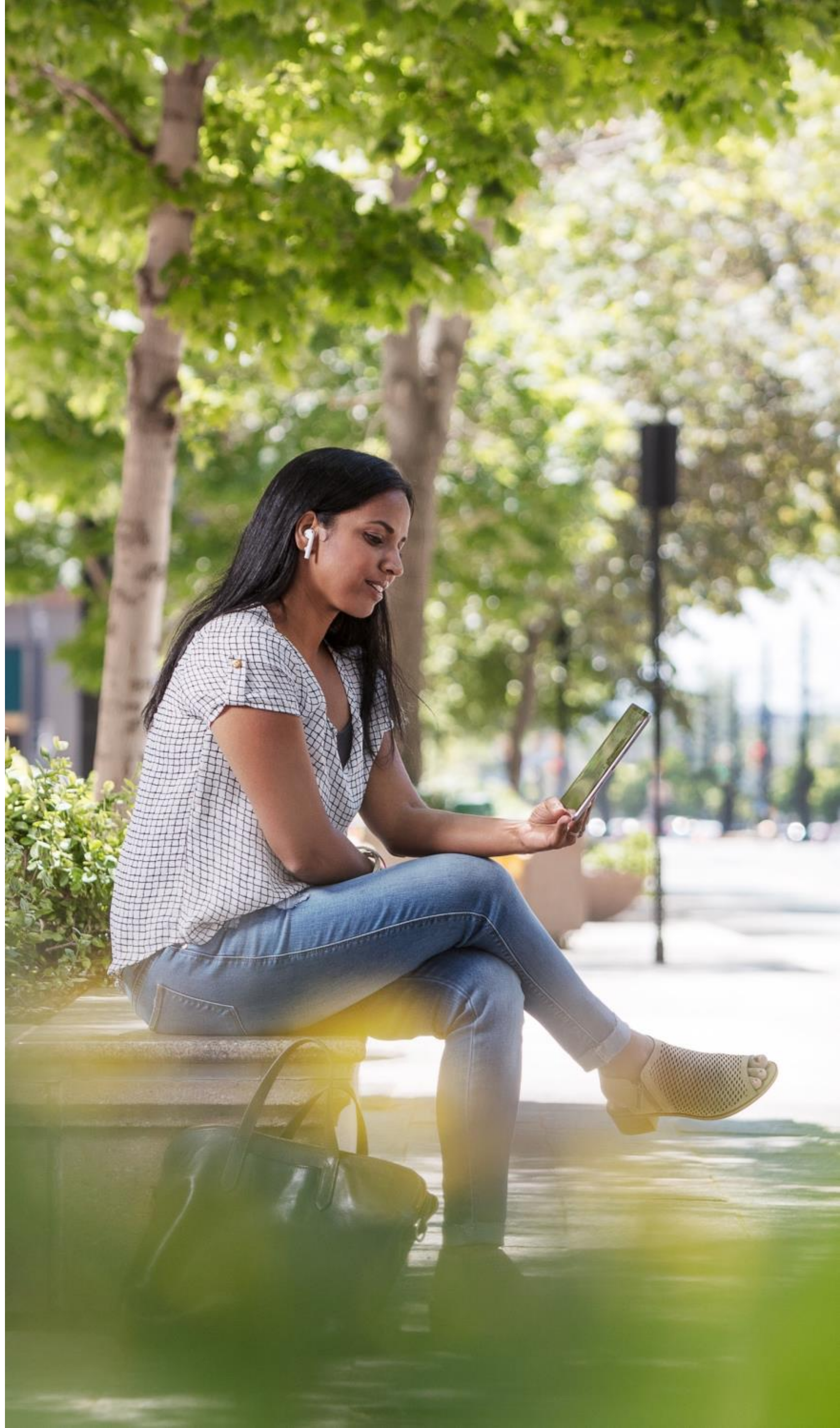
High Speed Firewall Innovations

Power of the Platform

Nikolaj Pabst Nielsen
Cisco Security Denmark
October 2023



AGENDA

1. Hardware & Software Innovations
2. Firewall Threat Defense 7.x
3. Cloud Firewalling

Why a Cisco Firewall?

Integrations

Innovation

Performance

AGENDA

1 Hardware & Software Innovations

2 Firewall Threat Defense 7.x

3 Cloud Firewalling

Firewall Management Center

Firewall Management Center Hardware

FMC1700 NEW

Specifications

No. of Managed Sensors	50
Maximum IPS Events	30 Million
Maximum Event rate pr. Second	5000 Eps
Power Consumption	1050W / 2626 BTU/hr
Formfactor	30 x 16.9 x 1.7 (1RU)

FMC2700 NEW

Specifications

No. of Managed Sensors	300
Maximum IPS Events	60 Million
Maximum Event rate pr. Second	12.000 Eps
Power Consumption	1050W / 2626 BTU/hr
Formfactor	30 x 16.9 x 1.7 (1RU)

FMC4700 NEW

Specifications

No. of Managed Sensors	1000
Maximum IPS Events	400 Million
Maximum Event rate pr. Second	30.000 Eps
Power Consumption	1050W / 2626 BTU/hr
Formfactor	30 x 16.9 x 1.7 (1RU)

HA is supported

Firewall Management Center Software

FMCv

Specifications	
No. of Managed Sensors	25
Maximum IPS Events	10 Million
Maximum Event rate pr. Second	Varies
vCPU	8
Storage	250GB

FMCv300

Specifications	
No. of Managed Sensors	300
Maximum IPS Events	60 Million
Maximum Event rate pr. Second	12.000 Eps
vCPU	32
Storage	2.2TB

cdFMC (SaaS)

Specifications	
No. of Managed Sensors	1000*
Maximum IPS Events	400 Million
Maximum Event rate pr. Second	100.000 Eps
Licensing	Pr. Device
Logging	Separate

