



# Ignite the Firewall

Secure Firewall Roadshow Ignite

Welcome

Oct 2024





# Welcome!

## Firewall Ignite Hands-On Training



Join at

<https://cs.co/FW-Ignite-Sign-in>

Please use your real name and email address + serial

This sign-in form is only being used to assign the hardware to you  
and track attendance.



# Firewall Ignite Roadshow – Customer Opportunity

*Identify firewall opportunities for collaborative development*

You will receive 10 additional AttackIQ Credits for each identified opportunity submitted.



<https://forms.office.com/r/TwXWHxBHCn?origin=lprLink>

# SWAG!



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Partner Confidential Information



# Yours after training...

- FTD 1010 for demo/lab use
- Personal SCC tenant with cdFMC provisioned
- Certificate of Completion\*
- AttackIQ Credits (great value)!
  - Credits subject to change, current allocations:
    - 10 for attending class
    - 10 for completing Certificate process
    - 10 for registering opportunity
- Memories to cherish



# Certificate of Completion Process

Thank you for attending the Firewall Ignite hands-on training! We hope you enjoyed the experience and can take the provided Cisco FTD 1010 to help you continue to learn, demo, and work with customers.

Obtaining your Certificate of Completion will entitle you to:

1. Keep your licensing active while continuing to operate your provided FTD1010 with SCC/cdFMC
2. Proof of completion that you may share as possible learning credits.
3. Additional AttackIQ credits provided.

## Process

1. Download and submit a final report from your Threat Lab of the AttackIQ breach and attack simulation.
2. Capture 1 simple screenshot after your FTD1010 has been deployed in your home/office lab.
3. Submit through this form:  
<http://cs.co/certificate-fw-ignite>

The next slides will demonstrate which screenshots to capture and use the form to submit.

Please allow for 10 business days to the certificate to be issued.



# Certificate of Completion Process

## AttackIQ Final Report

Upon completing the Threat Lab, download the final test results after completing the policy setup.

1. Login to your AttackIQ portal and select Analyze
2. View and download your final report

The screenshot shows the AttackIQ FLEX portal interface. On the left, a sidebar menu includes 'Getting Started', 'Home', 'Test Packages', and 'Analyze', with 'Analyze' being highlighted. The main area is titled 'Analyze' and contains fields for 'Label' and 'Description', along with a file upload section. Below this is a 'Credits' section showing 13 credits available. At the bottom is a table listing two security scans:

Label	File Name	Test Package	Test Point	Upload Date	Status	Action
Final Security Scan	PCAPCiscoSecure...	Cisco Secure Fire...	win10x64	03/04/2024 08:06 ...	Completed	<a href="#">VIEW</a>
Initial Security Scan	PCAPCiscoSecure...	Cisco Secure Fire...	win10x64	02/21/2024 15:49 ...	Completed	<a href="#">VIEW</a>

# Certificate of Completion Process

## AttackIQ Final Report

Upon completing the Threat Lab in dCloud, download the final test results after completing the FTD policy setup.

The report will be in PDF format and should include:

1. Executive summary
2. Results, which should show all with a green checkbox as illustrated.

This will validate you have successfully accessed AttackIQ and configured the FTD policy.

NOTE: You may continue to use AttackIQ for demo, lab, and POV purposes. This report is something you can share with customers to show the value of effective policy enforcement.

Results		
TABLE 1 Security Control Baseline - Cisco Secure Firewall Extended Baseline v2		
23/23 scenario executions were prevented		
Category	Scenario	Result
Security Intelligence	PCAP Replay - Web Access to Cisco Malware test site	✓
	PCAP Replay - 2022-05 ViperSoftX PowerShell Download Payload Requests	✓
	PCAP Replay - Web Access to Cisco Botnet test site	✓
	PCAP Replay - 2022-06 LokiBot HTTP Command and Control Traffic	✓
Intrusion	PCAP Replay - Hancitor CnC Web Communication	✓
	PCAP Replay - 2022-03 NanoCore RAT Custom TCP Command and Control Traffic	✓
	PCAP Replay - APT28 Zebrocy Delphi Downloader	✓
	PCAP Replay - NetWire C2 Communication	✓
URL Filtering	PCAP Replay - Web Access to Filter Avoidance site proxyway	✓
	PCAP Replay - Web Access to Gambling site PokerStars	✓
	PCAP Replay - Web access to Pornography site Pornhub	✓
	PCAP Replay - Web access to Hacking site www.hackthissite.org	✓
Application Filtering	PCAP Replay - Application WinSCP	✓
	PCAP Replay - Application TeamViewer	✓



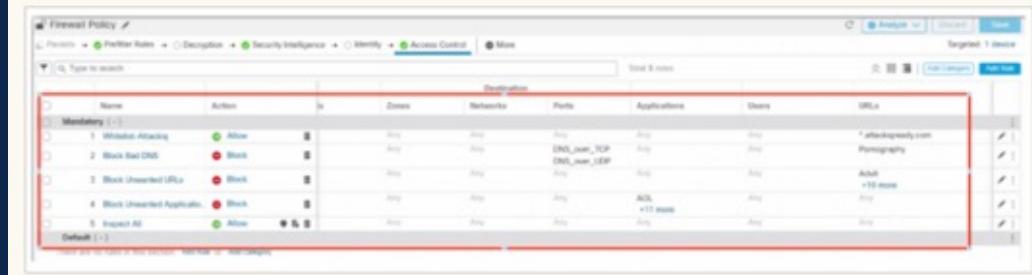
# NOTE: Highly Recommended

This is not required for your certificate of completion but is highly recommended.

 Additional Steps for POV/Customer Demo

To ensure additional configuration options within Access Control Policy, it is highly recommended that you follow the steps in the Task 2 of the [Threat \(Attack IQ\) - Training Outline](#) guide before you plan to present the demo to customers or leverage the firewall to secure your network.

A sample access control policy highlighting most of the capabilities of Secure Firewall Threat Defense looks as follows:



Name	Action	In	Zones	Networks	Ports	Applications	Shares	URLs
1 Whichever-Attacking	Allow	Any	Any	Any	Any	Any	Any	* attackready.com
2 Block Bad URLs	Block	Any	Any	Any	DNS_over_TCP	Any	Any	Pornography
3 Block Unwanted URLs	Block	Any	Any	Any	Any	Any	Any	Adult
4 Block Unwanted Applications	Block	Any	Any	Any	Any	Any	Any	>10 more
5 Inspect All	Allow	Any	Any	Any	Any	Any	Any	Any
Default								

Configure the policy defined in Task 2 from  
<https://secure.cisco.com/secure-firewall/docs/threat>

Repeat the steps to add a stronger policy on your FTD device.

 Lab Tasks

- Task 2 - Configure policies for NGFW1
  - Prefilter policy
  - DNS policy
  - Malware & File policy
  - Intrusion policy
  - Network Analysis policy
  - Decryption policy
  - Access Control policy



# Certificate of Completion Process

## Capture 1 screenshots

*After your FTD1010 has been deployed in your lab*

### Screenshot 1: Health report of your 1010

Once you deploy the 1010 in your home/office lab

1. Login to your SCC tenant  
<https://www.defenseorchestrator.com/> and navigate to **Security Devices**.
2. Select your 1010 FTD from the list.
3. Scroll on the right side and select **Health**.
4. Within the Health view, expand **System & Troubleshoot Details** from the top.
5. Change the timeframe to Last 1 week, as illustrated to the right.

The screenshot shows the Cisco Security Cloud Control interface. On the left, there's a sidebar with navigation links like Home, Multicloud Defense, Monitor, Insights & Reports, Events & Logs, Manage, Policies, Objects, and Security Devices (which is highlighted). The main area is titled 'Security Devices' and lists several devices: FPR-1010-LAB Chassis (selected and highlighted with a yellow box), FTD4225InstanceA FTD, NetSec TME Lab Universe Generation, RD Cloud Firewall FTD, RTP4225 Chassis, and SUC-FTDv-01\_30.1.100.36 FTD. To the right of the list is a 'Device Details' panel for the selected FPR-1010-LAB, showing its name, location, model (Cisco Firepower 9300 Supervisor), serial number (JAX010141E3), type (Chassis), and version (7.4.2). Below the list is a 'Device Actions' section with options like 'Check for Changes', 'Workflows', and 'Remove'. A large orange arrow labeled '1' points to the 'Security Devices' link in the sidebar. Another orange arrow labeled '2' points to the selected device in the list. A third orange arrow labeled '3' points to the 'Health' button in the 'Device Actions' panel. A fourth orange arrow labeled '4' points to the 'System & Troubleshoot Details' tab in the expanded Health view at the bottom. A fifth orange arrow labeled '5' points to the 'Last 1 week' timeframe selector in the same view.

This screenshot shows the expanded 'Health' view for the FPR-1010-LAB chassis. At the top, it says 'Health: 1010-01LAB' and 'View System & Troubleshoot Details'. Below that is a navigation bar with tabs: Overview (which is selected), CPU, Memory, Interface, Connections, Snort, ASP Drops, and a plus sign. To the right of the tabs is a 'Last 1 week' button with a count of 5. A yellow arrow labeled '4' points to the 'System & Troubleshoot Details' tab, and another yellow arrow labeled '5' points to the 'Last 1 week' button.

# Certificate of Completion Process

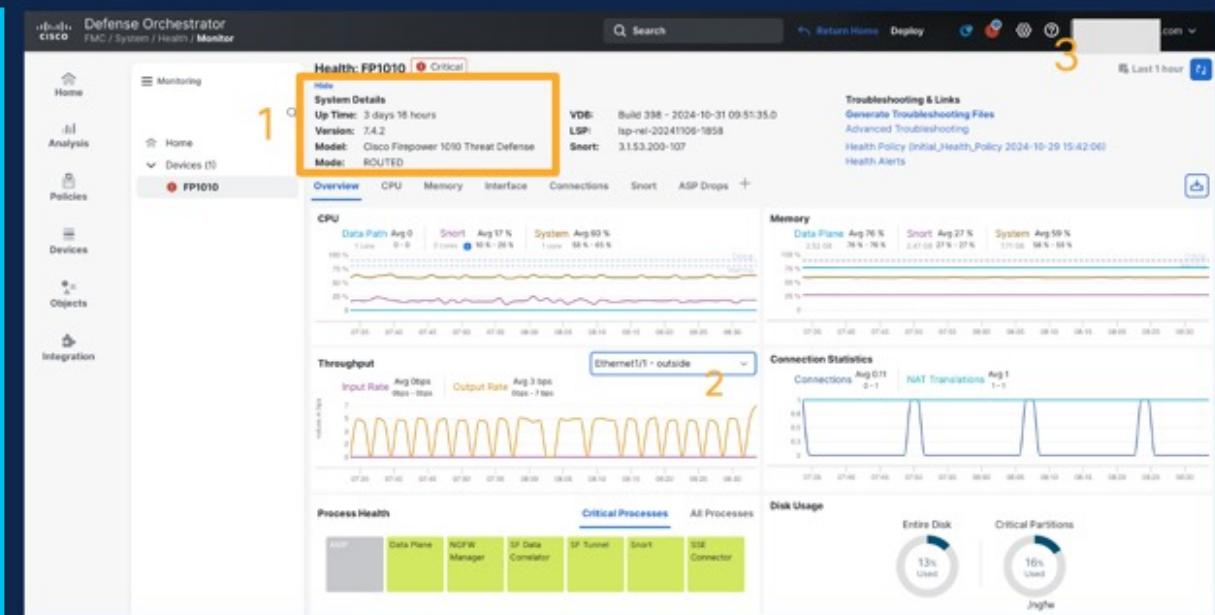
## Capture 1 screenshots

*After your FTD1010 has been deployed in your lab*

### Screenshot 1: Health report of your 1010

Take a screenshot of the Health report reflecting below

1. You are running 7.4.1 or greater.
2. Throughput and traffic is passing through the 1010 in your home/office lab.
3. Your Cisco login, as illustrated to the right.



# Certificate of Completion Process

## Submit Form

*After your FTD1010 has been deployed in your lab*

Please complete all relevant fields in the form including:

Submit through this form: <http://cs.co/certificate-fw-ignite>

1. Select the category: **Firewall Ignite Completion Certificate**
2. Stage: N/A
3. Query: use text like below

*Attached is my proof of completion for the Firewall Ignite training on [date] at [location] if you could issue my certificate of completion*

4. Drag-and-drop or upload the file(s) containing screenshots validation completion.
5. Submit the form

Please allow for 10 business days for the certificate to be issued.

Category \*  
Please visit the Cisco Fire Jumper FAQ - 2023 located at the first orange link to the left to find more information before making any submissions.

1 Firewall Ignite Completion Certificate

Are you a Partner or Cisco Employee

If Applicable pls specify Partner/Country

Are you submitting this query on behalf of someone else? \*

No

First Name \*

Cisco.com User ID (CCD ID) \*

The Cisco.com User ID (CCD ID) is different from the Cisco Testing ID (CSCO #), CCIE # and Contact ID. If you look up your contact information in [Partner Self Service](#), you will find the Cisco.com User ID in the details section of Partner Self Service right above the "Added On" field. For Cisco employees, typically this is the beginning of your email address without the @Cisco.com domain.

2

Last Name \*

Email Address \*

Stage \*

N/A

GED \*

3

Country \*

UNITED STATES

Role \*

SE/Pre-Sales

Company Name \*

4

Company BEGEIDH

Cisco Partner TSA Contact (Name & Email)

Query \*

Please provide a detailed explanation of your query.

3 Please issue my certificate of completion for the Firewall Ignite training on [date] at [location]

File Uploaded

Please provide screenshots that will better explain your query. Such as screenshots of your status, completion or certification. For First-Time Elite Validations, or Elite Renewal Validations, please upload the completed Self-Tracker as this is mandatory.

4

11-18-18-00  
11-18-18-00  
11-18-18-00

5

Send me a copy of my responses

Submit



# Webex STUDENT ROOM



*Webex Teams*

<https://eurl.io/#abcdefg>



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Partner Confidential Information

Cisco Security | 13

# Timeline

Topic	Speaker(s)	Time
Welcome & Introduction	Proctor	9:00am - 9:15am
Goals and environmental overview	Proctor	9:15am - 9:30am
Lab Work (1010) – Getting Started Guide	Proctor	9:30am - 10:15am
Vision and Strategy	Proctor	10:15am - 11:00pm
Lab Work (dCloud) – Device Registration and Setup	Proctor	11:00am - 12:00am
LUNCH		12:00pm - 12:45pm
Lab Work – Preparing for Customer Demos (Finishing 1010 config)	Proctor	12:45pm - 1:45pm
Lecture – Lab Overviews & Call to Action	Proctor	1:45-2:15
Lab Work (dCloud) – Software Defined Area Network (SD-WAN)	Lab work	2:15 pm - 5:00pm
Lab Work (dCloud) – Threat with AttackIQ	Lab work	2:15 pm - 5:00pm
Lab Work (1010) – Remote Access VPN (optional)	Lab work	2:15 pm - 5:00pm
* Survey * Take notes throughout the day	ALL	Before you leave

**NOTE:** You can take breaks as you need them. There is some wait time in labs that allows for natural breaks.



# Why are we here?

 Get to grips with why firewalls are important and why Cisco is a top choice.

 Show you how Cisco's Firewall stands out from others.

 Teach you how to set up Cisco's firewall.

 Equip you with the tools you need to demonstrate Cisco's firewall to customers.

 Gather your feedback and measure the expectations.

# Did you do your homework ☺

Raise your hand if you didn't complete these



1. You must have a Cisco Account. If needed, sign up at <https://id.cisco.com>.
2. You must have a Security Cloud Control tenant. If needed, request one at <https://getcdo.com>.
3. Once provisioned, provision Cloud-Delivered FMC. Login to SCC at <https://defenseorchestrator.com> then:
  - a) Go to *Administration > Integrations > Firewall Management Center*.
  - b) Click *Enable Cloud-Delivered FMC*.
4. Note SCC Tenant Name (top-right of screen in SCC) which is needed during Slido registration.
5. AttackIQ account creation: Check your registered email for this information. Use <https://firedrill.attackiq.com> to find your custom URL if you loose.

cisco Defense Orchestrator

Search

Hide Menu

Dashboard

Multicloud Defense

Inventory

Configuration

Policies

Objects

VPN

Events & Monitoring

Analytics

Change Log

Jobs

Tools & Services

You are in a free trial of CDO with 30 days left.

Welcome to Cisco Defense Orchestrator

Quick Actions

Get started

Multicloud Defense

Connect a cloud account  
Gain visibility and control of what's happening in your cloud environment while ensuring they are managed securely.  
[Learn more](#)

CDO Full Version

Thank you for choosing Cisco Defense Orchestrator! Please enter your sales order number to begin using the full version of CDO.

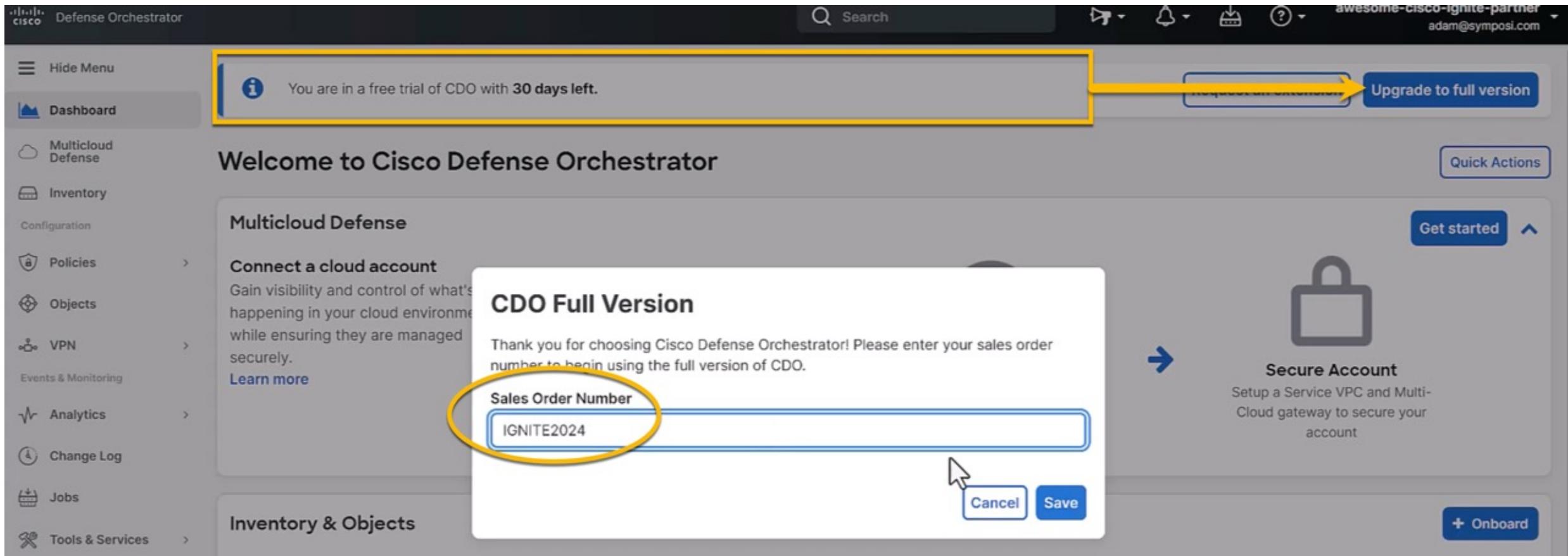
Sales Order Number

IGNITE2024

Secure Account

Setup a Service VPC and Multi-Cloud gateway to secure your account

Onboard



A screenshot of the Cisco Defense Orchestrator (CDO) web interface. At the top, there's a banner stating 'You are in a free trial of CDO with 30 days left.' with a yellow arrow pointing to a 'Upgrade to full version' button. Below the banner, the title 'Welcome to Cisco Defense Orchestrator' is displayed. On the left, a sidebar lists various menu items like 'Multicloud Defense', 'Inventory', and 'Analytics'. In the center, a modal window titled 'CDO Full Version' appears, prompting the user to enter a sales order number to begin using the full version. The input field contains the text 'IGNITE2024', which is circled in yellow. At the bottom of the modal are 'Cancel' and 'Save' buttons, with a cursor hovering over the 'Save' button. To the right of the modal, there's a section titled 'Secure Account' with a brief description and an 'Onboard' button.

# PARTNERS ONLY

Select **Upgrade to Full Version** within the trial banner enter **IGNITE2024** within the prompt.



