

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC



Intelligent Security for the Hybrid Cloud and Multi-Cloud

AI Powered and Cloud Delivered

Eric Kostlan
Technical Marketing Engineer
BRKSEC-2581

CISCO *Live!*

#CiscoLiveAPJC

Cisco Webex App

Questions?

Use Cisco Webex App to chat with the speaker after the session

How

- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until November 15, 2024.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-2581>



*“The public cloud is easy to learn.
Step 1. Forget everything you
know about networking.”*

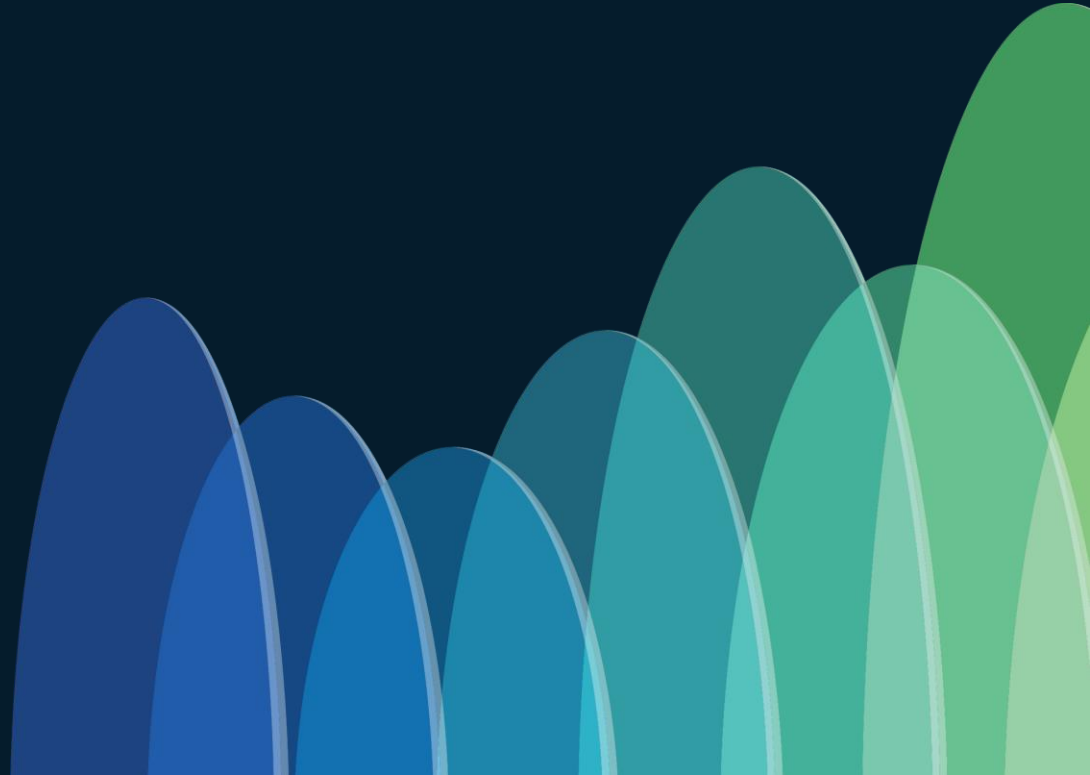
Technical Marketing Maxim

```
ubuntu@Azure200 :~ $ ping -c 1 10.200.101.6 > /dev/null
ubuntu@Azure200 :~ $ ping -c 1 10.200.101.8 > /dev/null
ubuntu@Azure200 :~ $ arp -an
? (10.200.101.1) at 12:34:56:78:9a:bc [ether] on eth0
? (10.200.101.6) at 12:34:56:78:9a:bc [ether] on eth0
? (10.200.101.8) at 12:34:56:78:9a:bc [ether] on eth0
ubuntu@Azure200 :~ $
```

Agenda

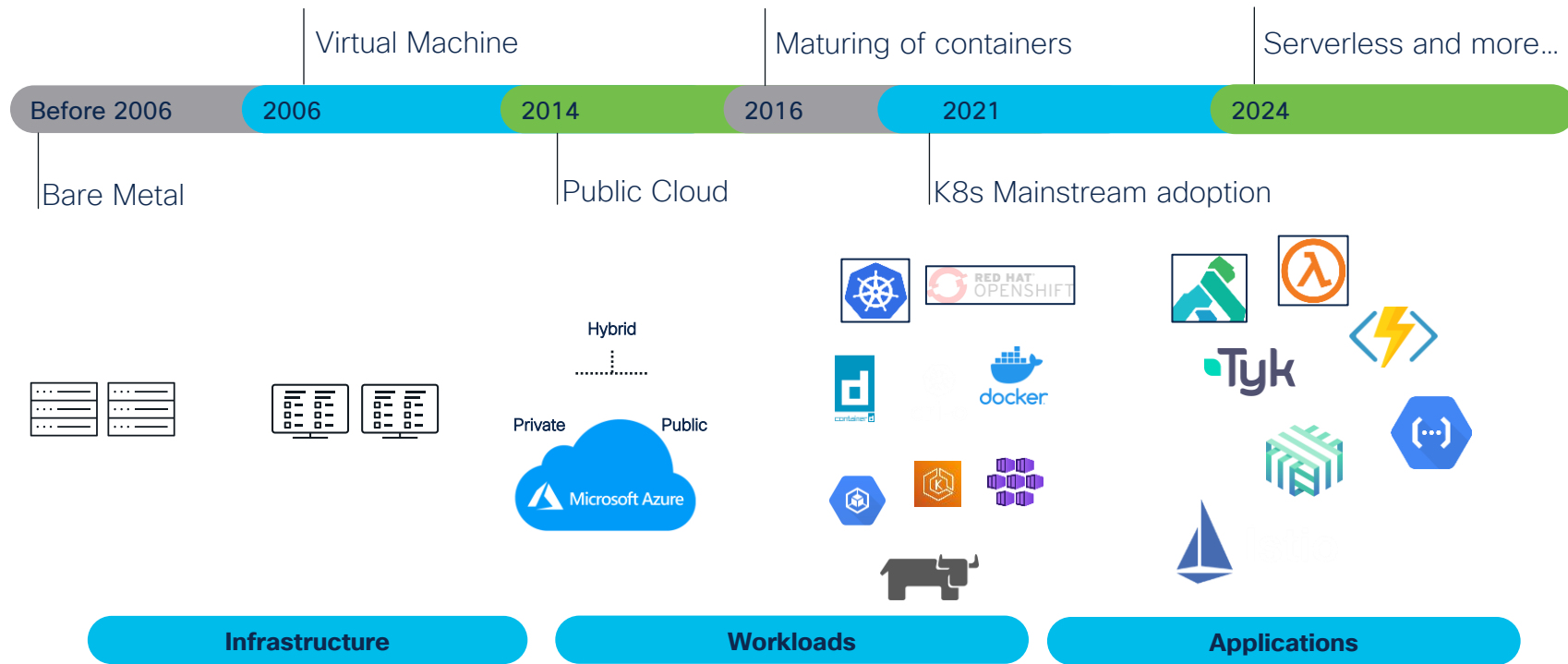
- Introduction
- Firewall Technologies
- Cisco Secure Firewall Portfolio
- Cisco Secure Firewall Innovation
- Cisco Multicloud Defense Overview
- Cisco Multicloud Defense Innovation
- Management
- Conclusion

Introduction



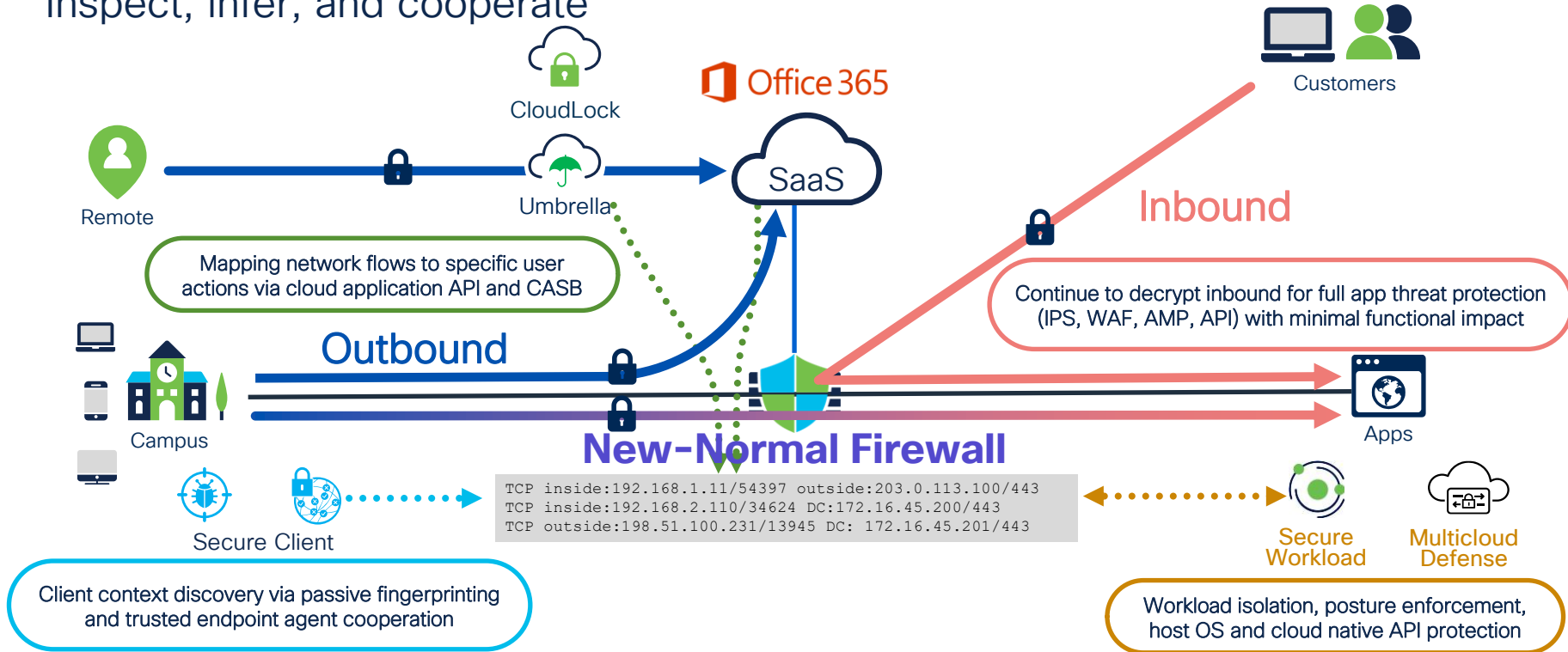
Technology Evolution

Rehost, refactor, revise, rebuild, and replace



Security Product Interoperation

Inspect, infer, and cooperate



Firewall Technologies



Cisco Firewall Portfolio

Physical appliances



Cisco Secure Firewall hardware appliances
running either ASA or FTD application

Private & Public cloud



ASAv and FTDv application
Running on all major public cloud and private cloud hypervisors

