

CISCO *Live!*

ALL IN

#CiscoLive



The bridge to possible

Keeping Up on Network Security with Cisco Secure Firewall

Subtitle goes here

Andrew Ossipov
Distinguished Engineer, CTO
BRKSEC-2236

CISCO *Live!*

#CiscoLive

Cisco Webex App

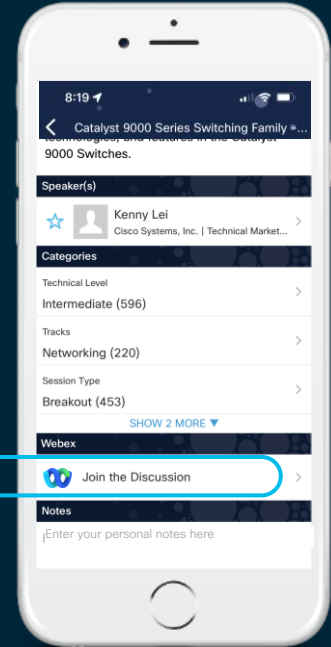
Questions?

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 June 17, 2022.



<https://cicolive.ciscoevents.com/cicolivebot/#BRKSEC-2236>

Your Speaker

Andrew Ossipov

aeo@cisco.com

Distinguished Engineer

Product CTO for Network, Workload, and Cloud Security

Firewall Architecture, Hybrid Cloud, Unified Policy, SASE

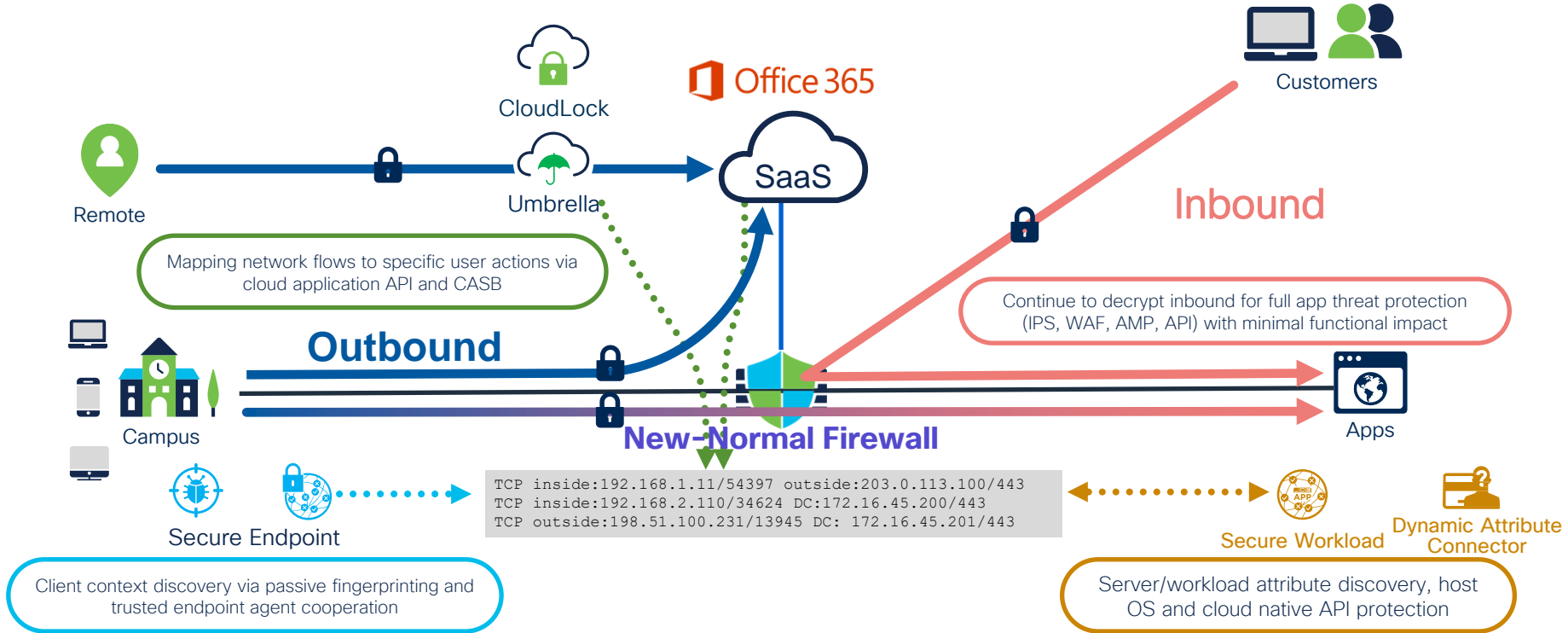




Agenda

- Introduction
- Secure Firewall 3100
- Threat Prevention
- Connectivity
- Private and Public Cloud
- Management
- Conclusion

