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!

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.

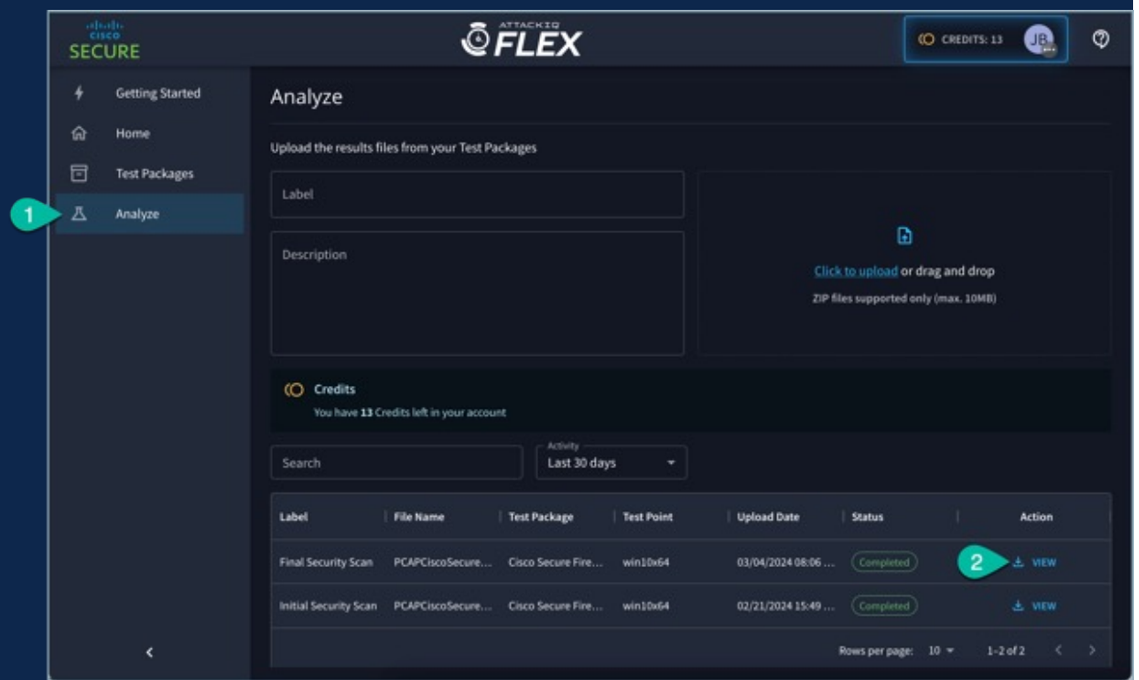
Please allow for 10 business days to the certificate to be issued.

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



Certificate of Completion Process

AttackIQ Final Report

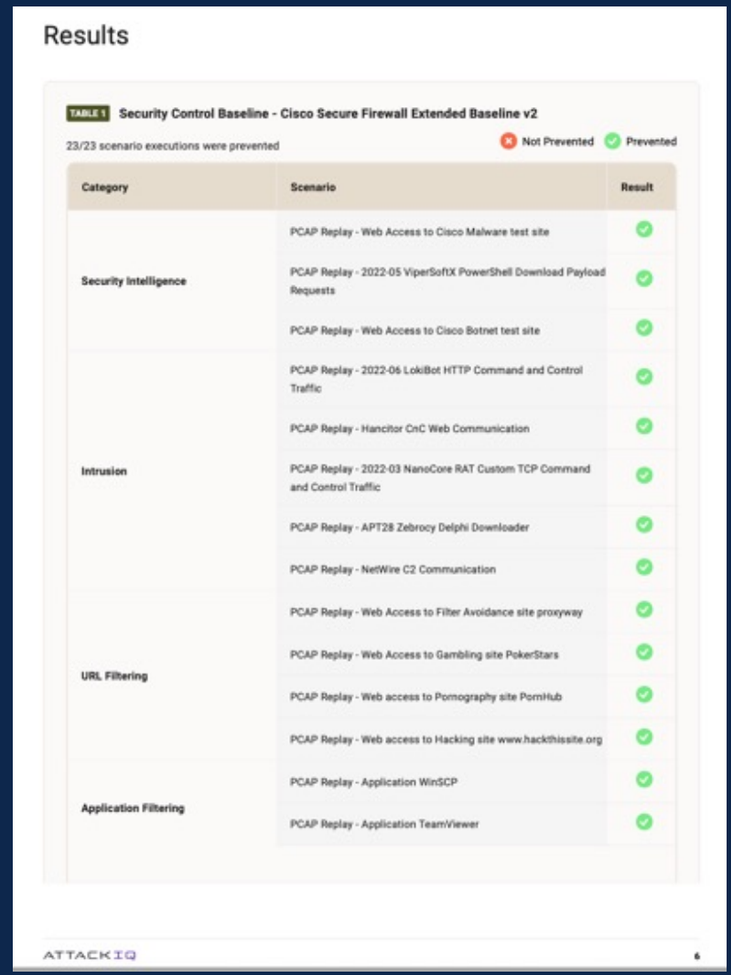
Upon completing the Threat Lab in dCloud, download the final test results after completing the FTD policy setup.

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

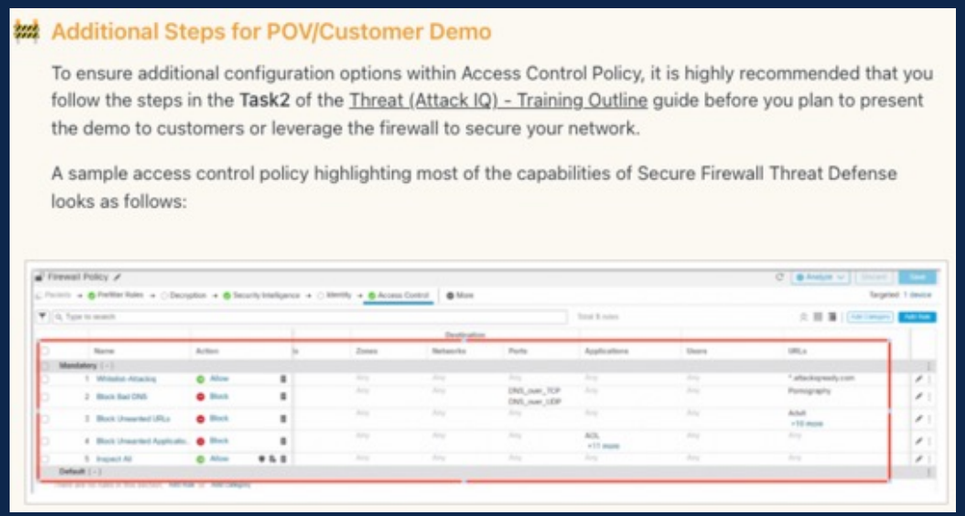
Not Prevented Prevented

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	✓
Intrusion	PCAP Replay - 2022-06 LokiBot HTTP Command and Control Traffic	✓
	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	✓

ATTACKIQ 6

NOTE: Highly Recommended

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



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

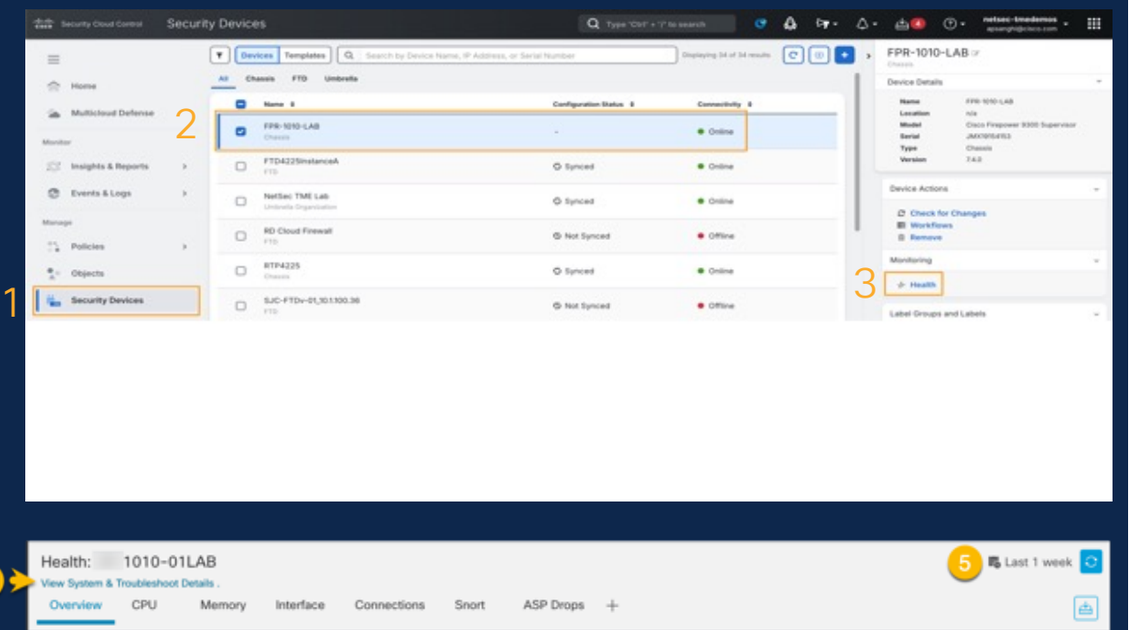
Capture 1 screenshots

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.



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:

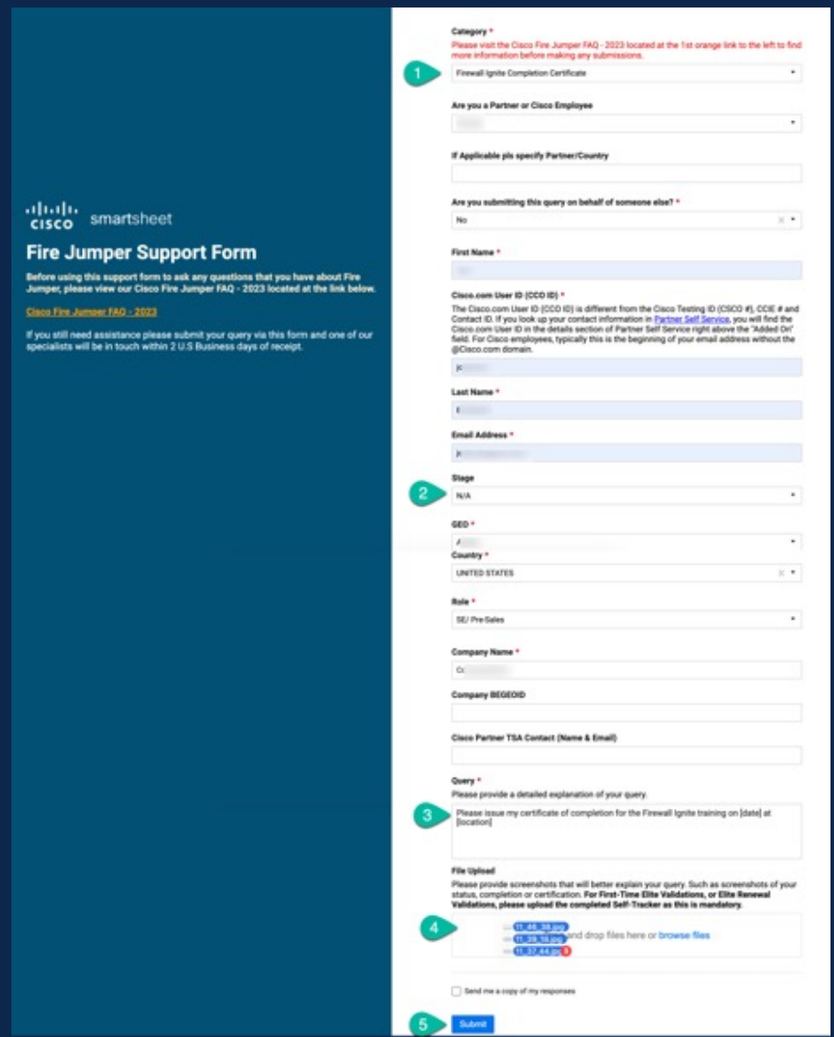
Submit through this form: http://cs.co/certificate-fw-ignite

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.



CONFIRM or ADD YOURSELF

Webex STUDENT ROOM

Webex Teams

https://eurl.io/#abcdefg

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.

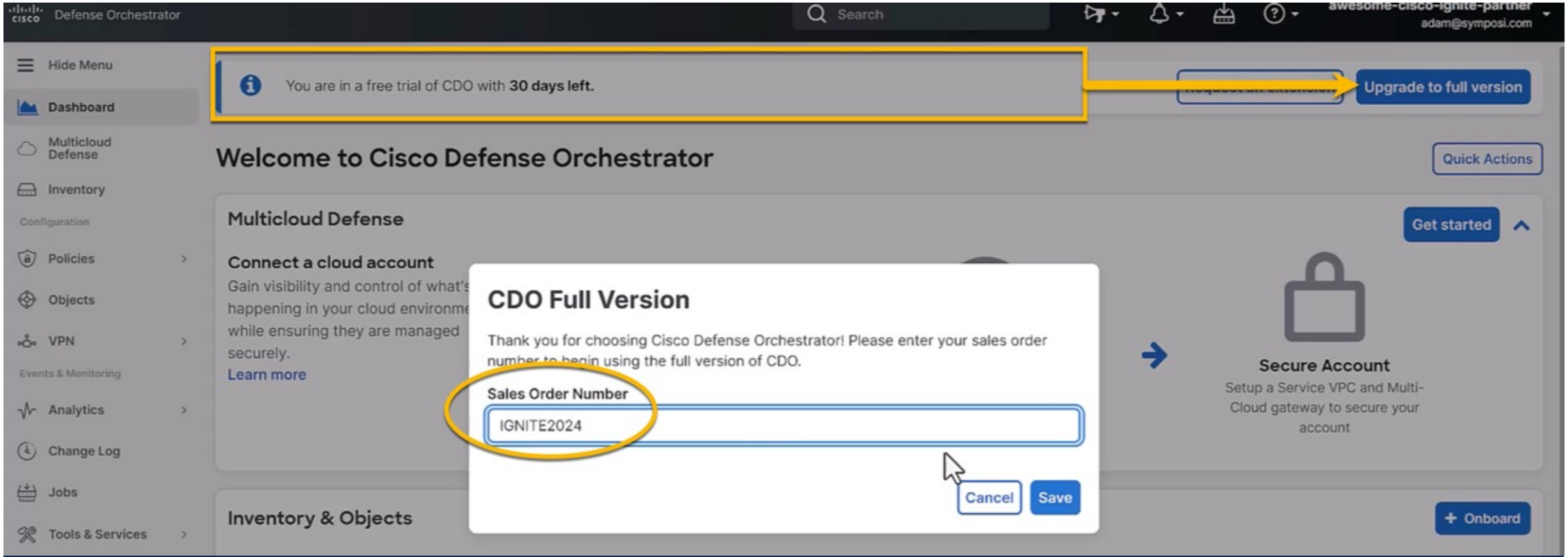
Equip you with the tools you need to demonstrate Cisco’s firewall to customers.

Gather your feedback and measure the expectations.

Did you do your homework ☺

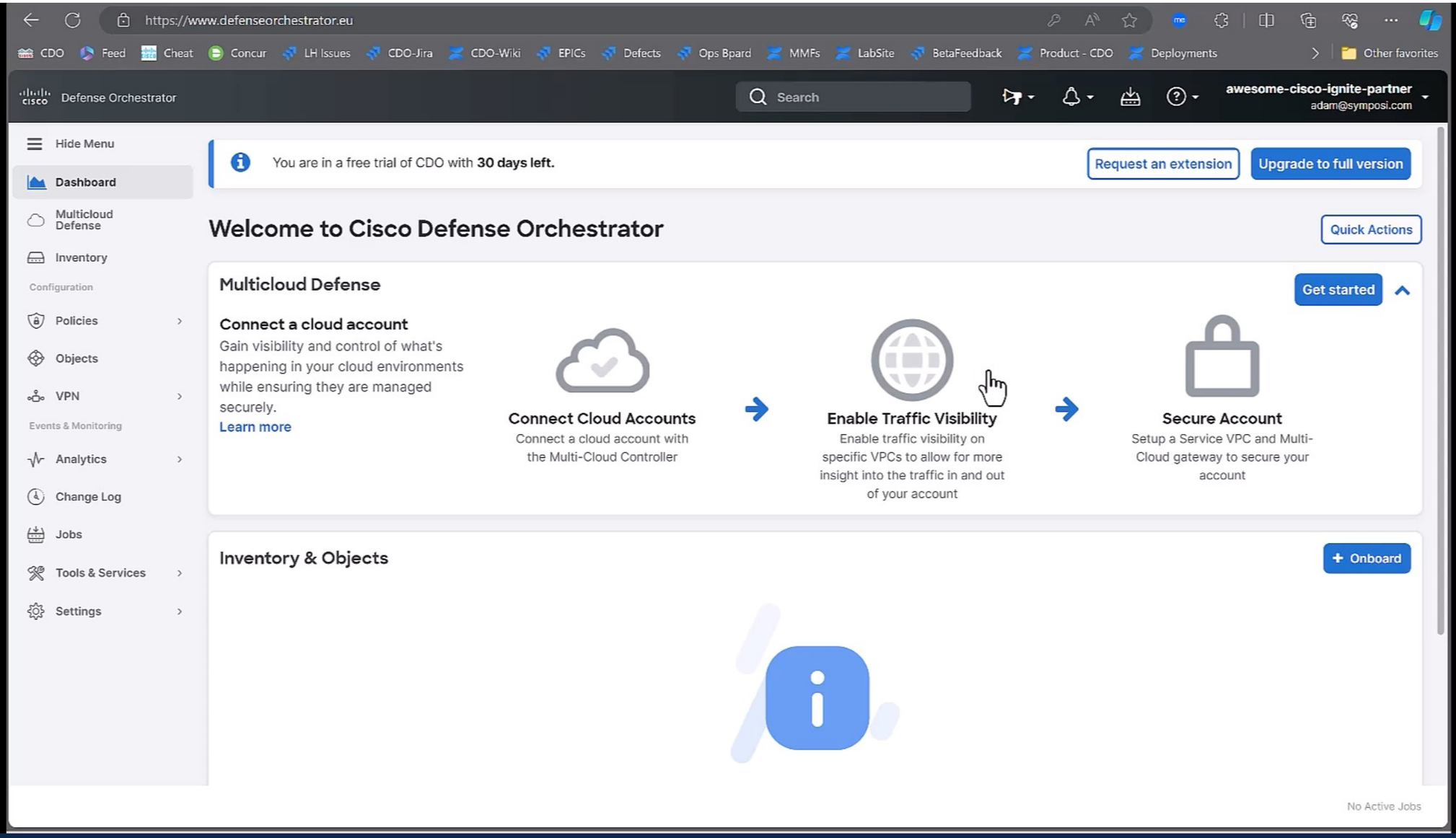
Raise your hand if you didn't complete these

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.



PARTNERS ONLY

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



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.