IoT and integrations



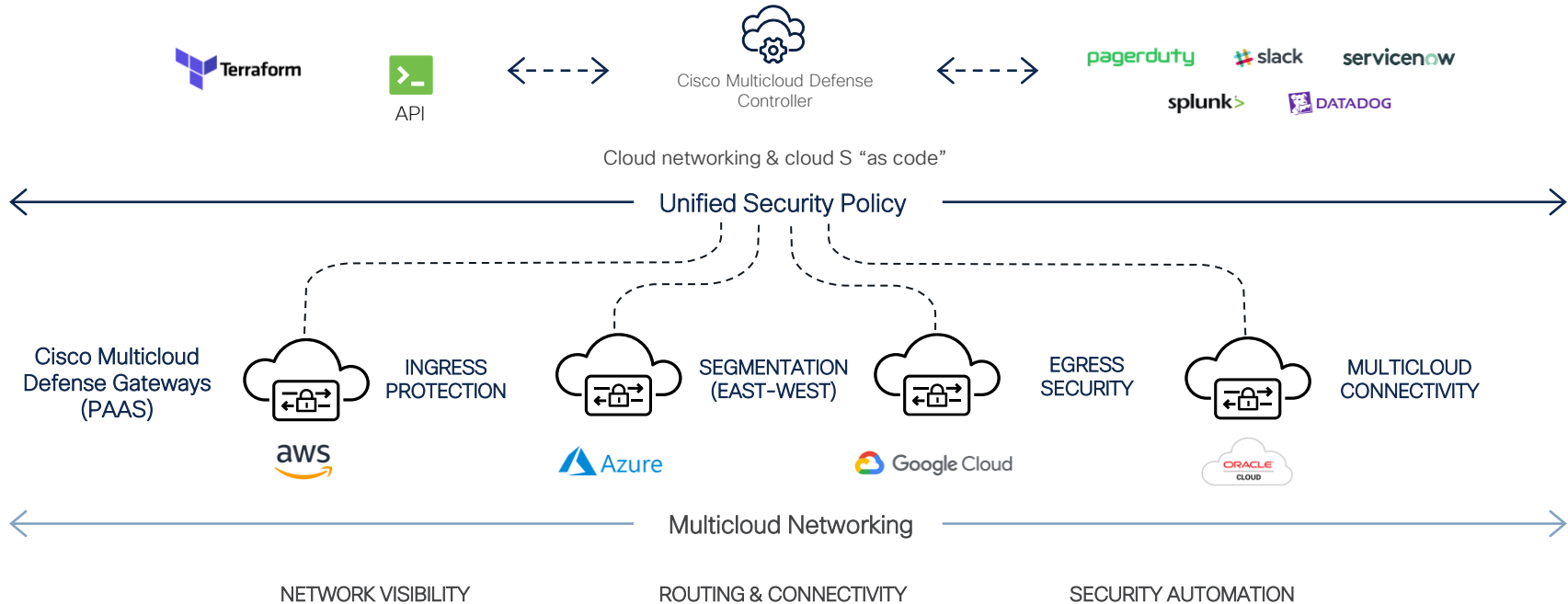
ISA 3000
Running either ASA or FTD application

Catalyst 9000
ASA running as a VM

Meraki MX
Snort 3 running in container

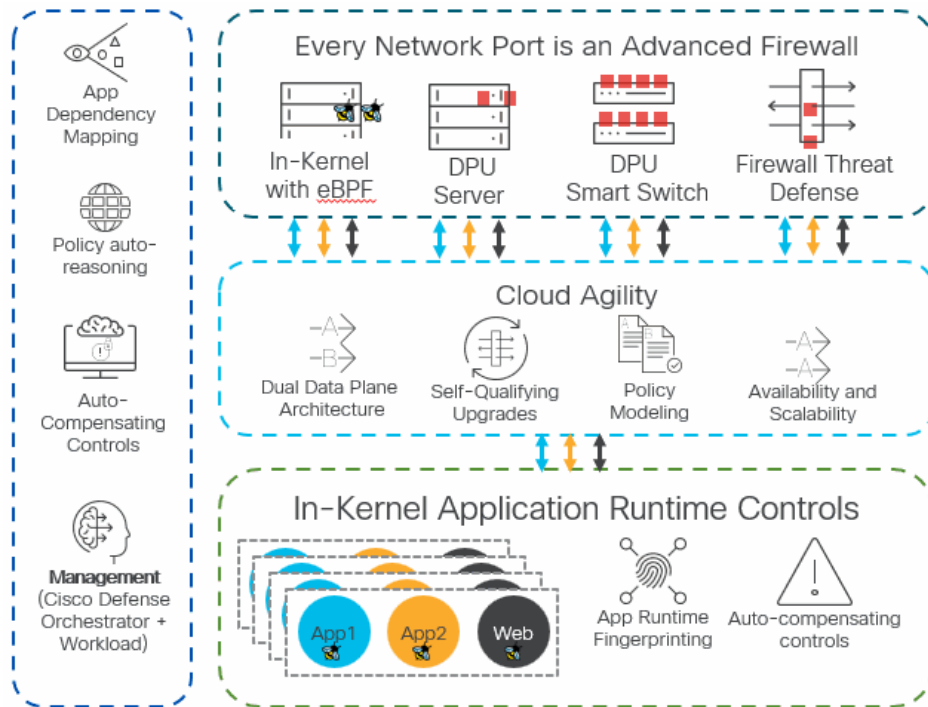
Cisco Multicloud Defense

Simplified Public Cloud Orchestration



Cisco Hypershield

Firewall function everywhere!



Hyper-distributed Architecture

Every physical, virtual, and cloud-native network interface becomes an advanced firewall. This is enabled by inline insertion with eBPF at host OS kernel level and by DPU-equipped servers and top-of-rack switches in the future.



Cloud Agility for Threat Protection

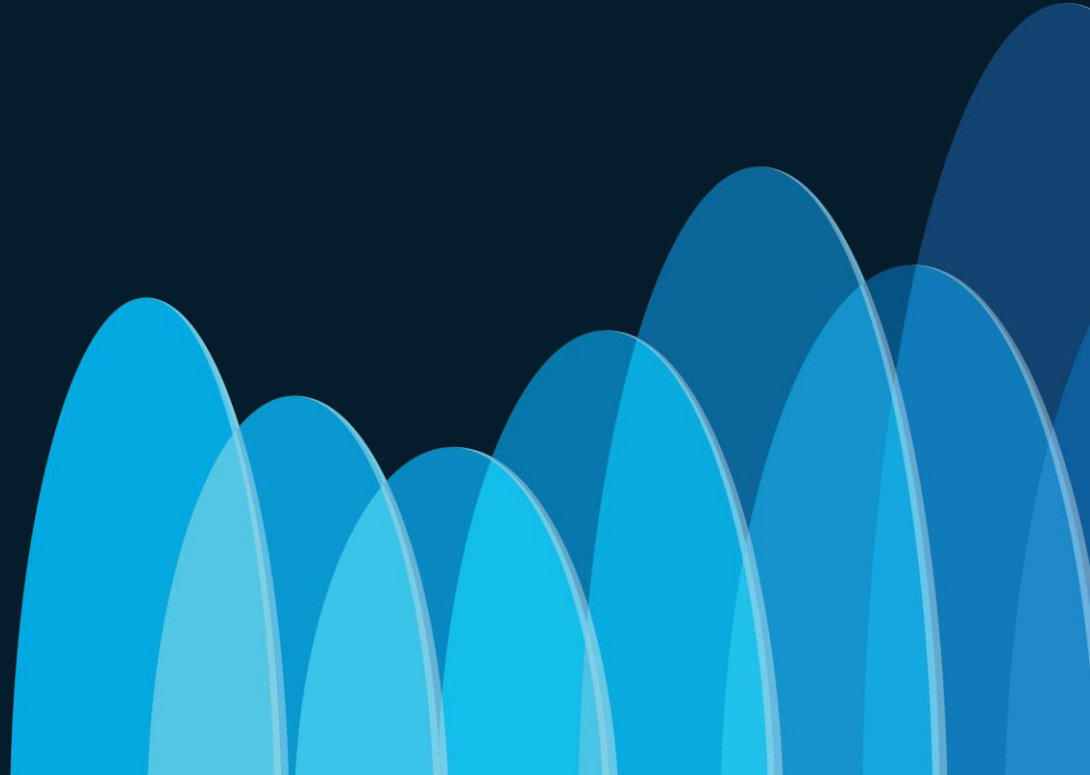
Dual data plane architecture enables self-qualifying upgrades, real-time policy modeling, and auto-scale-out use cases. It evolves from Workload agent visibility to advanced and flexible inline threat prevention.



AI-assisted Adaptive Runtime Policy

Expands on Workload visibility and policy modeling capabilities with runtime application fingerprinting and auto-compensating controls. Extends human language into security policy with generative AI capabilities.

Cisco Secure Firewall Portfolio



Physical Firewall Portfolio

650 Mbps
AVC+IPS

1.5-2.2 Gbps
AVC+IPS

2.6-6 Gbps
AVC+IPS

17-45 Gbps AVC+IPS
8 - 22.4 Gbps IPsec VPN
8 Node Cluster:
With 3140, up to
AVC+IPS(1024B) = 288 Gbps

Stand-alone device:
12-53 Gbps AVC
10-47 Gbps AVC+IPS
Sixteen node cluster:
Up to 680 Gbps AVC
Up to 675 Gbps AVC+IPS

Stand-alone device:
70-150 Gbps AVC
70-145 Gbps AVC+IPS
Sixteen node cluster:
Up to 1.7 Tbps AVC
Up to 1.6 Tbps AVC+IPS

One Module:
30-70 Gbps AVC
24-64 Gbps AVC+IPS
Sixteen node cluster:
AVC+IPS
SM40*16n = 704 Gbps
SM48*16n = 830 Gbps
SM56*16n = 950 Gbps



