
TURN
IT
UP
cisco Live!
#CiscoLive

The bridge to possible

Keeping Up on Network Security with Cisco Secure Firewall

Andrew Ossipov
Distinguished Engineer

BRKSEC-2417

Your Speaker

Andrew Ossipov

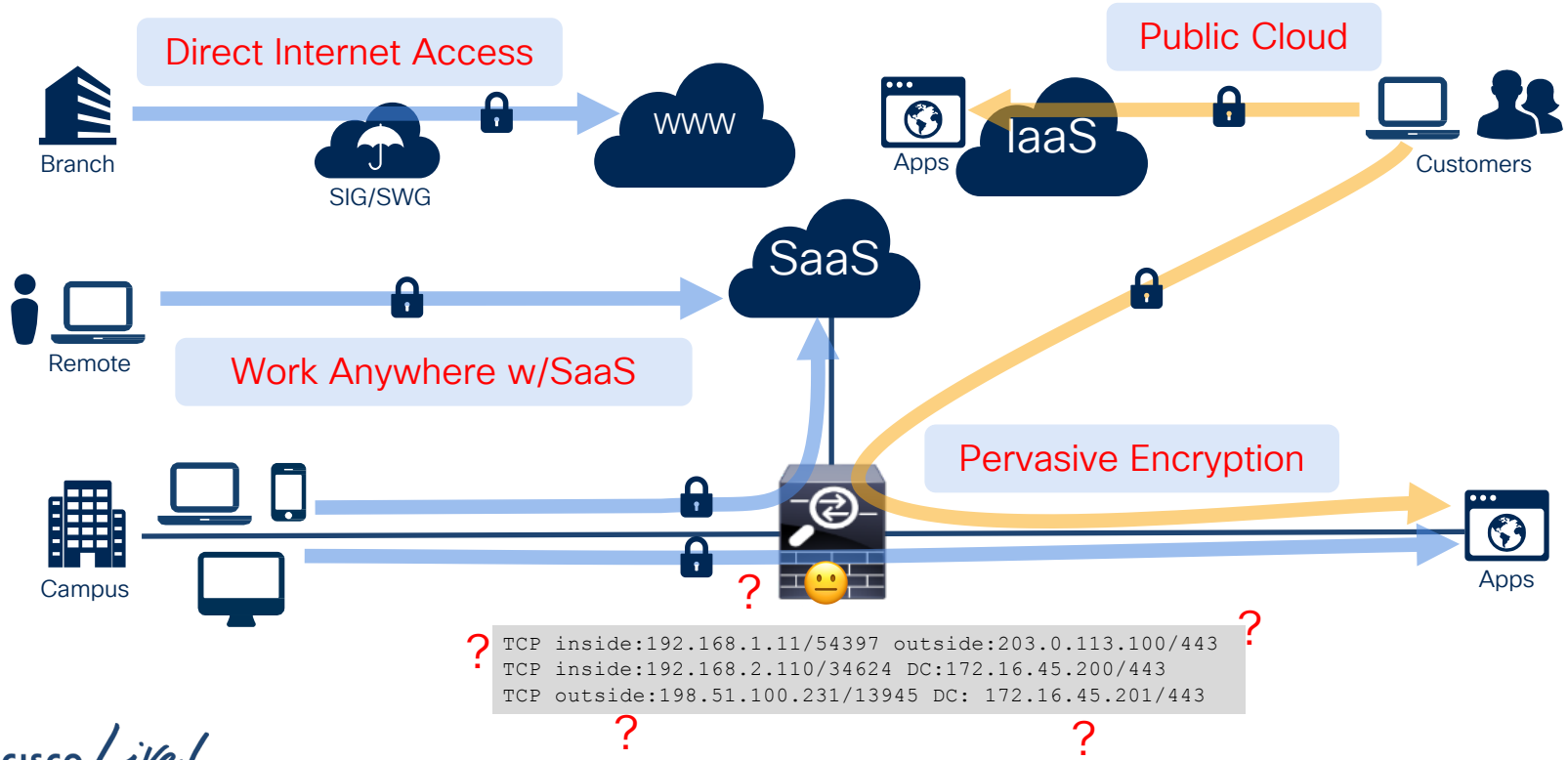
aeo@cisco.com

Distinguished Engineer