Full Security POV and Lab Licensing and Software Access guide

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 FTD1010
2. Device Registration and Initial Setup
3. Preparing for Customer Demos FTD1010
4. Software Defined Wide Area Network (SD-WAN)
5. Threat (Attack IQ)
6. (Optional) Remote Access Virtual Private Network (RAVPN) FTD1010

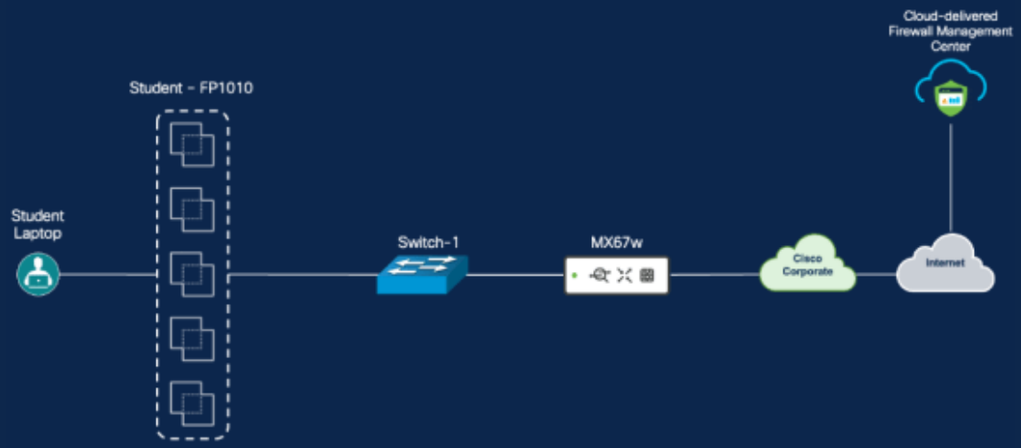
NOTE: The labs for your 1010 are separate from what you will be doing in dCloud

Lab Environment Overview

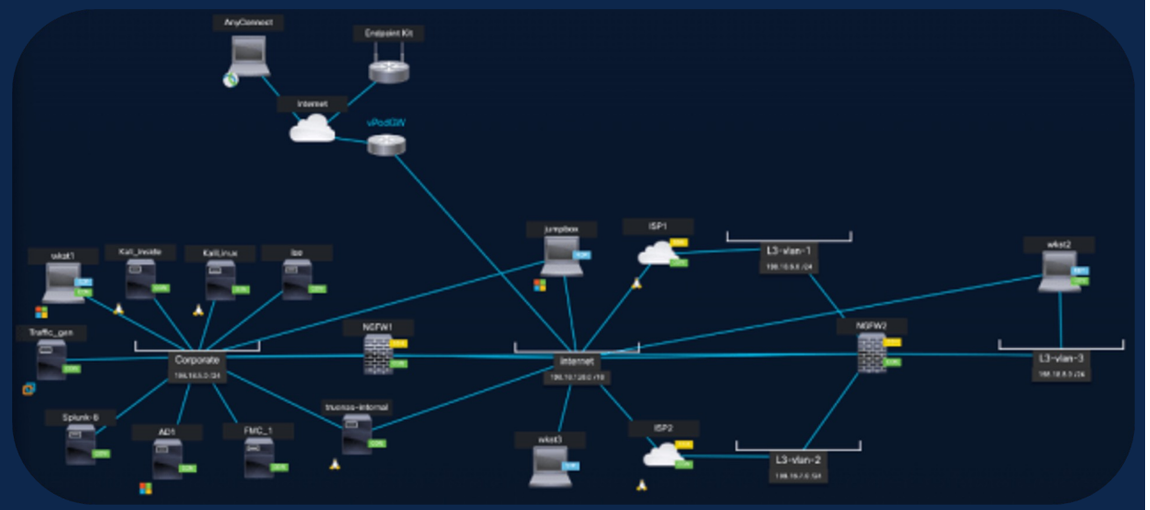
Topology Overview

Topology 1 – On-Site

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

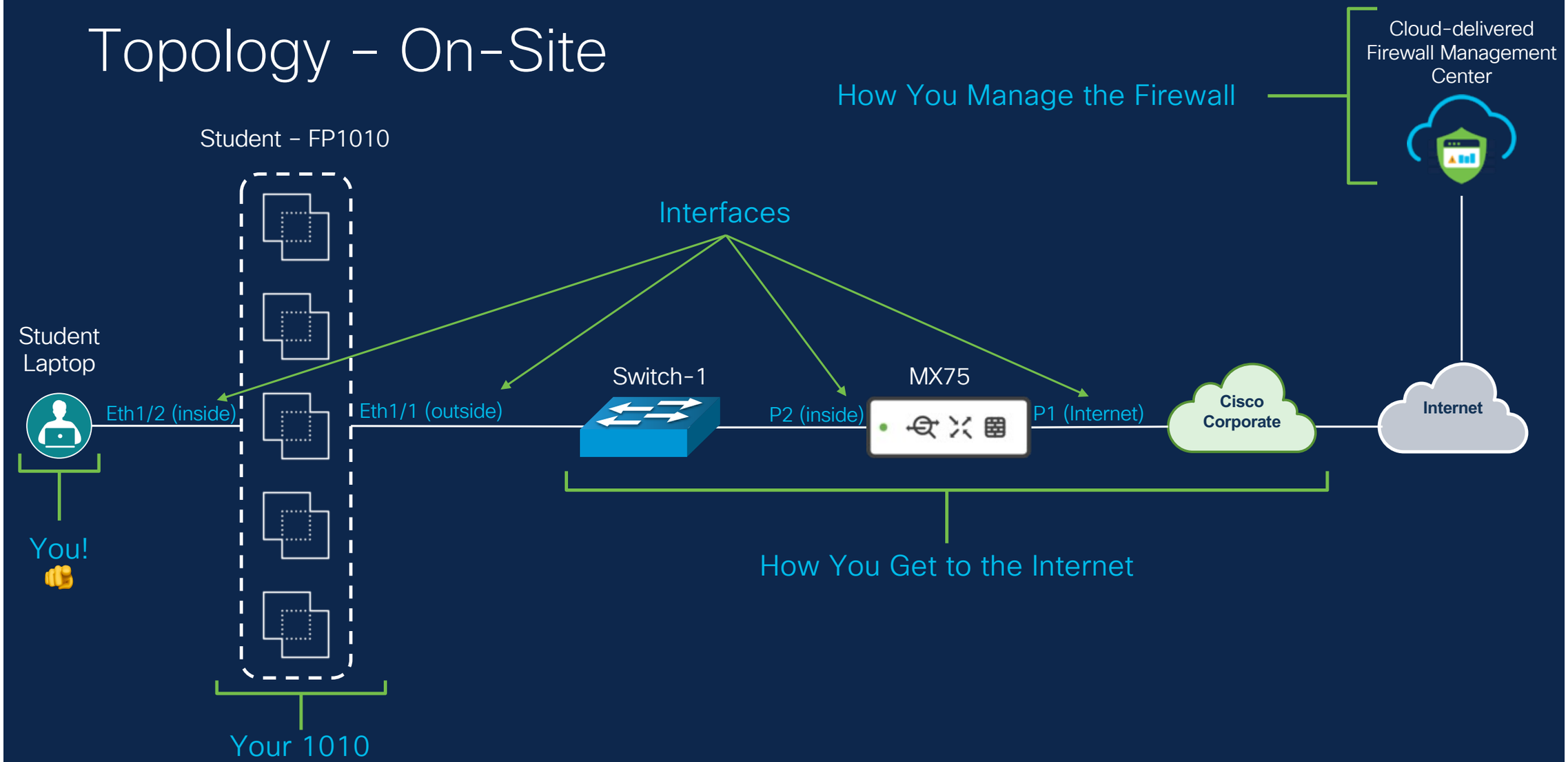


Topology 2 – dCloud



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

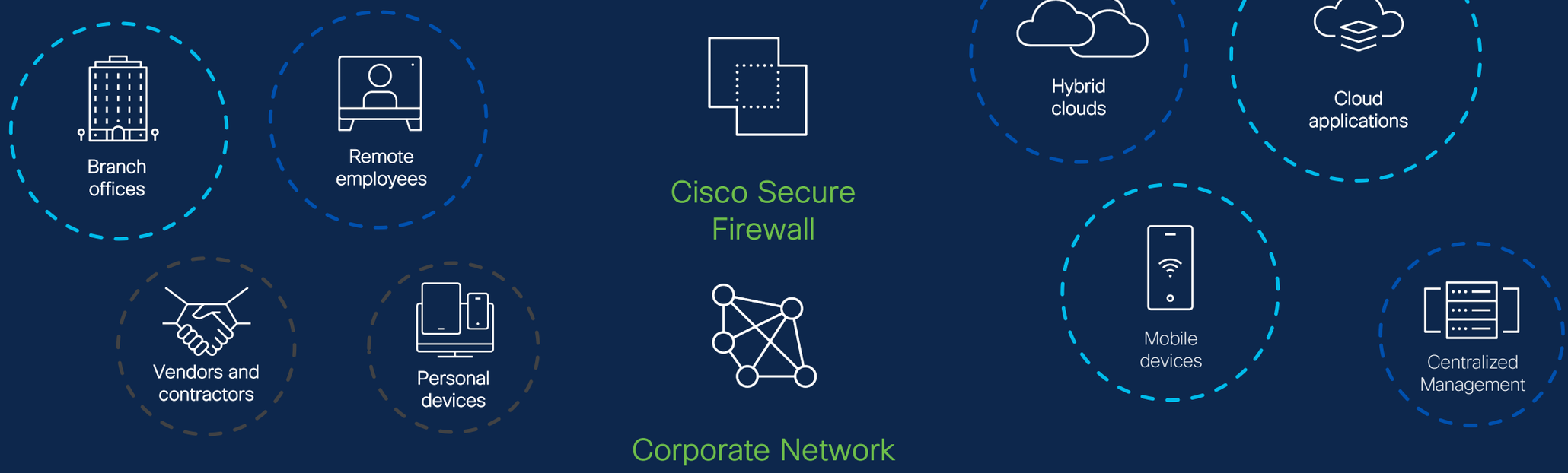
Simplify management, with visibility across your networks

Integrate Network & Security

Transform your network into an extension of your security architecture

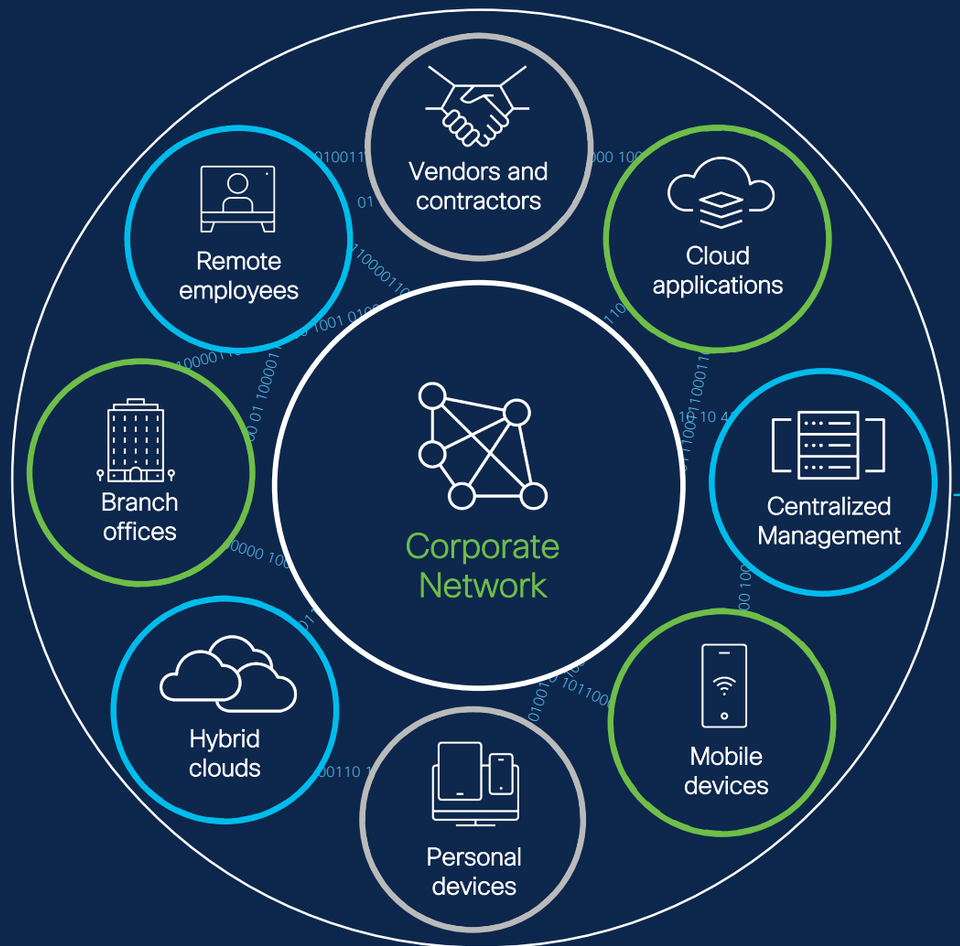
Times have changed...

With multiple perimeters to protect

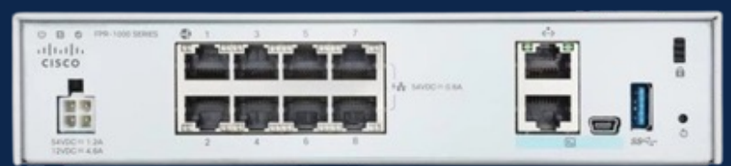


... as a result, the typical environment now requires numerous enforcement points