1010



SMB



1120/40/50



Branch Office



1210/1220



Mid Enterprise



3105/10/20/30/40



Large Enterprise



4112/15/25/45



Data Center



4215/25/45



Service Provider



9300 Series
SM-40
SM-48
SM-56

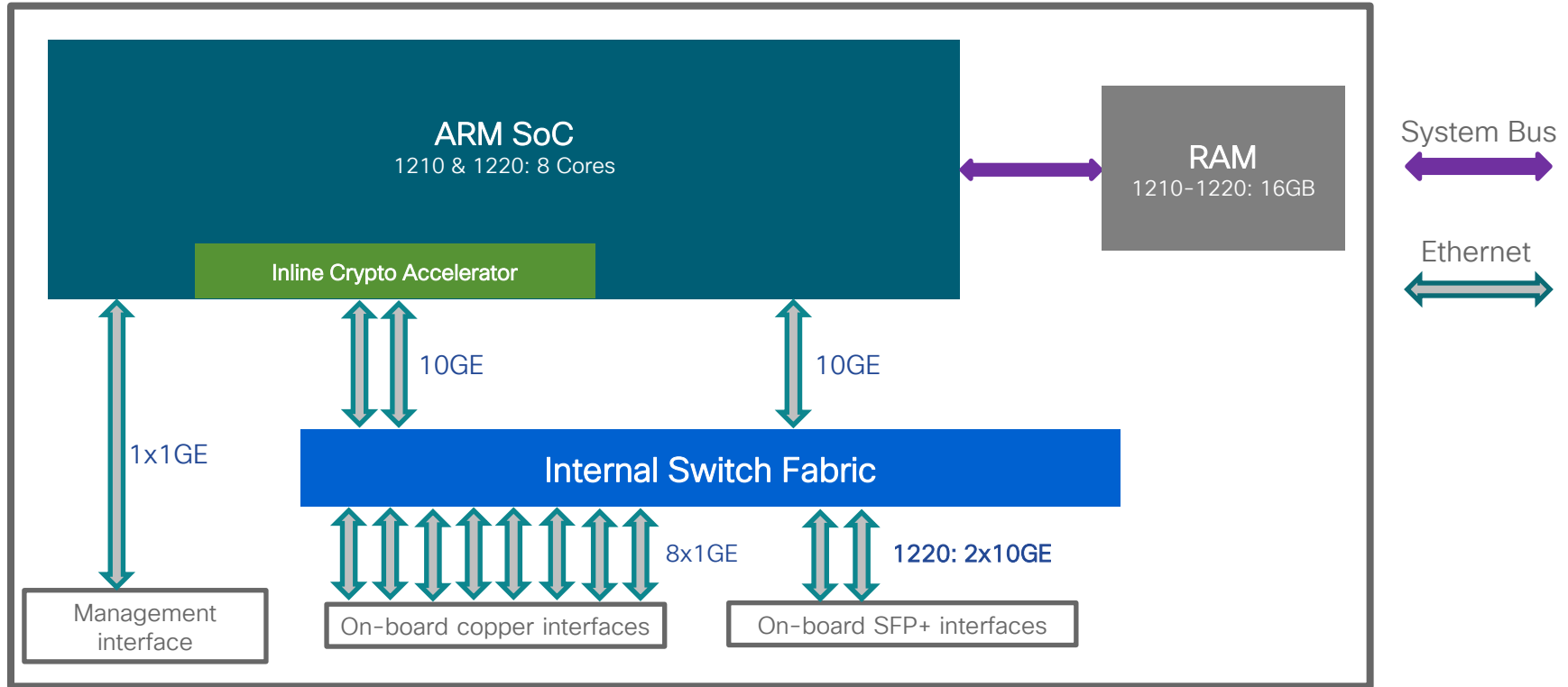
All appliances can run either ASA or FTD applications, FP9300 can run both on different SMs

Secure Firewall 1200C Series

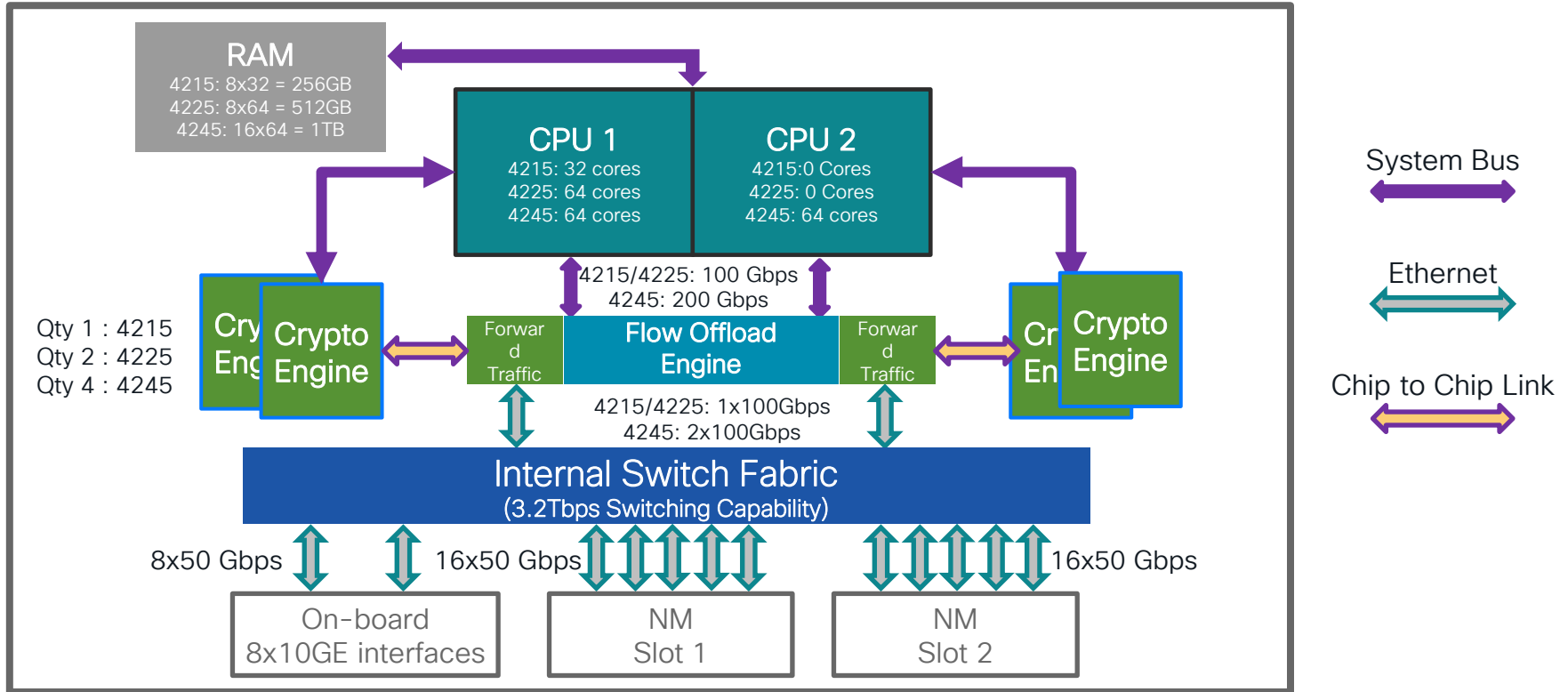
- 3 compact models – 1210CE, CP, 1220CX
 - 8 core SoC ARM design
 - 16GB of RAM
 - 480GB of NVMe storage
 - Fixed 8x1GE:
 - 1210CP – 4x1GE with UPoE+ support (120W total, max of 90W per port)
 - 1220CX – plus 2x 1/10G SFP+
- Multiple SoC-embedded accelerators
 - Encryption/decryption
 - Traffic processing
- Up to 2.6Gbps (450B) or up to 6Gbps (1024B) for NGFW traffic profiles (~10x over 1010, ~3x over 11xx)
- Up to 5Gbps for IPsec VPN, and up to 1.7Gbps for TLS 1.2/1.3



1200 Series Architecture



4200 Series Architecture



Cisco Secure Firewall Virtual



Virtual firewall performance-based licensing from 100Mbps up to 16Gbps

Cloud Leadership

Clustering & Auto Scaling

Integration with cloud native services & infrastructure

Accelerated Networking

Smart & Tiered Licensing

Dynamic Policy

Quickstarts, Infrastructure as Code and Automation

Gateway Load balancer integration

Snapshots

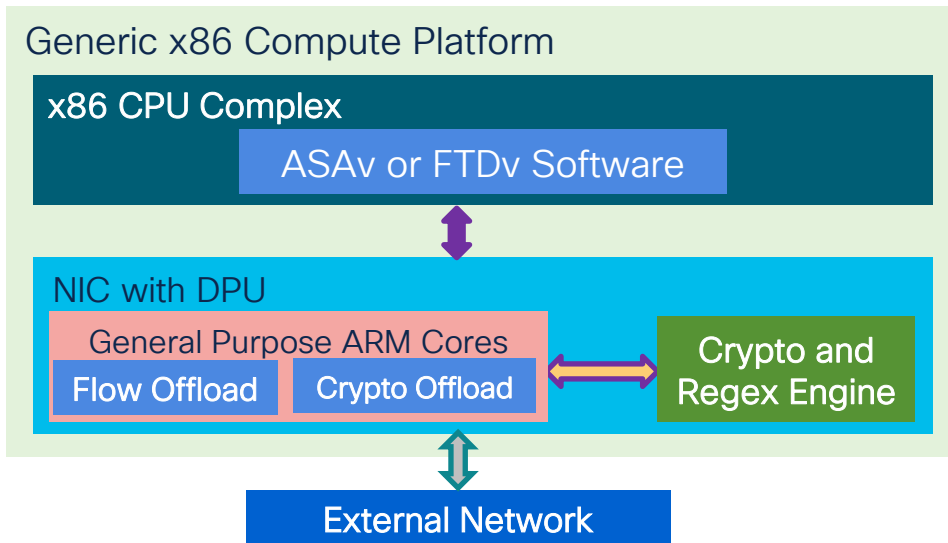
Virtual Firewall on Data Processing Unit (DPU)

Future

- Network Interface Controller (NIC) with a DPU in a server or switch
 - Inline hardware acceleration for broad packet processing functionality
 - Perfect opportunity to accelerate and scale firewall in hybrid data centers

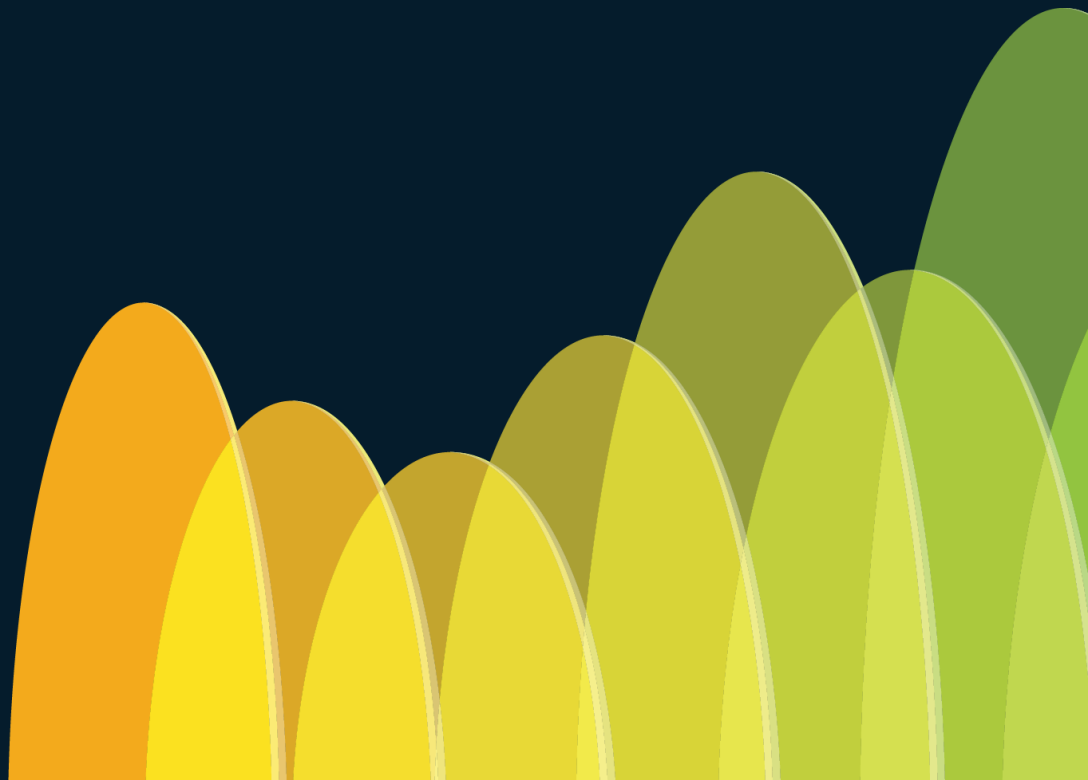
ASAv/FTDv software and Multicloud Defense is deployed on x86 CPU in generic private and public cloud environments.