← ⏪ 🔍 https://www.defenseorchestrator.eu

CDO Feed Cheat Concur LH Issues CDO-Jira CDO-Wiki EPICs Defects Ops Board MMFs LabSite BetaFeedback Product - CDO Deployments > Other favorites

cisco Defense Orchestrator Search

You are in a free trial of CDO with **30 days left.**

Request an extension Upgrade to full version

Hide Menu Dashboard Multicloud Defense Inventory Configuration Policies Objects VPN Events & Monitoring Analytics Change Log Jobs Tools & Services Settings

Welcome to Cisco Defense Orchestrator

Quick Actions Get started

**Multicloud Defense**

**Connect a cloud account**  
Gain visibility and control of what's happening in your cloud environments while ensuring they are managed securely.  
[Learn more](#)

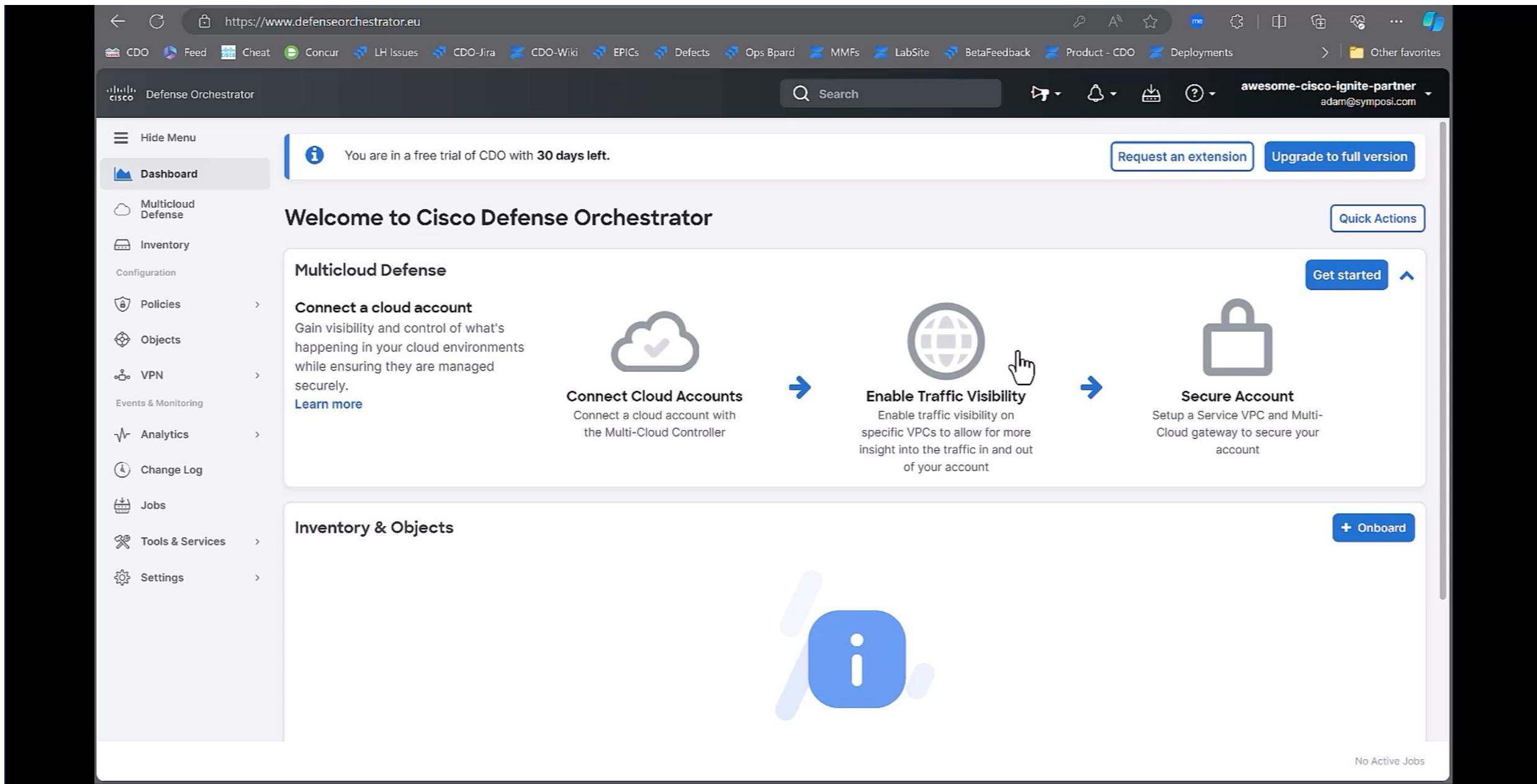
**Connect Cloud Accounts**  
Connect a cloud account with the Multi-Cloud Controller

**Enable Traffic Visibility**  
Enable traffic visibility on specific VPCs to allow for more insight into the traffic in and out of your account

**Secure Account**  
Setup a Service VPC and Multi-Cloud gateway to secure your account

**Inventory & Objects** + Onboard

No Active Jobs



Reminder: Perform these steps to have licensing applied to your Smart Account as shared in the Know Before You Go

1. Create 1 case using the text to the right:  
<https://cep.cloudapps.cisco.com/#/pov>
2. Use request type and description as shown
3. Edit and paste in the description to include **your Smart Account information** and submit.



**Request type:**

- Primary Technology = Network Security
- Title = Licensing for Firewall Ignite Training

**Description:**

Lab licenses for Firewall Ignite training program.

Please deposit the below lab licenses for the Firewall Ignite training program into my smart account.

Product type [FTD & AnyConnect]

PIDs:

- L-AC-APX-LIC-SMART= (Remote Access VPN) - Quantity 1
- L-FPR1010T-TMC= (Threat/Malware/URL Features) Quantity 1
- Sensor type: [Cisco Firepower Threat Defense Hardware 1010 Appliance]
- Smart Account Domain ID [----.com]
- Smart Account [-----]
- Smart Virtual Account [-----]
- Duration: 365 Days

# Within 30 days after training...



1. Install your new shiny 1010 at your home office, lab, or anywhere really
2. Check in with your firewall regularly, get to know it, did it find threats?
3. Perform customer and colleague demos with your firewall and your classy AttackIQ licenses

After 45 days of neglect...



The SCC system automatically will deprovision stale accounts every 45 days

The cdFMC will de-activate when no devices are connected for roughly 45days, your SCC instance will persist.

# Overview

Training Objective: Equip participants with hands-on experience in the streamlined management of Cisco Firewalls and provide a deep-dive into the platform's unique features and capabilities.

Lab Scenarios Included:

1. [Getting Started Guide](#) 
2. [Device Registration and Initial Setup](#)
3. [Preparing for Customer Demos](#) 
4. [Software Defined Wide Area Network \(SD-WAN\)](#)
5. [Threat \(Attack IQ\)](#)
6. [\(Optional\) Remote Access Virtual Private Network \(RAVPN\)](#) 

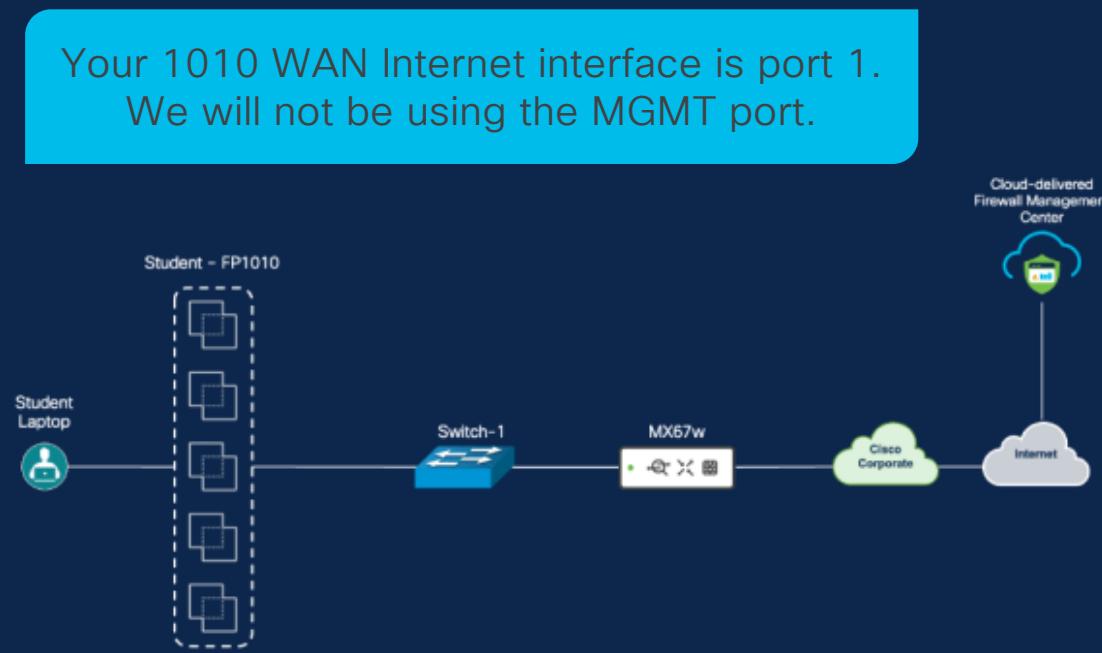
NOTE: The labs for your 1010 are separate from what you will be doing in dCloud



# Lab Environment Overview

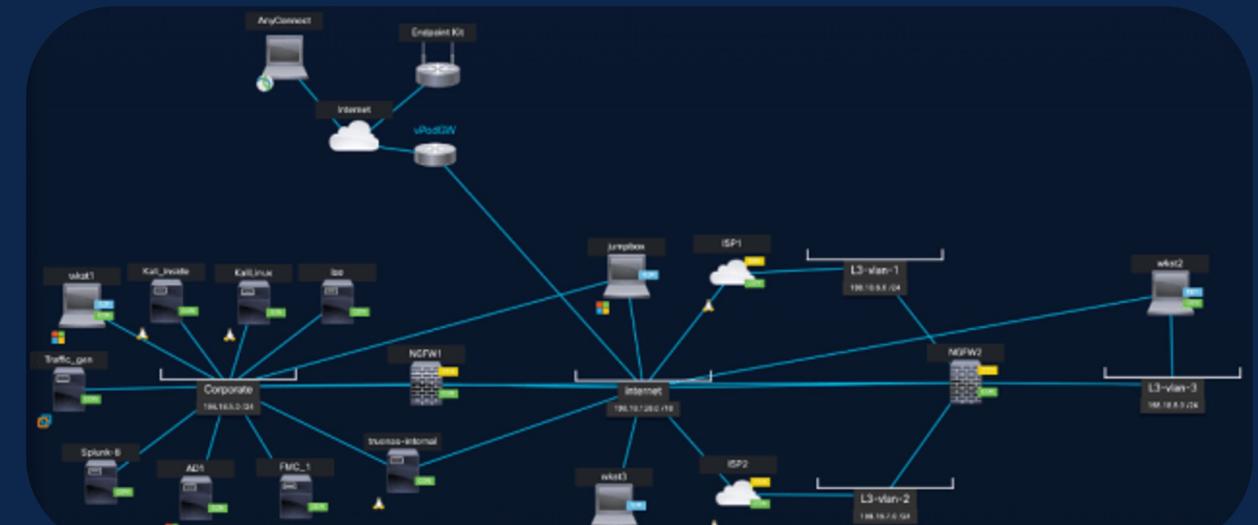
# Topology Overview

Topology 1 - On-Site



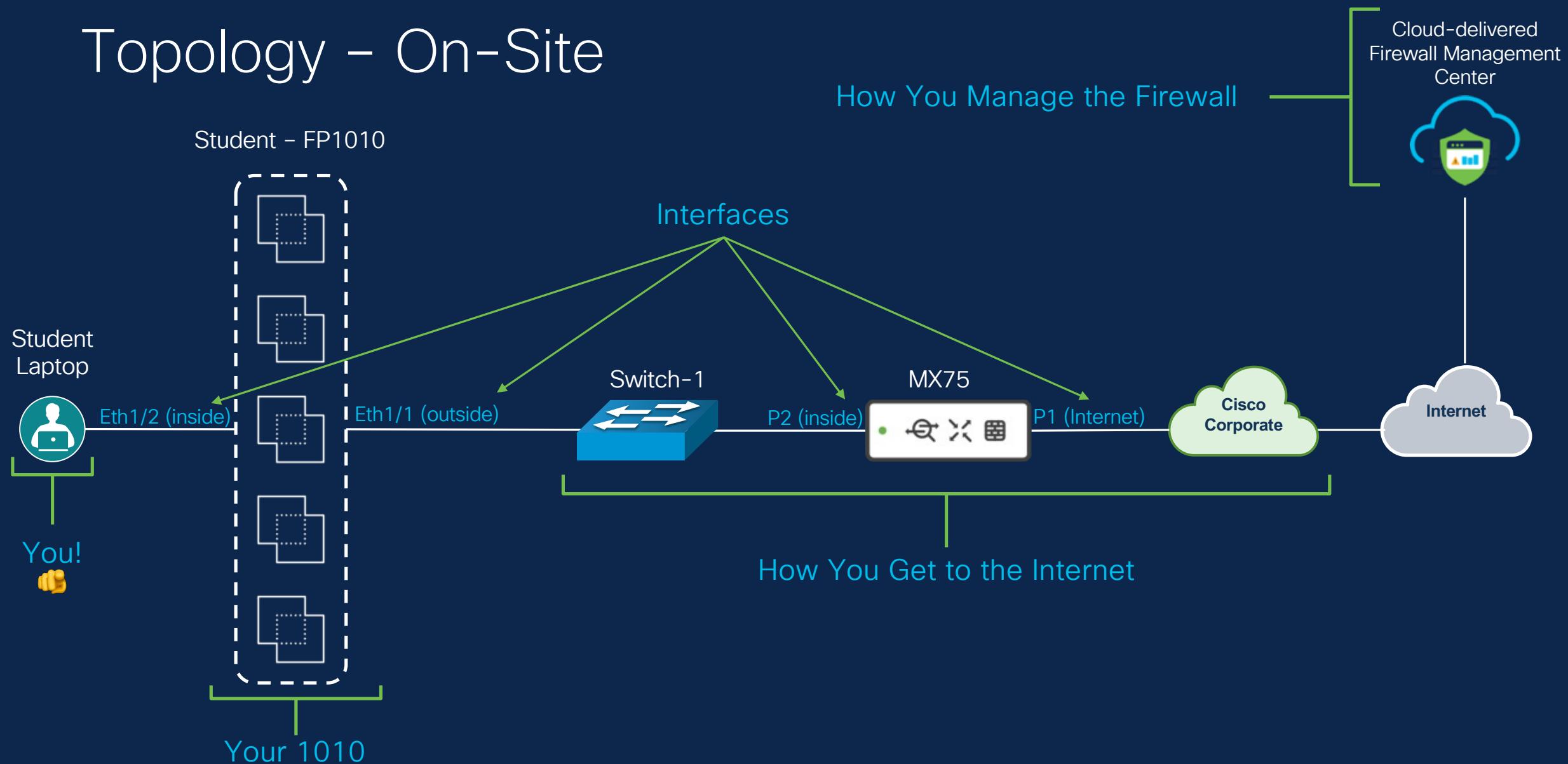
Your 1010 WAN Internet interface is port 1.  
We will not be using the MGMT port.

Topology 2 - dCloud



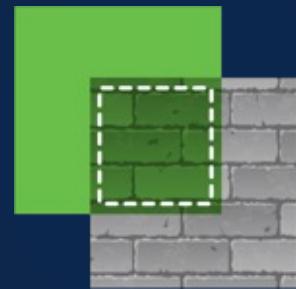
# Firepower 1010

# Topology - On-Site



# Cisco Firepower 1010

A high-performance compact firewall designed for the Small to Medium Business (SMB)



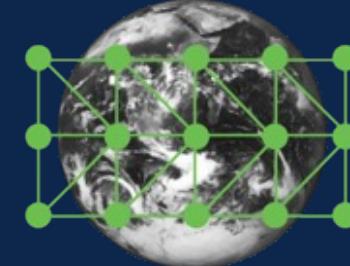
## Intelligence

Provide Cisco Talos threat intelligence, automatically updated daily



## Visibility

Simplify management, with visibility across your networks



## Integrate Network & Security

Transform your network into an extension of your security architecture

# Times have changed...

With multiple perimeters to protect



Cisco Secure Firewall

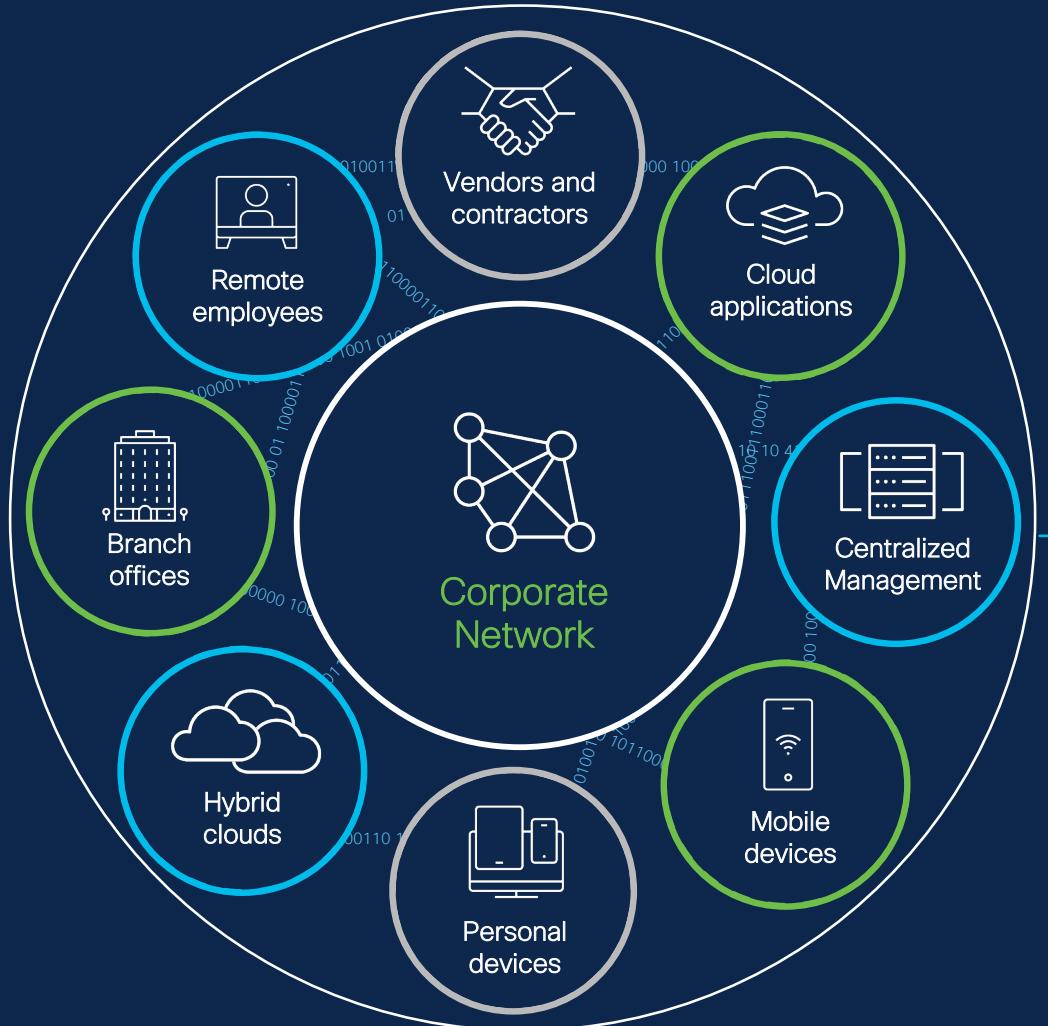


Corporate Network

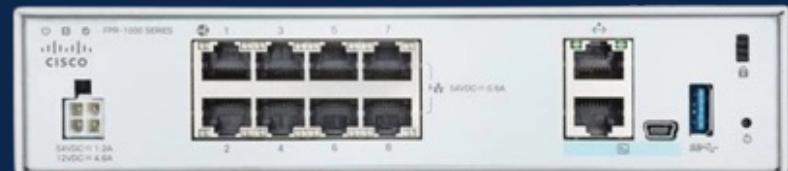


... as a result, the typical environment now requires numerous enforcement points

# Ignite the Firewall



Firepower 1010



Onboard



Upgrade



Prepare

# Cisco dCloud

# What is Cisco dCloud?

## Cisco dCloud

A cloud-based virtual demonstration offering

## Demonstrations

Focused on Cisco products and solutions that are  
Packaged, pre-configured, and scripted.

