


CISCO
SECURE

 CISCO The bridge to possible

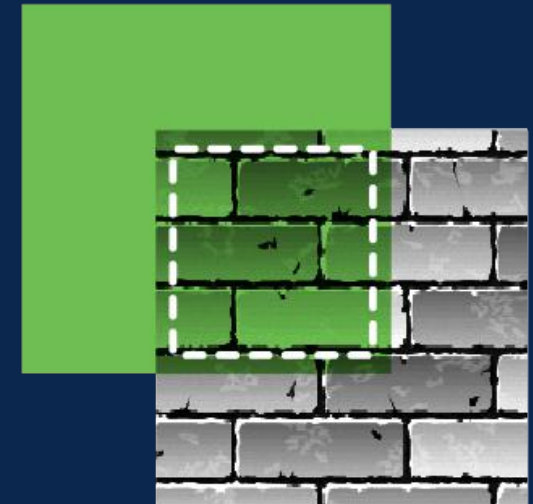
Cisco Secure Firewall

Tech Club

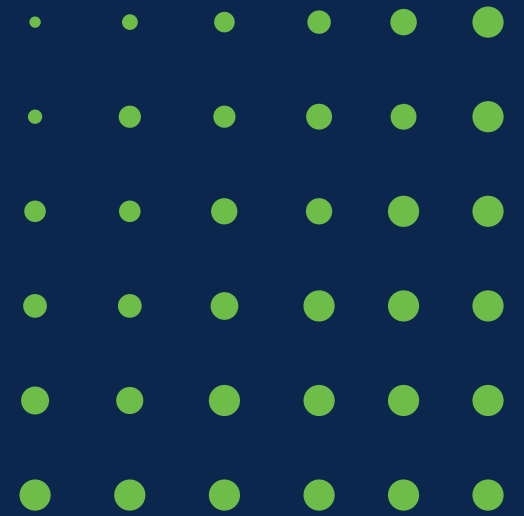
Jiří Tesař

TSA, jitesar@cisco.com

27.7.2021



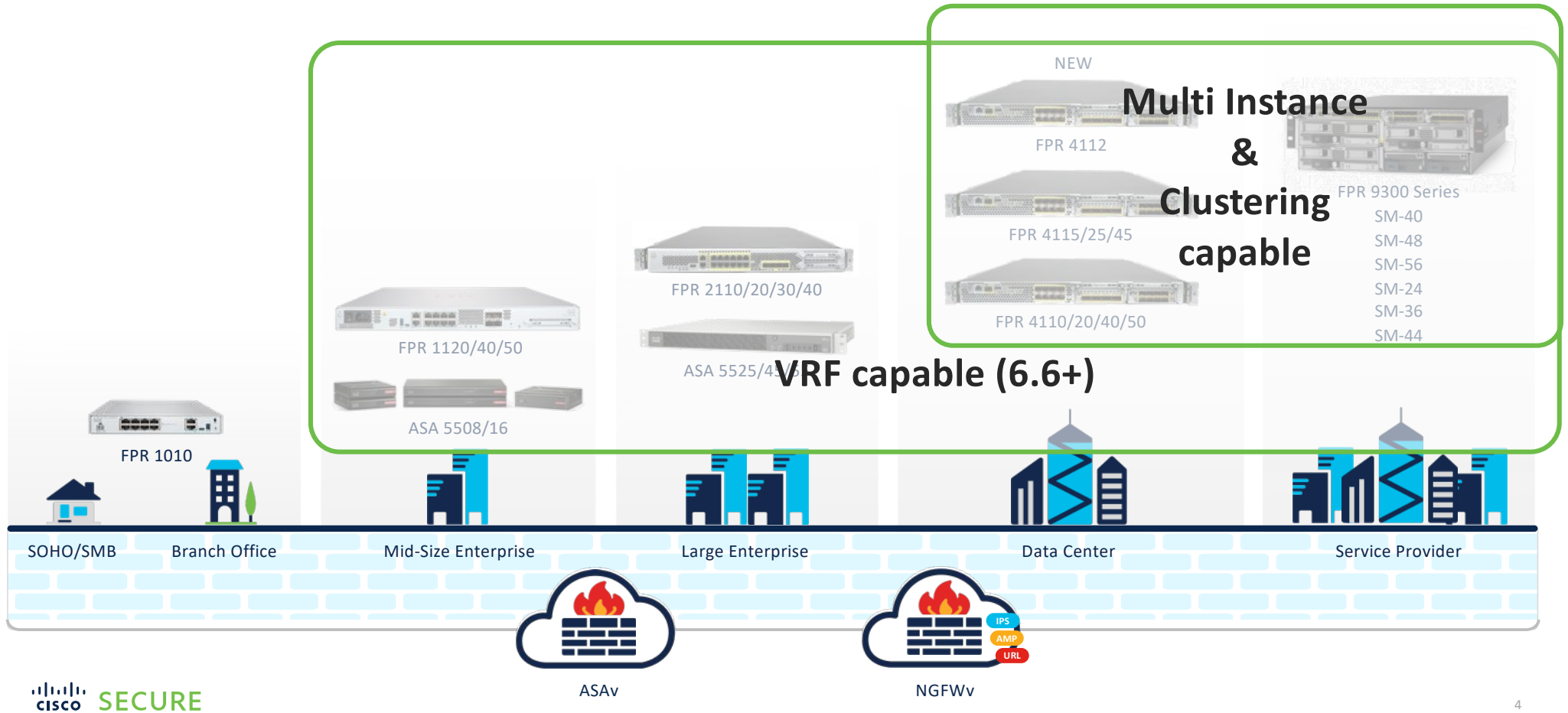
Secure Firewall Platforms



Secure Firewall Portfolio



Cisco Secure Firewall portfolio



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	1000

Current Challenges

Demands

Scalable and Elastic

Programmable

Resilient

Current Challenges

Scaling

- Smart Load-balancing
- Custom metric tracking
- Resiliency and statefulness

Config management

- Initial config
- Config sync
- Consolidated tracking

Monitoring

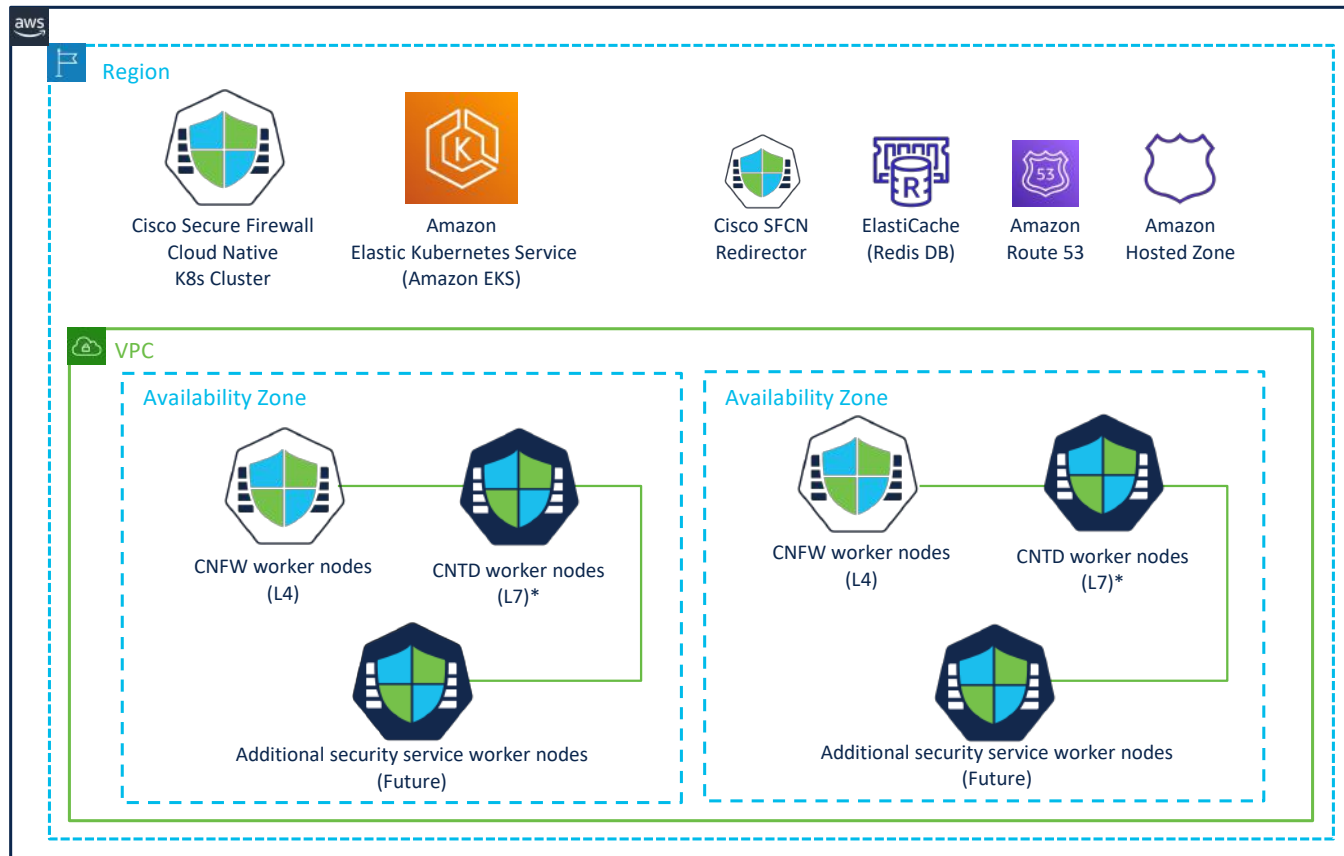
- Troubleshooting
- Event consolidation

Automation

- Independent deployment (iaC)
- Integration



Cisco Secure Firewall Cloud Native Platform for AWS



* L7 service is planned for release CY22H1

- Scalable architecture
(Horizontal Pod Autoscaler - HPA)
- Modular security architecture
- K8s orchestrated deployments
(Amazon EKS)
- DevOps friendly
(YAML + CI/CD + GitOps)
- CRDs and Helm Charts
- Config management
(REST API/YAML/CDO UI)
- Data externalization (Redis)
for stateless services
- Multi-region and multi-AZ support
- Multi-tenant aware
- Bring your own license (BYOL)
- CNFW footprint
4 core

Secure Firewall Cloud Native

Enabling the cloud transition



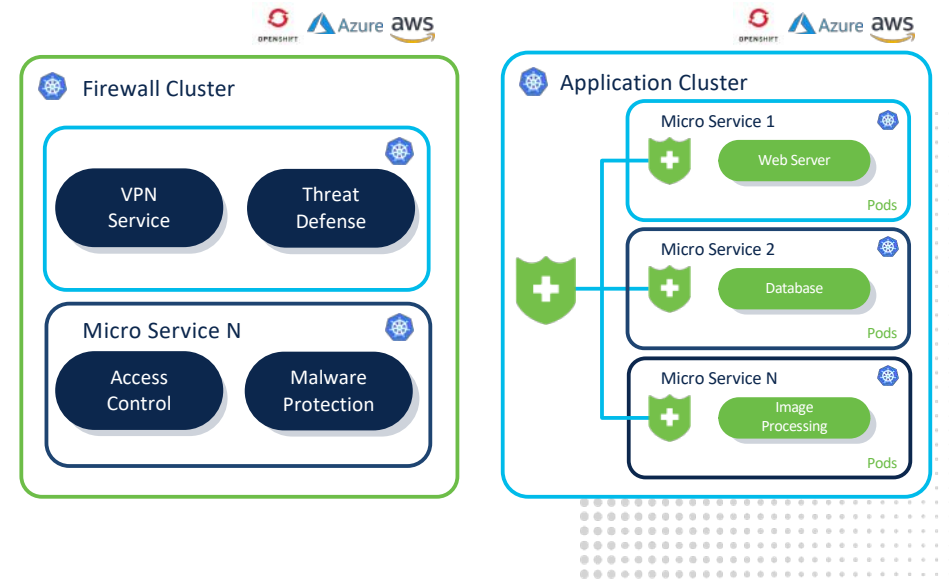
Easily deliver **firewall services** with massive scale and resiliency in cloud environments



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*

* FCS in May 2021 in AWS EKS, followed by Azure and OpenShift this Fall

Resources

- SFCN CCO page: <http://cs.co/SFCN>
- SFCN At-a-Glance: <http://cs.co/SFCN-at-a-glance>
- Cisco blog on SFCN
 - Technical Blog: <http://cs.co/SFCN-blog>
 - Blog: <http://cs.co/SFCN-business-blog>
- SFCN Marketplace Listing: <http://cs.co/SFCN-aws-listing>
- SFCN GitHub: <https://github.com/CiscoDevNet/sfcn>

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



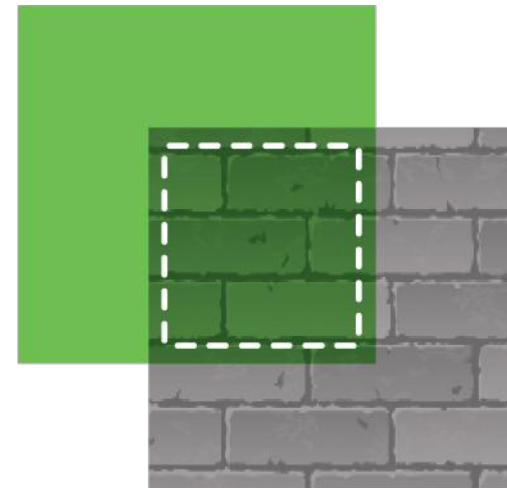
More connections

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



Improved encrypted traffic throughput

- Up to 3x boost in encrypted traffic performance



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+

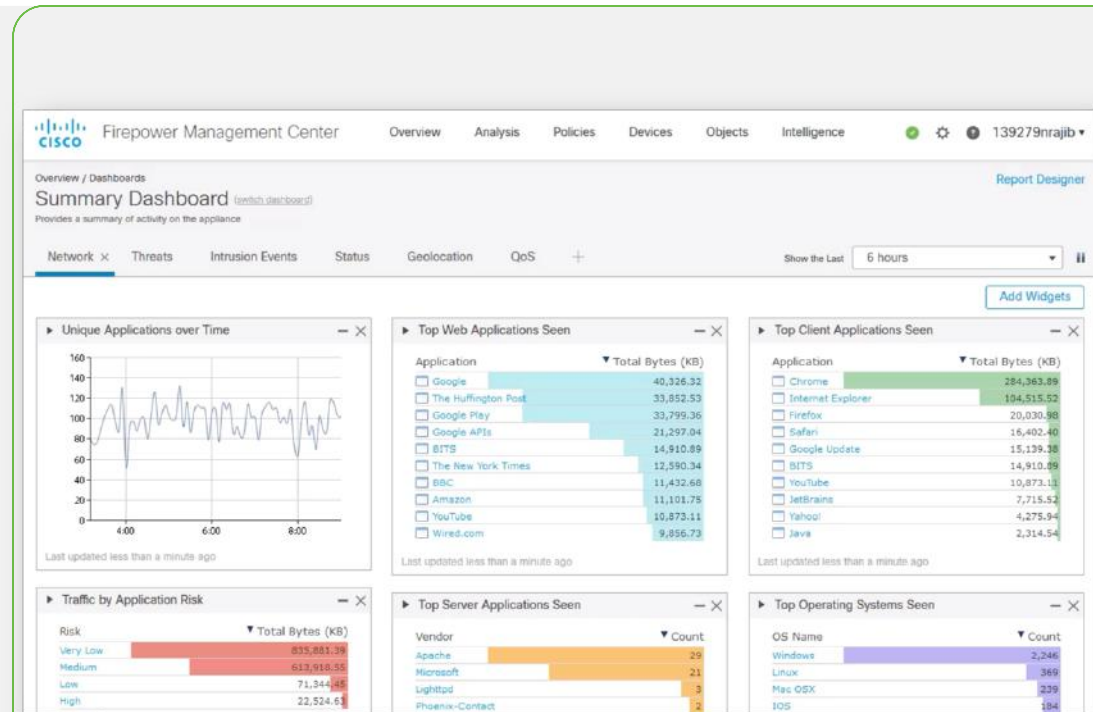


3 new 9300 SM models:
SM-40, SM-48, SM-56
up to **153 Gbps** Firewall throughput*

*1024B FW+AVC+IPS

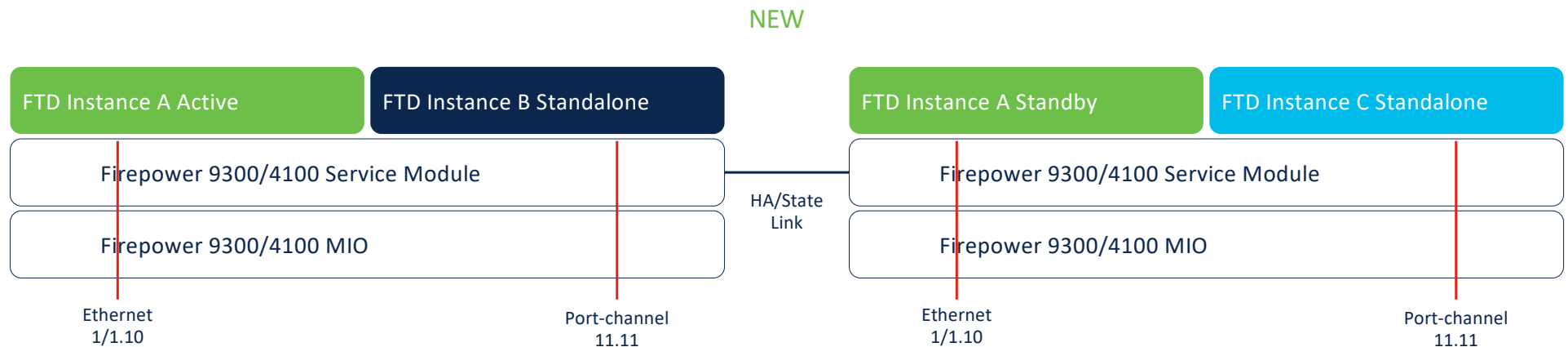
FMC Virtual 300

- 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
- Supported software releases:
 - FTD 6.5 or higher – including multi-instance
 - FMC 6.5 or higher



Multi-Instance Expands Deployment Options

- Install multiple FTD logical devices on a single module or appliance
 - Container architecture
 - Instance failure does not affect other instances
- Allows tenant management separation, independent instance upgrade
- Supports HA between identical instances on different physical devices
- Example: 54 instances on a FPR9300 chassis with 3 x SM-56 modules
- Improved crypto acceleration in hardware



Clustering

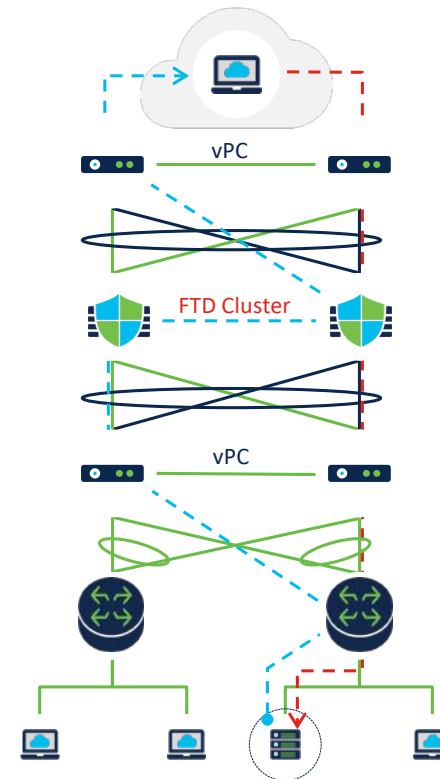
Drive high return on investment while maintaining high availability

- Combine multiple devices to make a single scalable logical device
- Scale as you grow
 - Scale throughput, concurrent and new connection
 - Can span multiple datacenters
- N+1 resilience
- Handles asymmetric traffic seamlessly

Example: 6 node cluster created by 2 x FPR9300 fully loaded chassis (with SM-56)

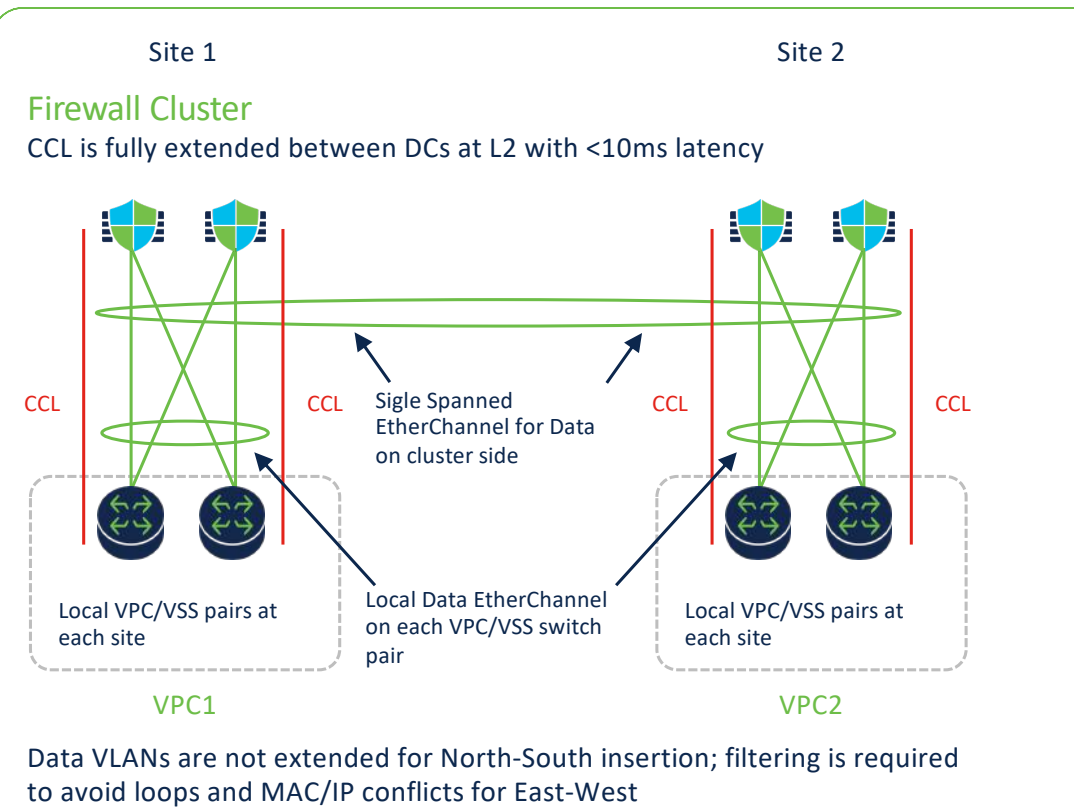
336 Gbps AVC

307 Gbps AVC+IPS



Multi-Site Data Center

- North-South insertion with LISP inspection and owner reassignment
- East-West insertion for first hop redundancy with VM mobility

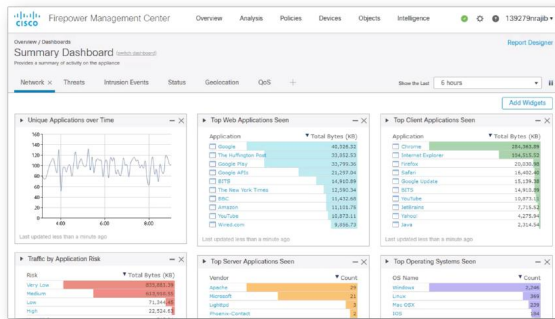


Management Designed for the User

Flexibility of Cloud or on-premises options

Security Integrations

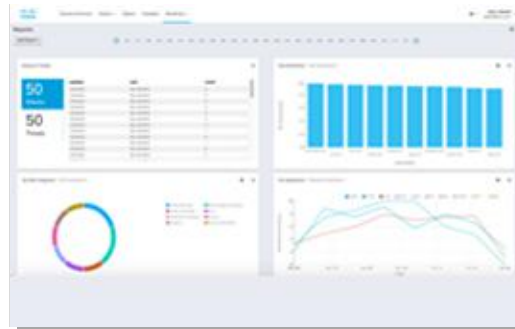
Firewall Management Center



On premise centralized manager
SecOps focused

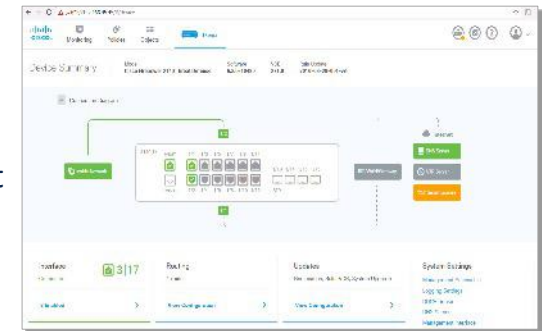
Common APIs

Cisco Defense Orchestrator



Cloud-based centralized manager
NetOps focused

Cisco Firewall Device Manager (FDM)



On-box manager
NetOps focused

Coexist

Management Platforms: When to Position?

Use case	Managers of choice	Details
Internet edge	CDO or FMC	<ul style="list-style-type: none">• Cisco Defense Orchestrator for ease of use and netops users• FMC for advanced security analytics• Ask your customer about their priority
Enterprise branch	CDO or FMC	<ul style="list-style-type: none">• FTD can connect to Cisco Defense Orchestrator directly through the data interface• Low-touch onboarding
SMB / Small Business Edition	CDO or FDM	<ul style="list-style-type: none">• FDM or Cisco Defense Orchestrator provide greater usability• CDO is recommended for multiple firewall management
Data center Edge / Core	FMC	<ul style="list-style-type: none">• FMC supports 4100 and 9300, clustering, TrustSec
Campus fabric	FMC	<ul style="list-style-type: none">• FMC supports 4100 and 9300, clustering, TrustSec
Firewall running in public cloud	FMC	<ul style="list-style-type: none">• FMC supports Firewall in AWS and Azure
IPS only	FMC	<ul style="list-style-type: none">• FMC supports all the advanced IPS features and provides a separate interface from the Firewall

What is Firewall Management Center (FMC)?