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

Availability

24x7 Access with Cisco.com credentials

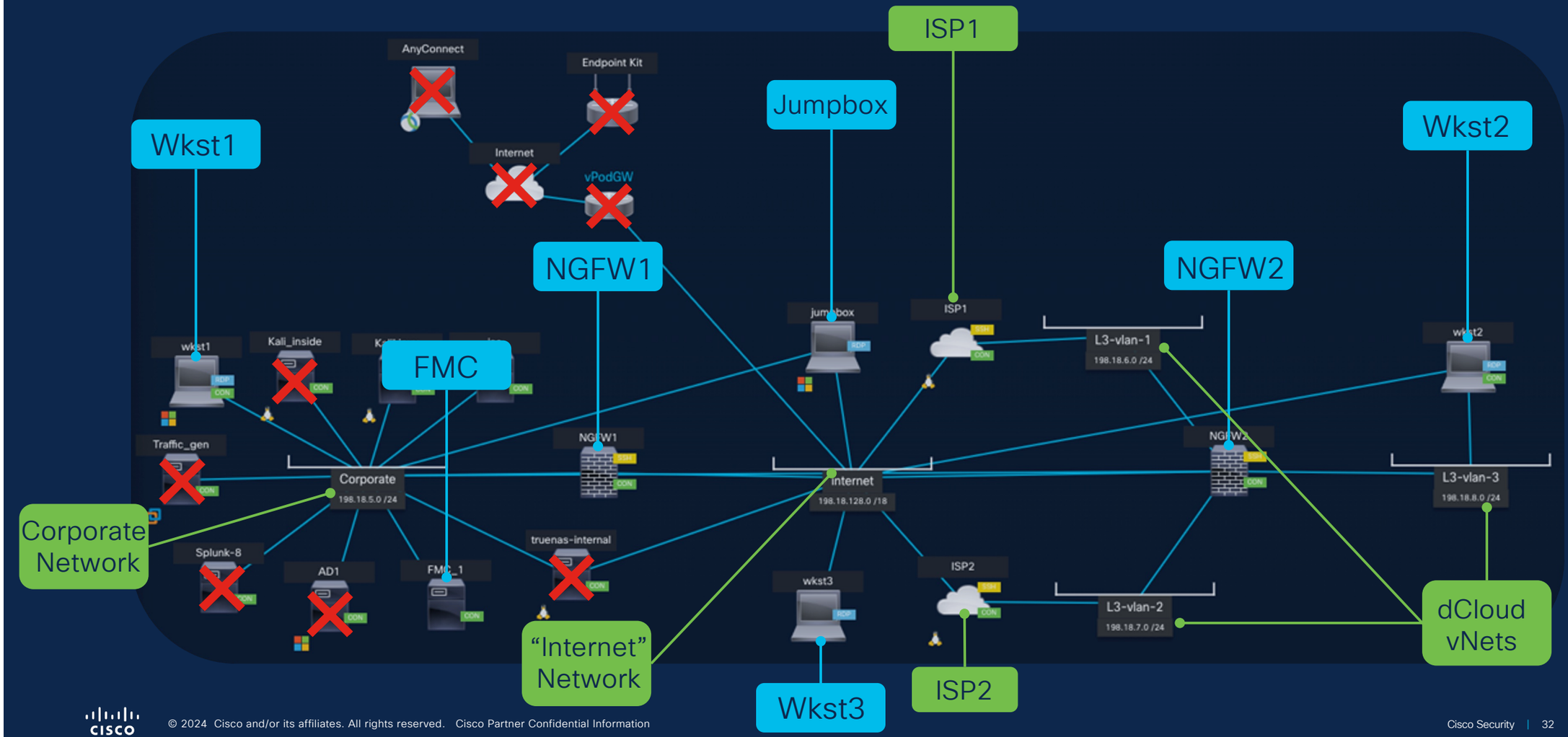
Any Use Case

See only or get hands-on

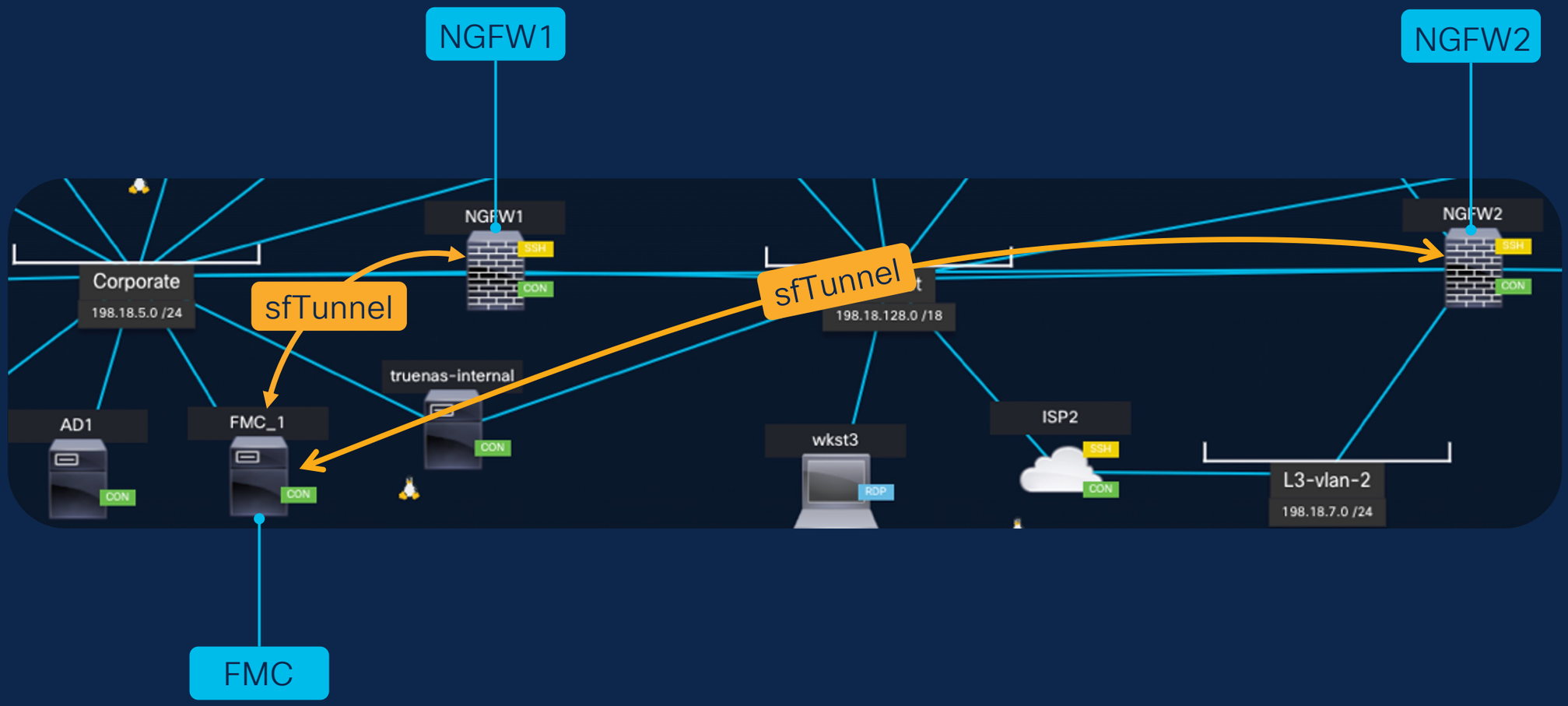
Supported

All demos are completely tested & validated
User feedback encouraged

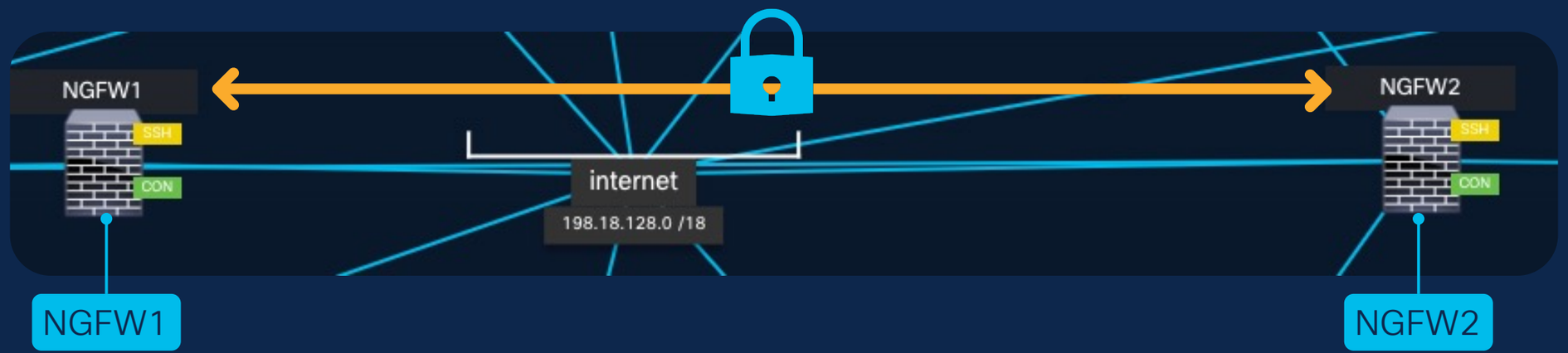
Cisco dCloud - Topology



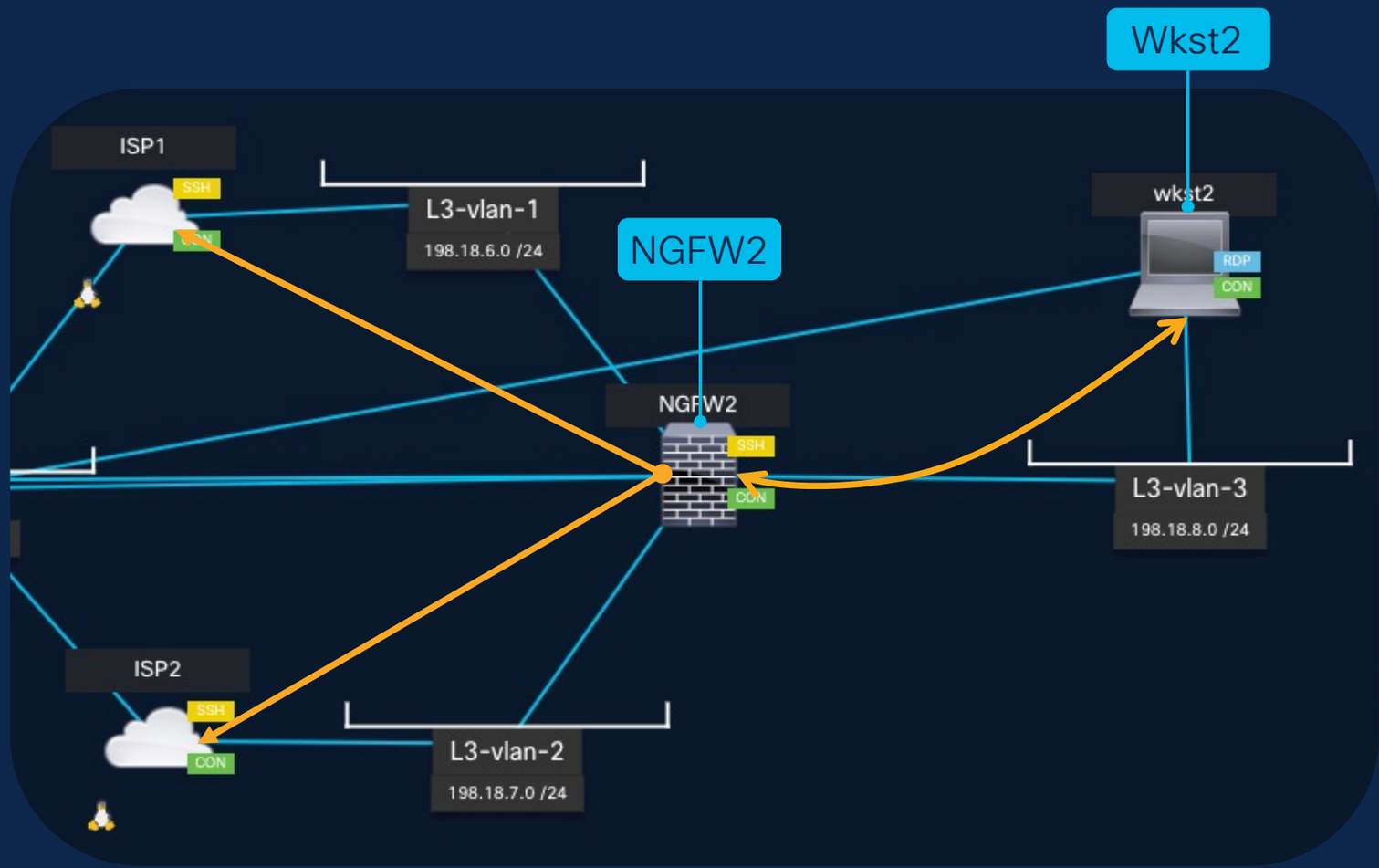
Cisco dCloud – Device Registration



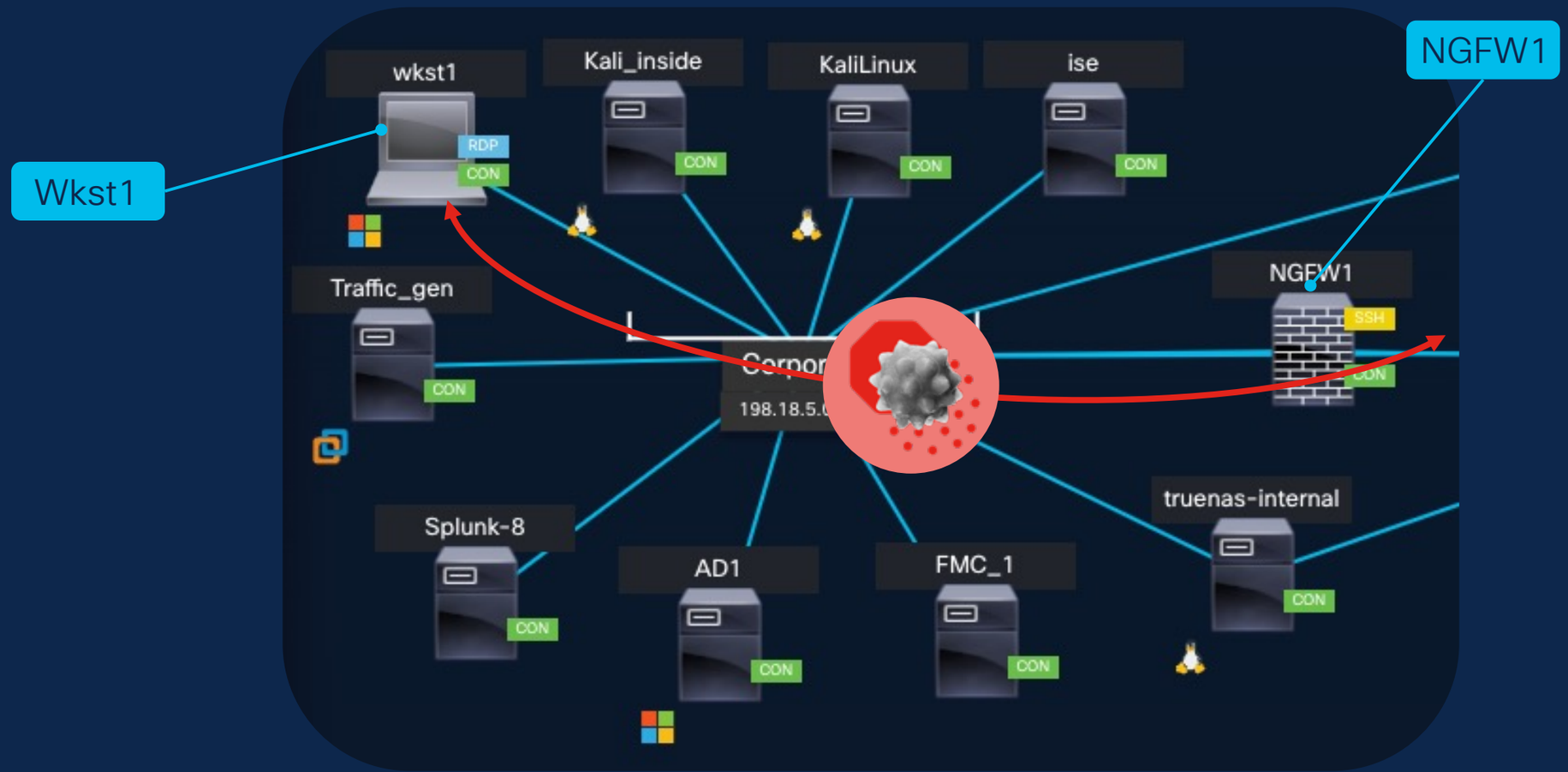
Cisco dCloud – SDWAN Branch to Site Secure VPN



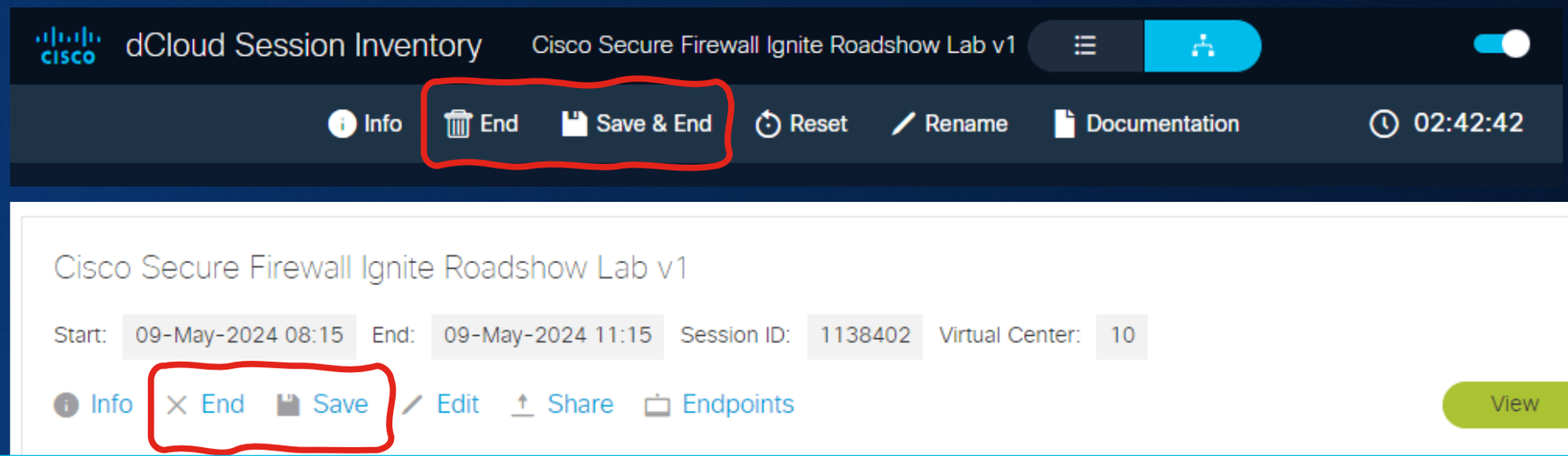
Cisco dCloud – SD-WAN App Aware Policy-based Routing



Cisco dCloud – Threat Efficacy with AttackIQ



Cisco dCloud



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

Getting Started Guide

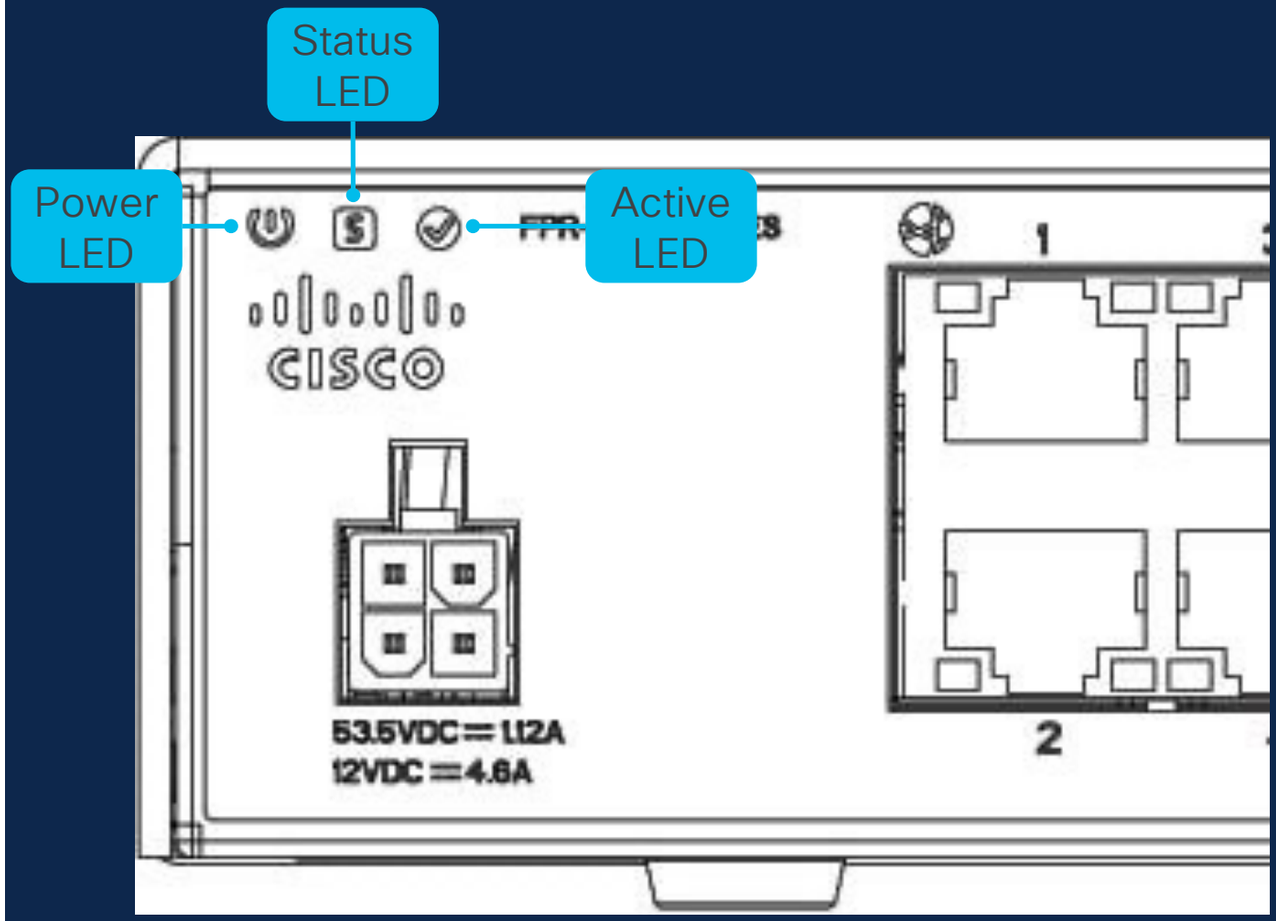
What  cdFMC Validation | Low Touch Provisioning | Upgrading the Firewall

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

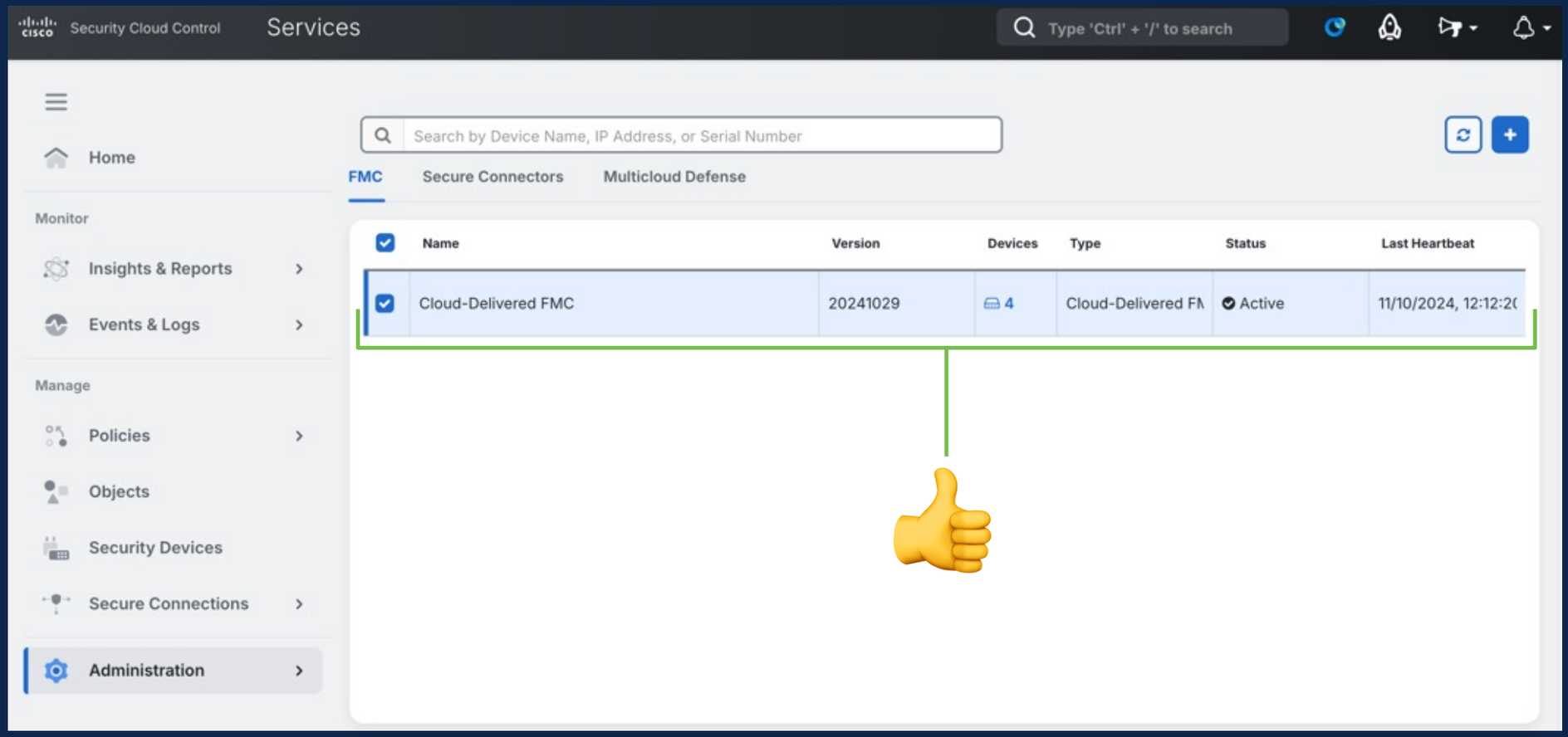


- Three LEDs:
  - Power
  - Status
  - Active
- Normal Operation:
  - Power – Solid Green
  - Status – Solid Green
    - Initially, Green flashing slowly
  - Active – Solid Green
- Contact your proctor if…
  1. Status LED – Solid Amber
  2. Status LED – Flashing green and amber

cdFMC: Is it enabled?

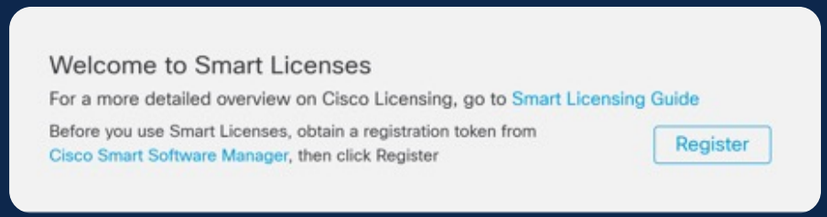
Navigation: SCC > Administration > Integrations > Firewall Management Center

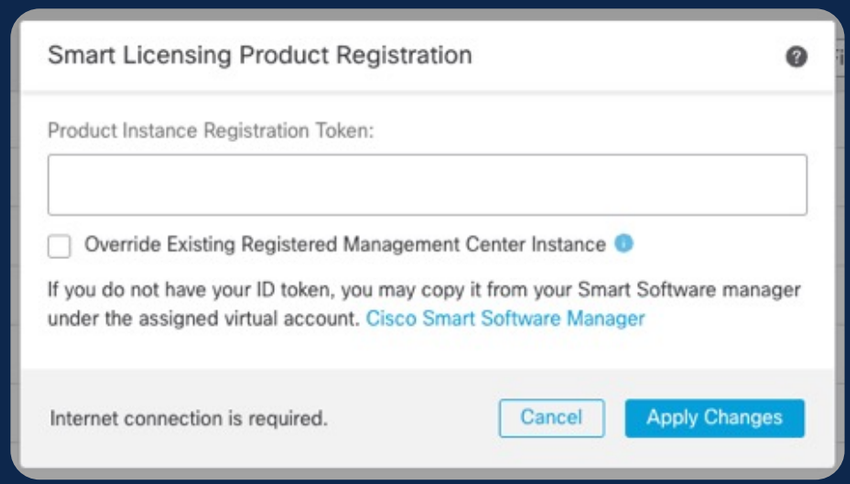
NOTE: You may find you need to navigate away or log out and back in for the cdFMC Status column to refresh

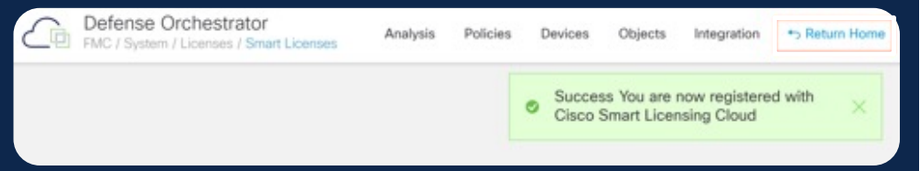


cdFMC: Is it licensed?