## Customizable

Full administrative control of your demo

## Cisco dCloud Data Centers

US (East & West), London,  
Sydney, & Singapore

[dCloud.cisco.com](https://dCloud.cisco.com)

## Availability

24x7 Access with Cisco.com credentials

## Any Use Case

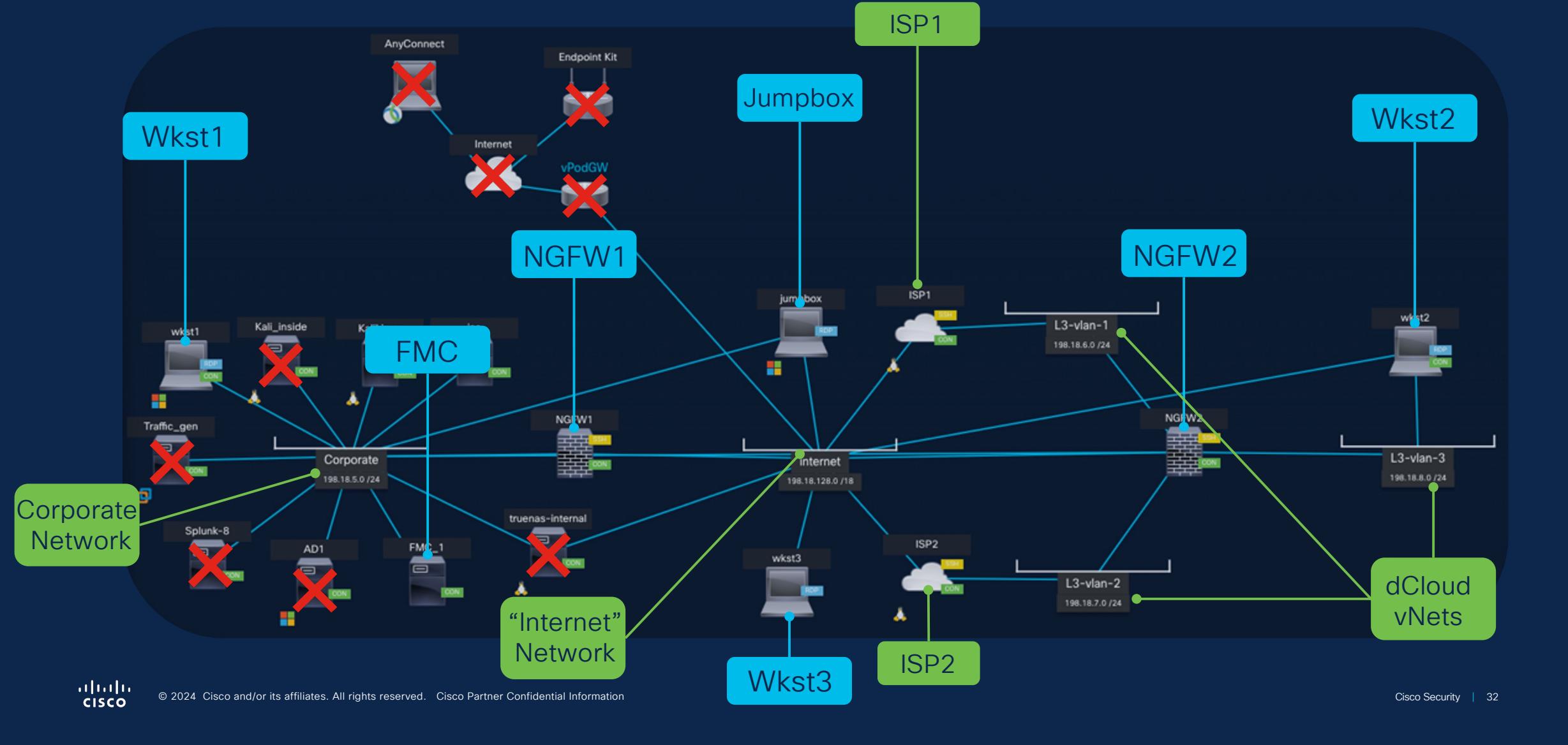
See only or get hands-on

## Supported

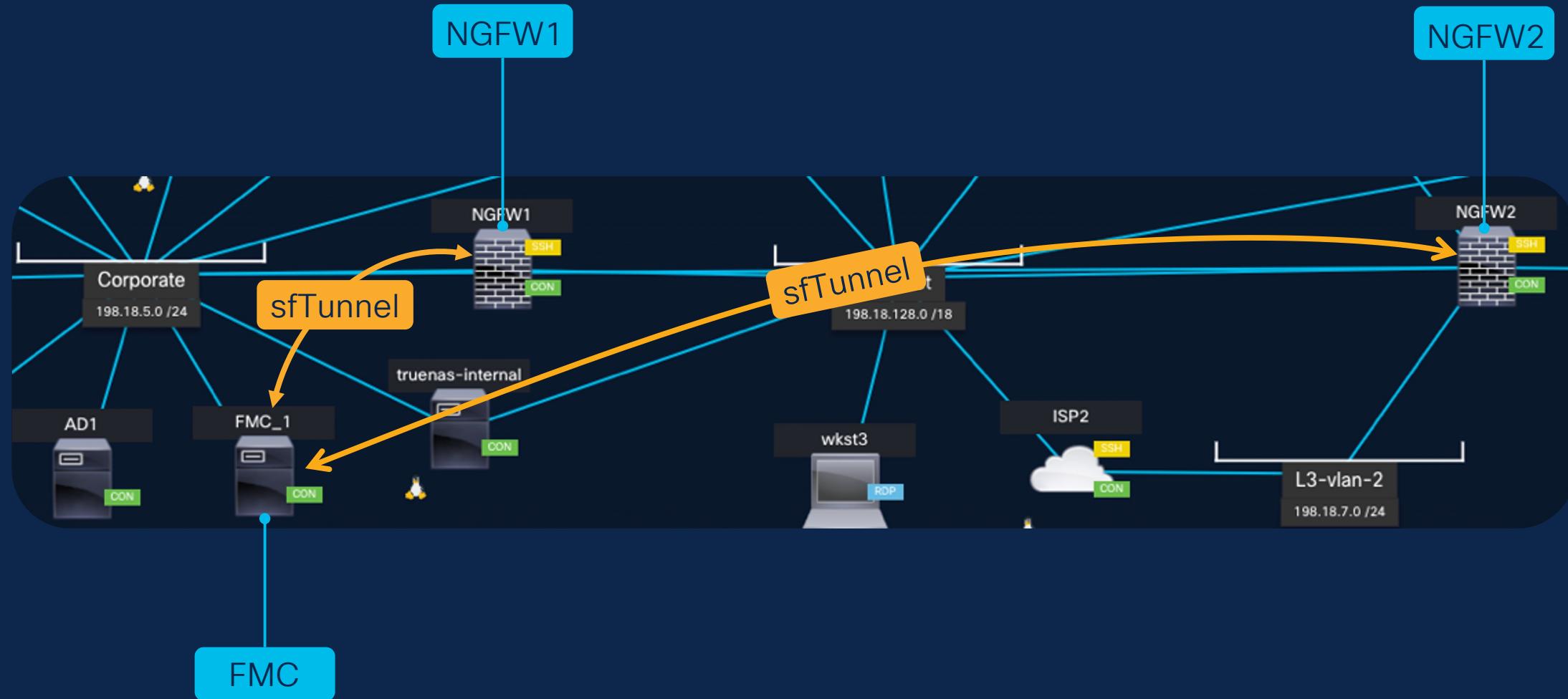
All demos are completely tested & validated  
User feedback encouraged



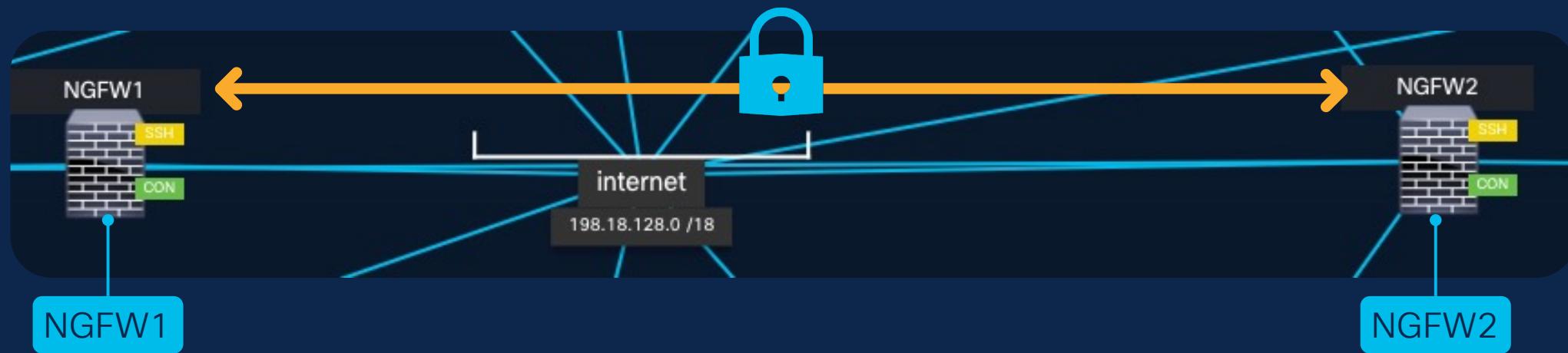
# Cisco dCloud - Topology



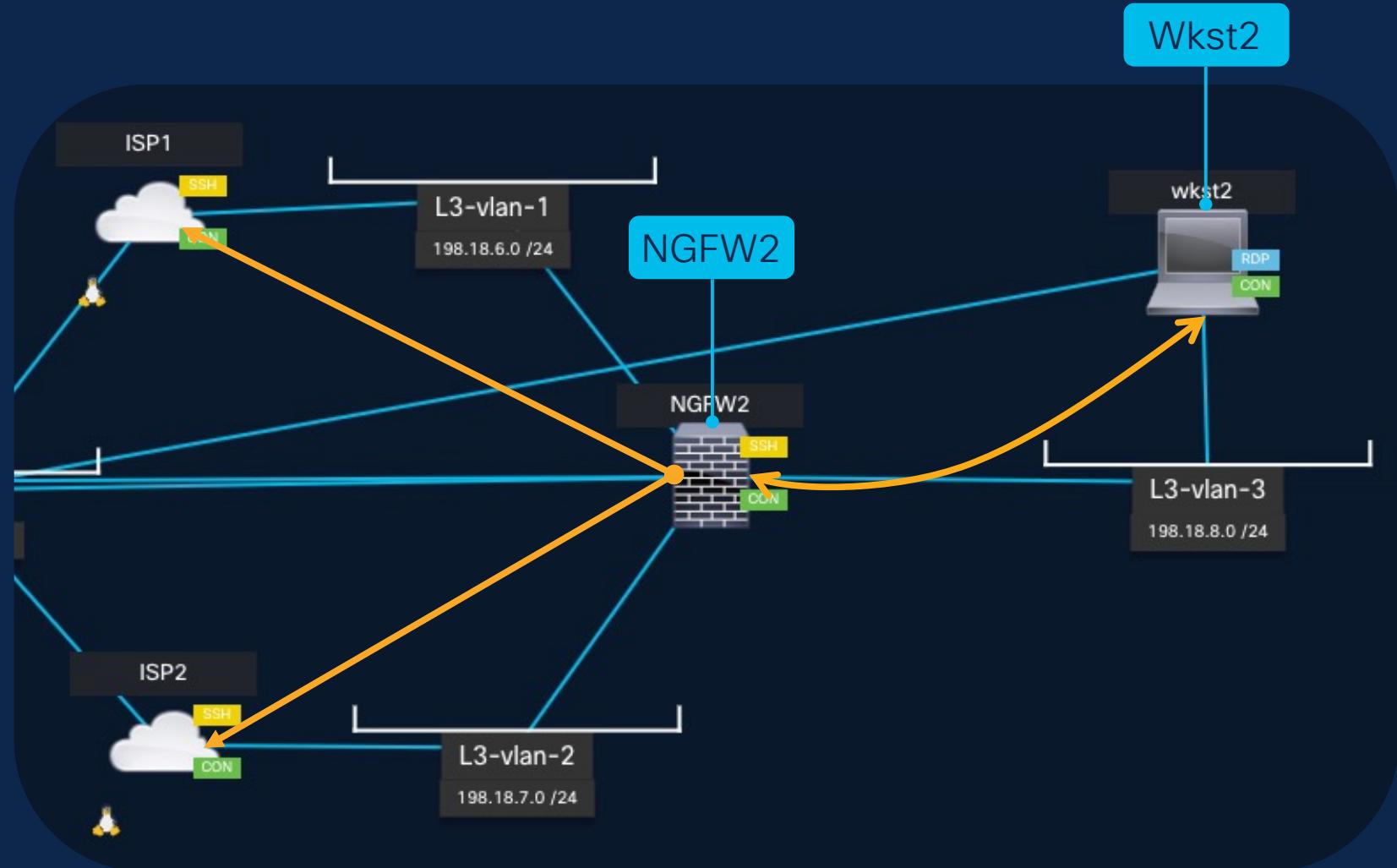
# Cisco dCloud – Device Registration



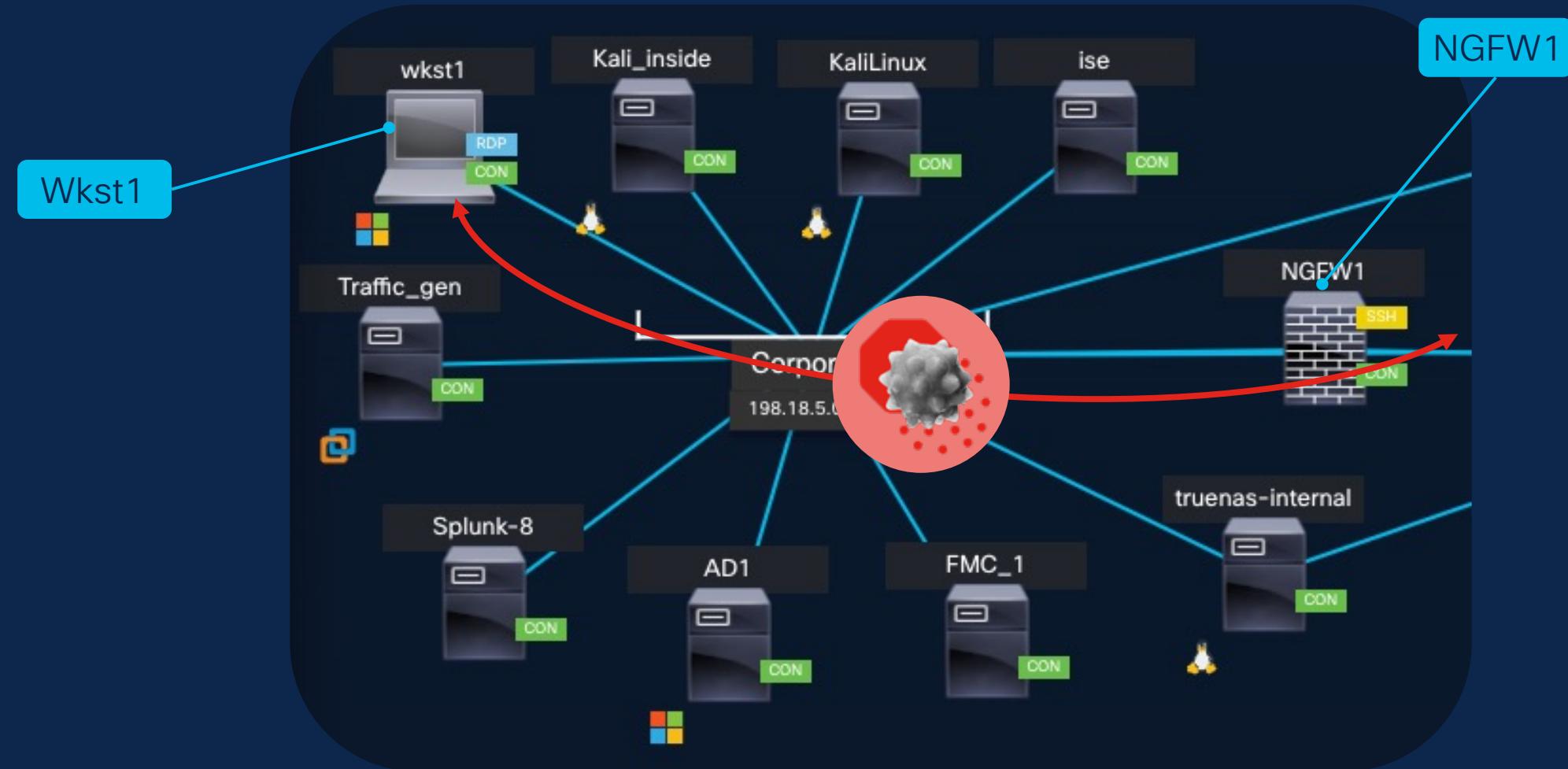
# Cisco dCloud – SDWAN Branch to Site Secure VPN



# Cisco dCloud - SD-WAN App Aware Policy-based Routing



# Cisco dCloud – Threat Efficacy with AttackIQ



# Cisco dCloud

The screenshot shows the Cisco dCloud Session Inventory interface. At the top, there is a navigation bar with the Cisco logo, the title "dCloud Session Inventory", the session name "Cisco Secure Firewall Ignite Roadshow Lab v1", and a toggle switch. Below the navigation bar is a toolbar with several buttons: "Info", "End", "Save & End", "Reset", "Rename", "Documentation", and a timestamp "02:42:42". Two buttons, "End" and "Save & End", are highlighted with a red rounded rectangle. The main content area displays session details for "Cisco Secure Firewall Ignite Roadshow Lab v1" with a start time of "09-May-2024 08:15", an end time of "09-May-2024 11:15", a session ID of "1138402", and a virtual center count of "10". Below this, there is a row of action buttons: "Info", "End", "Save", "Edit", "Share", "Endpoints", and a "View" button. The "End" and "Save" buttons are also highlighted with a red rounded rectangle.

**CAUTION : Both “END” and “SAVE” will BOTH END YOUR SESSION.**

# Getting Started Guide

What



cdFMC Validation | Low Touch Provisioning | Upgrading the Firewall

Why



Required for managing your 1010 | Simplified Onboarding | Enhanced features gained through upgrade

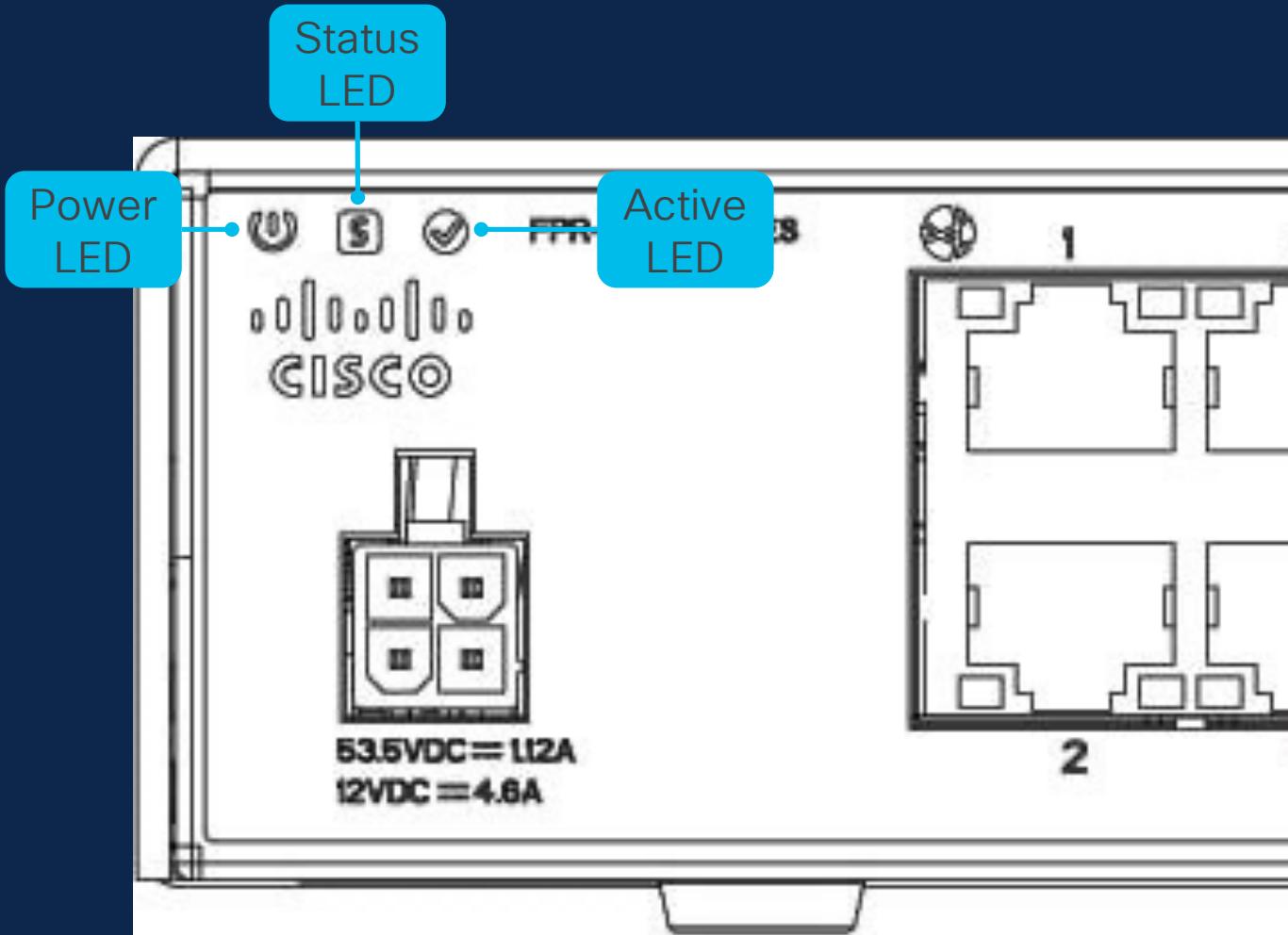
How



Via the SCC Web Interface | Serial Number Method | Unattended Mode

# Firepower 1010: Is it connected?

NOTE: Your WAN Internet interface is port 1 – we do not use the MGMT port



- Three LEDs:
  - Power
  - Status
  - Active
- Normal Operation:
  - Power – Solid Green
  - Status – Solid Green
    - Initially, Green flashing slowly
  - Active – Solid Green
- Contact your proctor if...
  1. Status LED – Solid Amber
  2. Status LED – Flashing green and amber

# cdFMC: Is it enabled?

Navigation: SCC > Administration > Integrations > Firewall Management Center

NOTE: You may find you need to navigate away or log out and back in for the cdFMC Status column to refresh

The screenshot shows the SCC interface with the 'Services' tab selected. On the left, the navigation menu includes 'Home', 'Monitor' (with 'Insights & Reports' and 'Events & Logs' sub-options), 'Manage' (with 'Policies', 'Objects', 'Security Devices', 'Secure Connections', and 'Administration' sub-options), and the current 'Administration' option which is highlighted with a blue border. The main content area displays the 'FMC' tab selected under 'Secure Connectors'. A search bar at the top allows searching by device name, IP address, or serial number. Below the search bar is a table with the following data:

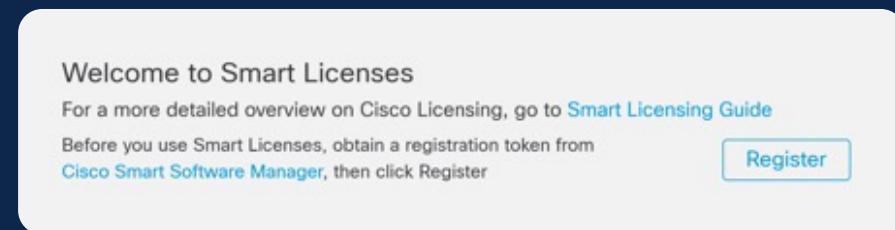
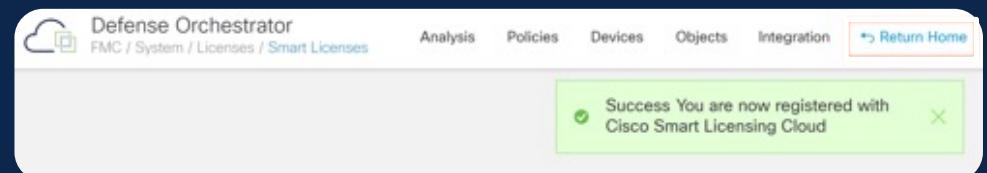
Name	Version	Devices	Type	Status	Last Heartbeat
Cloud-Delivered FMC	20241029	4	Cloud-Delivered FM	Active	11/10/2024, 12:12:20

A large yellow thumbs-up emoji is overlaid on the right side of the table.