Firewall: From DPI to Inference and Cooperation



Secure Firewall 3100



Secure Firewall 3100 Overview

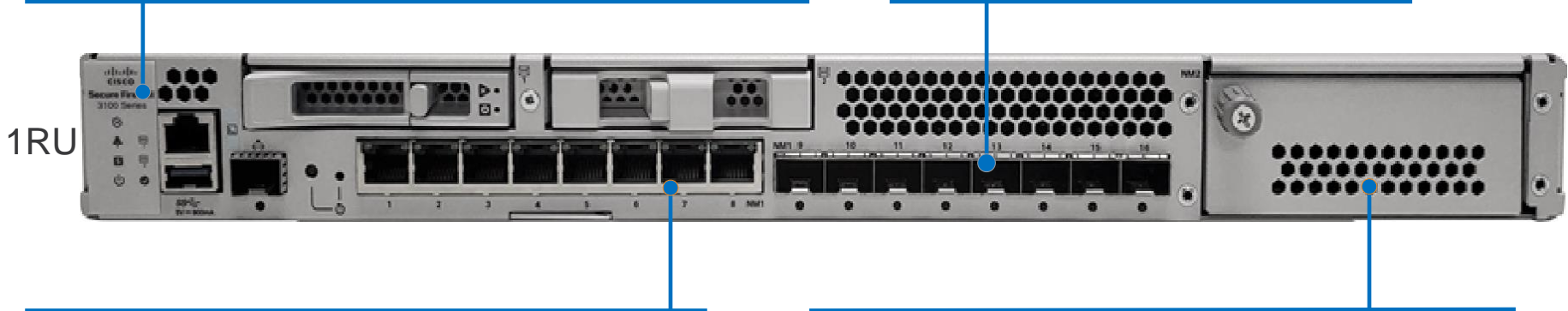


Appliance-Mode Security Platform for FTD or ASA Application

- Fixed configurations: 3110, 3120, 3130, 3140
- Lightweight virtual Supervisor module w/Multi-Instance
- Integrated Datapath FPGA w/Flow Offload and Crypto Engine
- Rear dual redundant power supplies and fan trays