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







Cloud Assisted Provisioning

Low Touch Provisioning

Low-skilled branch staff

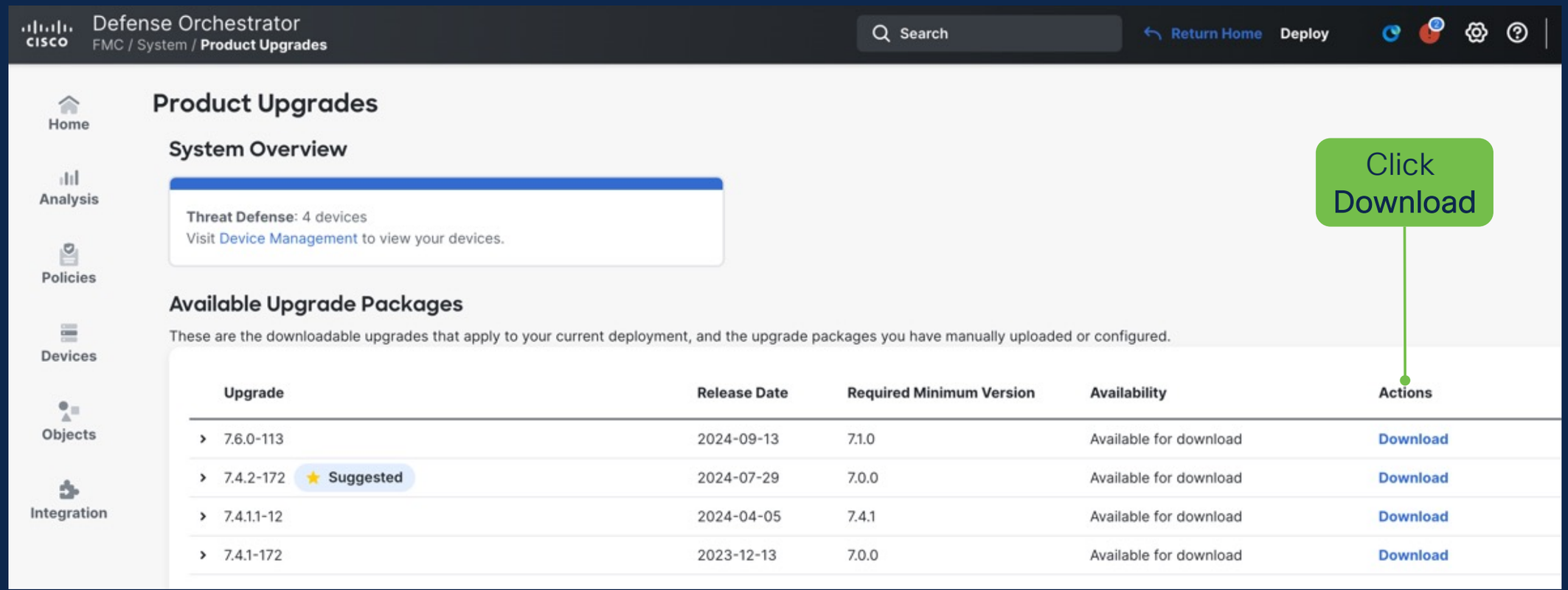
Device Auto onboards upon bootup

No pre-configuration

Onboarding using Serial Number

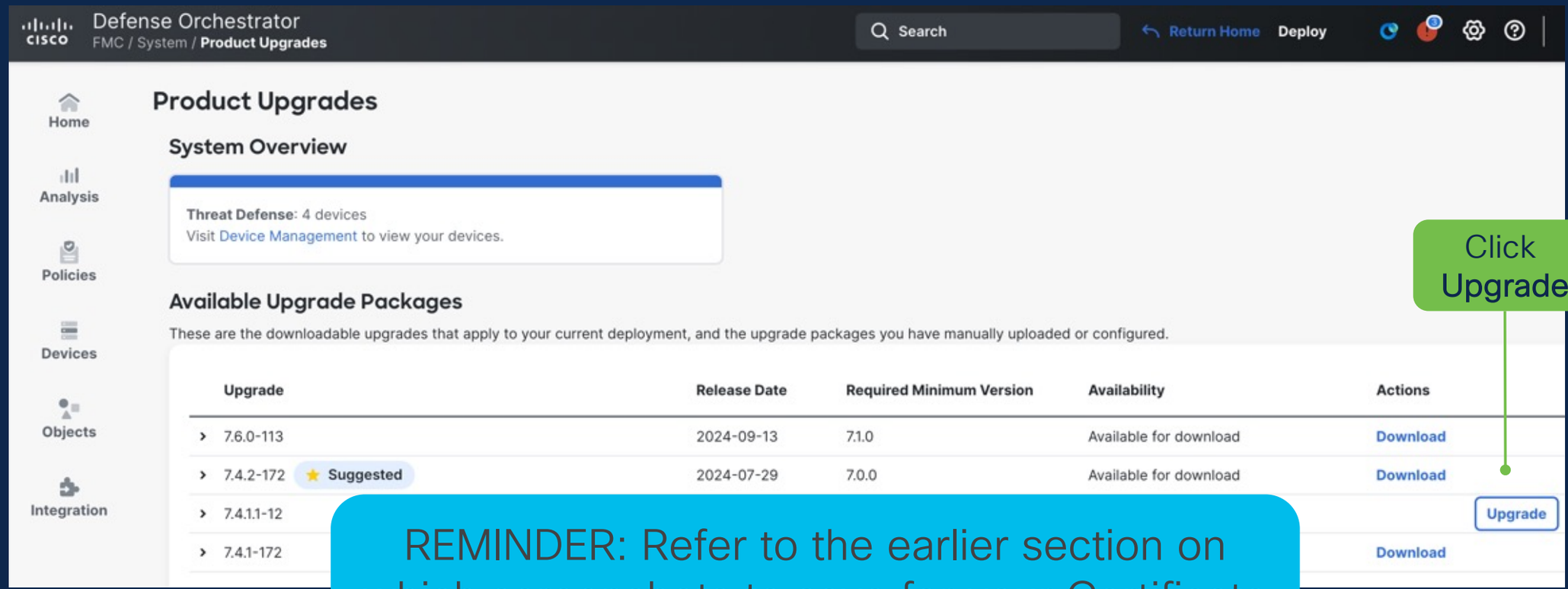
Upgrade! (1/2)

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



Upgrade! (2/2)

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



Click Upgrade

REMINDER: Refer to the earlier section on which screenshots to save for your Certificate of Completion after your upgrade completes

Important!

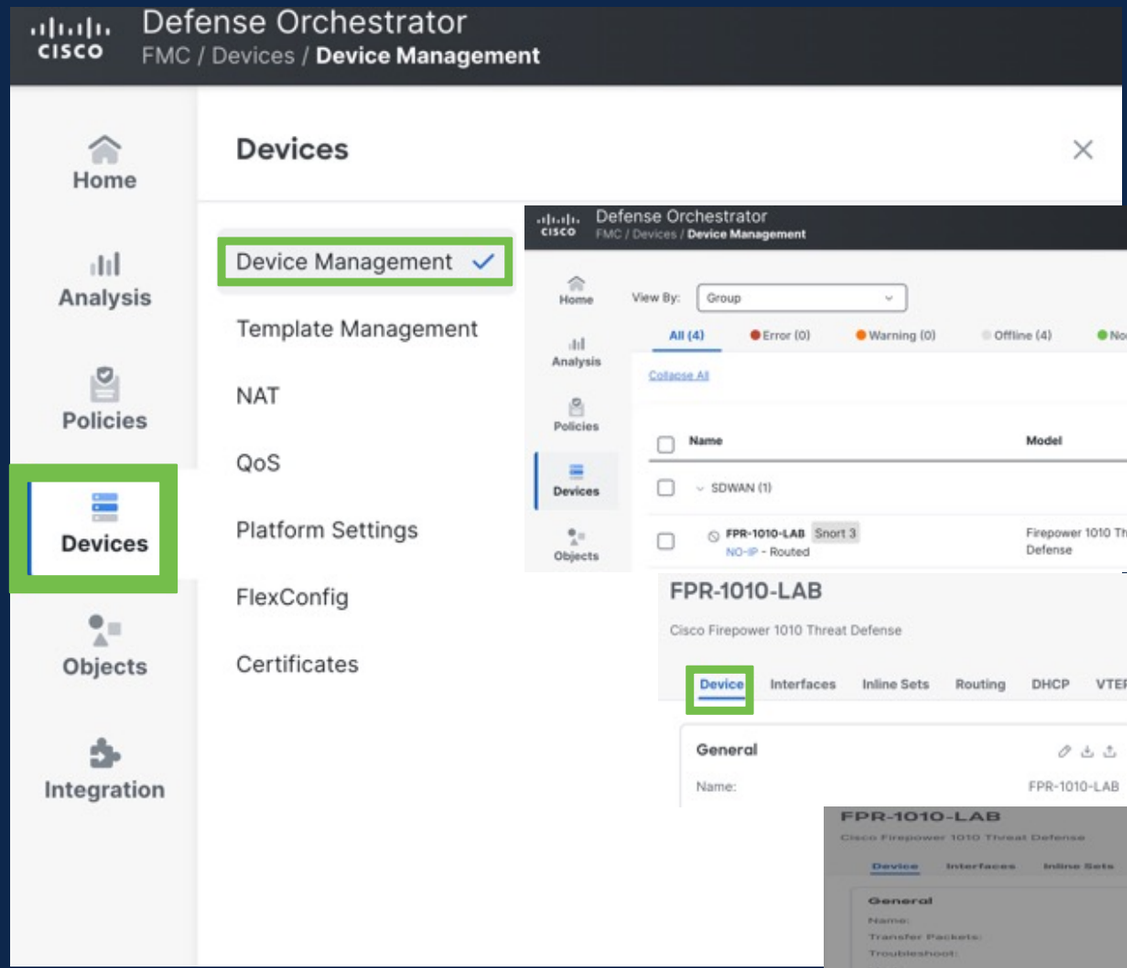
Unlike an ASA, there is no running config or startup config.

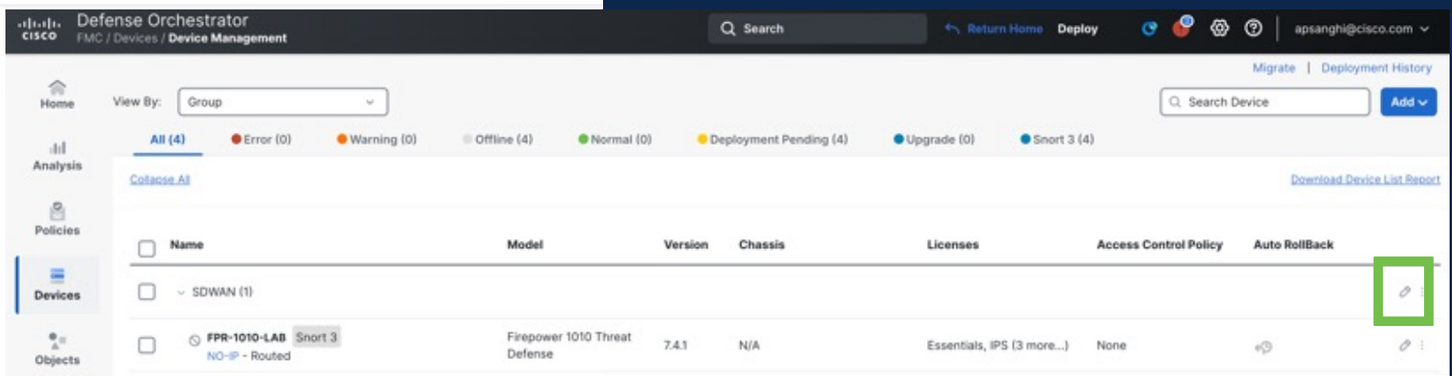
With FTD, there are several databases and services running that must be shut down safely before removing power.

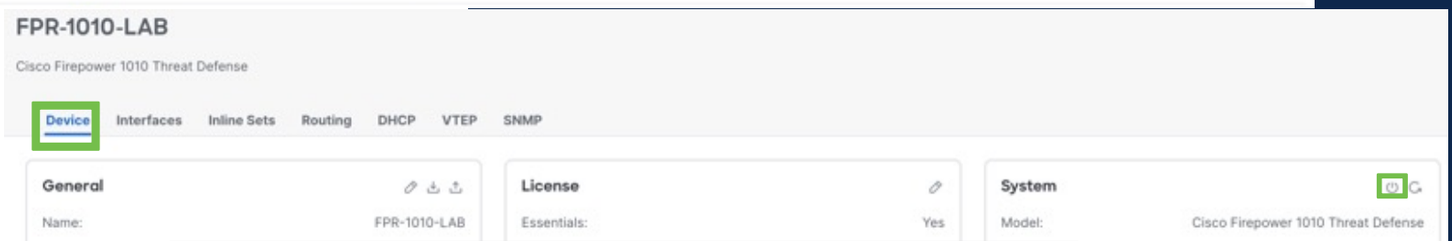
*** Yes, even for troubleshooting ***

Important

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!

CERTIFCATION ITEMS!

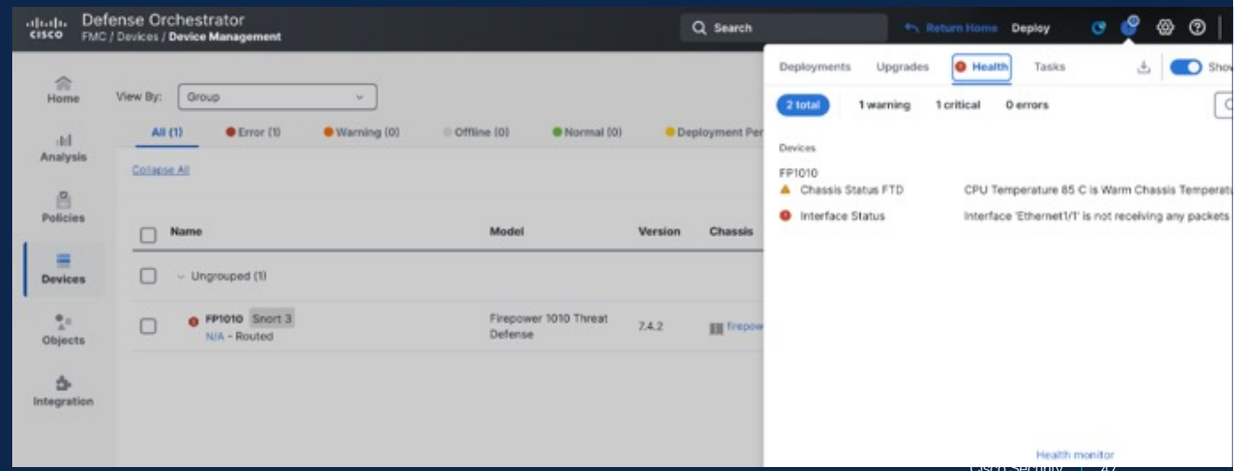
First Steps Guide

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

Getting Started Guide

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

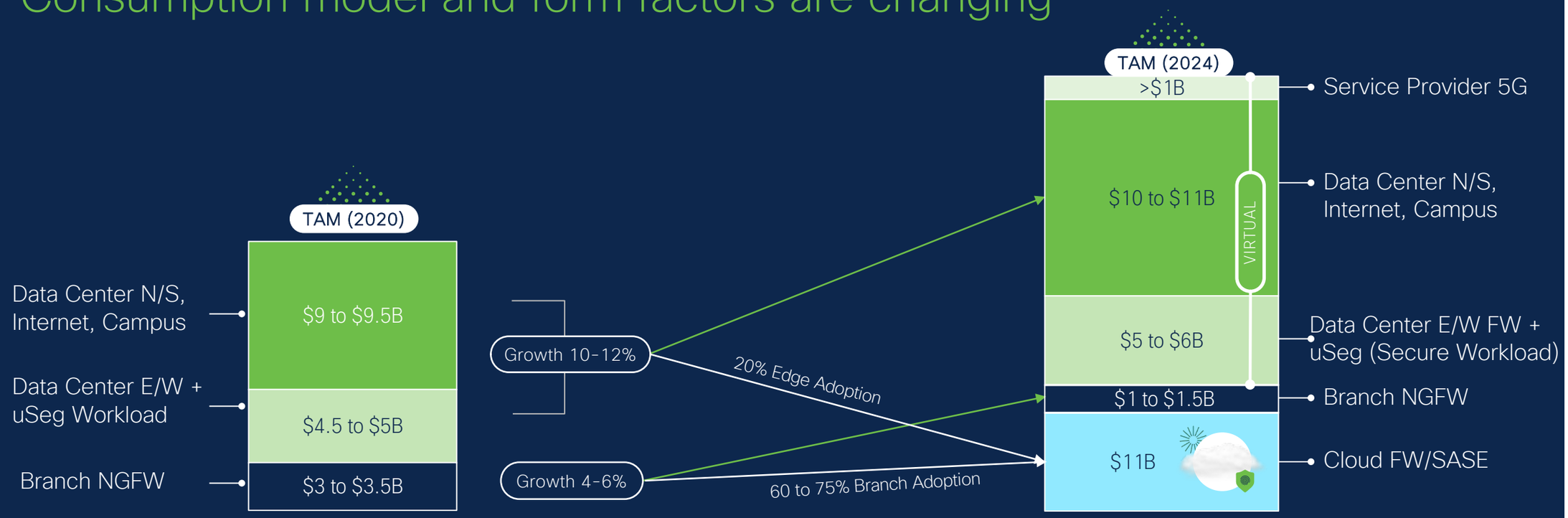
NOTE: Many of the Red (!) can safely be ignored. When there is nothing connected to the management0 or LAN interfaces, these will flag Red Health alerts.



Cisco’s Vision & Strategy

The firewall market is growing

Consumption model and form factors are changing



Source: External Analysts, Cisco Internal Analysis

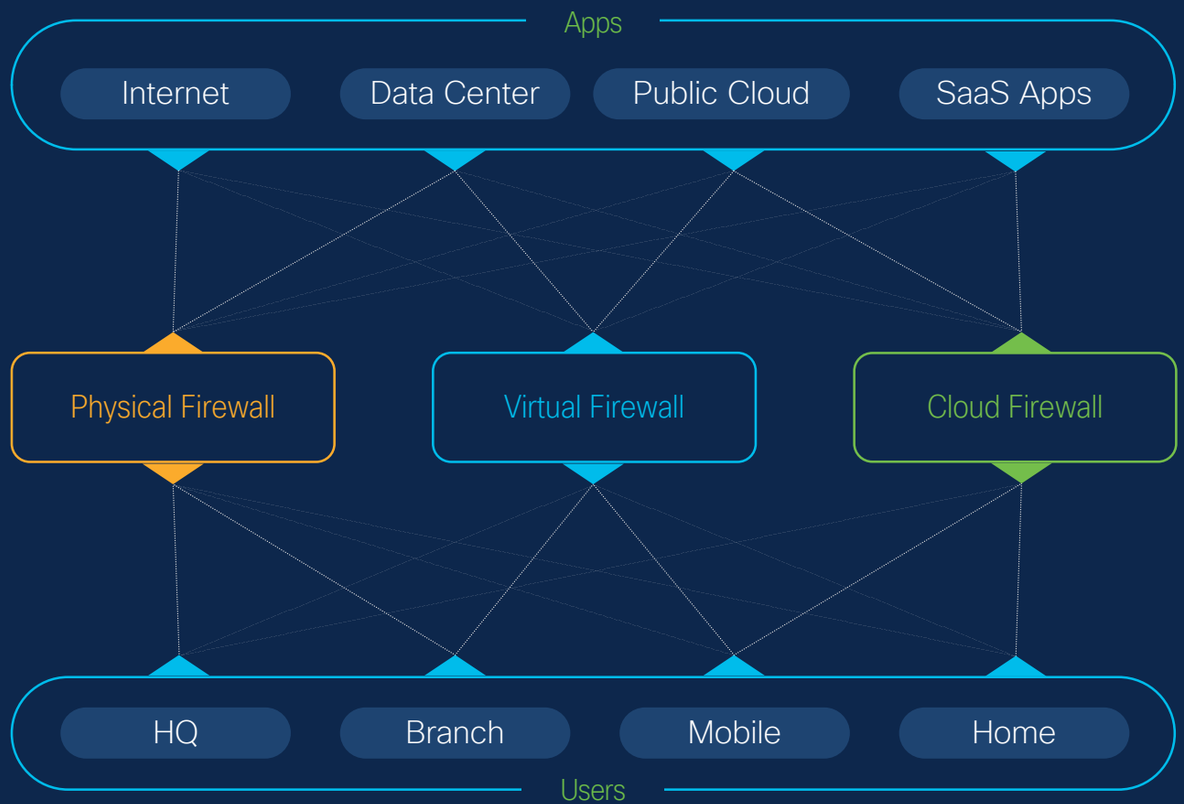
Branch transitioning to cloud-delivered SSE