HA is supported

*Scaling to 5000 in LA

Firewall Hardware

Cisco Secure Firewall Hardware Portfolio

650 Mbps
AVC+IPS

SMB

1.5-2.2 Gbps AVC+IPS

1120/40/50

Branch Office

2.3-20 Gbps
AVC+IPS

2110/20/30/40

Mid Enterprise

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

NEW

3105/10/20/30/40

Large Enterprise

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

4112/15/25/45

Data Center

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

NEW

4215/25/45

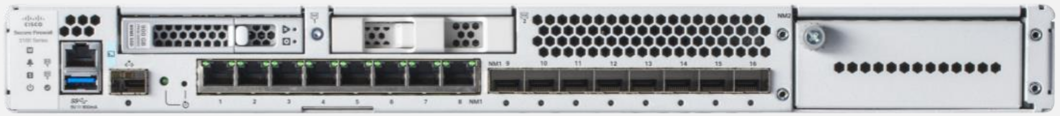
One Module:
30-70 Gbps AVC
24-64 Gbps AVC+IPS
Sixteen node cluster:
AVC+IPS
SM40*16n = 704 Gbps
SM48*16n = 830 Gbps
SM56*16n = 950 Gbps

9300 Series
SM-40
SM-48
SM-56

Service Provider

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

3100 Series



4200 Series

AGENDA

1 Hardware & Software Innovations

2 Firewall Threat Defense 7.x

3 Cloud Firewalling

Cisco Secure Firewall 7.x

Zero Trust Microsegmentation

Protecting application environments with integrated firewall & workload protection

Securing Multicloud environments

New CSPs & Hypervisor, Flexible & Tiered Licensing, Cloud FW-aaS, Horizontal Scaling

Securing Hybrid Worker

Simplified remote worker security - advance posture, passwordless authentication & new unified client

Modern NGIPS

Superior threat visibility & performance with Snort 3

Visibility & Enforcement in encrypted traffic

Delivering threat & application visibility with TLS 1.3 decryption, Server Identity and Encrypted Visibility Engine

Simplified Branch Deployments

New WAN capabilities for intelligent path selection and direct internet access

Secure Dynamic Attribute Connector

Enabling strong policies for infrastructure without fixed IP addresses

Scalable Analytics, Threat Response & Orchestrator

Accelerate detection & remediation – “See x, Do y”

With 300+ agile features, usability improvements, software optimizations

Now offering newer RTMs, Marketplace offerings, Flexible & Tiered Licensing

Encryption is Ubiquitous

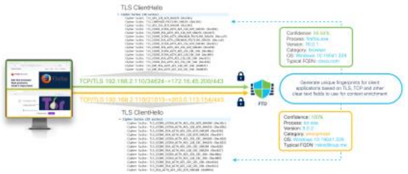
010110
110010
001011

Deep packet inspection becomes challenging

Decryption increases hardware costs

Many sites/protocols cannot be decrypted due to certificate pinning

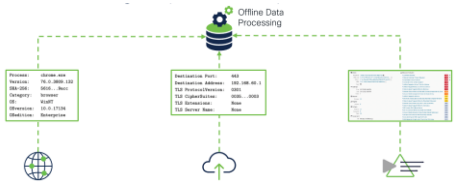
Encrypted Visibility Engine Benefits


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
TLS ClientHello
FTD
Generate unique fingerprints for client applications based on TLS, TCP and other clear text fields to use for context enrichment

Confidence: 99.64%
Process: firefox.exe
Version: 76.0.1
Category: browser
OS: Windows 10 1909/1.339
Typical FQDN: cisco.com

Confidence: 100%
Process: tor.exe
Version: 9.0.2
Category: anonymizer
OS: Windows 10 1909/1.339
Typical FQDN: [illegible]

Encrypted Visibility Engine

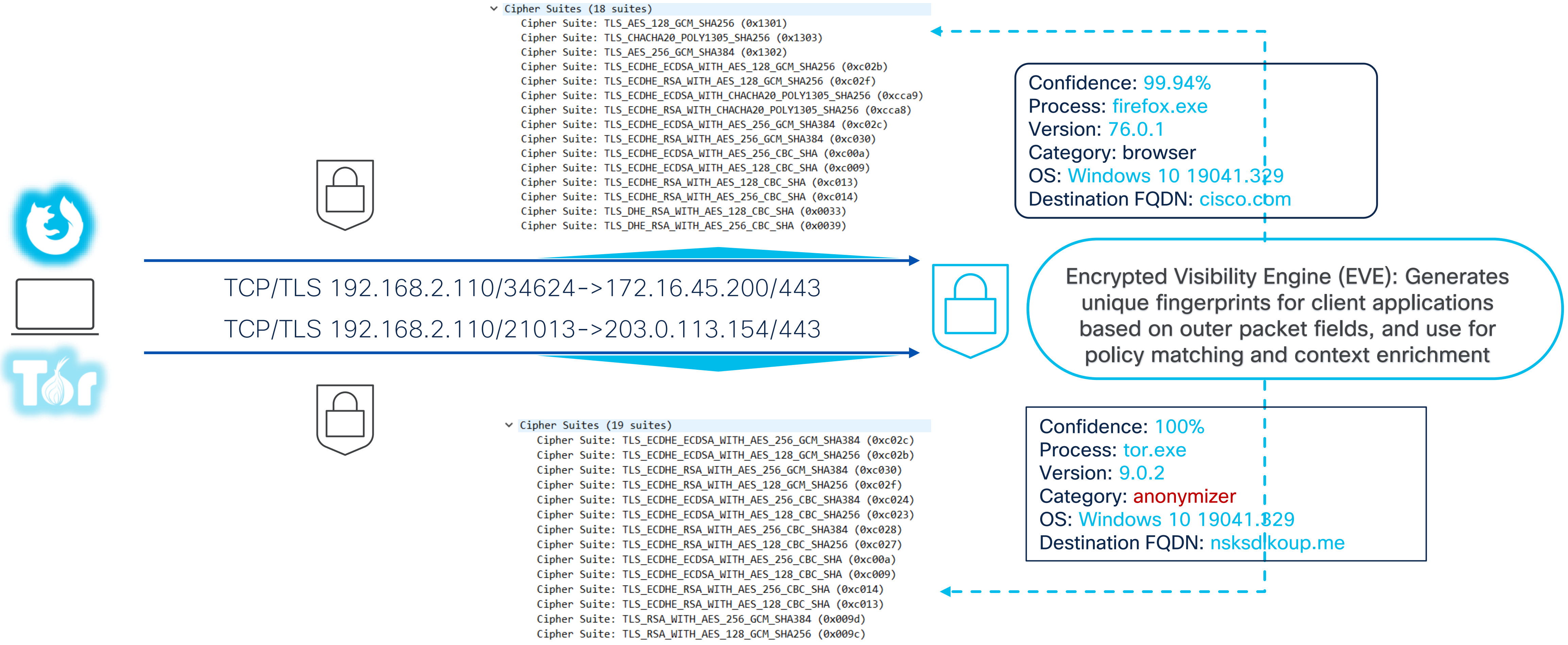


```
Process:      chrome.exe
Version:      76.0.3809.132
SHA-256:      5616...9acc
Category:     browser
OS:           WinNT
OSversion:    10.0.17134
OSedition:    Enterprise
```

```
Destination Port:       443
Destination Address:    192.168.40.1
TLS ProtocolVersion:    0301
TLS CipherSuites:       0035...0003
TLS Extensions:         None
TLS Server Name:        None
```