Network and Workload Security Portfolio CTO

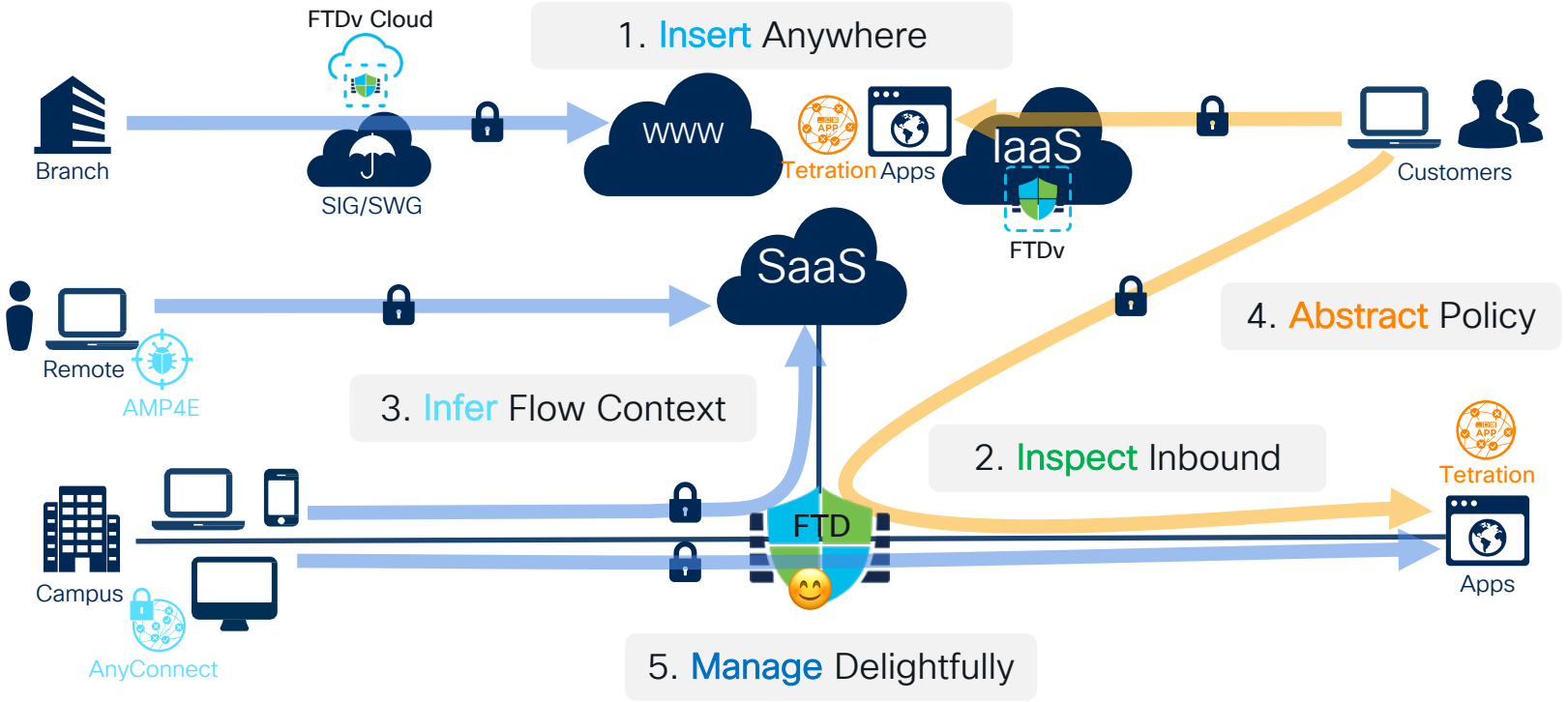
IETF: OpSec and TLS Working Groups

Is Network Firewall Dead?



Agenda: Cisco Secure Firewall Threat Defense

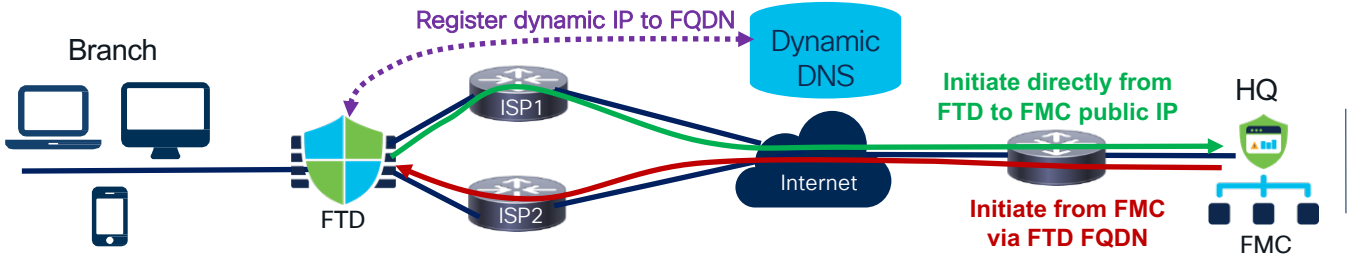
Past and Present are set in stone, but the Future may change at any time