Data Centers transitioning to virtual and **C**loud Native FW

Security stack becoming agile and moving closer to applications

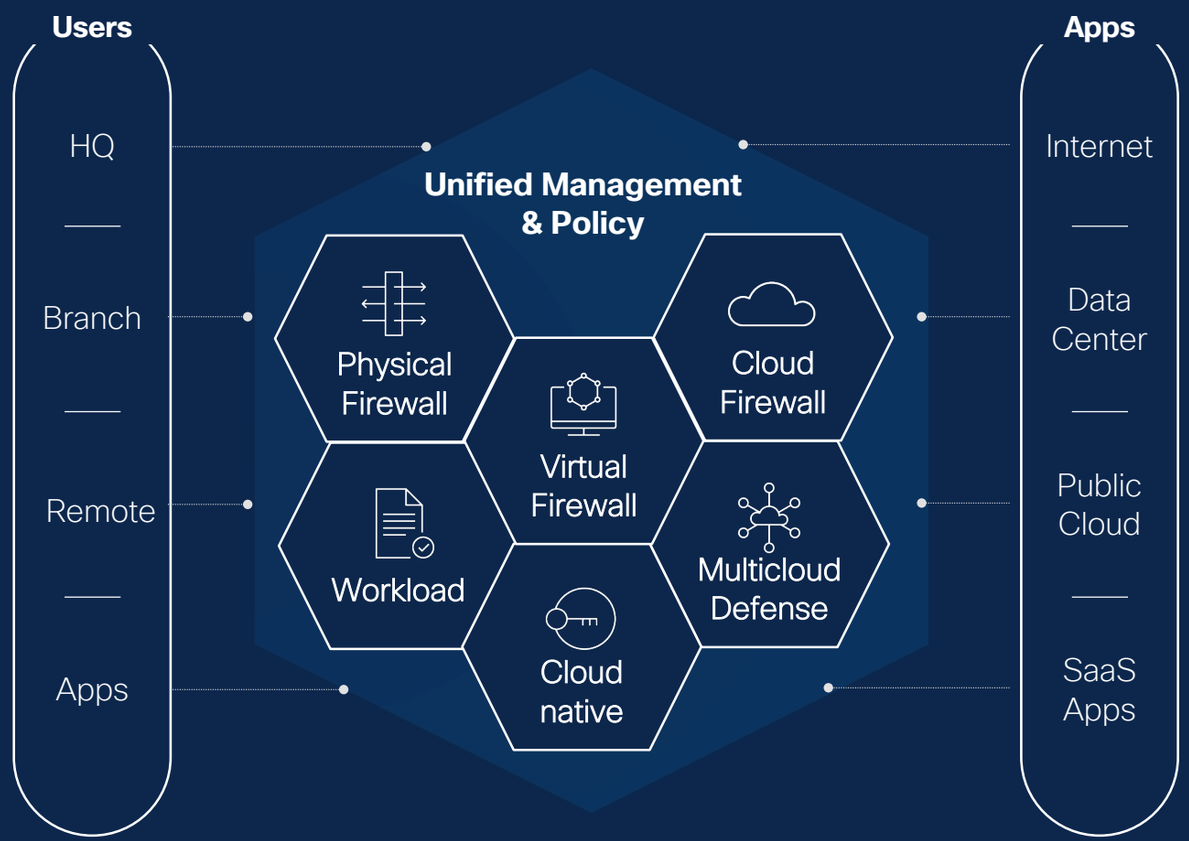
Enterprise Firewall Market Today

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

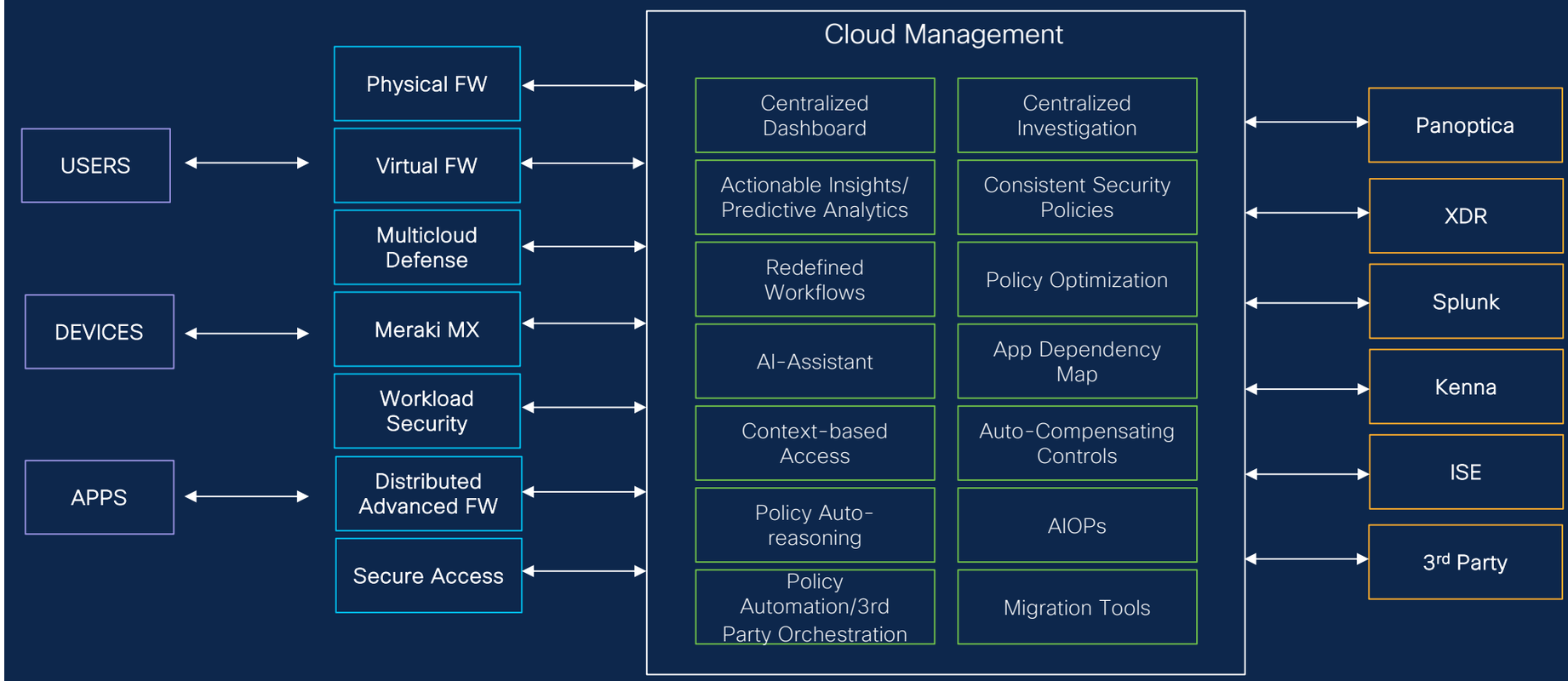
Firewall capabilities expanding to application, networking, and user

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

- AI Assistant
- Cloud On-ramp, Object Share
- AIOps for Firewall
- Kenna Integration

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 Engine | ML/ Contextual

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

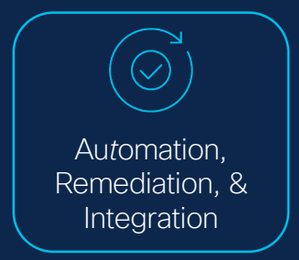
ISE & Catalyst | Meraki | Secure Access

Ease of purchase and deployment of multiple security and networking

Our Firewall has comprehensive capabilities

Superior Threat Protection - AI Assistant and SnortML

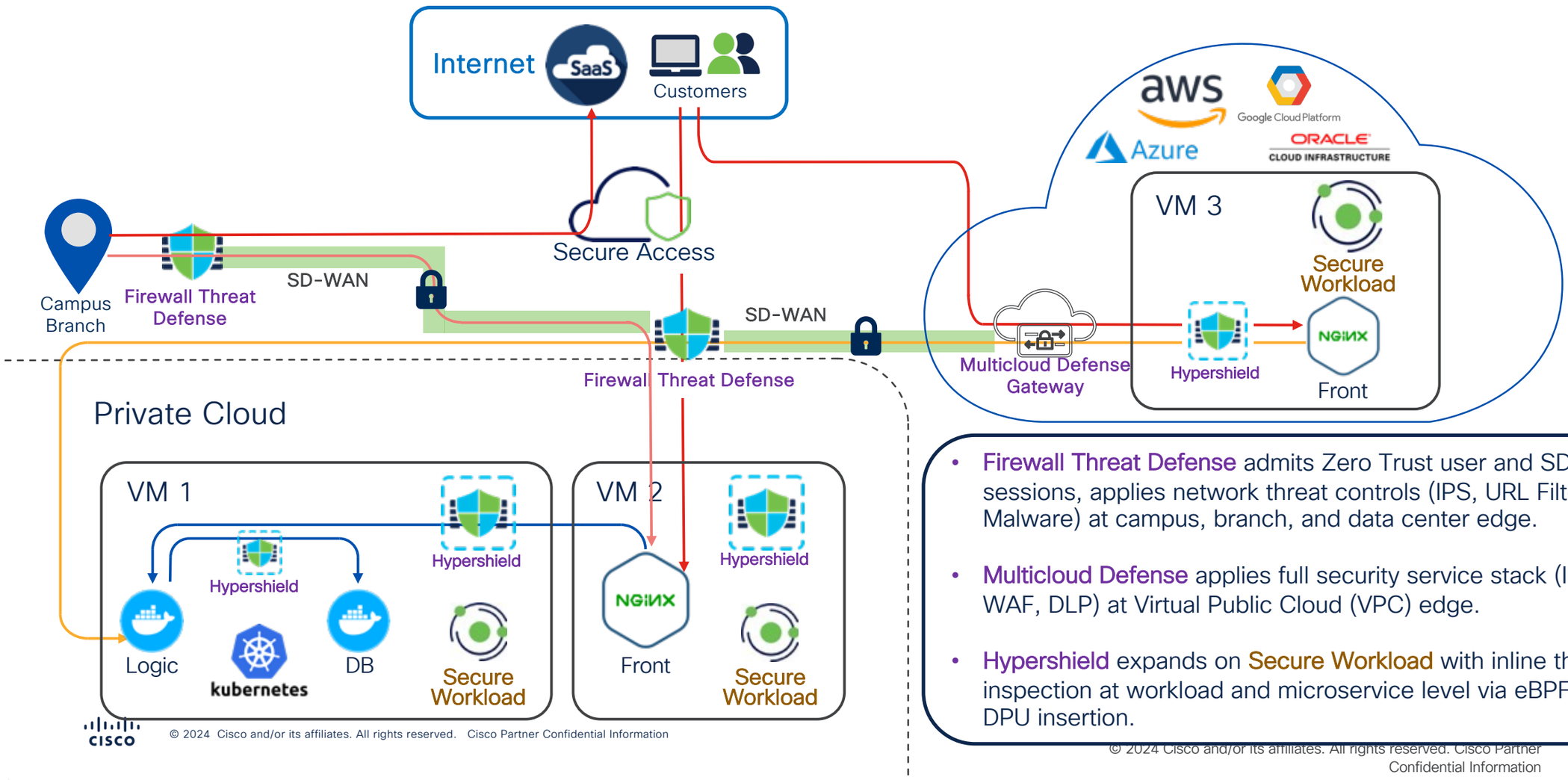
AI Assistant, SnortML - Configuration and Analytics Console



Cisco Talos Security Intelligence

Firewall Vision: Network, Workload, and Cloud

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



- **Firewall Threat Defense** admits Zero Trust user and SD-WAN sessions, applies network threat controls (IPS, URL Filtering, Malware) at campus, branch, and data center edge.
- **Multicloud Defense** applies full security service stack (IPS, WAF, DLP) at Virtual Public Cloud (VPC) edge.
- **Hypershield** expands on **Secure Workload** with inline threat inspection at workload and microservice level via eBPF and DPU insertion.

Preparing for Customer Demo Overview

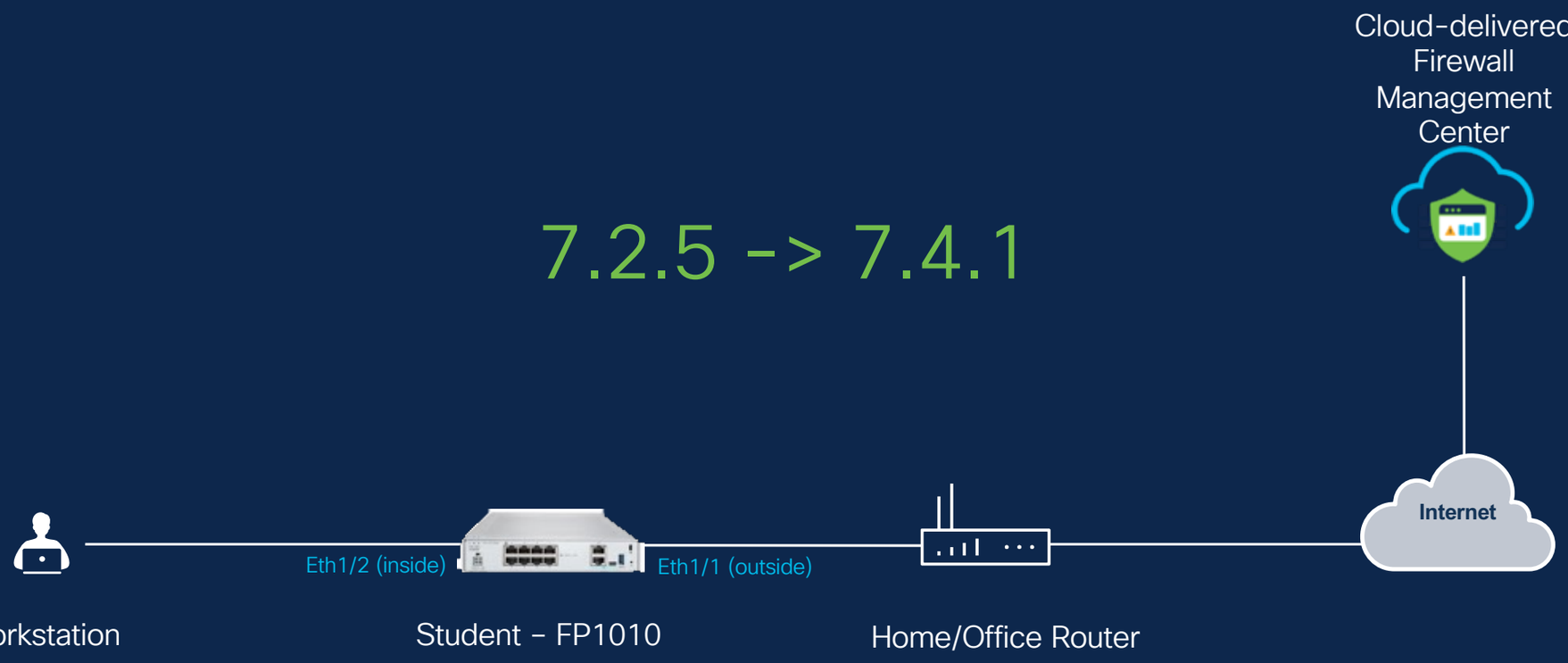
What  Complete the 1010 upgrade | Initial configuration

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

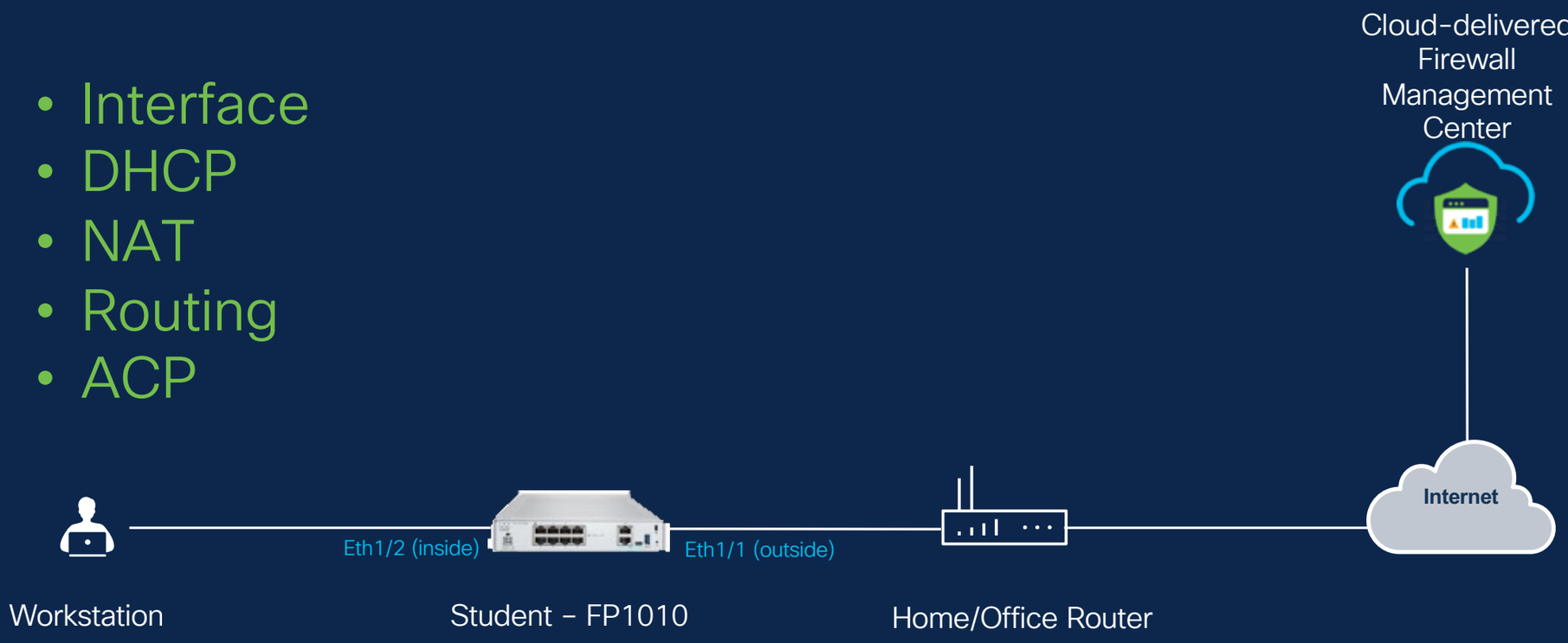
Step 1: Validate the Upgrade



Preparing For Customer Demo

Step 2: Getting your 1010 ready for the demo

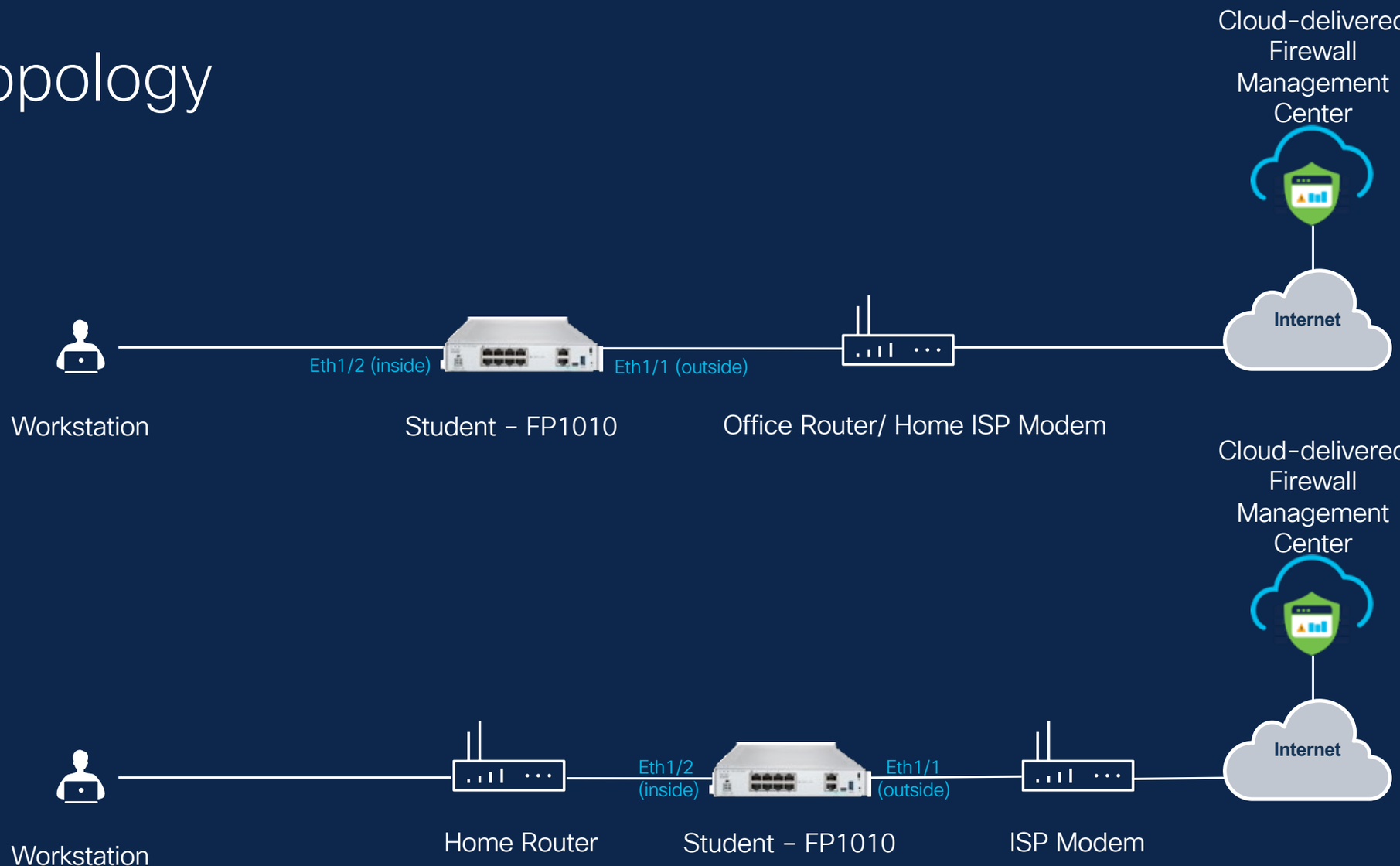
- Interface
- DHCP
- NAT
- Routing
- ACP



Objectives

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

Topology



Important

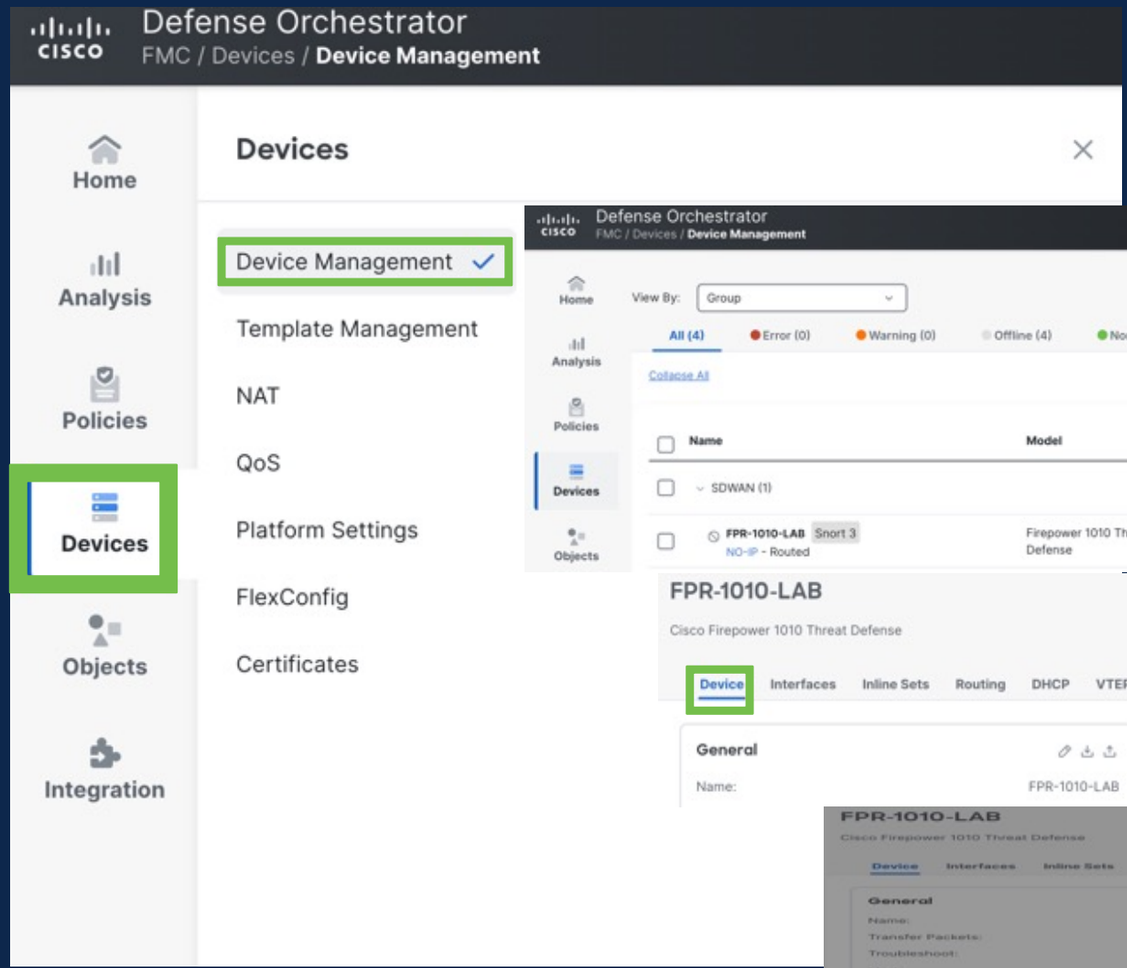
Unlike an ASA, there is no running config or startup config.

