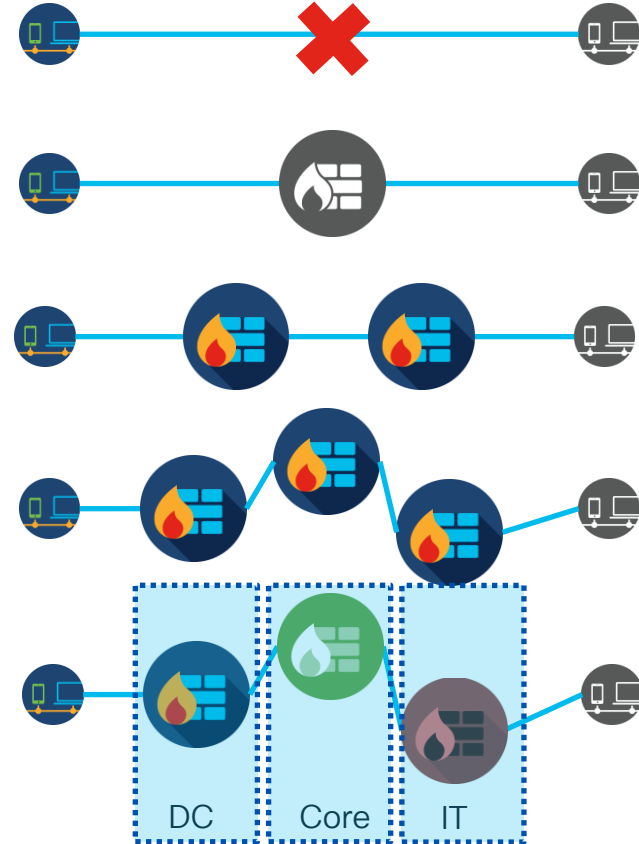
Can you configure firewall to allow my access?

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

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

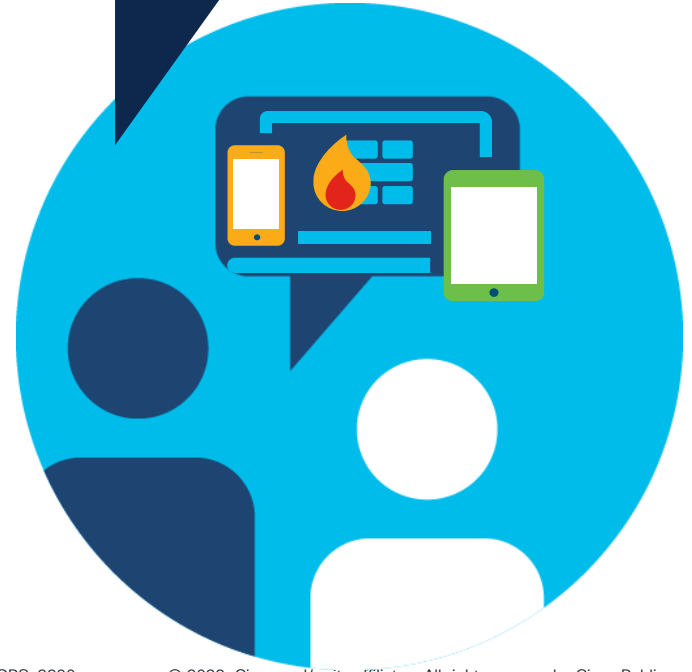
Which team can configure the firewalls in my path to  
access AAA server?

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

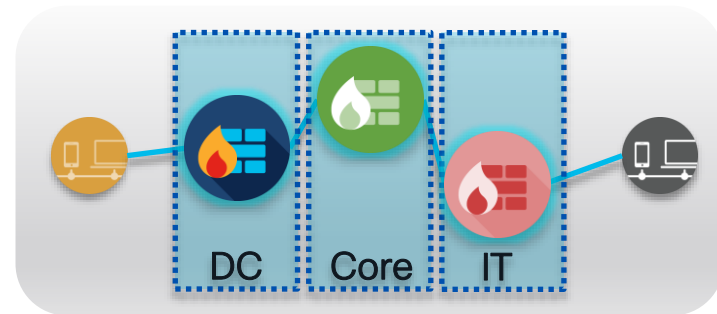


# Request

Allow HTTPS access from 10.0.0.10 to 20.0.0.20 starting from 13<sup>th</sup> of June 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