SFP Data Interfaces

- 8x1/10GE on Firepower 3110-3120
- 8x1/10/25GE on Firepower 3130-3140



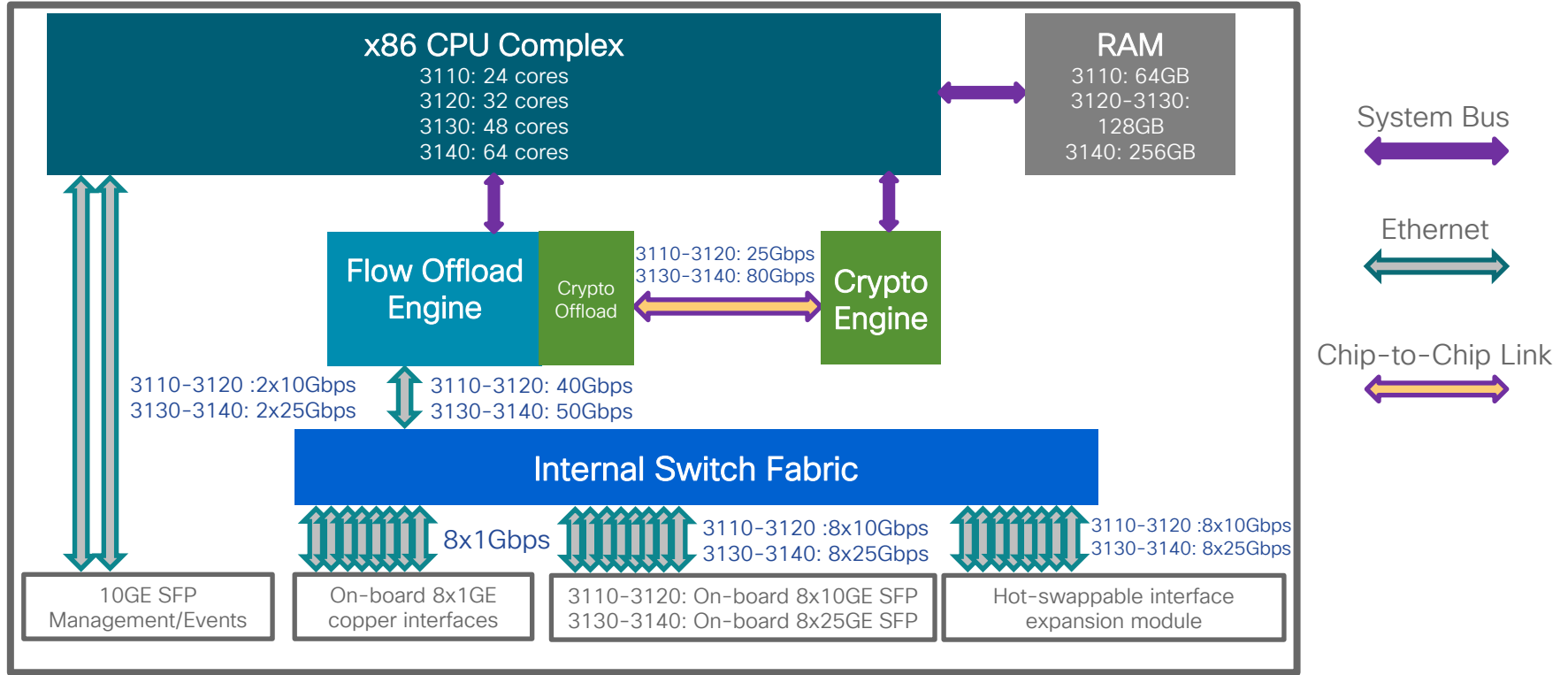
Copper Data Interfaces

- 8x10M/100M/1GE Ethernet

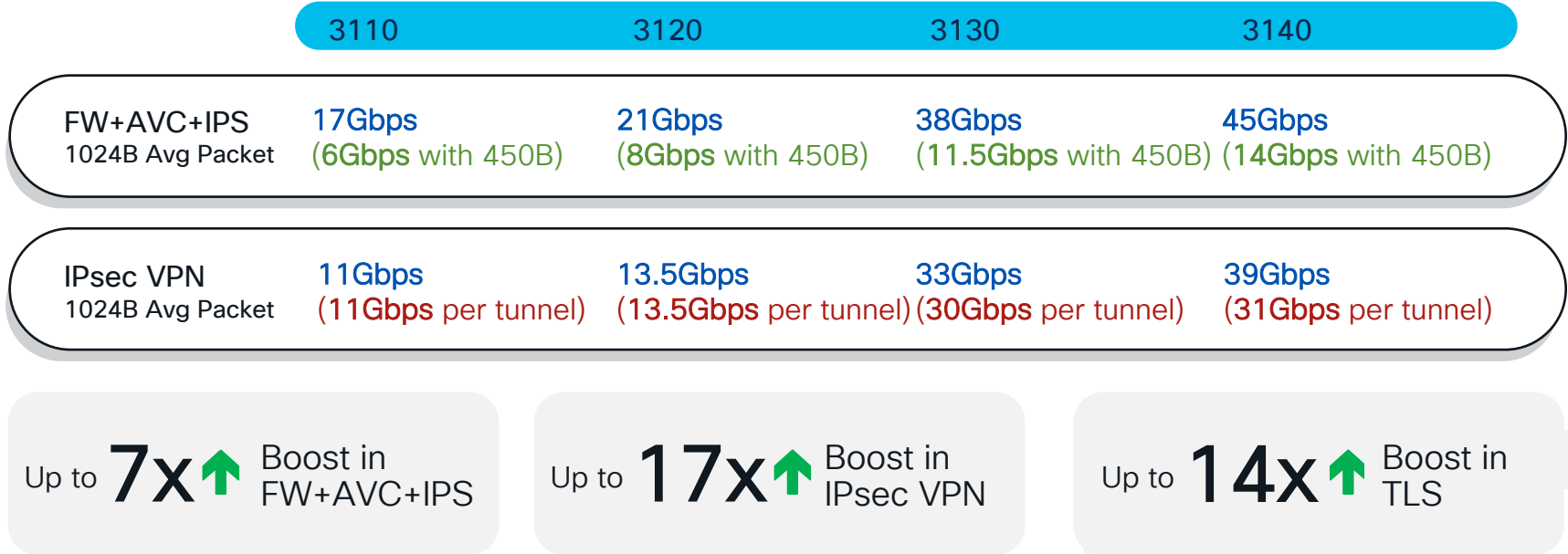
Network Module

- 8x1/10/25GE or 6x10/25GE FTW on Firepower 3110-3120
- 4x40GE or 2x40GE FTW on Firepower 3130-3140

Secure Firewall 3100 Architecture



Secure Firewall 3100 Performance



*Performance Estimates are subject to change in public release.

Threat Protection



Encrypted Visibility Engine (EVE)

TLS ClientHello

```

    Ciphers 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 (0xc03a)
    Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xc038)
    Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc030)
    Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc034)
    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.

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



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



Firewall

TLS ClientHello