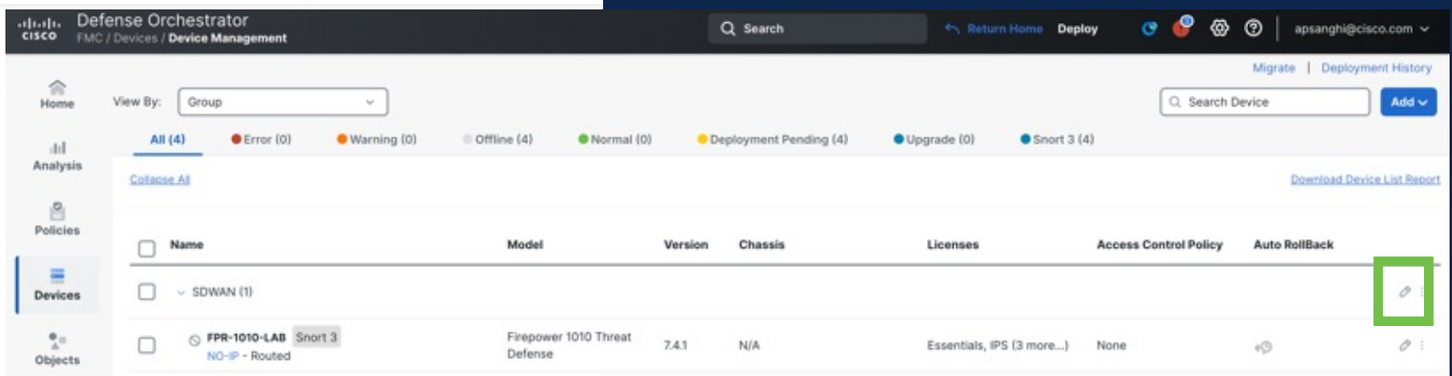
With FTD, there are several databases and services running that must be shut down safely before removing power.

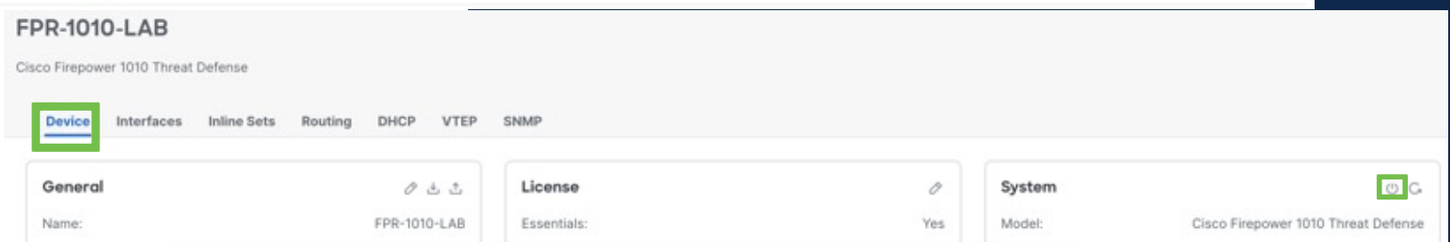
*** Yes, even for troubleshooting ***

Important

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

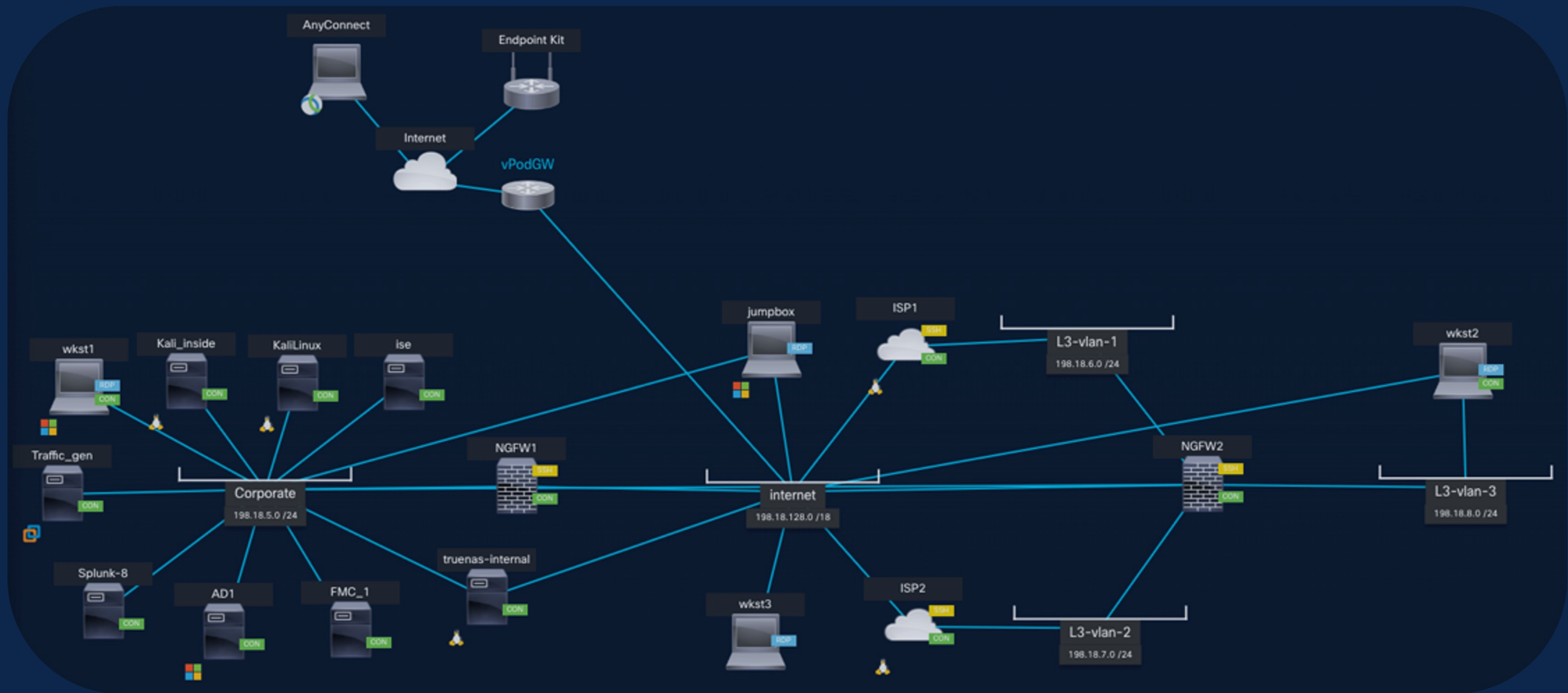
Device Registration

What  Virtual Threat Defense Registration and Configuration

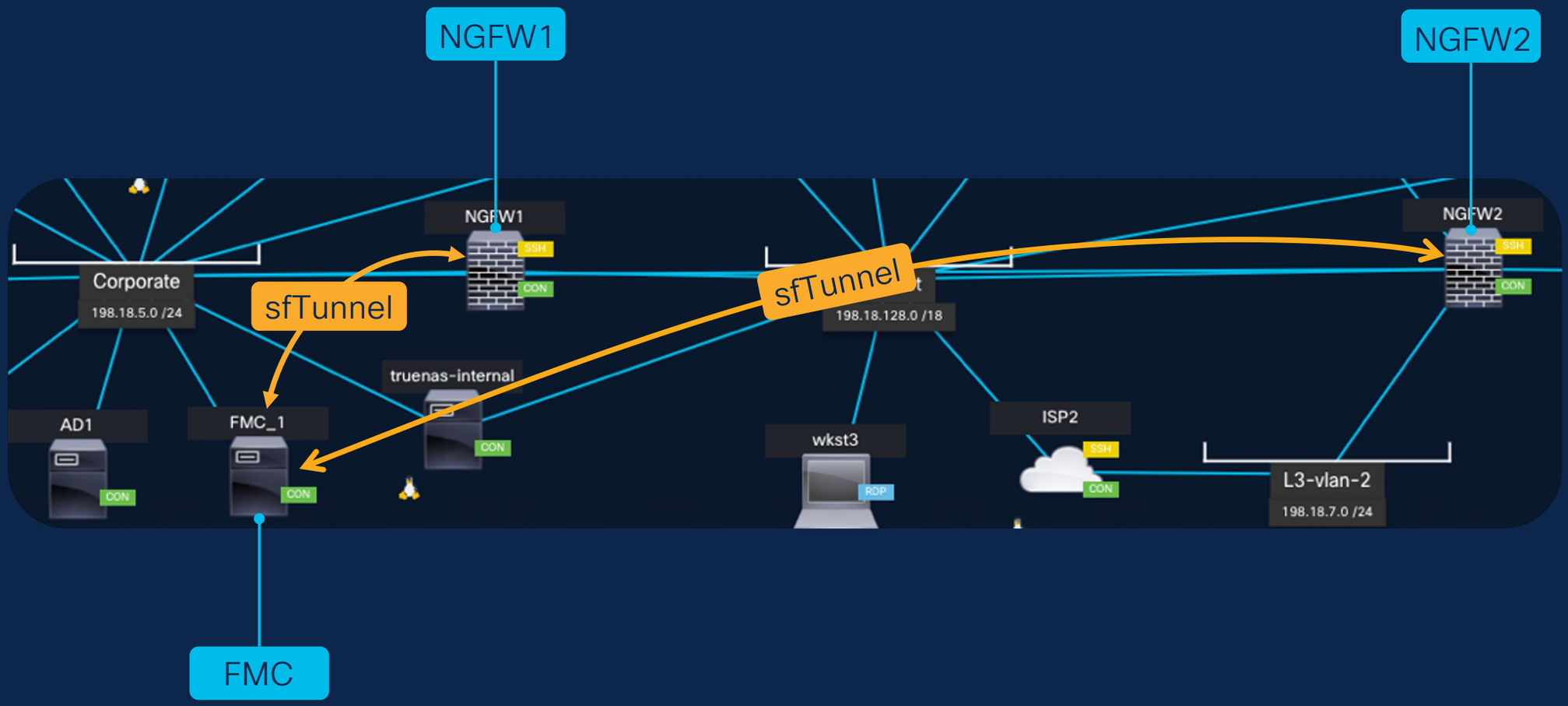
Why  Setting up the virtual Threat Defenses for the upcoming lab tasks

How  Via the on-prem Firewall Management Center hosted in dCloud

Topology



Cisco dCloud – Device Registration

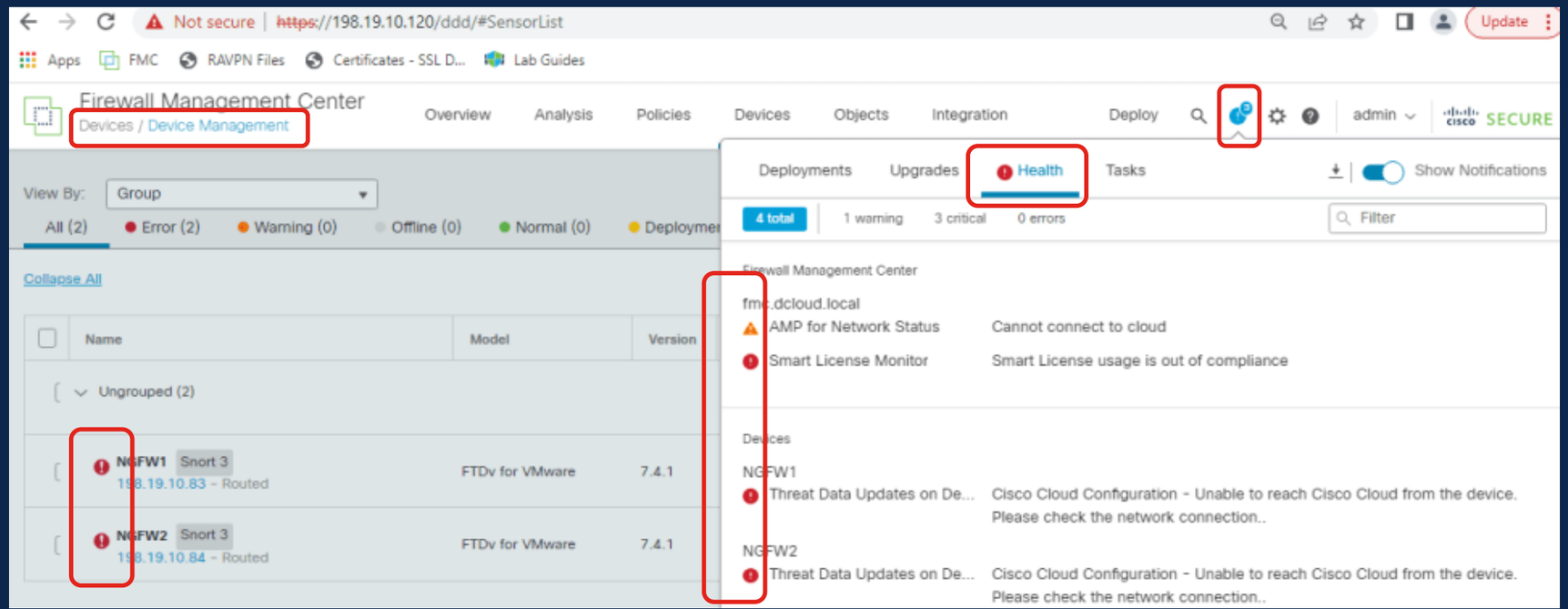


Lab Time!

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.

Device Registration and Initial Setup

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



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

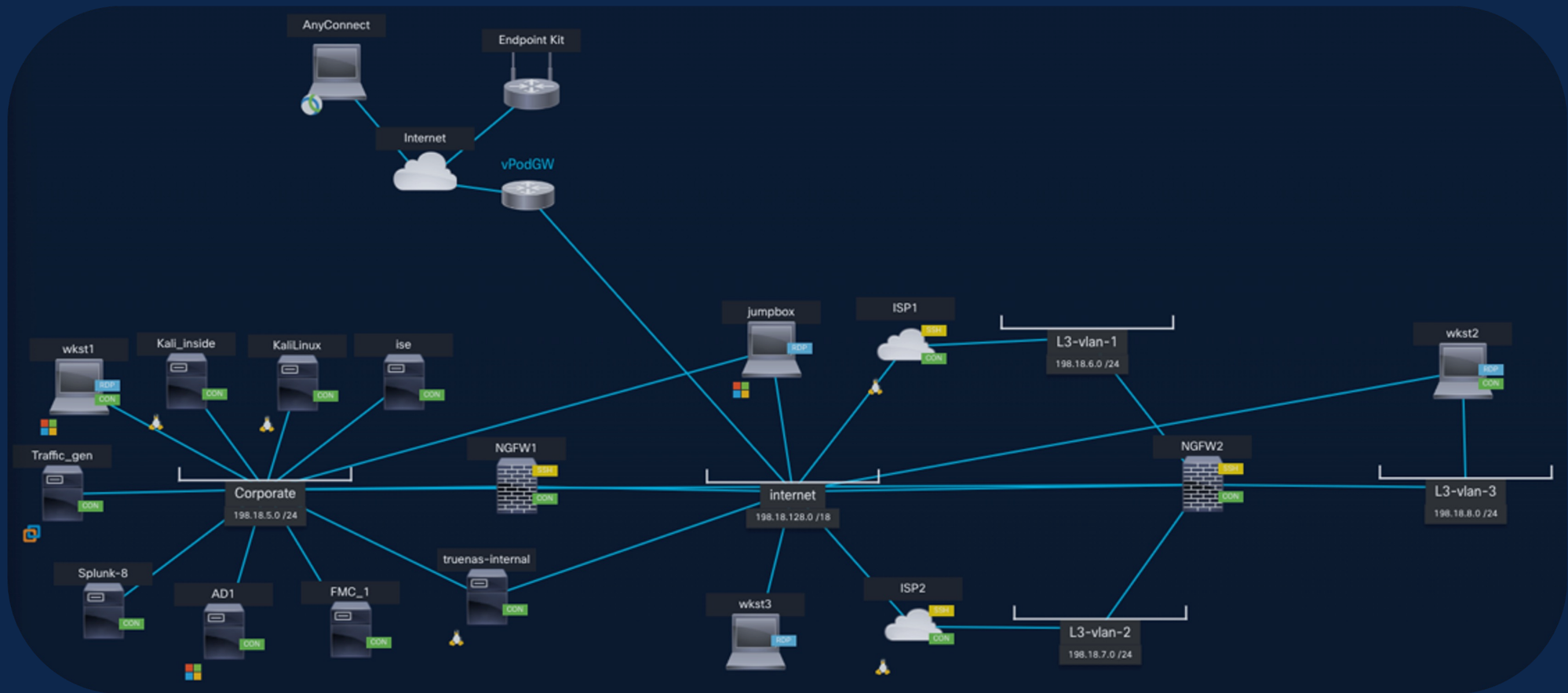
SD-WAN Definition

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.