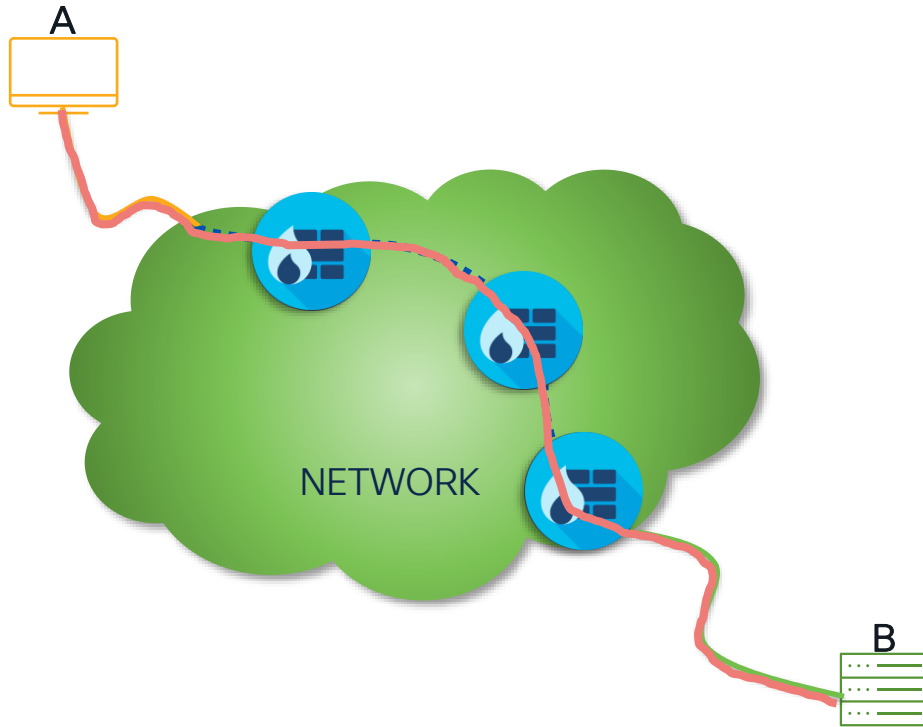


# Firewall Policy Intent

... things to consider



# How to establish connection from A to B?



Connect A



Connect B



Check/Install Route

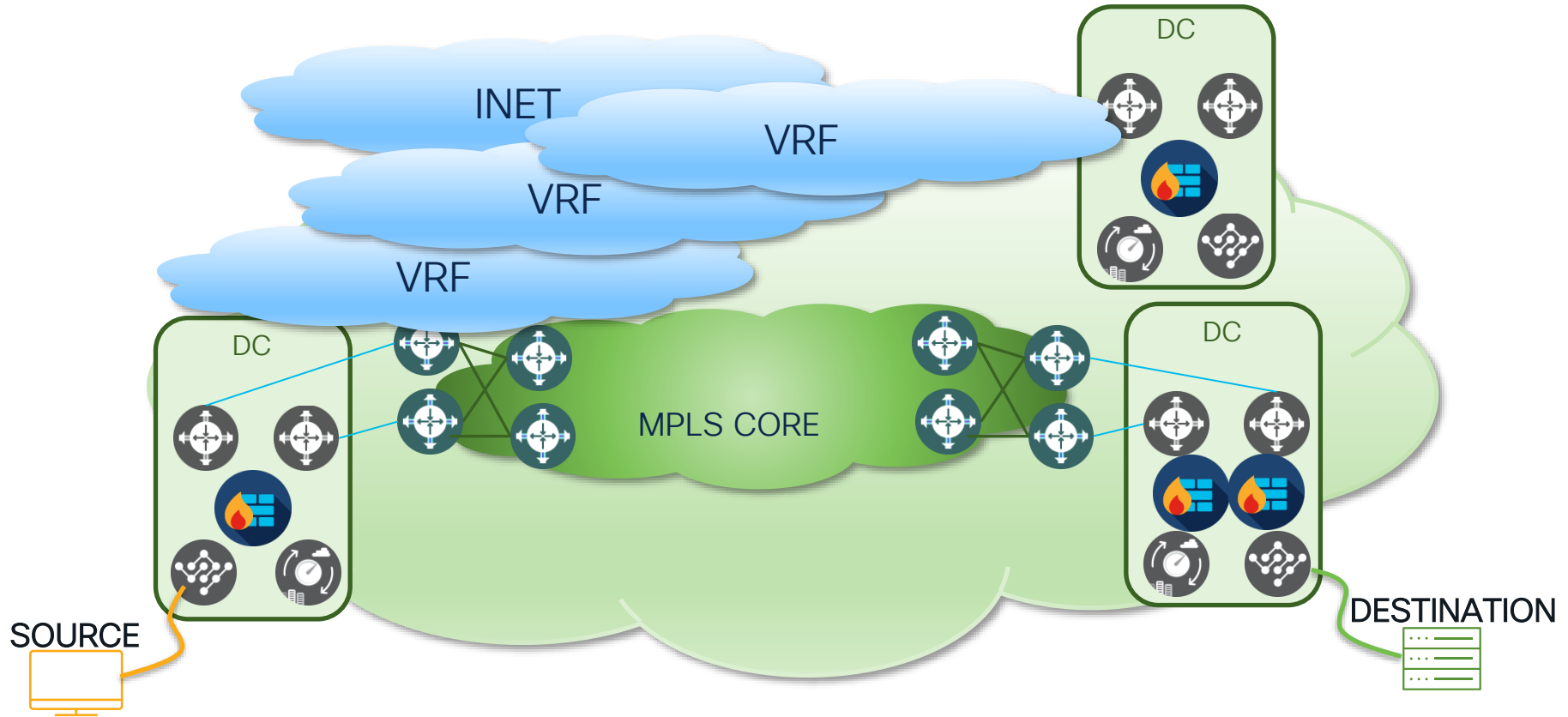


Identify Firewalls



Allow Access

# 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.



CISCO *Live!*

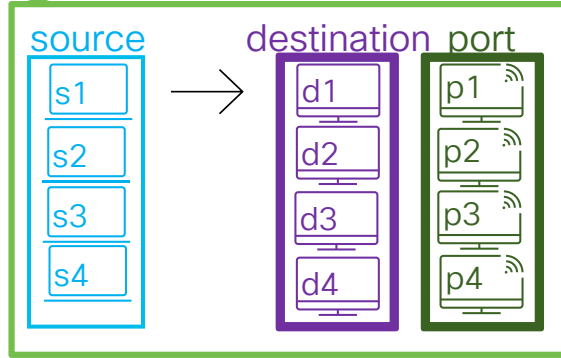
	Example	User	Automation
<u>PARAMETERS</u>			
Source IP Address	✓ 10.0.0.10/24	✓	
Destination IP Address	✓ 20.0.0.20;30.0.0.30	✓	
Protocol ( UDP   TCP   ICMP   IP )	✓ TCP	✓	
Port	✓ 8080;8888	✓	
Firewall Device(s)			✓
Existing or New Policy			✓
Policy Name			✓
Source Interface(s)			✓
Destination Interface(s)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

# Multiple addresses, multiple ports

Allow HTTPS access from 10.0.0.10 to 20.0.0.20 and 30.0.0.30.



✓ Firewall Policy Intent

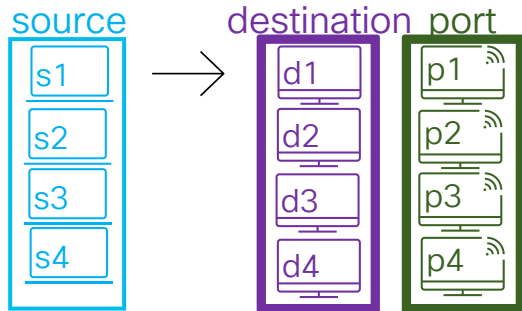


# Example Communication Matrix



Requester

✓ Firewall Policy Intent



	A	B	C	D	E	F
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						
10						

# Firewall Configuration

Allow HTTPS access from 10.0.0.10 to 20.0.0.20 and 30.0.0.30.