# cdFMC: Is it licensed?

Navigation: SCC > Administration > Integrations > Firewall Management Center > Smart Licenses

A screenshot of the 'Smart Licensing Product Registration' dialog. It asks for a 'Product Instance Registration Token' and has an optional checkbox for overriding an existing instance. It also provides instructions for copying the token from Cisco Smart Software Manager. A note at the bottom states an internet connection is required, with 'Cancel' and 'Apply Changes' buttons below.

# Cloud Assisted Provisioning

Low Touch Provisioning

Low-skilled branch staff



Device **Auto onboards** upon bootup



No pre-configuration



Onboarding using **Serial Number**



# Upgrade! (1/2)

Navigation: SCC > Administration > Integrations > Firewall Management Centre > Device Overview > System > Product Upgrades

The screenshot shows the 'Product Upgrades' section of the Cisco Defense Orchestrator interface. On the left, a sidebar lists navigation options: Home, Analysis, Policies, Devices, Objects, and Integration. The main area displays a 'System Overview' box with a message about Threat Defense (4 devices) and a link to Device Management. Below this is a section titled 'Available Upgrade Packages' with a table listing four packages. The table columns are: Upgrade, Release Date, Required Minimum Version, Availability, and Actions. The first package, '7.6.0-113', is marked as 'Suggested'. A large green button labeled 'Click Download' with a green arrow points to the 'Actions' column of the first row.

Upgrade	Release Date	Required Minimum Version	Availability	Actions
7.6.0-113	2024-09-13	7.1.0	Available for download	<a href="#">Download</a>
7.4.2-172 ★ Suggested	2024-07-29	7.0.0	Available for download	<a href="#">Download</a>
7.4.1.1-12	2024-04-05	7.4.1	Available for download	<a href="#">Download</a>
7.4.1-172	2023-12-13	7.0.0	Available for download	<a href="#">Download</a>

# Upgrade! (2/2)

Navigation: SCC > Administration > Integrations > Firewall Management Centre > Device Overview > System > Product Upgrades

The screenshot shows the 'Product Upgrades' section of the Cisco Defense Orchestrator interface. On the left, there's a sidebar with icons for Home, Analysis, Policies, Devices, Objects, and Integration. The main area has a 'System Overview' section with a message about Threat Defense and a link to Device Management. Below it is a 'Available Upgrade Packages' section with a table. The table has columns for Upgrade, Release Date, Required Minimum Version, Availability, and Actions. It lists four packages: 7.6.0-113 (Release Date 2024-09-13, Version 7.1.0, Available for download, Download button), 7.4.2-172 (Suggested, Release Date 2024-07-29, Version 7.0.0, Available for download, Download button), 7.4.1-12 (Release Date 2024-07-29, Version 7.0.0, Available for download, Download button), and 7.4.1-172 (Release Date 2024-07-29, Version 7.0.0, Available for download, Download button). A green callout bubble points to the 'Upgrade' button next to the 7.4.2-172 package. Another green callout bubble at the bottom left contains the text: 'REMINDED: Refer to the earlier section on which screenshots to save for your Certificate of Completion after your upgrade completes'.

Upgrade	Release Date	Required Minimum Version	Availability	Actions
> 7.6.0-113	2024-09-13	7.1.0	Available for download	Download
> 7.4.2-172 ★ Suggested	2024-07-29	7.0.0	Available for download	Download
> 7.4.1-12	2024-07-29	7.0.0	Available for download	Download
> 7.4.1-172	2024-07-29	7.0.0	Available for download	Download



# Important!



Unlike an ASA, there is no running config or startup config.

With FTD, there are several databases and services running that must be shut down safely before removing power.

\* Yes, even for troubleshooting \*

# Important

The screenshot shows the Cisco Defense Orchestrator interface. On the left sidebar, the 'Devices' icon is highlighted with a green box. The main content area is titled 'Device Management'. A table lists devices, with one row for 'FPR-1010-LAB' selected and highlighted with a green box. The 'Actions' column for this row also has a green box around it. Below the table, a detailed view for 'FPR-1010-LAB' is shown, including tabs for General, License, and System. In the bottom right corner of the system details, a modal dialog box titled 'System Shutdown' is displayed, asking 'Are you sure you want to shutdown the system?'. The 'Yes' button in this dialog is also highlighted with a green box.

Defense Orchestrator  
FMC / Devices / Device Management

Devices

Device Management

Template Management

NAT

QoS

Platform Settings

FlexConfig

Certificates

Analysis

Policies

Objects

Integration

Home

Search

Return Home Deploy

Migrate Deployment History

Search Device Add

Download Device List Report

Name Model Version Chassis Licenses Access Control Policy Auto RollBack

FPR-1010-LAB Snort 3

SDWAN (1)

Firepower 1010 Threat Defense 7.4.1 N/A Essentials, IPS (3 more...) None

FPR-1010-LAB

Cisco Firepower 1010 Threat Defense

Device Interfaces Inline Sets Routing DHCP VTEP SNMP

General Name: FPR-1010-LAB License Essentials: Yes System Model: Cisco Firepower 1010 Threat Defense

General Name: FPR-1010-LAB Transfer Packets: No Troubleshoot: Log CLI Routed Mode: None Compliance Mode: TLS Crypto Acceleration: Disabled Device Configuration: Import Export OnBoarding Method: Download Registration Key

License Essentials: Export-Controlled Features: Malware Defense: System Shutdown Are you sure you want to shutdown the system? No Yes

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Partner Confidential Information

Cisco Security | 46

Wait for 5 minutes after the steps to ensure the system has shut down successfully.  
**TIP:** Watch for the ethernet interface lights to shut off.

# Lab Time!

## First Steps Guide

- <https://secure.cisco.com/secure-firewall/docs/first-steps>



## Getting Started Guide

- <https://secure.cisco.com/secure-firewall/docs/getting-started-guide>



NOTE: Many of the Red (!) can safely be ignored. When there is nothing connected to the management0 or LAN interfaces, these will flag Red Health alerts.

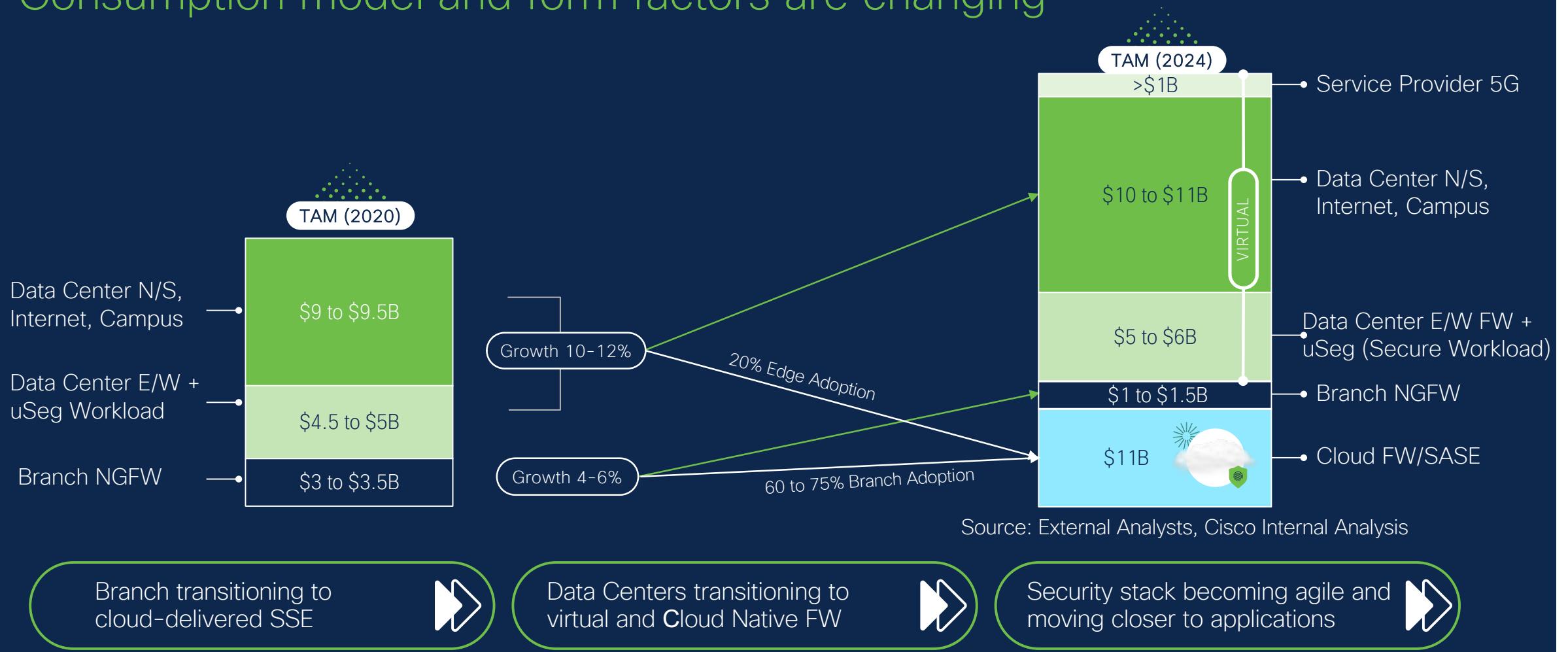
The screenshot shows the Cisco Defense Orchestrator interface. On the left, a sidebar has tabs for Home, Analysis, Policies, Devices, Objects, and Integration. The main area displays a table of devices. At the top of the table, there are filters: 'View By' (set to 'Group'), 'All (1)', 'Error (1)', 'Warning (0)', 'Offline (0)', 'Normal (0)', and 'Deployment Pending (0)'. Below the table, under 'Devices', there is one entry: 'FP1010 Snort 3 N/A - Routed' with model 'Firepower 1010 Threat Defense', version '7.4.2', and chassis 'firepower'. To the right of the table, a 'Health' section shows '2 total', '1 warning', '1 critical', and '0 errors'. A detailed view of the 'FP1010' device shows two alerts: 'Chassis Status FTD' (warning) and 'Interface Status' (critical). The alert for 'Interface Status' states: 'CPU Temperature 85 C is Warm Chassis Temperature' and 'Interface 'Ethernet1/1' is not receiving any packets'.



# Cisco's Vision & Strategy

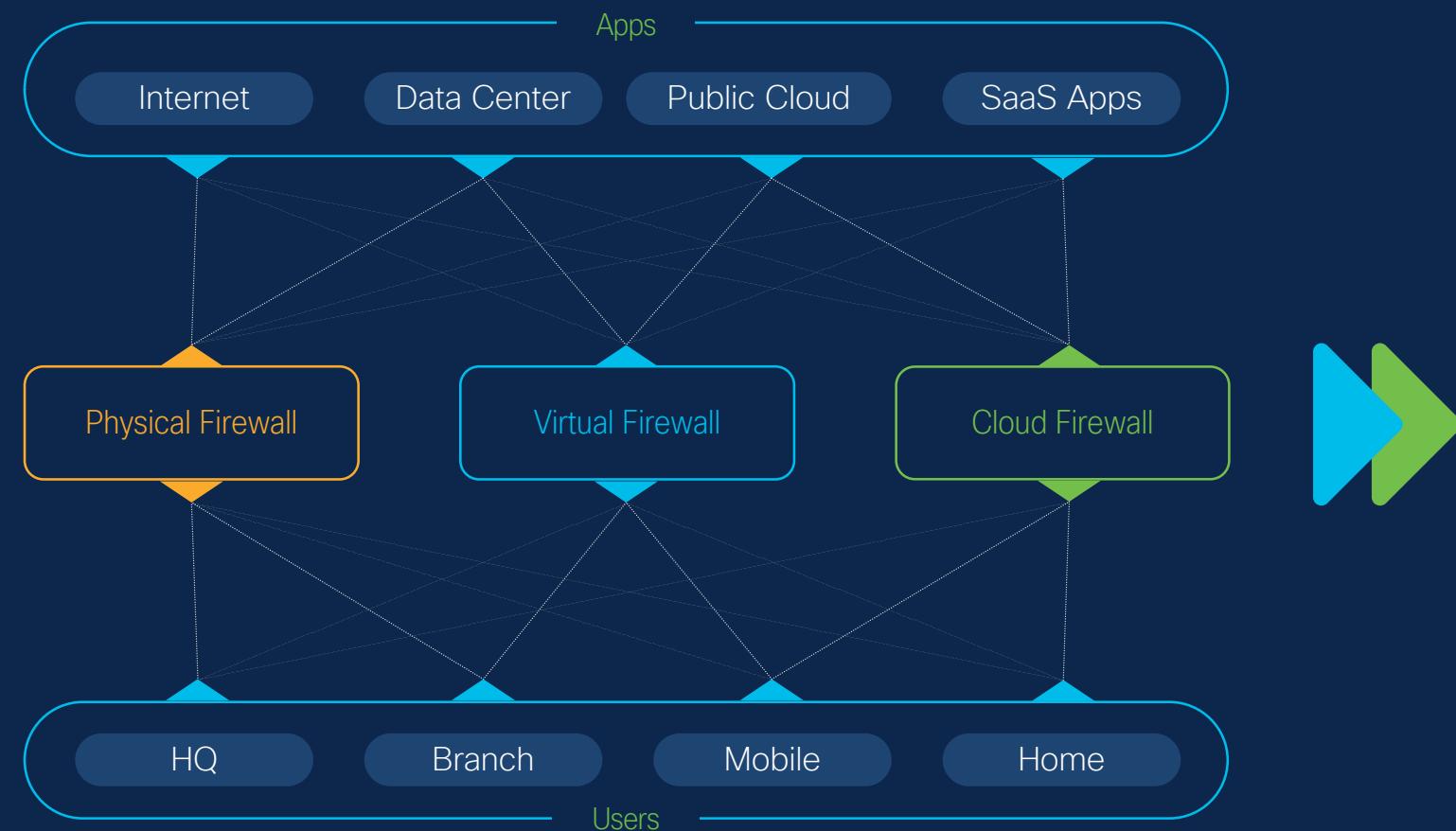
# The firewall market is growing

## Consumption model and form factors are changing



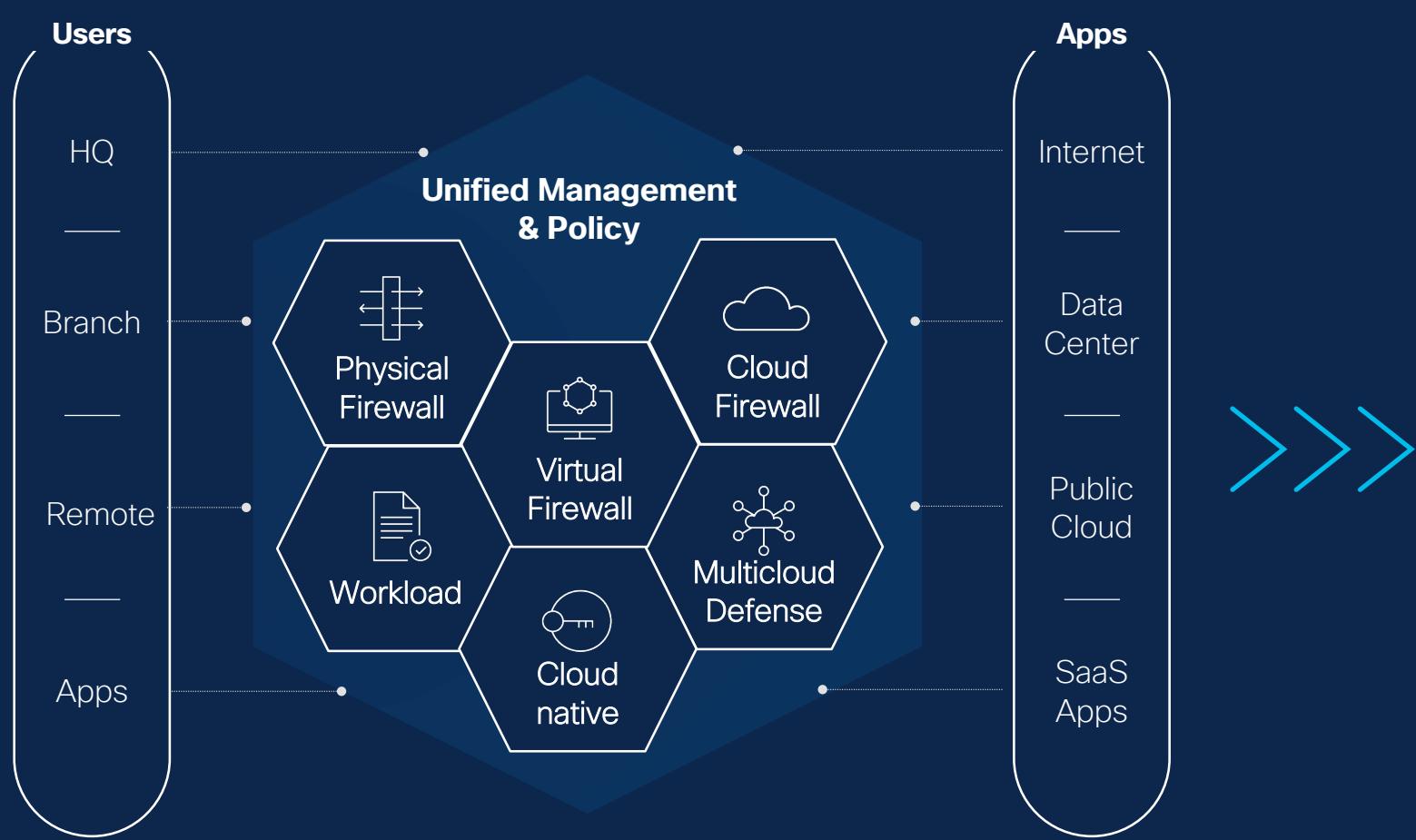
# Enterprise Firewall Market Today

Our customers consume network security in a variety of ways



Complex security environment connecting hybrid users to hybrid application environments using a mix of firewall form factors leveraging deep packet inspection, in siloes