- Detects and blocks malware in encrypted flows
- Can be used for APP control in the firewall policy
- Triggers Indications of Compromise
- Minimal performance impact
- Enriches Endpoint DB with Application and OS

Encrypted Visibility without Decryption



```
⌄ 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 (0xcca8)
    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

TCP/TLS 192.168.2.110/34624->172.16.45.200/443

TCP/TLS 192.168.2.110/21013->203.0.113.154/443

Encrypted Visibility Engine (EVE): Generates unique fingerprints for client applications based on outer packet fields, and use for policy matching and context enrichment

```
⌄ 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: nsksdlkoup.me

Are Cisco Firewalls “SDWAN” ready?

SDWAN Features on FTD

Connectivity

- **Routebased VPN over VTIs**
- IPv6 VTI w. BGP
- BGP(v6) over VTI
- EIGRP & OSPF over VTI
- **DVTI including DHCP support**

Bandwidth

- **Dual ISP Configuration**
- **Active/Standby VTIs w. SLA monitoring**
- Optimal Path Selection based on application monitoring
- **ECMP Support for VTIs & ISPs**
- **Application based LB & PBR**

Simplicity

- Auto Config Rollback
- **Low Touch Provisioning**
- **Umbrella Auto Tunnel Deployment**
- **DVTI Hub'n'Spoke topologies**
- **Data Interface Mangement**

Are Cisco Firewalls SDWAN ready?

Zero Trust Application Access

Securely and Simply Connect Users to Private Applications

Limit who is allowed

Per application access with clientless SAML, Azure AD, ISE, and Duo

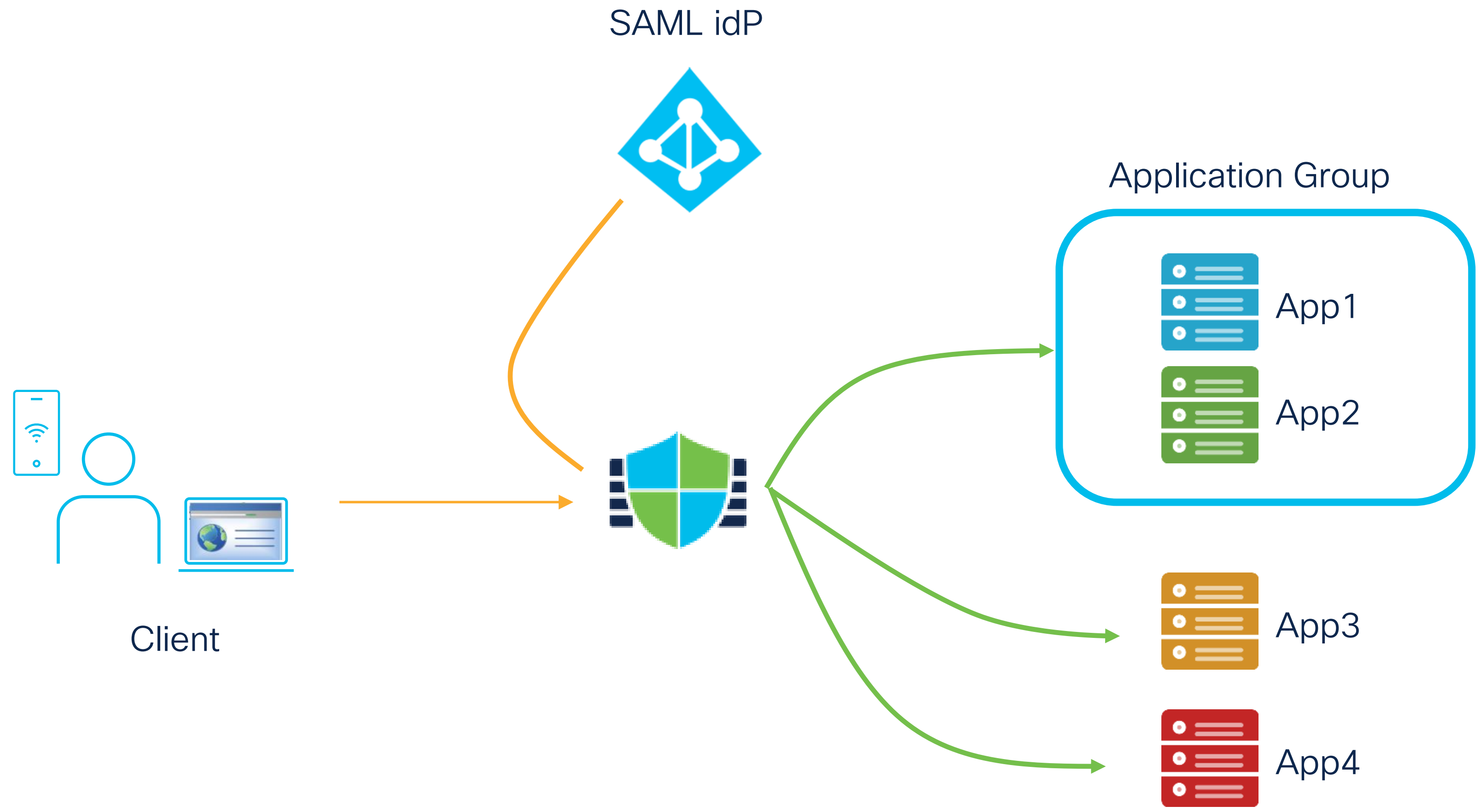
Limit where they can go

Reduce access to specific apps to limit attack surface and lateral spread of threats