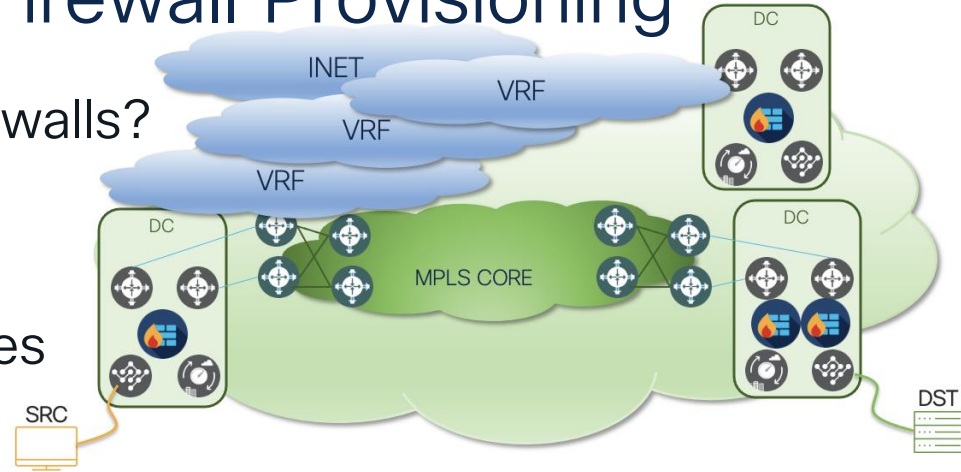
```
admin@ncs# show running-config devices device
FortiGate-FW-1 config vdom firewall policy 458
devices device FortiGate-FW-1
config
config vdom
edit vdom-core
config firewall policy
edit 458
srcintf FW-APP
dstintf FW-WEB
srcaddr 10.0.0.10/24
dstaddr 20.0.0.20/25 30.0.0.30/26
action accept
schedule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

!

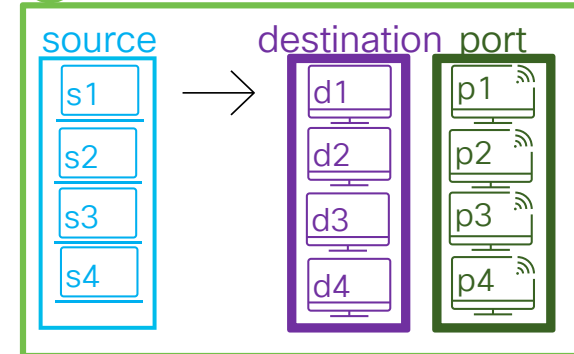


# Building Automation for Firewall Provisioning

- How to find path and identify the firewalls?
  - Path from source to destination
  - asymmetric path, address grouping, etc.