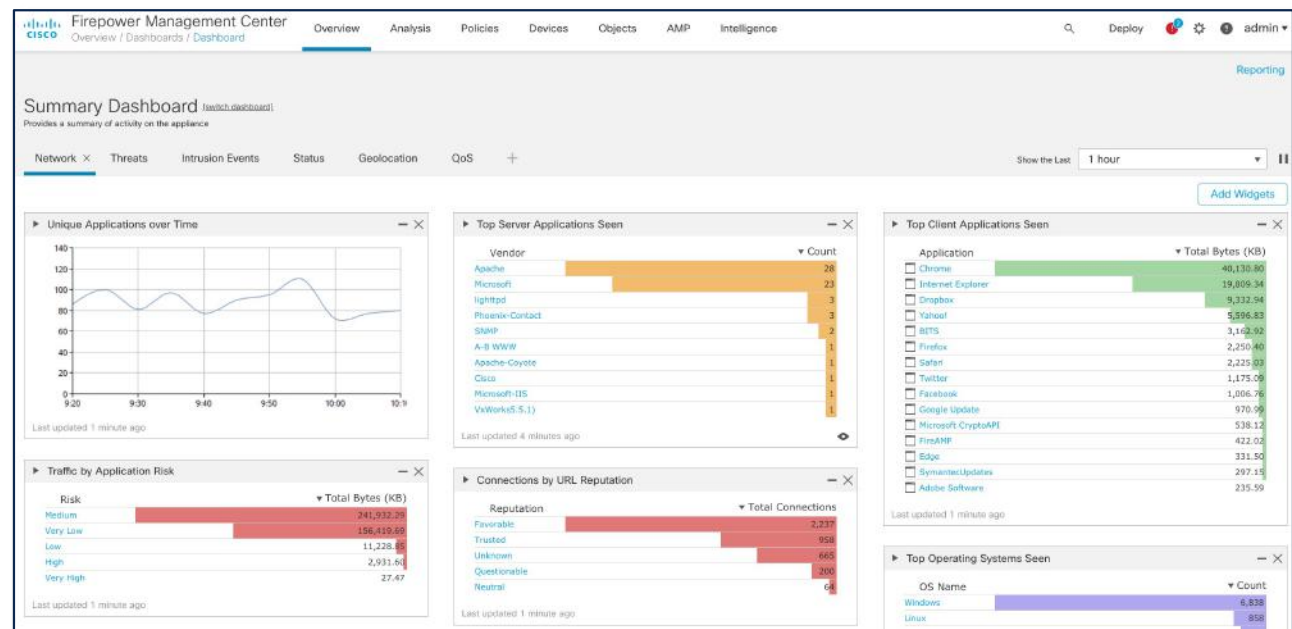
On-premise, centralized management for multi-site deployments

• Key Benefits

- Manage across many sites
- Control access and set policies
- Investigate incidents
- Prioritize response
- Available in physical and virtual options

• Features


- Multi-domain management
- Role-based access control
- High availability
- APIs and pxGrid integration
- Policy & device management
- Endpoint
- Security intelligence



FMC REST API

API Explorer

[https://\[FMC IP\]/api/api-explorer/](https://[FMC IP]/api/api-explorer/)

 Cisco Firepower Management Center - API Explorer logout

API INFO

FMC Version: 6.2.3
(build 84)

Policy Services

Policy

Domains Global

API CONSOLE

`/api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169-6d9ed49b625f/policy/accesspolicies`

Identifier for access control policy.

+ query parameter

Content-Type Header application/json

Accept Header application/json

DELETE

[Response Text](#) [Response Info](#)

[Request Info](#)

API INFO

Audit

Deployment

Device Groups

Device HA Pairs

Devices

Object

Policy

Policy Assignments

Status

System Information

Implementation Notes

[Examples](#)

Parameters

Parameter	Required	Description	Type	Data Type
<code>objectId</code>	<code>true</code>	Identifier for access control policy.	<code>path</code>	<code>string</code>

Response

Response Content Type application/json

Response Object `AccessPolicy`



FTD REST API

API Explorer

Error Catalog

TRY IT OUT!

Hide Response

Curl

```
curl -X GET --header 'Accept: application/json' 'https://192.168.43.183/api/fdm/v4/policy/intrusionpolicies'
```

Request URL

```
https://192.168.43.183/api/fdm/v4/policy/intrusionpolicies
```

Response Body

```
{
  "items": [
    {
      "version": "eme2gofltkcif",
      "name": "Maximum Detection",
      "description": "Maximum Detection Layer",
      "rules": {
        "links": {
          "self": "https://192.168.43.183/api/fdm/v4/policy/intrusionpolicies/206e5d90-a8c8-11e9-aac1-67bf391e0d45/intrusionrules"
        }
      },
      "id": "206e5d90-a8c8-11e9-aac1-67bf391e0d45",
      "type": "intrusionpolicy",
      "links": {
        "self": "https://192.168.43.183/api/fdm/v4/policy/intrusionpolicies/206e5d90-a8c8-11e9-aac1-67bf391e0d45"
      }
    },
    {
      "version": "ldbyvez737mdw",
      "name": "Connectivity Over Security",

```

Response Code

```
200
```

Response Headers

FMC REST API Examples

Health status, health policy, licenses allocated for particular firepower,...

https://{FMC IP}/api/fmc_config/v1/domain/{Domain ID}/devices/devicerecords/{Device ID}

```
{
  "id": "f3e05e96-3880-11ea-9e48-ffc21568cd01",
  "type": "Device",
  "links": {
    "self": "https://192.168.43.133/api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169-6d9ed49b625f/devices/devicerecords/f3e05e96-3880-11ea-9e48-ffc21568cd01"
  },
  "name": "ftdv66.prglab.local",
  "description": "NOT SUPPORTED",
  "model": "Cisco Firepower Threat Defense for VMWare",
  "modelId": "A",
  "modelName": "75",
  "modelType": "Sensor",
  "healthStatus": "green",
  "sw_version": "6.6.0",
  "healthPolicy": {
    "id": "85b17b0a-387e-11ea-8cce-953bf222dbdb",
    "type": "HealthPolicy",
    "name": "Initial_Health_Policy 2020-01-16 16:37:44"
  },
  "advanced": {
    "enableOGS": true
  },
  "hostName": "192.168.43.134",
  "license_caps": [
    "URLFilter",
    "MALWARE",
    "BASE",
    "THREAT"
  ],
  "keepLocalEvents": false,
  "prohibitPacketTransfer": false,
  "ftdMode": "ROUTED",
  "metadata": {
    "readOnly": {
      "state": false
    }
  },
  "inventoryData": {
    "cpuCores": "1 CPU (4 cores)",
    "cpuType": "CPU Xeon E5 series 2800 MHz",
    "memoryInMB": "8192"
  },
  "domain": {
    "name": "Global",
    "id": "e276abec-e0f2-11e3-8169-6d9ed49b625f",
    "type": "Domain"
  },
  "isPartOfContainer": false,
  "isMultiInstance": false
}
```

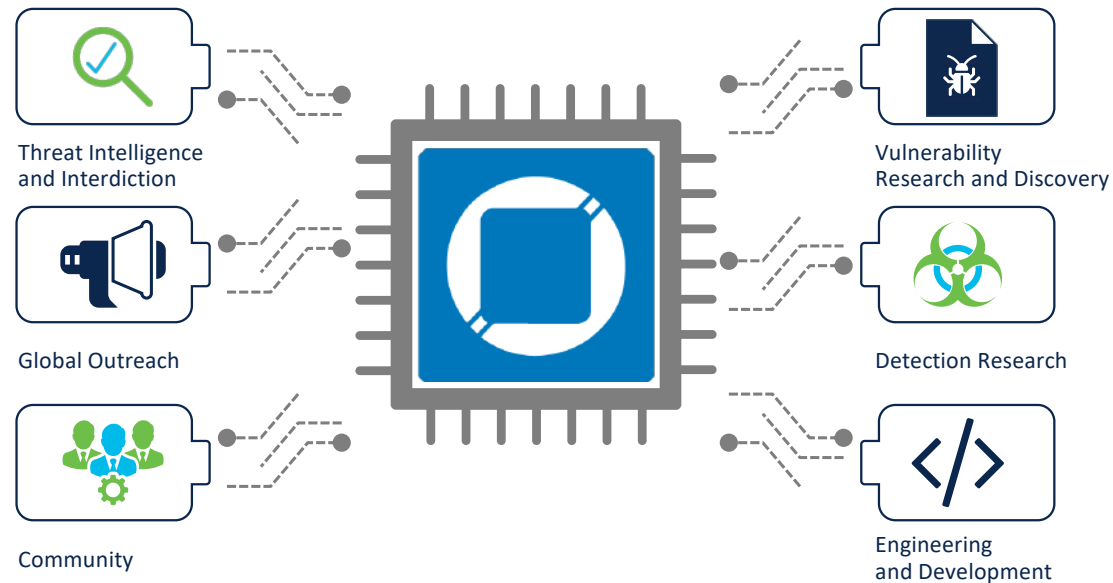
REST API outputs from FMC/FTD 6.6

Talos

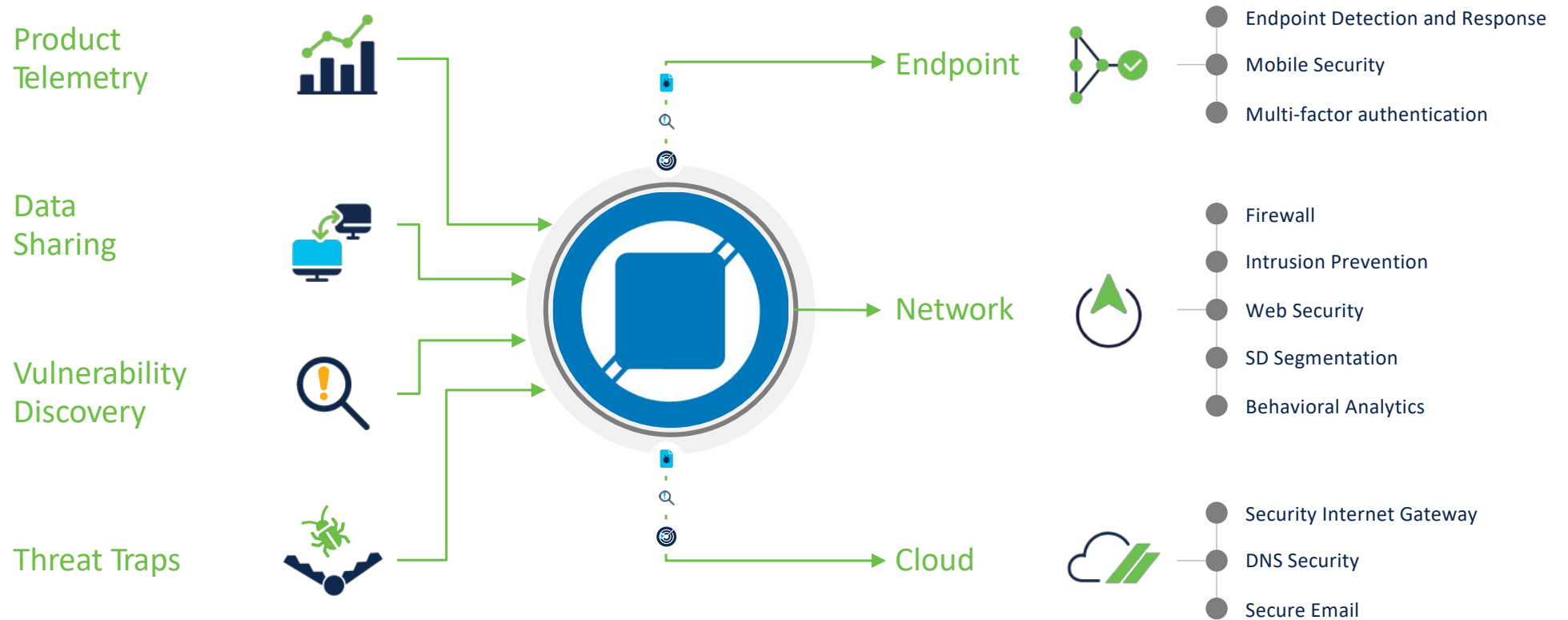


What is Talos?

Talos is the threat intelligence group at Cisco. We are here to fight the good fight — we work to keep our customers, and users at large, safe from malicious actors.



From Unknown to Understood



Backed by the industry's best threat intelligence



Web/URL



Network Analysis



Email



Malware/Endpoint



DNS/IP



Network Intrusions



300+
threat intel researchers;
24 – 7 – 365



Millions
of telemetry agents



4
Global data centers



Over 100 Threat intelligence
partners

iiiooo ooiooo ioiooooo io io io oo ooio ooio oo
iiiooo ooiooo ioioooo ooio ooioooo io ooiooo oo ooiooo
ooiooo ooiooo ioiooo ooiooo ooiooo ooiooo ooiooo io oo



ooiooo ooiooo ooiooo ooiooo ooiooo ooiooo ooiooo
ooiooo ooiooo ooiooo ooiooo ooiooo ooiooo ooiooo
iiiooo ooiooo ooiooo ooiooo ooiooo ooiooo ooiooo
ooiooo ooiooo ooiooo ooiooo ooiooo ooiooo ooiooo
ooiooo ooiooo ooiooo ooiooo ooiooo ooiooo ooiooo



180 billion
Daily DNS requests



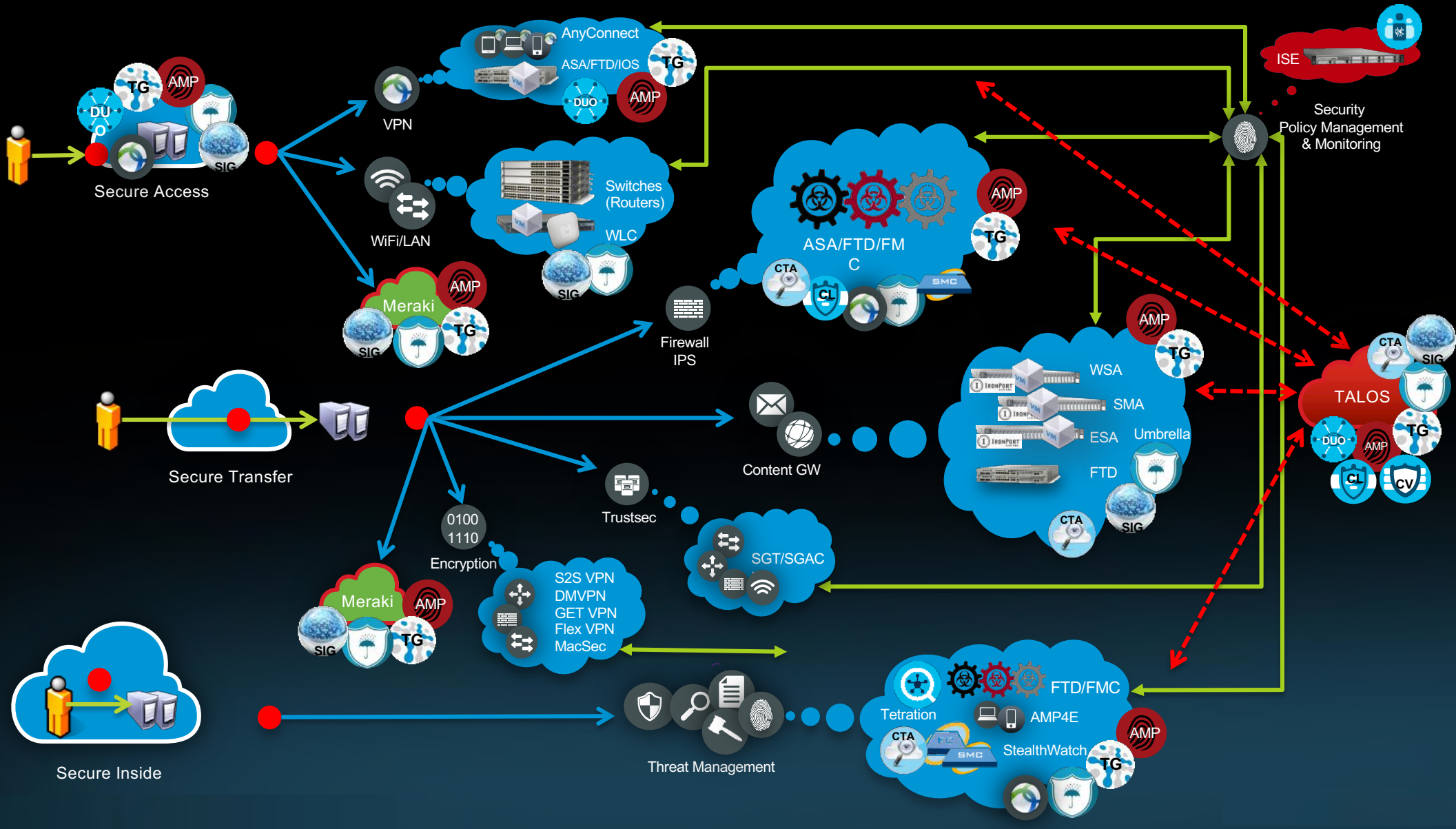
1.5 million
Daily malware samples



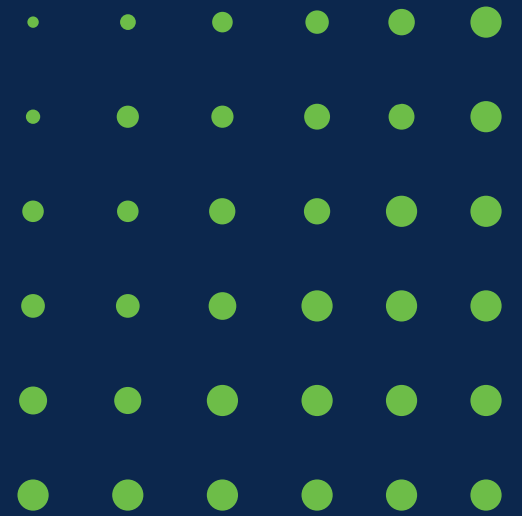
600 billion
Daily email messages



16 billion
Daily web requests

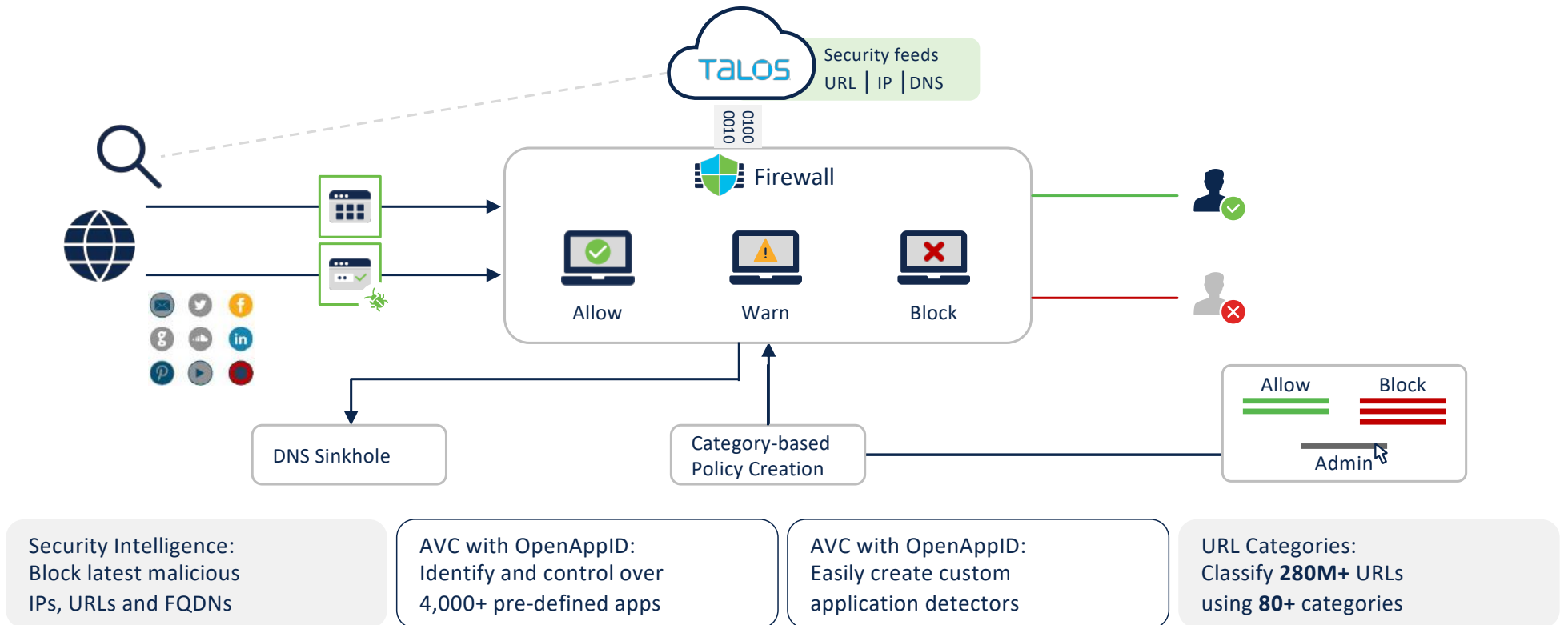


Secure Firewall Threat Defense



Firewall Policy Powered by Talos and OpenAppID

Control traffic based on IP, URL, FQDN, or application



Network Discovery

Provides the right data, at the right time, in the right format

- Discovers applications, users, and hosts through passive analysis of network traffic
- Provides context and helps determine the impact of attacks
- Tune IPS signature sets to devices discovered on the network
- Update host profiles with 3rd party vulnerability management integration

The screenshot displays a network discovery tool interface with several sections:

- Servers (3):** A table listing protocols and ports. The data is as follows:

Protocol	Port	Application Protocol	Vendor and Version
tcp	139	pending	
udp	0	IGMP	
tcp	80	HTTP	
- Applications (1):** A table listing application protocols and clients. The data is as follows:

Application Protocol	Client	Version	Web Application
NetBIOS-dgrm	NetBIOS-dgrm		
- User History:** A table showing user activity. The data is as follows:

Users	2020-01-12 11:31:21	2020-01-13 11:31:21
malik pennington (D\CLOUD-SOC\ypenn, LDAP)		
vicente vanbuskirk (D\CLOUD-SOC\pvanb, LDAP)		
maureen cepeda (D\CLOUD-SOC\scepe, LDAP)		
diane tibbott (D\CLOUD-SOC\dtibbott, LDAP)		
chassidy francisco (D\CLOUD-SOC\hfran, LDAP)		
garth harrington (D\CLOUD-SOC\aharr, LDAP)		
oula gruber (D\CLOUD-SOC\sgrub, LDAP)		
joy shanklin (D\CLOUD-SOC\jshan, LDAP)		
cherilyn spicer (D\CLOUD-SOC\ispic, LDAP)		
misty pagano (D\CLOUD-SOC\apaga, LDAP)		
elmira shih (D\CLOUD-SOC\eshih, LDAP)		
julian ibarra (D\CLOUD-SOC\oibar, LDAP)		
laurine gibb (D\CLOUD-SOC\ygibb, LDAP)		
jaclyn parris (D\CLOUD-SOC\inparr, LDAP)		
takako collado (D\CLOUD-SOC\icoll, LDAP)		
collin carlson (D\CLOUD-SOC\wcarl, LDAP)		
lavenia cohn (D\CLOUD-SOC\lcohn, LDAP)		
rochell gaspar (D\CLOUD-SOC\vgasp, LDAP)		
- Host Profile:** A detailed view of a host with the following information:
 - Domain: Global \ Cisco_Backend \ Cisco_SOC
 - IP Addresses: 10.0.10.151
 - NetBIOS Name: NGIPSV.dcloud.cisco.com (1)
 - Device (Hops): NGFW.dcloud.cisco.com (128)
 - MAC Addresses (TTL): 00:0C:29:03:DF:AD (VMware, Inc.) (128), 00:0C:29:61:F5:5F (VMware, Inc.) (128), 00:10:45:CE:A7:2B (Nortel Networks) (128)
 - Host Type: Host
 - Last Seen: 2020-01-13 10:31:46
 - Current User: sean crowley (D\CLOUD-SOC\vcrow, LDAP)
- Indications of Compromise (1):** A table showing a detected malware event:

Category	Event Type	Description	First Seen	Last Seen
Malware Detected	Threat Detected in File Transfer	The host has encountered malware	2020-01-13 07:39:38	2020-01-13 07:39:38
- Operating System:** A table showing the operating system details:

Vendor	Product	Version	Source
Microsoft	Windows	8.1	Firepower





Secure IPS

Reduce the noise/volume of events and prioritize administration

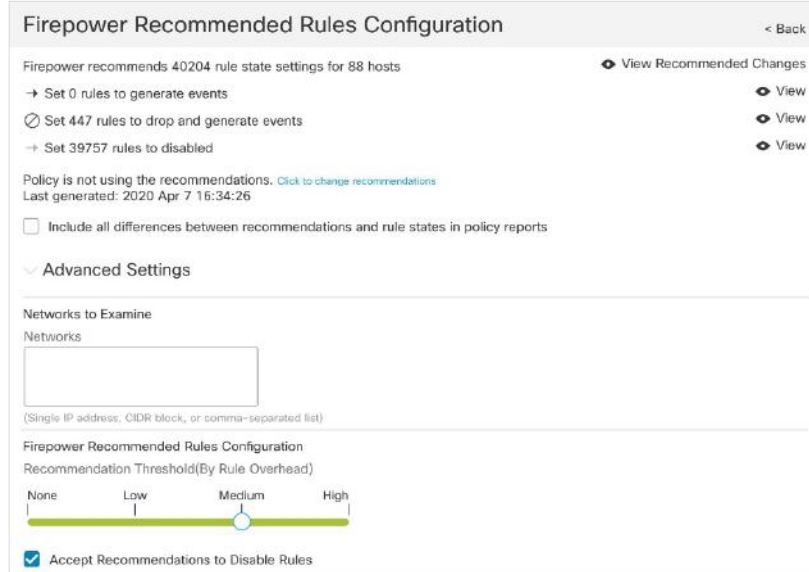
Powered by Snort 3 – Best of breed, open source IPS

Firewall brings the power of context to IPS

Impact of IPS events can be deduced.