Limit threats they may bring

Go beyond traditional ZTNA by continuously inspecting allowed traffic/behaviors with IPS/malware protection

Zero Trust Application Access Flow



Clientless ZTAA in 7.4

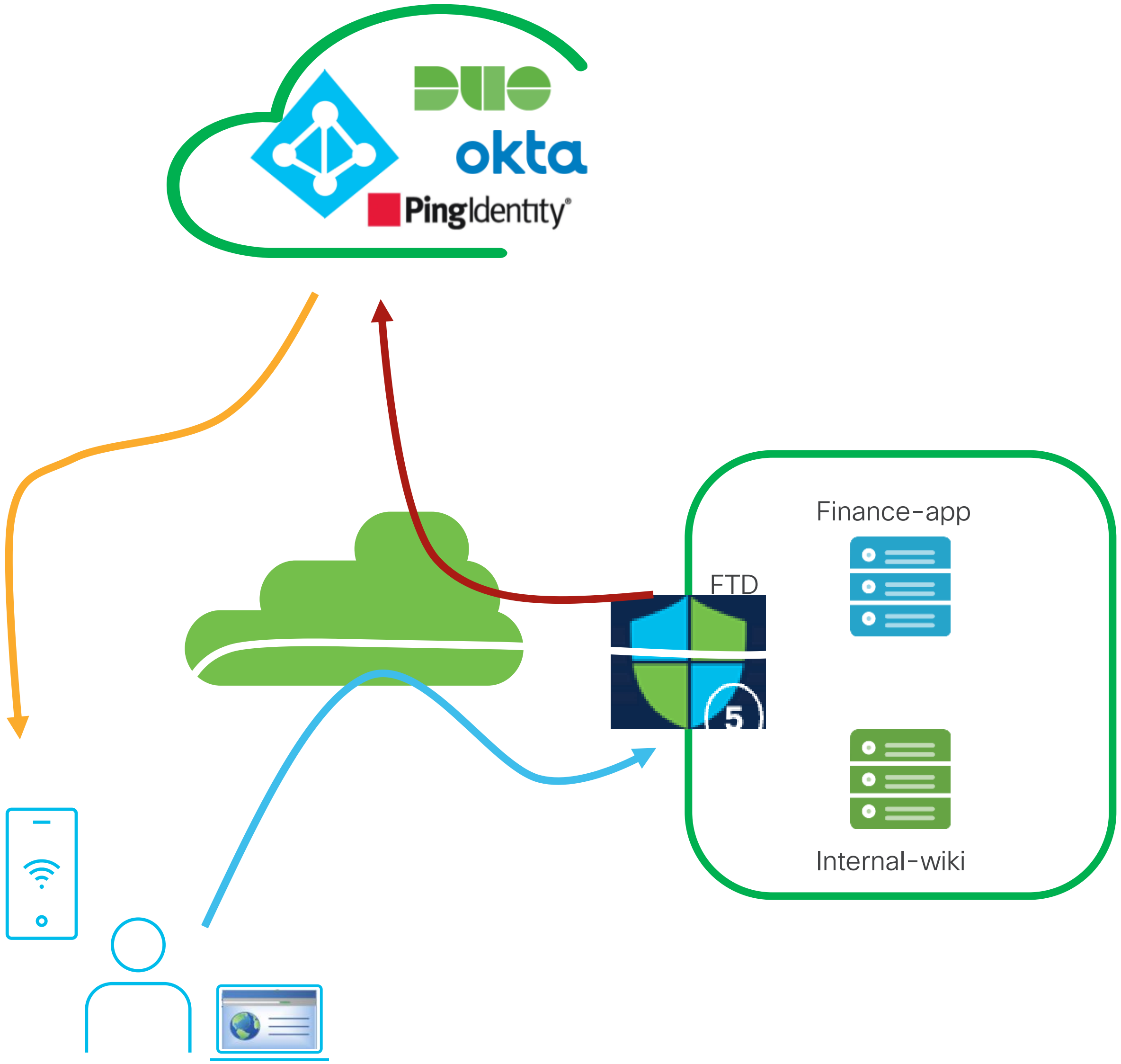
1 User connects to application via a web browser (HTTPS), DNS resolves to the FTD.