- The ingress and the egress interfaces
- Configure firewall policy
  - Newly, existing, *modification/optimization*
- Unknown sources or destinations
- Fast fulfillment of the intent
  - *asynchronous APIs*
  - *offline data stores*

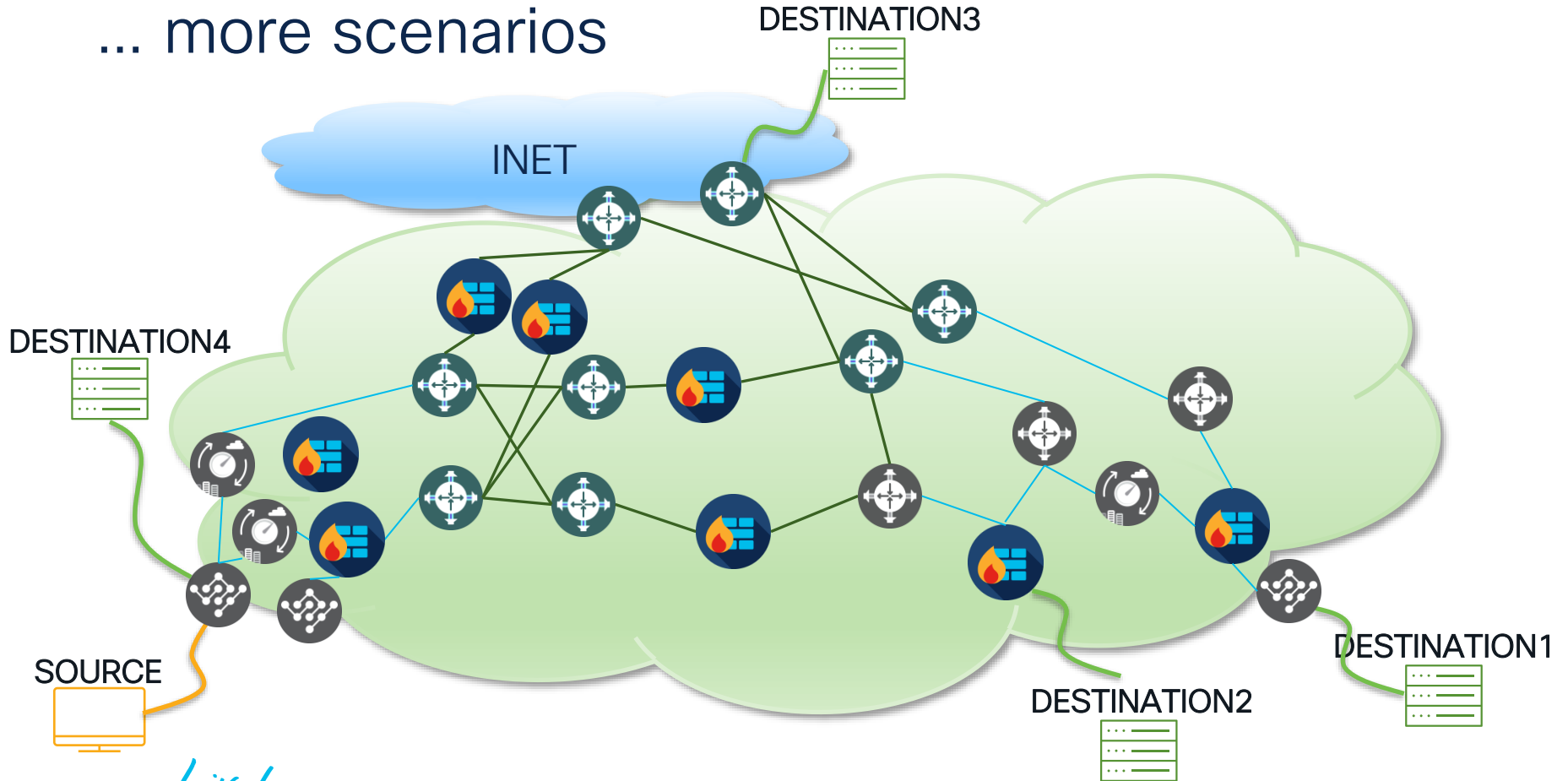


✓ Firewall Policy Intent



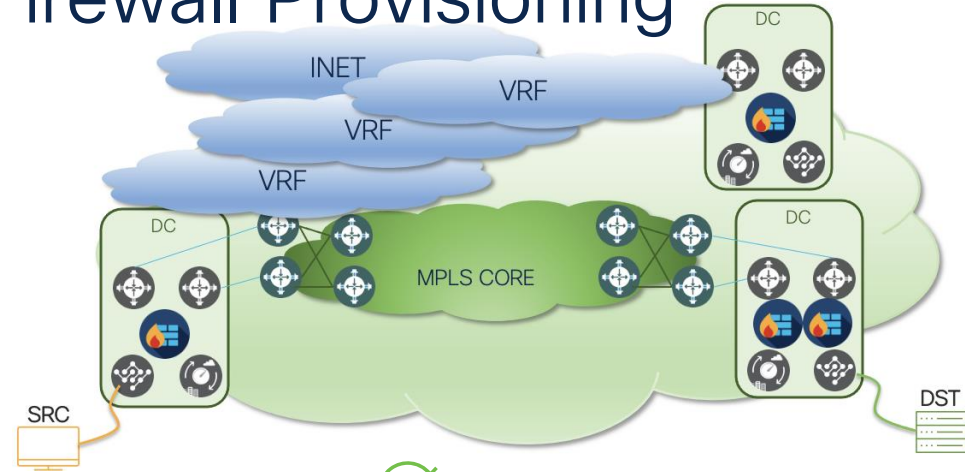


## ... more scenarios

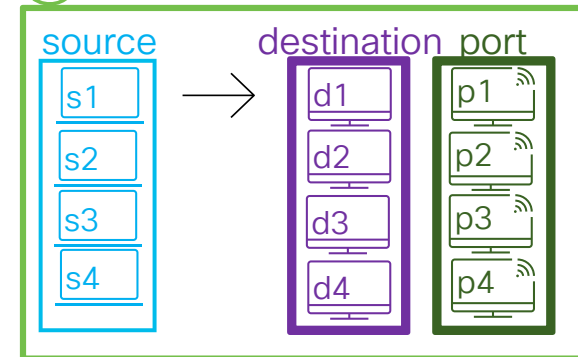


# Building Automation for Firewall Provisioning

- 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)
  - Deny list
  - SLA (approve timer)
  - Excluded VRFs

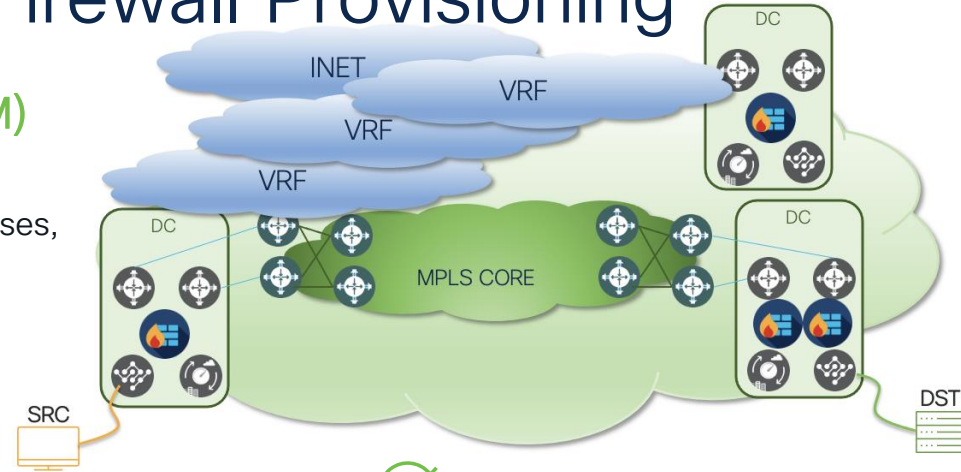