Impact flag	Administrator action	Why
1 	Act immediately, Vulnerable	Event Corresponds to vulnerability mapped to host
2 	Investigate, Potentially Vulnerable	Relevant port open or protocol in use but no vuln mapped
3 	Good to know, Currently Not available	Relevant port not open or protocol not in use
4 	Good to know, Unknown Target	Monitored network but unknown host
0 	Good to know, Unknown Network	Unmonitored network

Firewall recommendation can tune IPS.



The screenshot shows the 'Firepower Recommended Rules Configuration' interface. It displays a summary of recommendations for 88 hosts, including: 'Set 0 rules to generate events', 'Set 447 rules to drop and generate events', and 'Set 39757 rules to disabled'. There are 'View' links for each of these items. Below the summary, there is a section for 'Advanced Settings' with a 'Networks to Examine' field. At the bottom, there is a 'Recommendation Threshold (By Rule Overhead)' slider set to 'Medium' and a checked box for 'Accept Recommendations to Disable Rules'.

Correlate Host Profile and IPS

Drive impact analysis and rule recommendations

Host Profile Scan Host Generate White List Profile

IP Addresses: 10.1.112.42
 NetBIOS Name:
 Device (Hosts): FTD (2)
 MAC Addresses (TTL): 00:01:24:56:9B:CF (Acer Incorporated) (128)
 00:04:00:81:81:D0 (LEXMARK INTERNATIONAL, INC.) (254)
 00:04:F2:E7:3E:52 (Polycom) (64)
 ... (show all)

Host Type: Host
 Last Seen: 2020-04-07 16:15:47
 Current User: kennedy.larson (dcloud.cisco.com|klarson, LDAP)
 View: [Context Explorer](#) | [Connection Events](#) | [Intrusion Events](#) | [File Events](#) | [Malware Events](#)

▼ **Indications of Compromise (3)** Edit Rule States Mark All Resolved

Category	Event Type	Description	First Seen	Last Seen
Malware Detected	Threat Detected in File Transfer	The host has encountered malware	2020-04-07 13:51:41	2020-04-07 13:51:41
Exploit Kit	Intrusion Event - exploit-kit	The host may have encountered an exploit kit	2020-04-07 13:51:40	2020-04-07 13:51:40
Impact: 1 Attack	Impact: 1 Intrusion Event - attempted-admin	The host was attacked and is likely vulnerable	2020-04-07 13:51:40	2020-04-07 13:51:40

▼ **Operating System** Edit Operating System

Vendor	Product	Version	Source
Microsoft	Windows	Vista, 7, Server 2008	Firepower

Applications (14)

Application Protocol	Client	Version	Web Application
<input type="checkbox"/> BitTorrent	<input type="checkbox"/> BitTorrent		
<input type="checkbox"/> HTTP	<input type="checkbox"/> Chrome	44.0.2403.107	Q, CNET Download
<input type="checkbox"/> HTTP	<input type="checkbox"/> Internet Explorer	9.0	Q, Catala



Impact flag	Administrator action	Why
1	Act immediately, Vulnerable	Event Corresponds to vulnerability mapped to host
2	Investigate, Potentially Vulnerable	Relevant port open or protocol in use but no vuln mapped
3	Good to know, Currently Not available	Relevant port not open or protocol not in use
4	Good to know, Unknown Target	Monitored network but unknown host
0	Good to know, Unknown Network	Unmonitored network

Firepower Recommended Rules Configuration Back

Firepower recommends 40204 rule state settings for 88 hosts View Recommended Changes

- Set 0 rules to generate events View
- Set 447 rules to drop and generate events View
- Set 39757 rules to disabled View

Policy is not using the recommendations. [Click to change recommendations](#)
 Last generated: 2020 Apr 7 16:34:25

Include all differences between recommendations and rule states in policy reports

Advanced Settings

Networks to Examine

Networks:

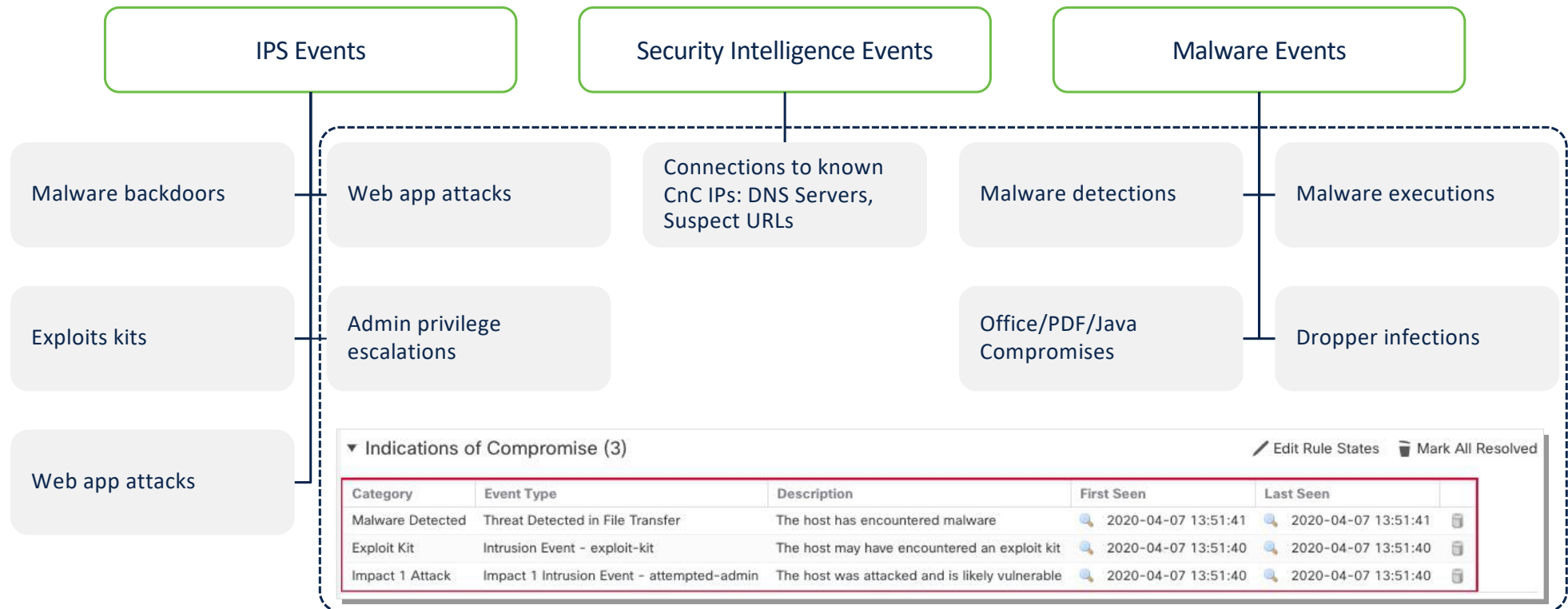
(Single IP address, CIDR block, or comma-separated list)

Firepower Recommended Rules Configuration
 Recommendation Threshold (By Rule Overhead)

None Low Medium High

Accept Recommendations to Disable Rules

Indications of Compromise (IoCs) Events

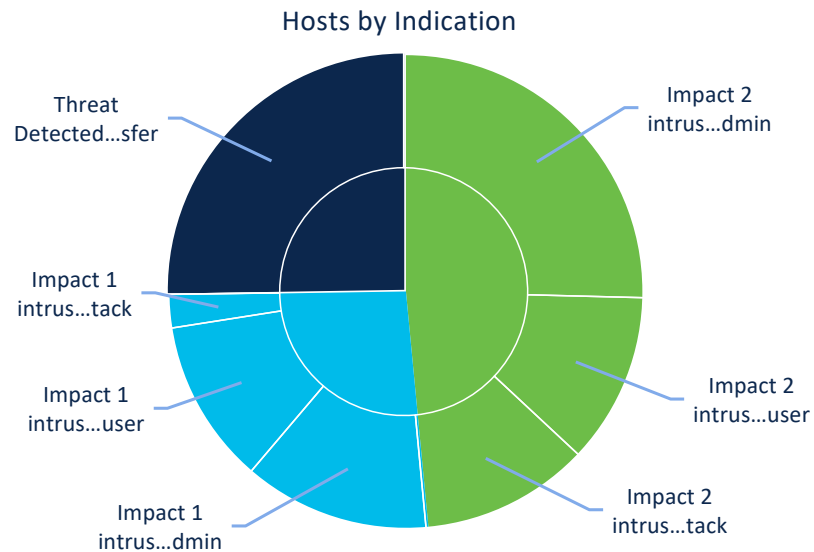


IoCs Facilitate Remediation

Facilitate understanding and remediation to reduce impact

- Identifies compromised and potentially compromised systems
- Take automatic action through **Cisco Rapid Threat Containment**

Indications of Compromise



Host Profile

IP Addresses: 10.1.112.42

NetBIOS Name: FTD (2)

Device (Hops): FTD (2)

MAC Addresses (TTL): 00:01:24:56:9B:CF (Acer Incorporated) (128), 00:04:00:81:81:D0 (LEXMARK INTERNATIONAL, INC.) (254), 00:04:F2:E7:3E:52 (Polycom) (64), ... (show all)

Host Type: Host

Last Seen: 2020-04-07 16:15:47

Current User: kennedy.larson (dcloud.cisco.com)\kjarson, LDAP

View: [Context Explorer](#) | [Connection Events](#) | [Intrusion Events](#) | [File Events](#) | [Malware Events](#)

Indications of Compromise (3)

Category	Event Type	Description	First Seen	Last Seen
Malware Detected	Threat Detected in File Transfer	The host has encountered malware	2020-04-07 13:51:41	2020-04-07 13:51:41
Exploit Kit	Intrusion Event - exploit-kit	The host may have encountered an exploit kit	2020-04-07 13:51:40	2020-04-07 13:51:40
Impact 1 Attack	Impact 1 Intrusion Event - attempted-admin	The host was attacked and is likely vulnerable	2020-04-07 13:51:40	2020-04-07 13:51:40

Operating System

Vendor	Product	Version	Source
Microsoft	Windows	Vista, 7, Server 2008	Firepower

Applications (14)

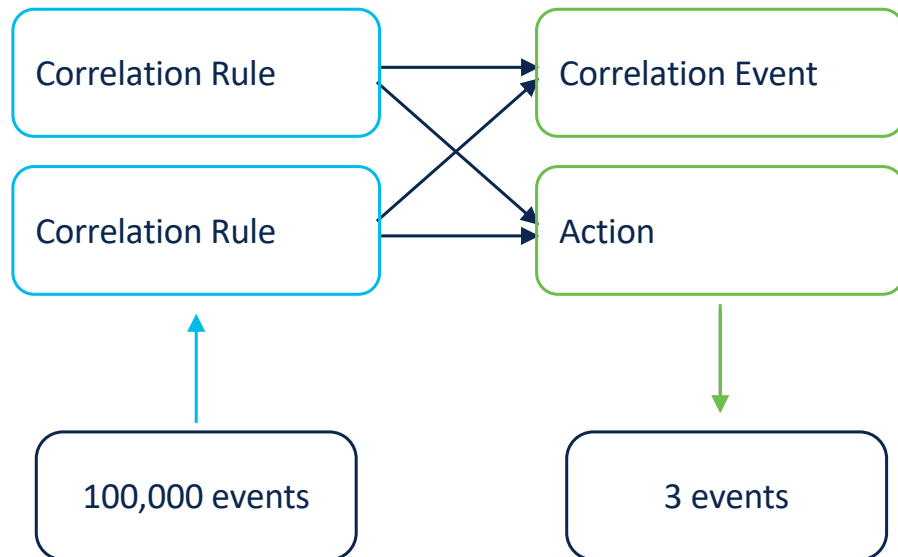
Application Protocol	Client	Version	Web Application
<input type="checkbox"/> BitTorrent	<input type="checkbox"/> BitTorrent		
<input type="checkbox"/> HTTP	<input type="checkbox"/> Chrome	44.0.2403.107	<input type="checkbox"/> CNET Download
<input type="checkbox"/> HTTP	<input type="checkbox"/> Internet Explorer	9.0	<input type="checkbox"/> Casale

FMC: Automate Security Response

Reduce the noise and connect the dots

- Correlate Security events
- Trigger automated response
 - Email
 - Syslog
 - SNMP
 - Remediation module
- Integration with Secure Network Access and other Cisco/3rd party products

Correlation Policy



Protect Your Network Using AMP

Understand the motion and behavior of files through network and endpoint visibility.

Breadth and Control points

Email Endpoints Web Network IPS Devices

Threat Visibility

Retrospective Detection Behavioral IoCs File Trajectory Threat Hunting

Telemetry Stream

File and Network I/O

Process Information

File Fingerprint and Metadata

Talos and Malware Analytics Intelligence

Trajectory

10:57 17:40 18:06 18:10 18:14 18:17

10.4.10.183 10.5.11.8 10.3.4.51 10.5.60.66

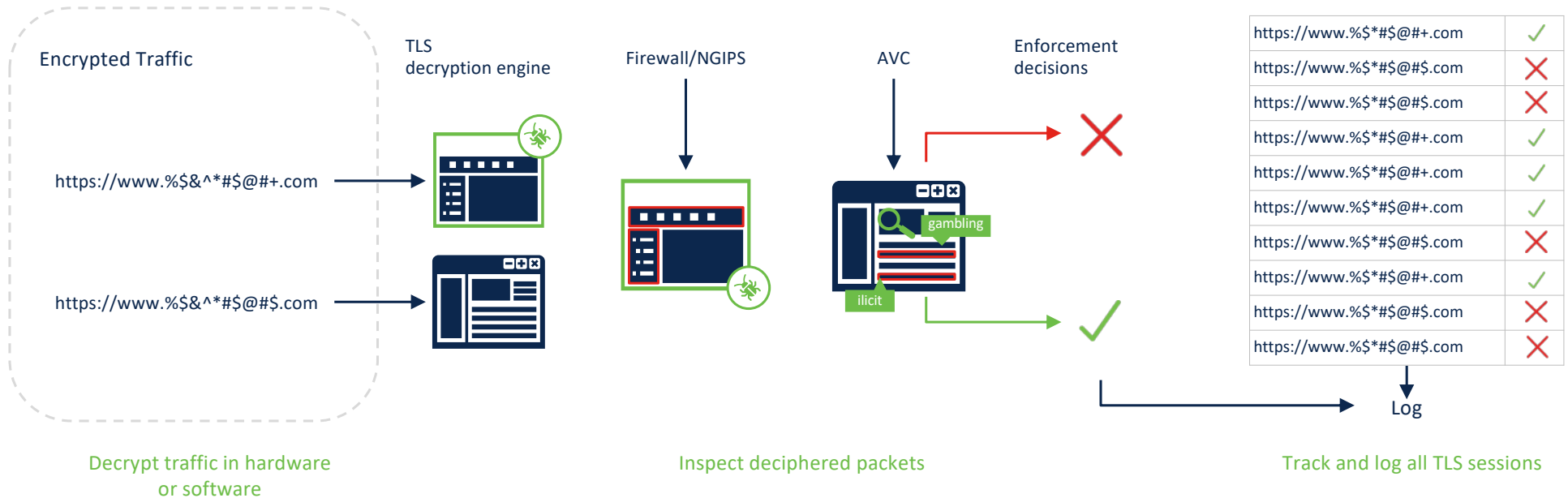
Events Transfer Block Create Move Execute Scan Retrospective Quarantine

Dispositions Unknown Malware Clean Custom Unavailable

Integrated TLS Decryption

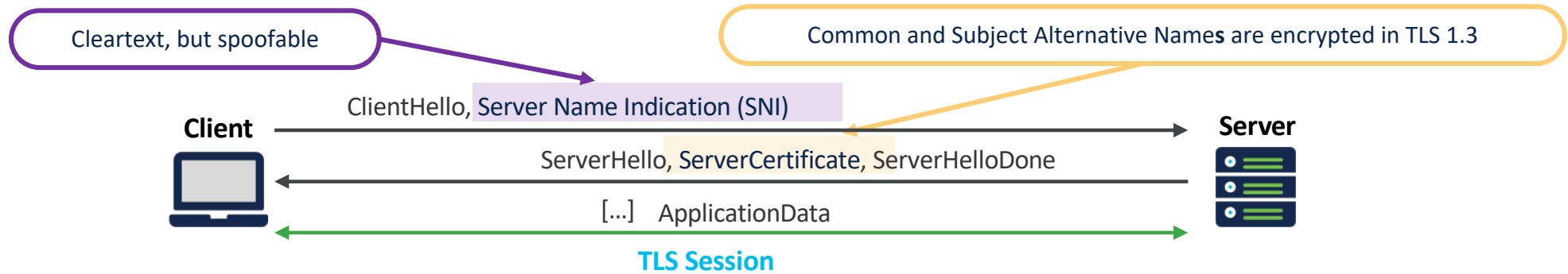
Finds encrypted threat while reducing performance impact

- TLS hardware acceleration delivers high-performance inspection of encrypted traffic
- Centralized enforcement of TLS certificate policies
 - Examples: Blocking self-signed encrypted traffic, specified TLS version, cypher suites

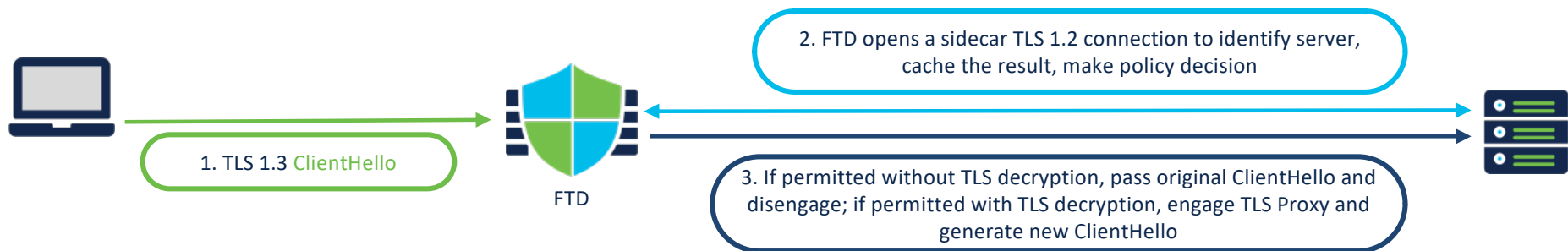


Fast App and URL Actions with TLS 1.3

AVC, URL, and Decryption Policy decisions on pre-1.3 TLS header



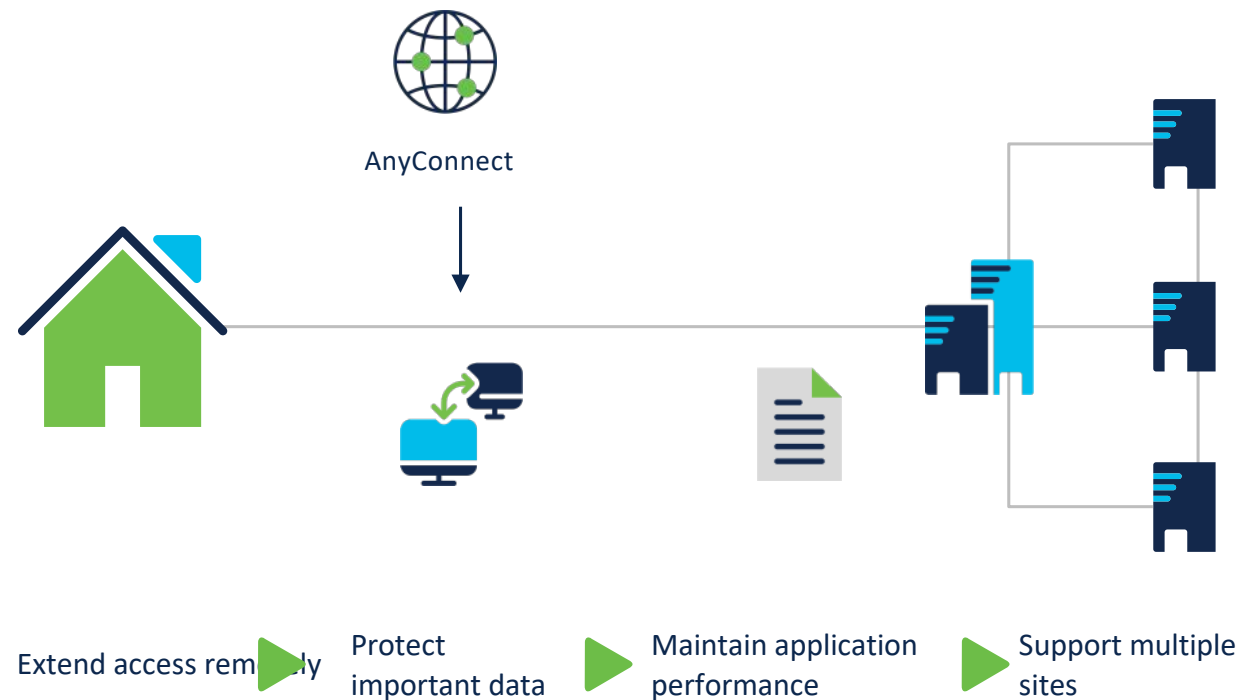
TLS Server Identity Discovery without decryption since **FTD 6.7**



Remote Access VPN with Secure Access by Duo

Provide ubiquitous secure access from remote and roaming users

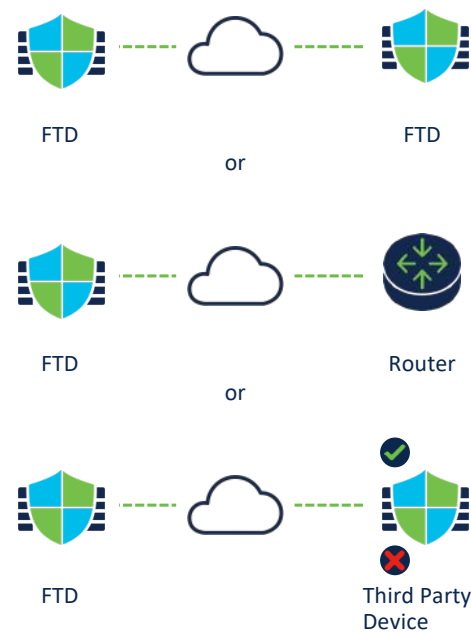
- Posture assessment
- Uses TLS, DTLS or IKEv2
- Easy wizard-based configuration
- Integration with LDAP and RADIUS
- Identity based security policies
- Enhanced security with 2 FA/MFA provided by Secure Access (Duo)



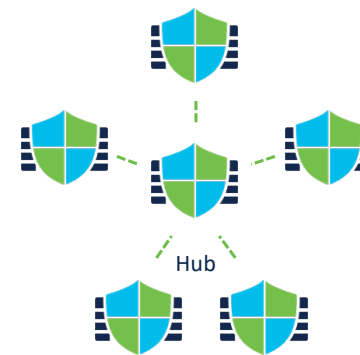
Site-to-Site VPN

Easily and securely interconnect remote sites

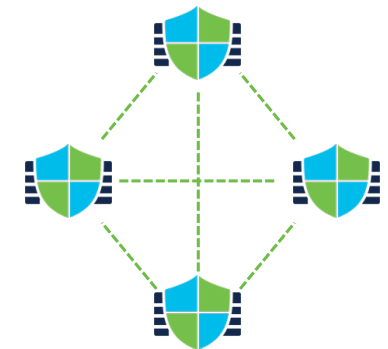
- IKEv1/IKEv2 policy-based VPN
- Easy topology-based management of VPN on multiple peers
 - Point-to-point
 - Hub and Spoke
 - Full Mesh
- Flexible authentication options – pre-shared key (automatic) and certificates



Point-to-Point



Hub and Spoke

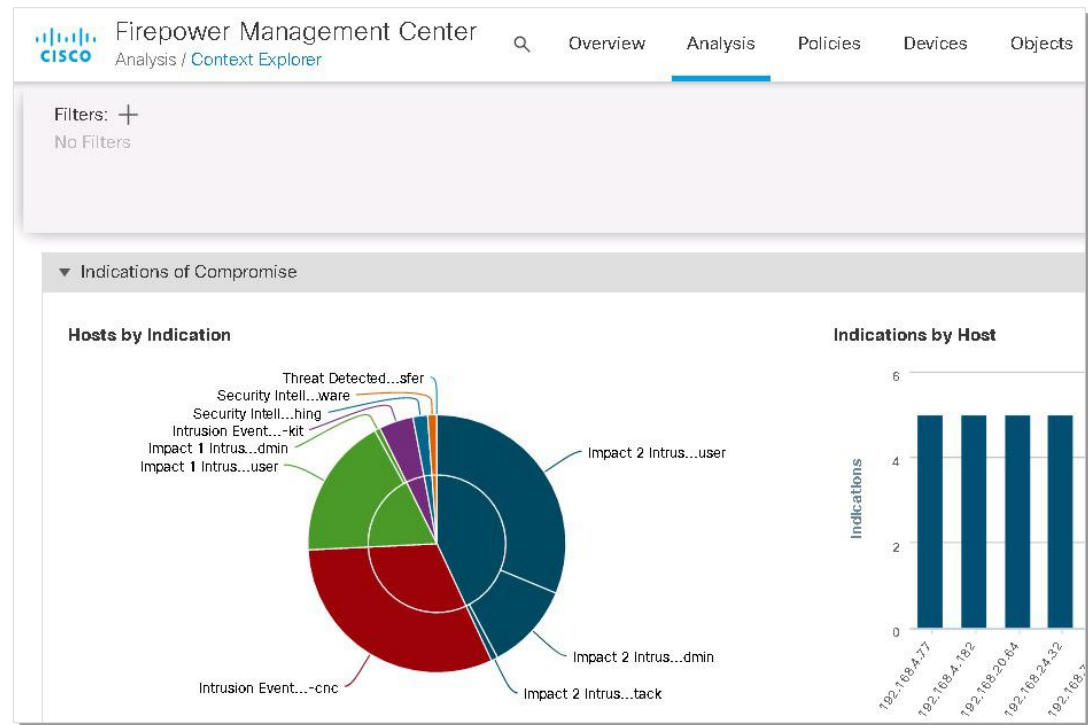


Full Mesh

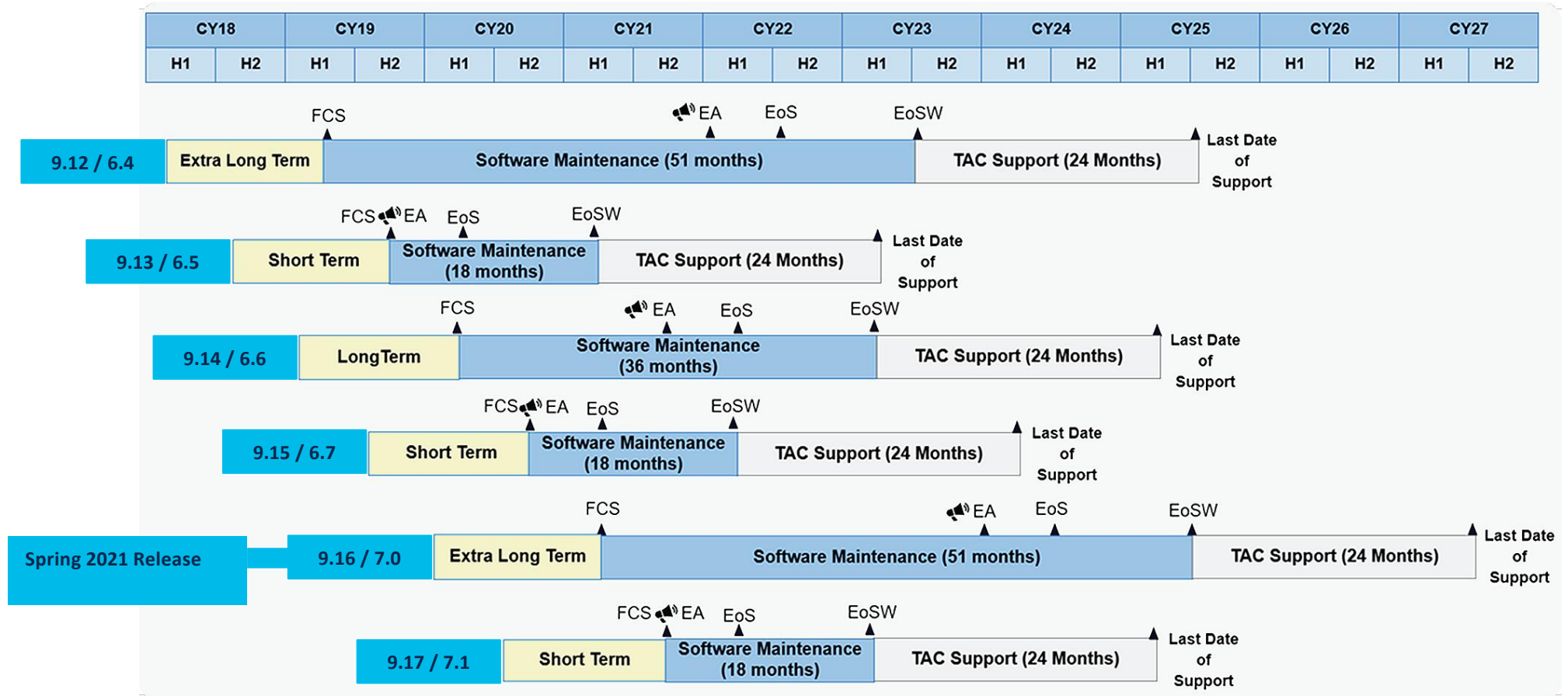
What is Secure Firewall Threat Defense (FTD)?