If a DPU is present, additional ARM software components program inline acceleration of flow processing, IPsec and (D)TLS encryption, Regex matching, and other capabilities.

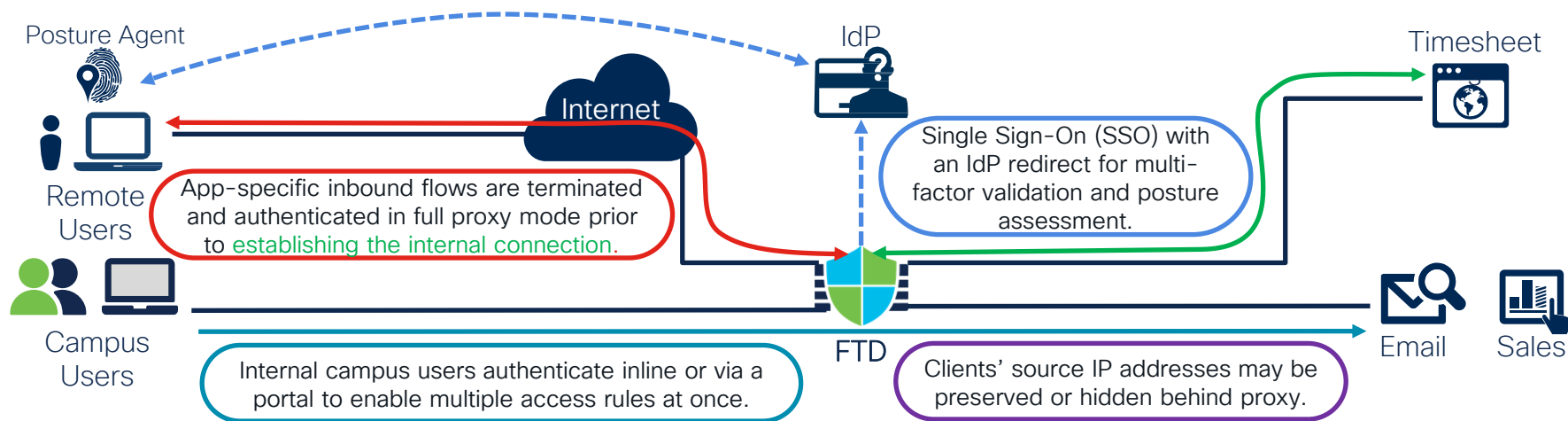


Cisco Secure Firewall Innovation

CISCO *Live!*



Clientless Zero Trust App Access (ZTAA)



Hybrid Zero Trust Network Access (ZTNA)

Future

2. **Secure Client** creates a control connection to **Secure Access**. It is used to authenticate and authorize application access and select the appropriate edge device based on policy or proximity.

Remote User



Secure Client



Secure Access

3. Per-application tunnels to public apps or private apps requiring advanced inspection features (e.g. DLP) go through **Secure Access** and **App Connectors**.

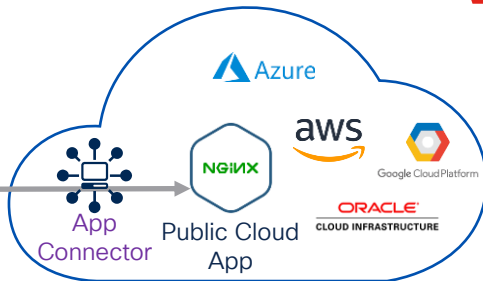
4. Eligible per-application tunnels to private apps are automatically directed to closest edge **Firewall Threat Defense** instance for full threat inspection.

1. **Secure Access** provisions private Firewall instances with appropriate private application access policies.

Firewall Threat Defense

Firewall Management Center

Private Cloud



Application-Aware Quality-Based Routing

Extend PBR using application base ACLs and path monitoring

The image displays two overlapping screenshots of the Cisco SD-WAN configuration interface.

Top Screenshot: Policy Based Routing

Policy Based Routing
Specify ingress interfaces, match criteria and egress interfaces to route traffic accordingly. Traffic can be routed across Egress interfaces accordingly.

Ingress Interfaces

Ingress Interfaces	Match criteria and forward action
inside	If traffic matches the Access List WebEx_Direct_Internet_Access

Match criteria and forward action

If traffic matches the Access List **WebEx_Direct_Internet_Access**, Send and load balance it through:

- #0 ISP1
- #0 ISP2
- If above link fails, Send through
- #1 ISP-Backup

Flexible egress interface selection policy, including ECMP over cleartext or VPN tunnels.

SaaS application aware first packet match.

Add Forwarding Actions

Match ACL:* Youtube +

Send To:* Egress Interfaces

Interface Ordering:* Minimal Jitter

Available Interfaces

Search by interface name

Interface

Inside	+
Outside	+

No interfaces selected

Jitter: Jitter is the term used to refer to variation in latency (rtt) of packet flow from endpoint to endpoint.

RTT: The Round-trip Time (RTT) is the duration, measured in milliseconds, from when a monitoring node sends an ICMP echo request to when it receives an ICMP reply from a remote node.

Packet-Loss: Packet loss describes packets of data not reaching their destination after being transmitted across a network. Packet loss is commonly caused by network congestion, hardware issues, software bugs, and several other factors.

MOS: Mean Opinion Score (MOS) is a way of quantifying the quantitative experience of a connection. Commonly used in streaming sessions where network effects can degrade communications quality. Audio and video communications are evaluated using this metric.

Simplified SD-WAN Setup Wizard

- Assisted creation of SD-WAN Hub-and-Spoke topology
 - Single or multiple interconnected hubs in Regions
 - Simplified Spoke addition without impacting existing devices
- Multiple configuration elements are automatically generated
 - Dynamic VTI interfaces and Security Zone assignment on Hub
 - Static VTI interfaces on Spokes with interface redundancy
 - Pre-shared tunnel keys and IKE/IPsec profiles
 - BGP overlay for Spoke-to-Hub and Hub-to-Hub connectivity

SnortML: Neural Exploit Engine

New detection engine available with Snort 3.1.82.0

- Traditional IPS rules are based on known and fixed patterns
 - Slight changes to payload patterns can evade static signatures
 - Undisclosed or new vulnerabilities take time to become signatures
- Neural Detector uses Machine Learning to expand IPS capabilities
 - Trained on all known embodiments for a given vulnerability type
 - Detects new patterns for the vulnerability without a static signature
 - TLS or QUIC decryption is still required
 - Enabled on Maximum Detection IPS policy initially
 - Can be enabled on custom IPS policies

Encrypted Visibility Engine (EVE)

Inspecting encrypted traffic without decryption

TLS ClientHello



TCP/TLS 192.168.2.110/34624->172.16.45.200/443

TCP/TLS 192.168.2.110/21013->203.0.113.154/443



Firewall

▼ Cipher Suites (18 suites)

```
Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
Cipher Suite: TLS_CHACHA20_POLY1305_SHA256 (0x1303)
Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9)
Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xccca8)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
Cipher Suite: TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x0033)
Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
```

Confidence: 99.94%
Process: [firefox.exe](#)
Version: 76.0.1
Category: [browser](#)
OS: [Windows 10 19041.329](#)
Destination FQDN: [cisco.com](#)

Generate unique fingerprints for client applications based on outer packet fields; use for policy matching and context enrichment with TLS and QUIC.

TLS ClientHello

▼ Cipher Suites (19 suites)

```
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
Cipher Suite: TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
```

Confidence: 100%
Process: [tor.exe](#)
Version: 9.0.2
Category: [anonymizer](#)
OS: [Windows 10 19041.329](#)
Destination FQDN: [nksdilkoup.me](#)

Access Control | Secure Firewall

Site to Site VPN | Secure Firewall

fmc.dcloud.local/ddd/#FirewallPolicyList

AUXISEFMC-2API ExplorerNGFW2(FDM)NGFW3(FDM)SPLUNKUnquarantineCertificates web ser...CSDACAWS-WEBAzure-webSNA

Firewall Management Center

Policies / Access Control / Access Control

OverviewAnalysisPoliciesDevicesObjectsIntegration

Deploy

admin

SECURE

Object Management | Intrusion | Network Analysis Policy | DNS | Import/Export

New Policy

Access Control Policy	Status	Last Modified	Lock Status	
NGFW2	Targeting 1 devices Up-to-date on all targeted devices	2024-02-21 10:14:58 Modified by "Firepower System"		
NGFW3	Targeting 1 devices Up-to-date on all targeted devices	2024-02-21 10:14:58 Modified by "Firepower System"		
Parent Policy common settings	Targeting 0 devices	2024-05-21 07:26:43 Modified by "admin"		
Branch Access Control	Targeting 1 devices Up-to-date on all targeted devices	2024-05-21 07:26:43 Modified by "admin"		
NGFW1	Targeting 1 devices Up-to-date on all targeted devices	2024-05-22 13:15:25 Modified by "admin"		
Traffic Generator	Targeting 1 devices Up-to-date on all targeted devices	2024-05-21 07:26:43 Modified by "admin"		

CISCO Live!

#CiscoLiveAPJC BRKSEC-2581

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

9:36 AM 5/24/2024

QUIC Decryption and Inspection

- QUIC (HTTP/3) uses UDP with modified TLS 1.3 for encryption



- Most firewall vendors require downgrade to HTTP/2 for inspection
- Some browsers ignore Enterprise CA in local trust store for decryption
- Encrypted Visibility Engine supported QUIC apps since FTD 7.3
- Full QUIC decryption and inspection is targeted for FTD 7.6

Intelligent Selective Traffic Decryption

- Effective threat protection requires some traffic to be decrypted
 - Decrypting everything will degrade performance even with fast hardware
 - Difficult to predict what to decrypt with static policies
- Goal: classify 90% traffic as benign, inspect remaining 10%



AI-powered, Future-ready Firewall Platform

- Assist, Augment and Automate with Cisco Security AI Assistant.
- Unify and simplify management with Secure Cloud Control.
- Utilize best of breed hardware including the 1200 series.
- Cisco Secure Firewall provides ground to cloud secure connectivity.
 - ZTAA
 - SD-WAN capabilities such as PBR and SD-WAN overlay configuration wizard and dashboard.
- Cisco Secure Firewall provides unmatched visibility and control.
 - Protection from zero-day attacks with SnortML
 - Encrypted traffic visibility and control without decrypting with EVE

Cisco Multicloud Defense Overview



Cisco Multicloud Defense is the Multicloud Network Security Platform



Consolidated security for cloud networks to consistently connect and protect workloads and data