# Cisco Secure Firewall Vision



Harmonizing the Firewall across all form factors

Firewall capabilities expanding to **application**, **networking**, and **user**

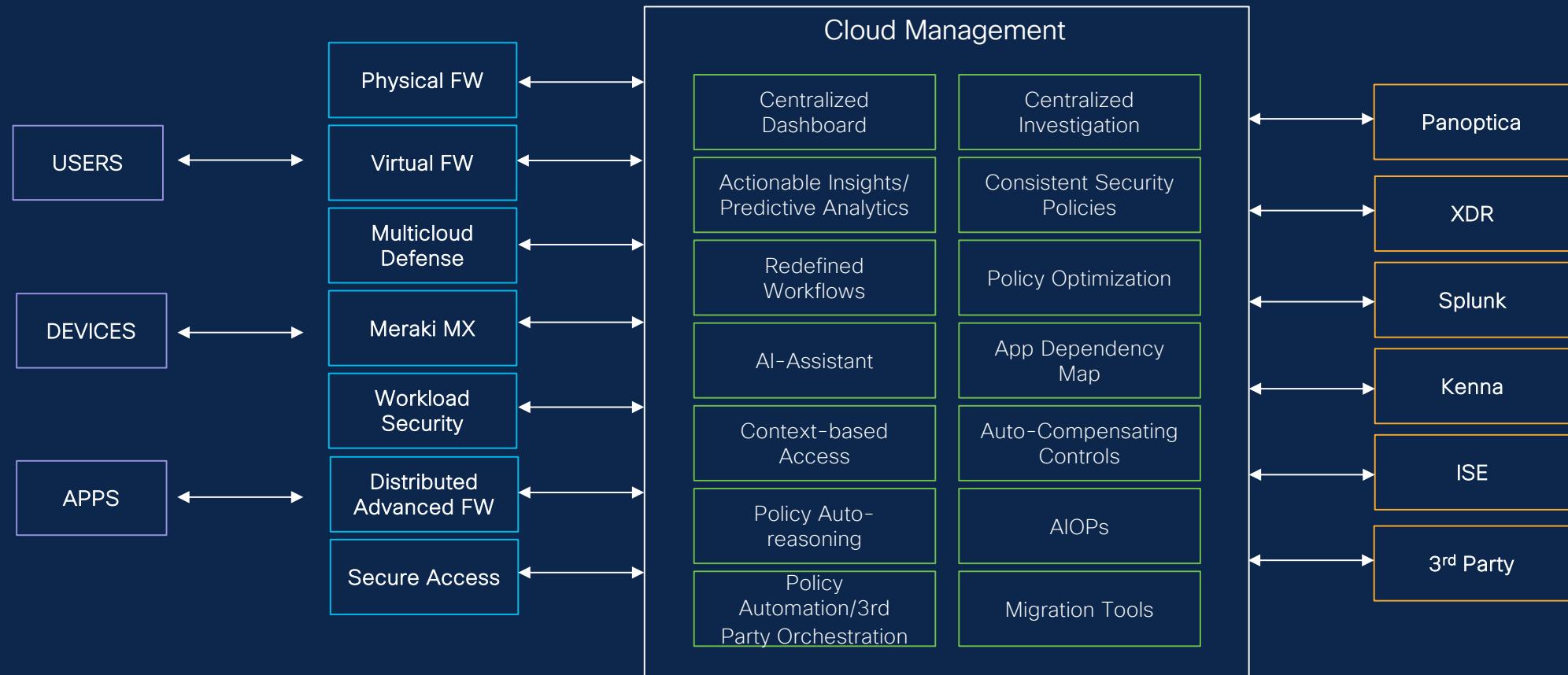
Unified **identity**, **management**, and **policy** to provide choice, consistency, and control

Augment deep packet inspection with **AI/ML** based inference & contextual insights

Flexible consumption model with **easy migration**

# Network Security Hybrid Mesh Platform

Roadmap  
Preview/GA: June 2024



# Our Execution Strategy

Harmonize network, workload, and application security across hybrid & multi-cloud environments

## Unified Management and Policy



Policy Orchestration Management

AI assistant throughout.  
Consistent management  
across Firewall, Workload  
Security, MCD & Security  
Service Edge

## Superior Threat Protection



Workload Segmentation  
Encrypted Visibility  
ML/Contextual Engine

AI/ML-based threat protection and application detection in encrypted traffic

## Future Ready Platforms



Best-in-Class Hardware  
Containerized Firewall  
Cloud MCD

Full range of market-leading firewall platforms for modern enterprise needs

## Integration Across Cisco



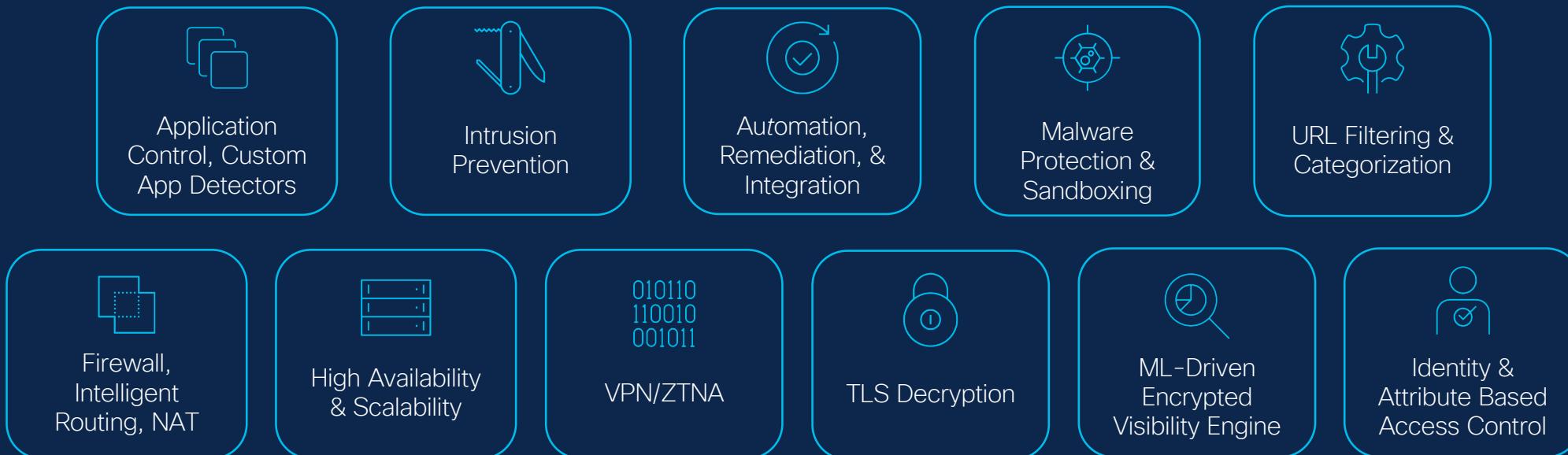
ISE & Catalyst Meraki Secure Access

Ease of purchase and deployment of multiple security and networking

# Our Firewall has comprehensive capabilities

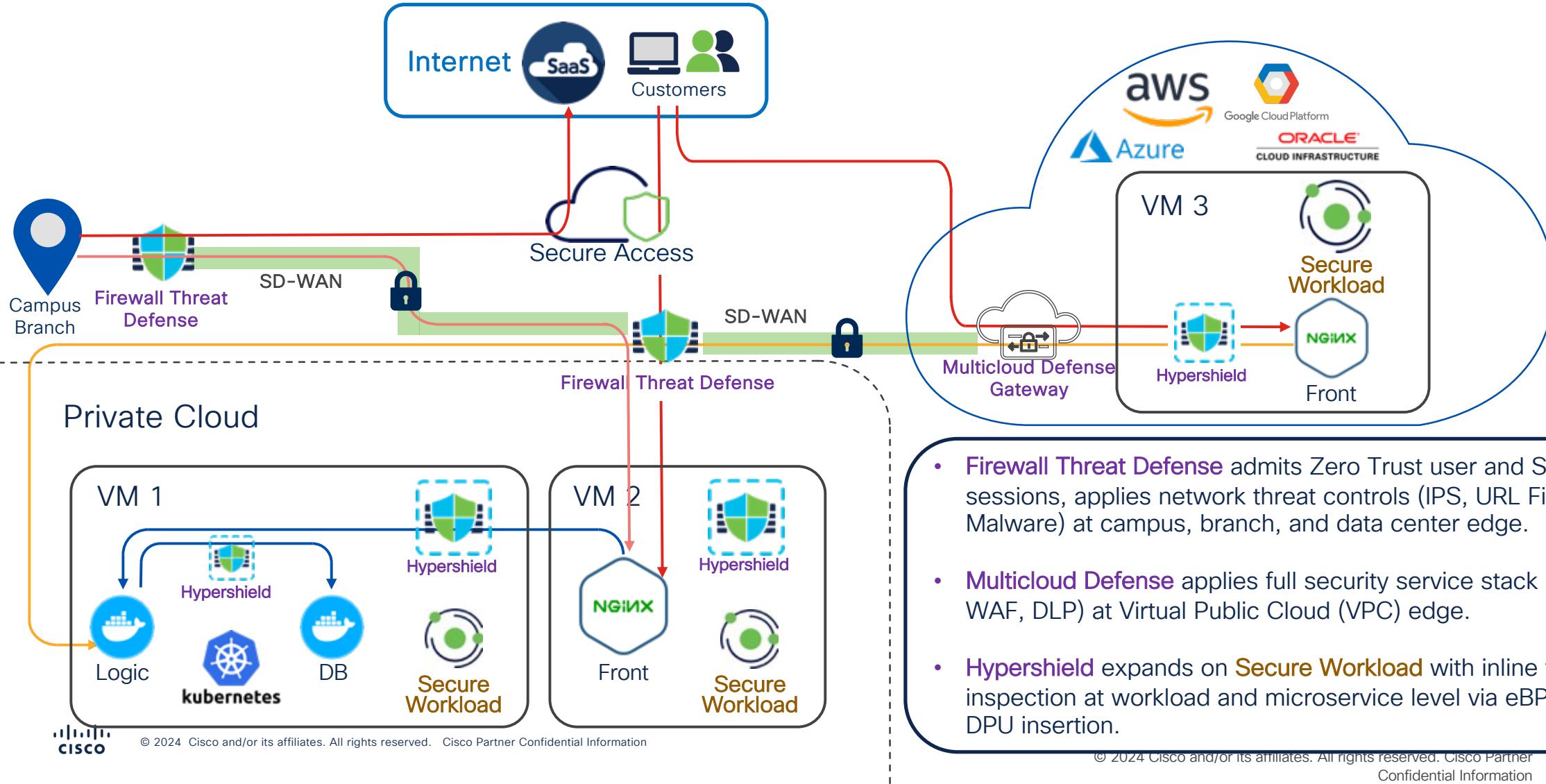
## Superior Threat Protection - AI Assistant and SnortML

### AI Assistant, SnortML - Configuration and Analytics Console



# Firewall Vision: Network, Workload, and Cloud

Cisco Security Cloud abstracts end-to-end policy intent from enforcement point specific configuration.



# Preparing for Customer Demo Overview

What



Complete the 1010 upgrade | Initial configuration

Why



New Features and optimizations | Ensure successful device connectivity and setup

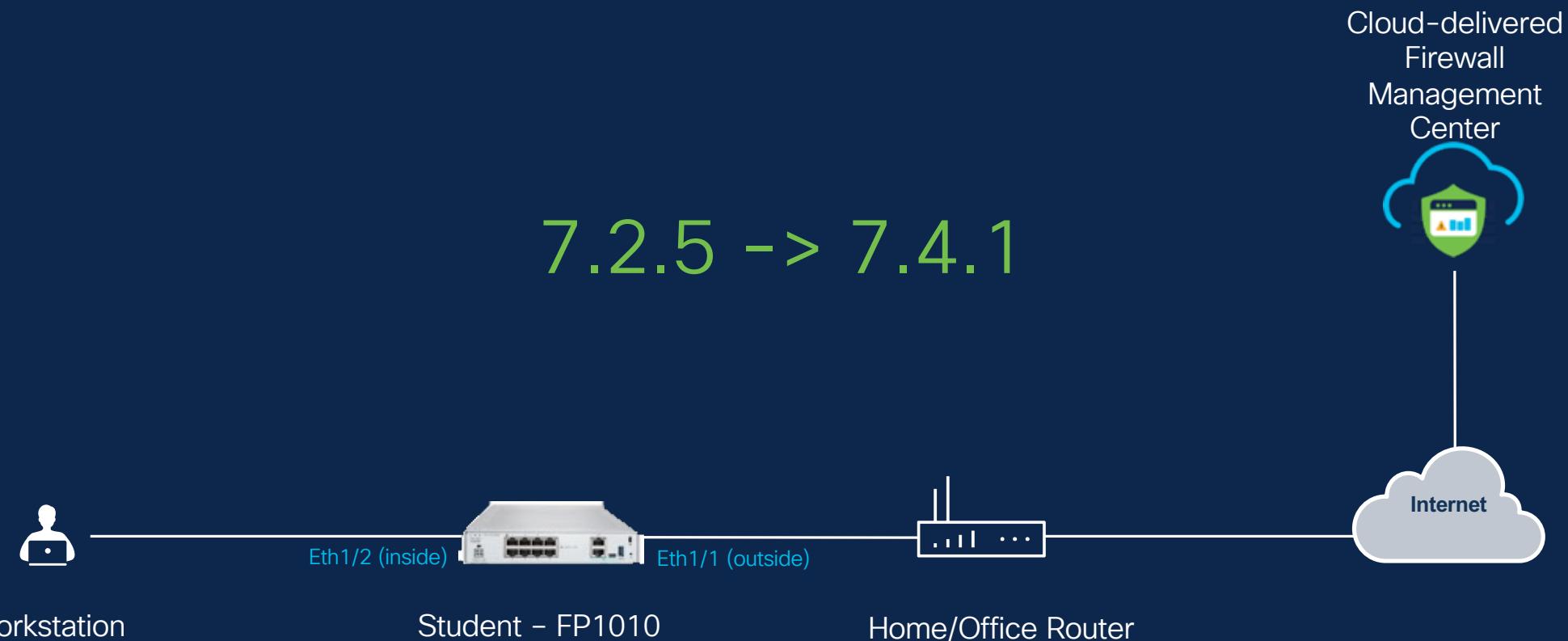
How



Unattended Mode | Configure interface, DHCP, DNS, NAT and ACP

# Preparing For Customer Demo

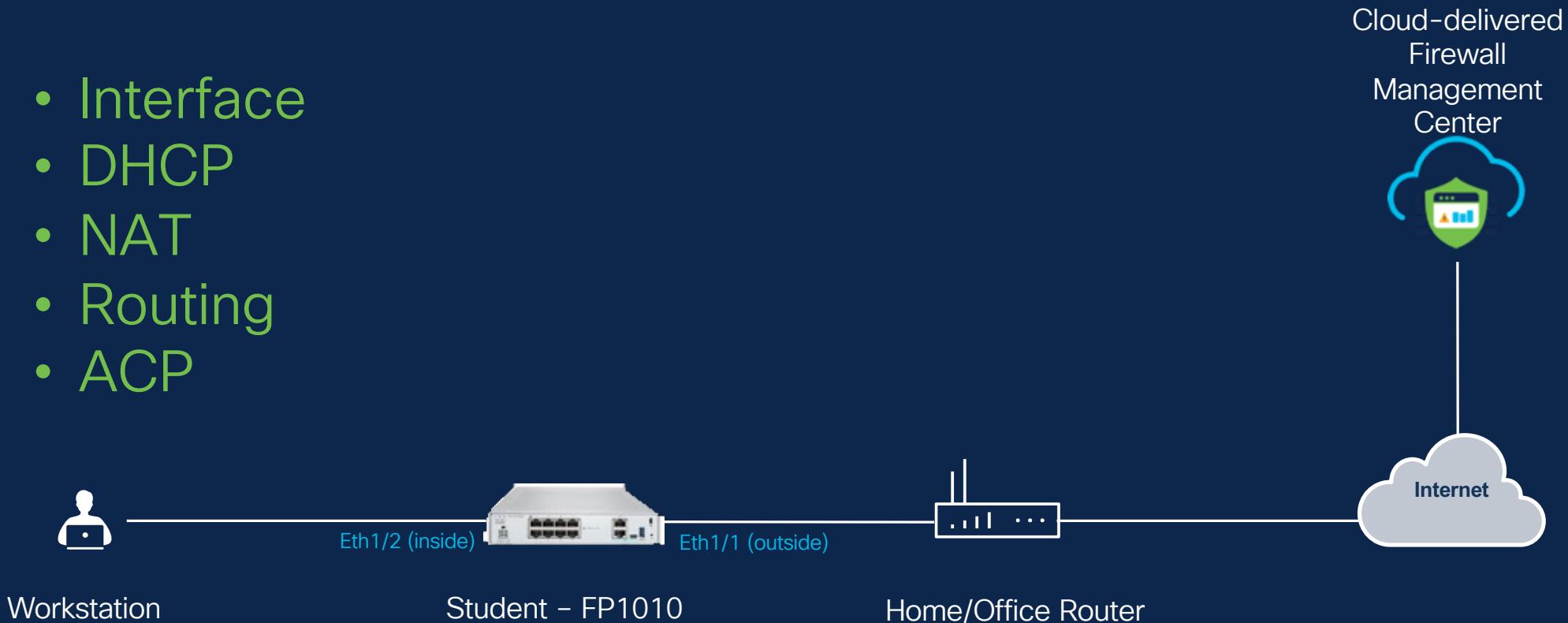
## Step 1: Validate the Upgrade



# Preparing For Customer Demo

Step 2: Getting your 1010 ready for the demo

- Interface
- DHCP
- NAT
- Routing
- ACP

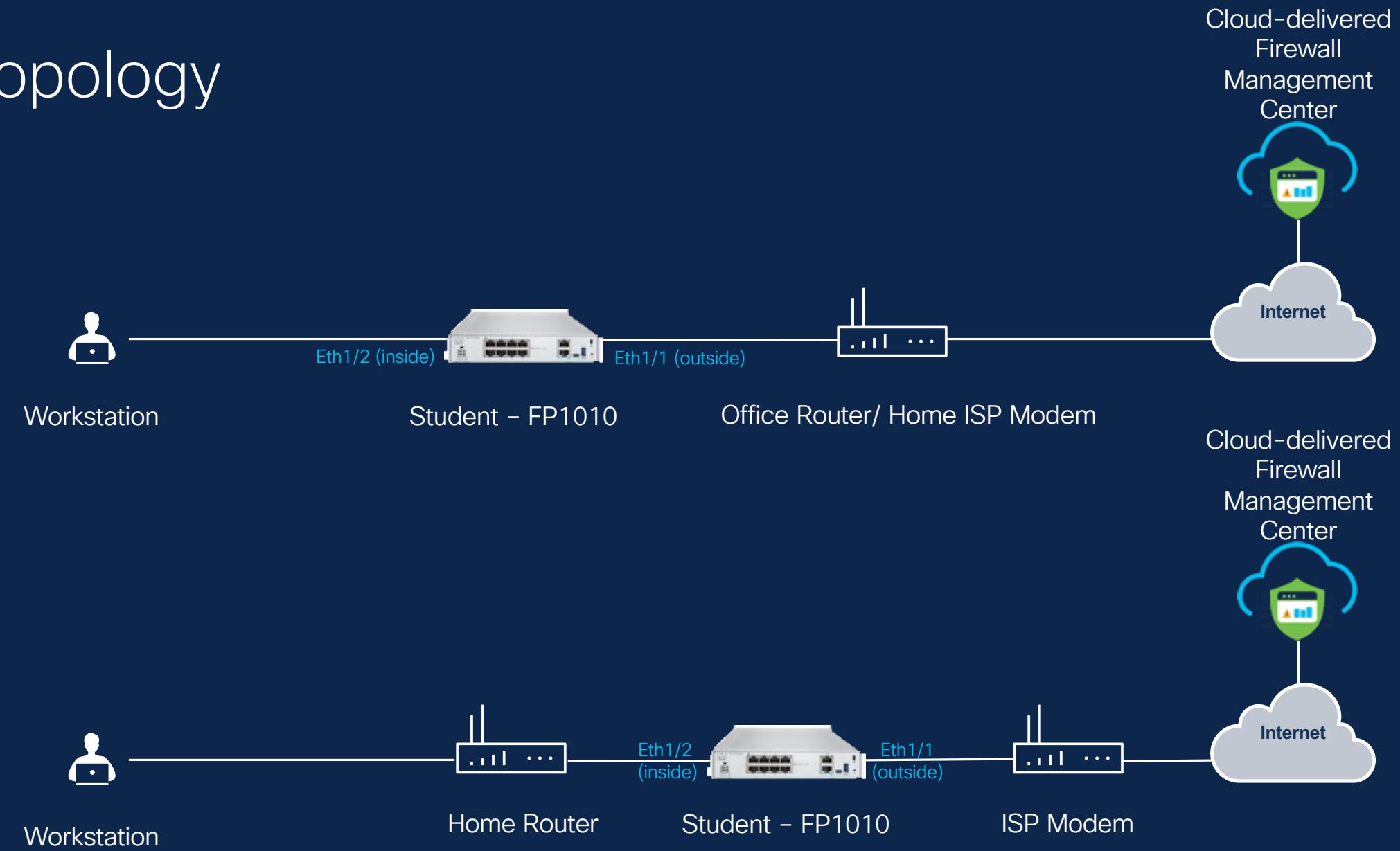


# Objectives

1. Ready to plug and play
2. Try new features
3. Demo



# Topology



# Important



Unlike an ASA, there is no running config or startup config.

With FTD, there are several databases and services running that must be shut down safely before removing power.

\* Yes, even for troubleshooting \*

# Important

The screenshot shows the Cisco Defense Orchestrator interface under the Device Management tab. On the left sidebar, the Devices icon is highlighted with a green box. The main pane displays a list of devices, with one entry for 'FPR-1010-LAB' selected. A modal window titled 'System Shutdown' is open over the device details, asking 'Are you sure you want to shutdown the system?' with 'No' and 'Yes' buttons. The status bar at the bottom indicates 'Cisco Security | 62'.

