cisco Live!

Let's go

The bridge to possible

Design, Deploy and Troubleshoot Network Detection and Response

Secure Network Analytics

Hanna Jabbour, Leader Technical Marketing Engineer SBG
@hanna_jabbour

BRKSEC-2248

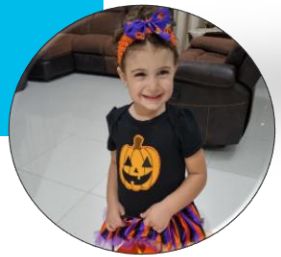
Agenda

- Introduction
- What are the core components
- Legacy and new Architecture
- Deployment Flow and Strategies
- Transitions
- Telemetry Ingest
- Conclusion

Who Is your presenter

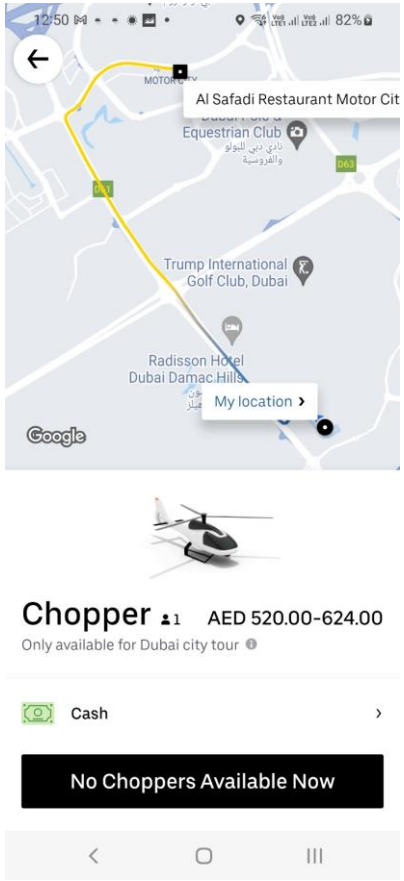
Hanna Jabbour

- 15 years of experience in Dev/Network/Security
- TME for Secure Analytics covering EMEAR/APJ
- Lebanese based out of the Dubai
- Yes, my name is Hanna



Lebanon | Dubai

https://www.youtube.com/watch?v=INiCIW2VpCI



Introduction

Secure Network Analytics

Cisco XDR

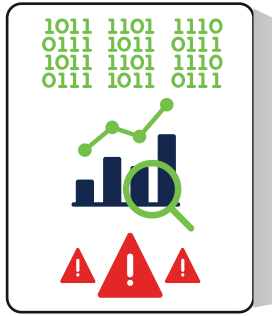
Extended Detection and Response with Cisco XDR. Advanced analytics extends local detections with global intelligence and integrations for accelerated response

Multilayered machine learning

Combination of supervised and unsupervised techniques to convict advanced threats with high fidelity

Behavioral modeling

Behavioral analysis of every activity within the network to pinpoint anomalies



Secure
Network Analytics

Endpoint Telemetry

Device and process insight with flow telemetry from Cisco Secure Client

Data collection

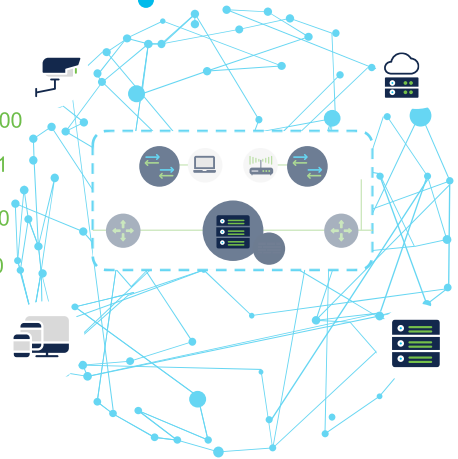
Rich telemetry from the existing network infrastructure including enhanced telemetry for encrypted traffic analytics

1001110111010111000

100111011101011

1001110111010

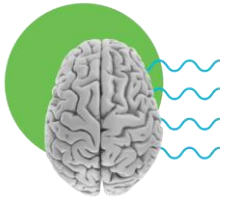
1001110111010111000



Cisco Secure Network Analytics

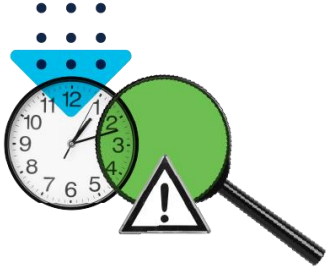
Contextual network-wide visibility

Agentless, using existing network and cloud infrastructure, even in encrypted traffic



Predictive threat analytics

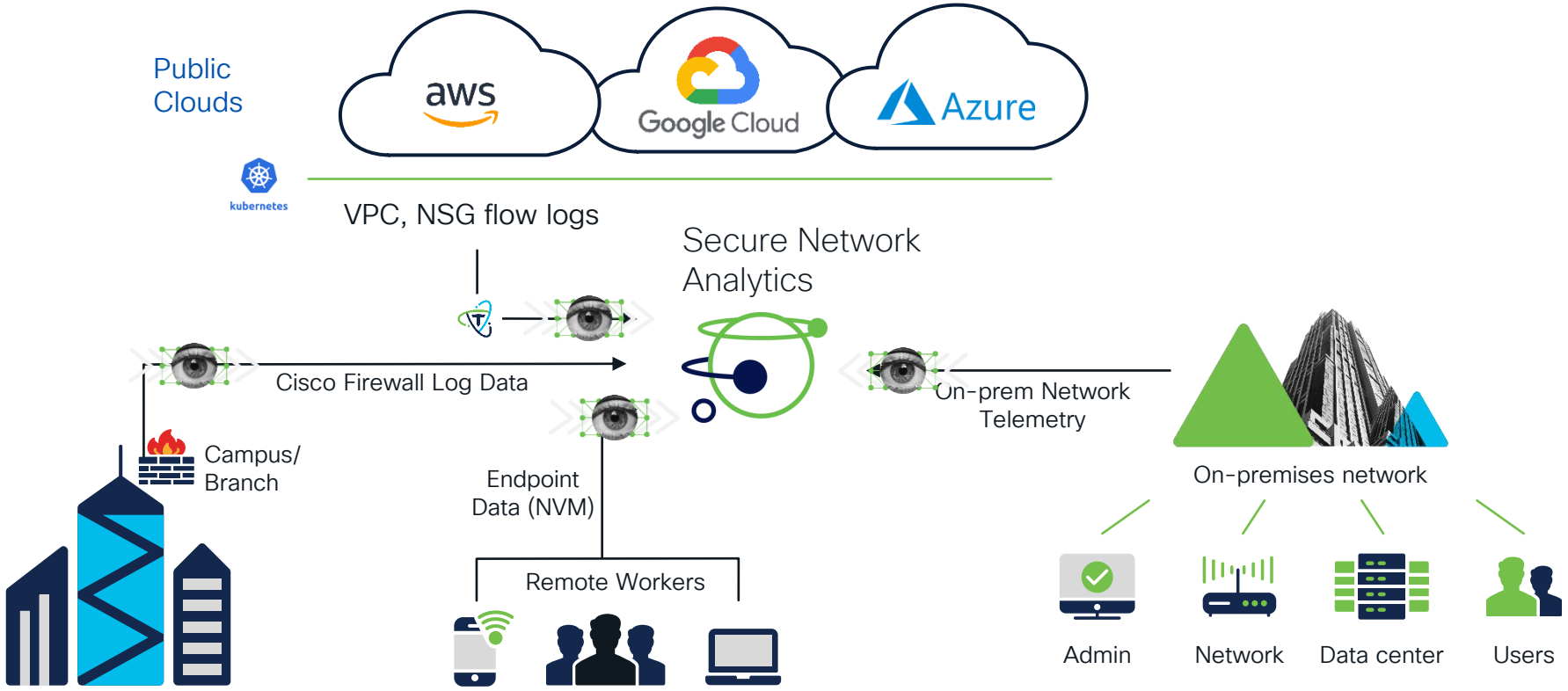
Combination of behavioral modeling, machine learning and global threat intelligence