Inbound

Stop Inbound
Threats for Web &
Non-Web Apps



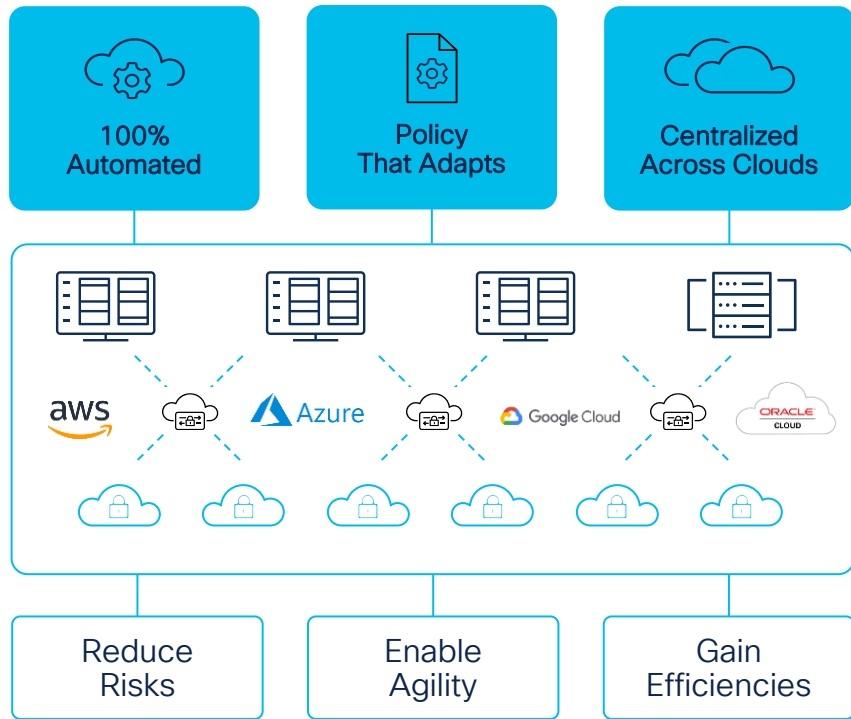
Outbound

Block Command
& Control, Botnets,
Data Exfiltration



Lateral

Mitigate
Attacker
Movement



Accelerate Cloud Infrastructure Conversion and Implementation

- Multicloud Defense provides rapid conversion and implementation of cloud infrastructure
- Cisco Multicloud Defense can generate Terraform files for components Multicloud Defense creates in your environment.
- This Terraform can be exported and used in your orchestration tools

The screenshot displays the Cisco Multicloud Defense web interface. The left sidebar contains navigation menus for Security Policies, Profiles, Threat Research, Networking, and Cloud Accounts. The main content area is titled 'Service VPCs/VNets: 4' and includes a search bar and a table of service VPCs/VNets. The table has columns for Name, ID, and Account. The 'Details' panel on the right shows instructions for exporting Terraform files and provides a code block with Terraform configuration for a VPC and its associated spokes.

Name	ID	Account
pod1-vnet	584	cisco-multicloud-def...
pod1-vpc-aws	583	cisco-multicloud-def...
pod1-vpc-gcp	585	cisco-multicloud-def...
pod2-vnet	590	cisco-multicloud-def...

Details

In order to export and use the selected service vpc/vnet object **pod1-vpc-aws**, you need to complete the following steps:

Step 1: Download the Terraform File. [Download](#)

or

Copy the resource block below and insert it into your Terraform script.

```
resource "ciscocloud_service_vpc" "pod1-vpc-aws" {
  name = "pod1-vpc-aws"
  csp_account_name = "cisco-multicloud-defense-aws01"
  region = "us-east-1"
  cidr = "192.168.1.0/24"
  availability_zones = ["us-east-1a"]
  transit_gateway_id = "tgw-0246827346cf2194"
  vpc_nat_gateway = false
}

resource "ciscocloud_spoke_vpc" "pod1-vpc-aws-spoke0" {
  service_vpc_id = ciscocloud_service_vpc.pod1-vpc-aws.id
  spoke_vpc_id = "vpc-67677d2a78339f999"
}

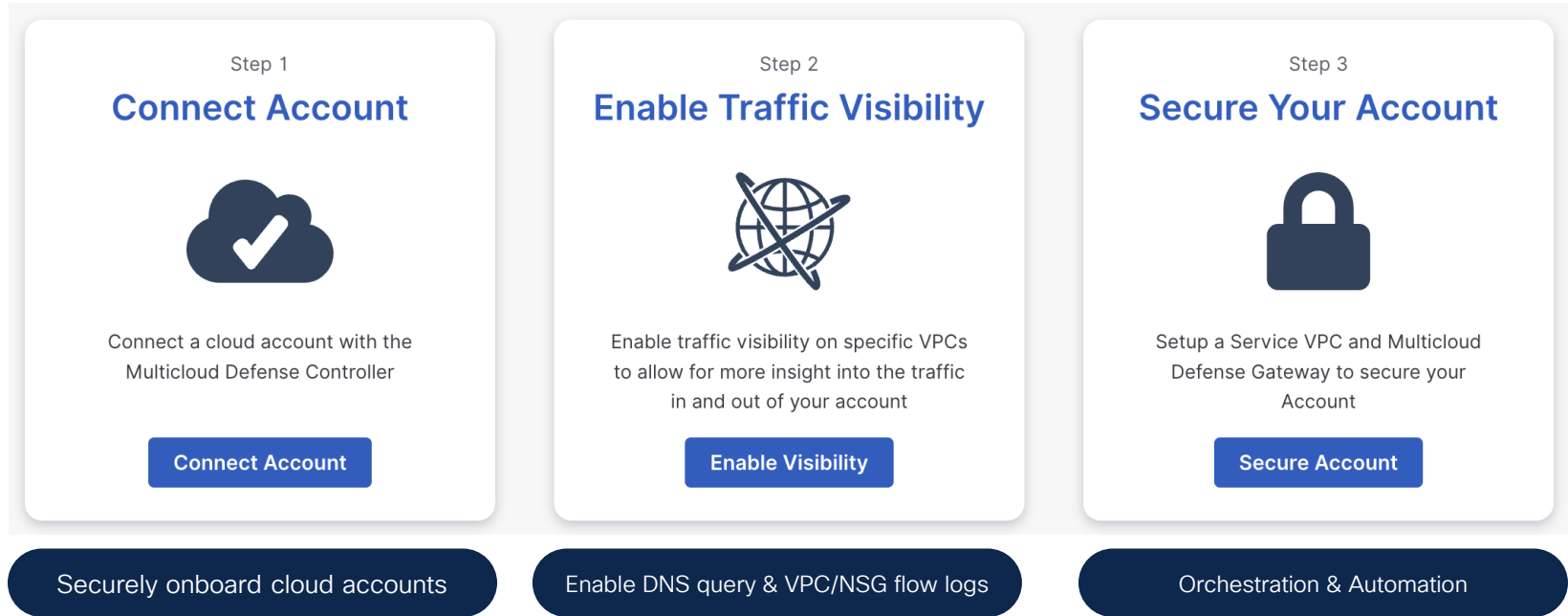
resource "ciscocloud_spoke_vpc" "pod1-vpc-aws-spoke1" {
  service_vpc_id = ciscocloud_service_vpc.pod1-vpc-aws.id
  spoke_vpc_id = "vpc-8ba9a1d4849efa1331"
}
```

[COPY CODE](#)

Step 2: Execute Command:

Multicloud Defense Wizards

Setup Wizards echo the workflow



Orchestrate, manage, control, and secure cloud infrastructure using Multicloud Defense

Simplified Account Onboarding and Inventory

- Multicloud environments are onboarded:
 - AWS: per account
 - Azure: per subscription
 - GCP: per project
 - OCI: per account
- All cloud assets are immediately discovered
 - Consolidated inventory is presented dashboards in Multicloud Defense console
 - You can drill down on assets to see details such as security rules and routes
- Changes in cloud assets are immediately pushed to Multicloud Defense and visible in the Multicloud Defense console

Home - Microsoft Azure

Cisco Defense Orchestrator

defenseorchestrator.com

Incognito

Defense Orchestrator

Type 'Ctrl' + '/' to search

cisco-multicloud_defense_lab01
erkostla@cisco.com

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

Inventory & Objects

Connectivity States

Reconnect (2)

4 total

2 Issues

2 Online

Configuration States

3 Synced

1 Not Synced

0 Conflict Detected

Object Issues

Object status	Number of objects
All Objects	95
Inconsistent	0
Duplicate	6
Unused	8

Site-to-Site VPN

View All Tunnels

VPN Tunnel Status

Issues

Pending Deploy

74°F Windy

CISCO Life!

Search

AIRBUS

Backdoor

1 item

1 item selected, 49.1 KB

#CiscoLiveAPJC

BRKSEC-2581

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

37

Traffic Visibility

Use cloud native traffic logging without installing anything

- Different public clouds use different mechanisms for traffic visibility
 - AWS uses **flow logs** and **DNS query logs**
 - AWS uses **NSG logs**
 - GCP uses **VPC logs**
 - OCI uses **VCN flow logs**
- Multicloud Defense orchestrates the configuration of these traffic logging mechanism – no need to have knowledge of configuration details
- Multicloud Defense presents a unified view of traffic
- Multicloud Defense can identify malicious traffic
 - Uses IP and domain reputation to identify threats using traffic metadata

Home - Microsoft Azure

Cisco Defense Orchestrator

defenseorchestrator.com/multicloud-defense

Incognito

Defense Orchestrator

Multicloud Defense

Type 'Ctrl' + '/' to search

cisco-multicloud_defense_lab01
erkostla@cisco.com

Hide Menu

Dashboard

Multicloud Defense

Inventory

Configuration

Policies

Objects

VPN

Events & Monitoring

Analytics

Change Log

Jobs

Tools & Services

Settings

Multicloud Defense Controller

+ Add Accounts

Accounts and Assets

Cloud Accounts

1 AWS

aws

2 Azure

A

1 GCP

0 Oracle

4

Total Accounts

View Accounts

Account Resources

47

VPCS/ VNets

211

Security Groups

51

Route Tables

65

Subnets

44

Instances

7

Load Balancers

921

Tags

7

Applications

Enable Traffic Visibility

Enable traffic visibility on specific VPCs to allow for more insight into traffic in and out of your account.

Enable visibility

Multicloud Defense Shared Objects

Object Type	Count
networks	4

66°F Clear

CISCO Life!