2 Browser is redirected to a SAML IdP for Authentication and Authorization.

3 Policy, MFA and Posture handled by the IdP as part of the SAML Flow.

4 Access is allowed based on SAML Assertion, cookie is tracked.

5 Optional IPS and Malware Inspection based on policy



Integrations

Powers the platform

ACI

ISE

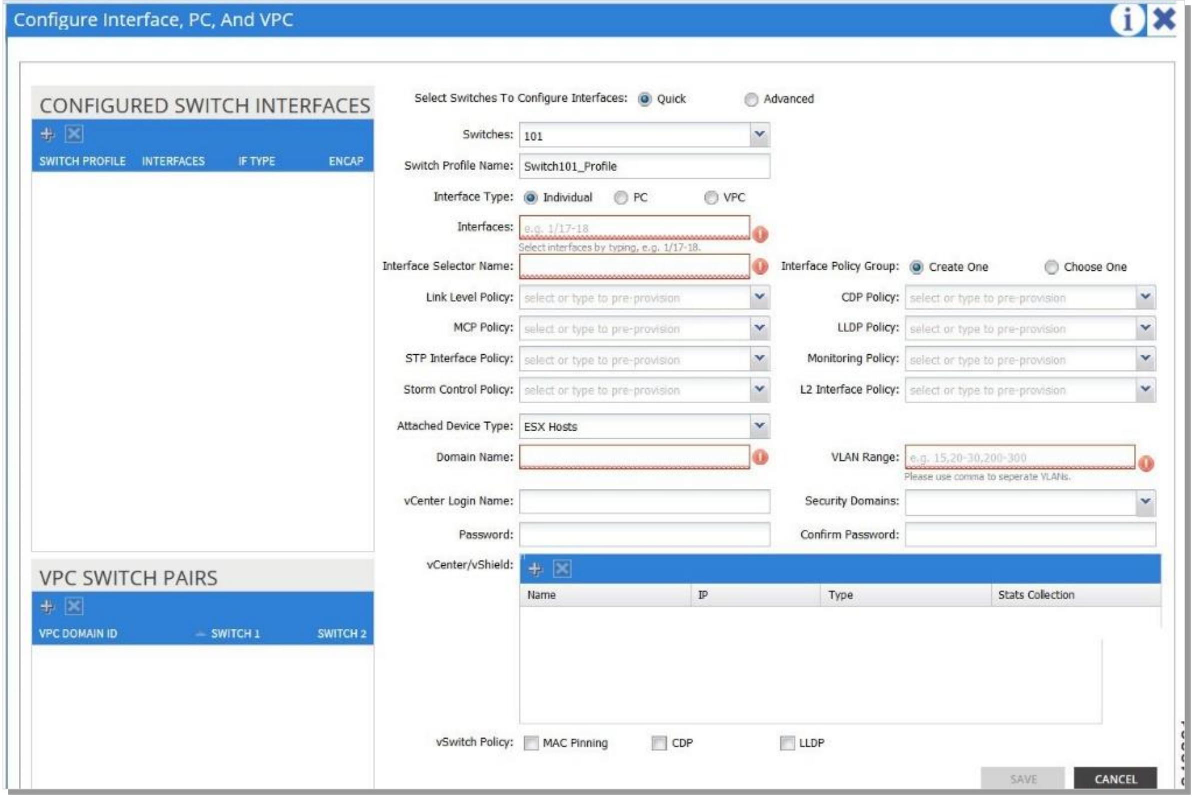
CSW

DNS

Application-Centric Infrastructure

Transparent policy-based security for both physical and virtual environments

- Link security to software defined networking
- Create identity-based policy with Application Policy Infrastructure Controller (APIC)
- Segment physical and virtual endpoints based on group policies with detailed and flexible segmentation



Configure Interface, PC, And VPC

Select Switches To Configure Interfaces: ● Quick ○ Advanced

Switches: 101

Switch Profile Name: Switch101_Profile

Interface Type: ● Individual ○ PC ○ VPC

Interfaces: e.g. 1/17-18

Select interfaces by typing, e.g. 1/17-18.

Interface Selector Name:

Interface Policy Group: ● Create One ○ Choose One

Link Level Policy: select or type to pre-provision

CDP Policy: select or type to pre-provision

MCP Policy: select or type to pre-provision

LLDP Policy: select or type to pre-provision

STP Interface Policy: select or type to pre-provision

Monitoring Policy: select or type to pre-provision

Storm Control Policy: select or type to pre-provision

L2 Interface Policy: select or type to pre-provision

Attached Device Type: ESX Hosts

Domain Name:

VLAN Range: e.g. 15,20-30,200-300

Please use comma to seperate VLANs.

vCenter Login Name:

Security Domains:

Password:

Confirm Password:

vSwitch Policy: □ MAC Pinning □ CDP □ LLDP

Integrations

Powers the platform

ACI

ISE

CSW

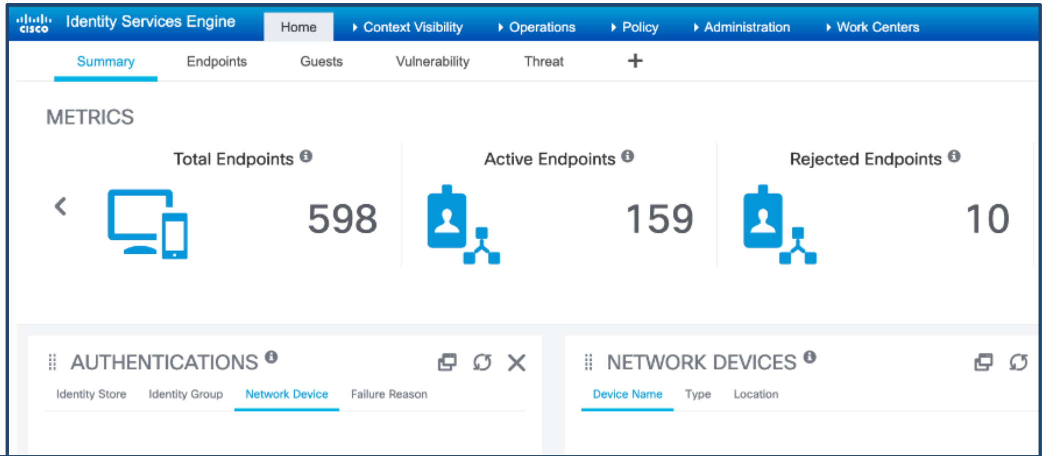
DNS

Integration with Cisco ISE

- Use Active Directory users and groups in policy configuration
- Use Cisco Identity Services Engine to provide identity
  - TrustSec Security Group Tag (SGT)
  - Device type (endpoint profiles) and location
  - Identity Mapping Propagation & device level filtering