Insert

Remote Branch Deployment in FMC 6.7

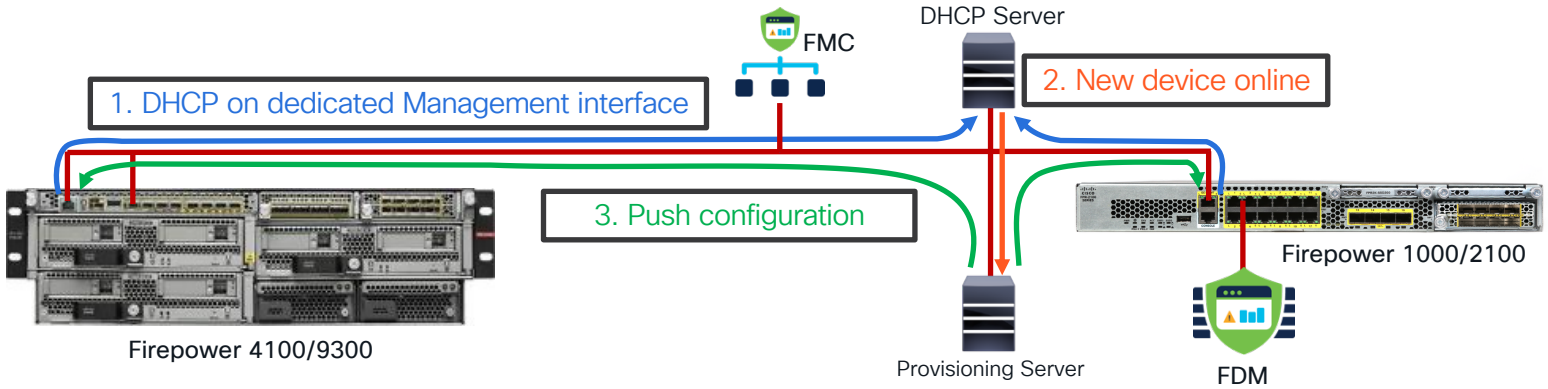
- FMC management over one data interface for non-VPN use case
  - Multiple data interfaces with redundancy will be supported in the **future**



- Initial outside interface configuration through a CLI wizard
  - Can be used to repair connectivity after an inadvertent change
- Support a manual FTD configuration rollback to last working state

Low-Touch Provisioning

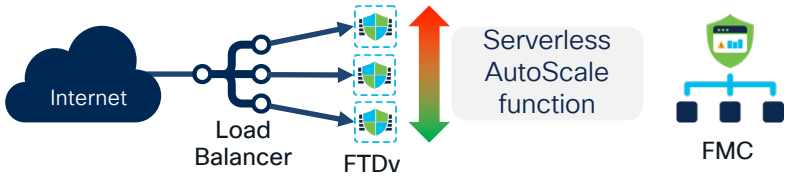
- Management flexibility for Enterprise and In-Band use cases



- Firepower 1000/2100 CDO on-boarding by serial number in 6.7
- Day 0 configuration files and automation templates for FTDv

Virtual Functions

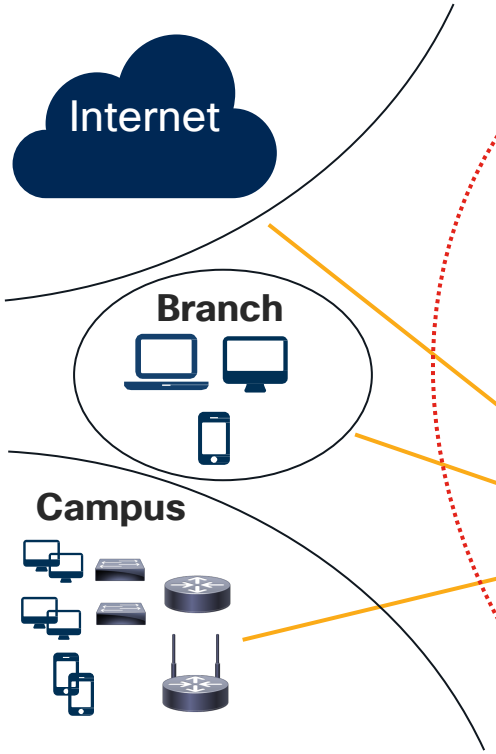
- Broad private and public cloud support for FTDv and ASAv
  - Now: aws Azure Google Cloud Platform KVM ORACLE CLOUD INFRASTRUCTURE vmware
  - FTDv 7.0: openstack.
- Fully automated stateless AutoScale in AWS and Azure



- Container-based ASAc with Kubernetes orchestration in 9.16

docker kubernetes

End-to-End Threat Protection in Modern DC



Hybrid Data Center

North-South Security

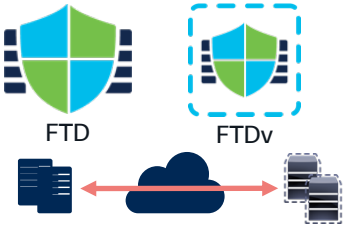
- NGFW/NGIPS at DC Edge
- See into Campus, Branch, Internet
- Attribute Based Policies

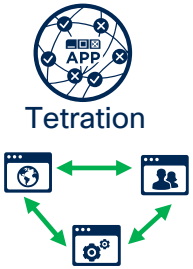
East-West Security

- Segment DC networks
- NGFW as gateway to servers and VMs
- Single- or multi-site, public cloud