Search

#CiscoLiveAPoC

RKSEC-2081

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

9:21 PM 8/23/2024

Securing an Account

Multicloud Defense Gateways



Ingress Gateway

- ✓ Reverse Proxy
- ✓ TLS decrypt
- ✓ WAF – L7 DoS
- ✓ IDS / IPS
- ✓ Antivirus
- ✓ Geo IP
- ✓ Malicious IP

Egress Gateway

Egress

- ✓ URL filtering
- ✓ Forward proxy
- ✓ TLS decrypt
- ✓ FQDN filtering*
- ✓ FQDN-based firewall policy
- ✓ DLP
- ✓ IDS / IPS
- ✓ Antivirus
- ✓ **Fully orchestrated IPsec VPN**
(site-to-cloud & cloud-to-cloud)

East/West

- ✓ FQDN filtering
- ✓ IPS / IDS
- ✓ Antivirus
- ✓ Segmentation
- ✓ FQDN-based firewall policy
- ✓ TLS decrypt

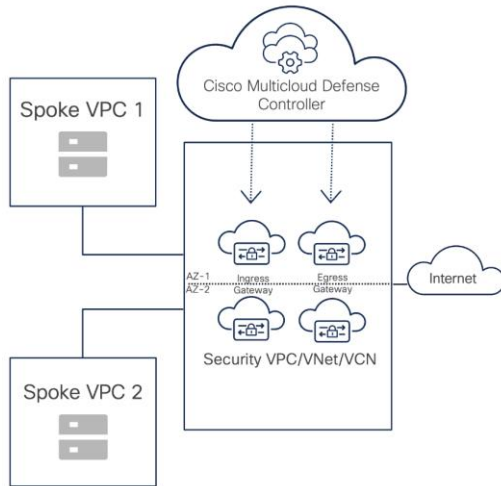
* No TLS decryption is needed
Forwarding mode is available on Multicloud
Defense Gateway

- Single Pass Architecture - Instance Size (2, 4 and 8 vCPU) - Available in AWS, Azure, GCP and OCI

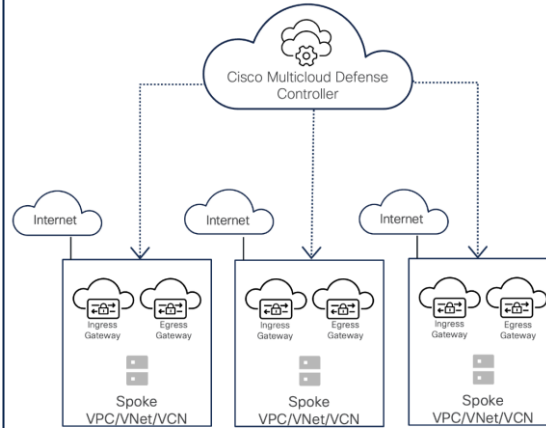
Securing an Account

Security models

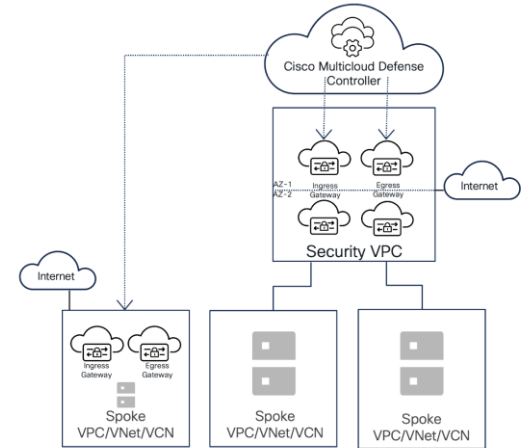
Centralized Security Model



Distributed Security Model

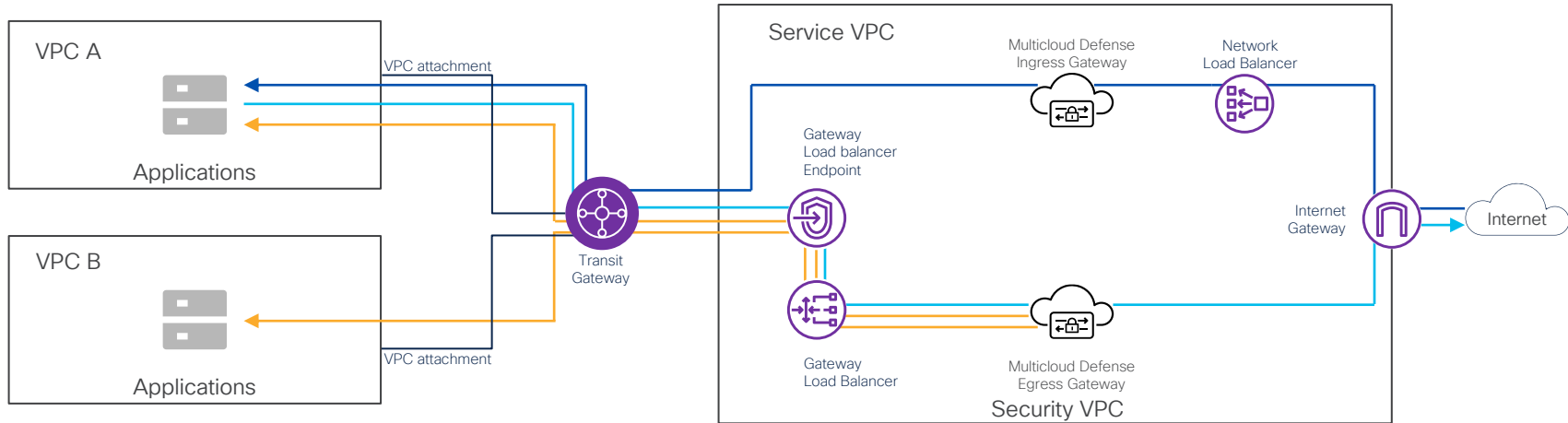


Combined Security Model



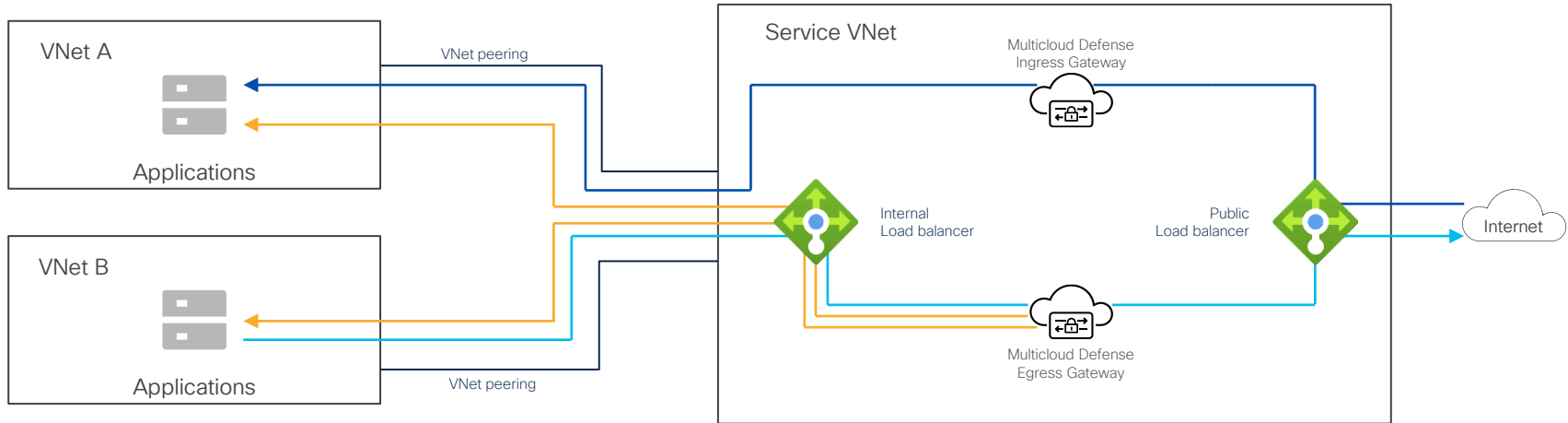
Securing an Account

AWS – centralized security model – simplified



Securing an Account

Azure – centralized security model – simplified (GCP and OCI are similar)



Home - Microsoft Azure

Cisco Defense Orchestrator

Cisco Multicloud Defense

prod1.mcd.us.cdo.cisco.com/dashboard?timeFrame=1hr

Incognito

Multicloud Defense

Admin: erkostla@cisc...

CDO: cisco-multicloud_defense_lab01

Dashboard

Discover

Investigate

Manage

Report

Administration

Favorites

Pinned navigation items will go here

Setup

Dashboard

Open Panel

Cloud Accounts

Discover

4

Cloud Accounts

1

aws

2

A

1

0

Add Account

View More

Account Resources

Discover

47

VPCs/VNets

65

Subnets

211

Security Groups

7

Load Balancers

44

Instances

921

Tags

51

Route Tables

7

Applications

View More

Top Ports With Mal. Traffic

Discover

443-TCP

3389-TCP

808-TCP

8181-TCP

8090-TCP

8088-TCP

44818-UDP

50358-TCP

8334-TCP

3283-UDP

0

20

40

60

80

View More

Top CSP Services

Discover

AWS Ssm

CCP L...

DNS Traffic

Discover

Computer ...

Business ...

Uncategori...

Entertainme...

Content...

Security Considerations

Deploy

7/7

Applications Not Protected

36/47

VPCs/VNets Not Protected

0/4

Service VPC/VNets without Gateways

66°F Clear

CISCO Live!