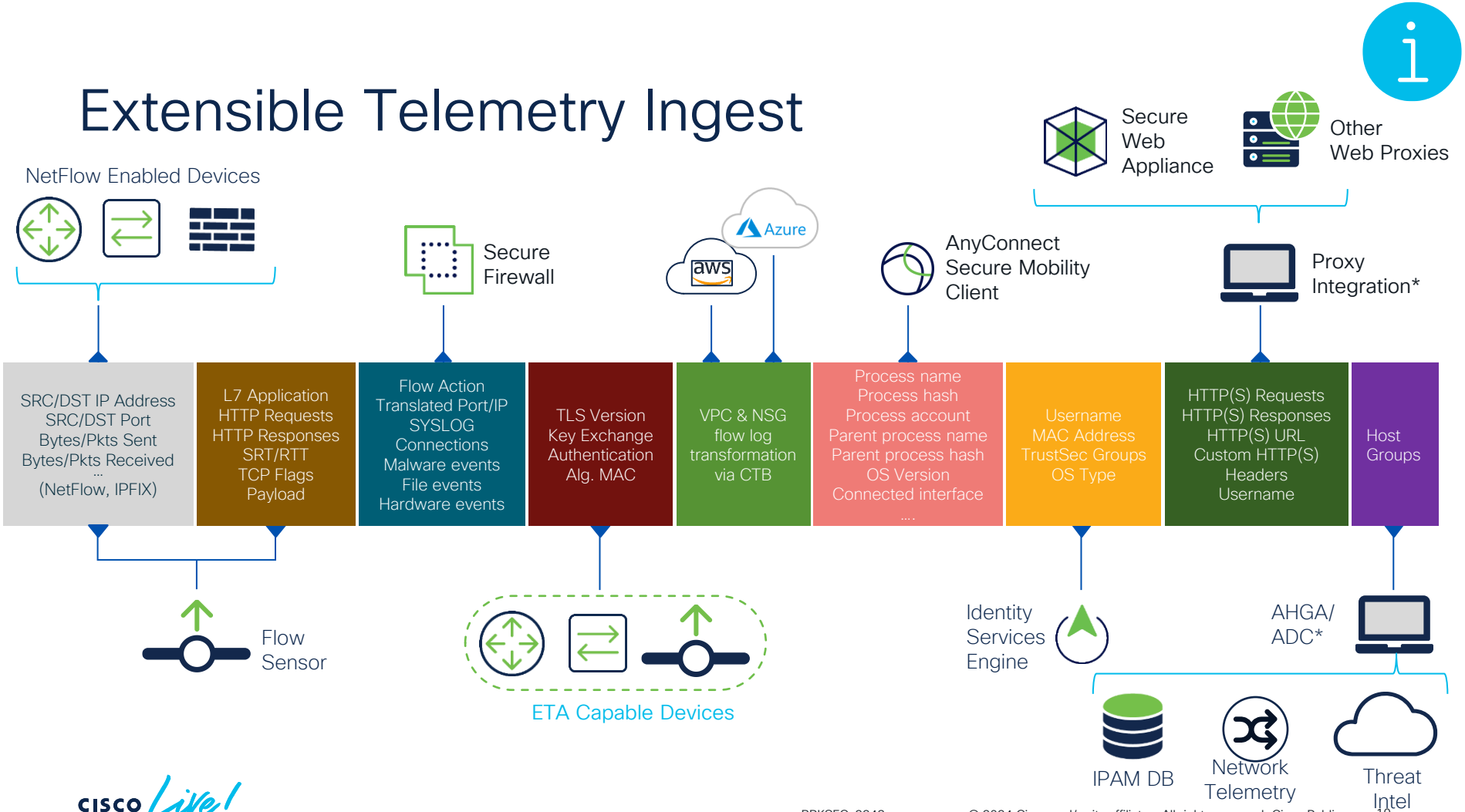
Automated detection and response

High-fidelity alerts prioritized by threat severity with ability to conduct forensic analysis

Multi-telemetry ingest and visibility



Extensible Telemetry Ingest

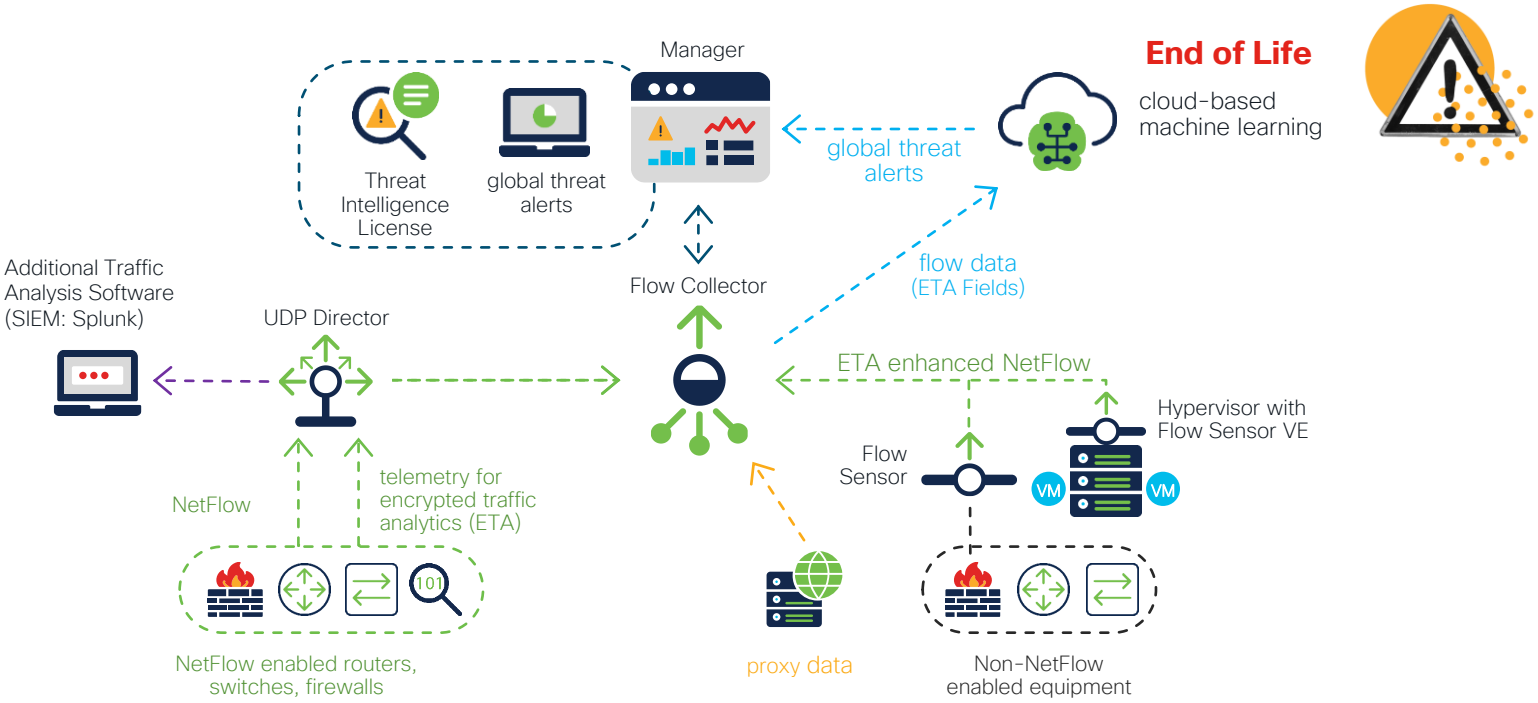


If You Fail to Plan, You Are Planning to Fail

Benjamin Franklin

Core Components
Old Architecture

Secure Network Analytics Component Icons



Secure Network Analytics components

Manager

SMC VE (Virtual Edition)
SMC 2210

- SMC for Management and Configuration supports:
- Up to 25 Flow Collectors
- 10000 Network Access User sessions
- 15 concurrent managing users
- Scale up to 6 Million FPS in one deployment