Delivers nearly 100% efficacy on blocking malicious flows and guards the network against threats

- Key Benefits
 - Tenant management separation
 - Scale as you grow
 - Impact analysis
 - Prioritize administration
- Features
 - Firewall
 - Intrusion Prevention
 - Integrated TLS Decryption
 - VPN
 - Cisco Threat Intelligence Director
 - Malware Continuous Analysis with Retrospection



ASA/FTD Release Lifecycle



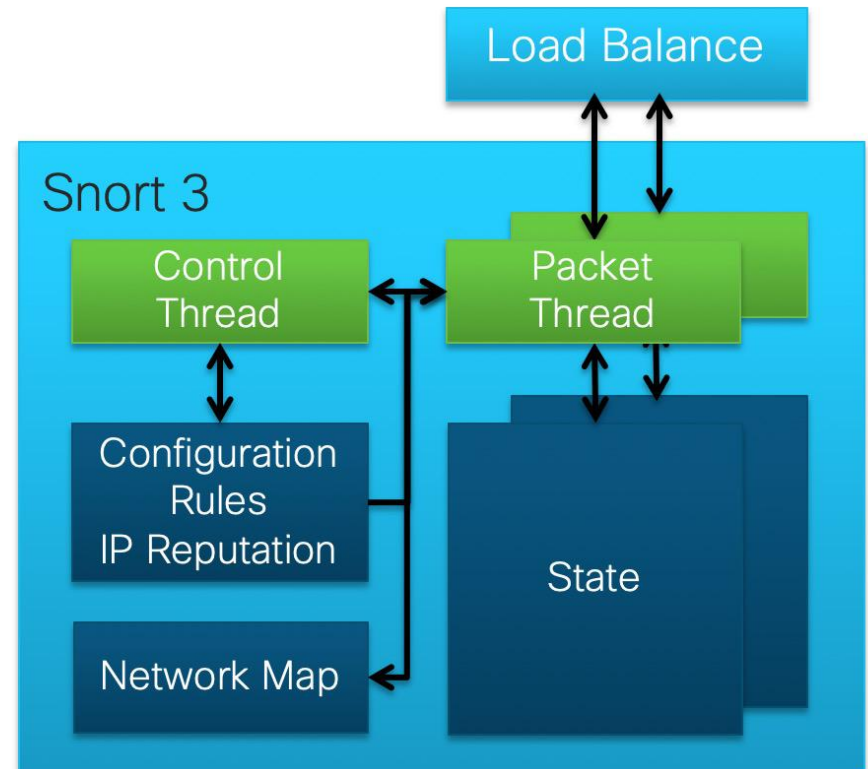
FTD Features Overviews

6.7 – Snort 3.0, Health Monitoring, VTI,...

- Snort 3.0 with FDM and CDO
- AnyConnect modules (Umbrella, AMP, others) & API integrations
- DUO SAML with FMC
- Route-based VPNs (VTI)
- HTTP 2.0 & TLS 1.3 ACP visibility
- Faster deployment, upgrades and downgrades
- Unified Health Monitoring dashboard
- Unified SNMP engine
- Manual FTD configuration and upgrade rollback to previous version
- Detailed deployment transcripts for per-user changes
- Search filter for ACP comments and NAT policies
- Copy & Paste rules between ACP & Prefilter
- FTDv HA for VMware
- pxGrid 2.0 & ThreatGrid v3 support

Snort 3.0 Architecture

- Threaded to utilize multiple cores
 - 1 control thread (main)
 - N packet threads per process
 - Reloads faster (1 vs N)
- A single config and network map
 - Uses less memory
 - Supports more IPS rules and larger netmap
- Rules written in text like Snort 2
 - More uniform syntax in Snort 3
 - Easier to read, write, and verify
 - “Snort2lua” converts 2.9 IPS rules to 3.0 format
 - LuaJIT will be added later by TALOS



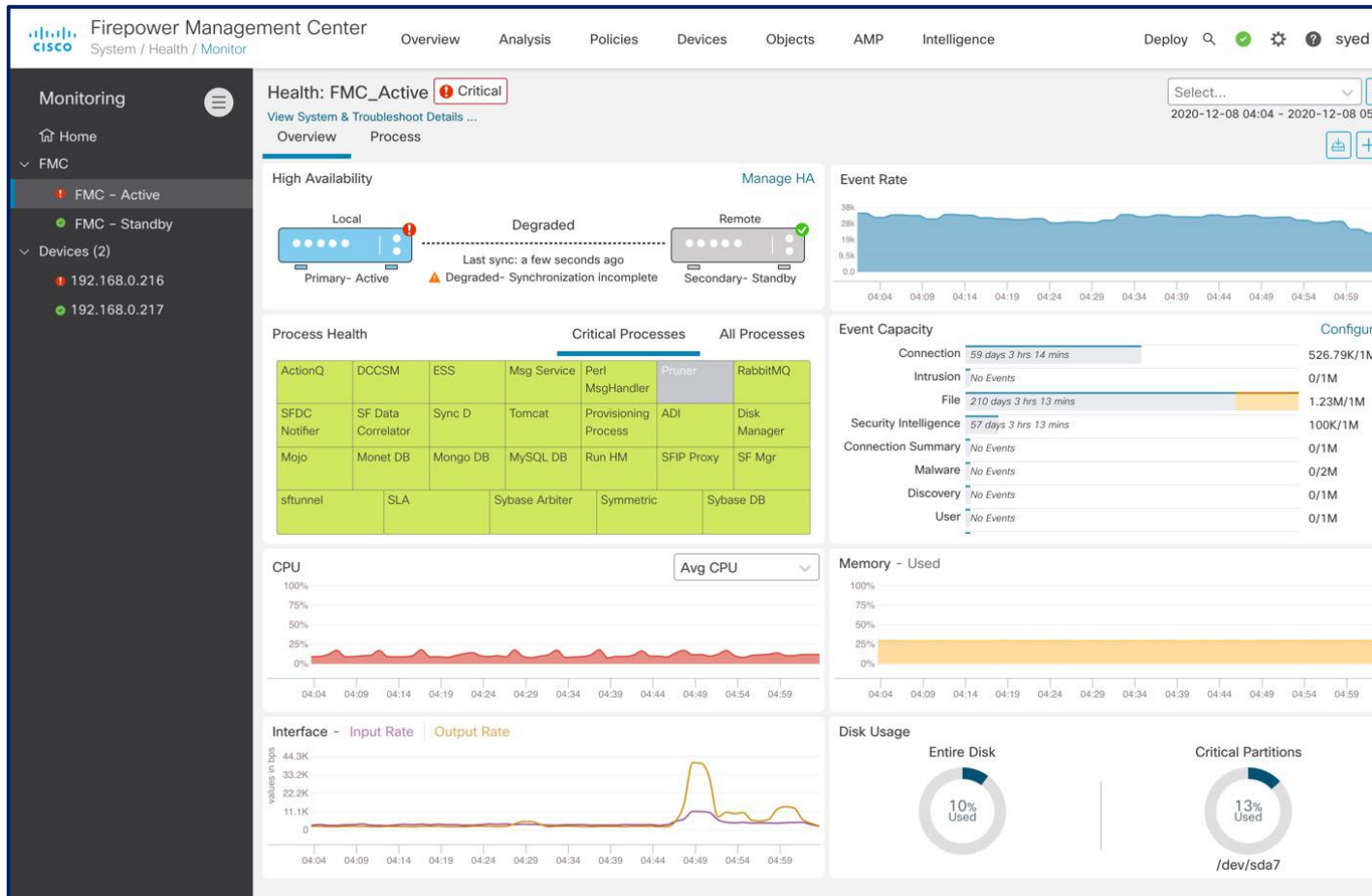
Snort 3 – Changes in IPS Rule

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"BLACKLIST URI request for known malicious URI"; flow:established,to_server; content:"/setup_b.asp?prj="; nocase; http_uri; content:"&pid="; nocase; http_uri; content:"&mac="; nocase; http_uri; pcre:"/\\/setup_b\\.asp\\?prj=\\d\\x26pid=[^\\r\\n]*\\x26mac=/Ui"; metadata:service http; sid:19626; rev:2;)
```