Workload Security

- Fine-grained inter-application controls
- No clearly defined network boundary
- Rapid automation

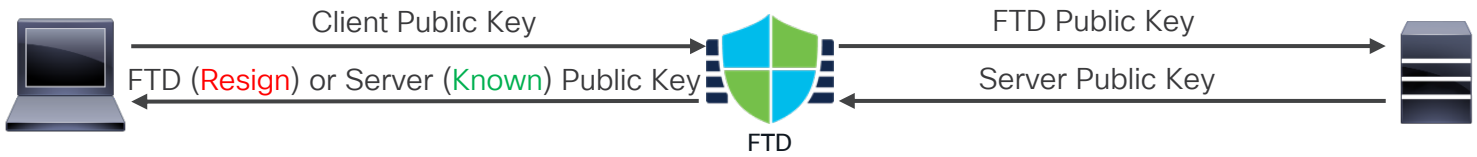




Inspect

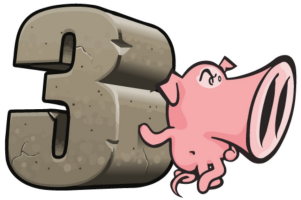
TLS Decryption

- TLS Decryption is mandatory for IPS, AMP, and other DPI functions

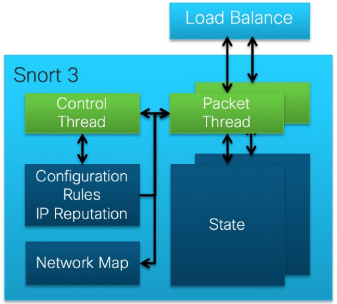


  - Resign: outbound, broken by public key pinning or native client apps
  - Known Key: inbound to controlled apps, broken by client cert auth
- TLS 1.3 allows decryption directly, or by downgrade to TLS 1.2
  - Per-session keys (DH) break passive IDS decryption with either version

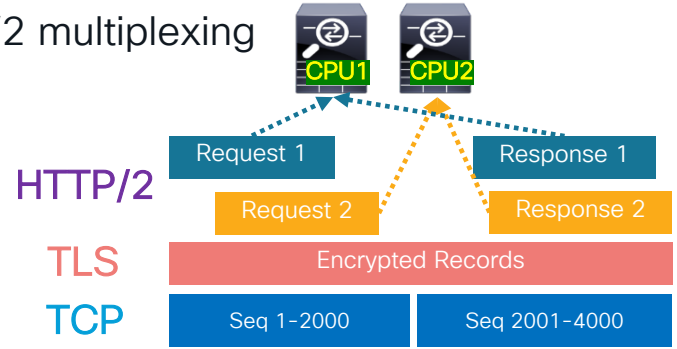
Snort 3 NGIPS Engine



- FDM/CDO availability in FTD 6.7; FMC in FTD 7.0
  - Much more efficient memory utilization from multi-threaded architecture
  - Faster/deeper pattern lookups with HyperScan for higher efficacy
  - Event-driven plugins replace preprocessors for quicker verdicts
  - Improved human-readable signature language



- Single-flow TCP/UDP throughput is still tied to a single CPU core performance
  - Future opportunity for parallel processing with HTTP/2 multiplexing



Future Look: Web Application Protection

SQL_Database_Servers

Protection for app servers that use SQL

Save | Cancel

Threat Signatures | HTTP Constraints | HTTP Header Editing | Advanced HTTP Rules

Add Constraint

Enable	Rule			
ON	Block	Header Length	Greater Than	8,192
OFF	Block	Header Line Length	Greater Than	1,034
ON	Block	Number of header Lines	Greater Than	32
OFF	Block	Total URL Length	Greater Than	8,192
OFF	Block	URL Parameters Length	Greater Than	8,192
OFF	Block	Number of URL Parameters	Greater Than	16
OFF	Block	Number of Cookies	Greater Than	16
OFF	Block	Number of Ranges	Greater Than	5
ON	Block	Malformed Request	Identified	
ON	Block	Illegal Host Name	Identified	

Impose general HTTP session constraints at individual Main Access Control Policy rule level.