Flow Collector

Flow Collector VE
FC 4210/FC5210

- Flow Collector is the center of Data Collection and Analytics.
- Up to 25 FC per deployment
- Up to 240 000 FPS per FC
- Up to 6TB of Flow Storage
- Up to 1Million Host Classified
- Up to 4000 Data Source per FC

Flow Sensor

Flow Sensor VE
FS1210/FS 3210/FS4210

- Ingest SPAN to generate telemetry and contextual data.
- Up to 80Gbps per FS, Copper and Fiber supported interface,
- 1Gb, 10Gb and 40 Gb monitor interfaces

NOT FOR SALE

UDP director

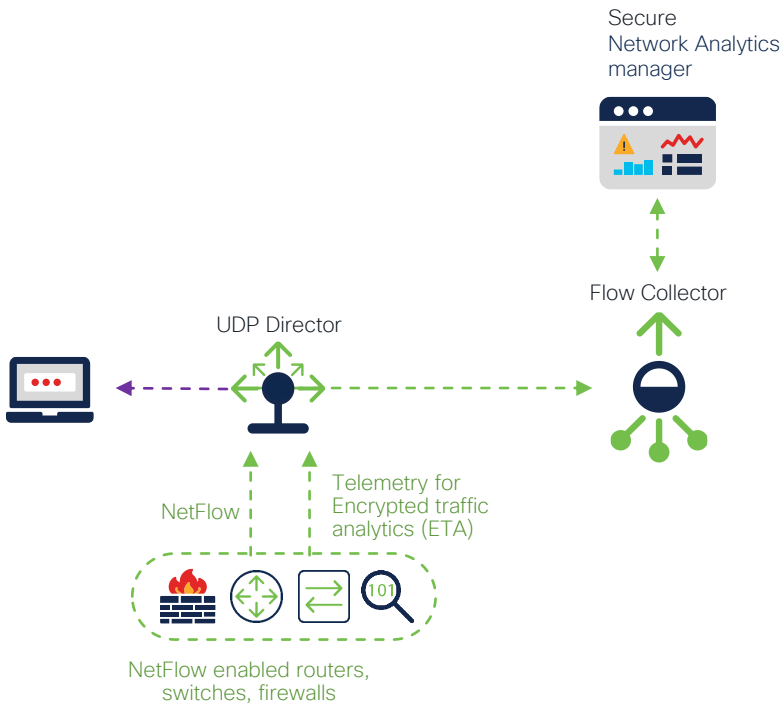
UDP Director VE (Virtual edition)
UDPD 2210

Replicates UDP traffic and generates NetFlow from SPAN traffic supporting:

- 1Gbps/10Gbps interfaces
- Up to 150,000 pps

Allows NetFlow, SYSLOG and SNMP data to be sent transparently to multiple collection points

Provides additional flexibility and ease of deployment



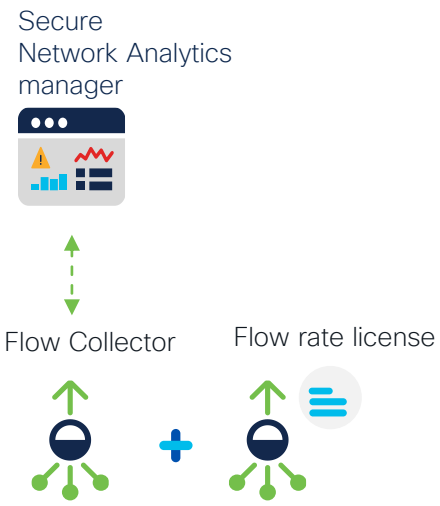
Required core components

Secure Network Analytics manager

- A physical or virtual appliance that aggregates, organizes, and presents analysis from flow collectors
- Central management for all Secure Network Analytics devices
- User interface to Secure Network Analytics
- Maximum 2 per deployment

Flow collector (FC)

- A physical or virtual appliance that aggregates, normalizes and analyze telemetry and application data collected from exporters such as routers, switches, and firewalls
- High performance NetFlow/SFlow/IPFIX collector
- Maximum 25 per deployment

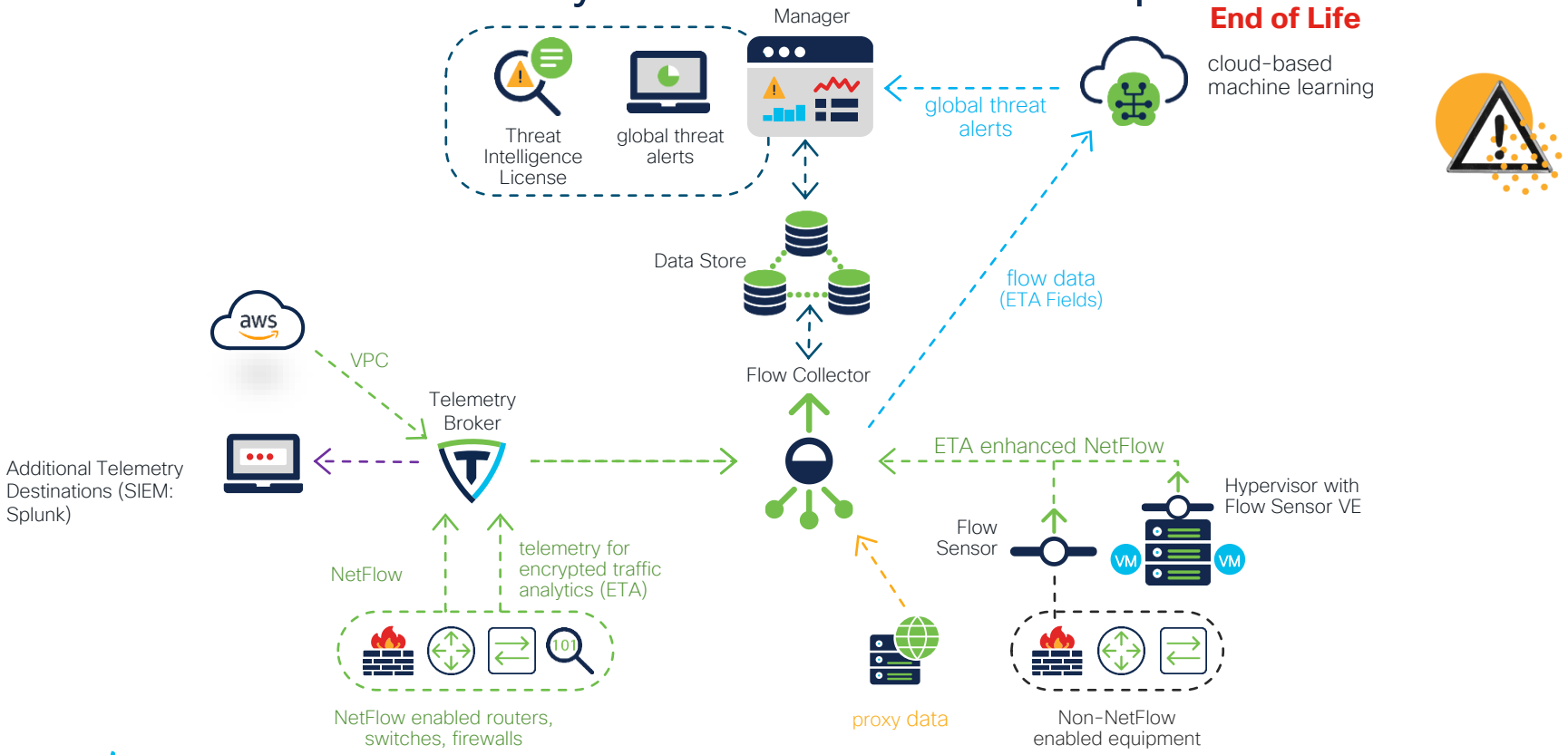


Flow rate license

- Collection, management, and analysis of telemetry by Secure Network Analytics
- The flow rate license is simply determined by the number/type of switches, routers, firewalls and probes present on the network
- FPS estimation Tool
  https://apps.cisco.com/cfgon/public/app/lancope/fpsestimator.jsp#/add-items