```
alert http
(
  msg:"BLACKLIST URI request for known malicious URI";
  flow:established,to_server;
  http_uri;
  regex:"/setup_b\\.asp\\?prj=\\d&pid=.*&mac=", nocase, fast_pattern;
  sid:19626; rev:4;
)
```

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

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

Hide

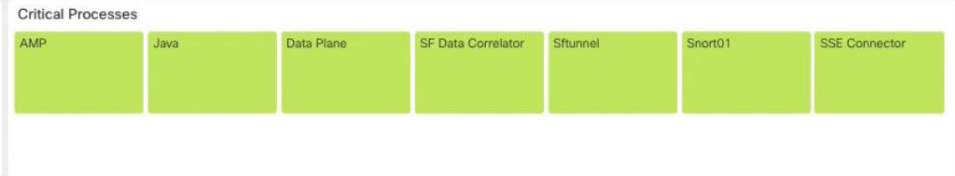
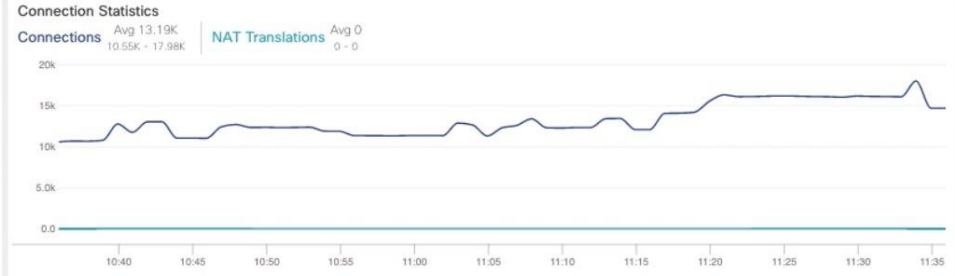
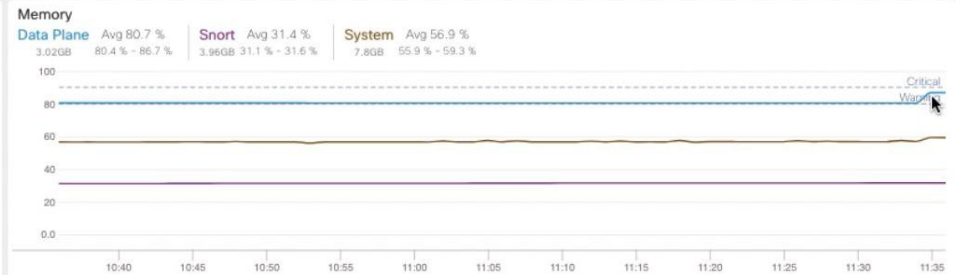
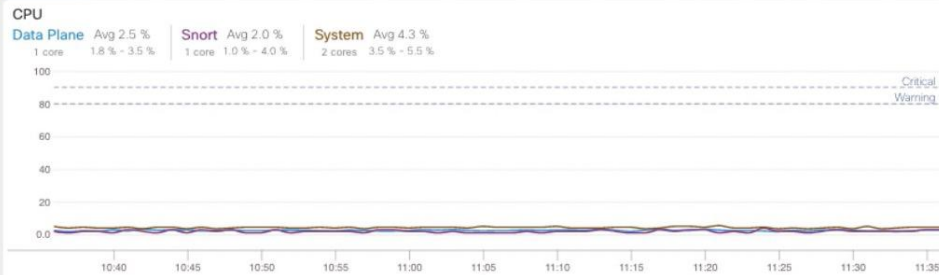
System Details

Up Time: VDB: Build 338 - 2020-09-24 12:58:48
Version: 6.7.0 SRU: 2020-10-14-001-vrt
Model: Cisco Firepower Threat Defense for VMWare Snort: 2.9.17 (Build 199 - daq12)
Mode: ROUTED

Troubleshooting & Links

[Generate Troubleshooting Files](#) [Health Policy \(Initial_Health_Policy 2019-02-18 16:18:32\)](#)
[Advanced Troubleshooting](#) [Alerts](#)

Overview **CPU** Memory Interfaces Connections Snort Correlation-CPU-Dataplane Correlation-Packetdrops



Device Health Monitoring

Monitoring

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

Health: NGFW1 ● Normal

Last 1 hour
2020-11-03 10:37 - 2020-11-03 11:37

System Details

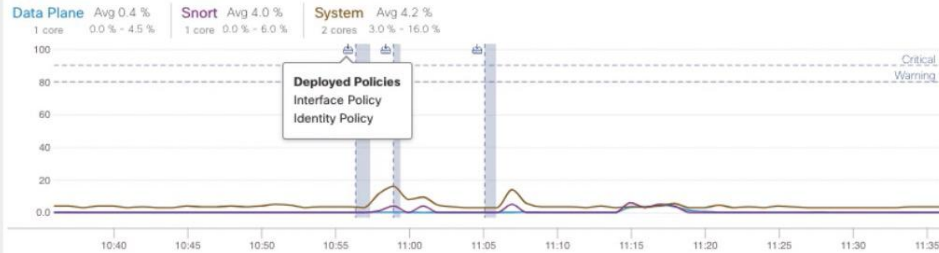
Up Time: 22 hours 45 mins VDB: Build 338 - 2020-09-24 12:58:48
 Version: 6.7.0 SRU: 2020-10-14-001-vrt
 Model: Cisco Firepower Threat Defense for VMWare Snort: 2.9.17 (Build 199 - daq12)
 Mode: ROUTED

Troubleshooting & Links

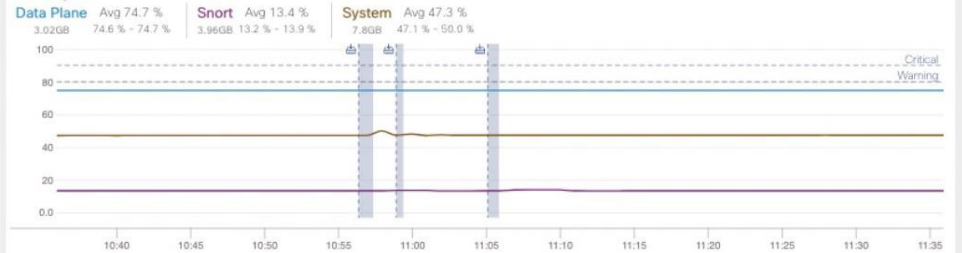
[Generate Troubleshooting Files](#) [Health Policy \(Initial_Health_Policy 2019-02-18 16:18:32\)](#)
[Advanced Troubleshooting](#) [Alerts](#)

Overview CPU Memory Interfaces Connections Snort Correlation-CPU-Dataplane

CPU



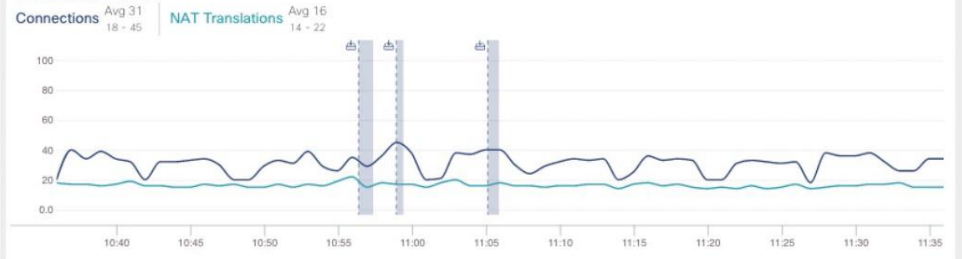
Memory



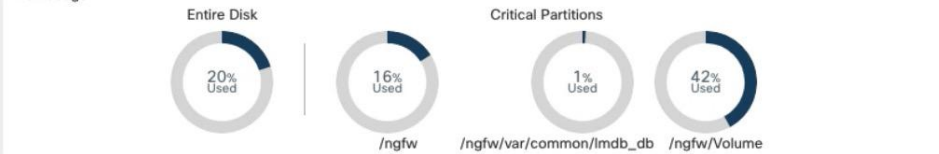
Throughput



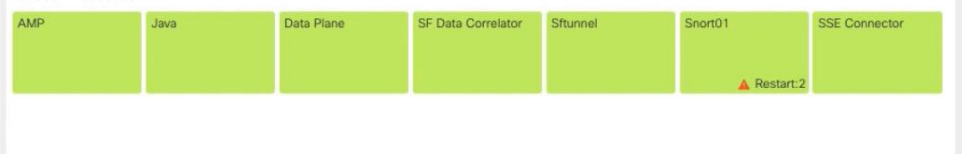
Connection Statistics



Disk Usage



Critical Processes



Device Health Monitoring

Firepower Management Center System / Health / Monitor

Overview Analysis Policies Devices Objects AMP Intelligence

Monitoring

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

Health: NGFW1 Normal

System Details

Up Time: 22 hours 45 mins VDB: Build 338 - 2020-09-24 12:58:48

Version: 6.7.0 SRU: 2020-10-14-001-vrt

Model: Cisco Firepower Threat Defense for VMWare Snort: 2.9.17 (Build 199 - daq12)

Mode: ROUTED

Troubleshooting & Links

- Generate Troubleshooting Files
- Advanced Troubleshooting
- Health Policy (Initial_Health_Policy 2019-02-18 16:18:32)
- Alerts

Overview CPU Memory Interfaces Connections Snort Correlation-CPU-Dataplane

CPU

Data Plane Avg 0.4 % | Snort Avg 4.0 % | System Avg 4.2 %

1 core 0.0% - 4.5% | 1 core 0.0% - 6.0% | 2 cores 3.0% - 16.0%

Throughput

Input Rate Avg 856.18Kbps | Output Rate Avg 182.55Kbps

24.64Kbps - 12.18Mbps | 11.81Kbps - 556.89Kbps

Disk Usage

Entire Disk: 20% Used

Critical Partitions:

- /ngfw: 16% Used
- /ngfw/var/common/lmdb_db: 1% Used
- /ngfw/Volume: 42% Used

Correlate Metrics

Correlation-Packetdrops

Metrics

Chosen metrics will be displayed as portlets in the dashboard.

- CPU: Control Plane x, Data Plane x
- CPU: Snort x
- Snort: Denied flows x, Packets bypassed due to Snort busy x, Packets bypassed due to Snort down x
- Interface: Drop Packets x, Input Packets x
- Connections: Connections in use x, Peak Connections x
- Connections: NAT Translations x, Peak NAT Translations x
- Deployed Configuration: Number of ACEs x

Cancel Add

Critical Processes

- AMP
- Java
- Data Plane
- SF Data Correlator
- Sftunnel
- Snort01
- SSE Connector

Restart:2

Route Based VPNs (VTI) – FTD 6.7

- VPN wizard with extra option and new, easier layout

Create New VPN Topology

Topology Name:*
VPN-LB-01

Policy Based (Crypto Map) Route Based (VTI)

Network Topology:
 Point to Point Hub and Spoke Full Mesh

IKE Version:* IKEv1 IKEv2

Endpoints **IKE** IPsec Advanced

Node A	Node B
Device:* FTDv-lab	Device:* Extranet
Virtual Tunnel Interface:* IF_OUTSIDE	Device Name*: HUB-VPN
<input type="checkbox"/> Tunnel Source IP is Private Edit VTI	Endpoint IP Address*: 192.51.110.6
Connection Type:* Bidirectional	
Tunnel IP Address : 193.19.143.251 Tunnel Source Interface : Tunnel Source Interface IP:	
Additional Configuration ⓘ Route traffic to the VTI : Routing Policy Permit VPN traffic : AC Policy	

Cancel Save

More value than ever!

Cisco Secure Firewall Threat Defense 7.0 delivers up to 30% throughput gains across AVC, IPS, & VPN for the majority of Secure Firewall platforms.*

**But that's not even
the most exciting news...**



Secure Firewall Threat Defense 7.0

Major improvements in an extra long-term release

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

Simplified Product Experience

Unified health metrics (via SNMP), health dashboard in FMC, Change management (rollback, change previews, improved audit logs), Searching and Filtering etc.

Threat Efficacy Enhancement

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

Public Cloud & Virtualization

Support dynamic policies for cloud-native policy and create quick instance (with Secure Threat Services)

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...

- Remote access and site-to-site VPN
- Secure-X Integration
- FMC API for orchestration and migration
- APIC FMC App Multi domain support
- PAT operations in clustering
- Multiple realm support for Identity

What's new? – FMC

FTD Release 7.0

- Snort 3
- Dynamic Objects
- Unified Event Viewer
- AD domain cross-domain trust
- DNS reputation filtering
- SecureX integration
- ACI integration – FMC Endpoint Update App
- Device install and upgrade improvements
 - Easier, faster, smaller
 - Enhanced upgrade status and error reporting
 - Easy to follow upgrade workflow
 - Upgrade more devices at once
- Usability Enhancements
 - Search for policies and objects
- Change Management
 - Deployment preview & history
 - Selective VPN deployment
 - Configuration rollback

What's New – Snort 3 Overview



Solution

- Snort 3 is now supported with FMC as well as FDM
- Snort 3 Device Management
 - Ability to toggle device Snort versions (Snort 2<->Snort 3) from FMC device management
- Upgrade / Migration Changes
 - Simplified Snort 2 to Snort 3 policies migration after upgrading to release 7.0
 - Support for synchronizing common Intrusion Policies between Snort 2 and Snort 3 versions

Snort Engine Selection



How it Works

- For existing deployments (upgrades), after upgrade to release 7.0, devices continue to use Snort 2 as the detection engine
- For new deployments (fresh install of FMC), new 7.x devices use Snort 3. Existing devices registered running 6.x remain at Snort 2

<input type="checkbox"/>	Name	Model	Version
▼ Ungrouped (3)			
<input type="checkbox"/>	10.10.20.202 10.10.20.202 - Routed	FTD on VMWare	6.6.1
<input type="checkbox"/>	10.10.20.207 Snort 3 10.10.20.207 - Routed	FTD on VMWare	7.0.0 ...3.0
<input type="checkbox"/>	10.10.20.208 10.10.20.208 - Routed	FTD on VMWare	7.0.0 ...3.0

Snort 2 vs. Snort 3

	Snort 2	Snort 3
Multi-Threaded Architecture		✓
Capable of running multiple Snort Processes	✓	✓
Port Independent Protocol Inspection		✓
IPS Accelerators / Hyperscan Support		✓
Modularity – Easier TALOS contributions		✓
Scalable Memory Allocation		✓
Next Gen TALOS Rules – e.g., Regex/Rule Options/Sticky Buffers		✓
New and Improved HTTP Inspector – e.g., HTTP/2 support		✓
Lightweight content updates from TALOS		✓

Release 7.0 Snort 3 Overview

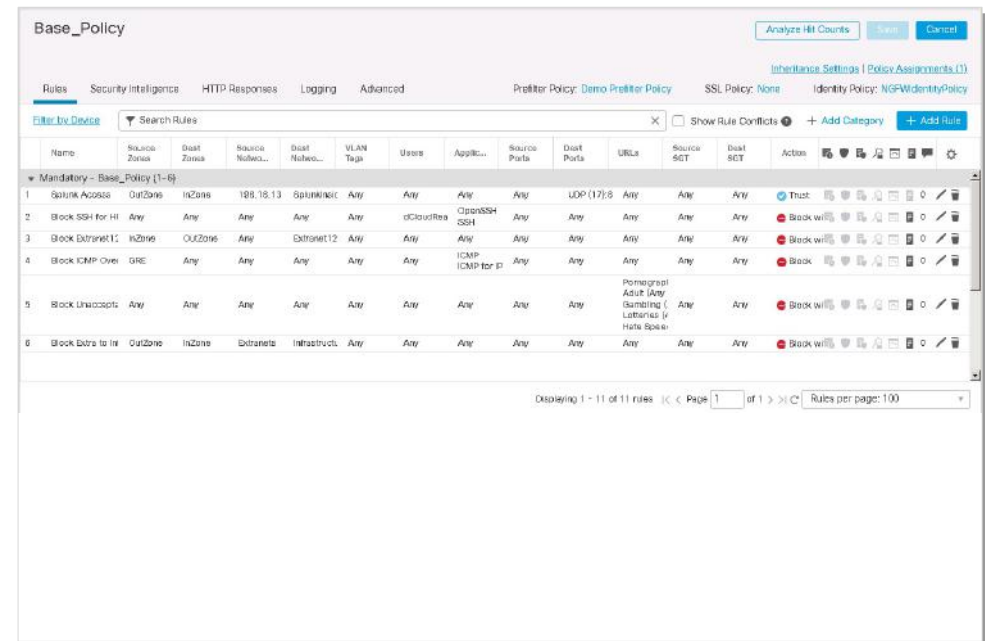
- Release 7.0 device upgrades continue to use Snort 2, new deployments default to Snort 3
- Toggle device Snort versions from the FMC Device Management tab
- Simplified Snort 2 to Snort 3 policy migration
- Intrusion policy synchronization
- Intrusion Rule Groups including custom groups
 - Rule Group security level customization
- Suppression/Threshold features are now available as rule objects
- Custom Snort 3 rules with new syntax



Policy Management

Reduce complexity of policy maintenance

- Centralized on premise management across multiple Firewall platforms
- Integrates multiple security features into a single access policy
- Reduces manual configuration of policy through inheritance and template use.



The screenshot displays the Cisco Policy Management interface for a policy named 'Base_Policy'. The interface includes a search bar, a table of rules, and a pagination control at the bottom. The table lists six rules with various source and destination zones, IP addresses, and protocols.

Name	Source Zone	Dest Zone	Source Subnet	Dest Subnet	VLAN Tags	Users	Applic...	Source Ports	Dest Ports	URLs	Source SET	Dest SET	Actions
Mandatory - Base_Policy (1-6)													
1	Spunk Access	OutZone	InZone	188.18.13	SpunkIntr...	Any	Any	Any	UDP (172)	Any	Any	Any	Trust
2	Block SSH for HI	Any	Any	Any	Any	Any	cidCloudRes	Any	Any	Any	Any	Any	Block with...
3	Block Extranet11	InZone	OutZone	Any	Extranet12	Any	Any	Any	Any	Any	Any	Any	Block with...
4	Block ICMP Over	GRE	Any	Any	Any	Any	Any	ICMP	ICMP for p...	Any	Any	Any	Block
5	Block Linacsoft	Any	Any	Any	Any	Any	Any	Any	Any	Pomegranat	Adult (Any	Any	Block with...
6	Block Extra to Int	OutZone	InZone	Extranet1	Infrastruct...	Any	Any	Any	Any	Any	Any	Any	Block with...

Displaying 1 - 11 of 11 rules | Page 1 of 1 | Rules per page: 100

VPN Updates

- ▶ Authentication and Authorization

 - Dynamic Access Policy

 - Custom Attributes

 - SAML Authorization

 - Local User

 - Multiple Certificates

- ▶ Scaling and Redundancy

 - Load Balancing

 - VTI Enhancements

- ▶ Minor Improvements

 - SSL Ciphers FDM UI

 - PKI Enhancements

 - VPN API



What's New – FMC DAP Support



Solution

- Introduction of Dynamic Access Policy in FMC for managed FTDs
- Simplified Dynamic Access Policy UI Editor
 - Configure AAA attributes
 - Configure Endpoint attributes
- Unified flow for both HostScan and Dynamic Access Policy configurations
- Easy DAP policies migration from ASA to FTD
 - FDM/FTD API to upload DAP xml file previously available in 6.7

Configuration Dialogs Example

General AAA Criteria **Endpoint Criteria** Advanced

Match criteria between sections: **Any** +

▼ **Anti-Malware** (1 criterion)

Match criteria: All **Any** +

Type	Op.	Value
Real Time Scanning	=	true
Product Description	=	McAfee AntiVirus Plus (Mac)
Version	=	4.9
Last Update	<	10

- > **Device** (0 criteria)
- > **AnyConnect** (0 criteria)
- > **NAC** (0 criteria)
- > **Application** (0 criteria)
- > **Personal Firewall** (0 criteria)
- > **Operating System** (0 criteria)
- > **Process** (0 criteria)
- > **Registry** (0 criteria)
- > **File** (0 criteria)
- > **Certificate** (0 criteria)

Anti-Malware

Installed

Real Time Scanning Enabled Disabled

Vendor McAfee, Inc.

Product Description McAfee AntiVirus Plus (Mac)

Version = 4.9

Last Update < 10

Cancel Save

Device

Host Name = #

MAC Address = #

BIOS Serial Number = #

Port Number = #

Secure Desktop Version = #

OPSWAT Version = #

Privacy Protection = # Select...

TCP/UDP Port Number = # TCP (IPv4)

Cancel Save

AnyConnect

Client Version =

Platform = # Select...

Platform Version =

Device Type = #

Device Unique ID = #

MAC Address Pool

MAC Address 1 = #

[Add another MAC Address](#)

Cancel Save

Registry

Entry Path* HKEY_CURRENT_USER\ Software\Cisco\Cisco AnyConnect

Existence Exists Does not exist

Type dword

Value = # 556

Case insensitive

Cancel Save

What's New – VPN Local User Authentication

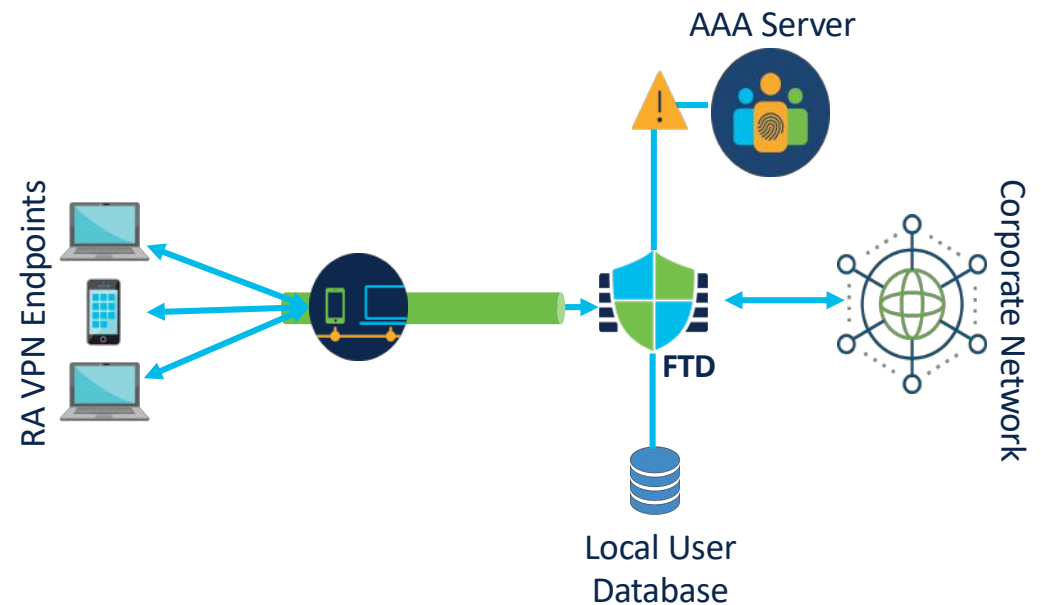


Solution

- In release 7.0,
 - FMC introduces the ability to configure and deploy Local Users to FTD via the GUI and REST API
- When a RADIUS/LDAP/AD Server used for RA VPN Authentication fails, a fallback to authenticate to the Corporate Network through RA VPN and fix the issue
- A quick way to setup RA VPN for a demo/test
- Use cases where the authentication requests cannot go outside of FTD to an external AAA server for reasons of securing data in transit and data at rest
- It is already supported with FDM management

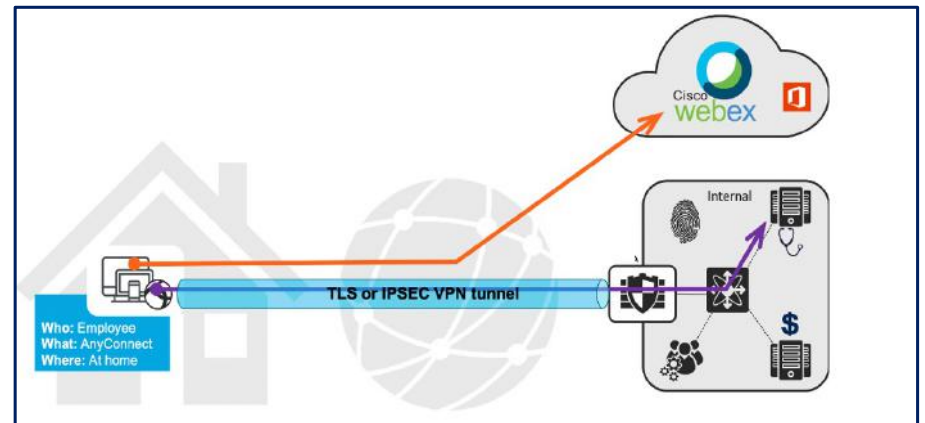
VPN Local User Authentication Overview

- Use Local User Database for VPN
 - Primary Authentication
 - Secondary Authentication
 - Fallback for Primary Authentication
 - Fallback for Secondary Authentication
- Local Users database configured as a Realm (like AD/LDAP implementation)
 - Reuse or shared across VPN configurations on multiple FTDs



Dynamic Split Tunneling

- Static split tunneling involves defining the host and network IP addresses to include in or exclude from the remote access VPN tunnel.
- Dynamic Split tunnel with AnyConnect was introduced to dynamically provision split include/exclude tunneling after tunnel establishment based on the host DNS domain name.
- Dynamic Split tunneling can be provisioned using
 - Dynamic Split Exclude
 - Dynamic Split Include



What's New – SAML Authorization



Solution

- Release 7.0 introduces
 - FMC SAML authorization support for Remote Access VPN using Dynamic Access Policy (DAP)
 - SAML authentication for Remote Access VPN users was added in release 6.7
- Support for user attributes delivered in SAML assertions within the AAA and DAP frameworks
- ASA 9.16 adds support for using SAML Assertion Attributes for Dynamic Access Policy outcomes

What's New – RA VPN Load Balancing

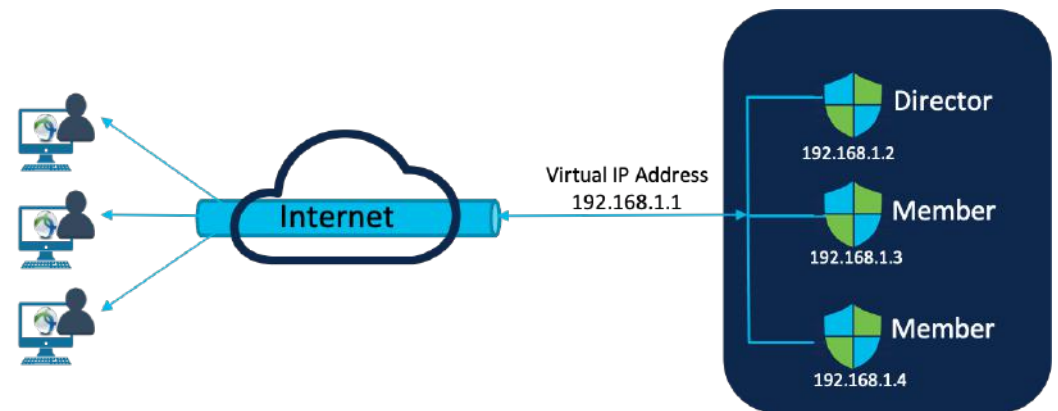


Solution

- Release 7.0 adds support for
 - Configuring and deploying two or more FTD devices in a logical group for Load Balancing Remote Access VPN sessions
 - Share the Load Balancing configuration among multiple devices
- VPN Scalability combined with increased availability
 - Different from FTD Clustering or FTD High Availability
 - FTD Standalone or High Availability pair can be added as part of the Load Balancing group
 - For FTD deployed in Multi Instance mode, Instances can be bundled together to form a VPN Load Balancing Group

RA VPN Load Balancing Overview