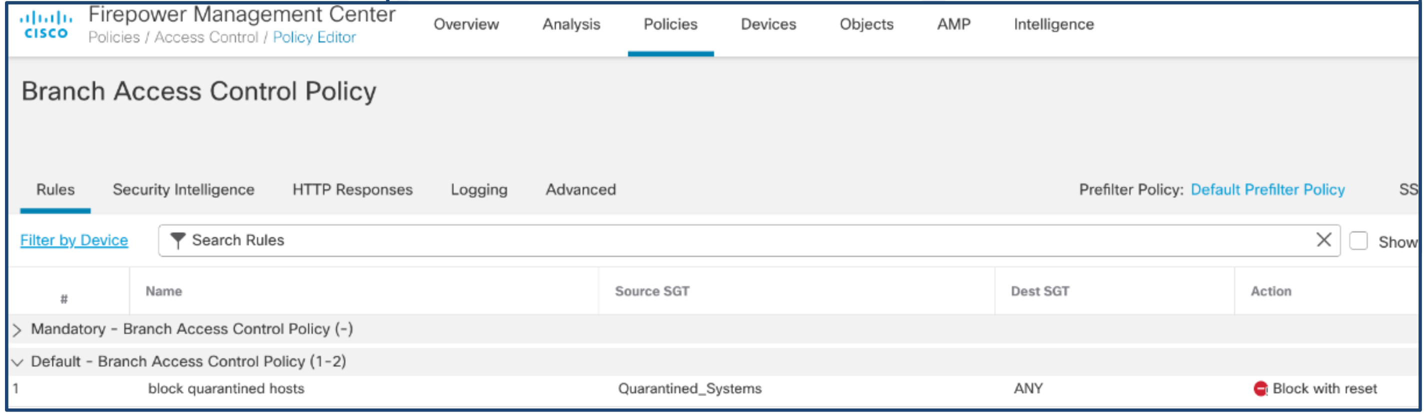
Key

- 🟧 Employee Tag
- ⬛ Developer Tag
- 🟪 Voice Tag
- 🟥 Non-Compliant Tag
- 🟩 Employee Info Tag
- 🟥 Developer Server Tag
- 🟦 Financial Server Tag
- 🟦 HTTP Tag



METRICS

Total Endpoints	Active Endpoints	Rejected Endpoints
598	159	10



Firepower Management Center
Policies / Access Control / Policy Editor
Overview
Analysis
Policies
Devices
Objects
AMP
Intelligence

Branch Access Control Policy

Prefilter Policy: Default Prefilter Policy

#	Name	Source SGT	Dest SGT	Action
	Mandatory - Branch Access Control Policy (-)			
	Default - Branch Access Control Policy (1-2)			
1	block quarantined hosts	Quarantined_Systems	ANY	Block with reset

cisco SECURE

Simplify Security Management with TrustSec

Leverage the network and investment

- Scalable and agile segmentation technology in over 40 different Cisco product families
- Enables dynamic, role-based policy enforcement anywhere on your network
- Extend TrustSec policies over Firepower Threat Defense with SRC & DST SGT matching

Simplified Access Management

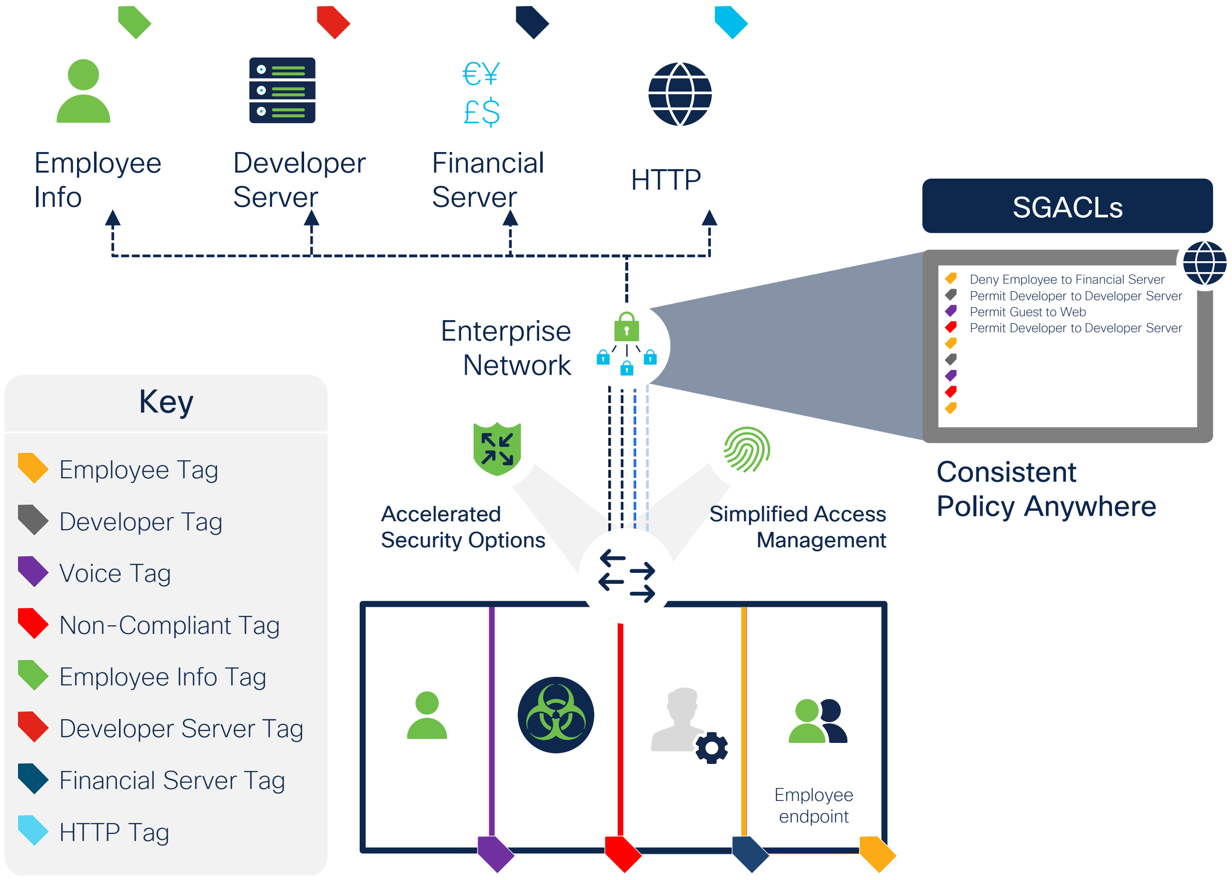
Manage policies using plain language and maintain compliance by regulating access based on business role

