



Cisco Secure Firewall

Nový Firepower 3100 je tady!

Jiří Tesař

jitesar@cisco.com, CCIE #14558, SFCE #124266, CEH

Technical Solution Architect - Security

Cisco Techclub, 10.5.2022



Secure Firewall 3100

Introduction

Cisco Secure Firewall 3100 Series

Make hybrid work and zero trust practical, with the flexibility to ensure strong return on investment

The new enterprise-class Cisco Secure Firewall 3100 Series supports your evolving world



Performance & Flexibility

Provide an exceptional hybrid work experience



Visibility & Enforcement

Keep the network from going dark and strengthen your zero-trust posture



Efficiency & Simplicity

Advanced automation and integrations drive cost-savings for modern environments

Why 3100 Series?

- Empower hybrid workers
 - Support more remote users with **up to 3X** performance enhancements with VPN
- Delight your employees
 - **Up to 3X inspected throughput** with multithreaded traffic handling technique, delivering strong video conferencing
- Get investment protection
 - **Clustering** and **high port density** flexibility allow your firewall to grow with you



Cisco Secure Firewall 3100 Series

Provide an exceptional
hybrid work experience

Secure Firewall 3100

Overview

3100 Series: Key Hardware Highlights



Crypto Accelerator

Accelerates bulk cryptographic operations.
Processes packets before the Firewall software.



Encrypted SSD Drive

Comes with a single SSD. A second SSD can be added to form RAID 1 (Optional).



Flow-Accelerator

A specially built circuit to provide flow acceleration and flow-offload*

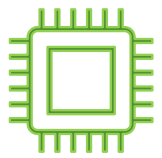
** Available from Version 7.2*



FIPS Compliance

Supports all FIPS 140-3 requirements

Hardware Resources: 3100 vs. FPR2100



Description	3110	3120	3130	3140
CPU	12-core	16-core	24-core	32-core
Memory	64 GB	128 GB	128 GB	256 GB
Storage (SSD)	960 GB	960 GB	960 GB	960 GB

Description	FPR 2110	FPR 2120	FPR 2130	FPR 2140
CPU/NPU	4/6-core	6/8-core	8/12-core	16/16-core
Memory/NPU RAM	16/8 GB	16/8 GB	32/16 GB	64/16 GB
Storage	100 GB	100 GB	200 GB	200 GB

Logical Capabilities: 3100 vs FPR2100



Description	3110	3120	3130	3140
Cluster	8	8	8	8
Multi-Instance	Will be supported from 2023			
VRF	30	30	50	50

Description	FPR 2110	FPR 2120	FPR 2130	FPR 2140
Cluster	Not Supported			
Multi-Instance	Not Supported			
VRF	10	20	30	40

Performance Boost



2110 vs 3110

2120 vs 3120

2130 vs 3130

2140 vs 3140

FW+AVC+IPS

2.6 → 17

3.4 → 21

5.4 → 38

10.4 → 45

IPsec VPN

0.9 → 8

1.2 → 10

1.9 → 17.8

3.6 → 22.4

**Performance Estimates are in Gbps, subject to 1024B packet size, protocol type, and other networking variables.*

Firepower Hardware Update

As the threat landscape evolves, our firewall portfolio does too. Gain more features and better performance at the same or lower price point.



Better performance

- Up to 3.5x boost in Firewall throughput
- Up to 5x boost in VPN throughput



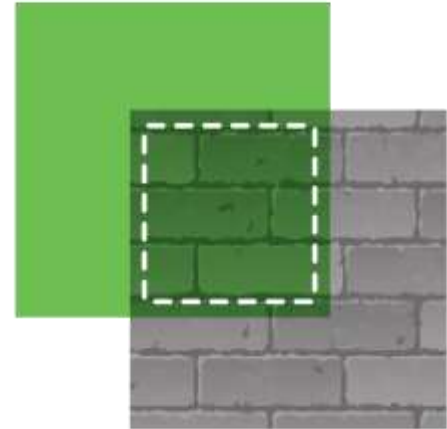
More connections

- Up to 2x more connections per second (CPS)



Improved encrypted traffic throughput

- Up to 3x boost in encrypted traffic performance



When It Comes to Refresh

22k/40k	FPR 2110/20	→	1150
62k	FPR 2130	→	3110
128k	FPR 2140	→	3120
138k/185k	FPR 4110/12	→	3130
247k	FPR 4115	→	3140

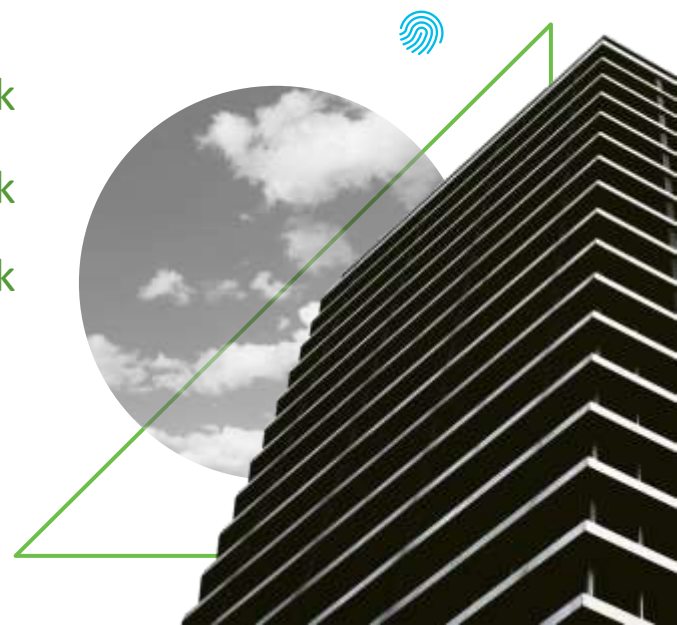
30k

71k

104k

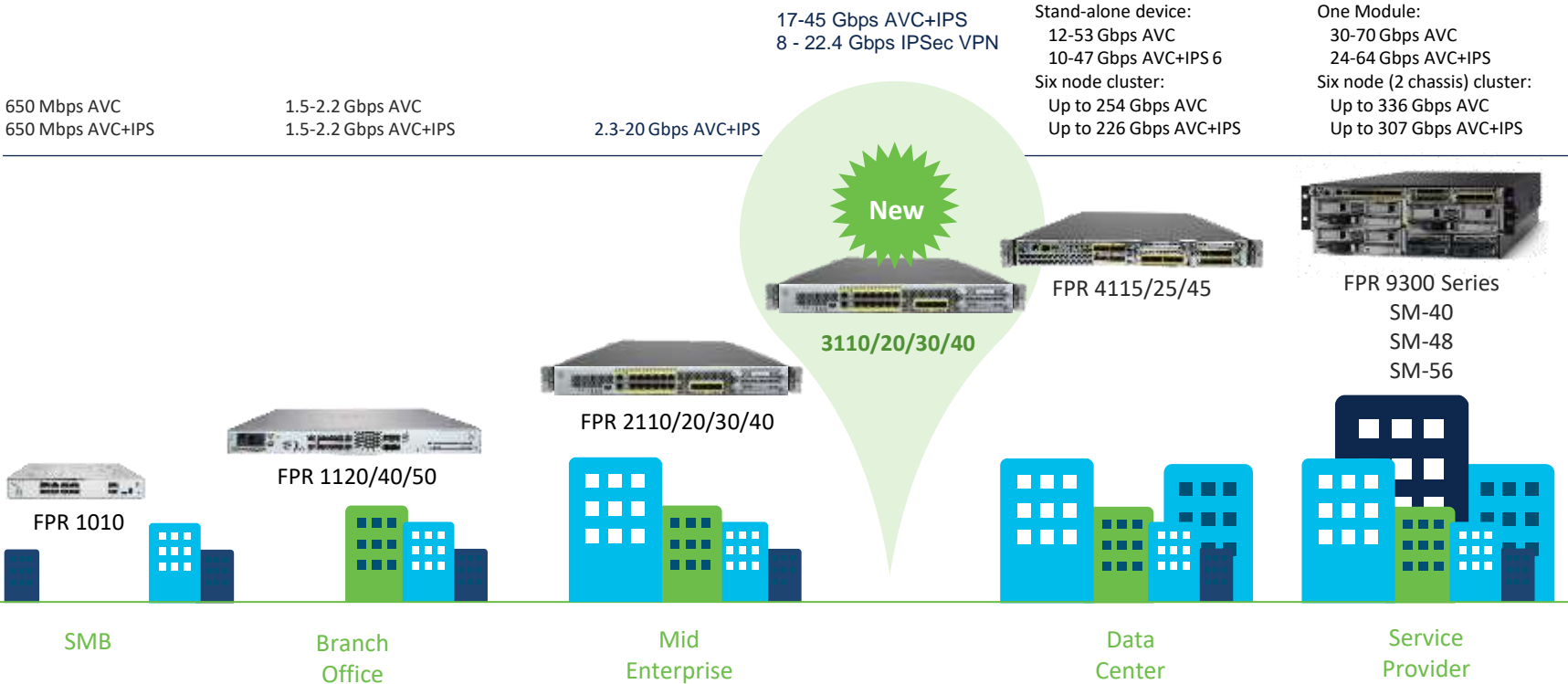
159k

184k



Physical Appliances

Supporting your choice of FTD or ASA software



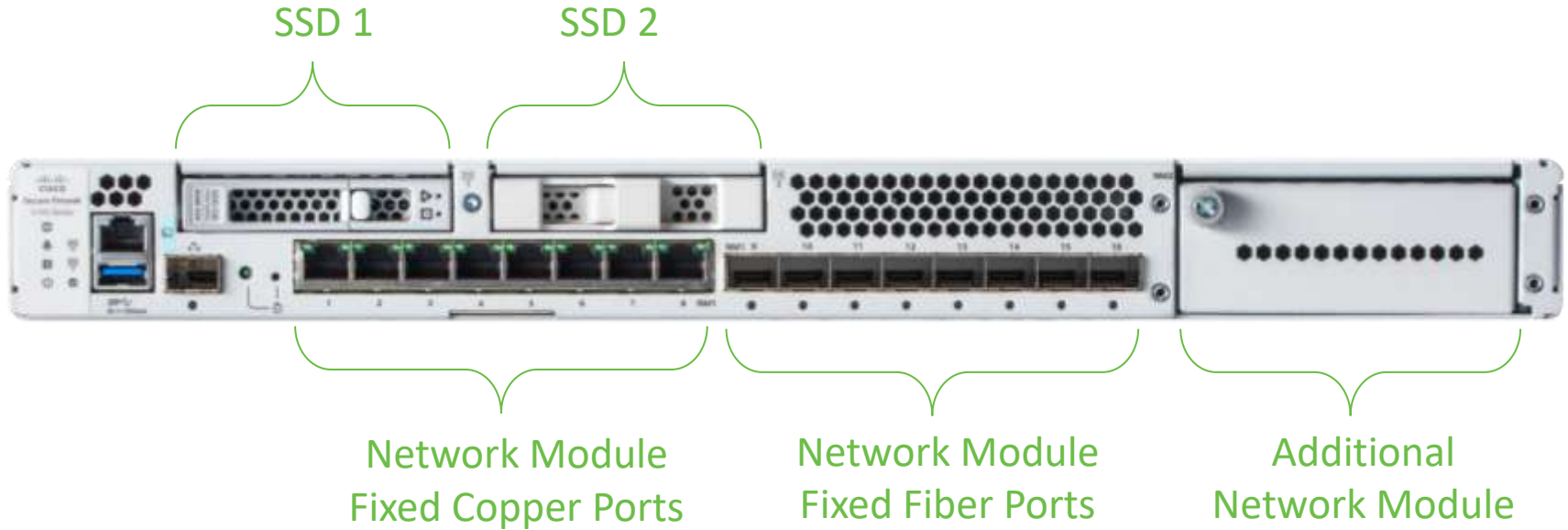
3100 Series: Minimum Supported Versions

Minimum Manager Version	Managed Devices Software	Minimum Version on Managed Devices
FMC 7.1	FTD	FTD 7.1
FDM 7.1	FTD	FTD 7.1
ASDM	ASA	ASA 9.17.1
CSM	ASA	ASA 9.17.1