Threat Signatures | HTTP Constraints | HTTP Header Editing | Advanced HTTP Rules

Add Rule

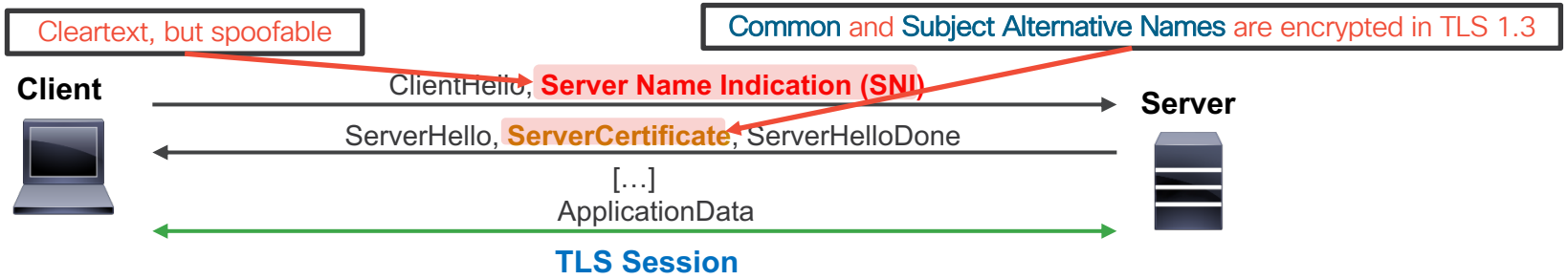
Enable	Rule		
ON	Remove	X-Forwarded-For	
OFF	Remove	X-Powered-By	
ON	Add	X-Custom-App1	
OFF	Replace	Server	X-Custom-App2

Perform granular HTTP header manipulation.

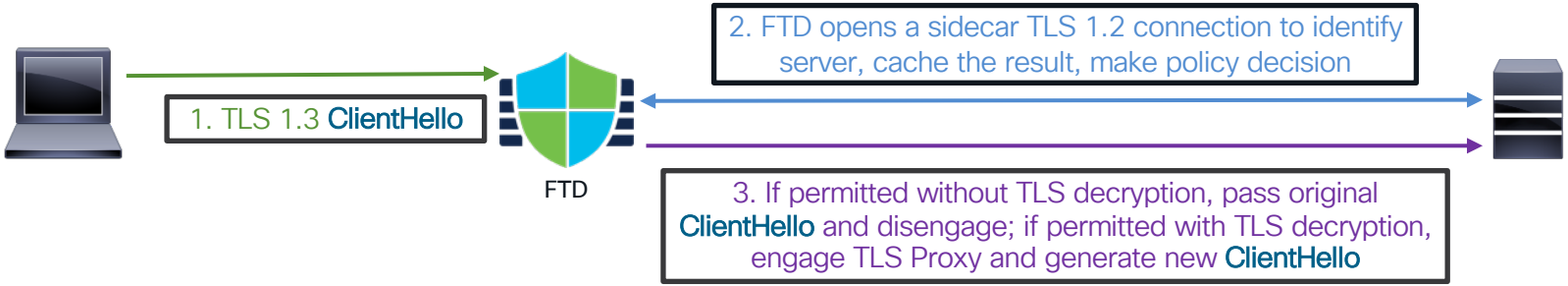
Infer

TLS Application and URL Visibility

- AVC, URL, and “SSL” Policy decisions on pre-1.3 TLS header



- TLS Server Identity Discovery without decryption in FTD 6.7



Future Look: App Fingerprinting

https://github.com/cisco/mercury

TLS ClientHello

```
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)
    Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
    Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
    Cipher Suite: TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)
```

Confidence: 99.94%
Process: firefox.exe
Version: 76.0.1
Category: browser
OS: Windows 10 19041.329
Typical FQDN: cisco.com

Firefox

TCP/TLS 192.168.2.110/34624->172.16.45.200/443

TCP/TLS 192.168.2.110/21013->203.0.113.154/443

FTD

Generate unique fingerprints for client applications based on TLS, TCP, HTTP, and DHCP fields and use for policy matching and context enrichment.