```

    Ciphers Suites (19 suites)
    Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc03e)
    Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
    Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc034)
    Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
    Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc03d)
    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)
  
```

<https://github.com/cisco/mercury>

EVE-enriched Unified Events



Client process name and detection confidence score; the name can be linked to a custom AppID for enforcement in FTD 7.2.

Firewall Management Center
Analysis / Unified Events

Overview Analysis Policies Devices Objects Integration

Deploy 🔍 ⚙️ alexst | cisco SECURI

Showing 23 events (📄 19 🍀 4) ↓

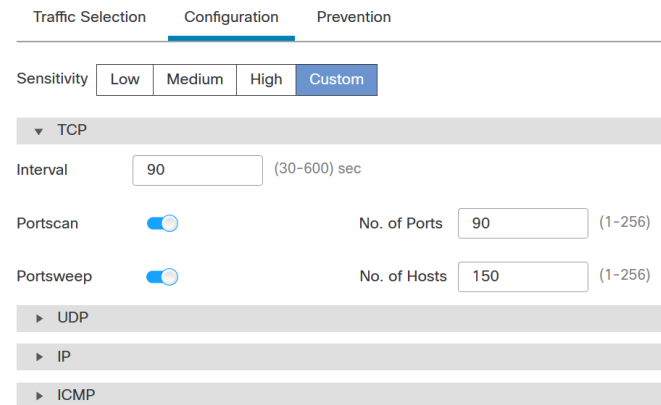
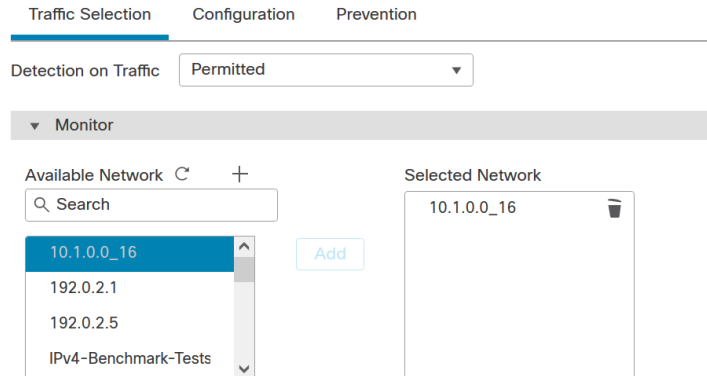
2022-04-06 09:45:32 MDT → 2022-04-06 09:46:30 MDT 58s ● Live

Time	URL	Source Port / ICMP Type	Destination Port / ICMP Code	Ingress Security Zone	Client Application	Encrypted Visibility Process Confidence Score	Encrypted Visibility Process Name	Encrypted Visibility Threat Confidence	Encrypted Visibility Threat Confidence Score
2022-04-06 09:45:59	https://www.carfax.com	56902 / tcp	443 (https) / tcp	Passive	Wget	100%	wget	Very Low	0%
2022-04-06 09:45:59		123 (ntp) / udp	123 (ntp) / udp	Inside-400	NTP client	0%			0%
2022-04-06 09:45:58	https://carfax.com	53856 / tcp	443 (https) / tcp	Passive	Wget	100%	wget	Very Low	0%
2022-04-06 09:45:56	https://www.farmersonly.com	35714 / tcp	443 (https) / tcp	Passive	Wget	100%	wget	Very Low	0%
2022-04-06 09:45:56	https://farmersonly.com	36158 / tcp	443 (https) / tcp	Passive	Wget	100%	wget	Very Low	0%
2022-04-06 09:45:56		123 (ntp) / udp	123 (ntp) / udp	Inside-400	NTP client	0%			0%
2022-04-06 09:45:54	https://google.com	54040 / tcp	443 (https) / tcp	Passive	Wget	100%	wget	Very Low	0%
2022-04-06 09:45:54	http://google.com/SID~28796/cnt.php?id=2	59272 / tcp	80 (http) / tcp	Passive	Wget	0%			0%
2022-04-06 09:45:54		59272 / tcp	80 (http) / tcp	Passive					
2022-04-06 09:45:50	https://www.google.com	49394 / tcp	443 (https) / tcp	Passive	Wget	100%	wget	Very Low	0%
2022-04-06 09:45:50	https://google.com	54034 / tcp	443 (https) / tcp	Passive	Wget	100%	wget	Very Low	0%
2022-04-06 09:45:48	https://endpoints.office.com	55002 / tcp	443 (https) / tcp	Passive	Python urllib	100%	python	Very Low	0%
2022-04-06 09:45:47	https://www.facebook.com	39642 / tcp	443 (https) / tcp	Passive	Wget	100%	wget	Very Low	0%
2022-04-06 09:45:47	https://pastebin.com	49160 / tcp	443 (https) / tcp	Passive	SSL client	90%	_malware	Very High	90%
2022-04-06 09:45:40		3 (Destination Unr)	3 (Port unreacha)	Passive	ICMP client	0%			0%

Inference-based threat alert and confidence level.

Portscan Detection and Prevention

- Evolved Portscan protection engine directly within the data plane
 - Much higher performance and detection efficacy
 - Recognizes single-host, decoy-based, distributed, and port sweep scanning types
 - Optional time-based blocking of potential attackers