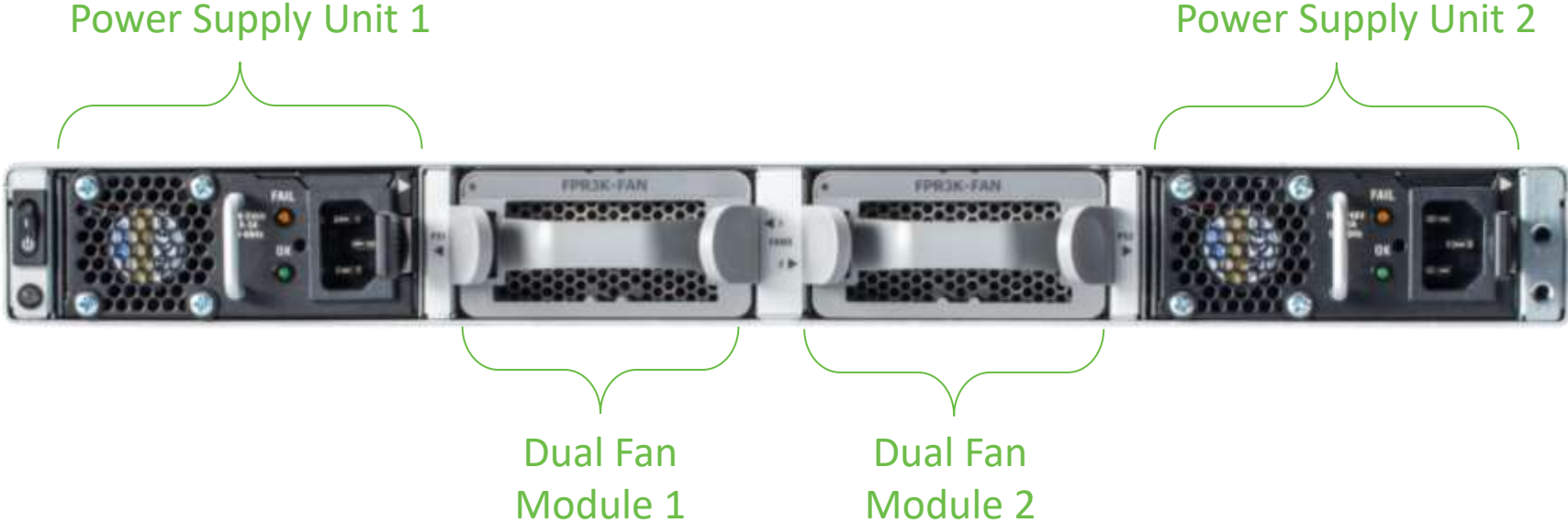
Secure Firewall 3100

Hardware

3100 Series: Front Panel



3100 Series: Back Panel



3100 Series: Network Interfaces



	3110	3120	3130	3140
Management	1 x 1/10G SFP	1 x 1/10G SFP	1 x 1/10G SFP	1 x 1/10G SFP
Integrated Interfaces	8 x 10M/100M/ 1GBASE-T Ethernet interfaces (RJ- 45),	8 x 10M/100M/ 1GBASE-T Ethernet interfaces (RJ- 45),	8 x 10M/100M/ 1GBASE-T Ethernet interfaces (RJ- 45),	8 x 10M/100M/ 1GBASE-T Ethernet interfaces (RJ- 45),
	8 x 1/10 Gigabit (SFP) Ethernet interfaces	8 x 1/10 Gigabit (SFP) Ethernet interfaces	8 x 1/10/25 Gigabit (SFP) Ethernet interfaces	8 x 1/10/25 Gigabit (SFP) Ethernet interfaces
Network Modules	8 x 1/10G Options	8 x 1/10G Options	8 x 1/10/25G, 4 x 40G Options	8 x 1/10/25G, 4 x 40G Options

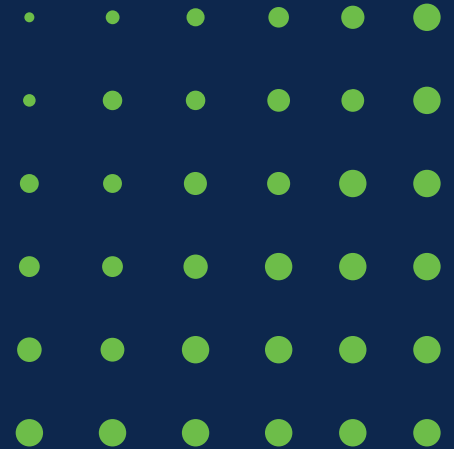
Hardware Specification Summary



	FPR3110	FPR3120	FPR3130	FPR3140
Core Count	12	16	24	32
System Memory	2x32GB@3200	2x64GB@3200	4x32GB@3200	4x64GB@3200
Front Panel Copper Ports	8x 10/100/1000MBase-T			
Front Panel Fiber Ports	8x 1/10G		8x 1/10/25G	
SSD, 2 slots FRU,	Default slot 1 populated, 2nd slot is for SW RAID1, 900GB minimum			
NetMod	1 Slot			
USB port	1x USB3.0 with 5W, type A connector			
Management Port	1x 1/10G SFP port			
Console	Supports 1x RJ45 interface			
PSU, FRU	1+1 (default 1)		1+1 (default 2)	

+	1.0	FPR3110-NGFW-K9 PLM SVIP SA more	168 days	70,840.88	1	70,840.88	0.00	70,840.88
		Cisco Secure Firewall 3110 NGFW Appliance, 1U						
		Valid as of 05-May-2022 10:40:23 PDT						
		<a>Edit Options <a>Edit Service/Subscription <a>Validate <a>Recommended Content <a>Add Note <a>More Actions	<a>Add Subtotal					
+	2.0	FPR3120-NGFW-K9 PLM SVIP SA more	168 days	103,690.51	1	103,690.51	0.00	103,690.51
		Cisco Secure Firewall 3120 NGFW Appliance, 1U						
		Valid as of 05-May-2022 10:40:41 PDT						
		<a>Edit Options <a>Edit Service/Subscription <a>Validate <a>Recommended Content <a>Add Note <a>More Actions	<a>Add Subtotal					
+	3.0	FPR3130-NGFW-K9 PLM SVIP SA more	168 days	158,942.05	1	158,942.05	0.00	158,942.05
		Cisco Secure Firewall 3130 NGFW Appliance, 1U						
		Valid as of 05-May-2022 10:41:51 PDT						
		<a>Edit Options <a>Edit Service/Subscription <a>Validate <a>Recommended Content <a>Add Note <a>More Actions	<a>Add Subtotal					
+	4.0	FPR3140-NGFW-K9 PLM SVIP SA more	168 days	183,919.96	1	183,919.96	0.00	183,919.96
		Cisco Secure Firewall 3140 NGFW Appliance, 1U						
		Valid as of 05-May-2022 10:43:44 PDT						
		<a>Edit Options <a>Edit Service/Subscription <a>Validate <a>Recommended Content <a>Add Note <a>More Actions	<a>Add Subtotal					

Secure Firewall Platforms recap..



What's new? – Firewall Virtual Platforms

Private Cloud

- FMCv and FTDv
 - ESXi 7.0 support
 - Support for: Cisco Hyperflex, Nutanix Enterprise Cloud, OpenStack
- ASAc Docker containers



Public Cloud

- Azure Application Insights for FTD metrics
- FMCv/FTDv ASAv on Google Cloud Platform & Oracle Cloud Infrastructure



Smart Licensing Performance Tiers

- 7.0 Evaluation mode and Smart License performance tiers
- Current perpetual BASE license moves to a subscription model

Performance Tier	Device Specifications	Rate Limit	RA VPN Session Limit
FTDv5	4 cores/8 GB	100Mbps	50
FTDv10	4 cores/8 GB	1Gbps	250
FTDv20	4 cores/8 GB	3Gbps	250
FTDv30	8 cores/16 GB	5Gbps	250
FTDv50	12 cores/24 GB	10Gbps	750
FTDv100	16 cores/32 GB	20Gbps	10000

Secure Firewall Cloud Native



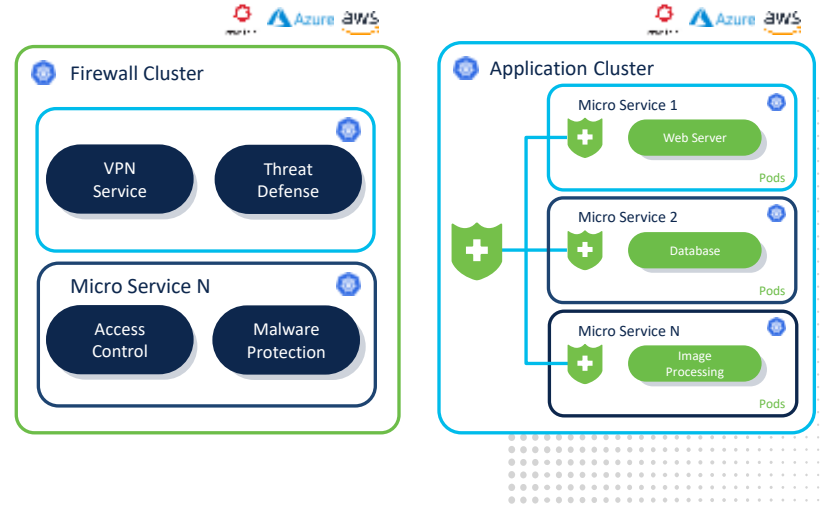
Easily deliver **firewall services** with massive scale and resiliency in cloud environments



Insert **security controls** next to application containers



Highly **scalable & elastic firewall** for edge use cases – RA VPN, DC Backhaul, Mobility carriers, MSP/MSSPs



Developer-friendly elastic firewall for Kubernetes-based environments

Firepower 1000 Series

Small business and branch office security with superior price/performance



Firepower 1010

- High-performance desktop firewall
- PoE, 8 10/100/1000 Base-T RJ45 switching ports
- Stateful firewall, AVC, NGIPS, AMP, URL filtering

650Mbps Firewall Throughput



Firepower 1120/40/50

- High-performance rackmount firewall
- 8 10/100/1000Base-T RJ45 switching ports, 4 1000Base-F SFP switching ports, 2 x 1/10Gbps SFP+ (1150)
- Stateful firewall, AVC, NGIPS, AMP, URL filtering

1120-1.5Gbps Firewall Throughput

1140-2.2Gbps Firewall Throughput

1150-3 Gbps Firewall Throughput

Firepower 4100 Series

- Up to **50% performance improvement** over previous models
- Up to **44% higher TLS performance!**
- Supported software releases:
 - FTD 6.4+ – including multi-instance
 - ASA 9.12.1+
 - FXOS 2.6.1+

Enterprise and data center security with exceptional price/performance



Four new appliance models:
4112*, 4115, 4125, 4145
up to **47 Gbps** Firewall throughput**

* 4112 FXOS 2.8.1, FTD 6.6 or ASA 9.14.1

** 1024B FW+AVC+IPS

Firepower 9300 Service Modules

- Up to **80% performance boost** than previous generation SM
- Up to **33% higher TLS performance!**
- Supported software releases:
 - FTD 6.4+ – including multi-instance
 - ASA 9.12.1+
 - FXOS 2.6.1+

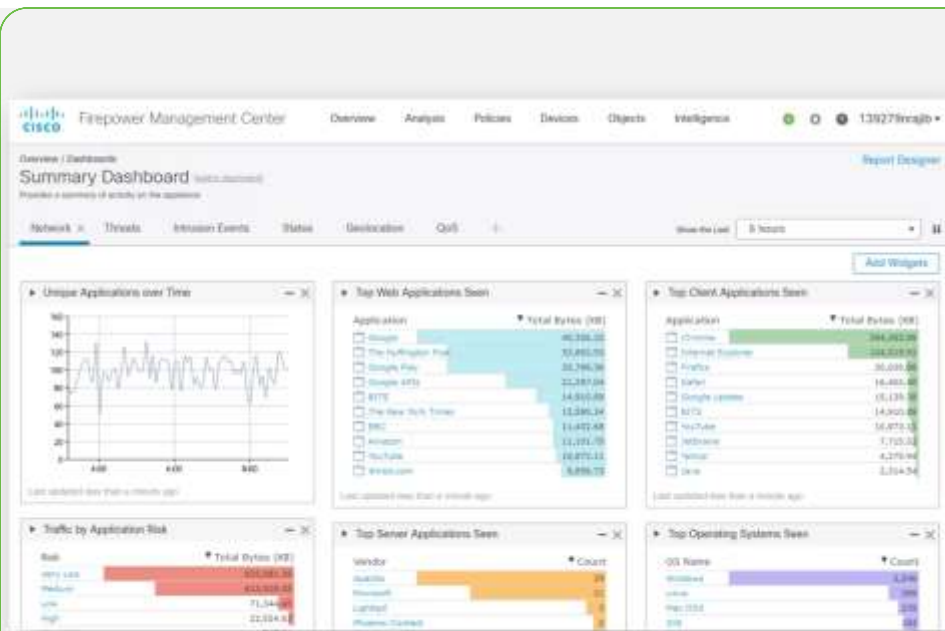


3 new 9300 SM models:
SM-40, SM-48, SM-56
up to **153 Gbps** Firewall throughput*