## ✓ Firewall Policy Intent

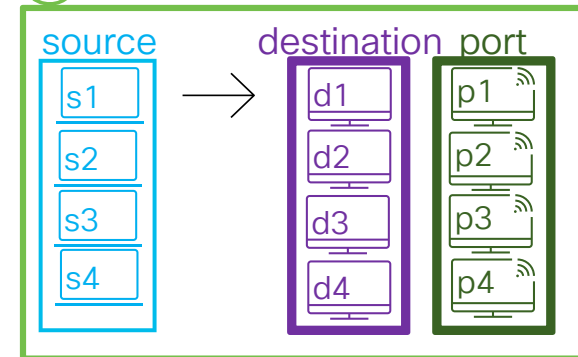


# Building Automation for Firewall Provisioning

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



## ✓ Firewall Policy Intent



# Solution & Architecture

# SPIS



portal

REST API



API Gateway



data collector  
*\*per device type*

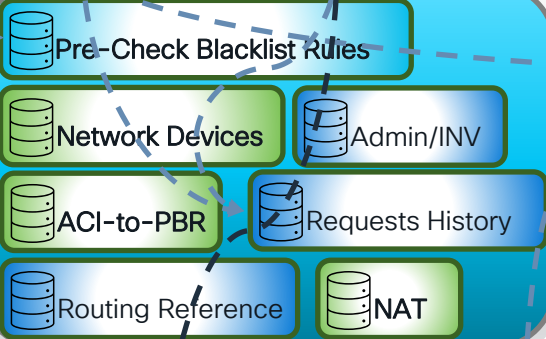
pre-check

path finding

provisioning

post-check

postgres



redis

\*Offline Data Sets

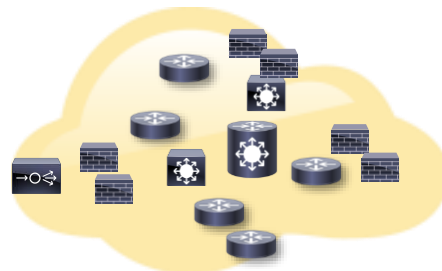
Subnets

Interface IP Addresses

Routing Information

# NSO

firewall policy provisioning



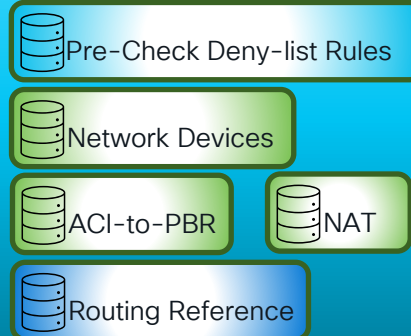