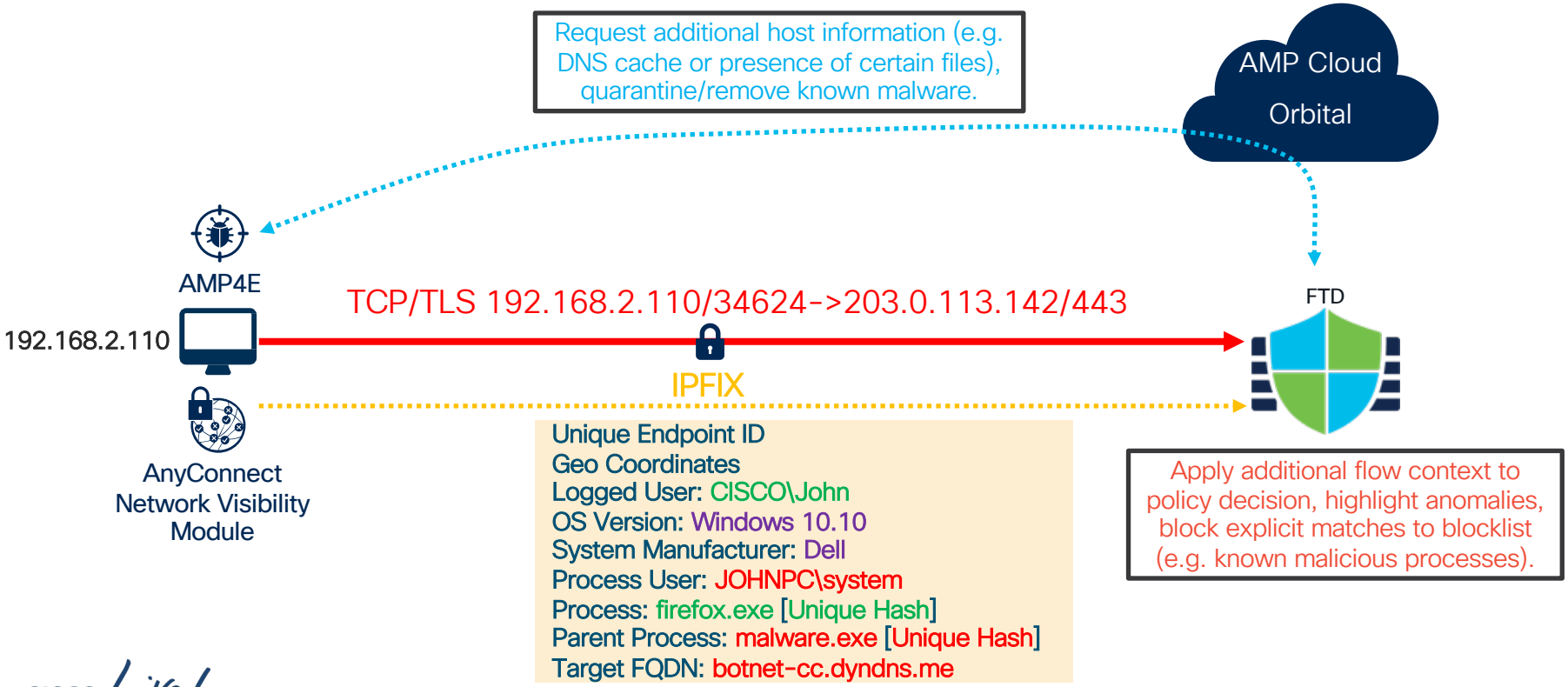
Tor

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)
    Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d)
    Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c)
    Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
    Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
    Cipher Suite: TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)
```

Confidence: 100%
Process: tor.exe
Version: 9.0.2
Category: anonymizer
OS: Windows 10 19041.329
Typical FQDN: nsksdlkoup.me

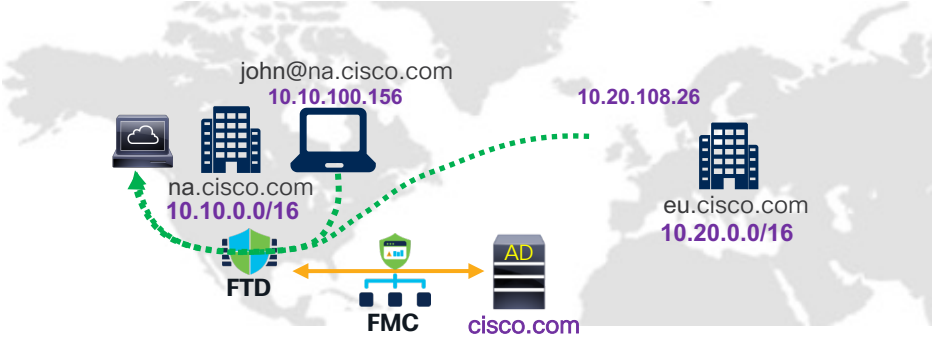
Future Look: Flow Context via Client Endpoint



Abstract

User Identity Policies in FMC 6.7

- AD user identity across multiple Forest domains in a single IP space



  - Support groups with users across multiple Forest member domains in FMC 7.0
- Higher FMC device scale per ISE/ISE-PIC instance with pxGrid 2.0

Attribute-Based Policies in FTD 7.0+

Custom Orchestrator

7.0 vmware 7.0 aws 7.0 Azure Future Tetration Future kubernetes Future APIC

Push Model: FMC REST API for populating/updating attribute mappings asynchronously.

Pull Model: Orchestrator-specific translation modules for subscribing to synchronous updates (Cisco Secure Dynamic Attributes Connector).

#	Name	Source Attribute	Dest Attribute	Action
Mandatory - Main ACP (1-2)				
1	Permit App Comm	webapp.cisco.com	DB_App	Allow
2	Permit Web App	MS_Windows	webapp.cisco.com	Allow

FMC

Attribute Type	Label	IP Address	Protocol	Port
FQDN	webapp.cisco.com	192.168.1.151	All	All
Host OS	MS Windows	192.168.1.120-130	All	All
Workload Name	DB App	172.16.45.90	TCP	13758

FTD FTD FTD