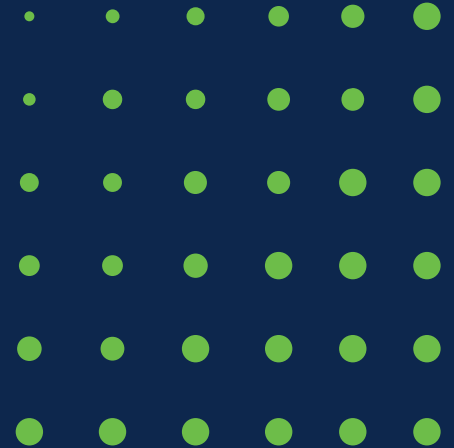
*1024B FW+AVC+IPS

FMC Virtual 300

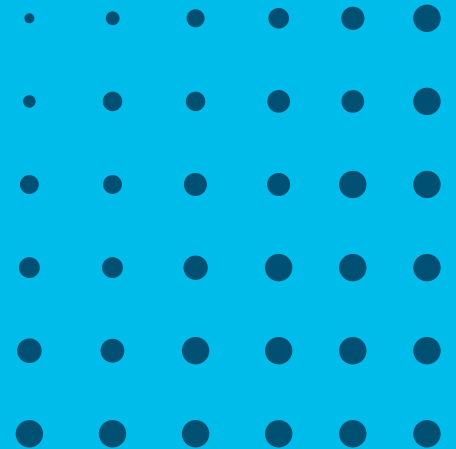
- Up to **300 managed devices!**
- CPU: 2 x 8 cores, Memory: 64 GB, hard disk: 2.2 TB
- **Migrate easily** from one FMC model to another
- High Availability for on prem, AWS and OCI clouds – 7.1 or higher
- Supported software releases:
 - FTD 6.5 or higher – including multi-instance
 - FMC 6.5 or higher



Secure Firewall Threat Defense 7.0/7.1



Snort 3



Snort 3 Rule Recommendations

Access Snort 3 Rule Recommendations under the Snort 3 version of the Intrusion Policy

The screenshot shows the Cisco Firepower Management Center interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', and 'Intelligence'. The 'Policies' tab is selected. Below the navigation bar, there are tabs for 'Intrusion Policies' and 'Network Analysis Policies'. A search bar is present with the text 'Search by Intrusion Policy, Description, or Base Policy'. To the right of the search bar are buttons for 'All IPS Rates', 'IPS Mapping', 'Compare Policies', and 'Create Policy'. Below these elements is a table with the following columns: 'Intrusion Policy', 'Description', 'Base Policy', and 'Usage Information'. The table contains one row for 'Custom Intrusion Policy'. The 'Usage Information' column for this row shows '1 Access Control Policy' and '2 Devices'. In the bottom right corner of the table row, there are two links: 'Snort 2 Version' and 'Snort 3 Version'. The 'Snort 3 Version' link is highlighted with a red rectangular box, and a large orange arrow points to it from the bottom right of the image.

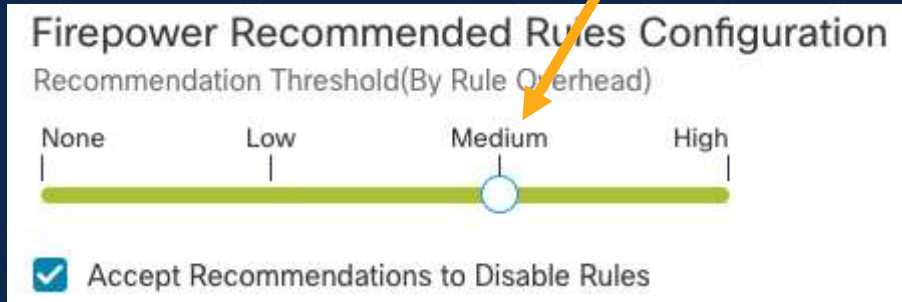
Intrusion Policy	Description	Base Policy	Usage Information
Custom Intrusion Policy Snort 3 is in sync with Snort 2	Custom Intrusion Policy Description	Maximum Detection	1 Access Control Policy 2 Devices Snort 2 Version Snort 3 Version

Recommendations Security Level

- Consider enabled rules from:
 - **Level 1** - Connectivity Over Security
 - **Level 2** - Balanced Security and Connectivity
 - **Level 3** - Security Over Connectivity
 - **Level 4** - Maximum Detection

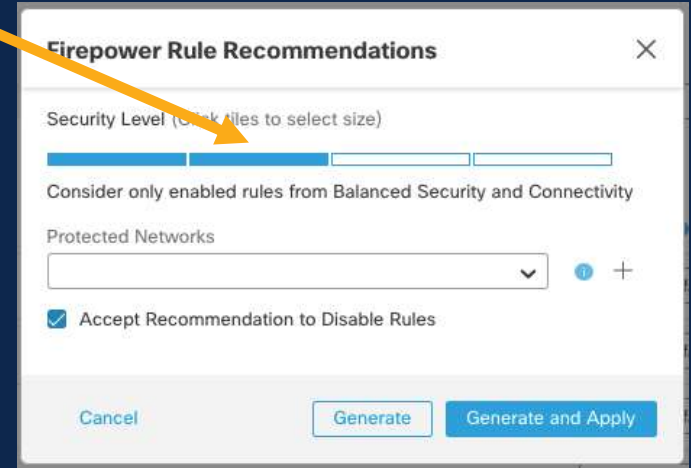
Snort 2 vs. Snort 3

Balanced (Security Level 2)



Snort 2

=



Snort 3

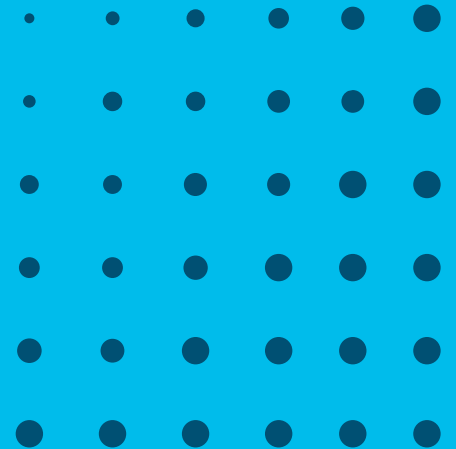
Snort 3 actions

- Starting in 7.0, FTD devices running Snort 3 supported six Snort rule actions - **Alert/Block/Reject/Rewrite/Pass/Drop**
- 7.0 FMC supported only two Snort 3 rule actions: **Alert/Block**
- Release 7.1 adds FMC capability to support additional Snort 3 rule actions
- Additional rule actions can be used on 7.0 or 7.1 devices

Actions for Snort 3 Rules

The screenshot displays the Snort 3 rule configuration interface. On the left, a table lists 160 rules, with rule 1:51384 selected. A dropdown menu is open, showing the following actions: Block (Default), Alert, Rewrite, Pass, Drop, Reject, Disable, and Revert to default. A green callout bubble points to the 'Disable' option with the text: 'Not an action keyword - rule is not enabled in policy'. The background shows a rule configuration page for 'Browser / WebKit' with a security level indicator and a list of rules.

FMC Upgrade Revert



What's New



Solution

- From 7.1.0 onwards, FMC has an “Enable revert after successful upgrade” option in the system updates page.
 - Enabled by default
- From FP 7.1.0 onwards, FMC has “Revert Upgrade” option for devices in device management page.
- After successful FTD upgrade, within 30 days, if customer wishes to roll back to the previous version for any unforeseen circumstances, then they can revert the upgrade



“Enable revert” option on updates page

Firepower Management Center
System / Updates / Upload Update

Overview Analysis Policies Devices Objects AMP Intelligence

Product Updates Rule Updates Geolocation Updates

Currently running software version: **7.1.0**

FMC is on 7.1.0

Selected Update

Type	Cisco FTD Upgrade
Version	7.1.0-1773
Date	Mon Jun 14 03:33:37 UTC 2021
Reboot	Yes

Automatically cancel on upgrade failure and roll back to the previous version (Applies to individual units in HA or Clusters)

Enable revert after successful upgrade

FTDs are on 6.7.0

<input type="checkbox"/>	Untraced (1 total)	Compatibility Check	Readiness Check Results	Readiness Check Completed	Estimated Upgrade Time
<input type="checkbox"/>	FTD-HA Cisco Firepower Threat Defense for VMWare Cluster				
<input type="checkbox"/>	10.10.6.3 (active) 10.10.6.3 - Cisco Firepower Threat Defense for VMWare v6.7.0	✔ Compatibility check passed. Proceed with readiness check.			10 min
<input type="checkbox"/>	10.10.6.4 10.10.6.4 - Cisco Firepower Threat Defense for VMWare v6.7.0	✔ Compatibility check passed. Proceed with readiness check.			10 min

[Back](#) [Check Readiness](#) [Install](#)

As part of Upgrading, there is a new “Enable revert after successful upgrade” checkbox

- By default, the “Enable revert after successful upgrade” checkbox is checked.
- If the user unchecks this option, after upgrading, Revert Upgrade will not be available for the device.

Device management page “Revert Upgrade” option

Firepower Management Center
Devices | Device Management

Overview Analysis Policies **Devices** Objects AMP Intelligence

Deploy Search Device Add

View By: Group

All (5) Error (1) Warning (0) Offline (0) Normal (4) Deployment Pending (0) Upgrade (4) Snort 3 (1)

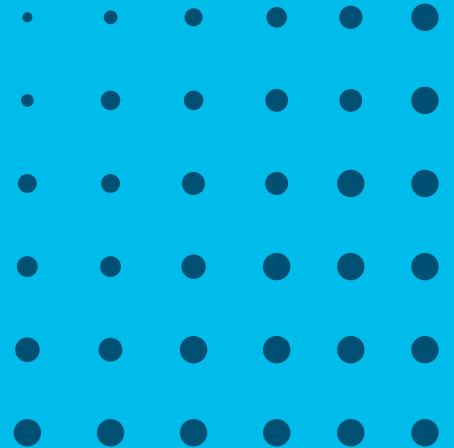
Deployment History

Collaps All

Name	Model	Version	Chassis	Licenses	Access Control Policy
10.10.6.5 10.10.6.5 - Routed	FTDv for VMware	7.1.0	N/A	Base, Threat (2 more ...)	upgrade_policy_1
10.10.6.6 10.10.6.6 - Routed	FTDv for VMware	7.1.0	N/A	Base, Threat (2 more ...)	upgrade_policy_1
10.10.6.7 10.10.6.7				Uncensored	upgrade_policy_1
FTD-HA High Availability					
10.10.6.3 (Primary, Active) 10.10.6.3 - Routed				Base, Threat (2 more ...)	upgrade_policy_1
10.10.6.4 (Secondary, Standby)					

On the Device Management page, devices have a Revert Upgrade option available

Cluster Upgrade Improvements



What's New



Solution

- The Device Upgrade workflow (**Devices -> Device Upgrade**) improvement to provide better support for cluster upgrades.
 - Cluster validations are performed, status and issues are reported on the UI
 - Offline nodes are excluded from upgrade automatically and user is informed as such.
 - Upgrade order is displayed on the UI. From the UI, user can also change upgrade order for data nodes if they want.
 - If the upgrade transaction has completed the upgrade for at least one node then it will tolerate one upgrade failure for the remaining nodes.
 - During a cluster upgrade transaction, if there is a newly-elected control node and that node has not been upgraded yet, then it will become the last node to be upgraded.
 - Similar improvements are also implemented for FTDs deployed in HA.
 - Infrastructure to enable the upgrade package sync in FTD nodes of Cluster/HA deployments using rsync over secure control/failover link leading to more reliable and faster upgrades

Upgrade Order

- Clusters
 - Control node is always upgraded last
 - Upgrade order for data nodes:
 - Default order: generated automatically based on **Priority** attribute of cluster nodes
 - Node with highest priority value gets upgraded first (since it has the least chance to become the control node)
 - Node with second highest priority value gets upgraded next, and so on.
 - Order can be customized by user if needed
- HAs:
 - Active unit is always upgraded last
 - There is only the auto-generated default order, user-defined order is not allowed

```
> show running-config cluster
cluster group FPR-9300_MI_Cluster-1
key *****
local-unit unit-1-1
cluster-interface Port-channel10 ip 127.2.1.1 255.255.0.0
priority 9
health-check holdtime 3
health-check data-interface auto-rejoin 3 5 2
health-check cluster-interface auto-rejoin unlimited 5 1
health-check system auto-rejoin 3 5 2
health-check monitor-interface debounce-time 500
site-id 1
no unit join-acceleration
enable
```

Upgrade Order (cont.)