# Software Solution - Process Stages

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

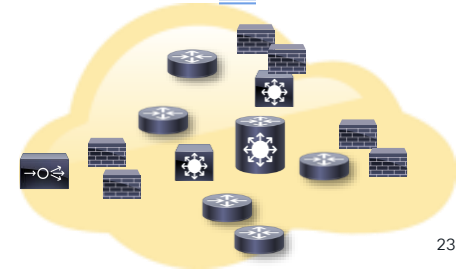
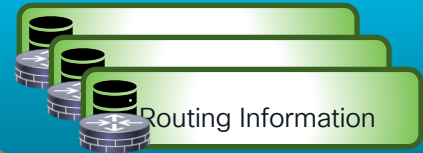
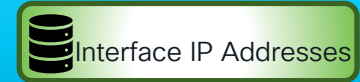
# Software Solution – Data Sets



## Manually Maintained Data Sets



## \*Offline Data Sets



# Firewall Policy Provisioning Job



Requester

request intent!  
allow access from  
**SOURCE** to **DESTINATION**  
on **PORT**



CM



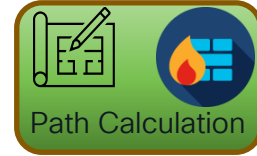
Approver

approve!



Implementer

commit!



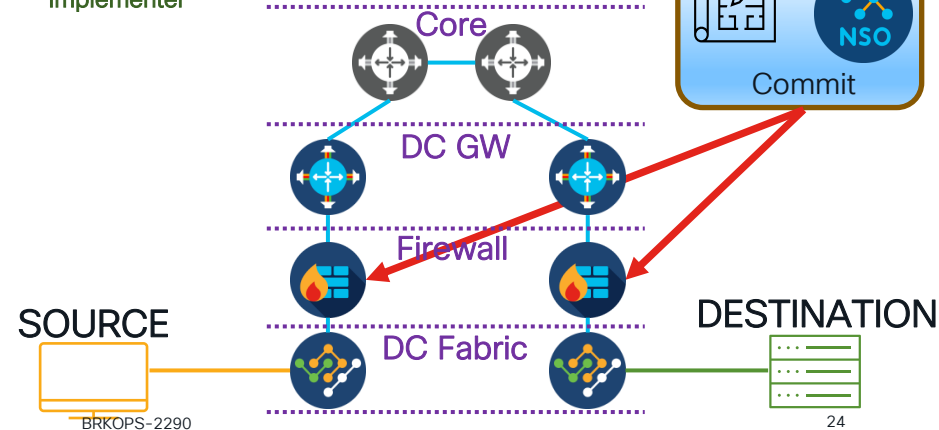
Path Calculation