- AnyConnect VPN session shared among devices
- Two or more devices virtually grouped to form a Load Balancing Group
- Members
 - FTDs participating in Load Balancing Group
 - Share the VPN connections
- Director
 - One FTD acts as a director
 - Distributes the load to other members in the group
 - Also participates in serving VPN sessions



Configuration Workflow

The screenshot shows the Cisco FMC configuration page for 'RAVPN_BLR_Site'. The 'Advanced' tab is selected, and the 'Load Balancing' option is highlighted in the left-hand navigation menu. A blue arrow points from the 'Load Balancing' menu item to a text box that reads: 'Load Balancing configuration is available under **Advanced** Tab'. The main content area shows a toggle switch for 'Enable Load balancing between member devices' which is currently turned off. Below the toggle, there is a descriptive text: 'While enabled, opted devices will share the load of VPN session traffic amongst them. This option can be disabled anytime without destroying the configuration.'

****Devices should be separately added to the VPN Configuration**

What's New - VTI



Solution

- Release 7.0 adds support for
 - IPv6 addressing on Static Virtual Tunnel Interface
 - Ability to configure backup VTI interfaces natively from FMC in a single topology
 - Supported in 6.7 but required two different topologies
 - Increased the maximum number of VTI from 100 to 1024
- Adds support for ASA and CSM UI as well

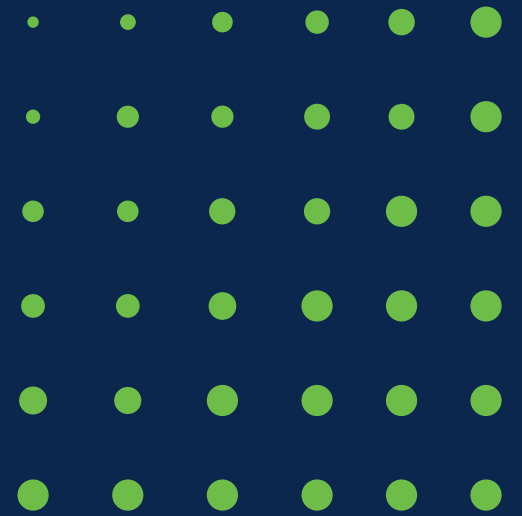
Enrollment over Secure Transport (EST)



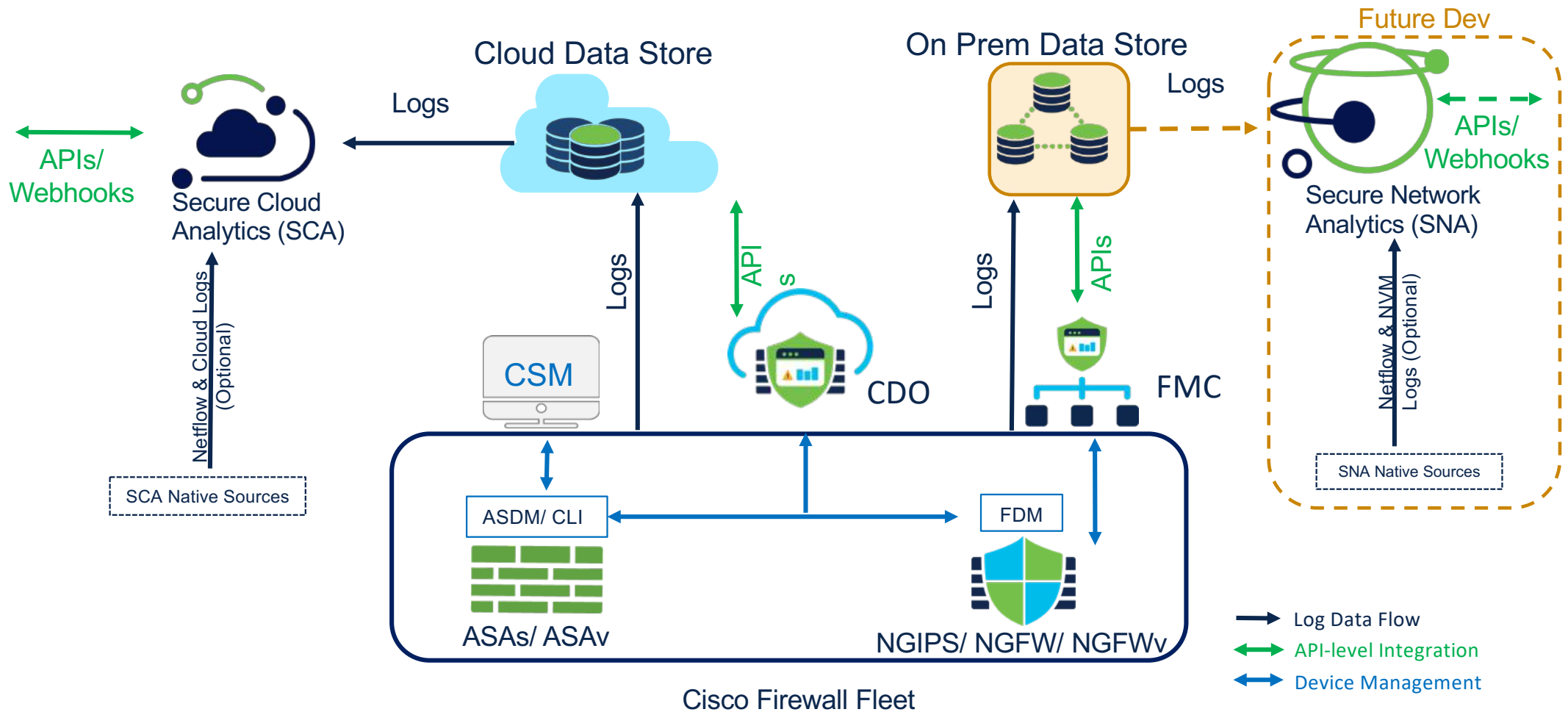
Solution

- A new enrollment type - Enrollment over Secure Transport (EST)
- EST is the successor to the Simple Certificate Enrollment Protocol (SCEP)
 - EST uses TLS for the secure message transport
 - In EST, the certificate signing request (CSR) can be tied to a requestor that is already trusted and authenticated with TLS
- EST is described in RFC 7030

Cisco Security Analytics and Logging



Analytics and Logging Architecture



SAL (SaaS) Cloud Hosted Features



Cloud storage 90 days (default) up to 3 years, with viewing and download enabled within CDO



Supports **all** Cisco FTD & ASA devices. Direct-to-cloud option enabled for FMC 7.0+ managed devices



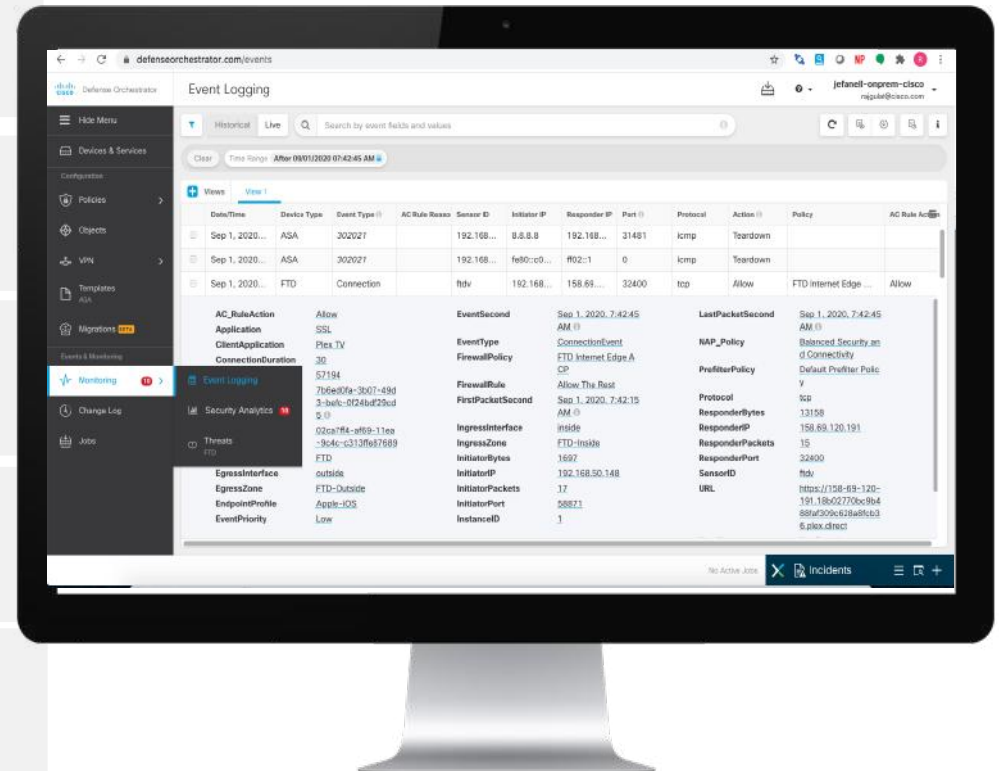
Firewall log analysis for advanced threat detections using Secure Cloud Analytics (SCA)



Correlation of firewall logs with internal network and cloud logs in SCA

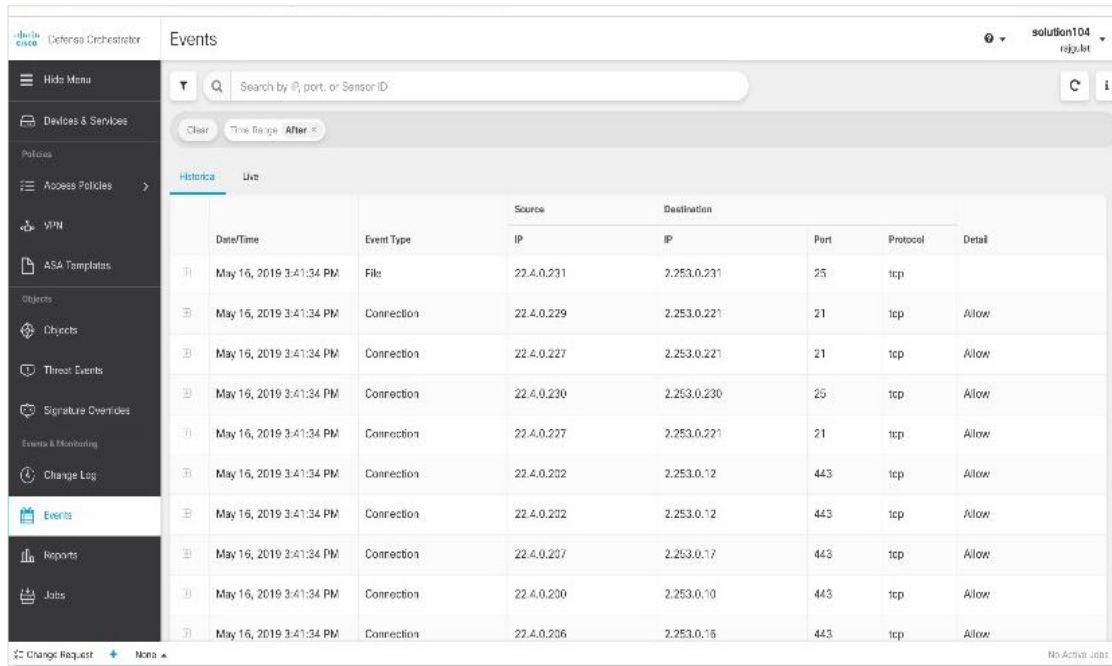


Existing CTR-SecureX customers can opt-in to SAL logging easily by merging with their SecureX tenant



CDO: Cisco Security Analytics and Logging

Reduce complexity and logging event volume



The screenshot shows the Cisco Defense Orchestrator (CDO) interface. The top navigation bar includes the Cisco logo, 'Defense Orchestrator', and 'Events'. A search bar is present with the text 'Search by IP, port, or Sensor ID'. Below the search bar are 'Clear', 'Time Range', and 'After' buttons. The main content area is a table with columns for 'DateTime', 'Event Type', 'Source IP', 'Destination IP', 'Port', 'Protocol', and 'Detail'. The table contains 10 rows of event data, all dated 'May 16, 2019 3:41:34 PM'. The event types are 'File' and 'Connection'. The source and destination IP addresses, ports, and protocols are listed for each event. The 'Detail' column for all 'Connection' events shows 'Allow'. The bottom of the interface shows 'Change Request' and 'None' buttons, and a status indicator 'No Active Jobs'.

DateTime	Event Type	Source IP	Destination IP	Port	Protocol	Detail
May 16, 2019 3:41:34 PM	File	22.4.0.231	2.253.0.231	25	tcp	
May 16, 2019 3:41:34 PM	Connection	22.4.0.229	2.253.0.221	21	tcp	Allow
May 16, 2019 3:41:34 PM	Connection	22.4.0.227	2.253.0.221	21	tcp	Allow
May 16, 2019 3:41:34 PM	Connection	22.4.0.230	2.253.0.230	25	tcp	Allow
May 16, 2019 3:41:34 PM	Connection	22.4.0.227	2.253.0.221	21	tcp	Allow
May 16, 2019 3:41:34 PM	Connection	22.4.0.202	2.253.0.12	443	tcp	Allow
May 16, 2019 3:41:34 PM	Connection	22.4.0.202	2.253.0.12	443	tcp	Allow
May 16, 2019 3:41:34 PM	Connection	22.4.0.207	2.253.0.17	443	tcp	Allow
May 16, 2019 3:41:34 PM	Connection	22.4.0.200	2.253.0.10	443	tcp	Allow
May 16, 2019 3:41:34 PM	Connection	22.4.0.206	2.253.0.16	443	tcp	Allow



Store firewall and network logs securely in the cloud, accessible and searchable from CDO



Identify and enrich high fidelity alerts



Enable smarter response and reduce investigation times



Enhance breach detection capability using best-in-class security analytics

SAL On-Premise Features



FTD (including data plane logs) and ASA logging in a scalable data store hosted on-premises



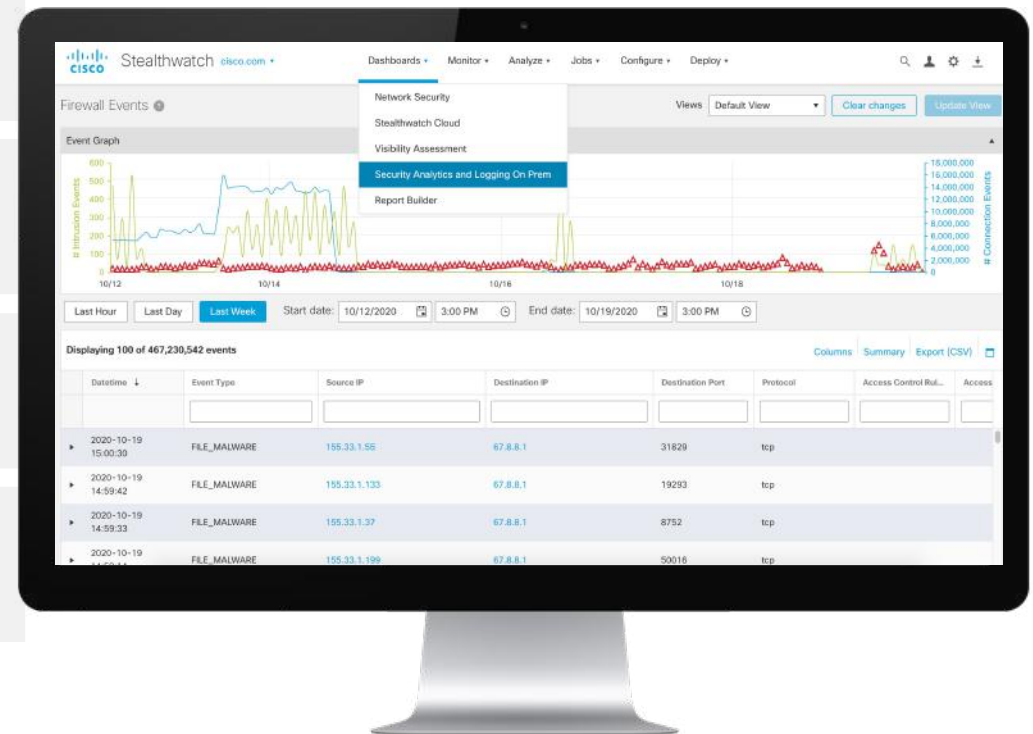
Logging wizard in FMC 7.0+ simplifies on-premises and cloud logging configuration



FMC 7.0+ logging and analytics scale drastically extended by a significant 300X magnitude via remote query of SAL/ SNA 7.3.2+



Context pivot to SAL's event viewer in Secure Network Analytics (SNA) for enhanced context



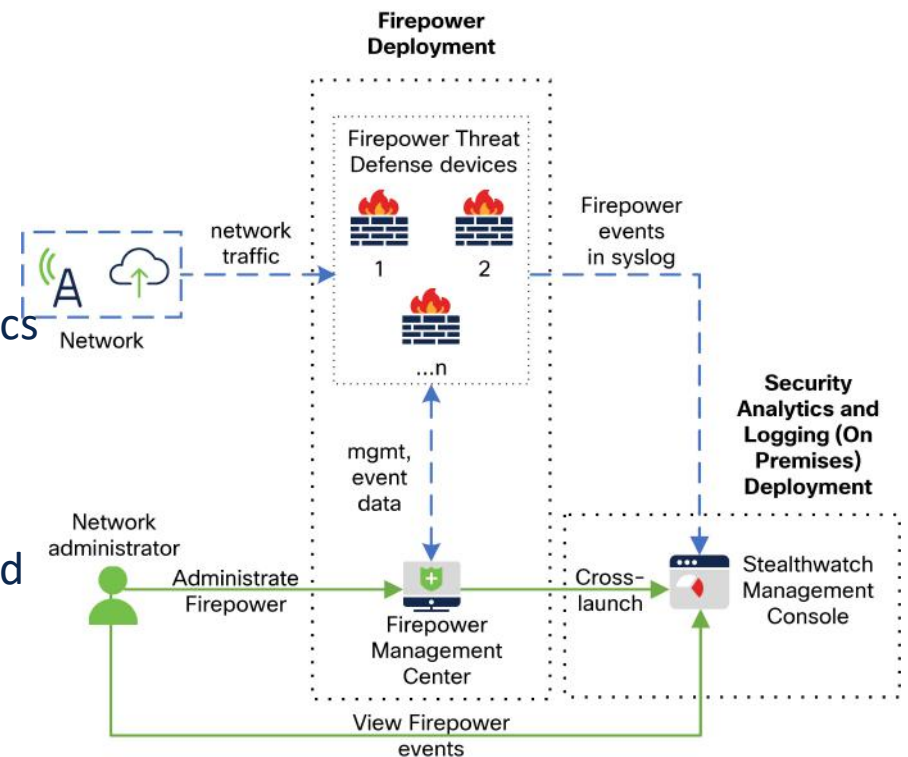
FMC Integration with Cisco Security Analytics and Logging (On-Prem)

Easy button for setup

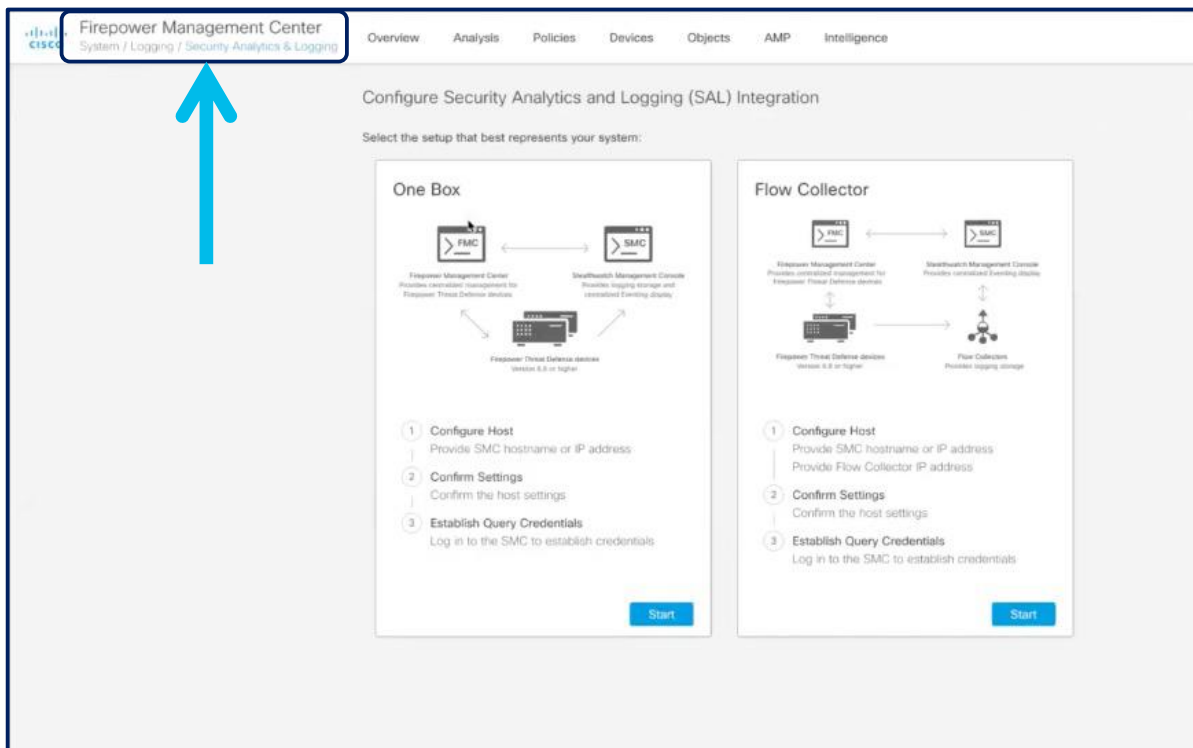
- Setup FMC analytics cross launch links to the Secure Analytics console
- Setup remote query credentials from Secure Analytics datastore

Longer Event Retention and increased scale

- External Storage through Cisco Security Analytics and Logging On-Prem
- Auto select event source or manually specify



FMC Integration with Cisco Security Analytics and Logging (SAL On Premise) – Easy Wizard



Easy button for setup

- Setup FMC analytics cross launch links to the Secure Analytics console
- Setup remote query credentials from Secure Analytics datastore

Security Analytics and Logging Licenses

3 license tiers (nested)



Logging and Troubleshooting*

Scalable FTD and ASA event logging both in the cloud and on-premises, with API integration with Manager; CDO for cloud, and FMC for on premises stores



Logging Analytics and Detection

Firewall log data analysis using the behavior-based threat detections of Secure Cloud Analytics (SaaS)



Total Network Analytics and Detection

Consolidated analysis run on combined dataset of firewall, internal and public cloud logs for comprehensive threat detection

*Security Analytics and Logging (On Premises) is currently only available with Logging and Troubleshooting License, which includes remote query by the FMC

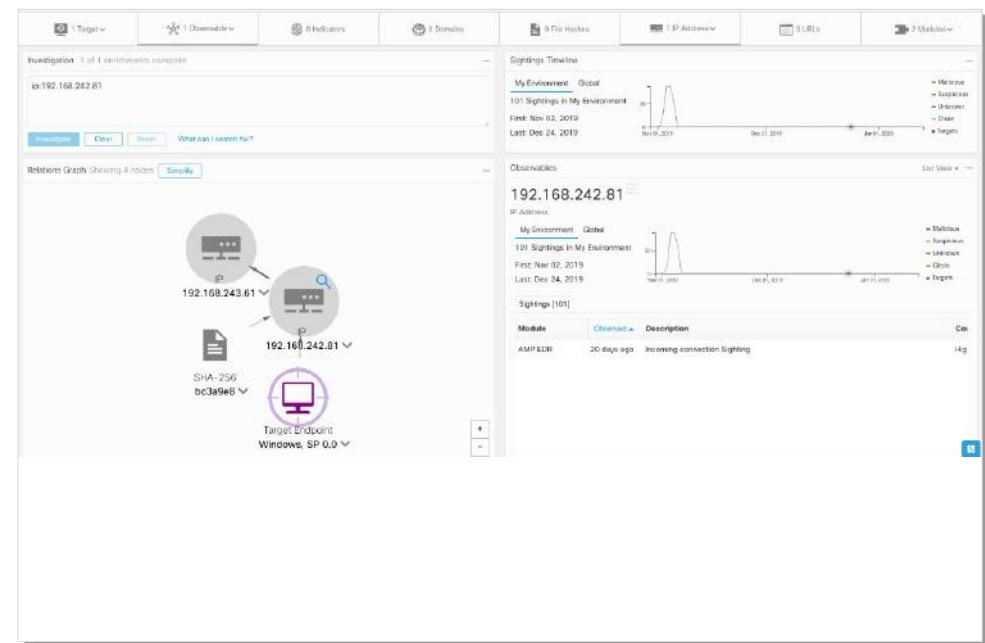
Integrations



FMC Integrations

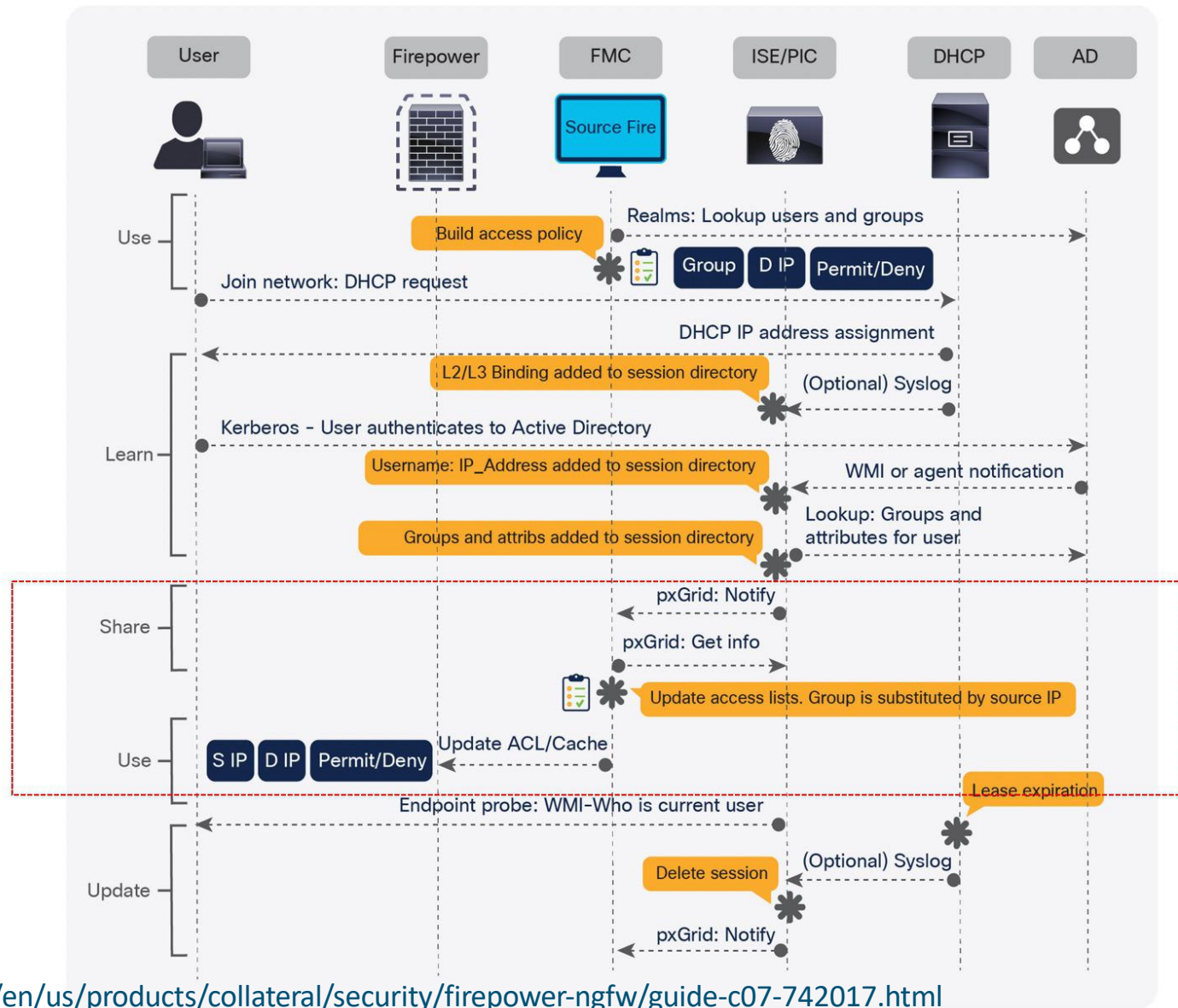
Visibility and analytics beyond network discovery

- Close integration of FMC with Secure Endpoint
- Standards based threat indicators (STIX/TAXII)
 - Cisco Threat Intelligence Director (CTID)
- Drive down TTR with broad detection and collation
 - SecureX threat response (CTR)
- Leverage other Cisco and 3rd party product to extend visibility
 - FMC external Cisco lookups
- Leverage SIEMs with Unified Events

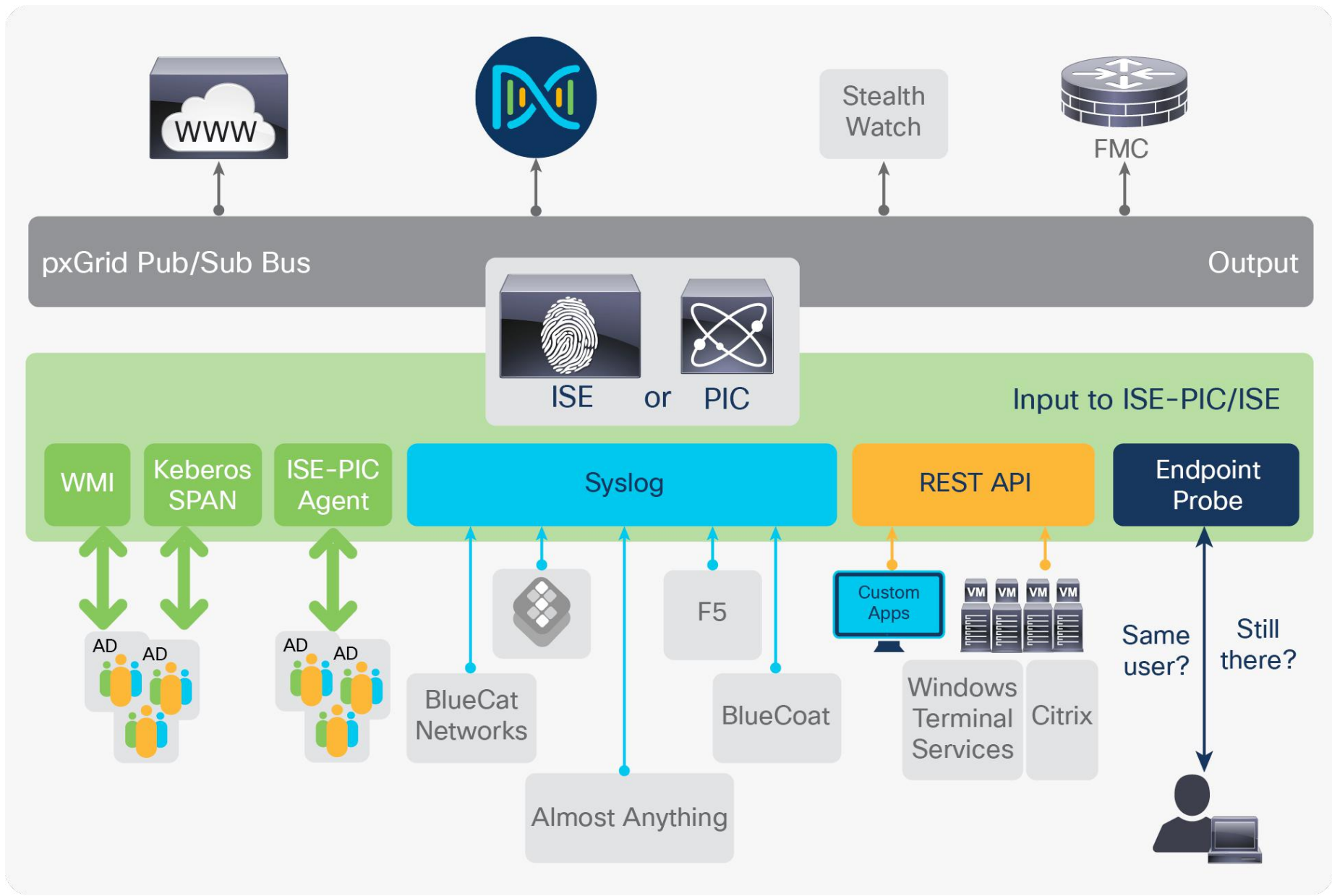


Identity Awareness and Control & ISE

Here

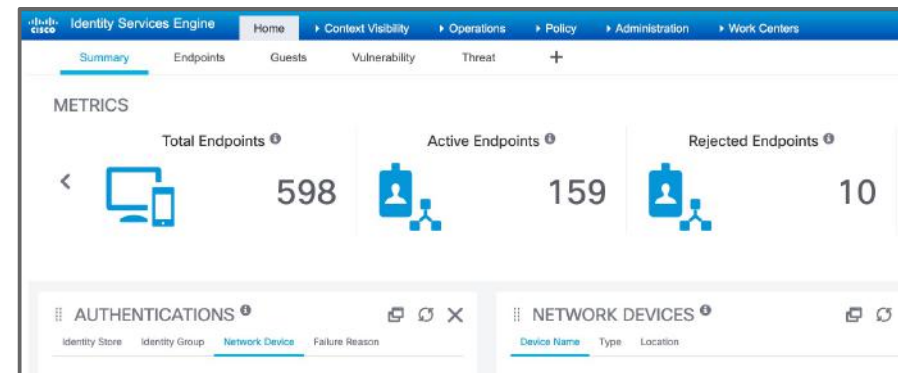


<https://www.cisco.com/c/en/us/products/collateral/security/firepower-ngfw/guide-c07-742017.html>



Control Traffic Based on User Awareness

- Use Active Directory users and groups in policy configuration
- Use Cisco Identity Services Engine to provide identity
 - TrustSec Security Group Tag (SGT)
 - Device type (endpoint profiles) and location
 - Identity Mapping Propagation & device level filtering
- Examples
 - Block HR users from using personal iPads
 - Create rules for quarantined iPhones



The screenshot shows the Cisco Firepower Management Center (FMC) Policies page. The page title is "Branch Access Control Policy". The navigation bar includes Overview, Analysis, Policies, Devices, Objects, AMP, and Intelligence. The page displays a table of rules for the "Branch Access Control Policy".

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

Application-Centric Infrastructure

Transparent policy-based security for both physical and virtual environments

- Link security to software defined networking
- Create identity-based policy with Application Policy Infrastructure Controller (APIC)
- Segment physical and virtual endpoints based on group policies with detailed and flexible segmentation
- Release 7.0 – FMC Endpoint Update app 1.2 adds multi-site / multi-domain support

Configure Interface, PC, And VPC

Select Switches To Configure Interfaces: Quick Advanced

Switches: 101

Switch Profile Name: Switch101_Profile

Interface Type: Individual PC VPC

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

Interface Selector Name:

Interface Policy Group: Create One Choose One

Link Level Policy:

CDP Policy:

MCP Policy:

LLDP Policy:

STP Interface Policy:

Monitoring Policy:

Storm Control Policy:

L2 Interface Policy:

Attached Device Type: ESX Hosts

Domain Name:

VLAN Range:
Please use commas to separate VLANs.

vCenter Login Name:

Security Domains:

Password:

Confirm Password:

vCenter/vShield:

Name	IP	Type	Status Collection
------	----	------	-------------------

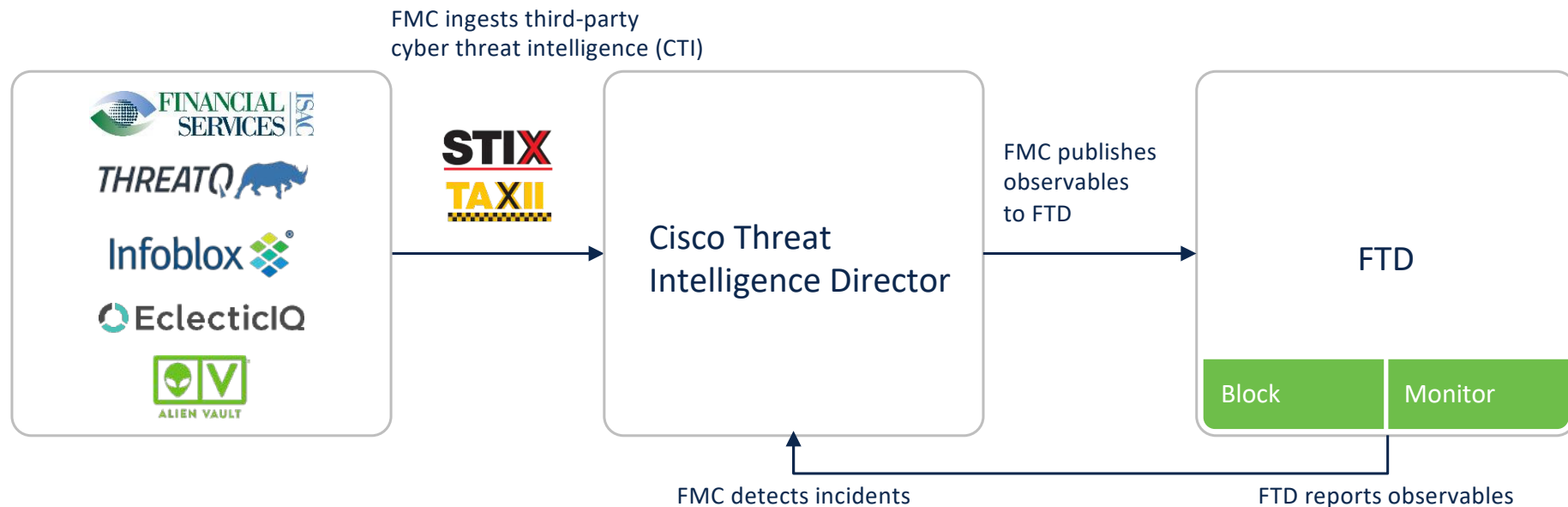
vSwitch Policy: MAC Flooding CDP LLDP

SAVE CANCEL

Cisco Threat Intelligence Director (CTID)

Support of open integration

- Extend Talos Security Intelligence with 3rd party cyber threat intelligence
- Parse and operationalize simple and complex threat indicators



Contextual cross-launch

Tight integration and pivoting to accelerate threat hunting

1 Right-click on an IP address

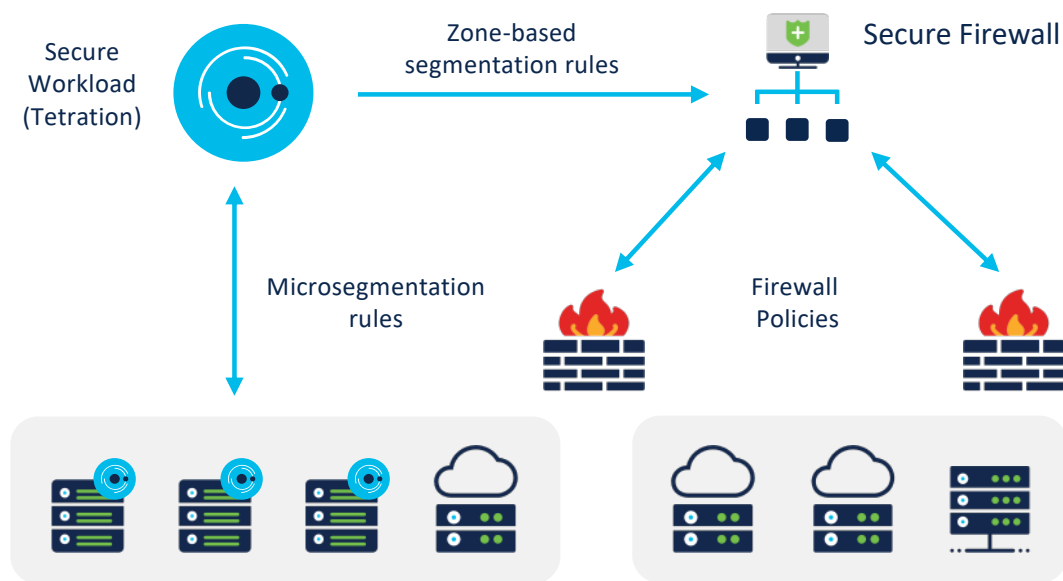
Responder IP	Responder Country	Ingress Security Zone	Egress Security Zone
184.24.33.12	USA	InZone	OutZone
184.24.33.12	USA	InZone	OutZone
52.8.		tZone	tZone
52.8.		tZone	tZone
52.8.		tZone	tZone
52.8.		tZone	tZone
52.8.		tZone	tZone
52.8.		tZone	tZone
52.8.		tZone	tZone
52.8.		tZone	tZone
52.8.		tZone	tZone
52.8.		tZone	tZone
52.8.		tZone	tZone
52.8.		tZone	tZone
52.8.		tZone	tZone
52.8.		tZone	tZone

2 Select Talos IP lookup

The screenshot shows the Talos IP lookup interface. At the top, there's a search bar with the IP address 122.234.28.28. Below the search bar, there are several tabs: Reputation Overview, Email & Spam Data, Malware Data, and Reputation Support. The main content area is divided into three sections: LOCATION DATA, OWNER DETAILS, and REPUTATION DETAILS. The LOCATION DATA section shows a map of China with a yellow pin indicating the location in Hangzhou. The OWNER DETAILS section shows the IP address 122.234.28.28, a reverse DNS match status of 'No', and the network owner as China Telecom Zhiliao. The REPUTATION DETAILS section shows three categories: EMAIL REPUTATION (Neutral), WEB REPUTATION (Neutral), and WEIGHTED REPUTATION (Neutral).

- Pivot directly to Cisco Architecture
- Pivot 3rd party tools
- Reduce time to analyze IoCs to drive down TTR
- Reduce complexity of integration

Dynamic Policy Across Multicloud Environments



Seamless Integration

Unified segmentation policy across Secure Firewall & Secure Workload



Dynamic Policies

Policy updated dynamically based on application communications information



Expanding to Cloud Providers

This fall, extending recommendation functionality to AWS and Azure security groups

“ Eagerly awaiting this! Integration across our multicloud controls will help drive better security in our distributed environment. ”

-- Global payments and fleet management enterprise

FMC Configuration: Prior-7.0 release

- AC Policy Rule has an SGT/ISE Attributes tab
- Selectors refer to “Metadata”

Add Rule ?

Name Enabled Insert into Mandatory

Action Allow Time Range None +

Zones Networks VLAN Tags Users Applications Ports URLs **SGT/ISE Attributes** Inspection Logging Comments

Available Metadata +

Selected Source Metadata (0) Selected Dest Metadata (0)

any any

Add to Source Add to Destination



FMC Configuration: Post-7.0 release

- AC Policy Rule has a Dynamic Attributes tab
- SGT, Device Type, Location IP, and Dynamic Objects can be selected from Available Attributes. Selectors refer to Attributes.

The screenshot shows the 'Add Rule' configuration page in FMC. The 'Dynamic Attributes' tab is selected and highlighted with a blue box. The 'Available Attributes' list is also highlighted with a blue box and contains the following items: Security Group Tag, Device type, Location IP, and Dynamic Objects. The 'Selected Source Attributes (0)' and 'Selected Destination Attributes (0)' sections are currently empty, with 'any' listed as the default attribute. The 'Add to Source' and 'Add to Destination' buttons are visible next to the attribute lists.

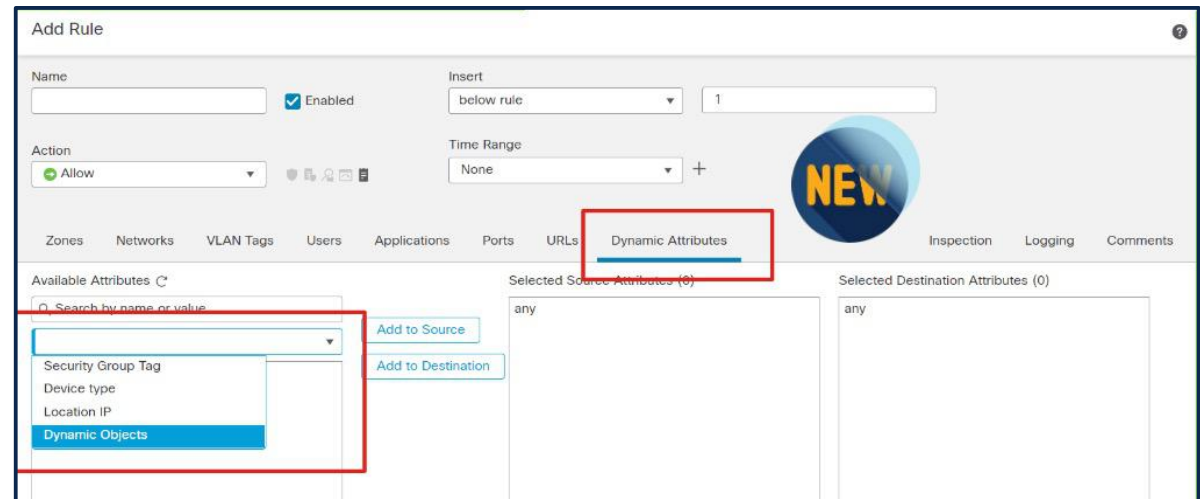
Cisco Secure Dynamic Attribute Connector



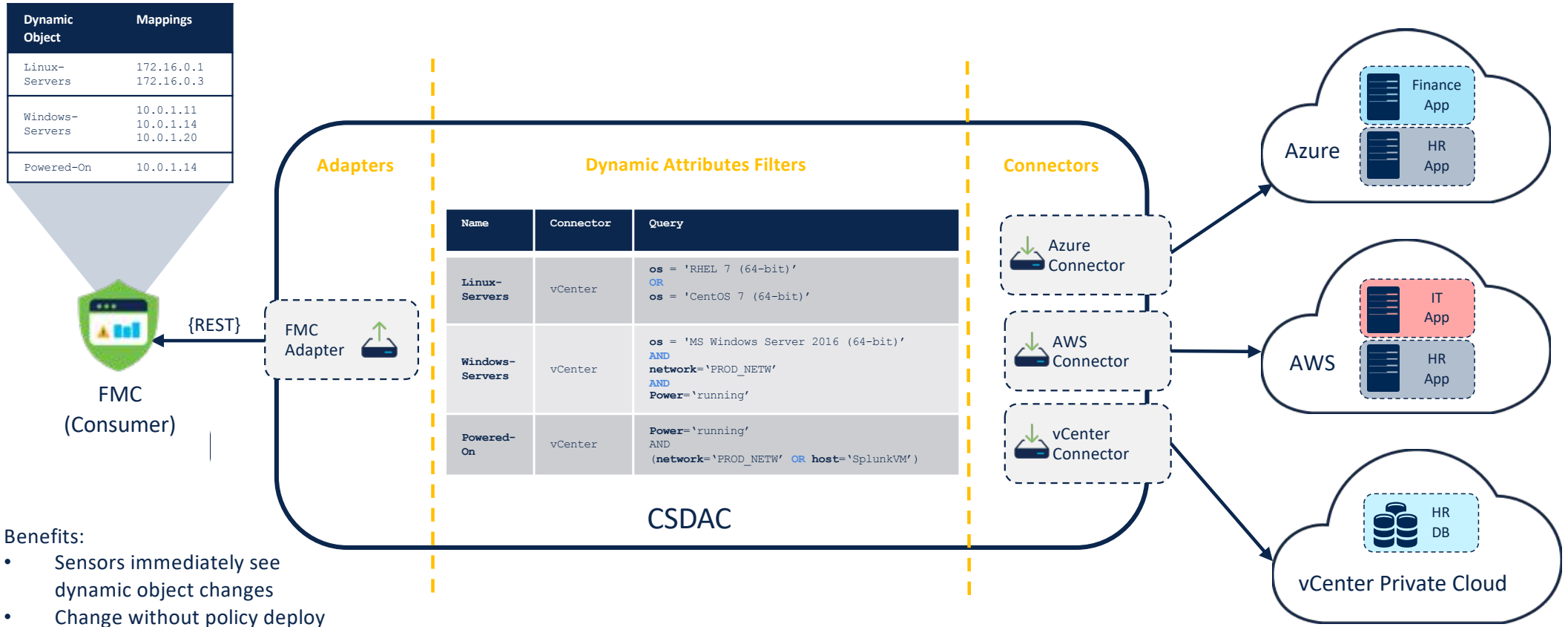
Problem: In a dynamic and multicloud world, admins struggle to keep up with ever changing object IPs as workloads are spun up, down and change.

Solution: Cisco provides a programmatic way to create, deploy and maintain dynamic objects. Enable for VMware, AWS, and Azure tags too.

Benefits: Dramatically reduces the admin overhead to keep security policies up to date, provides on demand updates without a deploy, and gains the confident control of cloud services and other dynamic environments.



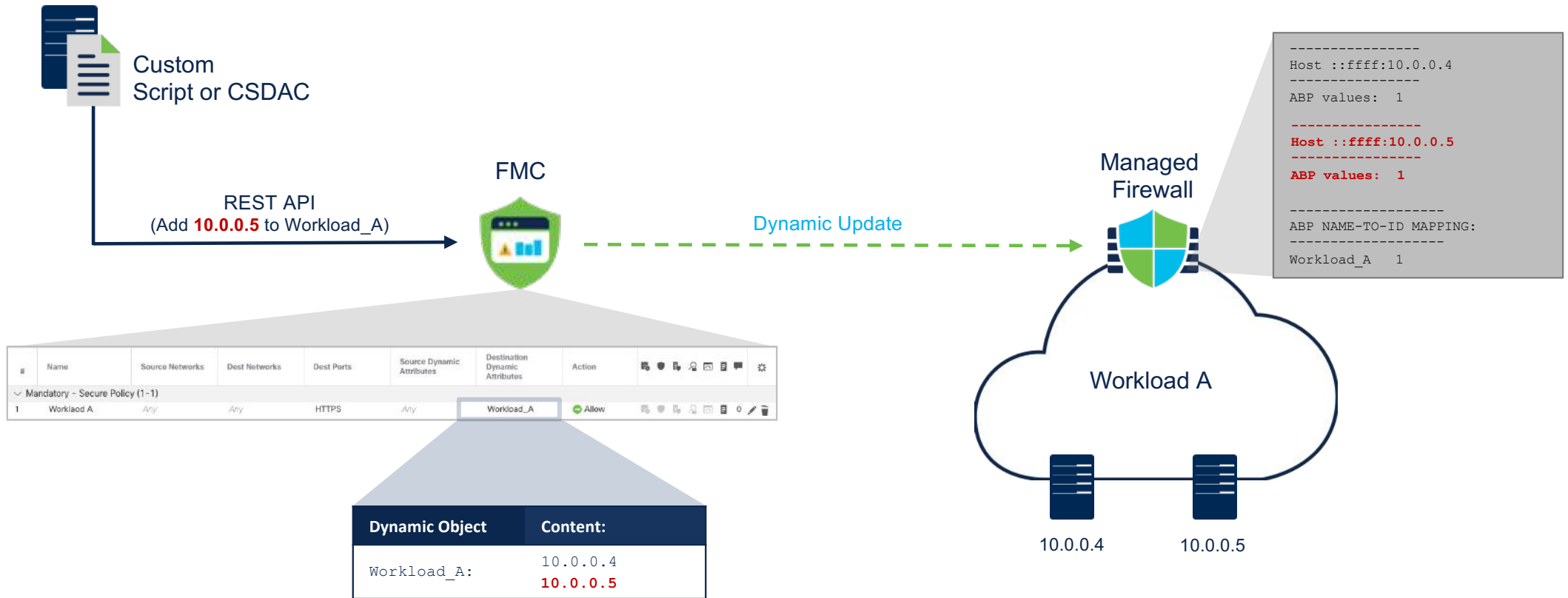
Cisco Secure Dynamic Attributes Connector (CSDAC)



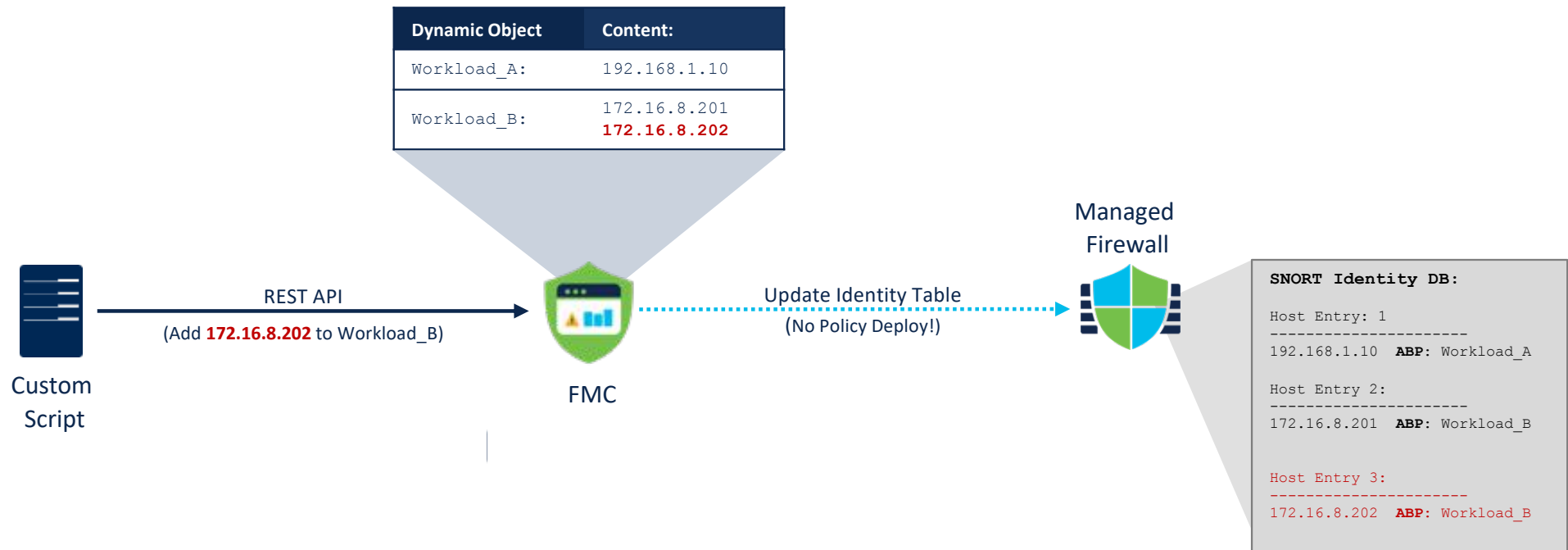
Benefits:

- Sensors immediately see dynamic object changes
- Change without policy deploy

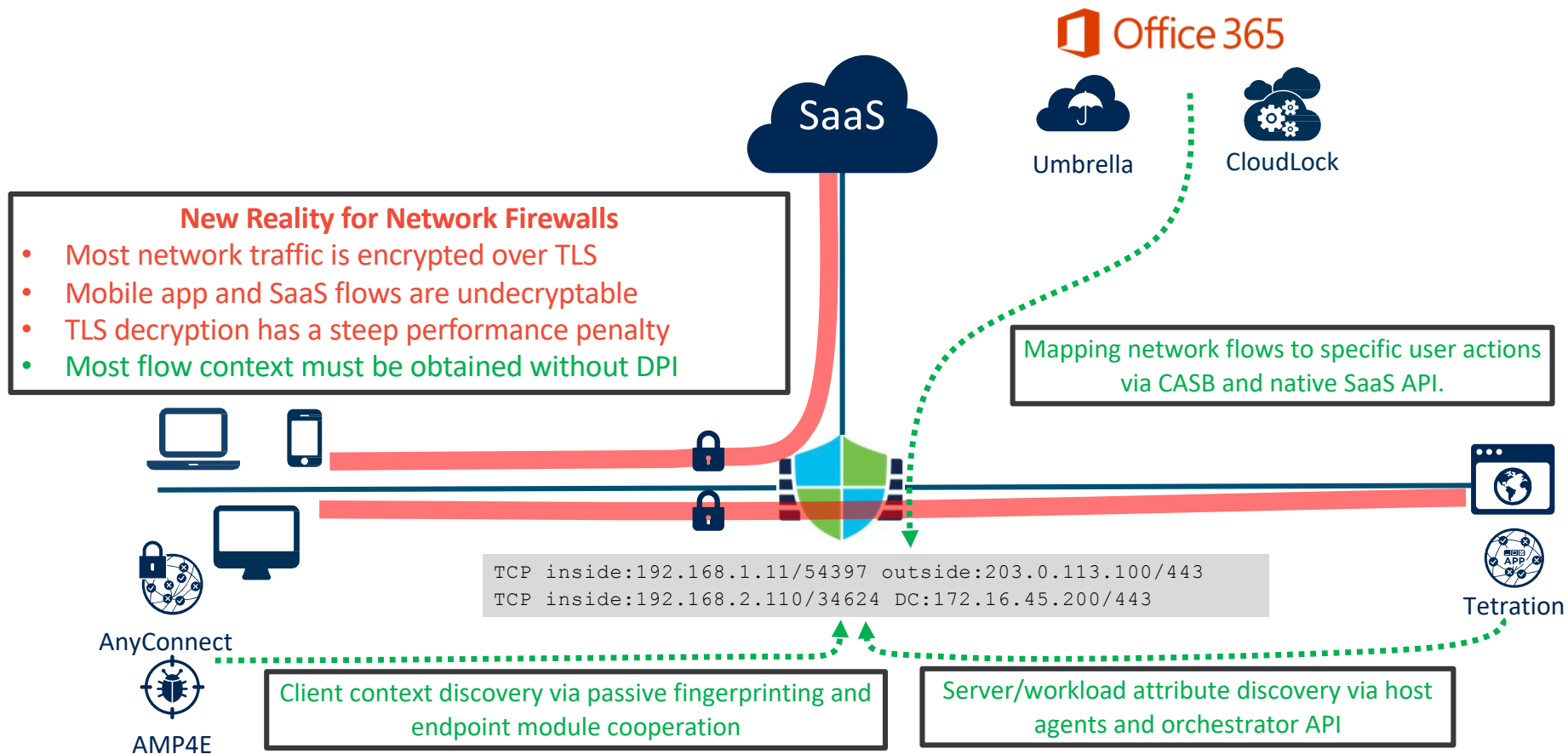
Solution: Dynamic Objects



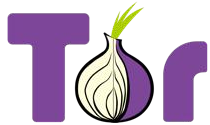
Identity Firewall – Dynamic Attributes



Flow inference beats Deep Packet Inspection (DPI)



App Fingerprinting



TCP/TLS 192.168.2.110/34624->172.16.45.200/443

TCP/TLS 192.168.2.110/21013->203.0.113.154/443

TLS ClientHello