Defense Orchestrator  
FMC / Devices / Device Management

Devices

Device Management

Template Management

NAT

QoS

Platform Settings

FlexConfig

Certificates

Analysis

Policies

Objects

Integration

Home

Search

Return Home Deploy

Migrate Deployment History

Search Device Add

Search Device

Download Device List Report

Name Model Version Chassis Licenses Access Control Policy Auto RollBack

FPR-1010-LAB Short 3 SDWAN (1) Firepower 1010 Threat Defense 7.4.1 N/A Essentials, IPS (3 more...) None

FPR-1010-LAB

Cisco Firepower 1010 Threat Defense

Device Interfaces Inline Sets Routing DHCP VTEP SNMP

General License System

Name: FPR-1010-LAB

Essentials: Yes Model: Cisco Firepower 1010 Threat Defense

General

Name: FPR-1010-LAB

Transfer Packets: No

Troubleshoot: Log CLI Command

Mode: Routed None

Compliance Mode: Disabled

TLS Crypto Acceleration: Disabled

Device Configuration: Import Export

OnBoarding Method: Download Registration Key

License

Essentials: Yes

Export-Controlled Features: None

Malware Defense: Enabled

System Shutdown

Are you sure you want to shutdown the system?

No Yes

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Partner Confidential Information

Cisco Security | 62

Wait for 5 minutes after the steps to ensure the system has shut down successfully.

**TIP:** Watch for the ethernet interface lights to shut off.

# Lab Time!

## Prepare for Customer Demos

- <https://secure.cisco.com/secure-firewall/docs/prepare-for-demo>



# Device Registration

What



Virtual Threat Defense Registration and Configuration

Why



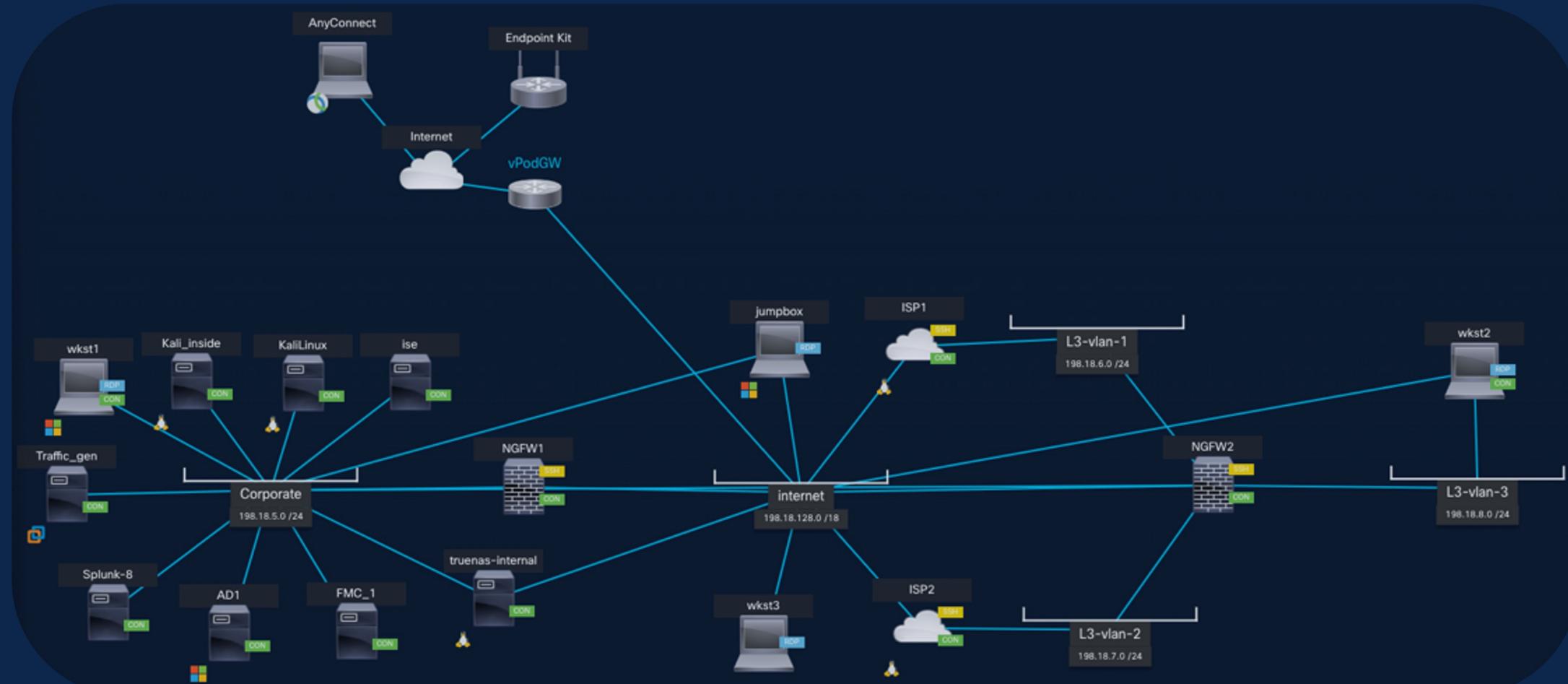
Setting up the virtual Threat Defenses for the upcoming lab tasks

How

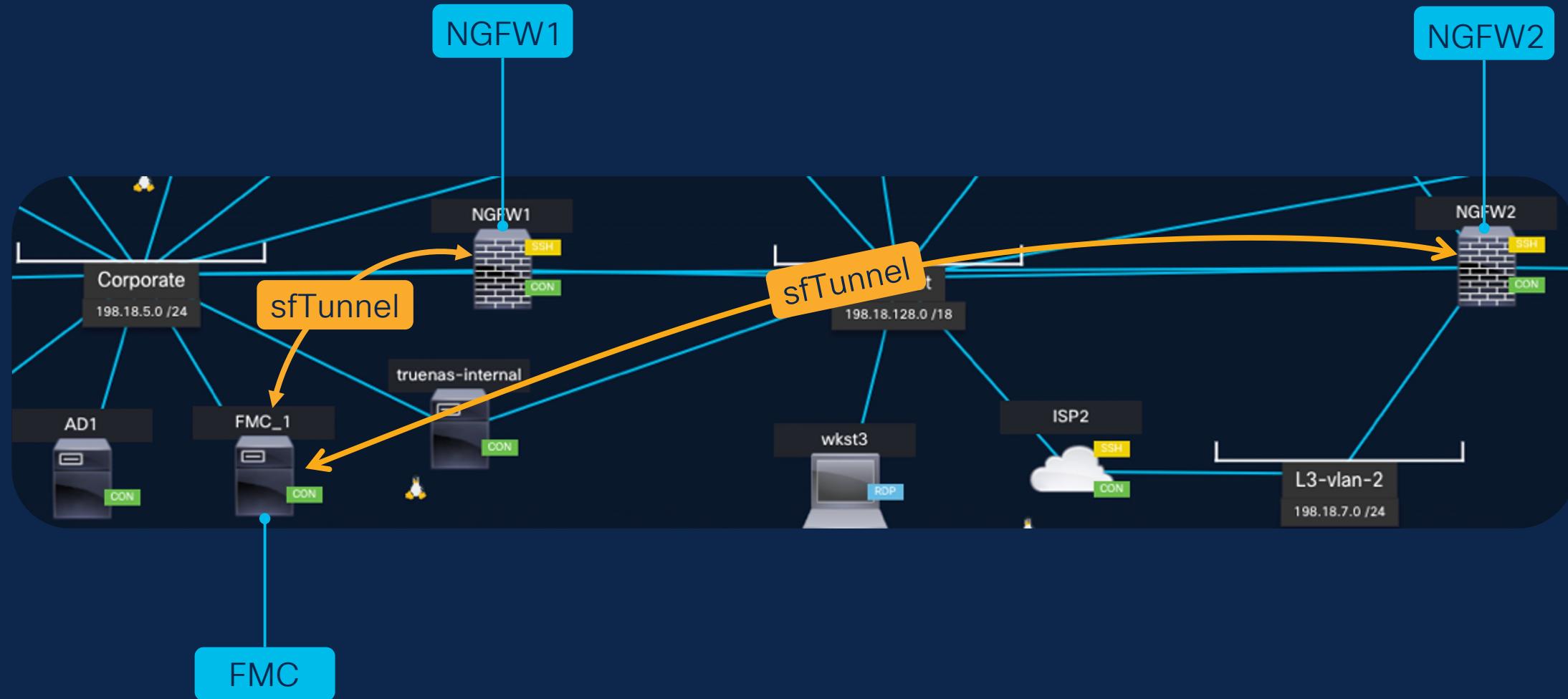


Via the on-prem Firewall Management Center hosted in dCloud

# Topology



# Cisco dCloud – Device Registration



# Lab Time!

## Device Registration and Initial Setup

- <https://secure.cisco.com/secure-firewall/docs/device-registration>

The screenshot shows the Firewall Management Center interface. The top navigation bar includes links for Apps, FMC, RAVPN Files, Certificates - SSL D..., and Lab Guides. The main menu has tabs for Overview, Analysis, Policies, Devices, Objects, Integration, Deploy, and a search bar. On the right, there's a user dropdown and a 'SECURE' badge.

The 'Devices / Device Management' tab is selected, indicated by a red box. Below it, a status bar shows 'All (2)' devices, with 2 errors (red), 0 warnings (orange), 0 offline (grey), 0 normal (green), and 0 deployment (yellow). A 'View By' dropdown is set to 'Group'. The main pane displays two devices under 'Ungrouped': NGFW1 (Snort 3, 198.19.10.83 - Routed) and NGFW2 (Snort 3, 198.19.10.84 - Routed). Both devices have a red exclamation mark icon next to their names, indicating errors.

A large red box highlights the 'Health' tab in the navigation bar of the right-hand panel, which lists system status. It shows '4 total' items: 1 warning, 3 critical, and 0 errors. The first item listed is 'fmc.dcloud.local' with an orange triangle icon, labeled 'AMP for Network Status' and 'Cannot connect to cloud'. The second item is 'Smart License Monitor' with a red circle icon, labeled 'Smart License usage is out of compliance'. The bottom section, 'Devices', lists NGFW1 and NGFW2, each with a red circle icon and the message 'Threat Data Updates on De...' followed by 'Cisco Cloud Configuration - Unable to reach Cisco Cloud from the device. Please check the network connection..'



NOTE: Many of the Red (!) can safely be ignored. The dCloud environment is intentionally unlicensed and will not be able to connect to the AMP cloud, Cisco Cloud, or other services.

# SD-WAN Lab Overview

What



Simplifying branch to hub communication | Direct Internet Access

Why



Ease of configuration | Scalability & Redundancy | Best path guaranteed without manual intervention

How



Dynamic Virtual Tunnel Interface (DVTI) | Application-Based Policy Based Routing

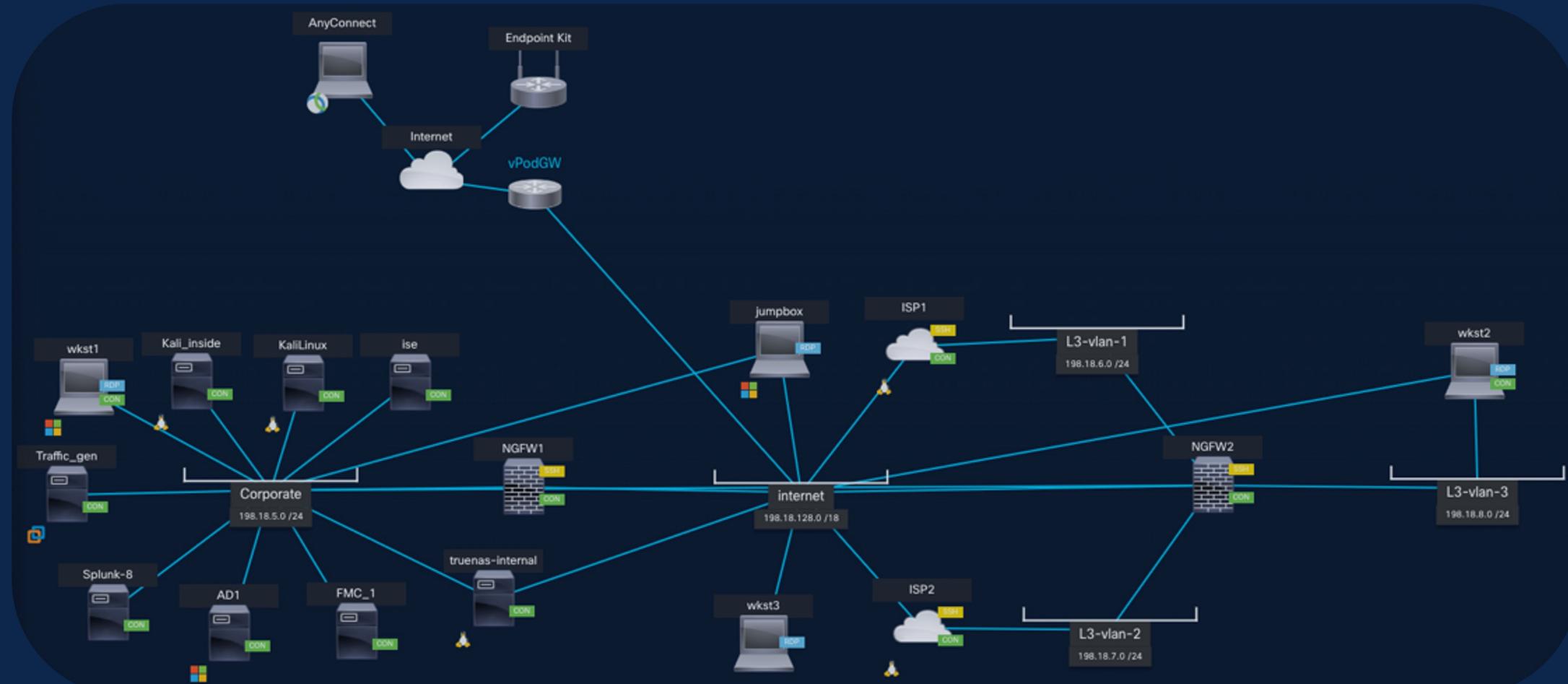
# SD-WAN Definition

SD-WAN solutions provide a replacement for traditional WAN routers and are agnostic to WAN transport technologies.

SD-WAN provides dynamic, policy-based, application path selection across multiple WAN connections and supports service chaining for additional services such as WAN optimization and firewalls.



# Topology



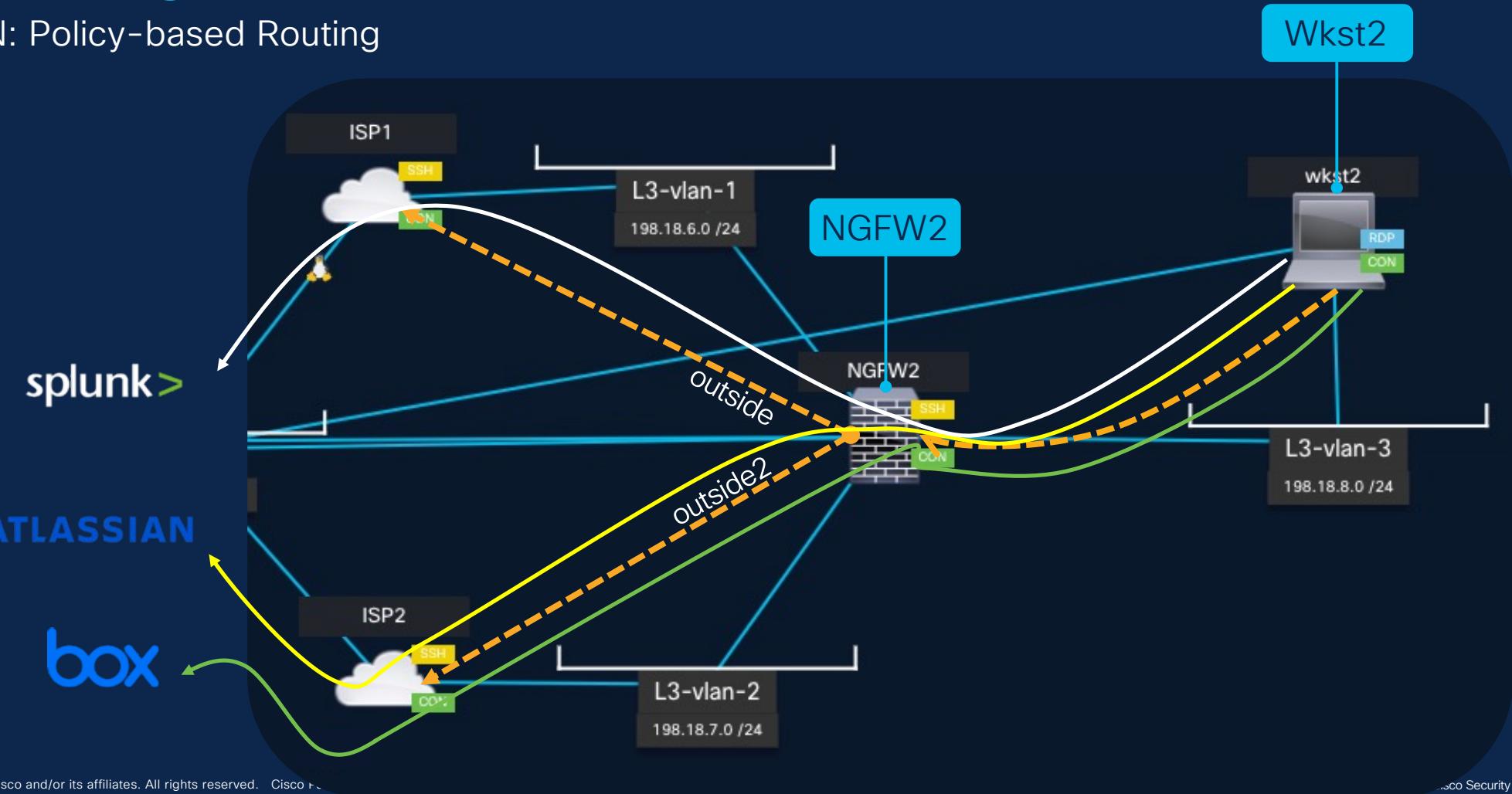
# Simplified Branch to Hub communication

SD-WAN: Site-to-Site VPN



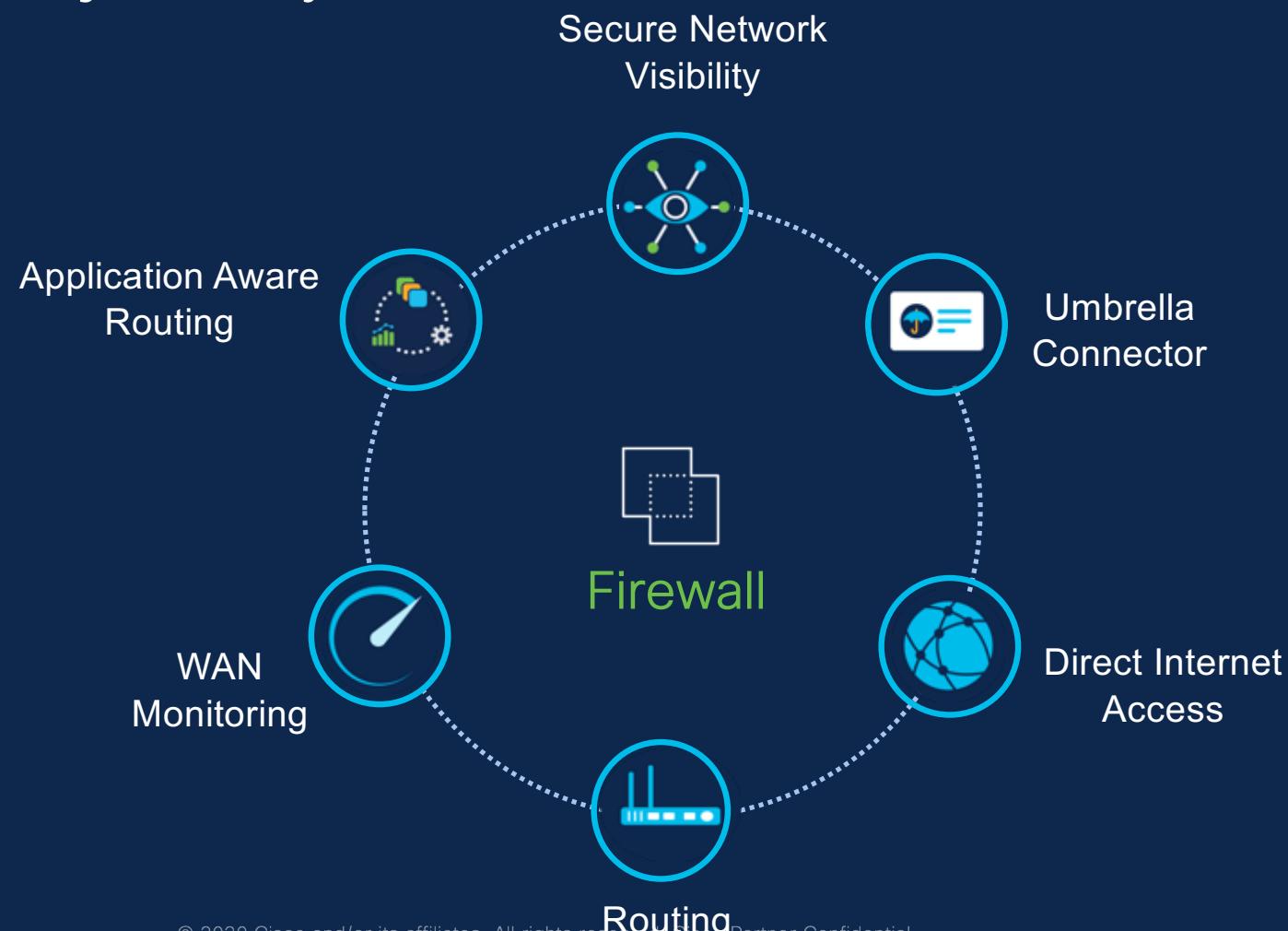
# Application based routing using dynamic path monitoring