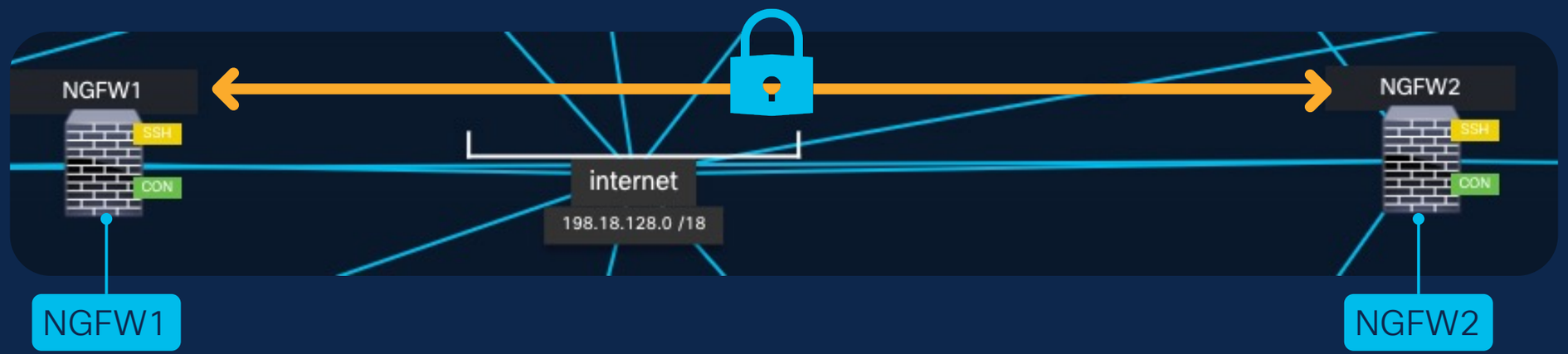
Source: Gartner

Topology



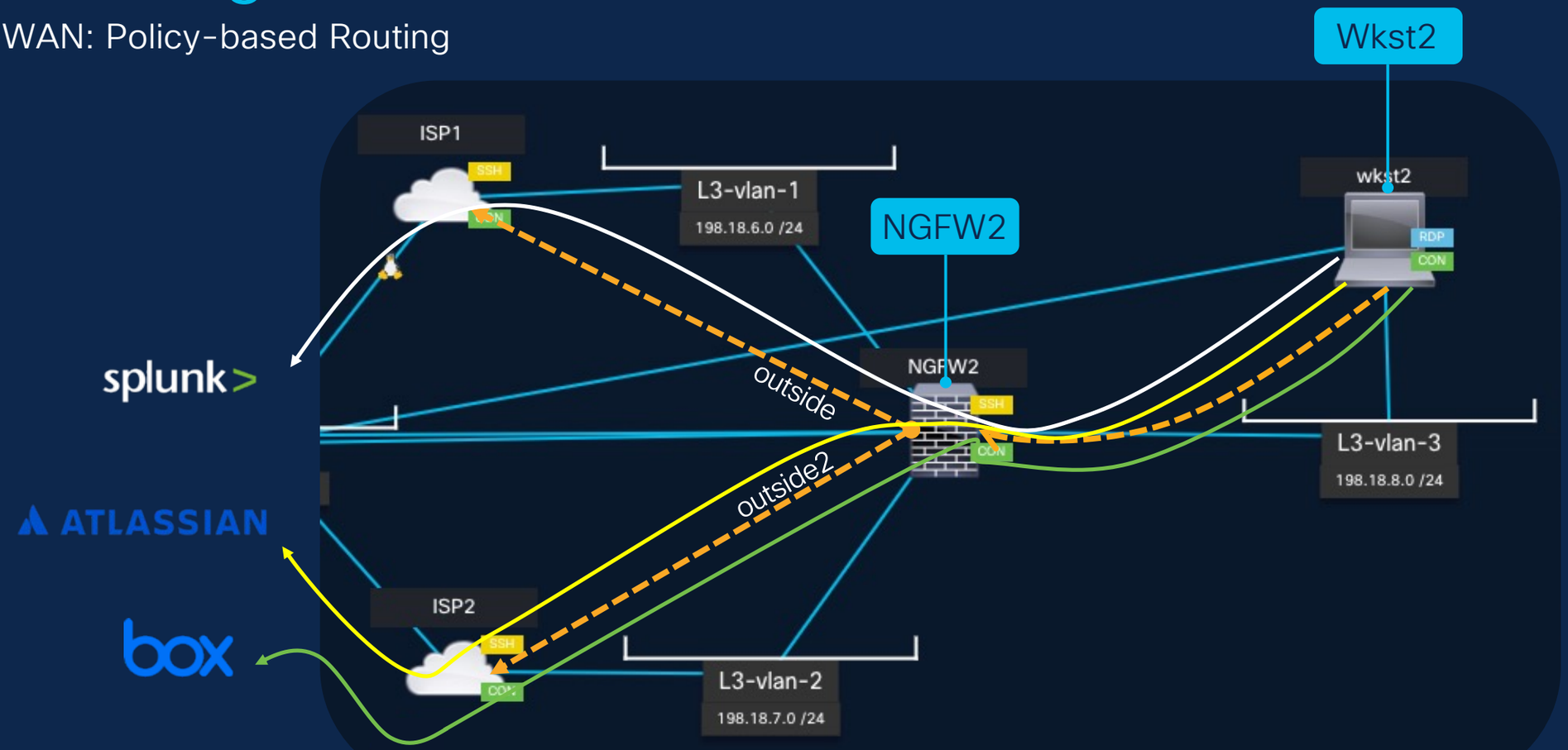
Simplified Branch to Hub communication

SD-WAN: Site-to-Site VPN

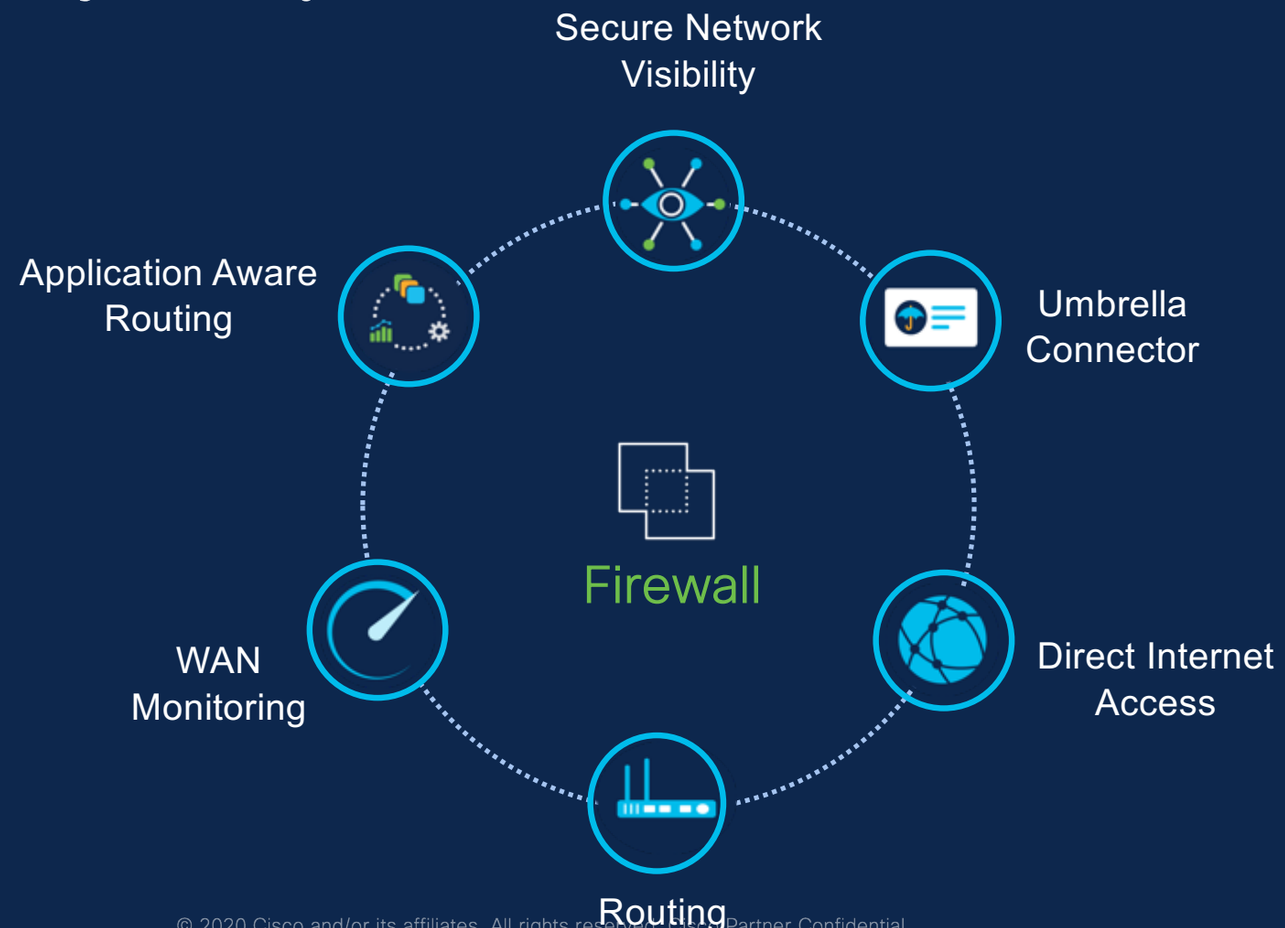


Application based routing using dynamic path monitoring

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

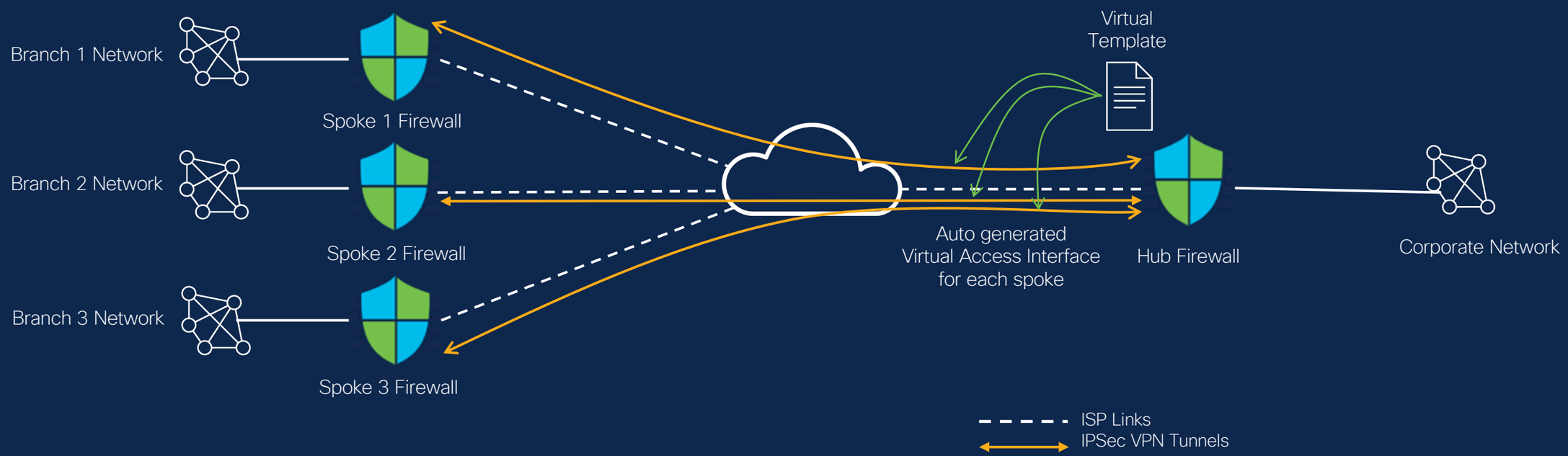
Direct Internet Access for Public Cloud and Guest Traffic

- 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

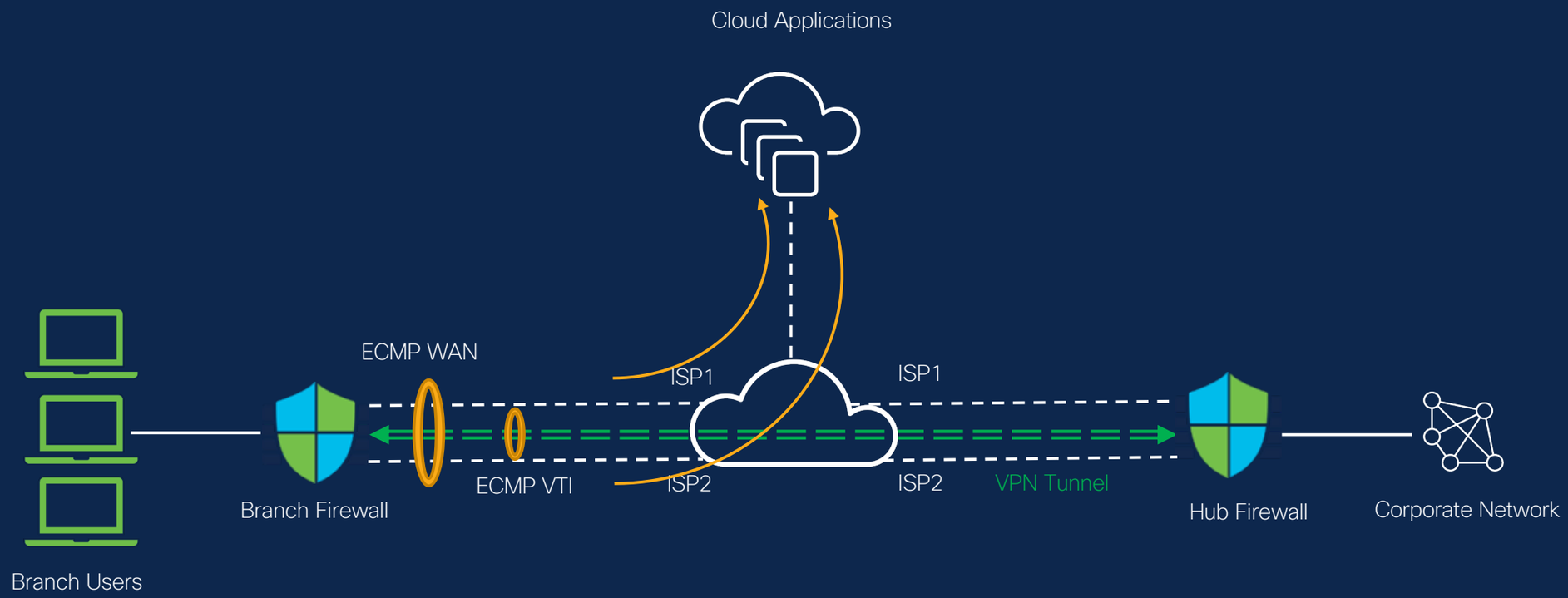
SD-WAN Management

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

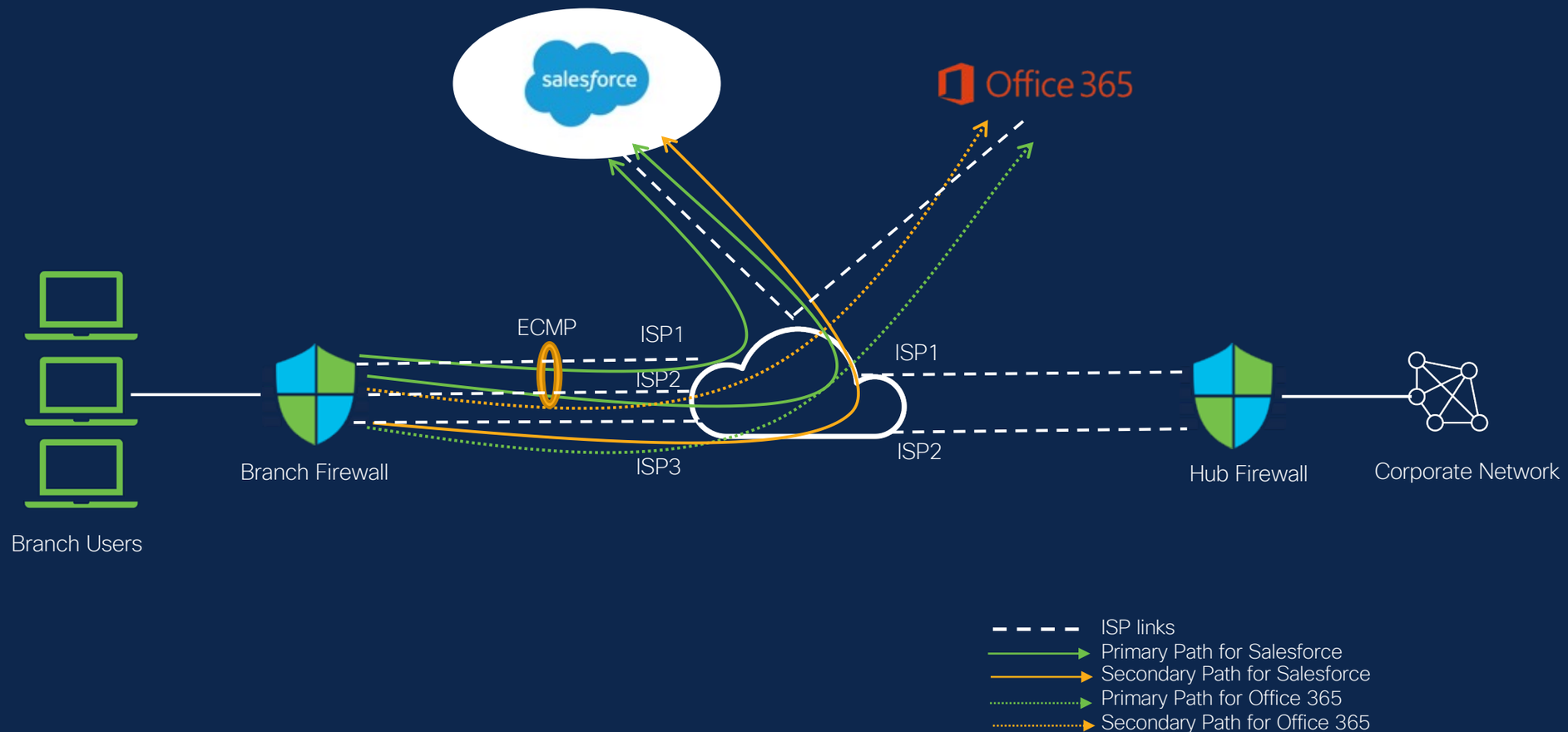
Simplifying Branch to Hub Communication using Dynamic Virtual Tunnel Interface (DVTI)



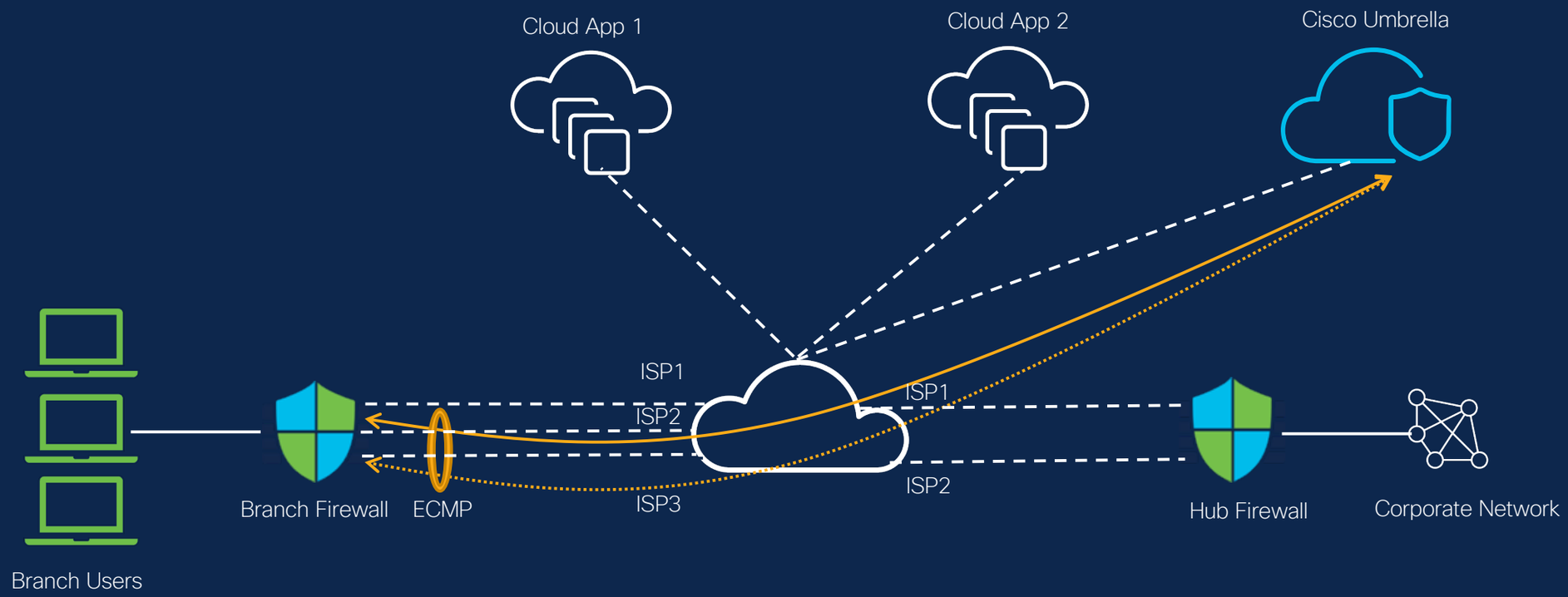
Direct Internet Access (DIA)



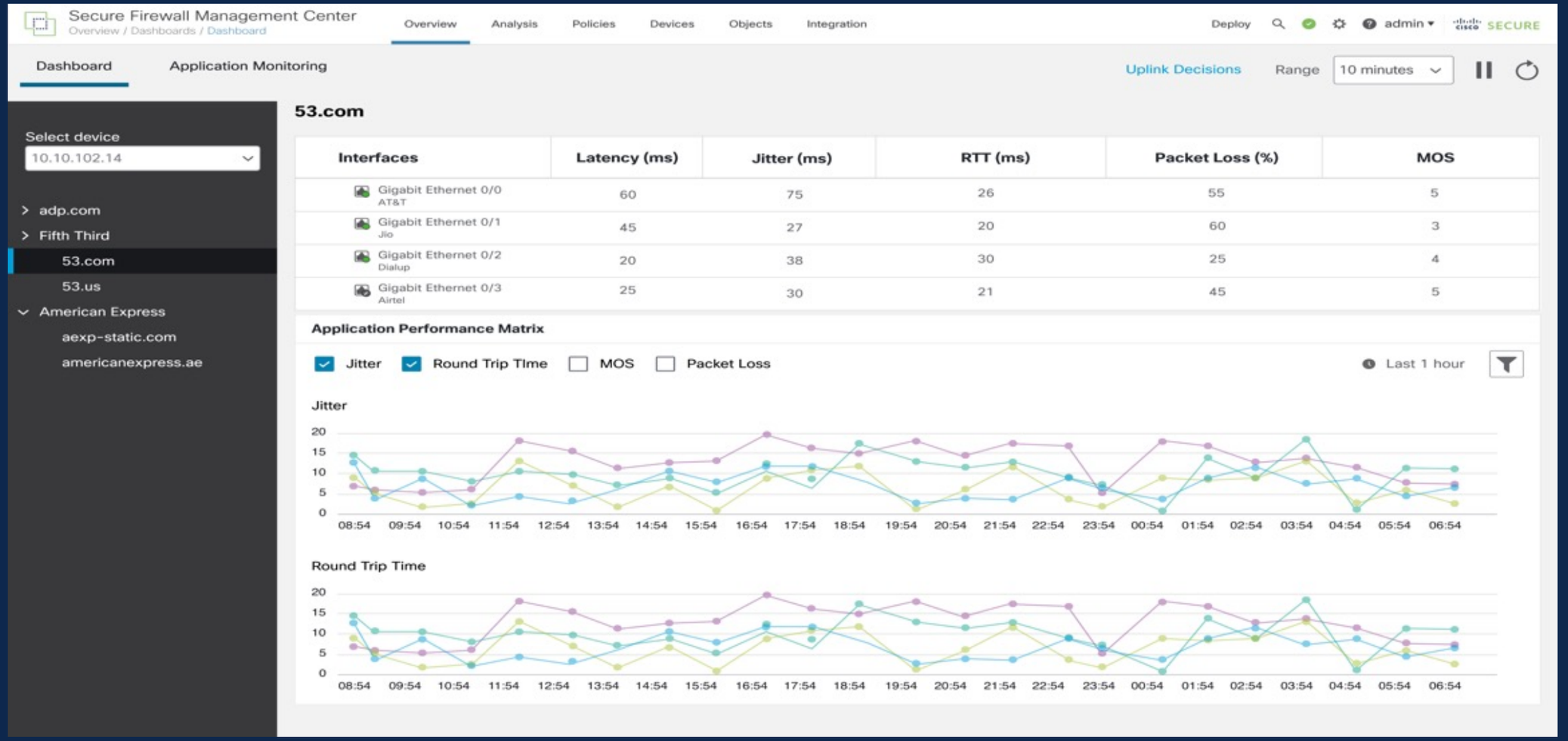
Direct Internet Access with Path Monitoring



Umbrella SASE Auto Tunnel



SD-WAN Summary Dashboard



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?