```
▼ 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 (0xc030)
Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xc031)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc032)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc033)
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 (0xc034)
Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0xc035)
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**

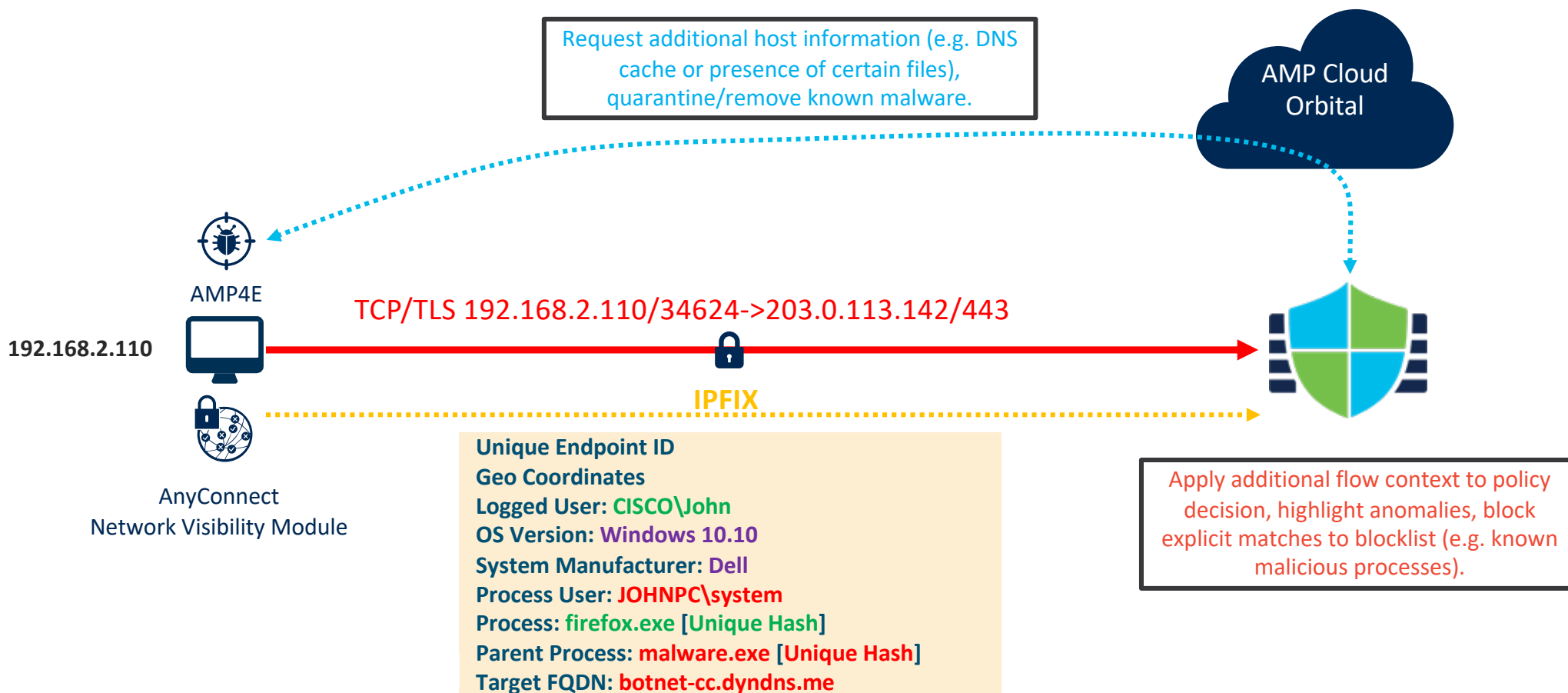
Generate unique fingerprints for client applications based on TLS, TCP, HTTP, and DHCP fields and use for policy matching and context enrichment.