SD-WAN: Policy-based Routing



# SD-WAN for managing WAN and Security

## Your journey to SASE



- Firewall capabilities extending to **WAN**
- Visibility of WAN infrastructure through a **Dashboard**
- Extended routing capabilities
- Monitoring of WAN links
- Routing **SaaS applications** to leverage **Internet Access**

# SD-WAN Deployments



## Secure Elastic Connectivity

- Configure Route-based VPN VTI tunnels between branches (Spokes) to headquarters (Hubs)
- IPv6 VTI with BGP
- BGPv6 over VTI
- EIGRP and OSPF over VTI
- DVTI Support DHCP



## High availability with near-Zero Network Down time / SD-WAN Optimization

- Dual ISP configuration
- Active-Standby Backup VTI tunnel configuration with SLA Monitoring
- Optimal Path Selection based on interface monitoring



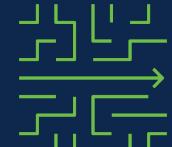
## Increased Usable Bandwidth

- ECMP Support for load-balancing across multiple ISPs
- ECMP Support for VTI
- Application based load balancing using PBR



## Direct Internet Access for Public Cloud and Guest Traffic

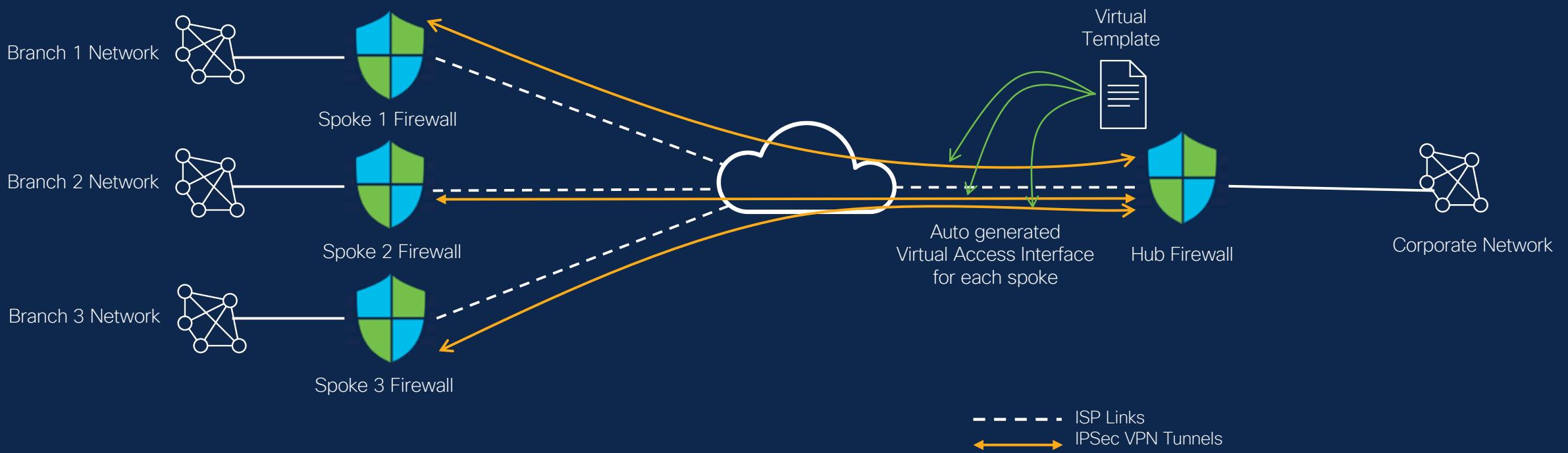
- SaaS Application detection (First Packet using AVC)
- DNS Snooping using trusted DNS servers
- Policy Based Routing using Application as matching criteria
- Local tunnel ID Support for Umbrella



## SD-WAN Management

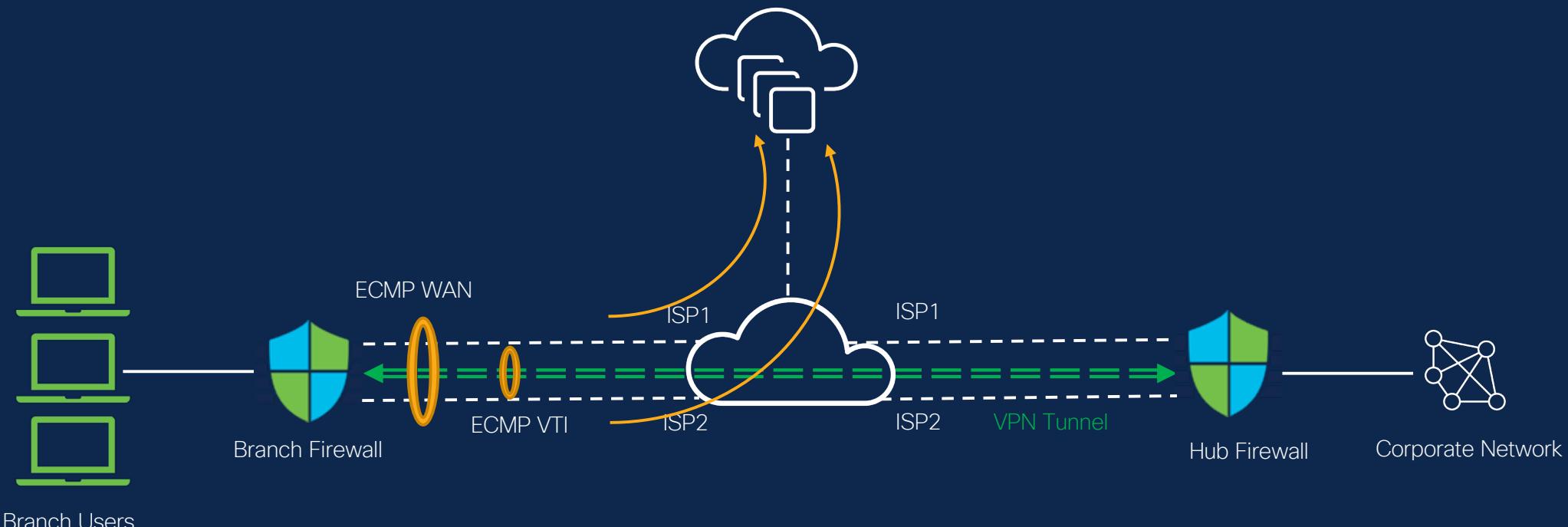
- Data Interface Management
- Auto Config Rollback
- SASE: Umbrella Auto-tunnel deployment
- DVTI Hub and Spoke topology simplification

# Simplifying Branch to Hub Communication using Dynamic Virtual Tunnel Interface (DVTI)



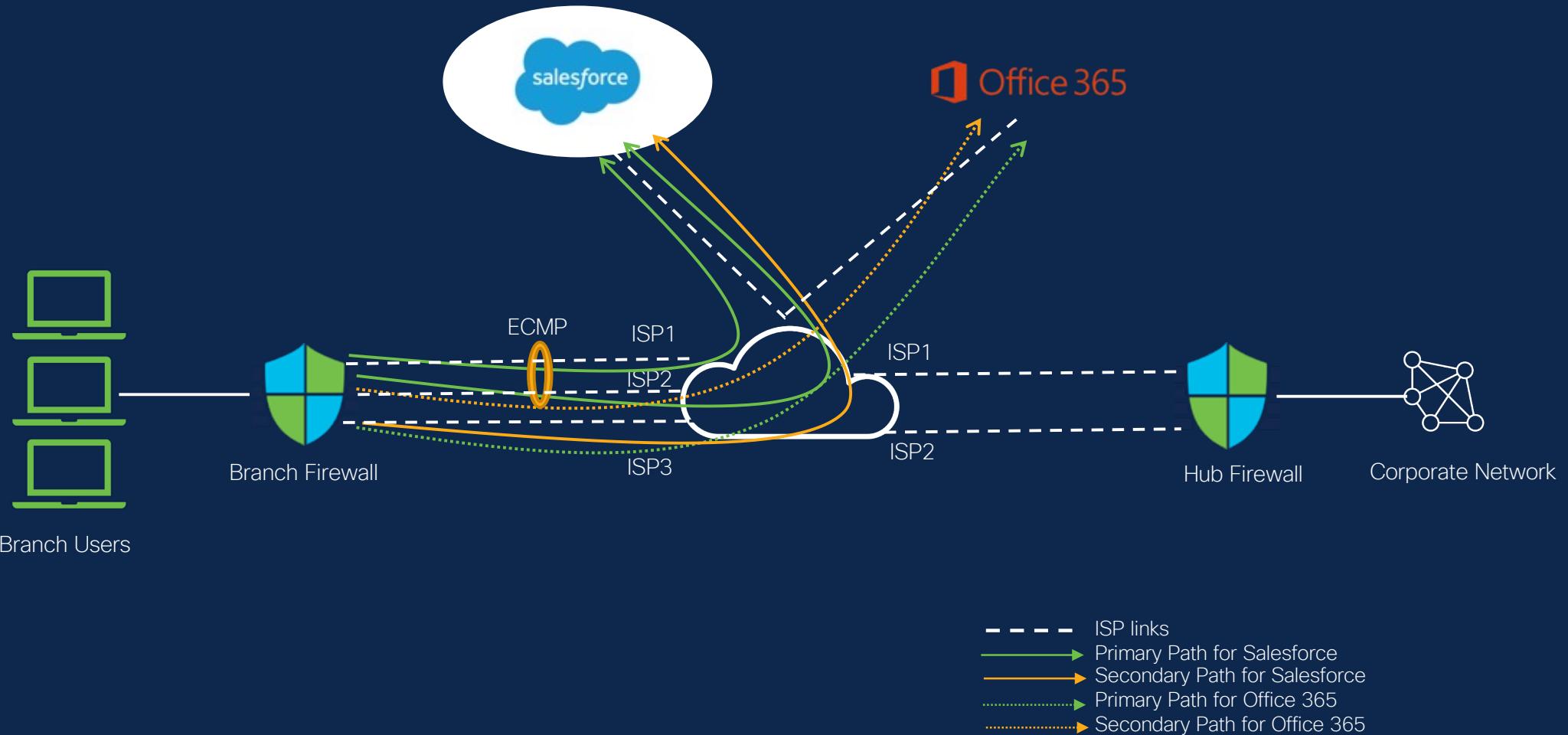
# Direct Internet Access (DIA)

Cloud Applications

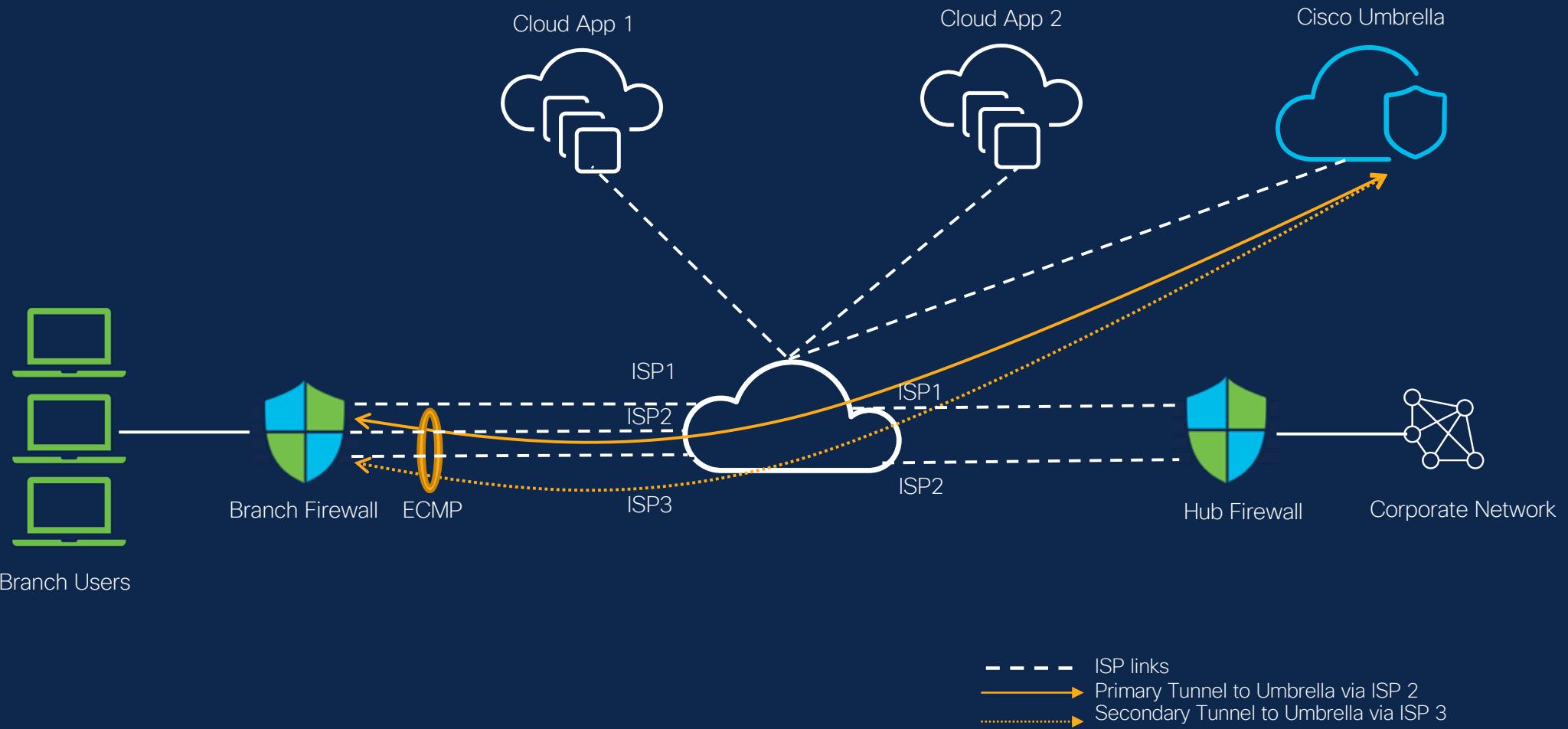


Legend:  
- - - ISP links from Branch FTD to Service Provider  
↔ VPN Tunnel between Branch and Corporate FTD  
→ Direct Internet Access Path for Cloud applications

# Direct Internet Access with Path Monitoring



# Umbrella SASE Auto Tunnel



# SD-WAN Summary Dashboard

Secure Firewall Management Center  
Overview / Dashboards / Dashboard

Overview Analysis Policies Devices Objects Integration Deploy 🔍 ⓘ admin ⓘ SECURE

Dashboard Application Monitoring Uplink Decisions Range 10 minutes || ⏪

**53.com**

Select device 10.10.102.14

- > adp.com
- > Fifth Third
- 53.com**
- 53.us
- ↳ American Express
  - aexp-static.com
  - americanexpress.ae

Interfaces	Latency (ms)	Jitter (ms)	RTT (ms)	Packet Loss (%)	MOS
Gigabit Ethernet 0/0 AT&T	60	75	26	55	5
Gigabit Ethernet 0/1 Jio	45	27	20	60	3
Gigabit Ethernet 0/2 Dialup	20	38	30	25	4
Gigabit Ethernet 0/3 Airtel	25	30	21	45	5

**Application Performance Matrix**

Jitter  Round Trip Time  MOS  Packet Loss ⏪ Last 1 hour ⏪

**Jitter**

The chart displays Jitter values ranging from 0 to 20 ms across various interfaces over a 24-hour period. The interfaces tracked are Gigabit Ethernet 0/0 (AT&T), Gigabit Ethernet 0/1 (Jio), Gigabit Ethernet 0/2 (Dialup), and Gigabit Ethernet 0/3 (Airtel). The data shows significant fluctuations, with peaks occurring around 11:54, 16:54, and 01:54.

**Round Trip Time**

The chart displays Round Trip Time (RTT) values ranging from 0 to 20 ms across the same four interfaces. The trends are similar to the Jitter chart, with notable peaks at the same times (11:54, 16:54, 01:54).

# Lab Time!

## SDWAN Overview

- <https://secure.cisco.com/secure-firewall/docs/sdwan>

# Threat - AttackIQ

What



AttackIQ

Why



Simulate attacks to provide visibility into threat efficacy on the Firewall

How



Breach and attack simulation platform that provides visibility into security performance with clear data-driven analysis and mitigation guidance.

# What is AttackIQ?

AttackIQ provides a platform for continuous security validation.

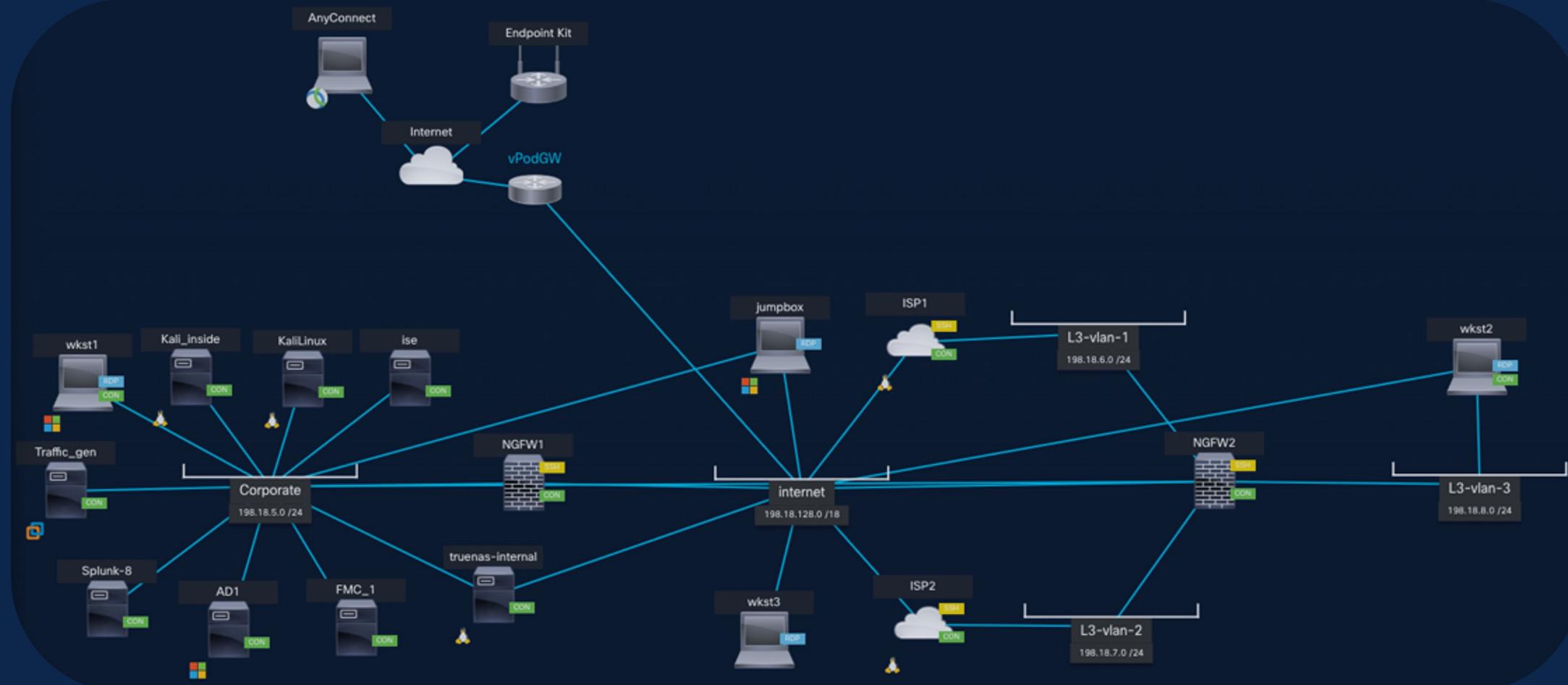
- Allow organizations to **test security defenses against real-world attack scenarios**.
- Help identify weaknesses and improve their overall security posture.
- Simulates cyber attacks and assessing their ability to detect and respond to them.