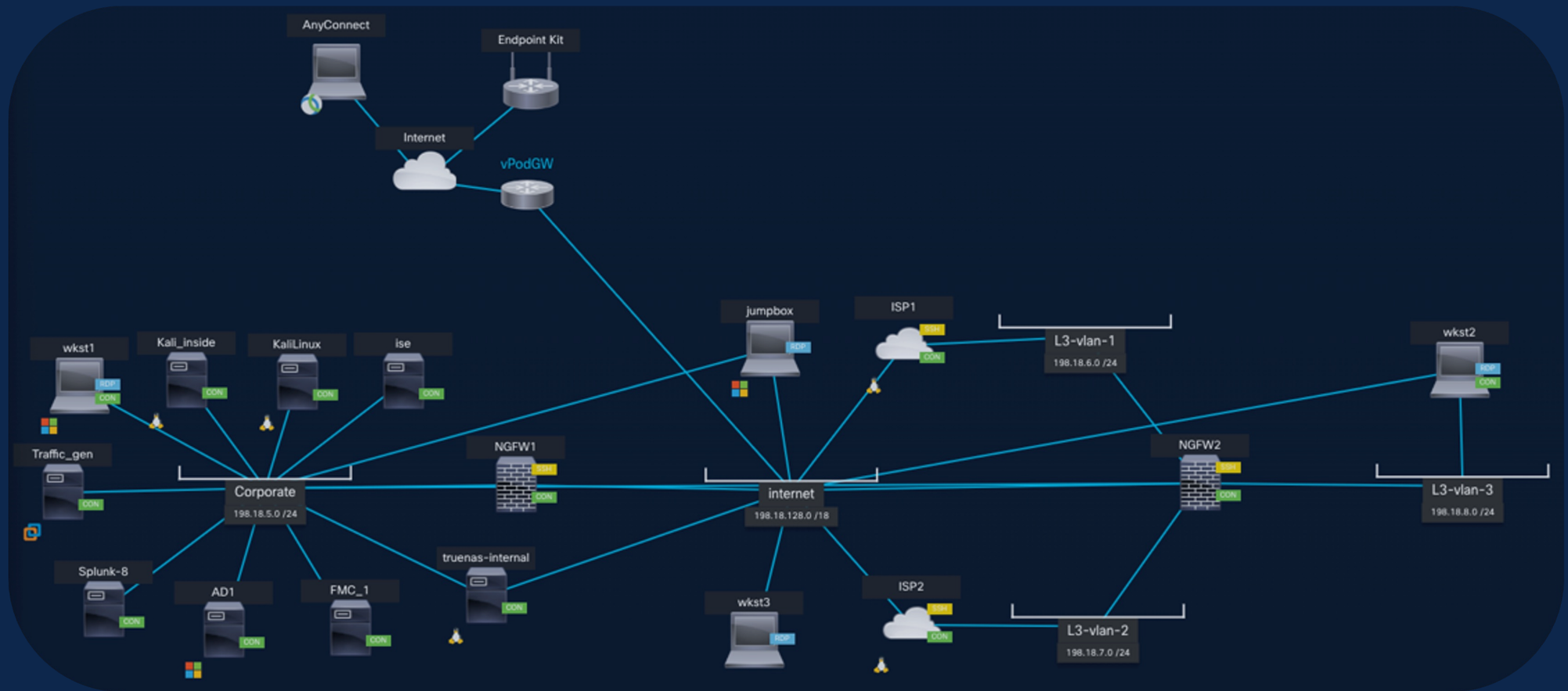
AttackIQ provides a platform for continuous security validation.

- 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.

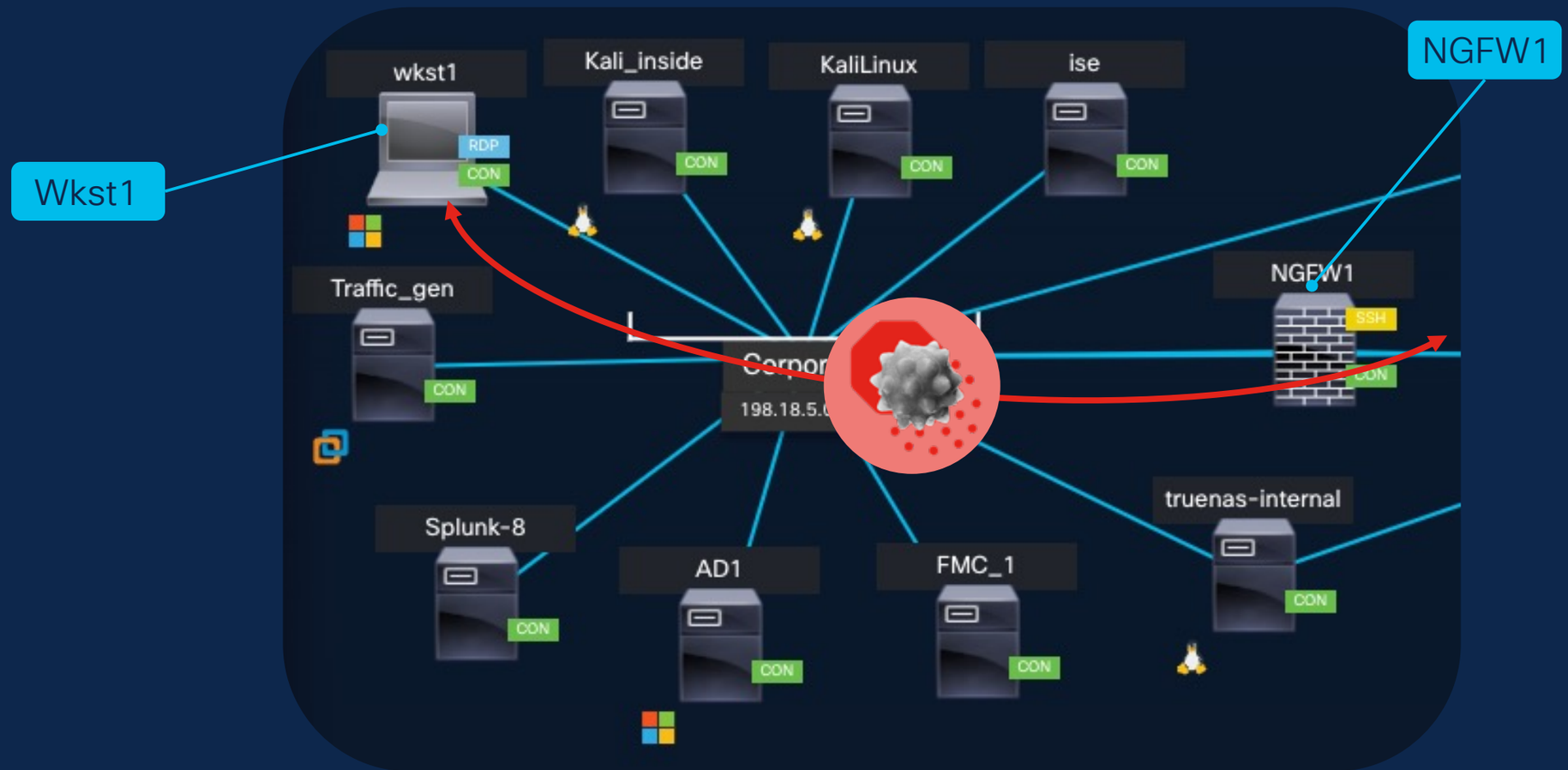
Product Offerings:

- 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

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

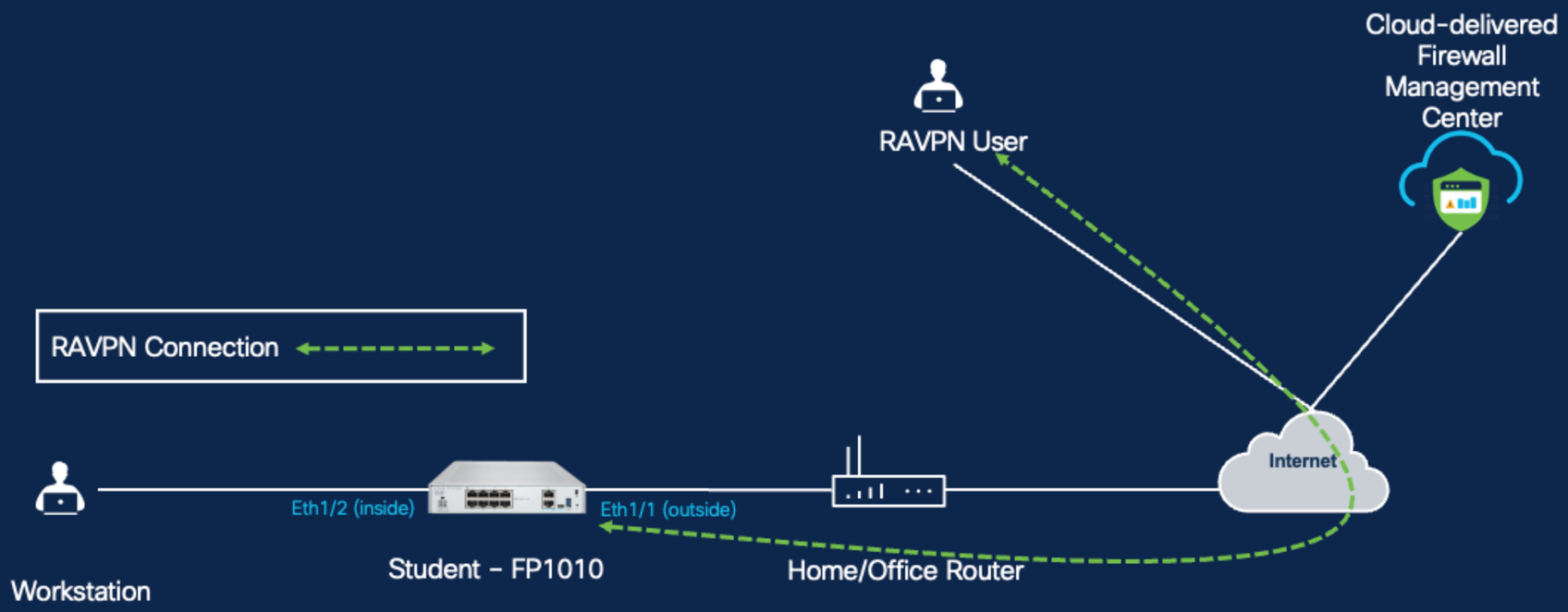
Remote Access Virtual Private Network (RAVPN)

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

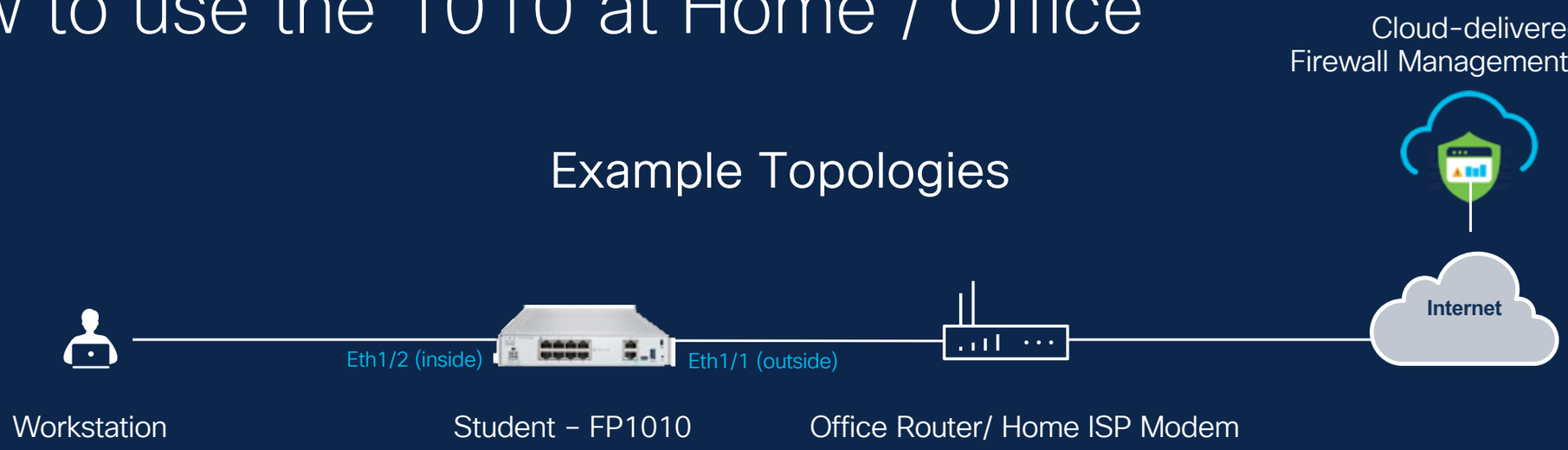
Secure

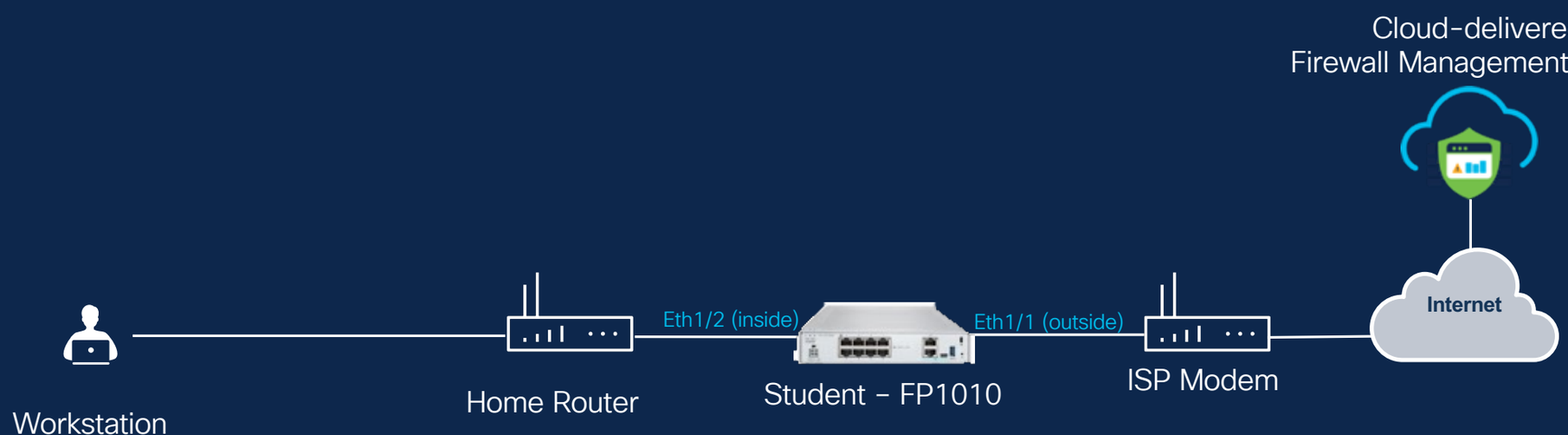
Demo

Engage

How to use the 1010 at Home / Office

Example Topologies

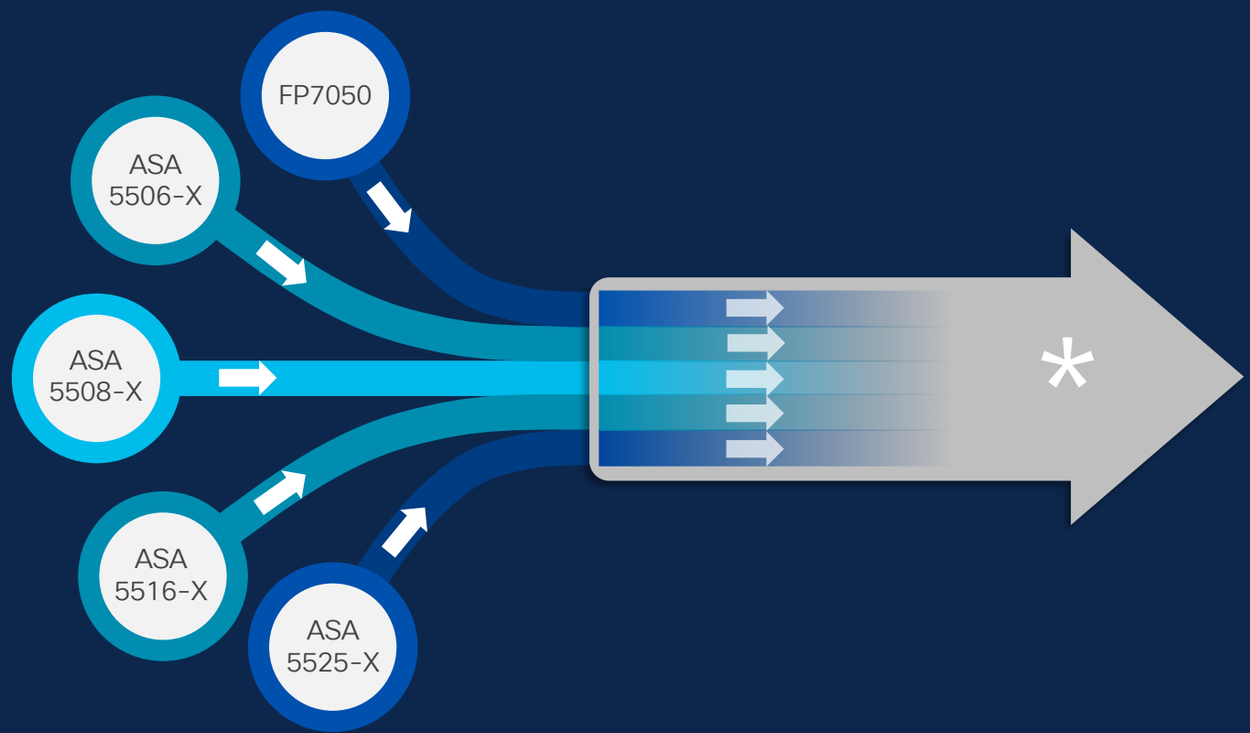




When It Comes to Refresh

Don’t assume. Use the Performance Estimator.

ngfwpe.cisco.com



Firepower 1010

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

Cisco Partner Confidential Information Partner Use Only

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	**Preview**	**Engage**	**Migrate**	**Close**
Employee/Partner completes initial submission and uploads supporting documentation	Help Desk engineer previews request & reaches out for questions and clarification	Help Desk engineer sets up WebEx sessions with the requestor and customer engineer (as required) to review & validate the configuration.	Engineer supports & provides guidance during the cutover within the 24/7 window; Pre-emptive TAC case for additional support.	Help Desk engineer closes case upon confirmation from customer & a satisfaction survey is sent.

cisco SECURE

Additional Resources

Lab licensing

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

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!

Replace with unique survey link with matching QR code for the specific city

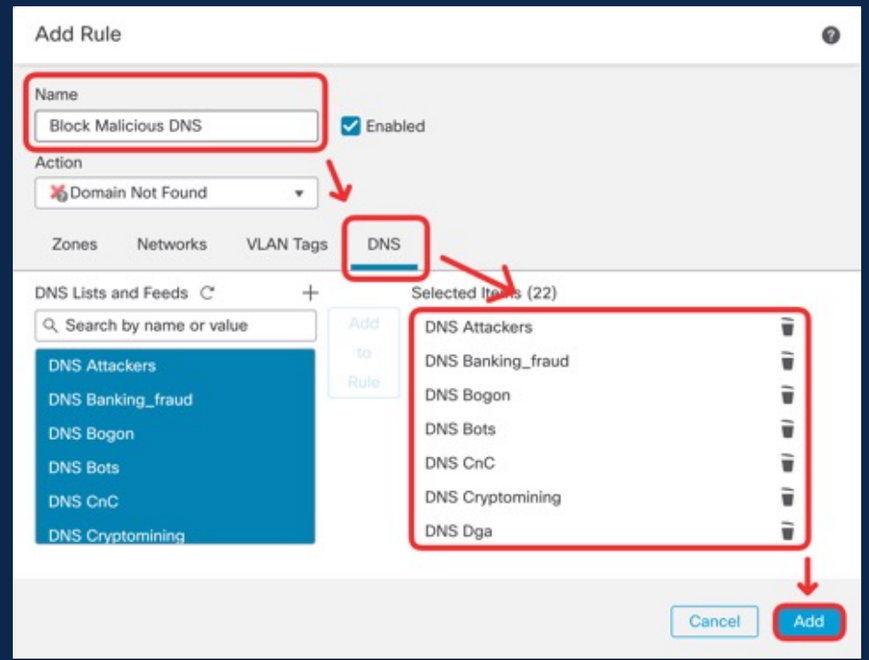
https://ciscochann e/form/SV_eWMmgFbnmnuz0Ls


CISCO

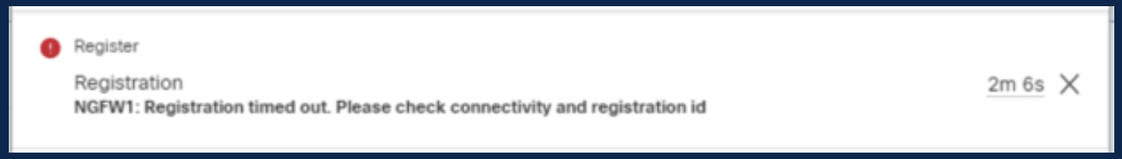
Firewall Ignite – Helpful Lab tips

- 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

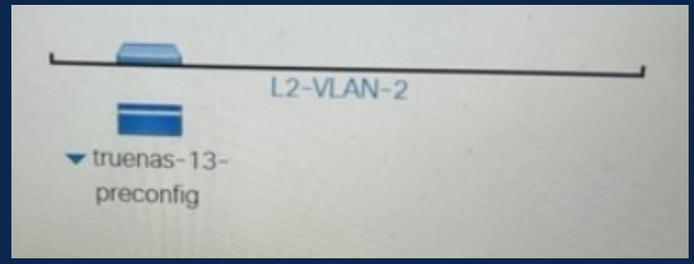
    Don't google AttackIQ Login



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, 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.