1 Copy Upgrade Packages to Devices — 2 Compatibility and Readiness Checks — 3 Upgrade

Upgrade to: 6.7.0.8123-65

Device Selection Action

1 cluster/HA pair is ready for upgrade to Version 6.7.0.8123-65.

Upgrade order is displayed, and you can click on “Change Upgrade Order” to change it if you want

Device Details

Search

1 cluster/HA pair is ready for upgrade.

Device	Model	Details
Cluster		
FPR-4100-MI-FTD-3		Change Upgrade Order
1 192.168.3.37 Version 6.7.0	Firepower 4145 with FTD	Ready for upgrade. Compatibility...
2 192.168.3.79 Version 6.7.0	Firepower 4125 with FTD	Ready for upgrade. Compatibility...
3 192.168.3.83 Version 6.7.0	Firepower 4145 with FTD	Ready for upgrade. Compatibility...
4 192.168.3.41 (Control) Version 6.7.0	Firepower 4125 with FTD	Ready for upgrade. Compatibility...

Ready for upgrade.
Compatibility and readiness checks passed.
Active unit (clustering is enabled.)

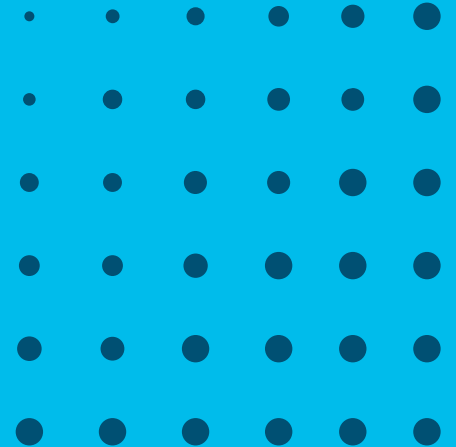
1 of 1 selected cluster/HA pair is ready for upgrade.

Reset

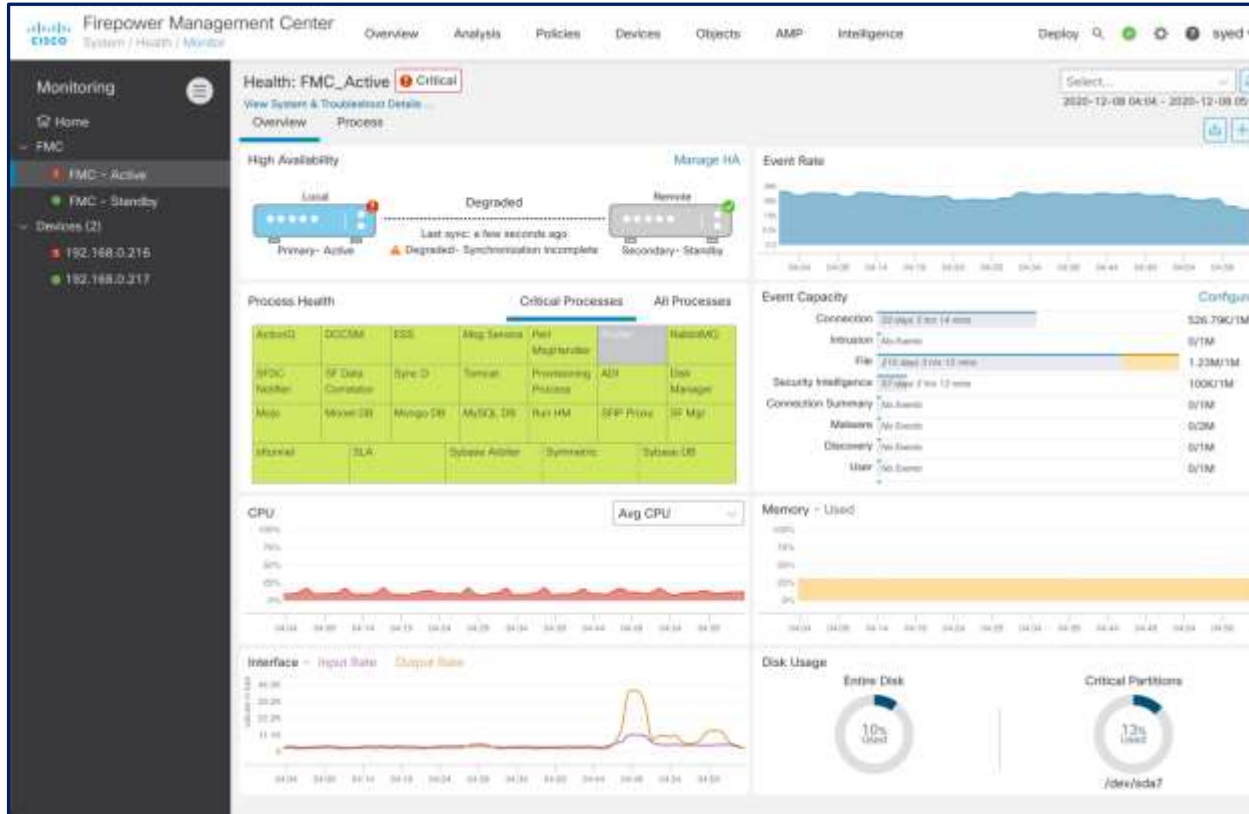
Previous

Start Upgrade

Health Monitoring Improvements



Health Monitoring - FMC



FMC Dashboard

- HA
- Event Rate
- Event Capacity
- Process Health
- CPU
- Memory
- Interface
- Disk Usage

This dashboard is available to both Active and Standby FMC

Health Monitoring - Devices

Firepower Management Center | System / Health / Monitor | Overview | Analysis | Policies | Devices | Objects | AMP | Intelligence | Deploy | admin

Monitoring

- Home
- FMC
- Devices (4)
 - NGFW1
 - NGFW2
 - NGFWBR1
 - NGFWTG**

Health: NGFWTG Warning

Last 1 hour
2020-11-03 10:38 - 2020-11-03 11:38

System Details

Up Time:	VDE:	Build 338 - 2020-09-24 12:58:48	Troubleshooting & Links
Version: 6.7.0	SRU:	2020-10-14-001-wrt	Generate Troubleshooting Files
Model: Cisco Firepower Threat Defense for VMWare	Score:	2.0.17 (Build 100 - dag12)	Advanced Troubleshooting
Mode: ROUTED			Alerts

Health Policy (Initial_Health_Policy 2018-02-18 16:18:32)

Overview | CPU | Memory | Interfaces | Connections | Smart | Correlation-CPU-Dataplane | Correlation-Packetdrops

CPU

Data Plane	Avg 2.5 %	Smart	Avg 7.0 %	System	Avg 4.3 %
1 core	18.5 - 22 %	1 core	1.0 % - 4.3 %	2 core	3.5 % - 11.5 %

Memory

Data Plane	Avg 80.7 %	Smart	Avg 31.4 %	System	Avg 26.9 %
3 core	80.4 % - 80.7 %	3 core	21.5 % - 31.4 %	1 core	30.2 % - 34.2 %

Throughput

Input Rate: Avg 825.2972pps (3.33 Gbps - 338.17 Mbps) | Output Rate: Avg 80.2192pps (30 Mbps - 16.8 Mbps)

Avg - All Interfaces

Connection Statistics

Connections: Avg 13.13K (10.00 - 11.00) | NAT Translations: Avg 0 (0 - 0)

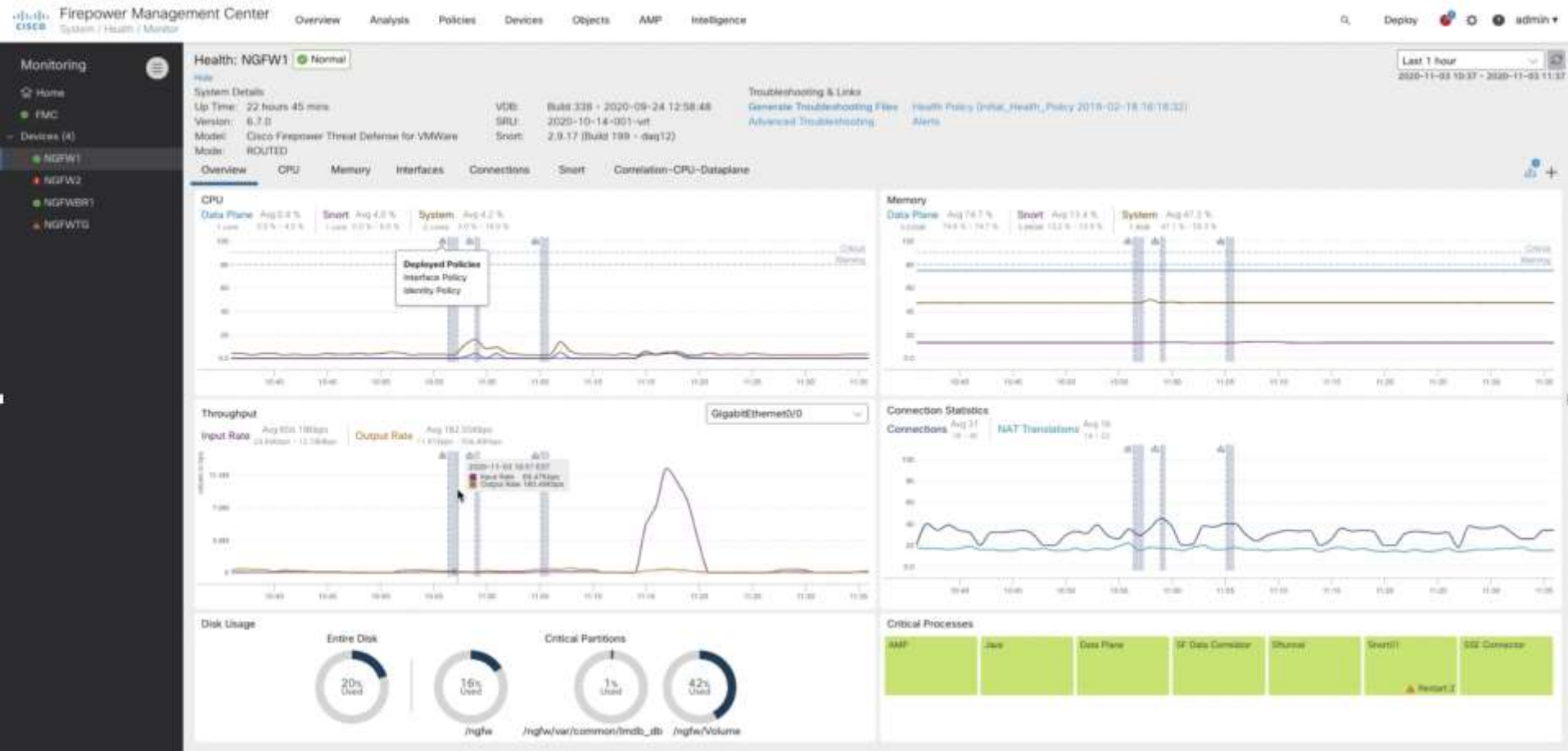
Disk Usage

Entire Disk	20% Used	Critical Partitions	
		/mgw: 16% Used	/mgw/Volume: 43% Used

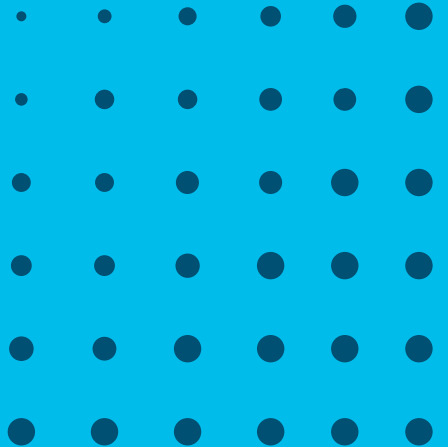
Critical Processes

AMP	Java	Data Plane	IP Data Connector	Shunex	SmartUI	SSZ Connector
-----	------	------------	-------------------	--------	---------	---------------