Rapid Security Administration

Speed-up adds, moves, and changes, simplifying firewall administration to speed up server onboarding

Consistent Policy Anywhere

Control all network segments centrally, regardless of whether devices are wired, wireless or on VPN



Deny Employee to Financial Server
Permit Developer to Developer Server
Permit Guest to Web
Permit Developer to Developer Server

Integrations

Powers the platform

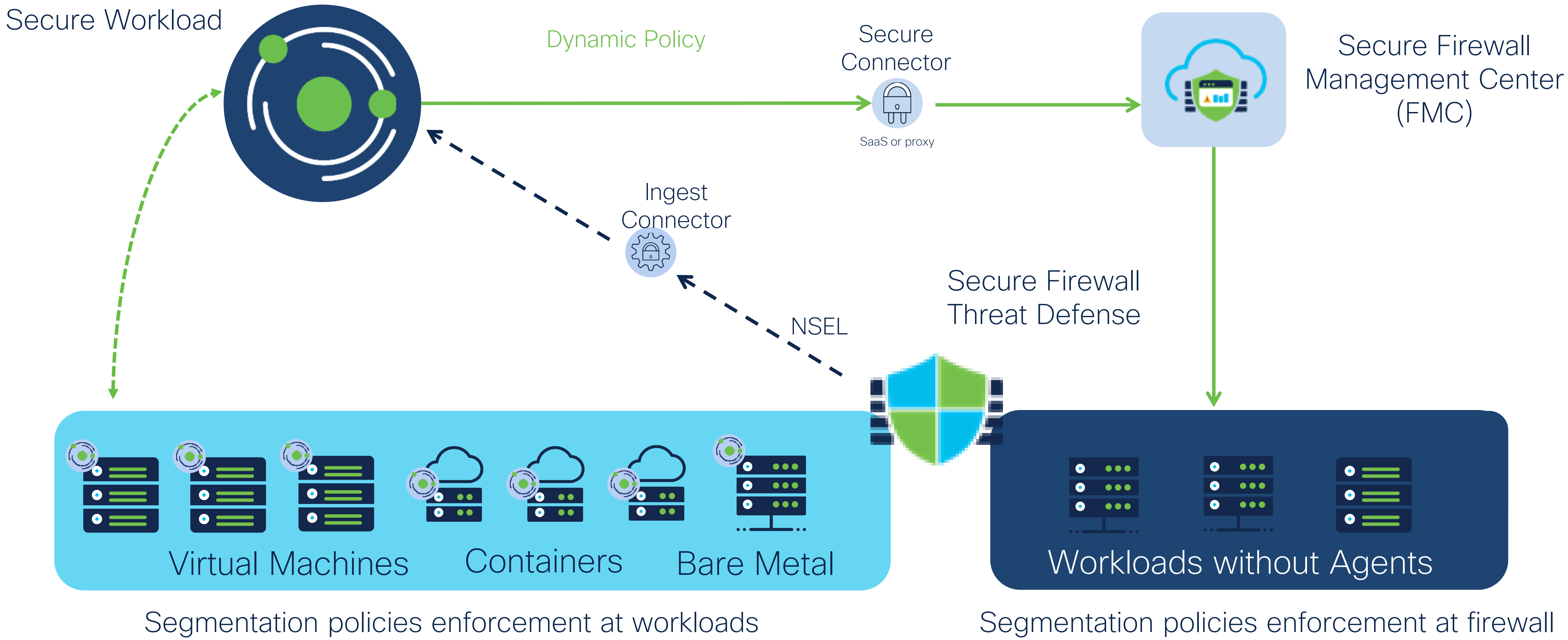
ACI

ISE

CSW

DNS

Secure Firewall – High Level Architecture


Secure Workload
Dynamic Policy
Secure Connector
SaaS or proxy
Secure Firewall Management Center (FMC)
Ingest Connector
NSEL
Secure Firewall Threat Defense
Virtual Machines
Containers
Bare Metal
Workloads without Agents
Segmentation policies enforcement at workloads
Segmentation policies enforcement at firewall