Core Components New Architecture

Secure Network Analytics Data Store Component & CTB



Data Store Required core components

Secure Network Analytics manager

- A physical or virtual appliance that aggregates, organizes, and presents analysis from flow collectors
- Central management for all Secure Network Analytics devices
- User interface to Secure Network Analytics
- Maximum 2 per deployment

Flow collector (FC)

- A physical or virtual appliance that aggregates, normalizes and analyze telemetry and application data collected from exporters such as routers, switches, and firewalls
- High performance NetFlow/SFlow/IPFIX collector
- Maximum 25 per deployment

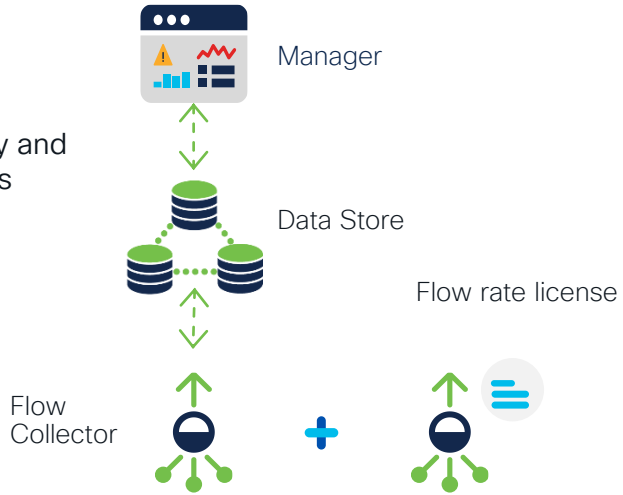
Data Store (DS)

- A physical or virtual appliance that store data in a scalable, resilient way.
- Maximum 12 per deployment (36 nodes)

Flow rate license

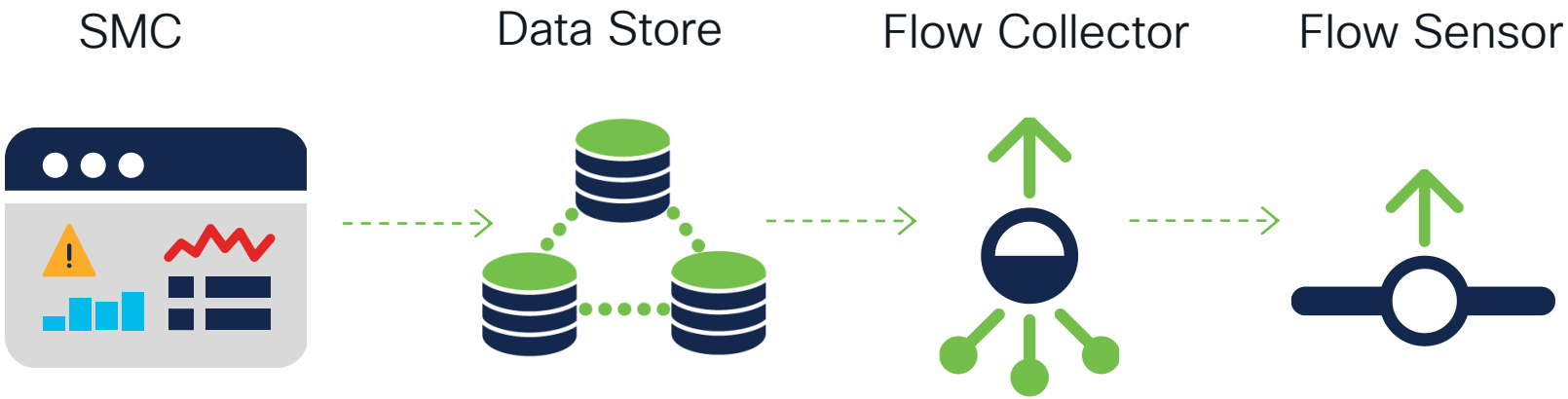
- Collection, management, and analysis of telemetry by Secure Network Analytics
- The flow rate license is simply determined by the number/type of switches, routers, firewalls and probes present on the network
- FPS estimation Tool: https://apps.cisco.com/cfgon/public/app/lancope/fpsestimator.jsp#/add-items

Secure Network Analytics Deployment



Deploy

Deployment Order



Virtual Edition Resources

RESERVERD RESOURCES

SMC

Concurrent Users*	Required Reserved CPUs	Required Reserved Memory	Required Minimum Storage
up to 9	6	40 GB	200 GB
over 10	12	70 GB	480 GB

FC with no Data store

Flows per second	Required Reserved CPUs	Required Reserved Memory	Required Minimum Data Storage for 30 Days	Interfaces	Exporters
Up to 10,000	2	24 GB	600 GB	Up to 65535	Up to 1024
Up to 30,000	6	32 GB	900 GB	Up to 65535	Up to 1024
Up to 60,000	8	64 GB	1.8 TB	Up to 65535	Up to 2048
Up to 120,000	12	128 GB	3.6 TB	Up to 65535	Up to 4096

Virtual Edition Resources

RESERVERD RESOURCES

FC With Data Store

Flows per second	Required Reserved CPUs	Required Reserved Memory	Required Minimum Storage	Interfaces	Exporters
Up to 10,000	2	24 GB	200 GB	Up to 65535	Up to 1024
Up to 30,000	6	32 GB	200 GB	Up to 65535	Up to 1024
Up to 60,000	8	64 GB	200 GB	Up to 65535	Up to 2048
Up to 120,000	12	128 GB	200 GB	Up to 65535	Up to 4096

Single Data STORE

Flows per second	Required Reserved CPUs	Required Reserved Memory	Required Minimum Storage for Single Data Node for 30 Days of Retention
Up to 30,000	6	32 GB	2.25 TB
Up to 60,000	6	32 GB	4.5 TB
Up to 120,000	12	32 GB	9 TB
Up to 225,000	18	64 GB	18 TB

Deployment Requirements

NOT FULL List of Ports

Device Information

- IP addresses for appliances to be deployed
- DNS Server IP(s)
- NTP Server IP(s)
- SMTP relay (if needed)
- Internal IP ranges in use/to be monitored

Only for Data Store per node

- Non-routable IP Address from the 169.254.42.0/24

Communication Ports –NOT Full LIST

From (Client)	To (Server)	Port	Protocol
Admin User PC	All appliances	TCP/443	HTTPS
Admin User PC	All appliances	TCP/22	SSH
All appliances	Network time source	UDP/123	NTP
Flow Collector	SMC	TCP/443	HTTPS
Manager	Flow Collector	TCP/443	HTTPS
Manager	Flow Sensor	TCP/443	HTTPS
Manager	Internet	TCP/443	HTTPS
Manager	DNS	UDP/53	DNS
Flow Sensor	SMC	TCP/443	HTTPS
Flow Sensor	Flow Collector	UDP/2055	NetFlow
NetFlow Exporters	Flow Collector	UDP/2055*	NetFlow

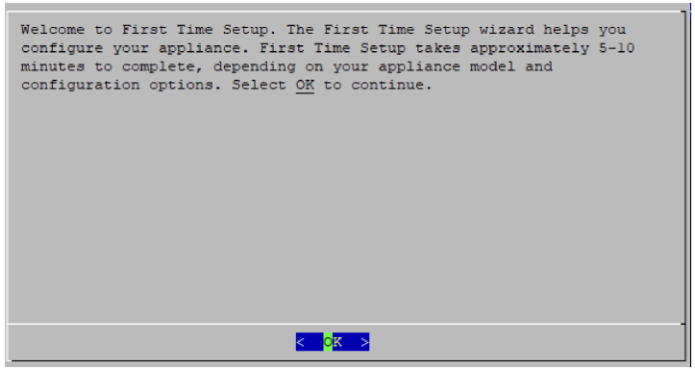
Deployment Steps

Reboot is common between steps

First Time Setup

- Interface SFP or BaseT Selection
- IP address Subnet Configuration
- For Data Node 2nd IP non-routable
- For FC Telemetry Selection and UDP Port Definition