Device Health Monitoring

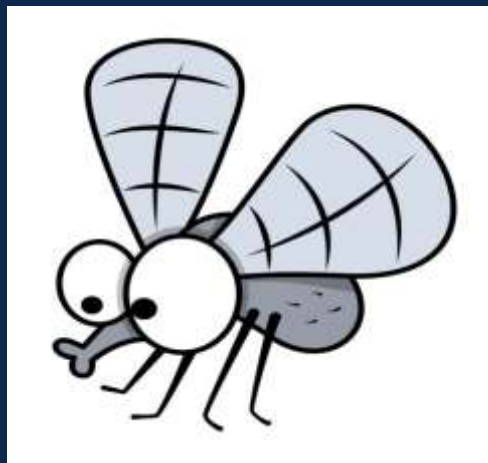


NAT Translations in Events



Feature Overview

- Before 7.1
 - Lina performed NAT translations
 - Snort engine received real IP address and ports
 - Events did not contain information about translated IP address and ports
- With 7.1: NAT IP and port translations in the connection events
 - Any connection event consumer receives 4 additional fields:
 - Translated source and destination IP addresses
 - Translated source and destination ports
 - Supported in both FMC and FTD
 - Both Snort 2 and Snort 3
 - No configuration required



FMC Example

https://10.197.82.111:18250/events/index.cgi

Overview **Analysis** Policies Devices Objects AMP Intelligence Deploy System Help admin

Context Explorer Unified Events **Connections** Events Intrusions File Hosts Users Correlation Advanced Search

Connection Events (switch workflow)

Connections with Application Details [Table View of Connection Events](#)

in Search Constraints [Edit Search](#)

Jump to:

<input type="checkbox"/>	First Packet	Last Packet	Action	Initiator IP	BAI Source IP	Initiator Country	Responder IP	BAI Destination IP	Responder Country	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	BAI Source Port	Destination Port / ICMP Code	BAI Destination Port
<input type="checkbox"/>	2021-06-14 06:54:49	2021-06-14 06:54:49	Allow	11.1.1.8	8.8.8.1	USA	12.1.1.3	12.1.1.3	USA	Inside_1	Outside_1	2377 / tcp	2380 / tcp	80 (http) / tcp	80 (http) / tcp
<input type="checkbox"/>	2021-06-14 06:54:49	2021-06-14 06:54:49	Allow	11.1.1.8	8.8.8.1	USA	12.1.1.3	12.1.1.3	USA	Inside_1	Outside_1	2378 / tcp	2378 / tcp	80 (http) / tcp	80 (http) / tcp
<input type="checkbox"/>	2021-06-14 06:54:49	2021-06-14 06:54:49	Allow	11.1.1.8	8.8.8.1	USA	12.1.1.3	12.1.1.3	USA	Inside_1	Outside_1	2382 / tcp	2382 / tcp	80 (http) / tcp	80 (http) / tcp
<input type="checkbox"/>	2021-06-14 06:54:49	2021-06-14 06:54:49	Allow	11.1.1.8	8.8.8.1	USA	12.1.1.3	12.1.1.3	USA	Inside_1	Outside_1	2374 / tcp	2373 / tcp	80 (http) / tcp	80 (http) / tcp
<input type="checkbox"/>	2021-06-14 06:54:49	2021-06-14 06:54:49	Allow	11.1.1.8	8.8.8.1	USA	12.1.1.3	12.1.1.3	USA	Inside_1	Outside_1	2372 / tcp	2373 / tcp	80 (http) / tcp	80 (http) / tcp
<input type="checkbox"/>	2021-06-14 06:54:49	2021-06-14 06:54:49	Allow	11.1.1.8	8.8.8.1	USA	12.1.1.3	12.1.1.3	USA	Inside_1	Outside_1	2368 / tcp	2371 / tcp	80 (http) / tcp	80 (http) / tcp
<input type="checkbox"/>	2021-06-14 06:54:49	2021-06-14 06:54:49	Allow	11.1.1.8	8.8.8.1	USA	12.1.1.3	12.1.1.3	USA	Inside_1	Outside_1	2370 / tcp	2373 / tcp	80 (http) / tcp	80 (http) / tcp
<input type="checkbox"/>	2021-06-14 06:54:49	2021-06-14 06:54:49	Allow	11.1.1.8	8.8.8.1	USA	12.1.1.3	12.1.1.3	USA	Inside_1	Outside_1	2381 / tcp	2384 / tcp	80 (http) / tcp	80 (http) / tcp
<input type="checkbox"/>	2021-06-14 06:54:49	2021-06-14 06:54:49	Allow	11.1.1.7	8.8.8.1	USA	12.1.1.3	12.1.1.3	USA	Inside_1	Outside_1	1648 / tcp	2630 / tcp	80 (http) / tcp	80 (http) / tcp
<input type="checkbox"/>	2021-06-14 06:54:49	2021-06-14 06:54:49	Allow	11.1.1.8	8.8.8.1	USA	12.1.1.3	12.1.1.3	USA	Inside_1	Outside_1	2384 / tcp	2387 / tcp	80 (http) / tcp	80 (http) / tcp
<input type="checkbox"/>	2021-06-14 06:54:49	2021-06-14 06:54:49	Allow	11.1.1.8	8.8.8.1	USA	12.1.1.3	12.1.1.3	USA	Inside_1	Outside_1	2389 / tcp	2373 / tcp	80 (http) / tcp	80 (http) / tcp
<input type="checkbox"/>	2021-06-14 06:54:49	2021-06-14 06:54:49	Allow	11.1.1.8	8.8.8.1	USA	12.1.1.3	12.1.1.3	USA	Inside_1	Outside_1	2383 / tcp	2386 / tcp	80 (http) / tcp	80 (http) / tcp
<input type="checkbox"/>	2021-06-14 06:54:49	2021-06-14 06:54:49	Allow	11.1.1.9	8.8.8.1	USA	12.1.1.3	12.1.1.3	USA	Inside_1	Outside_1	1037 / tcp	7039 / tcp	80 (http) / tcp	80 (http) / tcp
<input type="checkbox"/>	2021-06-14 06:54:49	2021-06-14 06:54:49	Allow	11.1.1.8	8.8.8.1	USA	12.1.1.3	12.1.1.3	USA	Inside_1	Outside_1	1033 / tcp	7035 / tcp	80 (http) / tcp	80 (http) / tcp
<input type="checkbox"/>	2021-06-14 06:54:49	2021-06-14 06:54:49	Allow	11.1.1.8	8.8.8.1	USA	12.1.1.3	12.1.1.3	USA	Inside_1	Outside_1	2373 / tcp	2376 / tcp	80 (http) / tcp	80 (http) / tcp
<input type="checkbox"/>	2021-06-14 06:54:49	2021-06-14 06:54:49	Allow	11.1.1.5	8.8.8.1	USA	12.1.1.3	12.1.1.3	USA	Inside_1	Outside_1	1888 / tcp	2620 / tcp	80 (http) / tcp	80 (http) / tcp
<input type="checkbox"/>	2021-06-14 06:54:49	2021-06-14 06:54:49	Allow	11.1.1.8	8.8.8.1	USA	12.1.1.3	12.1.1.3	USA	Inside_1	Outside_1	2378 / tcp	2379 / tcp	80 (http) / tcp	80 (http) / tcp
<input type="checkbox"/>	2021-06-14 06:54:49	2021-06-14 06:54:49	Allow	11.1.1.5	8.8.8.1	USA	12.1.1.3	12.1.1.3	USA	Inside_1	Outside_1	1662 / tcp	2664 / tcp	80 (http) / tcp	80 (http) / tcp

FDM Example

+

All Events Connection Intrusion File Malware File Security Intelligence

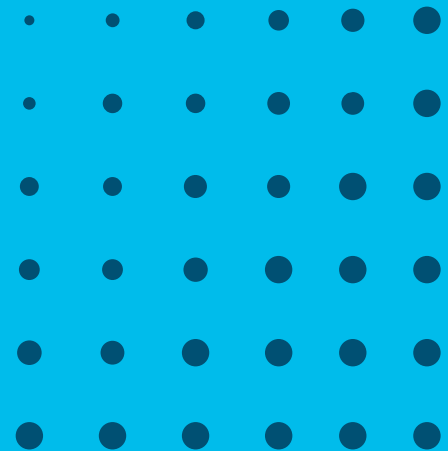
Enter Filter Criteria RESET FILTERS

5 seconds PAUSE

11 Jun 2021, 11:42 AM (IST) Add

RECEIVE TIMES	ACTION	FIRST PACKET	LAST PACKET	REASON	INITIATOR IP	RESPONDER IP	SOURCE PORT
06/08/2021 4:03:15 PM	Trust	06/08/2021 4:03...	06/08/2021 4:03...		8.8.8.100	10.10.10.200	0
06/08/2021 4:03:14 PM	Trust	06/08/2021 4:03...		View Details	8.8.8.100	10.10.10.200	0
06/08/2021 4:03:14 PM	Trust	06/08/2021 4:03...	06/08/2021 4:03...		8.8.8.100	10.10.10.200	0

VPN



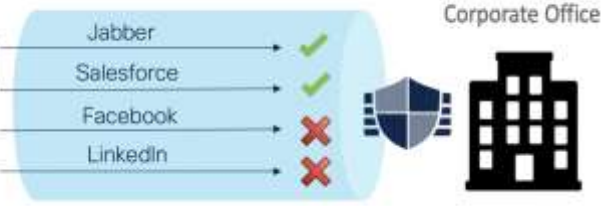
Dynamic Access Policy

The screenshot shows the configuration page for a Dynamic Access Policy in the Cisco Firepower Management Center. The page is titled "Firepower Management Center" and "Devices / VPN / Dynamic Access Policy". It has tabs for "Overview" and "Analysis". The "General" tab is selected, showing the following configuration:

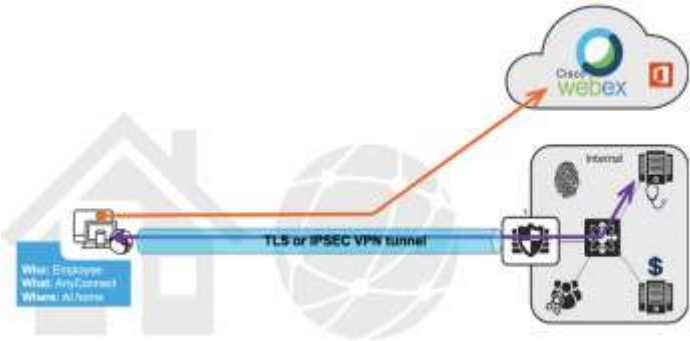
- Name:** Engineering Users
- Priority:** 5
- Action:** Continue (selected), Terminate, Quarantine
- Display User Message on Criterion Match
This message will be displayed to the VPN user if the DAP record matches.
- Apply a Network ACL on Traffic
Engineering_Access
- Apply one or more AnyConnect Custom Attributes
Engineering_Anyconnect_Attributes: x



Mobile User



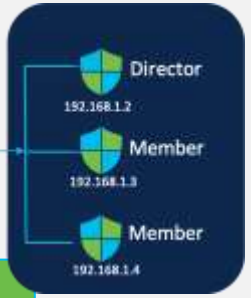
Per App VPN



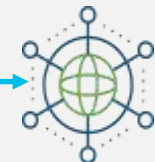
Dynamic Tunneling



Virtual IP Address
192.168.1.1



VPN Load Balancing



Local User Database

Local Authentication

Other 7.1 Features – Slide 1 of 2

- Routing
 - BGP IPv6 support for VRFs and VTIs
 - BGP VRF route leaking (IPv4 and IPv6)
 - ECMP/Traffic Zones configurable in the FMC UI
 - Policy based routing, including application-based routing for DIA using feeds
- TLS Enhancements
 - Certificate feeds
 - Advanced options in FMC
 - Encrypted Visibility Engine (experimental debut)
- Wild card (discontiguous) masks
- FQDN Based NAT

Encrypted Visibility Engine

- Experimental feature in release 7.1
- Utilizes machine learning to determine the application (client process) generating the Client Hello packet
- Identifies known processes/browsers
- Identifies malware based on Secure Malware Analytics fingerprints