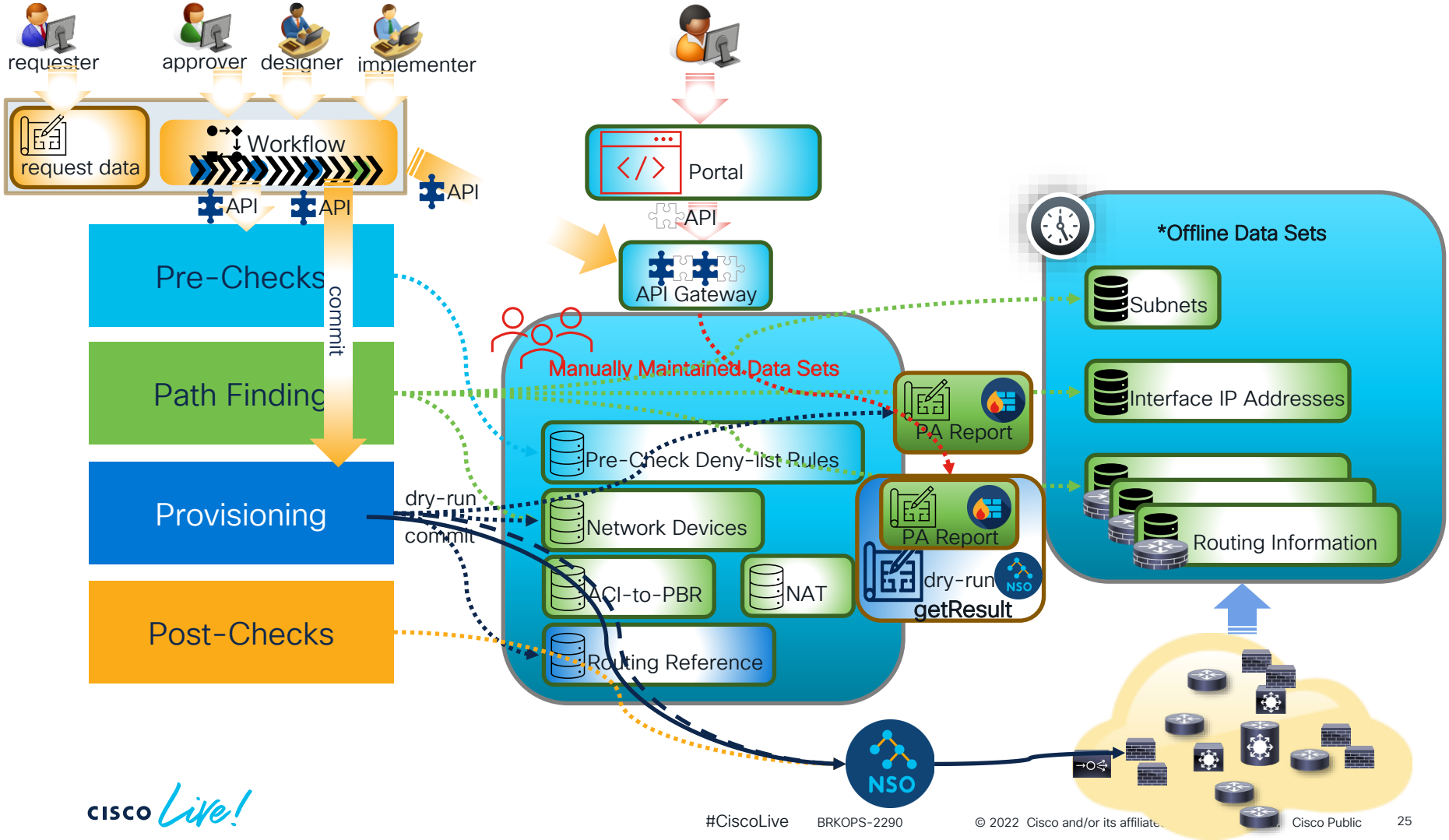
Dry-Run



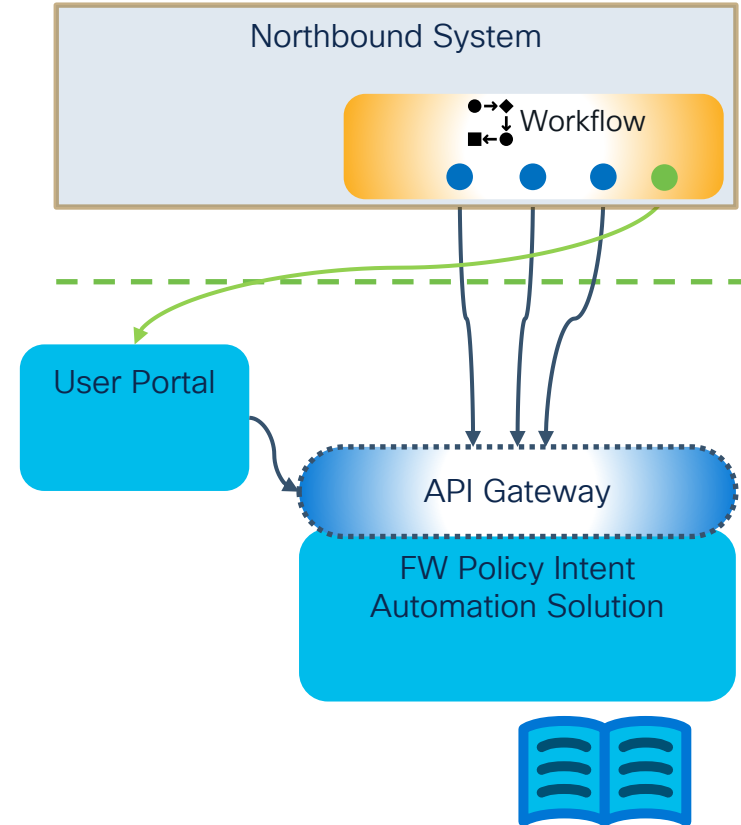
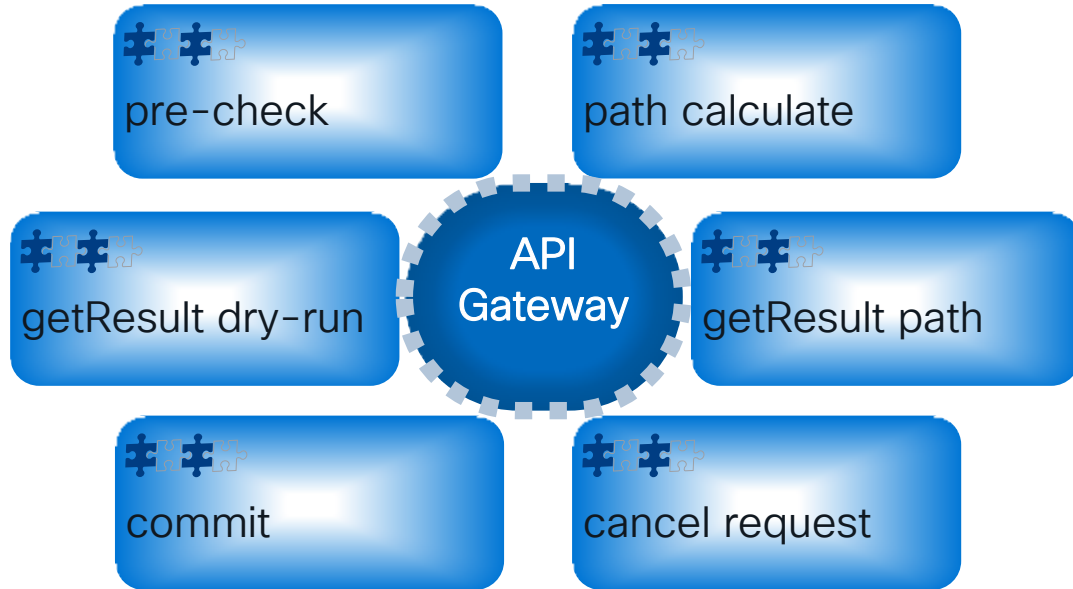
Commit







# Northbound Integration APIs

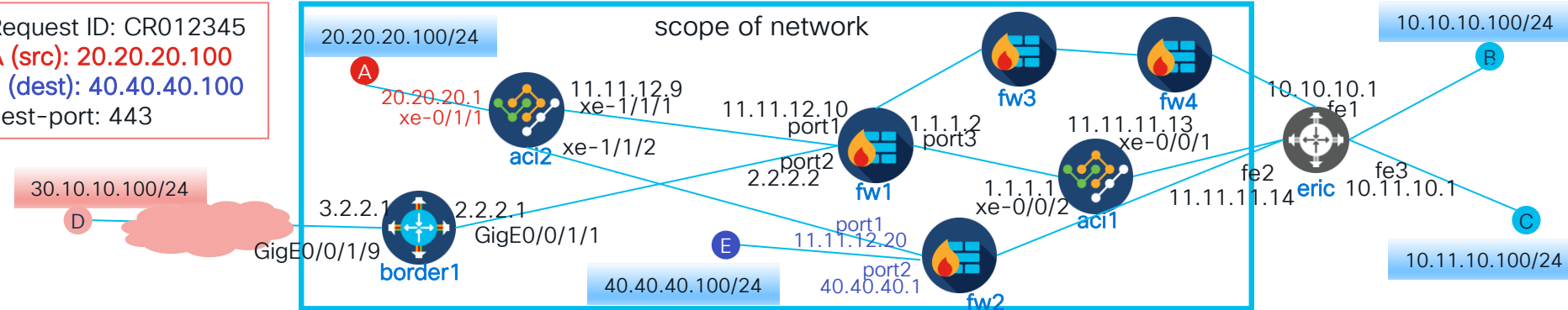


# Path Finding

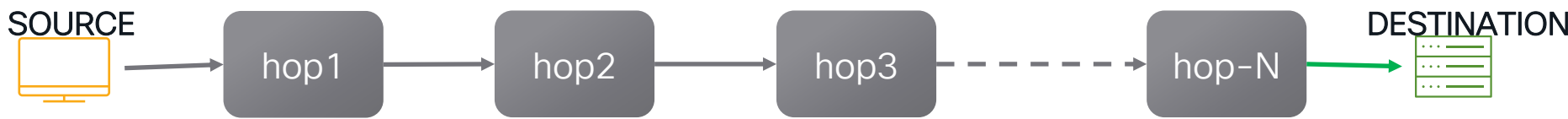


# Firewall Policy Intent Request to give access for : A --> E

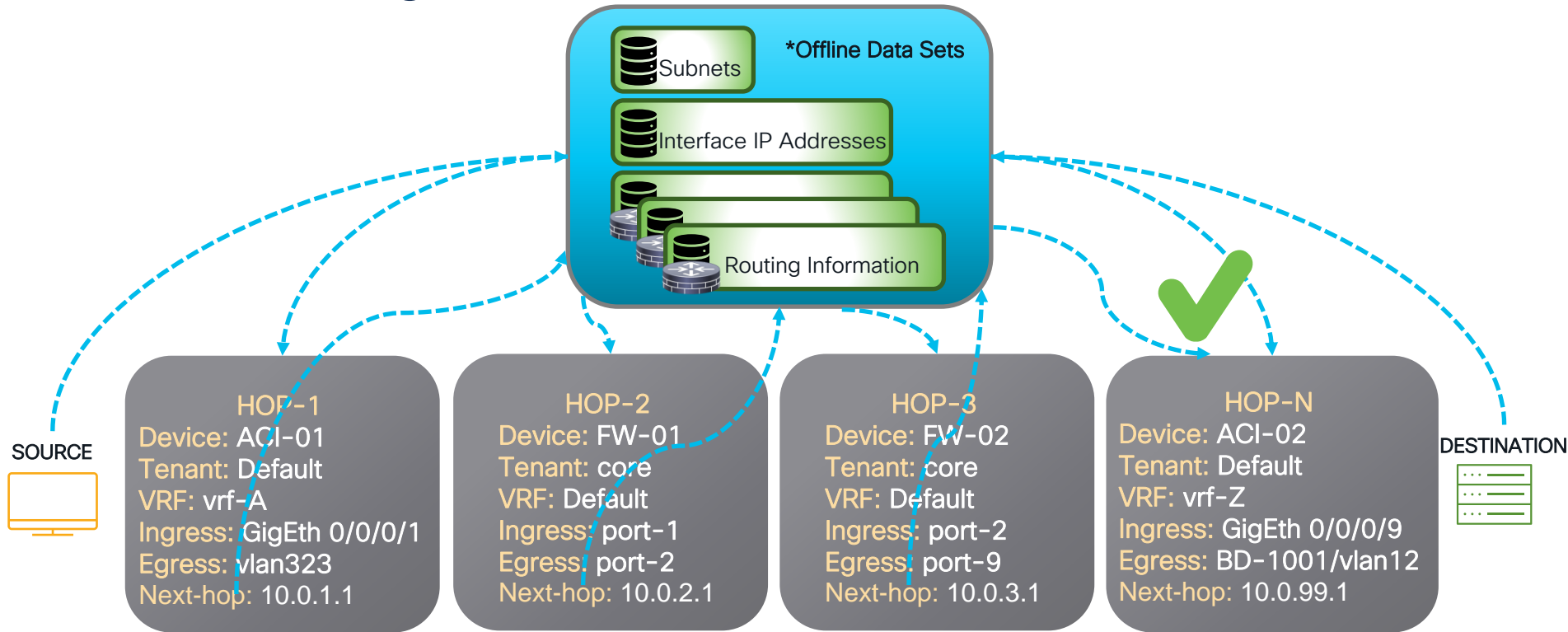
Request ID: CR012345  
**A (src): 20.20.20.100**  
**E (dest): 40.40.40.100**  
dest-port: 443



What is the path from source to destination?



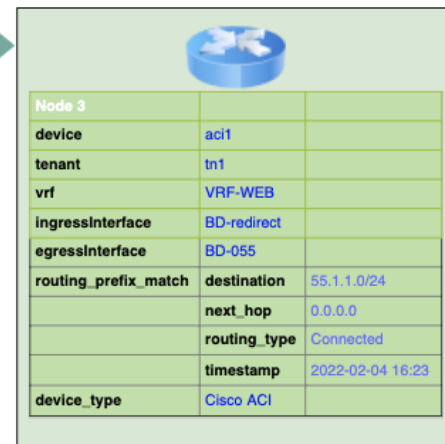
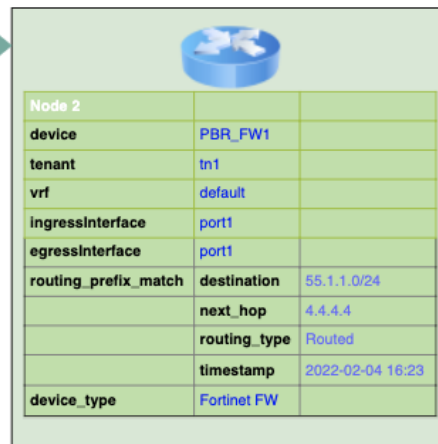
# Path Finding