Console



Appliance Setup Tool

Removed 7.5
Less Restart

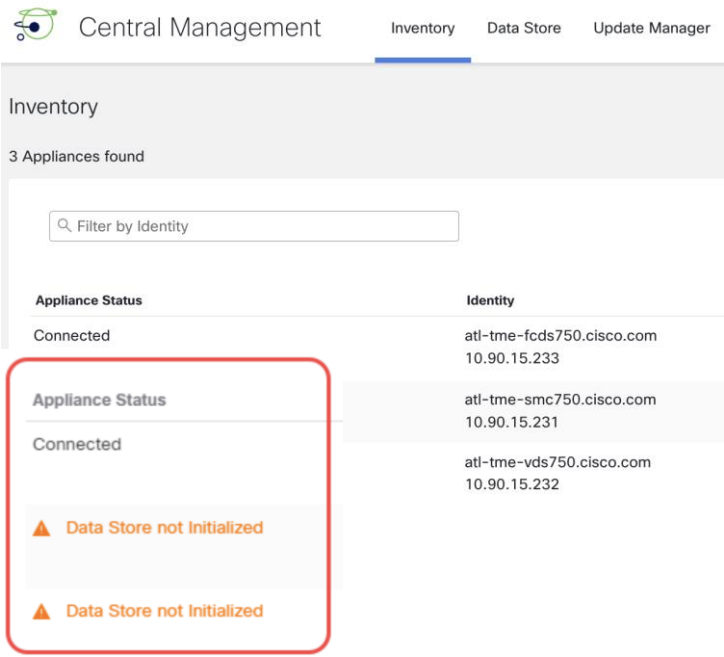
- Password Change
- IP address Subnet Configuration Verification
- SNA Domain and Type Type (DS or Not)
- DNS and NTP
- Registration to Central Manager

Http://IPaddress

Cenralized Management

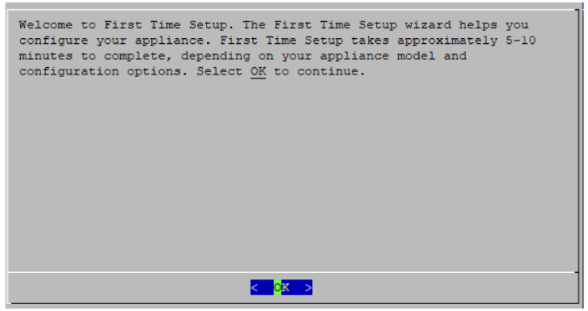
Connect With the Manager

- Connecting to the Manager
- Will also Use the AST (Appliance Setup Tool) (From FST in 7.5)
- After the AST Reboot
- Devices Connected
- Data Store Not Initialized



Initialize the Data Store

- Go back to the Central Manager console
- Initialize the Data Store



Smart Licensing Deployment Options

Direct

- Cisco product sends usage information directly over the internet. No additional components are needed.

On-Prem

- Cisco products send usage information to a locally installed appliance.
- Periodically, exchange information with Cisco to ensure license usage is accurate.
- This synchronization can occur automatically in connected environments or manually in disconnected environments.

Offline
(not recommended)

- Use copy/paste information between product and Cisco.com to manually check in and out licenses.
- Functionally equivalent to older node locking, but with Smart License tracking.

Licensing Notes

- After 90 Evaluation period ends the system will stop processing new flows
  - Still functional with historical data, but new flow data will not be processed
  - This is the <u>ONLY</u> hard enforcement used in Smart Licensing

- After a system is registered and the associated licensing periods expire or are exceeded there is no hard enforcement
  - The system will display banners informing users they are out of compliance, but the system will still process flow

Flow estimation

- It is an estimated Value unless you do a PoV

- FPS license is based on 95th percentile, for 95% of the time the FPS actual is AT or BELOW the stated amount

Expand All | Collapse All

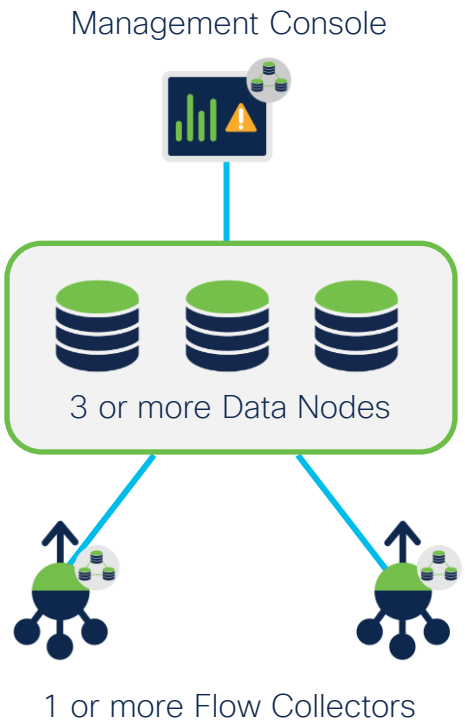
Access Switch	0	0.00
Distribution Switch	0	0.00
WAN Router	0	0.00
Wireless Access	0	0.00
Data Center	0	0.00
Core Switch	0	0.00
Flow Sensor Throughput	0	0.00
Firewall	0	0.00
End Point License (anyconnect)	0	0.00
Weblogs	0	0.00
	Total FPS Count	0.00

For every 1000 fps per day you need 1 GB storage at the Flow Collector

The Data Store

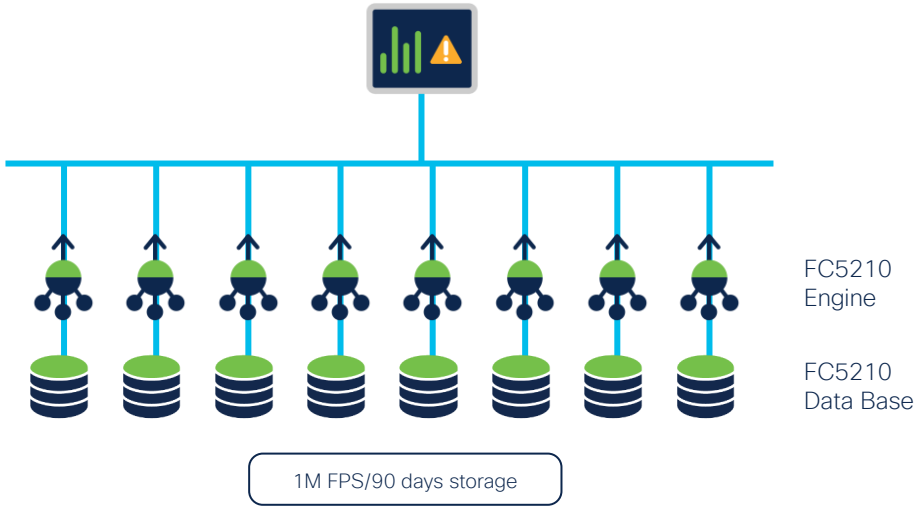
What is the Data Store

- The Data Store is a new and improved database architecture design for SNA
- Each individual Data Store appliance will include a 3-Node database cluster
- Flow ingest by Flow Collectors is separated from data storage
- This distributed design enables scalable and resilient data storage, providing retention times of over a year
- Queries are handled by the Data Store, effectively increasing performance across all metrics by a significant magnitude