Real-time mapping updates without a full configuration deployment.

FTD 7.0: Dynamic Attributes Connector UI

Cisco Secure Dynamic Attributes Connector

Connectors | Adapters | Dynamic Attributes Filters

Add Dynamic Attribute Filter / Classifiers

Name*: vCenter.os

Connector*: vCenter

Query*

Type		Op.	Value
all	os	=	any Ubuntu Linux (64-bit)
			CentOS 4/5 or later (64-bit)
			FreeBSD Pre-11 versions (64-bit)
	network	=	any u90c04p11-1511

Cancel | Save

Learn and reference environment-specific attributes freely across the policy.

Cisco Secure Dynamic Attributes Connector

Connectors | Adapters | Dynamic Attributes Filters

Dynamic Attributes Filters

3 dynamic attributes filters

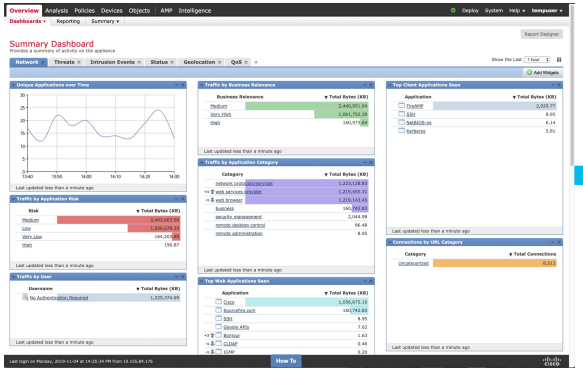
#	Name	Connector	Query	Actions
1	Azure App	Azure	(**Finance** = 'App') **AND** (**HR** = 'App')	
2	vCenter.os	vCenter	(**os** = 'Ubuntu Linux (64-bit)' **OR os** = 'CentOS 4/5 or later (64-bit)' **OR os** = 'FreeBSD Pre-11 versions (64-bit)') **AND** (**network** = 'u90c04p11-1511')	
3	AWS App	AWS	(**Sports** = 'App') **OR** (**News** = 'App')	

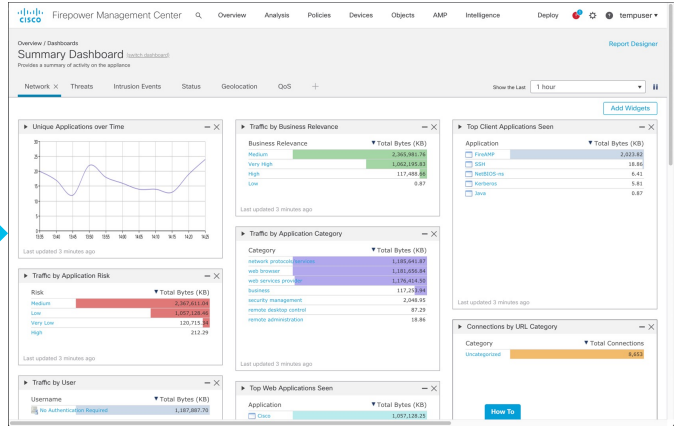
Narrow down tracked workload sets to reduce noise.

Manage

Reinforcing the Foundation

- New FMC user interface in 6.5





- Dramatically faster (10x+) event lookup starting in FMC 6.5 monetdb
- Each new release consistently drops deployment times by 10-20%
- Software optimizations for 25% higher throughput in FTD 7.0

Multi-Column Policy Filtering in FMC 6.6

Rules | Security Intelligence | HTTP Responses | Logging | Advanced | Prefilter Policy: Default Prefilter Policy | SSL