```

1  "path": [
2    {
3      "device": "aci1",
4      "context": "tn1",
5      "vrf": "VRF-WEB",
6      "ingressInterface": ["BD-050"],
7      "egressInterface": ["BD-redir"],
8      "routing_prefix_match": {
9        "destination": "55.1.1.0/24",
10       "next_hop": "<PBR_FW_IP>",
11       "routing_type": "Redirected",
12       "timestamp": "2022-01-04 09:04"
13     },
14     "device_type": "Cisco ACI"
15   },
16   {
17     "device": "PBR_FW_1",
18     "context": "tn1",
19     "vrf": "Default",
20     "ingressInterface": ["port1"],
21     "egressInterface": ["port1"],
22     "routing_prefix_match": {
23       "destination": "55.1.1.0/24",
24       "next_hop": "10.247.2.9",
25       "routing_type": "Routed",
26       "timestamp": "2022-01-04 09:04"
27     },
28     "device_type": "Fortinet Firewall"
29   },
30   {
31     "device": "aci1",
32     "context": "tn1",
33     "vrf": "VRF-WEB",
34     "ingressInterface": ["BD-redir"],
35     "egressInterface": ["BD-055"],
36     "routing_prefix_match": {
37       "destination": "55.1.1.1/24",
38       "next_hop": "0.0.0.0",
39       "routing_type": "Connected",
40       "timestamp": "2022-01-04 09:04"
41     },
42     "device_type": "Cisco ACI"
43   }
44 ]

```



# 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



Multi-Path support



Logging and monitoring



Overlapping policy cases

- Shadow policies
- Duplicate policies
- Conflicting policies



Firewall missing routes

Route provisioning

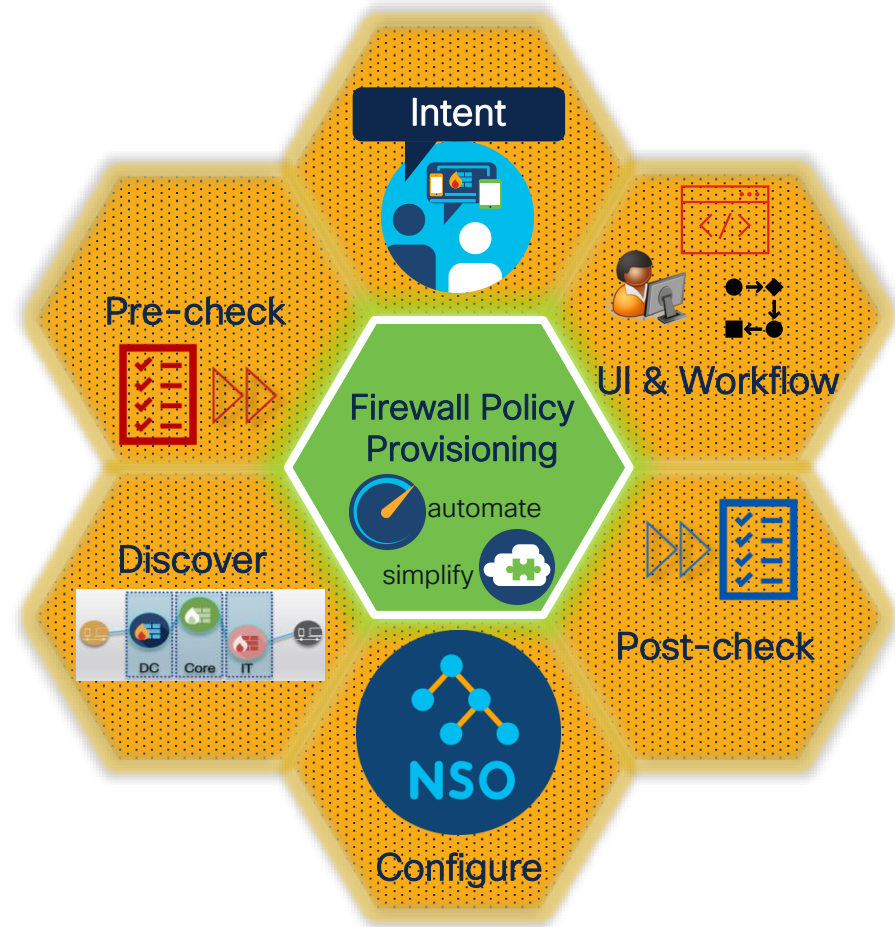


Post-checks

- re-execute PC



# Automation Concepts

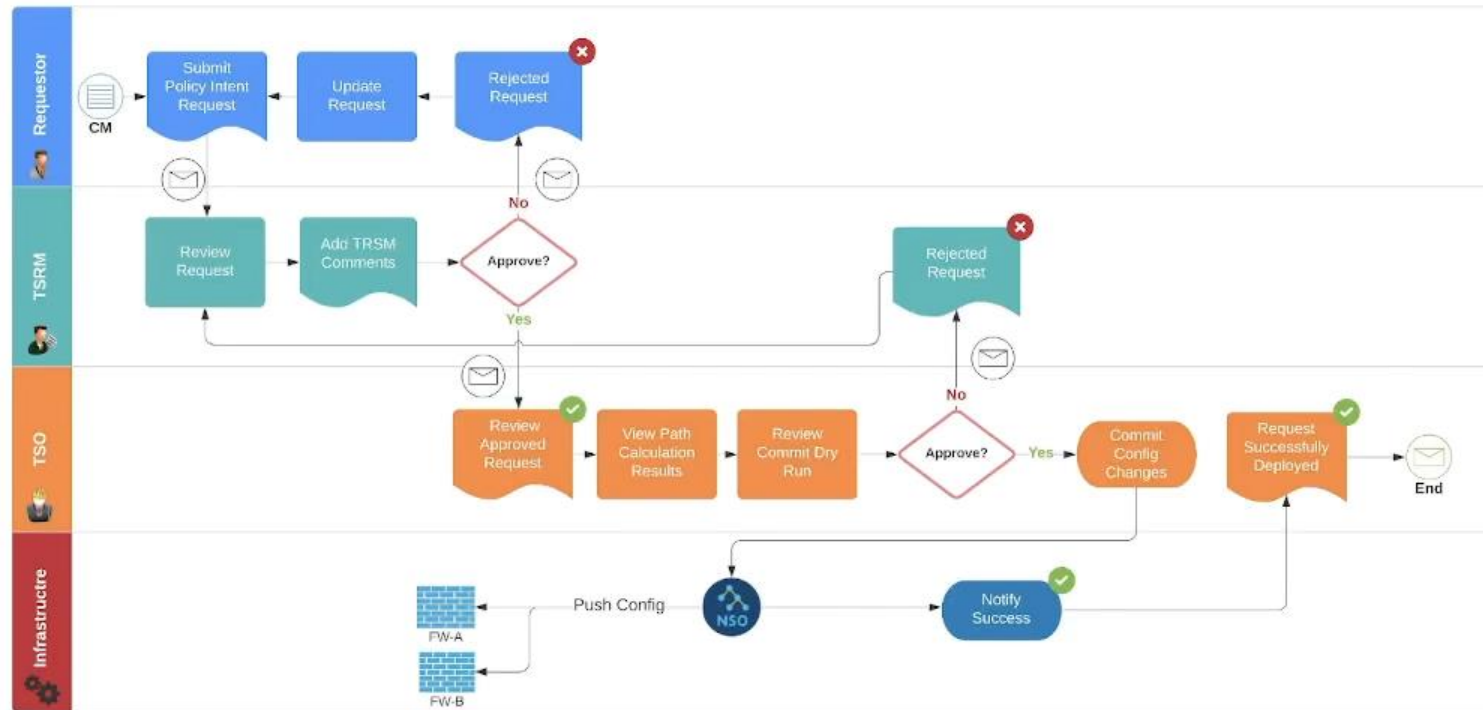




# Demo



# Communication Request Flow



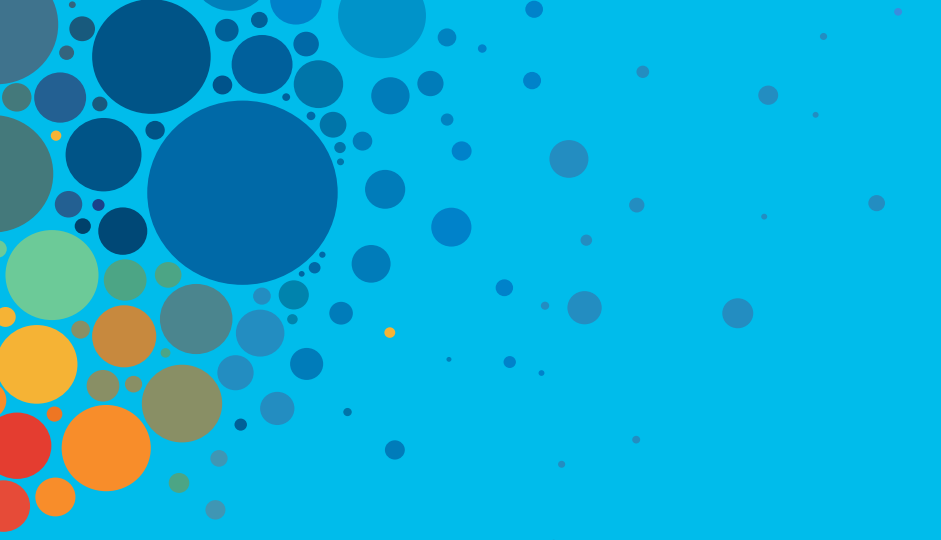
# Q&A



# Technical Session Surveys

- Attendees who fill out a minimum of four session surveys and the overall event survey will get Cisco Live branded socks!
- Attendees will also earn 100 points in the Cisco Live Game for every survey completed.
- These points help you get on the leaderboard and increase your chances of winning daily and grand prizes.





# Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at [www.CiscoLive.com/on-demand](https://www.CiscoLive.com/on-demand)



The bridge to possible

# Thank you

CISCO *Live!*



#CiscoLive