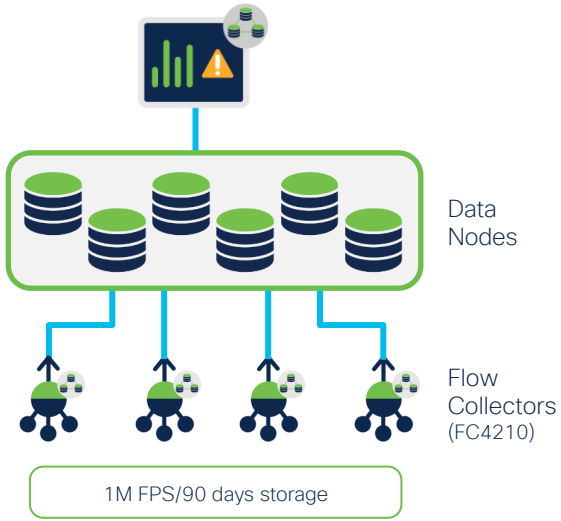
With and Without the Data Store

Current Customer Deployment



- 16 total nodes: 8 data nodes + 8 Flow Collectors (FC)
- Coupled Data collection & storage

New Data Store Deployment



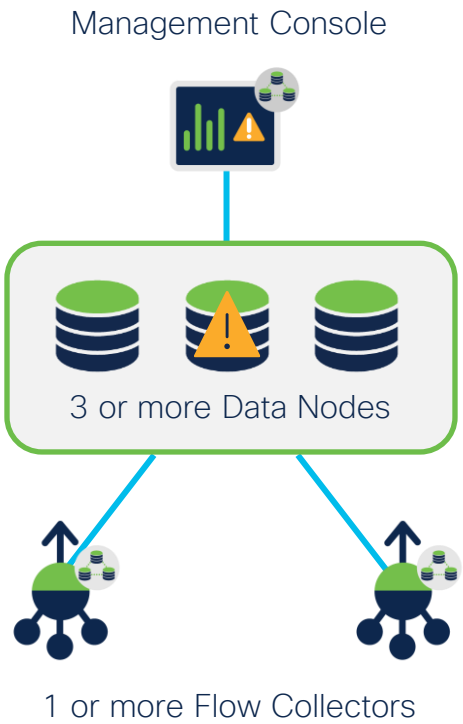
- 10 total nodes: 6 data nodes + 4 FC
- Independent data collection & storage
- Efficient and optimized data storage

Data Resiliency

In addition to extending retention time, the Data Store also introduces enterprise-class data resiliency

- Telemetry data is stored redundantly across nodes to allow for seamless availability during single node failures
- Seamless availability for a Data Store deployments

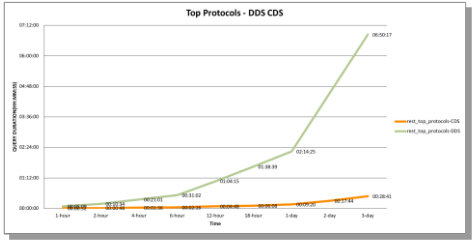
- In addition the Data Store supports redundant inter-connection switches, thus remaining in operation during network upgrades and unplanned outages

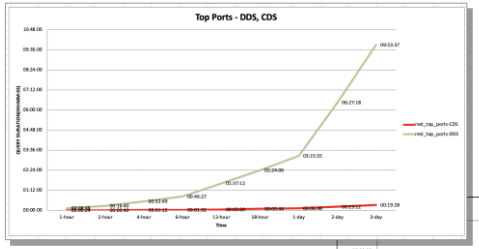


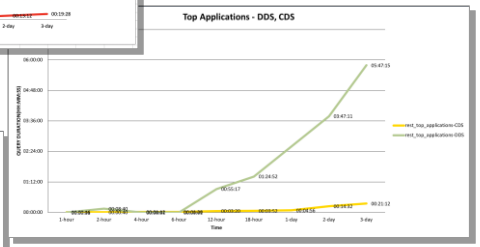
Data Store Performance

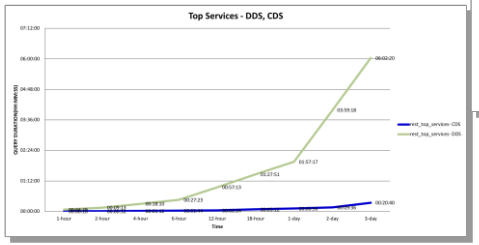
Top Reports	Non-DS	Data Store
Applications	5hr 47min	21min
Hosts	29hr 36min	19min
Ports	9hr 53min	19min
Protocols	6hr 50min	28min
Services	6hr 2min	20min

- Large Enterprise traffic, ran for **3 days at 150,000 fps** into two hardware testbeds:
  - FC5210 (Non-Data Store)
  - 3-Node Data Store with a FC4210
- After 3 days, **19.4 Billion flows** were written to each testbed bed



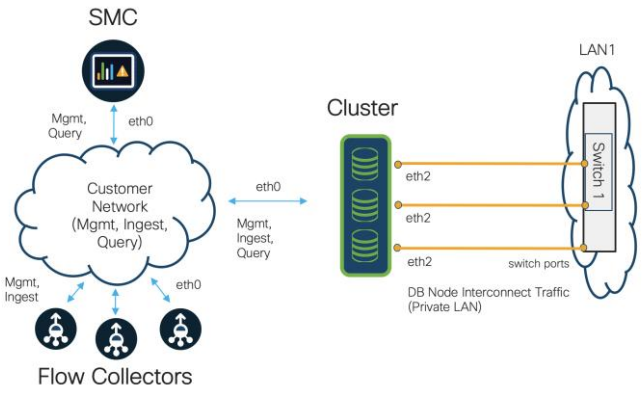






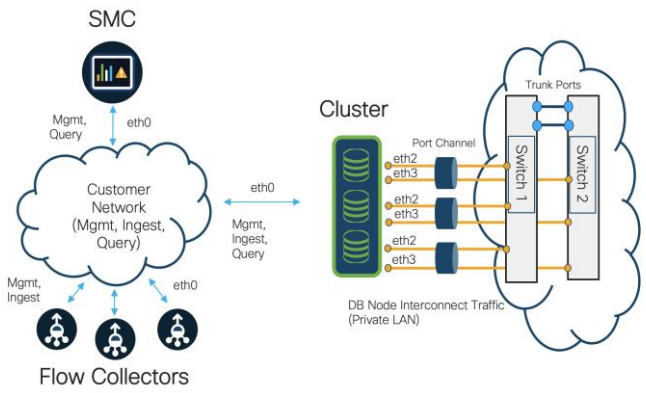
Data Store Deployment

Single Switch Architecture



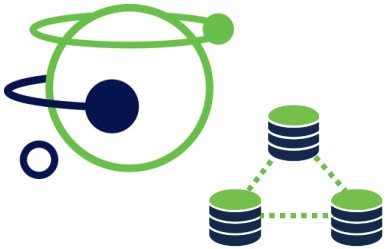
- eth2 or eth3 can be used for internode communications
- Must be 168.254.42.x/24

Two Switch Architecture



- Provides resiliency for switch failure using port channels and interconnected trunk ports
- Uses both eth2 and eth3 for port channel

Data Store Evolution



7.3.0

Data Store on HW Data Nodes is introduced

7.3.1

Virtual Data Nodes were added, enabling virtual deployment

7.3.2

Added new telemetry types, Firewall logs and Remote worker visibility, all NVM fields

7.4.0

Virtual Manager and Flow Collector(s) and a physical Data Store Support added for ASA firewall logs

7.4.1

Expand to Data Store

- Single Node
- Multi-Telemetry
- New Analytics

7.4.2

Transition to Data Store

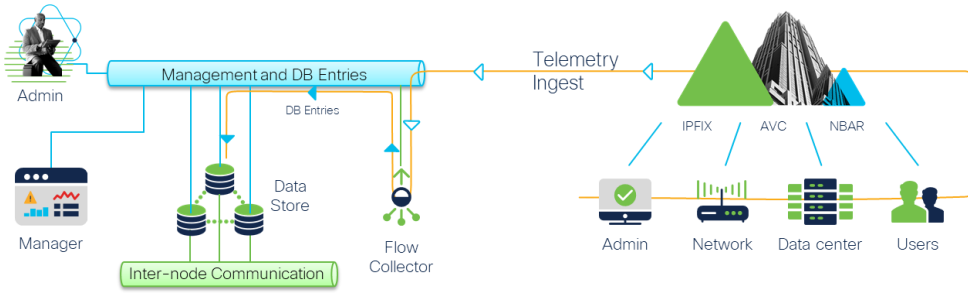
- Existing customers can transition to Data Store