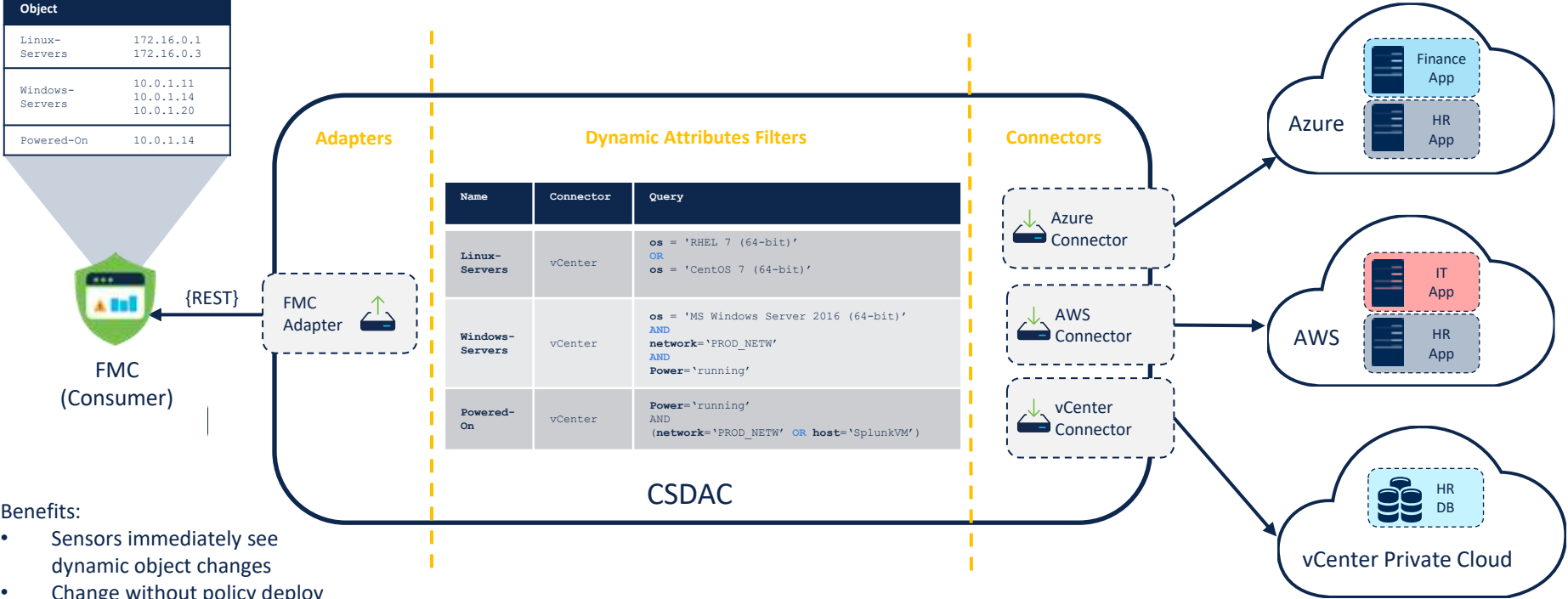


Other 7.1 Features – Slide 2 of 2

- Auto Rollback for Remote Branch Deployment
- Enhanced troubleshooting including new FTD packet tracer
- VPN – striving for parity with ASA: VPN filter, multiple IKE policies
- VPN – enhancements: local tunnel ID support for integration with Umbrella, tunnel monitoring dashboard, remote access VPN configuration copy
- Dynamic feeds for O365 and Azure Service Tags using dynamic objects
- Virtual
 - GENEVE tunnel support for Gateway Load Balancer in AWS
 - ASA v Clustering for private cloud
 - Enhancements to Cisco Secure Managed Remote Access (CSRA)
 - Enhancements to Cisco Secure Firewall Cloud Native (CSFCN)

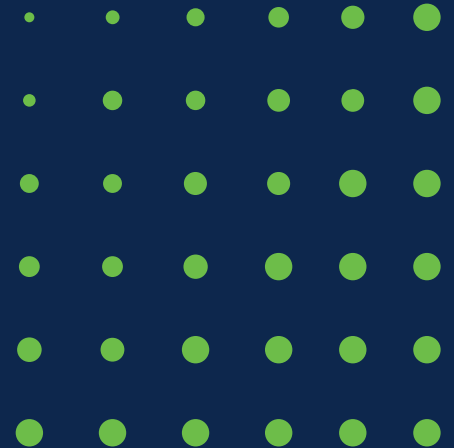
Cisco Secure Dynamic Attributes Connector

Dynamic Object	Mappings
Linux-Servers	172.16.0.1 172.16.0.3
Windows-Servers	10.0.1.11 10.0.1.14 10.0.1.20
Powered-On	10.0.1.14



- Benefits:**
- Sensors immediately see dynamic object changes
 - Change without policy deploy

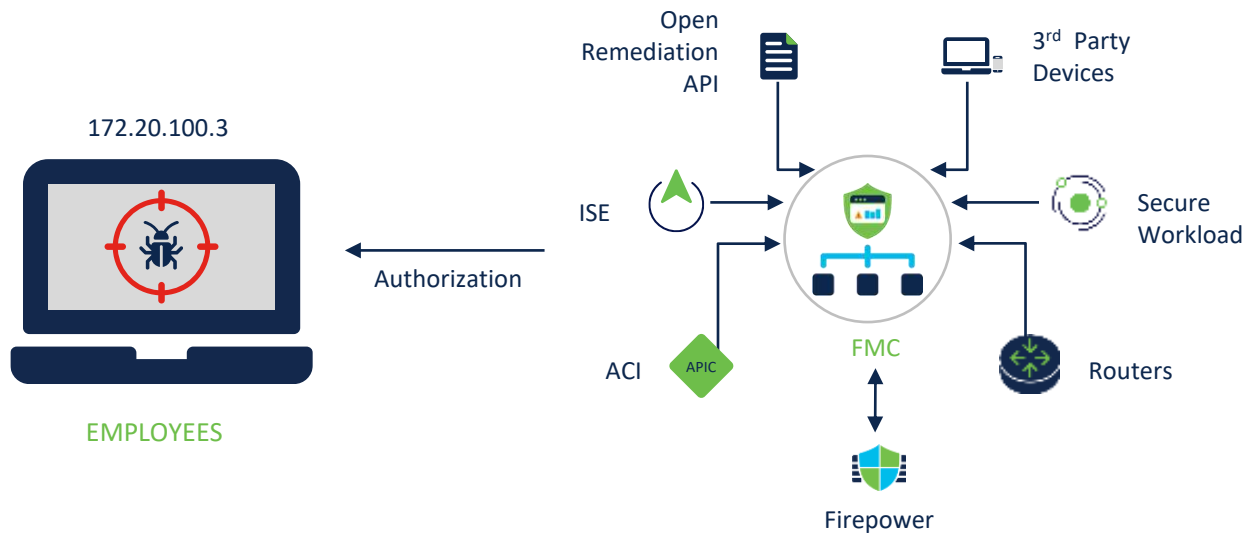
Integrated Security Portfolio



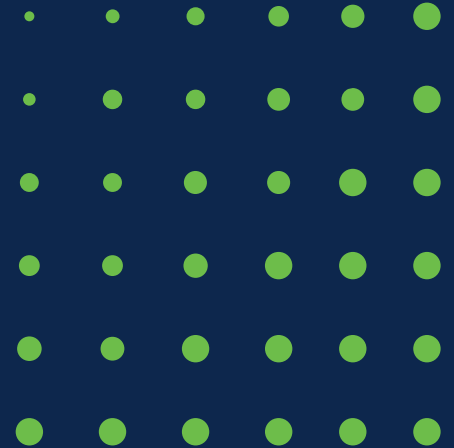
Cisco Rapid Threat Containment

Proven approach to reduce time and impact of threat

- Automatic network threat containment using the network as an enforcer
- Threat-centric network access determines network access based on IoCs
- Richer visibility from bidirectional data sharing with the network access



Firepower Competitive Advantages



Silver Bullets

DC Technology:

- Clustering (geo-clustering)
- ACI integration
- Virtual contexts
- IPS/IDS/FW flexibility

Identity, Device, Health,...

- Integration with ISE, AMP, Vulnerability Scanners, Threat Director feeds...
- Dynamic Objects
- Secure Analytics and Logging (SAL)

Talos

- IPS
- Security Intelligence
- AMP

VPN

- Easy to install, also with virtual
- DUO MFA

Encrypted traffic

- Integration with other platforms: AnyConnect, AMP, Stealthwatch, Tetration

Automation

- Correlation, Indication of compromise
- Learning => Recommendation, Events Filtering
- Remediation
- SecureX
- API

XDR (SecureX)



- Applications & Integrations
 - Applications
 - Threat Response [Launch](#)
 - Security Services Exchange [Launch](#)
 - Enabled Integrations
 - Cisco Integrations
 - AMP for Endpoints [Add](#) [Learn More](#) | Free Trial
 - Cisco Defense Orchestrator [Add](#) [Learn More](#) | Free Trial
 - Cisco Tetration - Application-First Workload Protection [Add](#) [Learn More](#)
 - Cisco Threat Intelligence API [Add](#) [Learn More](#)
 - Email Security Appliance [Add](#) [Learn More](#) | Free Trial
 - Firepower [Add](#) [Learn More](#) | Free Trial
 - Orbital [Add](#) [Learn More](#)
 - Orbital (deprecated) [Add](#) [Learn More](#)

Private Intelligence

Incident statuses and assignees

Last 90 Days

- new (1)
- open (1)

- Assigned to Me (2)
- Assigned to Other (1)

78

Firepower

Incident Promotion Reason

Last 7 Days

- Talos Disposition (0)
- User Promoted (0)
- Security Intelligence Category: IP (0)
- Security Intelligence Category: DNS (0)
- Security Intelligence Category: URL (0)
- Intrusion Rules Category (0)
- Malware Threat Score (0)
- Custom IP Address (0)

The data returned a value of 0.

Firepower

Event Summary

Last 7 Days

Total: 1	Intrusion: 1	Malware: 0	Security Intelligence: 0
----------	--------------	------------	--------------------------

Firepower

Talos IP Reputation

Last 7 Days

Poor: 0	Questionable: 0	Neutral: 1	Favorable: 0	Good: 0
---------	-----------------	------------	--------------	---------

Firepower

Intrusion Top Attackers

Last 7 Days

- #### News
- Welcome to SecureX
 - Maximize your experience by reviewing these key topics:
 - About SecureX
 - Configure Integration Modules
 - Configure Dashboards and Tiles
 - Activate Orchestration
 - Navigate SecureX
 - SecureX Ribbon
 - SecureX
 - SecureX Academy is LIVE
 - Cisco Secure is happy to announce the immediate availability of SecureX Academy, a new guided learning experience to walk you through access, adoption,...
 - SecureX Videos
 - Splunk Integration Tutorial and Demo video
 - The Splunk integration with SecureX is now live! Many of our customers are also Splunk users, and they have been clamoring for the ability to use their existing Splunk investments a...
 - SecureX Videos
 - Add 10 Free Threat Intelligence Sources in under 3 minutes
 - Cisco has made it easier than ever to integrate some of your favorite free, paid, open source, or vendor-provided threat intelligence and other network security tools into...

Applications & Integrations

- Applications
 - Threat Response [Launch](#)
 - Security Services Exchange [Launch](#)
- Enabled Integrations
- Cisco Integrations
 - AMP for Endpoints [Add](#) [Learn More](#) | [Free Trial](#)
 - Cisco Defense Orchestrator [Add](#) [Learn More](#) | [Free Trial](#)
 - Cisco Tetration - Application-First Workload Protection

PoC SWATCH Firewall Workloads Email Security Web Security Stealthwatch prglab Er > [Customize](#) Maximum Available Interval

Firepower Device Inventory

Suggested version: 6.6.1

Firepower Management Center	FMC needs upgrade	Managed devices needing upgrade
fmcw.prglab.local	No	0

Firepower Security Update Status

Firepower Management Center	Installed Version	Status
Intrusion Rule Update	fmcw.prglab.local	2021-07-21-001-wt

News

Welcome to SecureX

Maximize your experience by reviewing these key topics:

- About SecureX
- Configure Integration Modules
- Configure Dashboards and Tiles
- Activate Orchestration
- Navigate SecureX
- SecureX Ribbon

SecureX

SecureX Academy is LIVE

Cisco Secure is happy to announce the immediate availability of SecureX Academy, a new guided learning experience to walk you through access, adoption...