- Granular configuration profiles at Access Control Policy level



Connectivity



Application-Aware Policy Routing

- Native support for Policy Based Routing configuration in FMC
 - Commonly used SaaS applications can be used as matching criteria
 - Automatically expanded by data plane into IP-based Network Service Groups
 - Monitors DNS traffic to Trusted Servers to support domain pattern matching
- Useful for Direct Internet Access (DIA) provisioning in SD-WAN deployments

Policy Based Routing

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

Configure Interface Priority

Add

Ingress Interfaces	Match criteria and forward action	
inside	<p>If traffic matches the Access List WebEx_Direct_Internet_Access</p>	<p>Send and load balance it through</p> <ul style="list-style-type: none"> #0 ISP1 #0 ISP2 <p>If above link fails, Send through</p> <ul style="list-style-type: none"> #1 ISP-Backup

SaaS application aware first packet match.

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

Elephant Flow Detection

- Per-flow bandwidth and load tracking replaces Intelligent

Elephant Flow ?

i For Snort 3 FTD devices 7.2.0 onwards, use this window to configure elephant flow.
 For all Snort 2 FTD devices or Snort 3 FTD devices 7.1 and earlier, use the IAB settings.

Elephant Flow

Generate elephant flow events when flow bytes exceeds MB and flow duration exceeds Seconds

Throughput threshold to qualify as an Elephant Flow

Elephant flow detection based on per flow CPU utilization

CPU hogging elephant flow is: When flow CPU utilization exceeds % in fixed time windows of Seconds

Optional flow-specific CPU resource consumption for the qualification.

Action i

Bypass the flow

Throttle the flow

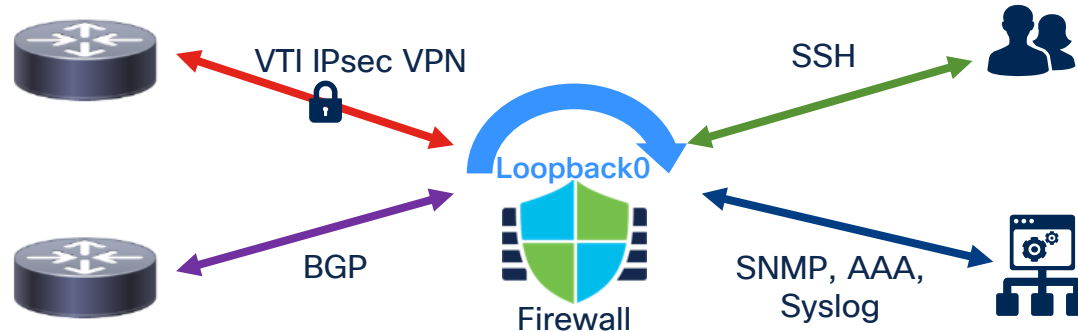
When Snort receives queue drops exceeds %

Optional flow actions based on configurable packet drop thresholds.

Loopback Interface



- Abstract to- and from-device connectivity from physical interfaces
 - IPv4 and IPv6 addressing in routed and transparent (except for VTI) modes
 - HA/failover and clustering (except for VTI) support

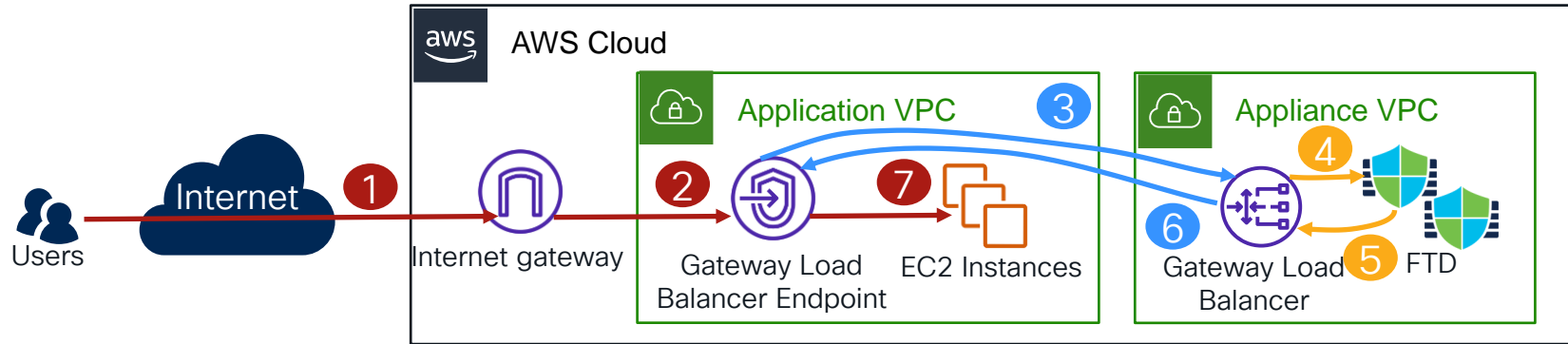


Private and Public Cloud

AWS Gateway Load-Balancer Integration



- Network firewall service insertion for both inbound and outbound flows
 - Redirection with GENEVE
 - Bring-your-own TLS decryption with available software capabilities

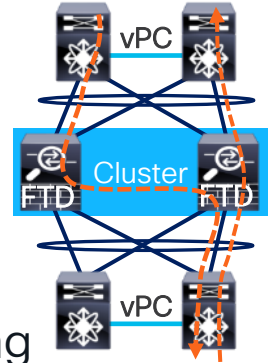


- **FTD 7.2** and **ASA 9.18** add Autoscale support and snapshot-based image bring-up

Clustering for Virtual Firewalls



- Clustering combines multiple firewalls into one logical device
 - Seamless scalability up to 16 FTD units with no traffic disruption
 - Stateful handling of asymmetric traffic and failure recovery
 - Single point of management and unified reporting
- Better elasticity and failure handling in hybrid cloud with clustering



- Individual IP addresses on data interfaces instead of a single Port-channel
- VxLAN-based Cluster Control Link for unicast inter-member communication
- Flow re-hosting on failure in supported environments

Infrastructure as Code



- Management and provisioning of Secure Firewall assets in hybrid cloud
- Declarative Teraform templates for ASA and FTD (via FMC)
 -      
 - FTD Dynamic Object integration with HashiCorp Consul
- Imperative Ansible tasks for ASA and FTD (FDM and now FMC)
- Continuously updated Cisco DevNet repositories
 - <https://developer.cisco.com/secure-firewall/cloud-resources/>
 - <https://github.com/CiscoDevNet/secure-firewall>
 - <https://github.com/CiscoDevNet/FMCAnsible>

Management





“Shallow” Access Policy Locking

Global_Policy

Enter Description

Try New UI Layout Show Warnings Analyze Hit Counts Save Cancel

Rules Security Intelligence HTTP Responses Logging **Advanced**

This Policy is locked by you.

Prefilter Policy: Default Prefilter Policy Inheritance Settings | Policy Assignments (1)
SSL Policy: None Identity Policy: None

- Policies
 - Access Control
 - Access Control Policy
 - Modify Access Control Policy
 - Override Access Control Policy Lock

Global_Policy

This Policy is locked by Jonny. You cannot edit this policy.

Show Warnings Analyze Hit Counts Save Back

Rules Security Intelligence HTTP Responses Logging **Advanced**

Prefilter Policy: Default Prefilter Policy Inheritance Settings | Policy Assignments (1)
SSL Policy: None Identity Policy: None

- Policies
 - Access Control
 - Access Control Policy
 - Modify Access Control Policy
 - Override Access Control Policy Lock

Global_Policy

This Policy is locked by andrew. You cannot edit this policy.

Show Warnings Analyze Hit Counts Save Back

Rules Security Intelligence HTTP Responses Logging **Advanced**

Prefilter Policy: Default Prefilter Policy Inheritance Settings | Policy Assignments (1)
SSL Policy: None Identity Policy: None

Simplified Access Control Policy View



Global_Policy
Enter Description

Try New UI Layout Show Warnings Analyze Hit Counts Save Cancel

Rules Security Intelligence HTTP Responses Logging **Advanced** Prefilter Policy: Default Prefilter Policy Inheritance Settings | Policy Assignments (1) SSL Policy: None Identity Policy: None

Filter by Device Search Rules Show Rule Conflicts + Add Category + Add Rule

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicati...	Source Ports	Dest Ports	URL	Source Dynamic Attributes	Destinati... Dynamic Attributes	Action	Icons
Mandatory - Global_Policy (1-7)															
1	Block Non-Business Apps	inside	outside	Campus	Any	Any	Any	Risks: High, \	Any	Any	Any	Any	Any	Block	Icons
2	Block_Unauthorized_Wr	inside	outside	Campus	Any	Any	Any	Any	Any	Any	Adult Child Abuse Content Extreme Gambling Hate Speech	Any	Any	Interacti	Icons
3	Campus_File_Inspection	inside	outside	Campus	Any	Any	Any	HTTP HTTPS	Any	Any	Any	Any	Any	Allow	Icons

Global_Policy Packets → Prefilter Rules → SSL → Security Intelligence → Identity → Access Control More Targeted: 1 device

Flow Total 7 rules Add Category Add Rule

Name	Action	Source	Destinations and Applications
Mandatory (1 - 7)			
1 Block Non-Business Apps	Block	NET Campus	ZONE inside ZONE outside APP Risks: High Risks: Very High
2 Block_Unauthorized_Web	Interactive ...	NET Campus	ZONE inside ZONE outside URL Adult Child Abuse Content Extreme Gambling Hate Speech
3 Campus_File_Inspection	Allow	NET Campus	ZONE inside ZONE outside APP HTTP HTTPS
4 Allow_Outbound	Allow	NET Campus	ZONE inside ZONE outside
5 Inbound_Mail	Allow	ZONE outside	NET Mail_Servers ZONE inside APP SMTP SMTPS

Simplified Rule Editor



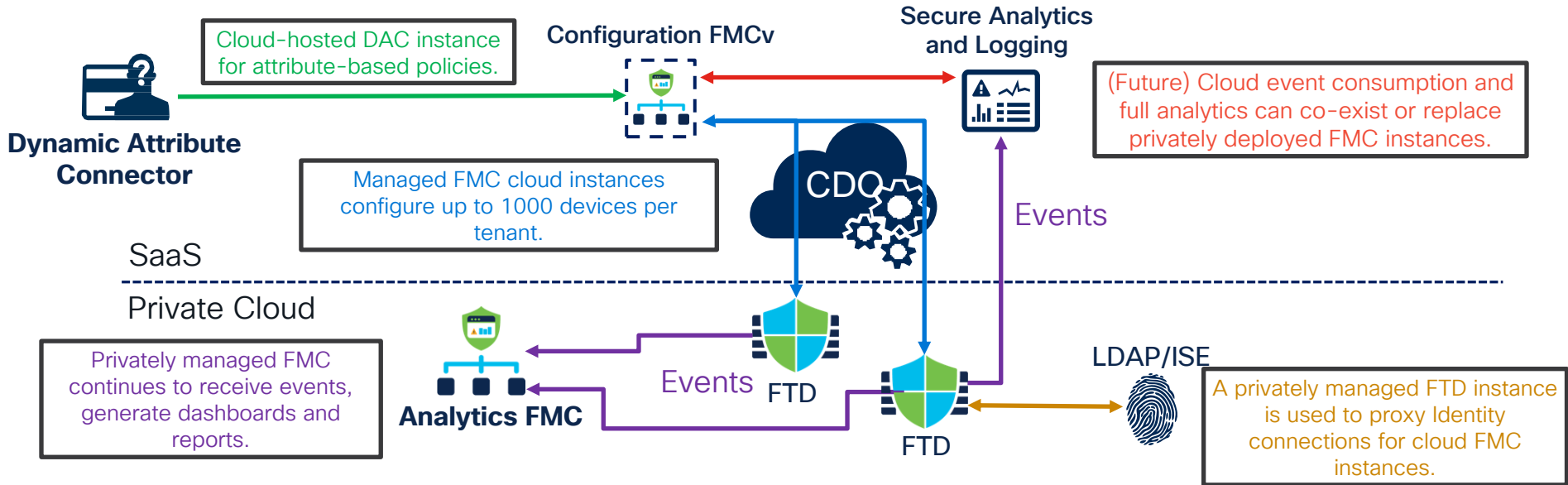
Inline rule navigation.

Direct access to all advanced actions.

Wizard-style object definition for all parameters.

Cloud-Delivered Firewall Management

- Embed fully-featured FMC experience within Cisco Defense Orchestrator
- Completely managed backend from platform upgrades to configuration backup



Cloud Analytics Dashboard



Cisco Defense Orchestrator

FTD Analytics Dashboard

Search, Notifications, Alerts, Help icons

- Hide Menu
- Inventory
- Configuration
- Policies
- Objects
- VPN
- Templates ASA
- FTD Services
- Events & Monitoring
- Monitoring**
- Change Log
- Jobs
- Admin

Overview **Threats** Network Applications and Users Status

Last 1 year | Select devices... | Refresh | Filter

Top Triggered Intrusion Rules

Rule Message	Events
Alert tcp rule (2000:1000000:1)	120,824
Alert ip rule (2000:1000003:1)	120,822
Alert udp rule (2000:1000001:1)	120,820
Alert icmp rule (2000:1000002:1)	120,820
FILE-EXECUTABLE Portable Executa...	39
OS-WINDOWS Microsoft Windows ...	28
FILE-MULTIMEDIA RealNetworks Re...	28
FILE-IDENTIFY Microsoft Windows ...	26

Top Intrusion Attackers

Initiator IP	Events
::192.168.104.245	405
::1.2.60.61	272
::1.2.19.52	268
::1.1.95.35	256
::1.2.61.191	256
::1.1.53.59	256
::1.2.67.78	256
::1.1.75.231	248

Top Intrusion Targets

Responder IP	Events
::192.168.105.1	405
::1.3.42.61	192
::1.4.88.105	184
::1.3.15.231	184
::1.4.28.84	176
::1.4.39.40	172
::1.4.24.239	172
::1.4.2.137	172

Top Intrusion Attackers



Top Malware Signatures

Threat Name	Events
Xls.Exploit.Swfdrop::95.sbx.tg	68
Doc.Exploit.Mspoint::95.sbx.tg	19

Top Malware Senders

Sending IP	Events
::192.168.104.245	77
::	4



Simple Migration of FTD to Cloud Management



- On-board privately managed FMC instances to CDO for fleet migrations

Defense Orchestrator Inventory / Change FTD Manager

Change FTD Management

Change FTD Manager from Firewall Management Center to CDO

1 Select FMC **FMC: 1771Fmc** **Per-device co-management dispositions.**

2 Select Devices

Select FTD devices to change management from FMC to CDO and specify an action in bulk or per device.

6 device(s) selected Multi-Device Action **Multiple Actions Selected**

<input checked="" type="checkbox"/>	Name	IP Address	Domain	Action
<input checked="" type="checkbox"/>	1771Fmc_10...	10.10.16.94:44	Global	Delete FTD from FMC
<input checked="" type="checkbox"/>	1771Fmc_10...	10.10.16.87:44	Global	Delete FTD from FMC
<input checked="" type="checkbox"/>	1771Fmc_10...	10.10.16.86:44	Global	Retain on FMC for Analytics
<input checked="" type="checkbox"/>	1771Fmc_10...	10.10.16.70:44	Global	Retain on FMC for Analytics

Change FTD Management

After completing the change FTD manager process, you have up to 14 days to commit to CDO as your FTD manager or revert to FMC as your FTD manager. After 14 days have passed, the actions you selected during this process will be automatically applied to your devices without further action from you. [Learn more.](#)

Warning: Deleting an FTD from FMC is final.

Migrations are reversible for 14 days.

Cisco Security Beta Programs



Sign-Up Now:

<http://cs.co/clive-security-beta>

"I've been involved in many beta programs...I must say that this one has been the best organized. This beta takes a very active, hands-on approach."

Higher-Ed Beta Customer



Early Feedback Programs



Beta Software Access



Product Training



Influence Product Roadmap



Presented by Security Customer Insights

Technical Session Surveys

- Attendees who fill out a minimum of four session surveys and the overall event survey will get Cisco Live branded socks!
- Attendees will also earn 100 points in the Cisco Live Game for every survey completed.
- These points help you get on the leaderboard and increase your chances of winning daily and grand prizes.



Cisco Learning and Certifications

From technology training and team development to Cisco certifications and learning plans, let us help you empower your business and career. www.cisco.com/go/certs

Pay for Learning with
Cisco Learning Credits

(CLCs) are prepaid training
vouchers redeemed directly
with Cisco.



Learn



Cisco U.

IT learning hub that guides teams and learners toward their goals

Cisco Digital Learning

Subscription-based product, technology, and certification training

Cisco Modeling Labs

Network simulation platform for design, testing, and troubleshooting

Cisco Learning Network

Resource community portal for certifications and learning



Train



Cisco Training Bootcamps

Intensive team & individual automation and technology training programs

Cisco Learning Partner Program

Authorized training partners supporting Cisco technology and career certifications

Cisco Instructor-led and Virtual Instructor-led training

Accelerated curriculum of product, technology, and certification courses



Certify



Cisco Certifications and Specialist Certifications

Award-winning certification program empowers students and IT Professionals to advance their technical careers

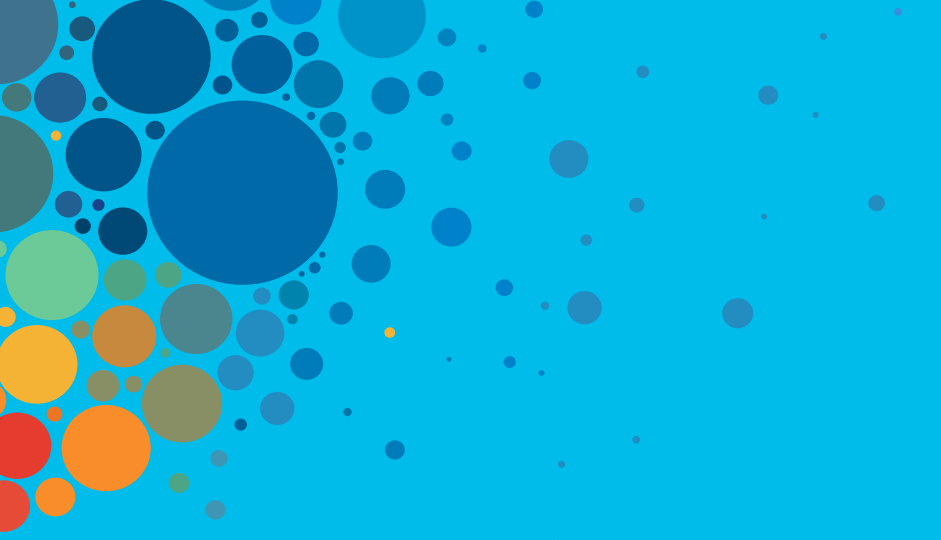
Cisco Guided Study Groups

180-day certification prep program with learning and support

Cisco Continuing Education Program

Recertification training options for Cisco certified individuals

Here at the event? Visit us at **The Learning and Certifications lounge at the World of Solutions**



Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer 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



The bridge to possible

Thank you

CISCO *Live!*

#CiscoLive

CISCO *Live!*

ALL IN

#CiscoLive