Geo-Redundancy

- New peer site design

M6 HW Support

- SFP Interfaces



The single node Data Store

- Single node Data Stores can be either virtual or physical appliances
- Supports up to 4 Flow Collectors
- Easily expands to a full 3 node cluster, which now supports N+1 horizontal scaling
  - Note: A Data Store must consist of homogenous data nodes, either all virtual or all physical appliances

Data Store
Single Data Node

Virtual or physical

Expand/Scale as needed with FCs

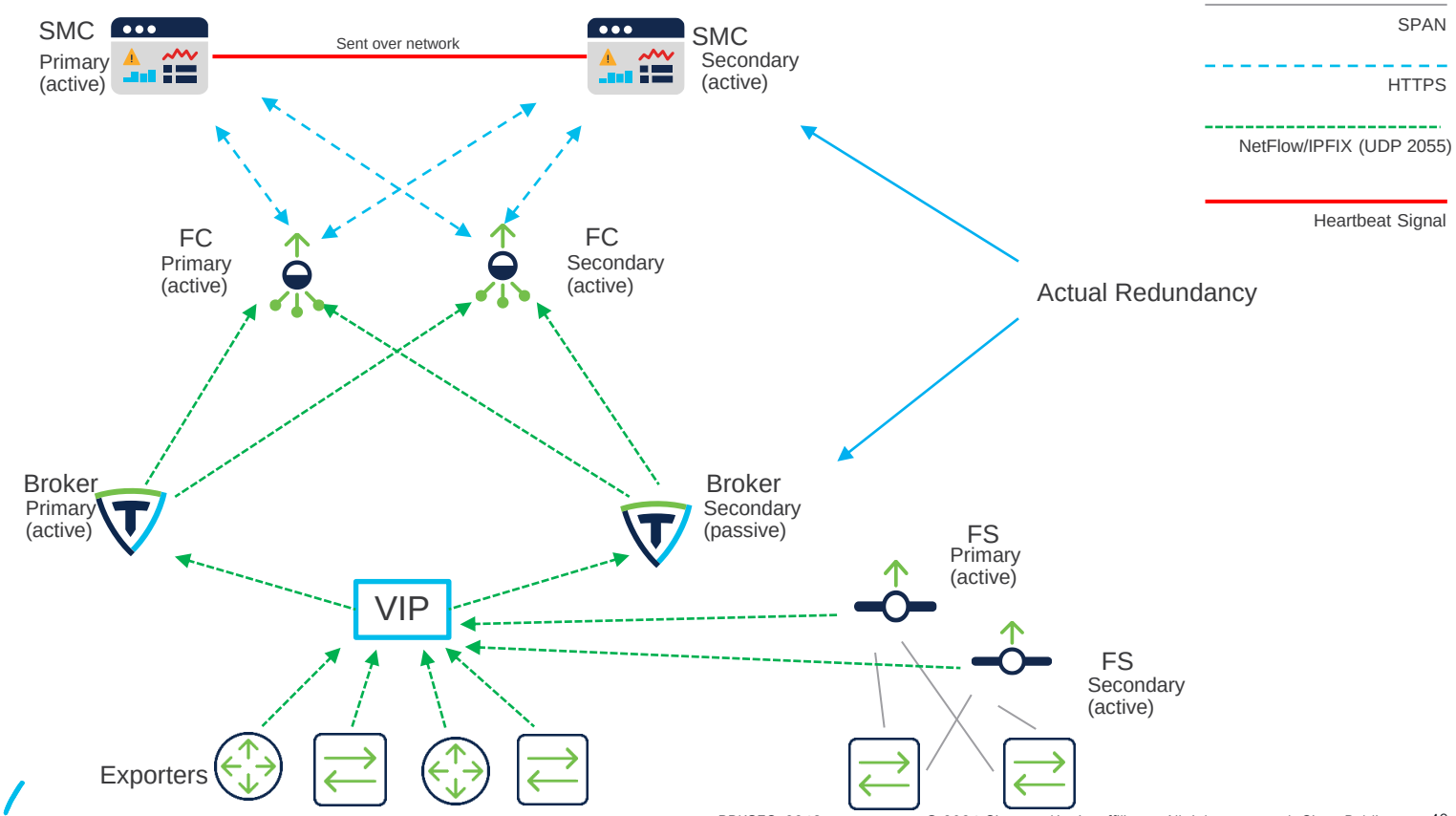
Single node virtual Data Store scales to 225K FPS

Single node physical Data Store scales to 500K FPS

Demo Data Store

Redundancy

Redundancy – High Level Design – Non-Data Store



Redundancy – Notes– Non Data Store

- SMC redundancy follows active – active (but no change)
- Flow Collector redundancy is active active and done by design

- Flow Collector redundancy required double licensing
- CTB help in achieving the flow collection redundancy

- Flow Sensor redundancy is active – active

Resilient central storage for multi-geo ingestion

- Flow Collector consolidates redundant flow date into context rich bi-flow records
- Highly efficient compression minimizes WAN impact when backhauling telemetry data
- Telemetry data is stored redundantly across data nodes to help ensure data availability even during a data node failure

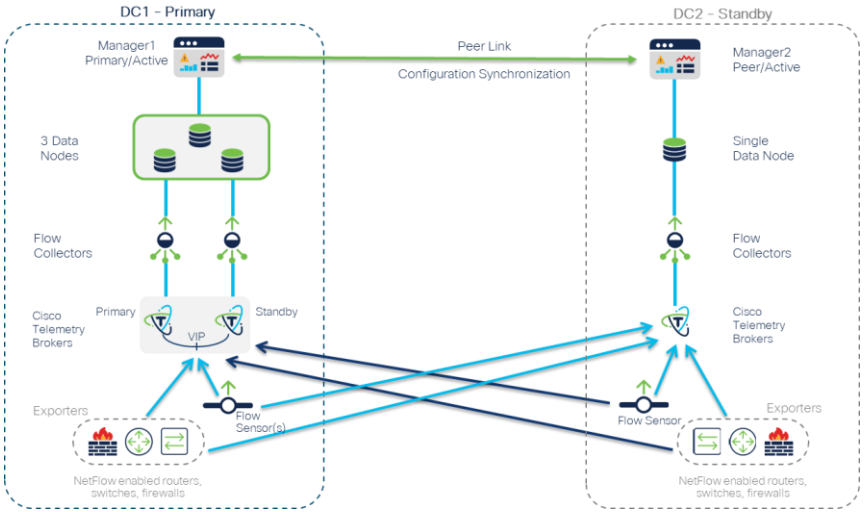
- Redundant inter-connection switches, help to ensure the Data Store stays in operation during network upgrades and unplanned outages

Redundancy – New Architecture

Requirement: Geographical redundancy while minimizing footprint

Solution: Peer Sites

- Primary deployment is associated to a peer site where configurations are sync'd
- Both sites run and operate independently, allowing great flexibility to meet customer operational reqs
- Site telemetry is sent to both primary and peer sites.
- Primary site can be robust HW appliances where peer site is smaller virtual deployment reducing OPEX
- Peer sites based on Active/Standby Managers design, and is supported within peer sights for large Enterprises demanding full redundancy



What are the gotchas?