SECURE X Incidents

Incidents [New Incident](#)

Search...

Assigned to me - Open (4)

- Excessive Access Attempts (External) f... Cisco Stealthwatch Cloud Jun 01, 2021
- Malware event Ransomware_Petya_1.bin NGFW Event Service Feb 26, 2021
- Malware event Ransomware_Petya_1.bin NGFW Event Service Sep 24, 2020
- Malware event Ransomware_Petya_1.bin NGFW Event Service Sep 03, 2020

Assigned to me - New (9)

- Malware event Ransomware_Petya.zip

Malware event Ransomware_Petya_1.bin

Investigate Incident Status Manage Incident Link

Malware event - Ransomware_Petya_1 bin:26b4699a7b9eeb16e76305d843d4ab05e94d43f3201436927e13b3ebafa90739

Open - Created By NGFW Event Service on 2021-02-25 19:26:59 UTC

Summary Observables Timeline Sightings Linked References (1)

Targets (1) - [Investigate these Targets](#)

192.168.44.150

Targeted by 5 unique observables, 5 times in the last 5 months

IP Address - 192.168.44.150

First: 2021-02-25T19:17:10.000Z Last: 2021-02-25T19:17:10.000Z

Incident Observables (5) - [Investigate these Observables](#)

26b4699a7b9eeb16e76305d843d4ab05e94d43f3201436927e13b3ebafa90739

Malicious SHA-256 - 1 Target - 1 Sighting

First: 2021-02-25T19:17:10.000Z Last: 2021-02-25T19:17:10.000Z

Info

Assignees - Add

- Jiri Tesar

Key Properties

- Categories: Select ...
- Disc. Method: NIPS
- Intend. Effect: Select ...
- Confidence: High
- TLP: Amber

Create New Incident

Investigate This Incident

Change Status

Link Reference

Download

jent-ddd30486-fb74-464a-b164-ce1a31f37c8e

0 / 2,238

Sort/Filter: 0

Malware event Ransomware_Petya_1.bin

NGFW Event Service - Feb 25, 2021 @ 20:20 CET

Malware event Ransomware_Petya_1.bin

Malware event - Ransomware_Petya_1.bin:26b4699a7b9eeb16e76305d843d4ab05e94d43f3201436927e13b3ebafa90739

Open - Created by NGFW Event Service on Feb 25, 2021 @ 20:25 CET

Summary Observables Timeline Sightings Linked References (1)

Sighting	Source/Sensor	Confid...	Severity	Enviro...	Resolu...	Obser...	Targets	Relatio...	...
Feb 25, 2021 @ 20:17 CET	NGFW Event Service...	High	High	Global	Detected	5	1	5	
<ul style="list-style-type: none"> Malware - Ransomware_Petya_1... <ul style="list-style-type: none"> Sighting Title Malware - Rans... 									

Description

Sighting Title Malware - Ransomware_Petya_1.bin:26b4699a7b9eeb16e76305d843d4ab05e94d43f3201436927e13b3ebafa90739:2f3338b0-0f17-47b4-952c-233e9923ae0e

Time 2021-02-25T19:17:10.000Z

Observed By thov.prglab.local

Source 192.168.44.150

Destination 192.168.42.150

FileDirection Download

SpersDisposition Spers detection perform...

FileAction Malware Block

5 Observables

IP 192.168.44.150

IP 192.168.42.150

SHA256 26b4699a7b9eeb16e76305d8...

Show more

1 Target

IP 192.168.44.150

5 Relations

IP 192.168.42.150 connected to IP 192.1...



SHA256 26b4699a7b9eeb16e76305d8...

IP 192.168.42.150 downloaded from SH...

Show more

First Seen: Feb 25, 2021 @ 20:17

Last Seen: Feb 25, 2021 @ 20:17

- 26b4699a7b9eeb16e76305d843...  
- Malware - Ransomware_Petya_1... - AMP Global Intellige...
- > There are 3 Verdicts for this observable.
[Investigate to learn more.](#)
- Add to current investigation
- Investigate in Threat Response
- Create Judgement
- AMP for Endpoints
- File trajectory
- Search for this SHA256
- Add SHA256 to custom detections SI...
- SecureX Orchestration
- Submit URL to Threat Grid
- AMP Host Isolation with Tier 2 Approval
- Move Computer to AMP Triage Group
- Take Forensic Snapshot and Isolate

Launch an investigation in Threat Response for this observable.

ASSIGNEES - Add

Jiri Tesar

KEY PROPERTIES

Categories: Select ...

Disc. Method: NIPS

Intend. Effect: Select ...

Confidence: High

TLP: Amber

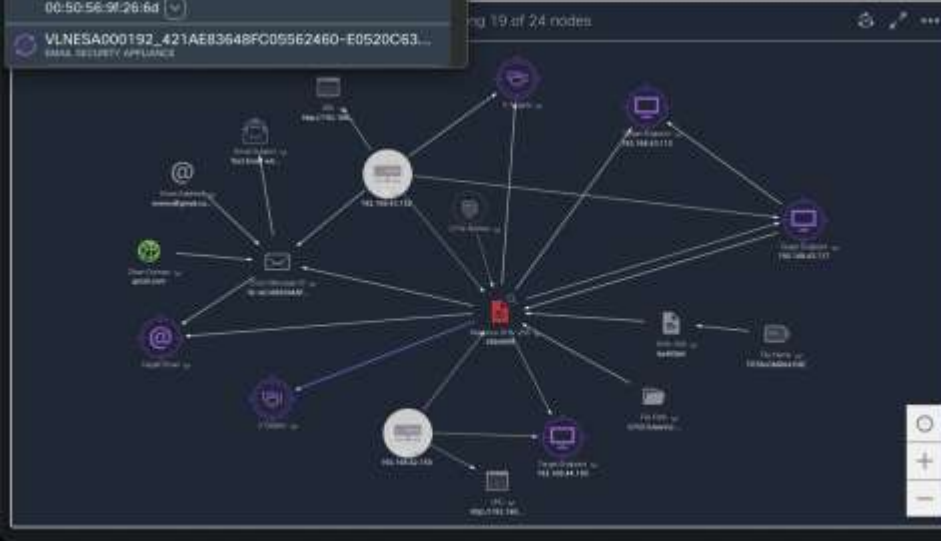
10 Targets 1 Investigated 0 Omitted 22 Related 6 Indicators 0 Modules

1 Network Gateway -> Endpoints - 1 Email Service - 1 Email

fmcv.prglab.local
 NETWORK GATEWAY
 AMP GUID: 122fe6db-3f5a-4106-b64f-52e4b8436c64
 HOSTNAME: fmcv.prglab.local

sec2-rdp
 WINDOWS / Endpoints
 AMP GUID: 9cf4e0ac-02d9-43cd-9f24-ac50091d6762
 HOSTNAME: sec2-rdp
 IP ADDRESS: 192.168.43.195
 MAC ADDRESS: 00:50:56:9f:26:6d

VLNESA000192_421AE83648FC05562460-E0520C63...
 EMAIL SERVICE / APPLIANCE



Details

sec2-rdp
Endpoint

fmcv.prglab.local
Network Gateway

VLNESA000192_421AE83648FC05562460-E0520C63...
Email Service

1 INVESTIGATED

26b4699a7b9e
Signatures My Environments

0 OMITTED

22 RELATED

122fe6db-3f5a-4106-b64f-52e4b8436c64
AMP GUID

71422a82-bbb-4106-b64f-52e4b8436c64
AMP GUID

sec2-rdp
Target Endpoint

Targeted by 1 unique observable, 3 times in the last 25 days
 Observed: Jun 29, 2021 @ 12:29 CEST - Jun 29, 2021 @ 12:30 CEST
 Hostname: sec2-rdp
 AMP GUID: 9cf4e0ac-02d9-43cd-9f24-ac50091d6762
 IP Address: 192.168.43.195
 MAC Address: 00:50:56:9f:26:6d

My Environment (3) Global (1)

Jun 29, 2021 @ 12:29:54 CEST - Jun 29, 2021 @ 12:30:15 CEST

● Malicious ● Suspicious ● Common ● Unknown ● Clean ● Targets

Signatures (3)

Add to Investigation ... **New Investigation** Snapshots ... 1 of 1 enrichments complete Automatic 3 Panel Layout

10 Targets 1 Investigated 0 Omitted 22 Related 6 Indicators 0 Modules



Graph

Disposition: All Types: All Mode: Simplified Showing 19 of 24 nodes

26b4699a7b9eeb16e76305d843d4ab05e94d43f3201436927e13b3ecafe90738

Malicious SHA-256 - AMP Global Intelligence...

There are 3 Verdicts for this observable. Investigate to learn more.

Investigate in Threat Response

Create Judgement

AMP for Endpoints

File trajectory

Search for this SHA256

Add SHA256 to custom detections Sk...

SecureX Orchestration

- Submit URL to Threat Grid
- AMP Host Isolation with Tier 2 Approval
- Move Computer to AMP Triage Group
- Take Forensic Snapshot and Isolate
- Take Orbital Forensic Snapshot

Details

26b4699a7b9... Malicious SHA-256 Hash

0 OMITTED

22 RELATED

122fe6db-3f5a-440b-8000-000000000000 AMP (5/0)

16-421AE836... Email Address

enemy@gmail.c... Email Address

jitesar@prglab.l... Email Address

26b4699a7b9eeb16e76305d843d4ab05...

Malicious SHA-256 Hash

My Environment (6) Global (63)

Jul 29, 2021 @ 12:29:54 CEST - Jul 29, 2021 @ 12:42:32 CEST

Time	Malicious	Suspicious	Common	Unknown	Clean	Targets
Jul 29, 2021 @ 12:29:54 CEST	2	1	0	0	0	0
Jul 29, 2021 @ 12:42:32 CEST	1	1	0	0	0	0

Judgements (66) Verdicts (3) Sightings (63) Indicators (0)

Judgements associate a disposition with an observable. Learn More

Search data Find ... Sort by Start Time Newest Filter by Current (66)

Dashboard

Dashboard Inbox Overview **Events** iOS Clarity

Filter: (New)

Select a Filter

Event Type Threat Detected

Group All Groups

Filters Computer: 9c4e0ac-02d9-43c0-9f24-ec50091d6762

Time Range 30 Days

Sort Time

Not Subscribed

Reset

Save Filter As

sec2-rdp detected c3c16b6d-7086-45de-9695-d73f59edbf0f.tmp	Win.Ransomware.Protected:W32.E908DCA957.Gen.A	Medium	Threat Detected	2021-06-29 12:32:38 CEST
sec2-rdp detected f_000f82	Win.Ransomware.Protected:W32.E908DCA957.Gen.A	Medium	Threat Detected	2021-06-29 12:32:38 CEST
sec2-rdp detected fddaaba9-756a-4449-8ec2-162339387d35.tmp	Win.Ransomware.Protected:W32.A6F10947D6.Gen.A	Medium	Threat Detected	2021-06-29 12:32:29 CEST
sec2-rdp detected f_000f81	Win.Ransomware.Protected:W32.A6F10947D6.Gen.A	Medium	Threat Detected	2021-06-29 12:32:29 CEST
sec2-rdp detected f_000f81	Win.Ransomware.Protected:W32.A6F10947D6.Gen.A	Medium	Threat Detected	2021-06-29 12:32:29 CEST
sec2-rdp detected Ransomware_Petya_1.bin	W32.Malwaregen:Petya.22kr.1201	Medium	Threat Detected	2021-06-29 12:29:54 CEST

File Detection	Detection	W32.Malwaregen:Petya.22kr.1201
Connector Details	Fingerprint (SHA-256)	29b4499a_afa00739
Comments	File Name	Ransomware_Petya_1.bin
	File Path	C:\Users\cisco\Downloads\Malware!!!\Ransomware_Petya_1.bin
	File Size	225.5 KB
	Parent Fingerprint (SHA-256)	6a465b00_29889771
	Parent Filename	TOTALCMD64.EXE
	Report 100	Restore File All Computers