Product Offerings:

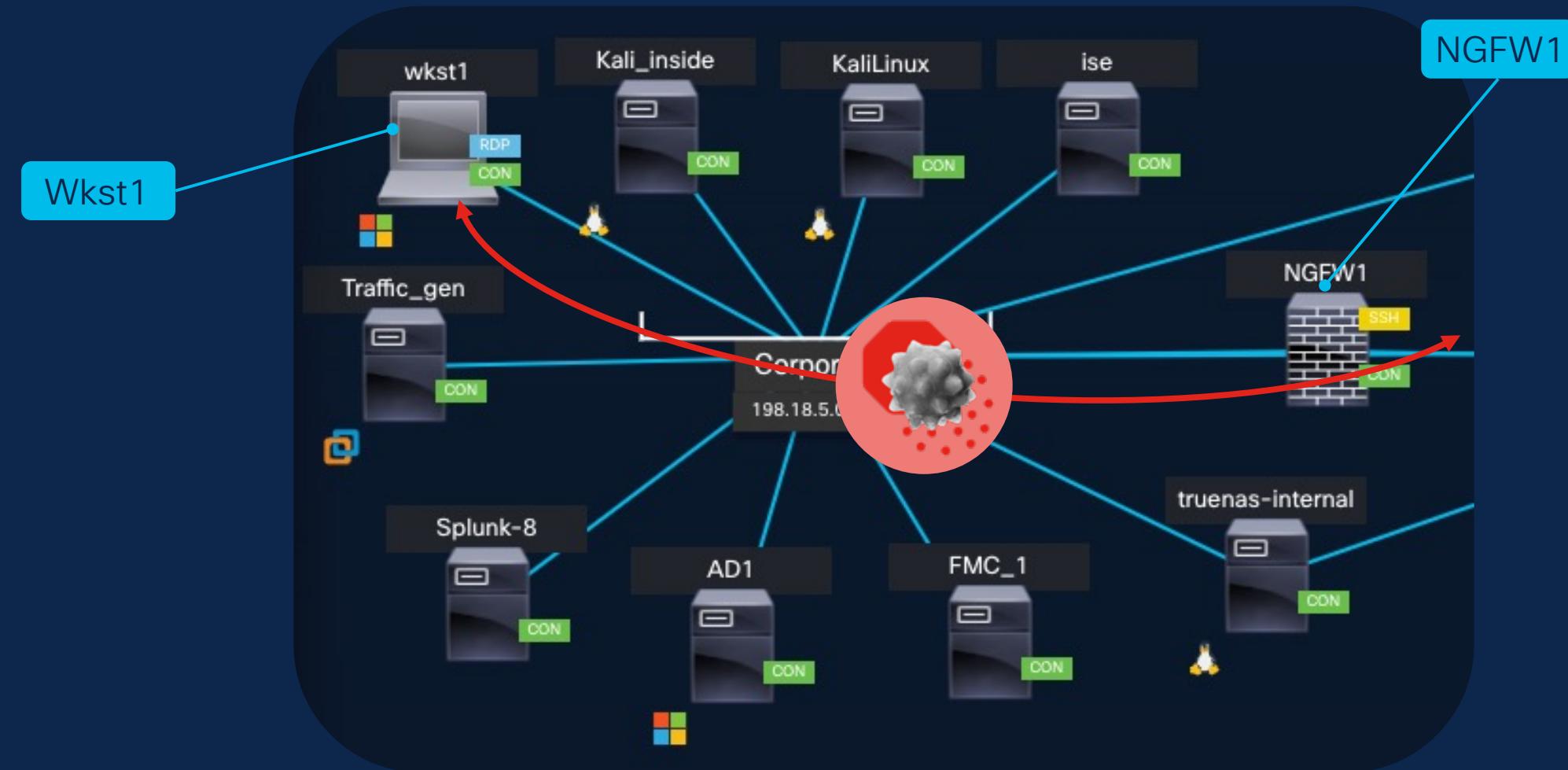
- **Flex** – “Easy button”
  - Click-and-Go Packages
  - Agentless
- **Enterprise** – “Full Offering”
  - Customizable
  - Agent-based



# Cisco dCloud - Topology



# Cisco dCloud – Threat Efficacy with AttackIQ



# Lab Time!

## Threat (AttackIQ)

- <https://secure.cisco.com/secure-firewall/docs/threat>



CERTIFICATION  
ITEM!

REMINDER: Refer to the earlier section on which AttackIQ reports to save for your Certificate of Completion



# Remote Access Virtual Private Network (RAVPN)

What



Remote Access VPN configuration on Threat Defense

Why



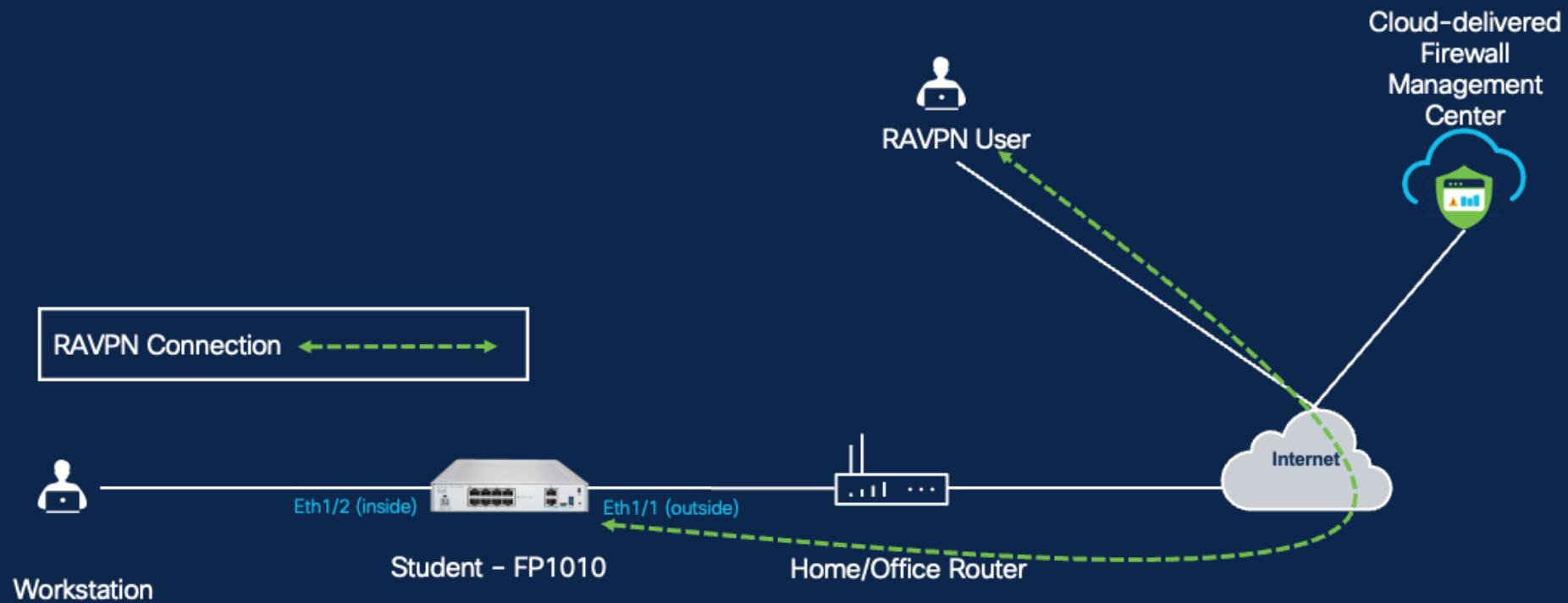
Secure network access for remote users over the internet

How



Using RAVPN wizard in Firewall Management Center

# Topology



# Lab Time!

## Remote Access VPN

- <https://secure.cisco.com/secure-firewall/docs/remote-access-vpn>



# Call to Action



Secure



Demo



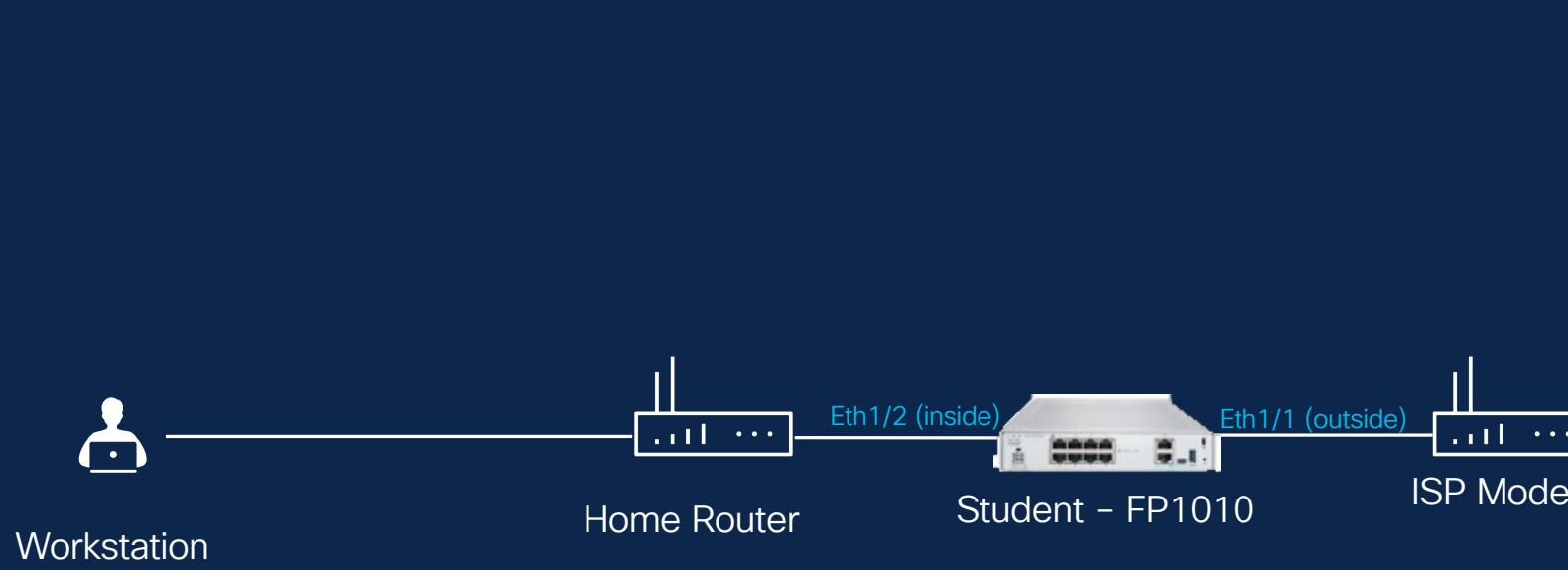
Engage

# How to use the 1010 at Home / Office

## Example Topologies



Cloud-delivered  
Firewall Management Center



Cloud-delivered  
Firewall Management Center

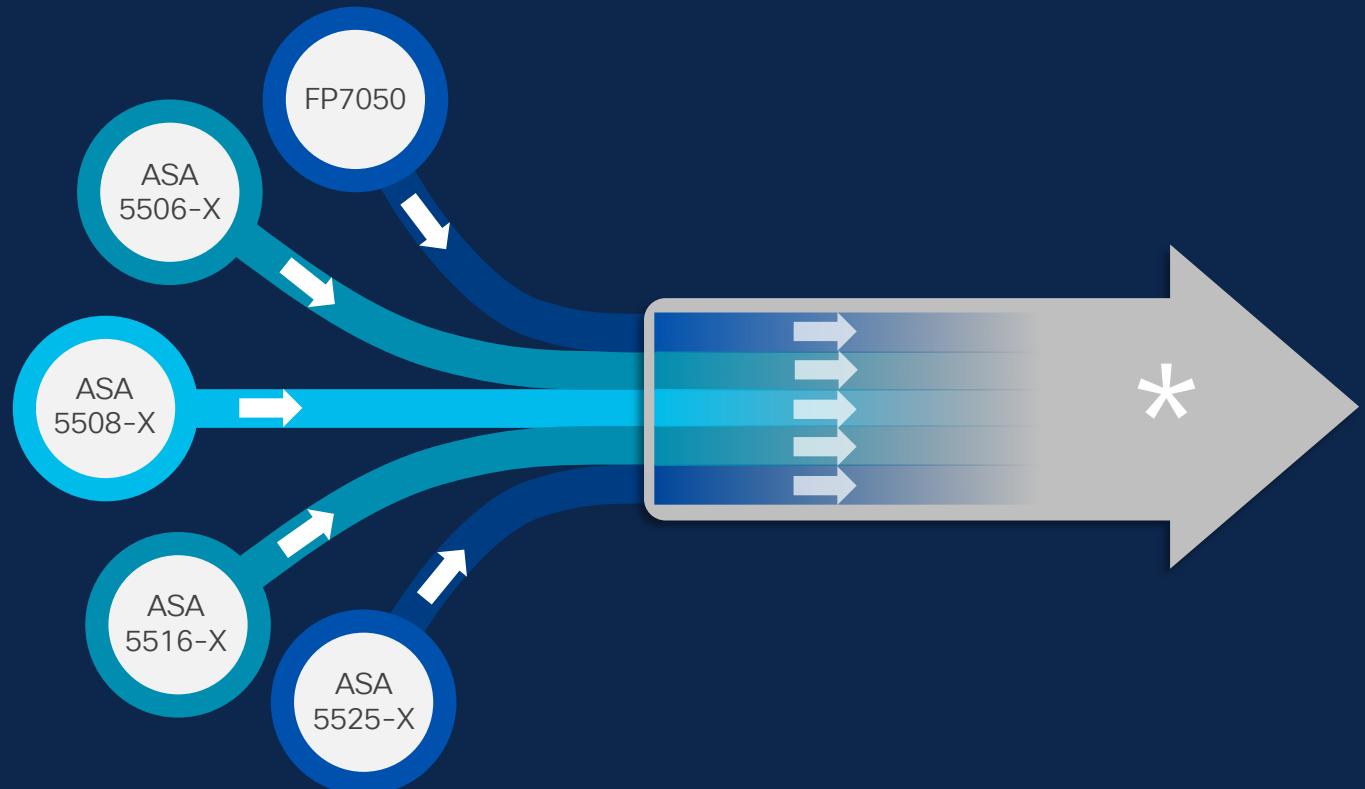


# When It Comes to Refresh

Don't assume. Use the Performance Estimator.



[ngfwpe.cisco.com](http://ngfwpe.cisco.com)



Firepower 1010

\*Migration data based on FW+AVC+IPS (1024B)



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Partner Confidential Information

Cisco Security | 91

# Internal or Partner submissions to the Firewall Refresh Help Desk receive a no cost Cisco-led:

- Migration and Refresh for **Unlimited\*** Firewall devices (\*Depends on the scale of the customer migration, determined by the first customer call, & may be limited if it conflicts with another migration).
- Complete configuration review & validation of migration process prior to cutover.
- Virtual Security Engineer supports & provides guidance during the 24/7 window;
  - Weekend cutovers require **7 business days notice**
  - Weekday cutovers require **2 business day notice**
  - Pre-emptive TAC case for additional support is also recommended. For any TAC escalations or BEMS, account team needs to provide support to the customer.

## Firewall Refresh Program Highlights

- 24/7 Globally Available Service\*
- Competitive migrations from PAN, Fortinet, Checkpoint, & Juniper\*
- ASA Migration support
- Support to refresh devices to the latest firewall version (beyond latest suggested release).

### Program & Customer Engagement Process

Day 0-1

Day 1-2

Day 2-3

Day 3-X

Day X

#### Submission

Employee/Partner completes initial submission and uploads supporting documentation

#### Preview

Help Desk engineer previews request & reaches out for questions and clarification

#### Engage

Help Desk engineer sets up WebEx sessions with the requestor and customer engineer (as required) to review & validate the configuration.

#### Migrate

Engineer supports & provides guidance during the cutover within the 24/7 window; Pre-emptive TAC case for additional support.

#### Close

Help Desk engineer closes case upon confirmation from customer & a satisfaction survey is sent.

# Additional Resources

## Public Information

Accessible & Shareable to Everyone

- [Cisco Secure Essentials Hub](#) – Is the “Hub” or starting point where users can obtain information on Secure Firewall, Microsegmentation, & by Q4 FY24 – Multicloud Defense
- [Cisco Secure Firewall & Workload Youtube Channels](#) – These channels provide product deep dives, integrations, release overviews, & highlights
- [Cisco DevNet Website](#) – Houses various labs where users can learn about Firewall Automation for AWS, Azure, GCP & SCC.
- [Cisco Developer Website](#) – offers Cloud templates to help users deploy firewalls in their preferred cloud provider environment, & Automation APIs allowing the exchange of security events, data and host information



## Lab licensing

## Internal & Partner Information

Only available to Cisco Employees or Partners



- [SalesConnect \(Firewall & Workload\)](#) – Houses in-depth technical documentation, best-practices, & demonstrations to help stakeholders realize the value of Firewall and Workload.

### Partners

<https://firestarterpartner.cisco.com>

### Internal

<https://firestarter.cisco.com>

# Please Fill Out this Survey

*How can we make these trainings better? What did you like? Would you recommend this training? Tell us your thoughts!*

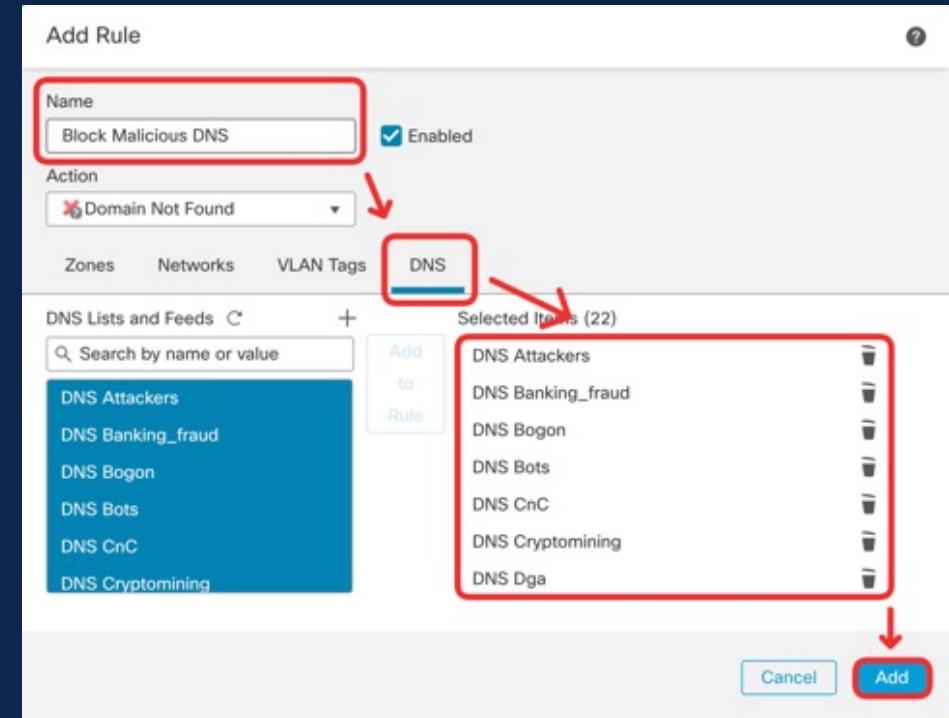
<https://ciscochannelsolutions.com/registration/>



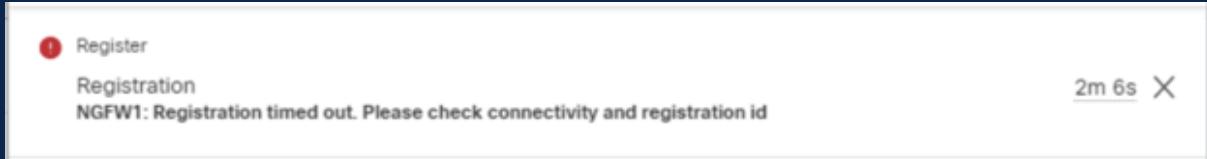


# Firewall Ignite - Helpful Lab tips

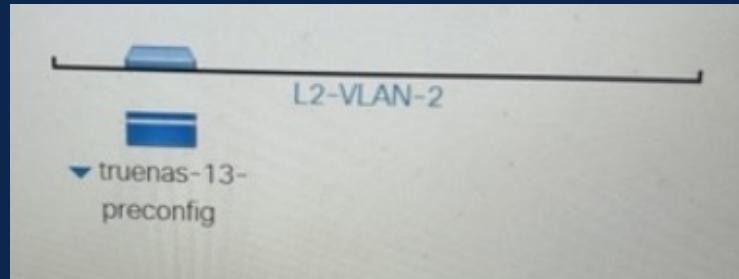
- Careful with your muscle memory, many labs will use **198.18** and not **192.168**
- If there are missing buttons (**edit/save**), expand browser window size or change browsers in dCloud
- Make sure you deploy the changes when the lab guides states
- If you are doing the threat lab:
  - If you suddenly have issues getting to internet on WKST1, check your DNS policy on NGFW1
  - Use this URL for AttackIQ:  
<https://firedrill.attackiq.com>
- Don't google AttackIQ Login



# Additional tips



- IP and or registration key mismatch between “configure manager add” on FTD and “device add” on FMC . Commonly caused by typo’s
- Retry device add in FMC again. Triple check IP address from guide and registration key matches what you typed in FTD CLI
- To redo FTD CLI
  - configure manager delete
  - Then configure manager add... again



- dCloud squish – corrupted browser cache commonly caused by use of browser back button
- Browse direct to [dcloud.cisco.com](https://dcloud.cisco.com), login , select appropriate DC, my hub, sessions, view. Look for list of servers within session , other than from the topology view, and open webRDP via the list instead
- Can also open a dCloud support ticket and they can reset the topology view of your unique session id. Include DC and session id with case.