Search

#CiscoLiveApriC

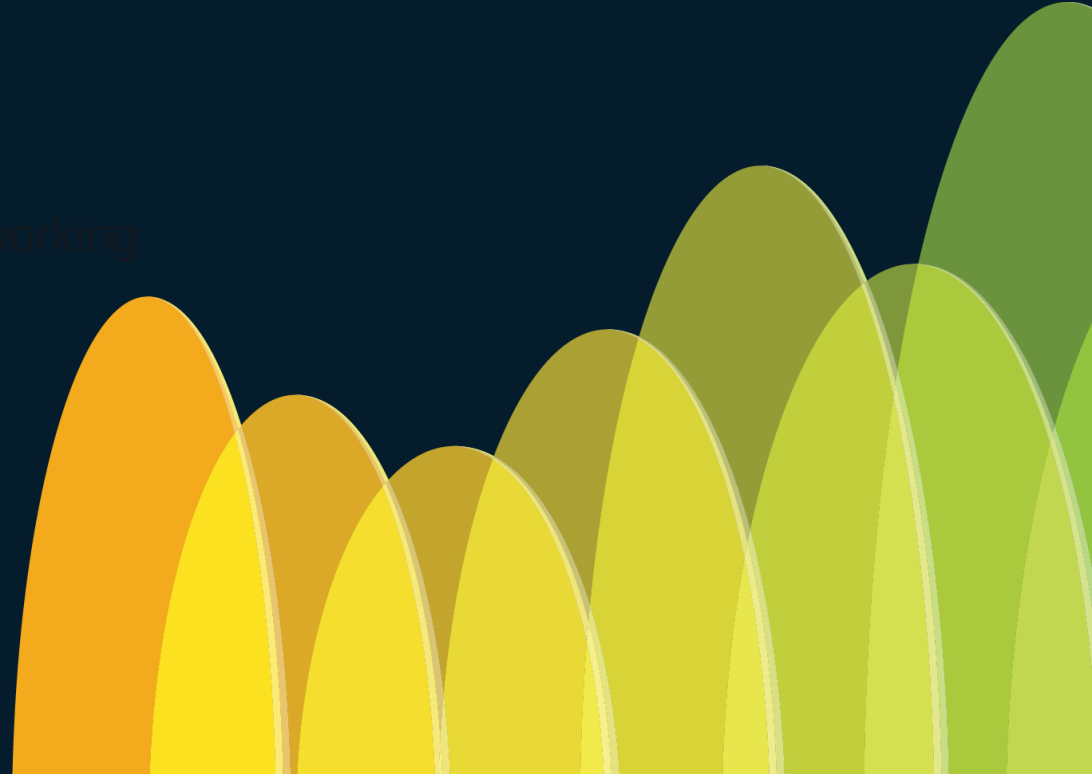
SRKSEC-2681

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

40:51 PM 6/25/2024

Cisco Multicloud Defense Multicloud Networking Innovation

CISCO *Live!*



Multicloud Networking

Orchestration of IPsec tunnels for intercloud communication

Site-to-cloud networking

Cloud-to-cloud networking

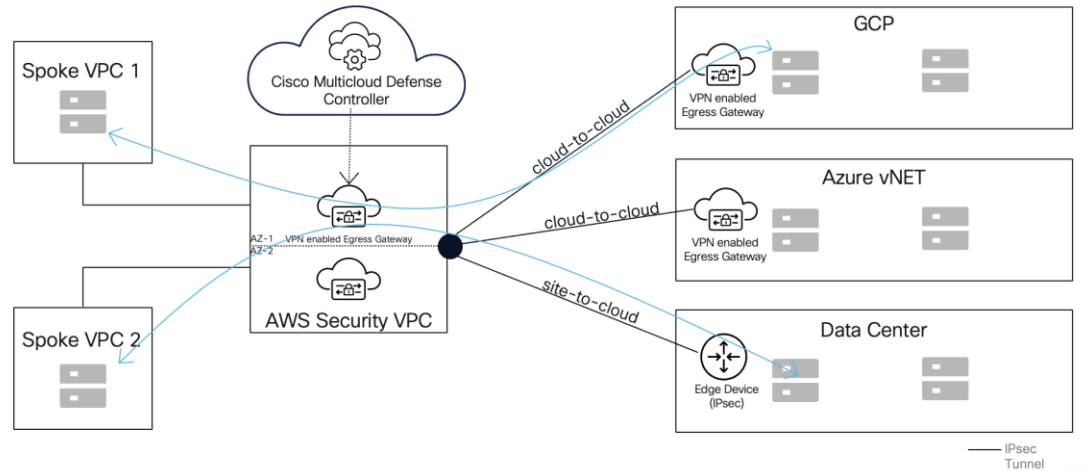
Built-in advanced security

Distributed and centralized

Route-based VPN + BGP

Automation

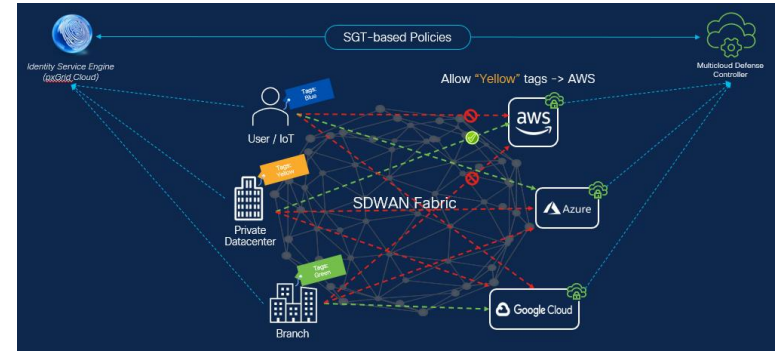
Simplified operations



Multicloud Networking

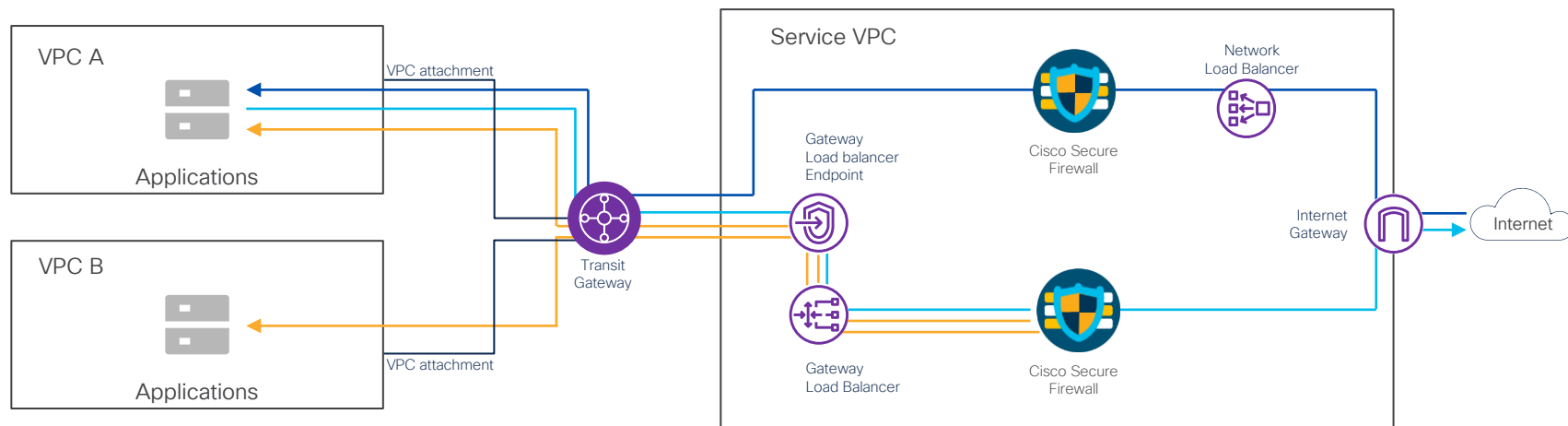
ISE Integration

- Multicloud Defense will integrate with Cisco Identity Services Engine (ISE)
- ISE utilizes Security Group Tags (SGTs)
 - STGs can correspond to business functions of devices, users, etc.
 - ISE (statically or dynamically) associates IP addresses to SGTs
- ISE will provide SGT-to-IP Address mappings to Multicloud Defense
- Multicloud Defense can then use these SGTs in policies.



Orchestrating Cisco Secure Firewall

Orchestration by Multicloud Defense, policy configuration by cloud FMC



Management



Cisco Defense Orchestrator (CDO)

CDO provides unified security management of Cisco security products

The screenshot displays the Cisco Defense Orchestrator (CDO) Onboarding interface. The top navigation bar includes the Cisco logo, the text "Defense Orchestrator", the "Onboarding" tab, a search bar with the placeholder "Type '/' to search", and user information for "cisco-att-cdo" with the email "erkostla@cisco.com".

A left-hand sidebar menu lists various navigation options: "Hide Menu", "Dashboard", "Multicloud Defense", "Inventory", "Configuration" (with sub-items "Policies", "Objects", and "VPN"), "Events & Monitoring" (with "Analytics"), "Change Log", "Jobs", "Tools & Services", and "Settings".

The main content area is titled "Select a Device or Service Type" and features a 3x3 grid of tiles for selection:

- ASA**: Adaptive Security Appliance (8.4+)
- Multiple ASAs**: Adaptive Security Appliance (8.4+)
- FTD**: Cisco Secure Firewall Threat Defense
- Meraki**: Meraki Security Appliance
- Integrations**: Enable basic CDO functionality for integrations
- AWS VPC**: Amazon Virtual Private Cloud
- Duo Admin**: Duo Admin Panel
- Umbrella Organization**: View Umbrella Organization Policies from CDO
- Import**: Import configuration for offline management

Managing Cisco Multicloud Defense

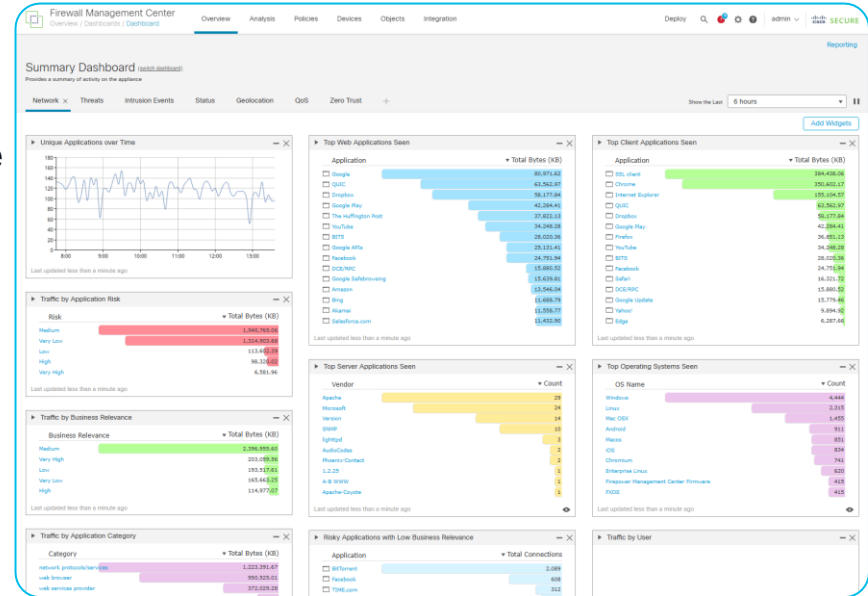
Firewall Management Center (FMC)

• Key Benefits

- Manage across many sites
- Control access and set policies
- Investigate incidents and prioritize response
- Available in physical and virtual options

• Features

- Multi-domain management
- Role-based access control
- High availability
- APIs and pxGrid integration
- Policy & device management
- Security intelligence



Managing Cisco Secure Firewall

Cloud-based FMC and on-premise FMCs can be launched from CDO

The screenshot displays the Cisco Defense Orchestrator (CDO) interface. The top navigation bar includes the Cisco logo, "Defense Orchestrator", and a "Services" tab. A search bar is present with the placeholder text "Type 'Ctrl' + '/' to search". The user profile "cisco-multicloud_defense_lab01" with email "erkostia@cisco.com" is visible in the top right.

The left sidebar contains a "Hide Menu" button and a list of navigation items: Dashboard, Multicloud Defense, Inventory, Configuration, Policies, Objects, VPN, Events & Monitoring, Analytics, Change Log, and Jobs.

The main content area shows the "FMC" (Firewall Management Center) configuration page. It includes a search bar "Search by Device Name, IP Address, or Serial Number" and a table listing FMCs.

☐	Name	Version	Devices	Type	Status	Last Heartbeat
☐	Cloud-Delivered FMC	20240808	1	Cloud-Delivered FMC	Active	09/02/2024, 23:41:25
☐	FMC741	7.4.1.1-build 12	6	On-Prem FMC	Synced	09/02/2024, 23:41:51

A "Tools & Services" dropdown menu is open, showing options: Dynamic Attributes Connector, Secure Connectors, Firewall Management Center (selected), Multicloud Defense Management, and ASA Templates. A "Migrations" section is also visible, containing "Firewall Migration Tool" and "Migrate FTD to cdFMC".

The bottom right corner of the interface indicates "No Active Jobs".

Managing Cisco Multicloud Defense

Multicloud Defense tab in CDO

The screenshot displays the Cisco Multicloud Defense interface within the Defense Orchestrator. The top navigation bar includes the Cisco logo, 'Defense Orchestrator', and 'Multicloud Defense'. A search bar and several status icons are also present. The sidebar on the left lists various navigation options, with 'Multicloud Defense' currently selected.