View Updated Status

Add to Allowed Applications

File Trajectory

6 total events 20 / page

< 1 of 1 >

Export to CSV

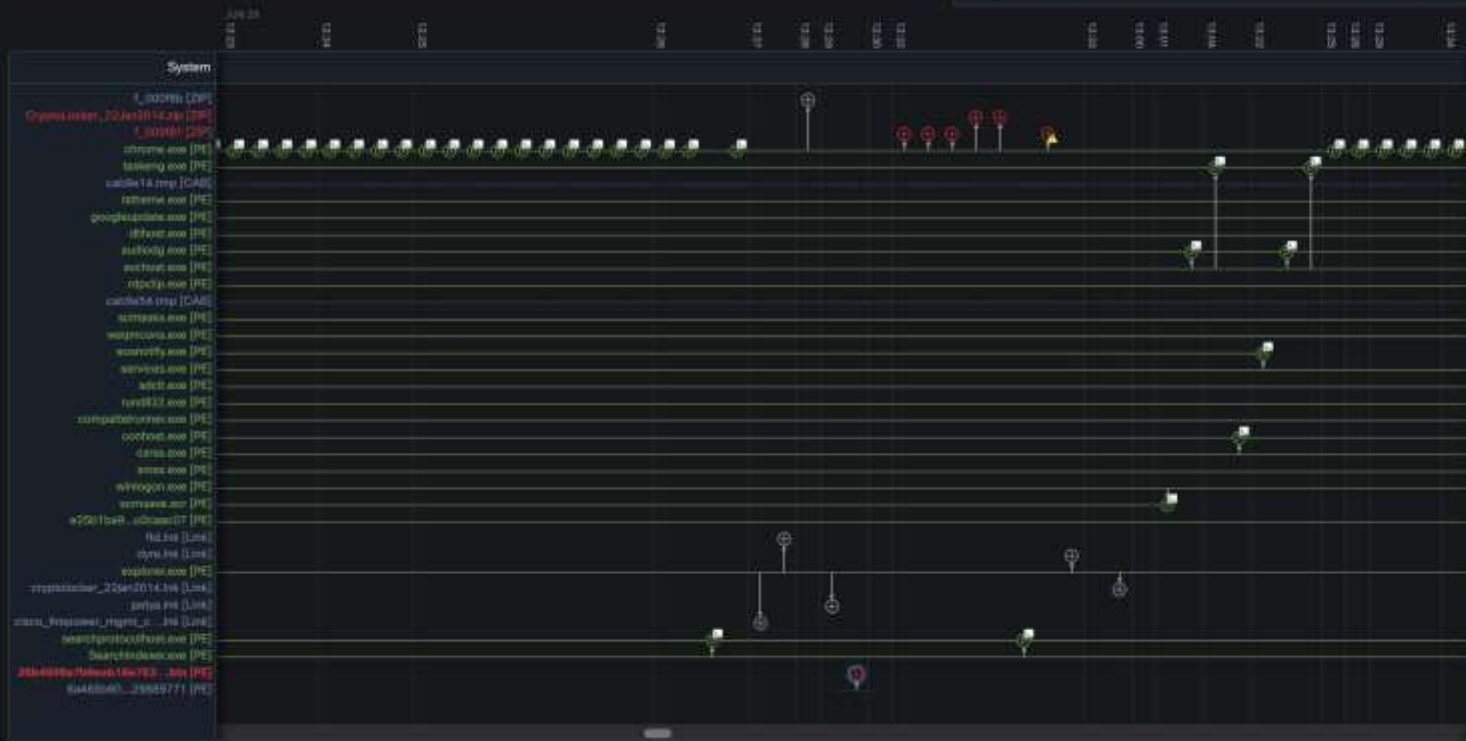


Device Trajectory

Take a Tour Share Use Legacy Device Trajectory

sec2-rdb in group JT prglab Protect Group 8 compromise events (spanning less than a ...)

Filters Search Device Trajectory



Event Details

Medium

2021-06-29 12:29:54 CEST

Detected **Ransomware_Petya_1.bin** (26b4696a...afa9c739 [PE_Executable]) as **W32/Malwaregen.Petya.Zho.1201**.

Created by TOTALCMD64.EXE (6a45b60...29885771 [Unknown]) executing as cisco@SEC2-RDP.

The file was quarantined.

File full path: C:\Users\cisco\Downloads\Malware\ff_Ransomware_Petya_1.bin

File SHA-1: 26b4696a70702c06b646334a0a6c4496

File MD5: 41273e46807ef0e446213267016

File size: 230912 bytes.

Parent file age: 0 seconds.

Parent process id: 5832.

Parent process SID: S-1-5-31-32167442-43443891-301474094-1006

Detected by the **Talos** engines.

We can integrate a lot of Partner platforms into SecureX

The image displays the 'Partner Security Tool' interface within the SecureX ecosystem. The interface is organized into a grid of cards, each representing a different partner platform. Each card includes a logo, a title, a brief description of the platform's capabilities, and two buttons: 'New Module' and 'Learn More'. The cards are arranged in rows and columns, with the first row containing 8 cards and subsequent rows containing 10 cards each. The background is dark blue with white text and icons.

Partner Security Tool

Row 1:

- SMA Web:** The SMA (Secure Mail Appliance) is a cloud-based email security solution that protects your organization's email from phishing, malware, and data loss.
- SecureX Orchestration:** SecureX Orchestration is a security orchestration platform that allows you to integrate and automate your security tools.
- SecureSwitch Cloud:** SecureSwitch Cloud is a cloud-based network security solution that protects your organization's network from threats.
- SecureSwitch Enterprise:** SecureSwitch Enterprise is a cloud-based network security solution that protects your organization's network from threats.
- Threat Grid:** Threat Grid is a cloud-based threat intelligence platform that provides real-time threat intelligence to your organization.
- Threat Grid (deprecated):** Threat Grid (deprecated) is a cloud-based threat intelligence platform that provides real-time threat intelligence to your organization.
- Unit42:** Unit42 is a cloud-based threat intelligence platform that provides real-time threat intelligence to your organization.
- Web Security Appliance:** The Web Security Appliance (WSA) is a cloud-based web security solution that protects your organization's web traffic from threats.

Row 2:

- Apptio:** Apptio is a cloud-based data management and analytics platform that helps you optimize your data and improve your business performance.
- AbuseIPDB IP Checker:** AbuseIPDB IP Checker is a cloud-based IP address reputation service that helps you identify and block malicious IP addresses.
- Akamai:** Akamai is a cloud-based content delivery network (CDN) and cloud security provider that helps you protect your website and applications from threats.
- Alembic Open Threat Exchange:** The Alembic Open Threat Exchange (OTX) is a cloud-based threat intelligence platform that provides real-time threat intelligence to your organization.
- Arcotek GuardDuty:** Arcotek GuardDuty is a cloud-based threat intelligence platform that provides real-time threat intelligence to your organization.
- Avast:** Avast is a cloud-based security solution that provides real-time threat intelligence to your organization.
- CyberCrime Tracker:** CyberCrime Tracker is a cloud-based threat intelligence platform that provides real-time threat intelligence to your organization.
- Cloudfire:** Cloudfire is a cloud-based security solution that provides real-time threat intelligence to your organization.
- Fortinet Security DRAGON:** Fortinet Security DRAGON is a cloud-based security solution that provides real-time threat intelligence to your organization.

Row 3:

- Genesys Services Relay:** Genesys Services Relay is a cloud-based security solution that provides real-time threat intelligence to your organization.
- Gigamon ThreatINSIGHT:** Gigamon ThreatINSIGHT is a cloud-based security solution that provides real-time threat intelligence to your organization.
- Google Chrome:** Google Chrome is a cloud-based security solution that provides real-time threat intelligence to your organization.
- Google Safe Browsing:** Google Safe Browsing is a cloud-based security solution that provides real-time threat intelligence to your organization.
- Graylog:** Graylog is a cloud-based security solution that provides real-time threat intelligence to your organization.
- How I Been Pwned:** How I Been Pwned is a cloud-based security solution that provides real-time threat intelligence to your organization.
- IBM XI-Force Exchange:** IBM XI-Force Exchange is a cloud-based security solution that provides real-time threat intelligence to your organization.
- IPFiring:** IPFiring is a cloud-based security solution that provides real-time threat intelligence to your organization.
- MSP:** MSP is a cloud-based security solution that provides real-time threat intelligence to your organization.

Row 4:

- Microsoft Graph Security API:** Microsoft Graph Security API is a cloud-based security solution that provides real-time threat intelligence to your organization.
- Microsoft Graph Security API:** Microsoft Graph Security API is a cloud-based security solution that provides real-time threat intelligence to your organization.
- Pal-Wi Networks AutoPro:** Pal-Wi Networks AutoPro is a cloud-based security solution that provides real-time threat intelligence to your organization.
- Pulsar:** Pulsar is a cloud-based security solution that provides real-time threat intelligence to your organization.
- Quake IOC:** Quake IOC is a cloud-based security solution that provides real-time threat intelligence to your organization.
- Resilient Cloud DDoS Protection:** Resilient Cloud DDoS Protection is a cloud-based security solution that provides real-time threat intelligence to your organization.
- Resilient Cloud WAF Service:** Resilient Cloud WAF Service is a cloud-based security solution that provides real-time threat intelligence to your organization.
- Recorded Future:** Recorded Future is a cloud-based security solution that provides real-time threat intelligence to your organization.
- SecureX CISA Relay:** SecureX CISA Relay is a cloud-based security solution that provides real-time threat intelligence to your organization.

Row 5:

- SecurityTrails:** SecurityTrails is a cloud-based security solution that provides real-time threat intelligence to your organization.
- ServiceNow Security Incident:** ServiceNow Security Incident is a cloud-based security solution that provides real-time threat intelligence to your organization.
- Shodan:** Shodan is a cloud-based security solution that provides real-time threat intelligence to your organization.
- Signal Sciences Next-Gen:** Signal Sciences Next-Gen is a cloud-based security solution that provides real-time threat intelligence to your organization.
- Stigint Darkfeed:** Stigint Darkfeed is a cloud-based security solution that provides real-time threat intelligence to your organization.
- Spikr Relay Module:** Spikr Relay Module is a cloud-based security solution that provides real-time threat intelligence to your organization.
- SpyCloud Account Takeover:** SpyCloud Account Takeover is a cloud-based security solution that provides real-time threat intelligence to your organization.
- Sumo Logic Log Manager:** Sumo Logic Log Manager is a cloud-based security solution that provides real-time threat intelligence to your organization.
- Threatcore | Cyberprotect:** Threatcore | Cyberprotect is a cloud-based security solution that provides real-time threat intelligence to your organization.

Row 6:

- VisualTotal:** VisualTotal is a cloud-based security solution that provides real-time threat intelligence to your organization.
- alphaMountain Threat Int.:** alphaMountain Threat Int. is a cloud-based security solution that provides real-time threat intelligence to your organization.
- uriscan.io:** uriscan.io is a cloud-based security solution that provides real-time threat intelligence to your organization.

Orchestration is easy to use “SDK” opened for any scenario of usage

The screenshot displays the Argo CD workflow editor interface. The main workspace shows a workflow diagram with the following steps:

- Start node (circle)
- Task: **CTRGenerateAccessToken** (Atomic)
- Task: **CTRListActions** (Atomic)
- Task: **Create Approval Request** (Task)
- Task: **Send Email** (Email)
- Task: **Wait for Approval** (Task)
- Decision node: **WAS THE REQUEST APPROVED?** (Yes/No)
- Task: **CTR Trigger an Action** (Atomic, inside a 'Yes' branch)
- End node (circle)

The right-hand panel shows the configuration for the workflow:

PROPERTIES
AMP HOST ISOLATION WITH TIER 2 APPROVAL

Variables

NAME	TYPE	SCOPE	VALUE	REQUIRED
AMPmode	String	Local	AMP for Endpoints	False
observability_type	String	Input		True
observability_value	String	Input		True

Triggers

NAME	TYPE	STATUS
+ ADD TRIGGER		

Target

TARGET TYPE: Select

No-Target

Execute On This Target

TARGET:

Specify Target On Workflow Start

Execute On This Target Group

Default targetGroup:

Left sidebar: Search and Filter, Webhook Teams - Send Message to User, DATABASE, EMAIL, FILE OPERATIONS, GOOGLE CLOUD PLATFORM, HERAKL, MICROSOFT WINDOWS, PYTHON, SNMP, SERVICE NOW, Service Now - Add Work Note to Incident, Service Now - Create Incident, TABLE, TASK, TERMINAL, TERRAFORM, UNIX/LINUX SYSTEM, WEB SERVICE, HTTP Request, Swagger HTTP Request.

NOVÝ FIREPOWER 3100 JE TADY!

- ▶ 10.5. – TechClub webinar
- ▶ 25.5. – Pro partnery, jen fyzicky – Golden Gate
- ▶ 26.5. – Pro zákazníky, jen fyzicky – Golden Gate





SECURE