Filter by Device | source_networks:("192.168.1.0/24" "192.168.101.0/28") applications:("DNS")

Reusable query language.

ow Rule Conflicts

	Name	Dest SGT
▼ Mandatory - ac1 (1-2)		
1	Allow Standard DNS	Any
2	Outbound Business Apps	Any
▼ Default - ac1 (-)		
There are no rules in this sectio		
Default Action		work Discovery

Name:	
Source Zones:	
Dest Zones:	
Source Networks:	192.168.1.0/24, 192.168.101.0/28
Dest Networks:	
VLAN Tags:	
Users:	
Applications:	DNS
Source Ports:	
Dest Ports:	
URLs:	
Source SGT:	
Dest SGT:	
Action:	

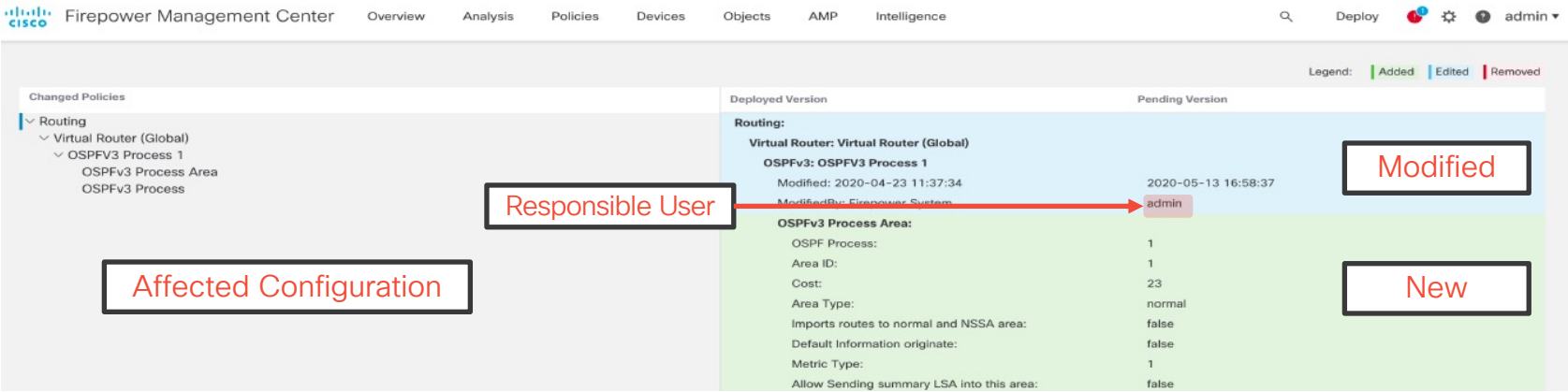
Clear | Search

OR matching within a single field.

AND matching across multiple fields.

Change Management

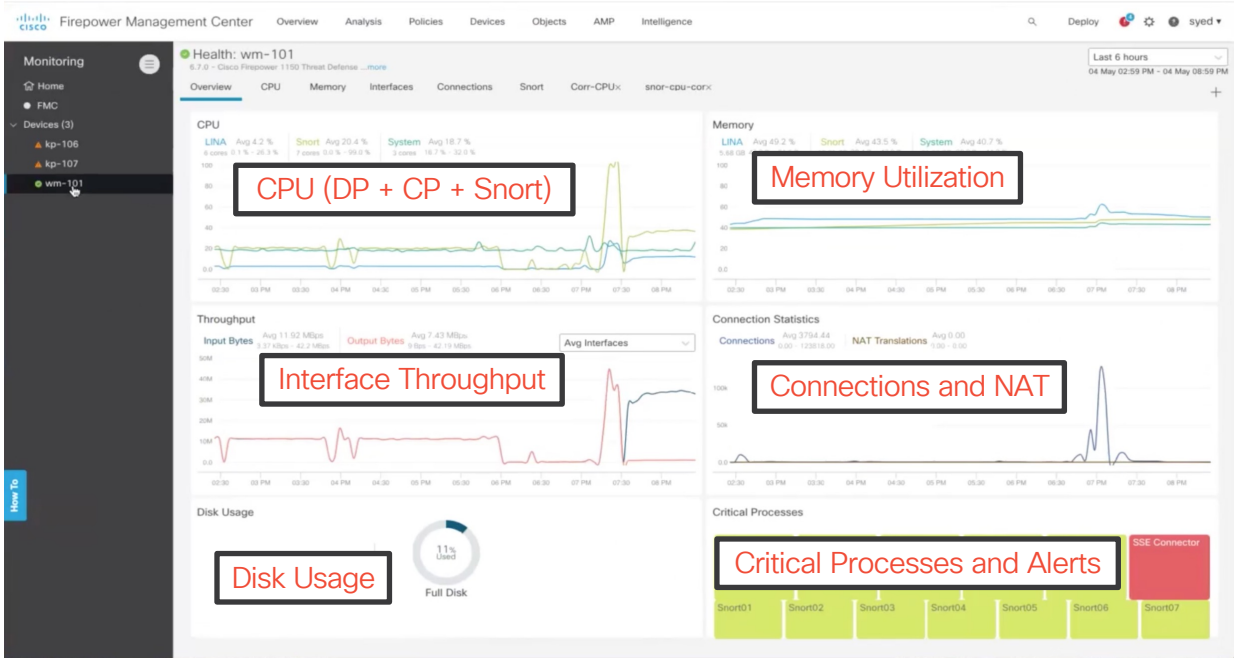
- Selective deployment, and detailed audit transcripts in FMC 6.7
  - Filtering individual changes by user in FMC 7.0



- Emergency rollback within last 10 configuration versions in FMC 7.0

Health and Event Monitoring

- New FTD monitoring dashboard and unified SNMP agent in 6.7



- FMC health dashboard, and real-time Event Viewer in 7.0

Thank you

Other Relevant Sessions

- BRKSEC-1022 *Health Monitoring in Next Generation Firewall*
- BRKSEC-2014 *Deploy Network Security as Code Using DevOps*
- BRKSEC-2029 *Security in an Encrypted World: Enhancing Firewalls, IPS, and Proxies*
- BRKSEC-2411 *Zero Trust: Securing Applications and Workloads Using a Cloud Native Approach*
- BRKSEC-2412 *Leveraging Endpoint Security in Our Encrypted World!*
- BRKSEC-2415 *The Future of Network Security is in the Cloud with Cisco SASE!*
- BRKSEC-3008 *Demystify Public Cloud Security Using Secure Firewall and Tetration*


TURN
IT
UP
cisco Live!
#CiscoLive