TLS ClientHello

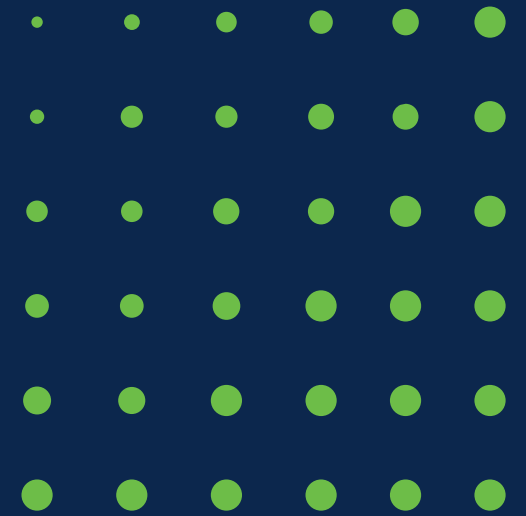
```
▼ Cipher Suites (19 suites)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (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: **nkskdlkoup.me**

Flow Context Enrichment via Client Endpoint



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 (77)
 open (1)

Assigned to Me (3)
 Assigned to Other (75)

Assigned to Me (2)

78

Firepower

Incident Promotion Reason

Last 7 Days

0

The data returned a value of 0

- 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)

Firepower

Event Summary

Last 7 Days

1 Total [🔗](#) 1 Intrusion [🔗](#) 0 Malware [🔗](#) 0 Security Intelligence [🔗](#)

Firepower

Talos IP Reputation

Last 7 Days

0 Poor [🔗](#) 0 Questionable [🔗](#) 1 Neutral [🔗](#) 0 Favorable [🔗](#) 0 Good [🔗](#)

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...
 - Talos Intelligence**

- 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
fmcv.prglab.local	No	0

Firepower Security Update Status

Firepower Management Center	Installed Version	Status
Intrusion Rule Update	fmcv.prglab.local	2021-07-21-001-vrt Latest

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 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 25, 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 19:25:59 UTC

Summary Observables Timeline Sightings Linked References (1)

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

192.168.44.150

IP · 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

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	
Malware - Ransomware_Petya_1.... Sighting Title Malware - Ransomware...									

Description

Sighting Title Malware - Ransomware_Petya_1.bin:26b4699a7b9eeb16e76305d843d4ab05e94d43f3201436927e13b3ebafa90739:2f3338b8-0f17-47b4-952c-233e9923ae0a

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

Observed By ftv.prglab.local

Source 192.168.44.150

Destination 192.168.42.150

FileDirection Download

SperoDisposition Spero detection performed

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 SHA...
- Show more

First Seen: Feb 25, 2021 @ 20:17
Last Seen: Feb 25, 2021 @ 20:17

26b4699a7b9eeb16e76305d843...

Malicious SHA-256 - 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

Threat Response Investigate Snapshots Incidents Intelligence Jiri Tesar

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 6 Modules

1 Network Gateway · 7 Endpoints · 1 Email Service · 1 Email

fmcv.prglab.local
 NETWORK GATEWAY
 AMP GUID: 122fe6db-3f5a-4106-b64f-52e4b8434c64
 HOSTNAME: fmcv.prglab.local

sec2-rdp
 WINDOWS 7 ENTERPRISE
 AMP GUID: 9cf4e0ac-02d9-43c0-9f24-ec50091d6762
 HOSTNAME: sec2-rdp
 IP ADDRESS: 192.168.43.195
 MAC ADDRESS: 00:50:56:9f:26:6d

VLNESA000192_421AE83648FC05562460-E0520C63...
 EMAIL SECURITY APPLIANCE

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

Jun 29, 2021 @ 12:30:15 CEST Jun 29, 2021 @ 12:36:36 CEST Jun 29, 2021 @ 12:42:30 CEST Jun 29, 2021 @ 12:42:32 CEST

Showing 19 of 24 nodes

Details

sec2-rdp
Endpoint

fmcv.prglab.local
Network Gateway

VLNESA000192...
Email Service

1 INVESTIGATED

0 OMITTED

22 RELATED

122fe6db-3f5a... AMP GUID

71422a82-bbb... 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-02d9-43c0-9f24-ec5009...
 IP Address: 192.168.43.195
 MAC Address: 00:50:56:9f:26:6d

My Environment (3) Global (3)

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

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

Sightings (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 6 Modules



Graph

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

26b4699a7b9eeb16e76305d843d4ab0594d43f3201436927e13b3ebafa90739

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 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
- Take Orbital Forensic Snapshot

Details

26b4699a7b9eeb16e76305d843d4ab0594d43f3201436927e13b3ebafa90739

Malicious SHA-256 Hash

6 Sightings in My Environ...

0 OMITTED

22 RELATED

122fe6db-3f5a... AMP GUID

16-421AE836... Cisco Message ID

enemy@gmail.c... Email Address

jitesar@prglab.l... Email Address

26b4699a7b9eeb16e76305d843d4ab0594d43f3201436927e13b3ebafa90739

Malicious SHA-256 Hash

My Environment (6) Global (63)

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

Judgements (66) Verdicts (3) Sightings (63) Indicators (6)

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 +

Group +

Filters

Time Range Sort ↕

Not Subscribed ▼

- ▶ **sec2-rdp** detected **c3c16b6d-7086-45de-9695-d73f59edbfbf.tmp** as **Win.Ransomware.Protected::W32.E908DCA957.Gen.A** Medium 📄 🗨️ ⚡ Threat Detected 2021-06-29 12:32:38 CEST
- ▶ **sec2-rdp** detected **f_000f82** as **Win.Ransomware.Protected::W32.E908DCA957.Gen.A** Medium 📄 🗨️ ⚡ Threat Detected 2021-06-29 12:32:38 CEST
- ▶ **sec2-rdp** detected **fddaaba9-756a-4449-9ec2-162539387d35.tmp** as **Win.Ransomware.Protected::W32.A6F10947D6.Gen.A** Medium 📄 🗨️ ⚡ Threat Detected 2021-06-29 12:32:29 CEST
- ▶ **sec2-rdp** detected **f_000f81** as **Win.Ransomware.Protected::W32.A6F10947D6.Gen.A** Medium 📄 🗨️ ⚡ Threat Detected 2021-06-29 12:32:29 CEST
- ▶ **sec2-rdp** detected **f_000f81** as **Win.Ransomware.Protected::W32.A6F10947D6.Gen.A** Medium 📄 🗨️ ⚡ Threat Detected 2021-06-29 12:32:29 CEST
- ▼ **sec2-rdp** detected **Ransomware_Petya_1.bin** as **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)	26b4699a...afa90739 ▼
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)	6a465b60...29889771 ▼
	Parent Filename	TOTALCMD64.EXE
<input type="button" value="Report"/> <input type="text" value="100"/> <input type="text" value="5"/> <input type="button" value="Restore File"/> <input type="button" value="All Computers"/>		<input type="button" value="View Upload Status"/> <input type="button" value="Add to Allowed Applications"/> <input type="button" value="File Trajectory"/>

6 total events / page

Device Trajectory

Take a Tour Share Use Legacy Device Trajectory

sec2-rdp 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** (26b4699a...afa90739 [PE_Executable] as W32.Malwaregen:Petya.22kr.1201).

Created by TOTALCMD64.EXE (6a465b60...29889771 [Unknown]) executing as cisco@SEC2-RDP.

The file was **quarantined**.

File full path: C:\Users\cisco\Downloads\Malware!!!\Ransomware_Petya_1.bin

File SHA-1: 39b6d40906c77f080e6bfa93324dddadcbdb9a.

File MD5: af2379cc4d607a45ac44d62135fb7015.

File size: 230912 bytes.

Parent file age: 0 seconds.

Parent process id: 5632.

Parent process SID: S-1-5-21-327574462-428459281-2074746256-1000.

Detected by the Tetra engines.

Device Trajectory

Take a Tour Share Use Legacy Device Trajectory

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

Hostname	sec2-rdp	Group	JT prglab Protect Group
Operating System	Windows 7 Enterprise	Policy	JT prglab Protect
Connector Version	7.4.1.20439	Internal IP	192.168.43.195
Install Date	2021-06-19 20:01:13 CEST	External IP	64.103.36.133
Connector GUID	9cf4e0ac-02d9-43c0-9f24-ec50091d6762	Last Seen	2021-07-23 16:18:55 CEST
Definition Version	TETRA 64 bit (daily version: 85200)	Definitions Last Updated	2021-07-20 17:58:15 CEST
Update Server	tetra-defs.eu.amp.cisco.com		
Processor ID	1f8bfbff00006f2		

Filters Search Device Trajectory

Related Events

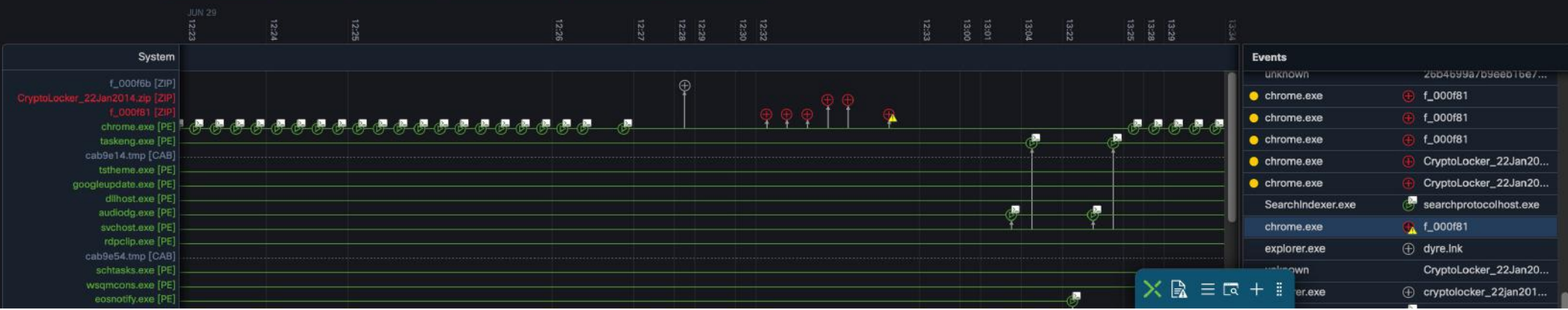
Vulnerabilities

Medium	Threat Detected	a6f10947...2c4f0b24	2021-06-29 12:32:29 CEST
Medium	Quarantine Fail...	a6f10947...2c4f0b24	2021-06-29 12:32:29 CEST
Medium	Threat Detected	a6f10947...2c4f0b24	2021-06-29 12:32:29 CEST
Medium	Threat Quaranti...	a6f10947...2c4f0b24	2021-06-29 12:32:29 CEST

No known software vulnerabilities observed.

Orbital: Unsupported OS (requires 64-bit Windows 10 version 1709 or later) Events Diagnostics View Changes

- Start Isolation
- Scan...
- Diagnose...
- Move to Group...
- Begin Work
- Mark Resolved



Events

UNKNOWN	26b4699a7d9e8016e7...
chrome.exe	f_000f81
chrome.exe	f_000f81
chrome.exe	f_000f81
chrome.exe	CryptoLocker_22Jan20...
chrome.exe	CryptoLocker_22Jan20...
SearchIndexer.exe	searchprotocolhost.exe
chrome.exe	f_000f81
explorer.exe	dyre.lnk
UNKNOWN	CryptoLocker_22Jan20...
er.exe	cryptolocker_22jan201...

Dashboard

Dashboard **Inbox** Overview Events iOS Clarity

No Agentless Cognitive Incidents detected

6.7% compromised

Reset New Filter

30 days 2021-06-24 19:45 2021-07-24 19:45 CEST

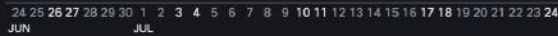


Significant Compromise Artifacts

FILE	a6f10947...2c4f0b24	Dyre.zip	1
FILE	e908dca9...92308b14	CryptoLocker_22J...	1

Compromise Event Types

Medium	Threat Quarantined	1
Medium	Threat Detected	1
Medium	Quarantine Failure	1



1 Requires Attention 0 In Progress 0 Resolved

Begin Work Mark Resolved Move to Group...

Sort Date

sec2-rdp in group JT prglab Protect Group 8 events

1 record 10 / page 1 of 1

Dashboard

Groups Select Groups

Dashboard **Inbox** Overview Events IOS Clarity

Refresh All Auto-Refresh

Take a Tour

30 days 2021-06-24 19:46 2021-07-24 19:46 CEST

6

Threats Detected

0

Network Threats

5

Quarantines

1

Compromises

0

Exploits Prevented

0

Retrospective Events

0

Connectors Deployed

0

Threat Grid Submissions

Compromises

1 Compromises total - 0 In Progress - 0 Resolved

By Event



By Host



Threats

Root Cause



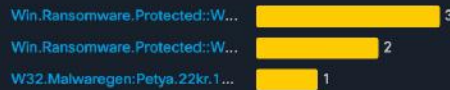
Resolution



By Host



By Threat Name



Vulnerabilities

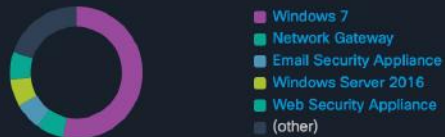
No data to display

File Analysis

No data to display

Computers

By Host



Version Deployment



Network Threats

No data to display

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

loads Email Security Web Security Stealthwatch prglab Endpoint Security **FW + Endpoint** > [Customize](#) Maximum Available Interval

AMP for Endpoints Computers Summary

15 Computers [↗](#) 9 Seen > 7 days ago [↗](#) 8 Need AV Update [↗](#)

AMP for Endpoints Summary

1 Computers With Quarantines [↗](#) 1 Computers Compromised [↗](#)

11 Out of Date Connectors [↗](#) 0 Vulnerable Executions [↗](#)

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,...

INCIDENTS

Incidents [New Incident](#) <

Search...

- Assigned to me - Open (4)
- Assigned to me - New (9)

Malware event Ransomware_Petya_1.bin	NGFW Event Service	Sep 03, 2020
Malware event Ransomware.Petya.zip	NGFW Event Service	Jun 29, 2021
Malware event Ransomware_Petya_1.bin	NGFW Event Service	Jun 29, 2021
Malware event Ransomware_Petya_1.bin	NGFW Event Service	Jan 14, 2021
Malware event Ransomware_Petya_1.bin	NGFW Event Service	

Malware event Ransomware_Petya_1.bin

Malware event - Ransomware_Petya_1.bin:26b4699a7b9eeb16e76305d843d4ab05e94d43f32

New · Created By [NGFW Event Service](#) on 2021-06-29 10:42:00 UTC

Summary Observables Timeline Sightings Linked References (1)

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

- 26b4699a7b9eeb16e76305d843d4ab05e94d43f3201436927e13b3ebafa90739 [Malicious SHA-256](#) · 1 Target · 1 Sighting
First: 2021-06-29T10:36:35.000Z · Last: 2021-06-29T10:36:35.000Z
- Ransomware_Petya_1.bin [File Name](#) · 1 Target · 1 Sighting
First: 2021-06-29T10:36:35.000Z · Last: 2021-06-29T10:36:35.000Z
- 192.168.42.150 [IP Address](#) · 1 Target · 1 Sighting

26b4699a7b9eeb16e76305d843d4ab05e94d43f32

[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 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](#)
 - [Take Orbital Forensic Snapshot](#)

[Request Tier 2 Approval for AMP Host Isolation] [Supported observable: AMP GUID]

Workflow Description:
When triggered, this workflow requests approval to isolate an endpoint using AMP host isolation. If approved, isolation is enabled using the CTR AMP isolation response action.

Workflow Requirements:
This workflow requires the Task Approver and Task Requestor global variables be populated. If you want to send emails, you need to enable the Send Email activity and verify your SMTP target configuration. Please verify these settings prior to execution.

Since the workflow uses the CTR response action, please ensure the endpoint can be isolated using the "AMP For Endpoints" module from the pivot menu.

Manage Incident [Link](#)

Info

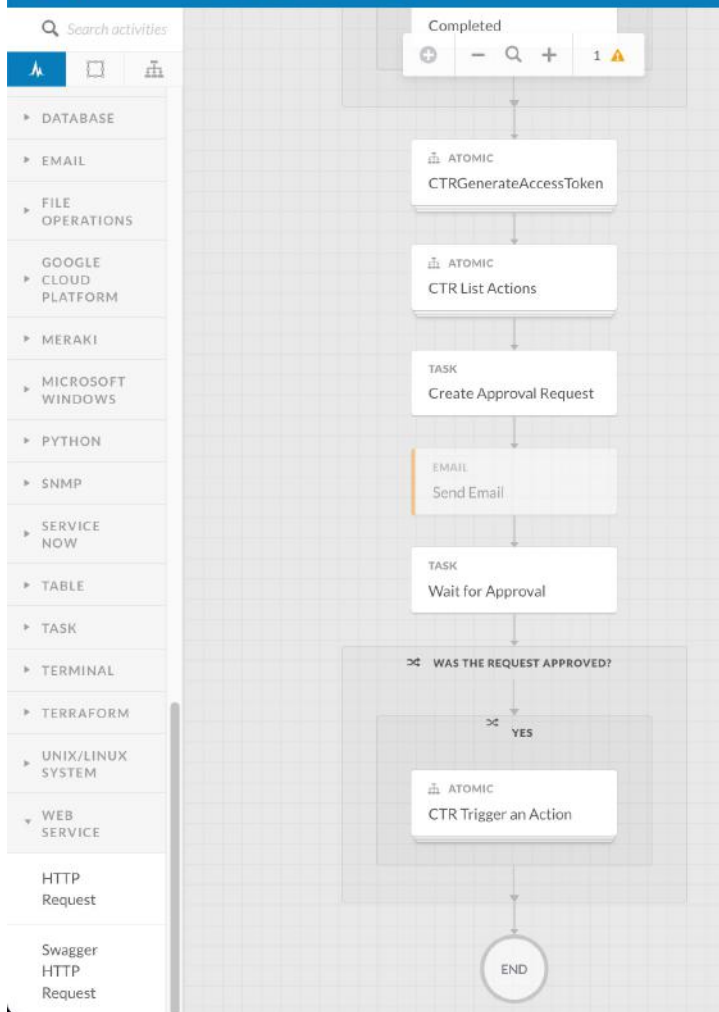
Assignees · [Add](#)

- Jiri Tesar

Key Properties

- Categories: [Select ...](#)
- Disc. Method: [NIPS](#)
- Intend. Effect: [Select ...](#)
- Confidence: [High](#)
- TLP: [Amber](#)

AMP Host Isolation with Tier 2 Approval



26b4699a7b9eeb16e76305d843...

Malicious SHA-256 - AMP Global Intelligence...

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

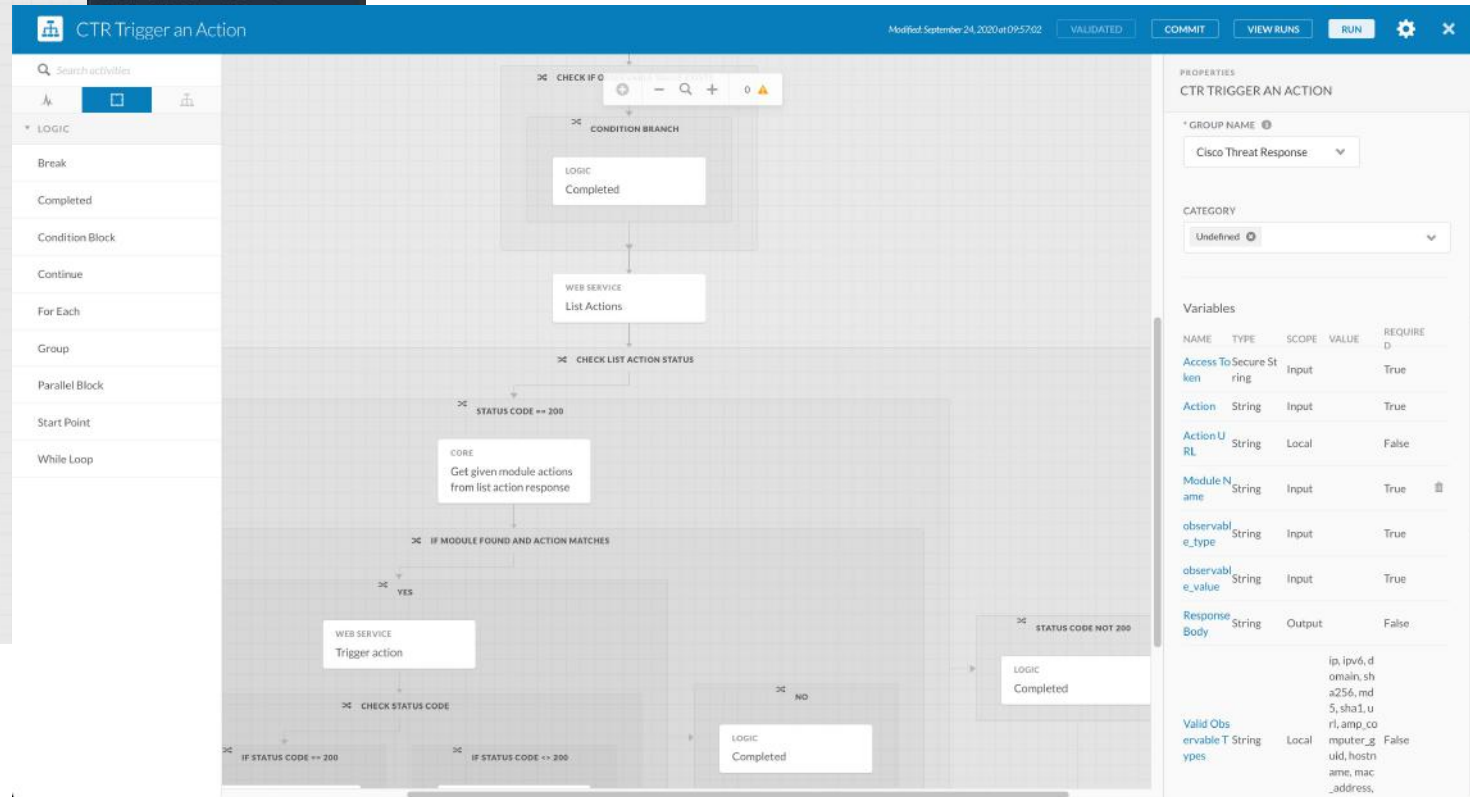
Investigate in Threat Response

- Create Judgement
- AMP for Endpoints
- File trajectory
- Search for this SHA256
- Add SHA256 to custom detections 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

SecureX Orchestration



PROPERTIES

CTR TRIGGER AN ACTION

* GROUP NAME

Cisco Threat Response

CATEGORY

Undefined

Variables

NAME	TYPE	SCOPE	VALUE	REQUIRED
Access To Secure St...	ring	Input		True
Action UR	String	Input		True
Action U	String	Local		False
Module N...	String	Input		True
observabl...	String	Input		True
observabl...	String	Input		True
Response B...	String	Output		False
Valid Obs...	T String	Local	ip, ipv6, d omain, sh a256, md 5, sha1, u rl, amp, co mputer_g uid, hostn ame, mac _address,	False

Fall 2020
6.7 / 9.15.1

Spring 2021
7.0 / 9.16.1



Ease of Use and Deployment

- Remote Deployment via CLI (bootstrap) 🔥
- Change Management for FMC (config rollback - 10 versions, audit log enhancements, syslog to multiple destinations) 🔥
- FMC Usability improvements (copy/move rules)
- Upgrade Improvements (rollback of major versions, better error reporting) 🔥
- Deployment Time Optimizations for standalone & HA
- Device Health Monitoring 🔥
- Multi-instance backup & restore

- Policy & Event troubleshooting improvements & unified live event view (FMC)
- Scalable eventing & logging (SWATCH integration)
- Device install & upgrades optimization (25% rule)
- Dynamic Objects capability
- Flow-offload support for multi-instance
- CDO as manager of FMCs
- No Snort 3 restarts on VDB updates



World-Class Security Controls

- Improved Identity Firewall scale (filtering via CLI) 🔥
- FMC UI responsiveness improved by 35%
- RA VPN feature parity with ASA phase 1
- Static VTI – S2S Cloud VPN connectivity
- Further PAT improvements for clustering 🔥
- Snort 3 use by CDO & FDM
- FMC – SSO with SAML support
- HTTP/2 support & threat efficacy improvements
- pxGrid 2.0 integration

- RA VPN feature parity with ASA phase 2 (SAML authorization 🔥, DAP policy editor 🔥, AC custom attributes, AC customization, load balancing)
- Static VTI – DHCP relay over VTI, OSPF and IPv6
- Snort 3 for FMC
- Further threat efficacy improvements & default config updates
- Global search in FMC



Unified Policy and Threat Visibility

- FTD support edge/branch <1000 users*:
 - IPS custom policies
 - Notifications
 - Basic health dashboard
 - FTD Low-touch onboarding in CDO (1000, 2100)
- Cloud management for MSPs (Cross tenant management, RBAC)
- Meraki Layer 7 support in CDO integration

- FTD support for Enterprises <1000 users*
 - API enhancements and resilience/scalability
- Cross-domain group controls
- Duo integration (with SAML)
- SNMPv3 for FTD
- Live event view streaming



Deploy Everywhere

- Autoscale for ASAv, Autoscale for FTDv in Azure & AWS
- Google Cloud, Oracle Cloud, Amazon Accelerated Networking
- FMCv HA for VMware hypervisor
- Massive enhancements in FMC, FDM and FTD API
- FXOS-FTD link-state sync

- SecureX integration & ACI integration pack
- FTDv and ASAv for OpenStack
- SD—WAN on FTD integration



Bring Customers to Next Era

- URL/AppID support for TLS 1.3
- ThreatGrid API v3

- Umbrella SIG integration (automatic tunnels)
- Web Application Firewall

Fall 2020
6.7 / 9.15.1

Spring 2021
7.0 / 9.16.1

	Fall 2020 6.7 / 9.15.1	Spring 2021 7.0 / 9.16.1
RA VPN (IPsec/ SSL/TLS)	<ul style="list-style-type: none">• LDAP Authorization for RA using LDAP attribute map• API Support for AnyConnect modules (enable/disable) and Configs• PKI enhancements: Certificate Revocation Support• DAP/Hostscan API• FMC support for LDAP Authorization for RA using LDAP attribute map• FMC - Support for Anyconnect modules (enable/disable) and Configs• FMC SAML 2.0 VPN-RA Authentication• FMC PKI Management Enhancements (cert chain support - at least 3 level of depth in the chain)• FTD - API Enabling back DAP/Hostscan Minimalistic API	<ul style="list-style-type: none">• Dynamic Access Policy Editor, includes Hostscan Config Editor• FMC SAML 2.0 VPN-RA Authorization• Support for AnyConnect custom attributes• Support for AnyConnect Customization• Load Balancing• Cert Mgt/PKI Enhancements• Monitoring Dashboard (FDM)• AnyConnect Profile attributes/Editor support• Local Authentication• SGT Assignment
S2S VPN	<ul style="list-style-type: none">• Static & Dynamic VTI – S2S Cloud VPN connectivity	<ul style="list-style-type: none">• DHCP relay on VTI• S2S VPN monitoring improvements• Support for:<ul style="list-style-type: none">• IPv6• EIGRP• OSPF

Silver Bullets

DC Technology:

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

Identity, Device, Health,...

- Integration with ISE, AMP, Vulnerability Scanners,...

Automation

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

Talos

- IPS
- Security Intelligence
- AMP

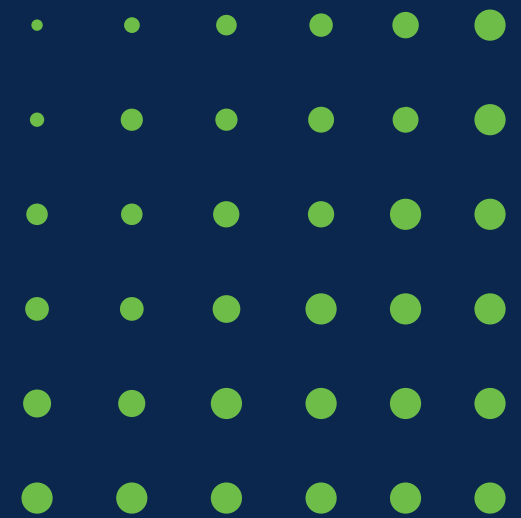
VPN

- Easy to install, also with virtual
- DUO MFA

Encrypted traffic

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

Děkuji za pozornost





SECURE