The main content area is titled 'Multicloud Defense' and features a 'Multicloud Defense Controller' button in the top right corner. The 'Accounts and Assets' section shows a summary of cloud accounts: 1 AWS, 1 Azure, 1 GCP, and 0 Oracle, totaling 3 accounts. A 'View Accounts' link is provided. The 'Account Resources' section displays a breakdown of resources: 20 VPCs/VNets, 182 Security Groups, 21 Route Tables, 30 Subnets, 18 Instances, 6 Load Balancers, 870 Tags, and 6 Applications. The 'Enable Traffic Visibility' section includes a description and an 'Enable visibility' button. The 'Multicloud Defense Shared Objects' section shows a table with 4 networks. The 'VPN Connections' section indicates 3 Multicloud Defense Connections and provides a link to 'Create a Site-to-Site VPN to Multicloud Defense'. The 'Tunnels' section shows a table with one tunnel named 'pod2-dc-to-aws'.

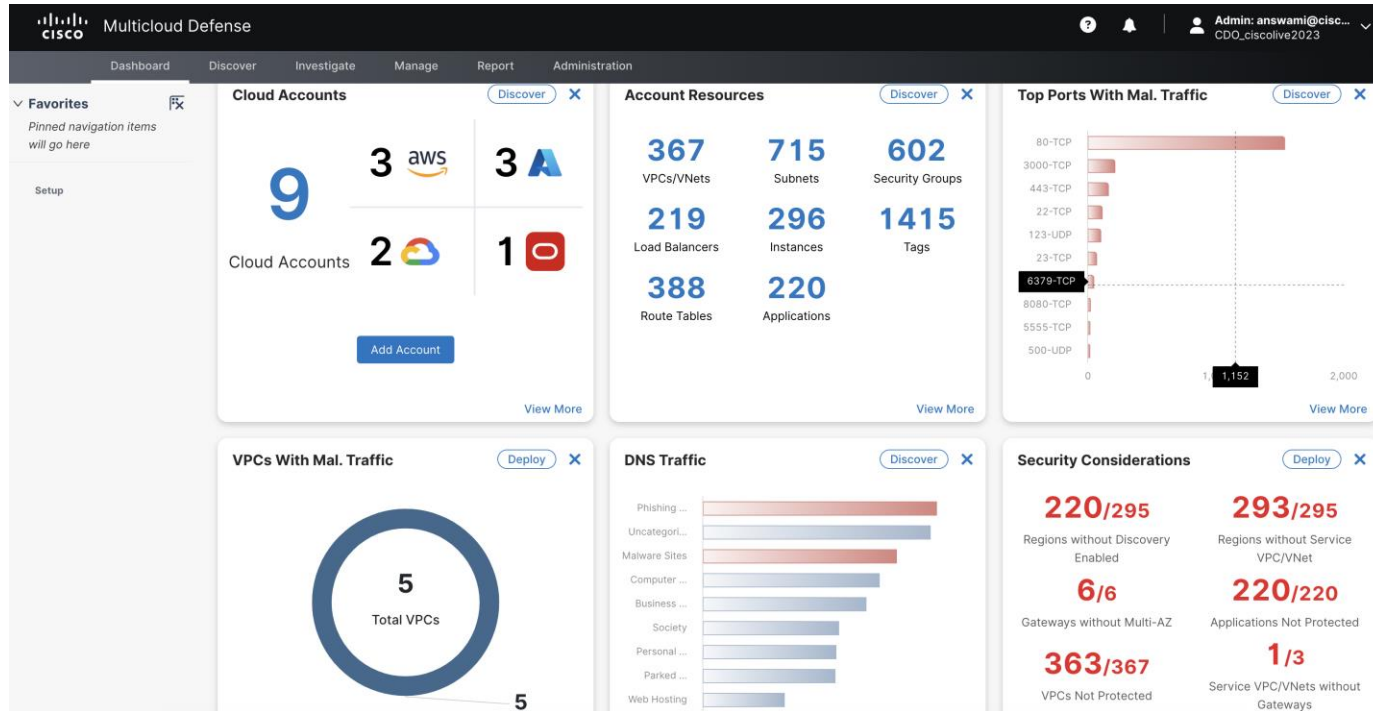
Object Type	Count
networks	4

Name	Peer 1 IP	Peer 2 IP	Active
pod2-dc-to-aws	3.80.231.87	172.16.2.15	No

No Active Jobs

Managing Cisco Multicloud Defense

Multicloud Defense console launched from CDO



Security Cloud Control

Cisco's unified security management platform



Simplify operations

- See everything happening in your security systems in real time.
- Get a complete view across all firewall and security service deployments, with detailed information about applications, users, devices and workloads.
- Clean up policies and remediate misconfigurations.



Enhance security

- Leverage AIOps insights to automate deployments based on best practices to improve security posture.
- Predict and prevent health and performance issues from a single place.
- Minimize downtime and reduce risk of exploitation due to misconfiguration.



Improve clarity

- Reduce burden on users on relying on tribal knowledge and manual work on adhering best practices.
- Reassure with AI insights through extra layers of validation and security insights.



Home



Dashboard



AI Ops Insights



Inventory



Policies



Objects



VPN



Analytics



Management



Settings

Dashboard

Customize | Report

Top insights & alerts

All insights

Elephant flow spike observed

Data sources: FTD

Traffic has risen steadily over three weeks with some large flows consuming excessive bandwidth, necessitating intervention to avoid performance issues.

Details >

RAVPN Head-End Capacity Utilisation

Data sources: FTD

RAVPN head-end capacity is approaching critical limits. This alert details active and idle sessions, indicating possible performance drops and connection problems if not resolved.

Details >

1% Decrypted traffic towards internet

Data sources: FTD

Failure to decrypt a significant portion of traffic poses a severe security risk, potentially concealing malicious activities, leaving your network vulnerable to cyber threats.

Details >

Top actions

Top information

Report

Policy optimizer

Last 90 days

Data sources: FTD

18k Rules with anomalies

5723 Shadowed



- 18263 Rules with anomalies
- 515 Disabled rules
- 79 Expired rules
- 11667 Healthy rules

Details >

Top risky apps and URL categories allowed

last 90 days

Applications

URL categories

Very High Risk

Data sources: FTD

App name	Business relevance	Category
AceProject	Very high	email
AD DSROL	Very high	CMR
Contently	Very high	business

Risk & vulnerabilities

CVM Integration

Last 90 days

Data sources: FTD



- 10 High risk
- 4 Medium risk
- 75 Low risk

14 high and medium

vulnerabilities not covered

Top intrusions & malware events

last 90 days

Data sources: FTD Multicloud

Intrusions events

Malware events

Allowed

Name	Priority	Count
Malware-CNCWin.Trojan	High	42

Cisco Live!

AI Assistant for the Firewall

Assist, Augment and Automate

Improve visibility



Reduce effort to learn about the policies you have deployed

“What are the rules in my #campus-fw policy?”

“This policy contains a total of 2,500 rules. About 1,500 rules are set to 'allow' action, while approximately 1,000 are set to 'block'.”

Speed up troubleshooting



Use knowledge base to autocomplete troubleshooting steps

“Have I enabled malware analysis on my access control policy?”

“Yes. You currently have malware analysis enabled on 120 rules out of 700.”

Act faster



Take actions to create new rules or block existing ones

“Remove duplicate rules.”

“Calling services to check and remove duplicates. We found 300 duplicate rules. Please confirm if you would like to delete these rules. You can restore the config file should anything fail.”



What do you want to ask today?

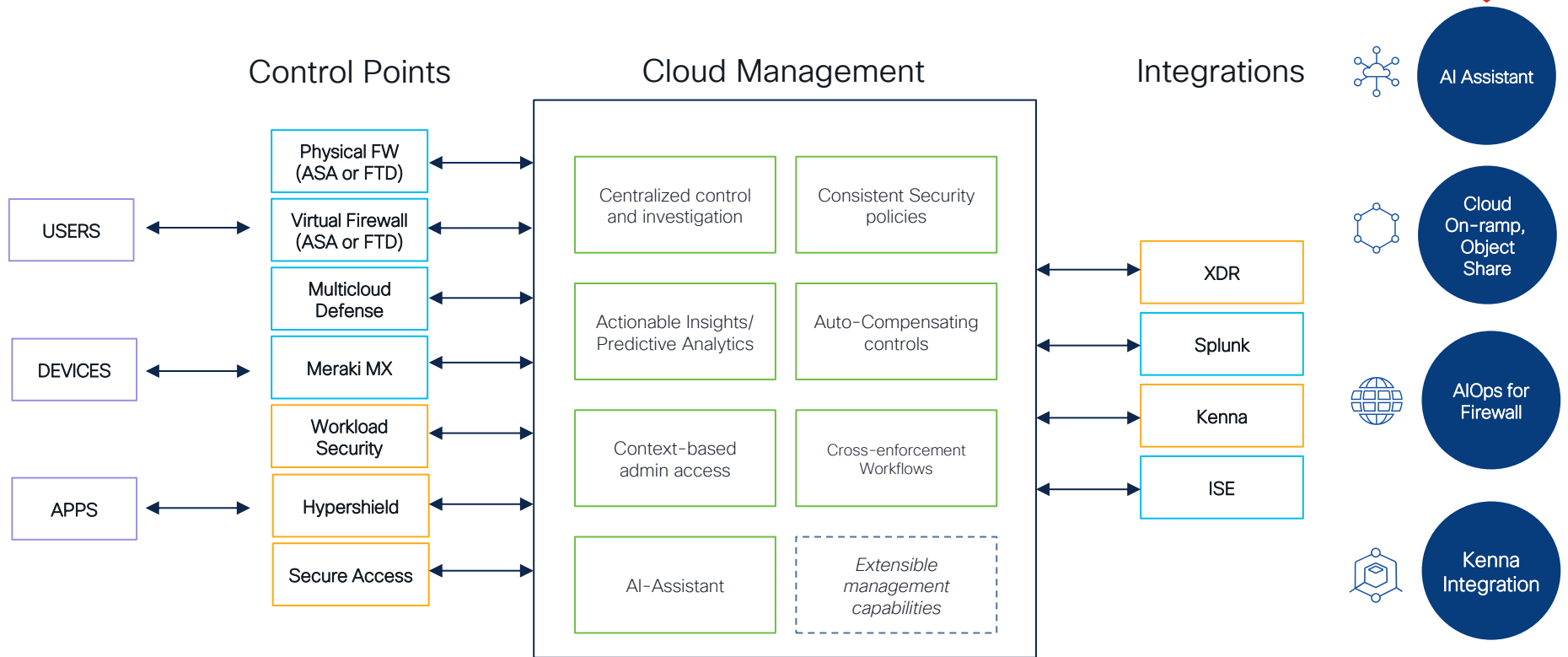
Choose a suggestion or use the text field to ask a question. I have limitations and won't always get it right, but your feedback will help me improve.

- How do I create a basic security policy for FTD?
- How do I schedule a recurring backup?
- How many access control rules are there?
- What's the difference between an Admin and a Super Admin?

Ask the AI Assistant a question ▶

The AI Assistant may display inaccurate information. Make sure to verify the responses. [View our FAQs](#) to learn more.

Security Cloud and Security Cloud Control



Complete Your Session Evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to claim a **Cisco Live T-Shirt**.



Complete your surveys in the **Cisco Live mobile app**.



Continue your education

- Visit the Cisco Stand for related demos
- Book your one-on-one Meet the Expert meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Contact me at: erkostla@cisco.com



Thank you



#CiscoLiveAPJC

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC