

CISCO *Live!*



#CiscoLive



The bridge to possible

Simplifying migrations to Cisco Secure Firewall

...with the Firewall Migration Tool 3.0

William Hansch
Sr. Product Manager, Cloud & Network Security

Ashish Sadhu
CX Product Manager, Cross Domain Automation

BRKSEC-1777

CISCO *Live!*

#CiscoLive



slido.com #FMT
Passcode:

bj1qdw

Cisco Webex App

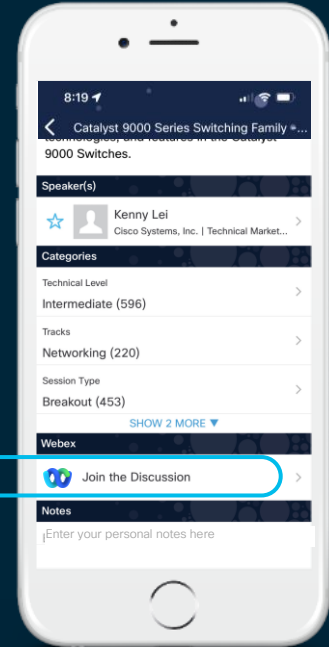
Questions?

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 speakers until June 17, 2022.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-1777>



Agenda

- Why migrate to Cisco Secure Firewall?
10,000ft overview of latest Threat Defense
- From where and what can be migrated?
FMT 3.0 overview on sources and capabilities
- What's planned going forward?
Roadmap of FMT and Threat Defense
- How to go about it?
Demo of migrations with FMT 3.0

Why Migrate to Cisco Secure Firewall?



Cisco Secure Firewall release 7.0 highlights

Scalable Eventing and Logging

Real time event viewer, scalable eventing and logging using on-prem SAL

Dynamic objects for quick changes

Attribute based policy feature adds dynamic network objects in AC policy in the first phase

Simplified Product Experience

Unified health metrics (via SNMP), health dashboard in FMC, Change management (rollback, change previews, improved audit logs), Converged Management Interface

Threat Efficacy Enhancement

Improved Threat Detection enabled via major architecture updates: Snort 3 in FMC

Public Cloud & Virtualization

Supports new platforms: Kubernetes, Openshift, Openstack
Additionally: new FTDv type: 16 core
Tiered Licensing (value proposition is much better)

Business Outcomes

Troubleshoot and track current and historical event data in common UI

Change dynamic objects in policies quickly without need for deploy configuration

Much better user experience, reduced operational complexity and cost

Customers get better detection with less resource consumption.

Hybrid cloud support ready for any customer environment

Many more improvements in...

- | | |
|--|--|
| <ul style="list-style-type: none">• Remote access and site-to-site VPN (DAP/Hostscan)• Secure-X Integration• FMC API for orchestration and migration | <ul style="list-style-type: none">• APIC FMC App Multi domain support• PAT operations in clustering• Multiple realm support for Identity |
|--|--|

Cisco Secure Firewall release 7.1 highlights



Snort 3 & Threat Features

- Elephant flow visibility
- Encrypted Visibility Engine
- Intrusion Rule Recommendations
- Additional rule actions



VPN

- Unique local tunnel ID for IKEv2
- Anyconnect native browser support
- RA VPN multiple trustpoint in SAML IDP
- Copy RA VPN access config on FMC
- Site to site VPN enhancements



Public Cloud

- Additional instance type support in AWS, Azure
- FMCv HA and FMCv300 in AWS and OCI
- Geneve AWS proxy support
- Automated FTDv horizontal scaling in OCI
- AWS CloudWatch health monitoring integration

Cisco Secure Firewall release 7.2 highlights



Snort 3 & Threat Features

- TLS 1.3 native support & inspection
- Encrypted Visibility Engine enhancements – Snort 3 / TLS/SSL policies
- Multiple SAL SaaS & on-prem destinations
- Improvements in file detections
- Access policy lock
- Persistent hit count



VPN

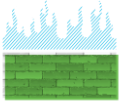
- Mutual LDAPS Authentication/client cert Auth
- Certificate and SAML for RAVPN Authentication
- SVTI & DVTI improvements, VTI in VRF support
- Umbrella DNS connector Support



Public Cloud

- ASAv and FTDv: support Azure stack hub, Alibaba, AWS security center integration (Guardduty)
- FTDv Cluster support for AWS, GCP, VMWare, KVM & Geneve auto scale
- FDM for GCP
- GCP ELB support

How to get to the latest Threat Defense



New Cisco Secure firewall purchases

- Select pre-installed software when ordering your new hardware



Software Upgrade

- Upgrade your install base with an improved upgrade experience, leverage [LevelUp](#)



Migration from ASA and 3rd party vendors

- Use the [firewall migration tool](#) to migrate from ASA, Check Point, Fortinet or Palo Alto Networks

From where and
what can be
migrated?



Firewall Migration Tool v3.0



Leverage your existing install base...

- ASA (incl FirePOWER Services)
- Check Point
- Palo Alto Networks
- Fortinet



... when migrating key capabilities and features...

- Objects and AC Policy
- NAT, Static routes, IPv6
- Physical interface, port channels
- RA VPN (incl. DAP) **[new]**, S2S VPN static crypto map & objects
- ACL Optimization **[new]** (Identify & remove shadow/redundant rules)



... to our Cisco Secure Firewall Threat Defense

- On-prem/virtual Firewall Management Center
- Cloud-delivered Firewall Management Center **[new]**

cisco.com/go/fmt



Result: Saving Customers and Partners Weeks of Effort

"I am happy on how effective migration has gone and how much less work I have to do. I am ecstatic because there is a lot less for me to do except for spot checking when I am done."

– Adventist Health

✓ Saved 144h when migrating two sites

"It went really smooth. I am happy to see migration tool is pretty easy to use. It saves a ton of time. Keep up the good work."

– Major Global Partner

40K+

Total Downloads

>98%

Device Migration
Success Rate

11K

Distinct Customers
and Partners

58

Net Promoter Score

What's planned
going forward?

Cisco Firewall Migration Tool Roadmap

FMT 3.0 (Summer 2022)

VPN support (from ASA only)

- RA VPN: DAP, Group policy, SSL for AnyConnect, Radius & LDAP authorization and authentication
- S2S VPN: Automating pre-shared key migration

Migrations to cloud-delivered FMC

- ASA
- Fortinet
- Check Point
- Palo Alto Networks

Threat Defense 7.2 validation

- EIGRP (planned for FMT 3.0.1)

FMT 4.0 (End of this Year)

FDM to (cloud-delivered) FMC [LA]

- Management migration from API/FDM to Firewall Management Center (for on-premise/virtual or cloud-delivered in CDO)
- Supporting migration of only management or change in management along with firewall hardware refresh
- Hosting of FMT inside CDO (stretch)

Threat Defense 7.3 unlock

- Routing enhancements: ECMP, PBR
- RA VPN: AnyConnect custom attributes & VPN load balancing

Cisco Firewall Migration Tool Backlog

Backlog (uncommitted, un-prioritized order)

Threat Defense 7.4 unlock & validation

Merging Configurations: Multi Context to VRF

- Routing separating migration (Multi Context to VRF, single instance)
- Merging policies (e.g. from multi context) to one instance

Enhanced Capabilities

- Configuration manipulation during migration (re-naming/adding objects/rules, etc.)

Additional Sources:

- FTD device migration from FMC to new Hardware

How to go
about it?

Demo

1. ACL Optimization & VPN Support
2. Migration to cloud-delivered FMC



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 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

CISCO *Live!*



Security Operations

SECURE X (XDR)

Managed Detection and Response Services

Security, Orchestration, Automation and Response

Incident Response and Remediation Services

Threat Visibility & Hunting

Device Insights

Kenna Vuln Mgmt

Secure Cloud Insights

3rd Party Integrations

User/Device Security

ZERO TRUST

Adaptive MFA | Passwordless | Trust

Duo Secure Access Secure E-mail

SASE/REMOTE WORKER

Unified Client | EDR | Cloud Managed



Cisco Secure Client

VPN
Posture
Telemetry
Threat
Query

ThousandEyes (Visibility)

Device Mgmt
Meraki SM
OS, App Control

Network Security

Cloud Edge

SECURE ACCESS SERVICE EDGE (SASE)

ZERO TRUST

PRIVATE CLOUD EDGE (MSP or CUSTOMER)

Threat Protection | Secure Access Control | Managed Remote Access

Reliable | Scalable | Flexible

Umbrella/Duo

ZTNA
 RaaS

DNS-layer security
 SSL decryption

Secure web gateway
 Remote browser isolation

L7 firewall + IPS
 Data loss prevention

Cloud access security broker/shadow IT
 Cloud malware detection

SDWAN

Cisco Meraki SDWAN

SDWAN by Viptela

Secure Firewall

ThousandEyes

Cloud DDoS, WAF

On-Premises

SASE/SDWAN

Scalable | Flexible | Visibility | Comprehensive Security

Network Edge

Cisco Meraki SDWAN

SDWAN by Viptela

Secure Firewall

ThousandEyes

IoT/OT SECURITY

Secure Critical Infrastructure | Unified IT and OT

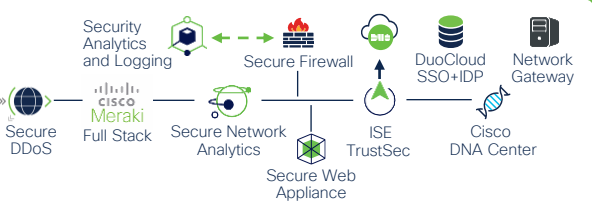
Industrial Router

Industrial Firewall

Industrial Switch/AP

Cyber Vision

ISE TrustSec



Application Security

ZERO TRUST

Policy | API Security
Application Segmentation
Run-time Application Security

Application Security Stack

Cloud Native Security
 APIC
 Secure Workload
 Secure Application by AppDynamics

App Observability | Detection | Response

Hybrid Private
 Public Cloud
 Secure Cloud Analytics
 Secure Firewall
 ThousandEyes
 Secure DDoS, WAF/Bot

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

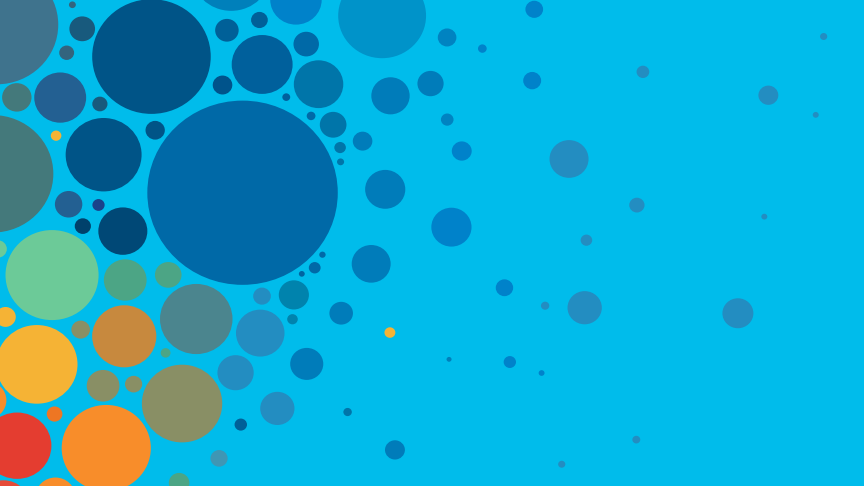
Cisco Guided Study Groups

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