cisco SECURE

Integrations

Powers the platform

ACI

ISE

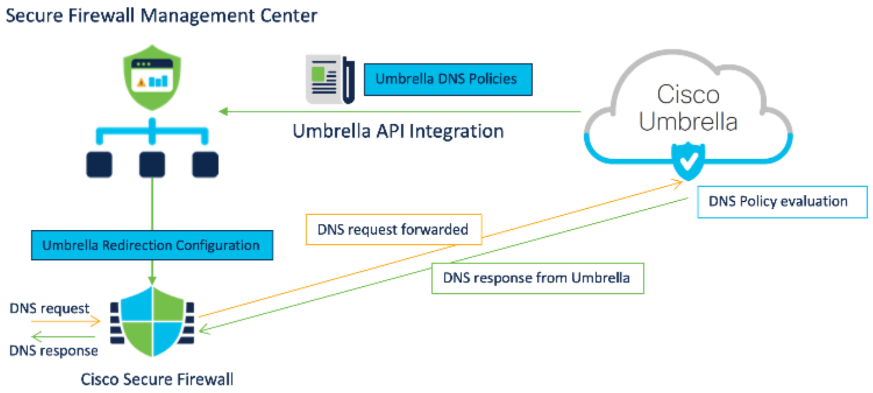
CSW

DNS

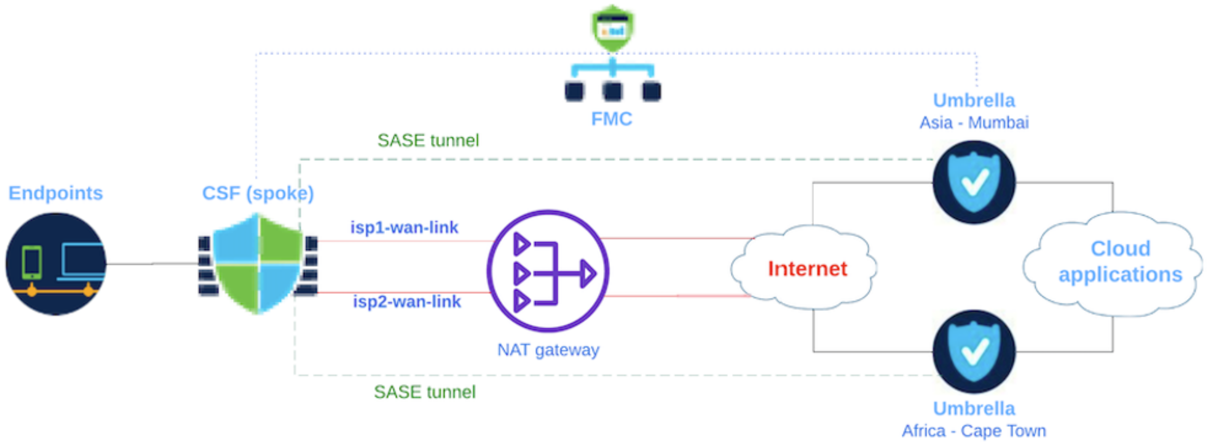
Umbrella Integration

SASE Deployments Auto Tunnel and Common DNS Security Policy

- Common Security Policies for all branches
- Multi-layered DNS Security
- Faster Protection
- Improved Internet Performance
- Uniform Security policy for Hybrid workers



- SASE use case
- Umbrella SIG – Cloud-delivered Firewall
- Auto-generation and deployment of configuration on Firewall and Umbrella



AGENDA

1 Hardware & Software Innovations

2 Firewall Threat Defense 7.x

3 Cloud Firewalling

Simplifying Multi-Cloud Enviror

Private Cloud

HyperFlex

NUTANIX NEW

KVM

openstack

vmware ESXi

Public Cloud

aws

Google Cloud Platform

Microsoft Azure

ackspa

ORACLE CLOUD INFRASTRUCTURE

EQUINIX NEW

Alibaba Clou NEW

Gov/IC Cloud

aws

Microsoft Azure

Google Cloud Platform NEW

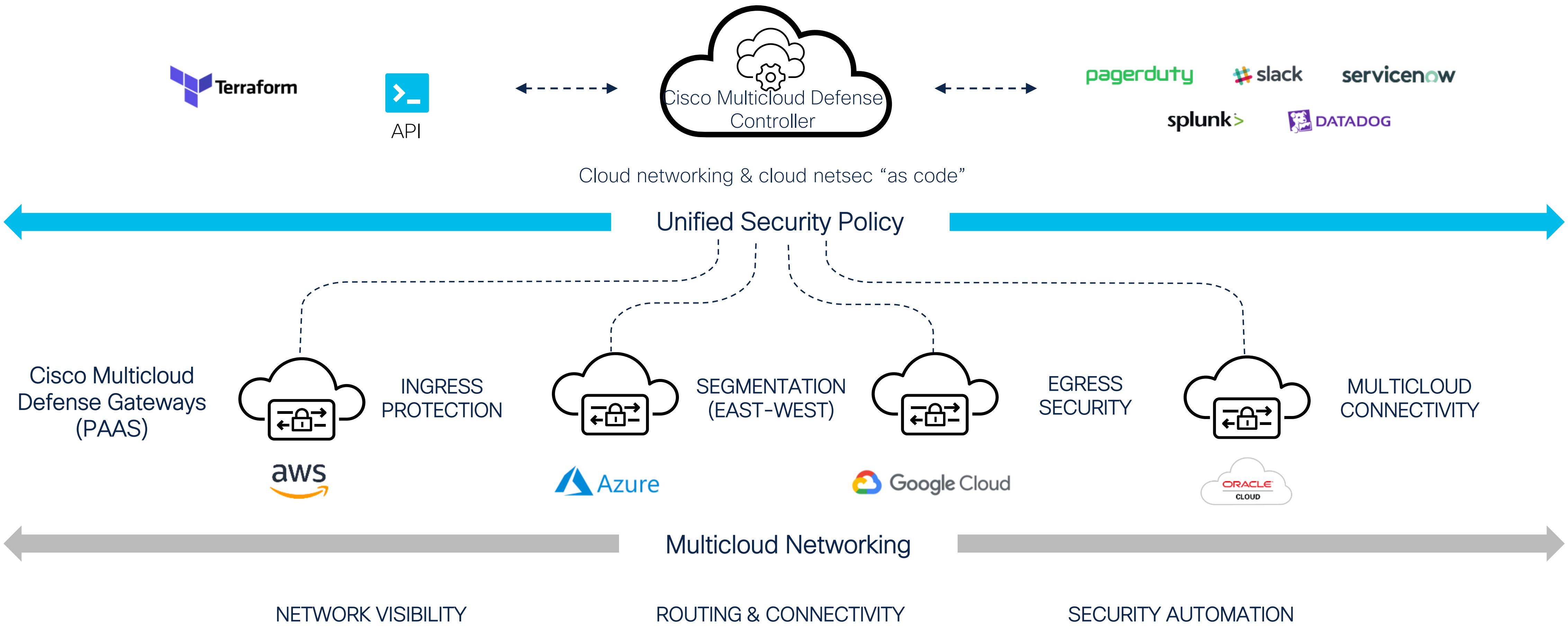
Virtual firewall performance-based licensing from 100M bps

Cloud Leadership

- Clustering & Auto Scaling
- Integration with cloud native services & infrastructure
- Accelerated Netw
- ered Licensing
- Dynamic Policy
- Quickstarts, Infrastructure as Code and Automation
- Gateway Load ba integratio
- apshots

Cisco Multicloud Defense

Combining multicloud networking, automation, and cloud-native network security controls



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

East/West

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

* No TLS decryption is needed

Forwarding mode is available on Multicloud Defense Gateway

The bridge to possible