- Java/Swing client is not supported with Data Store
  - BU is actively working to close reporting and data visibility gaps
- Peer Site sync is manual
- 3+ DC designs are not supported today
  - BU: Investigating extending peer site for this purpose
- Multiple Data Stores are not supported by a single Manager
- Converged Analytics cannot support multiple domains, it runs on one domain at a time

Cisco Telemetry Broker

Telemetry Sources

- NetFlow / sFlow
- Syslog
- SNMP Trap
- VPC Flow Logs
- Endpoint (NVM)
- Application Sources ...and more

Sources = Network, Application, or Cloud provider points of telemetry egress.

CTB Distributed Nodes

- **Broker**
- **Transform**
- **Filter**
- **Anonymize**

↑

API

Telemetry Destinations

- Cisco Secure Network Analytics
- Cisco On-Prem Platforms (DNA Center, Secure Workload)
- Cisco Cloud Services (Secure Cloud Analytics, CDO, SecureX, SSE*)
- 3rd Party On-Prem (Home grown Data Lakes, Live Action, SevOne)
- 3rd Party Cloud Services (SIEM/Datadog/ServiceNow)
- Storage (Archival, Audit)

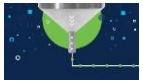
*integrations under investigation

Cisco Telemetry Broker Democratizes Telemetry Data

Brokering

The ability to route and replicate telemetry data from multiple source locations to multiple destinations

Replicate Telemetry	>>>>>>	Quickly enable PoV/onboarding of non-incumbent tools
Route Telemetry	>>>>>>	Let teams run the tools of their choice without deploying new agents/collectors



Filtering

The ability to filter data being replicated to enable fine grain control over what destinations ingest and analyze

Filter to Drop and Segment	>>>>>>	Control Costs: Only index high value data
	>>>>>>	Compliance: Keep low value data in low-cost storage

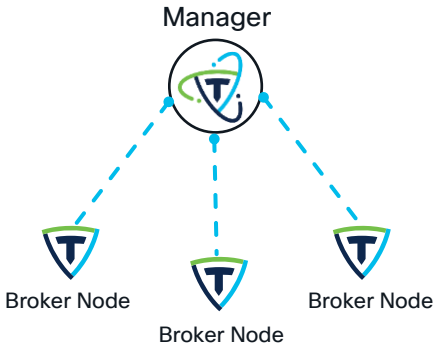
Transforming

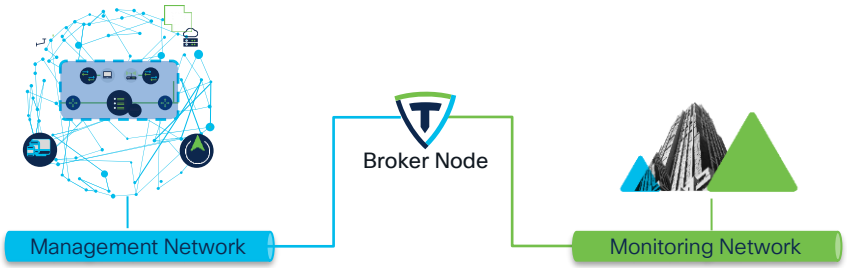
The ability to transform data protocols from the source to the destinations protocol of choice

Legacy protocol to Modern tool	>>>>>>	Increased visibility of legacy sources
Modern protocol to Legacy tool	>>>>>>	Increased visibility into modern sources

Components of the Telemetry Broker

- CTB Manager node:
  - Only one manager is deployed and can manage multiple Broker nodes*
  - Maintains the policy/rules for the broker nodes enabling central management from one view
  - If the manager goes down, broker nodes continue to process telemetry
  - Backup configurations are created for recovery
- CTB Broker node:
  - Where the telemetry brokering work occurs
  - Can be deployed closest to telemetry sources





*A single Manager supports up to 10 Broker nodes

Cisco Telemetry Broker

Minimum requirements for a Cisco Telemetry Broker Manager:

- CPU: 2 cores
- Memory: 8 GB
- Storage: 50GB

vmware vSphere

Versions 6.7 or 6.5

Minimum requirements for a Cisco Telemetry Broker Node:

- CPU: 2 cores (1 Gbps) or 5 cores (10Gbps)
- Memory: 4 GB (1 Gbps) or 8 GB (10 Gbps)
- Storage: 20GB

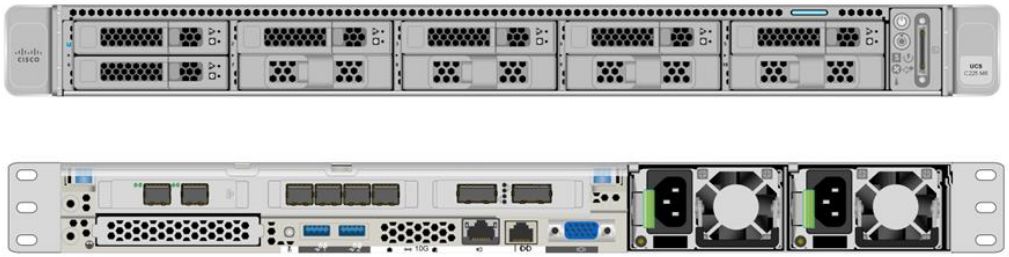
Can also be deployed on a UCS server!

https://cs.co/telemetrybroker

**See notes for more details

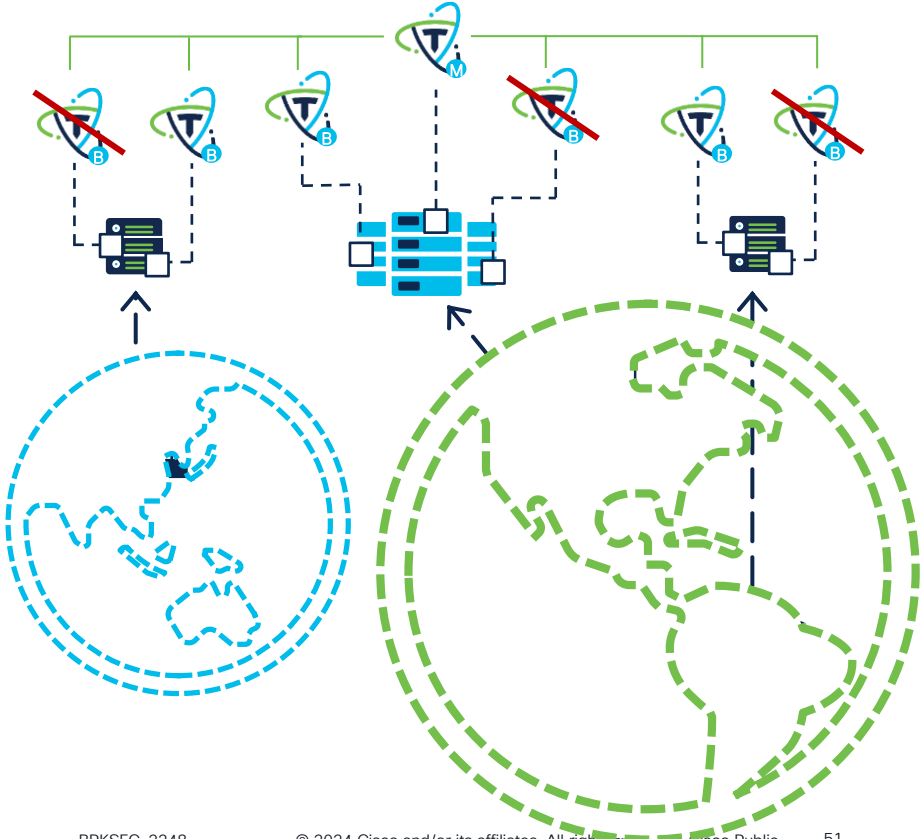
Hardware broker node

- Supports 300k FPS capable of uploading to Cisco XDR
- Dedicated 10GB Management and Monitoring interfaces
- 16 x 16 GB DDR4 3200 memory
- 6 x 600GB 10K RPM RAID6(data), 2 x 240GB Data M.2 RAID1 (OS) storage
- 2 x Processor AMD EPYC 7313 16C/32T @ 3.0Ghz or boost 3.7Ghz processor



High Availability

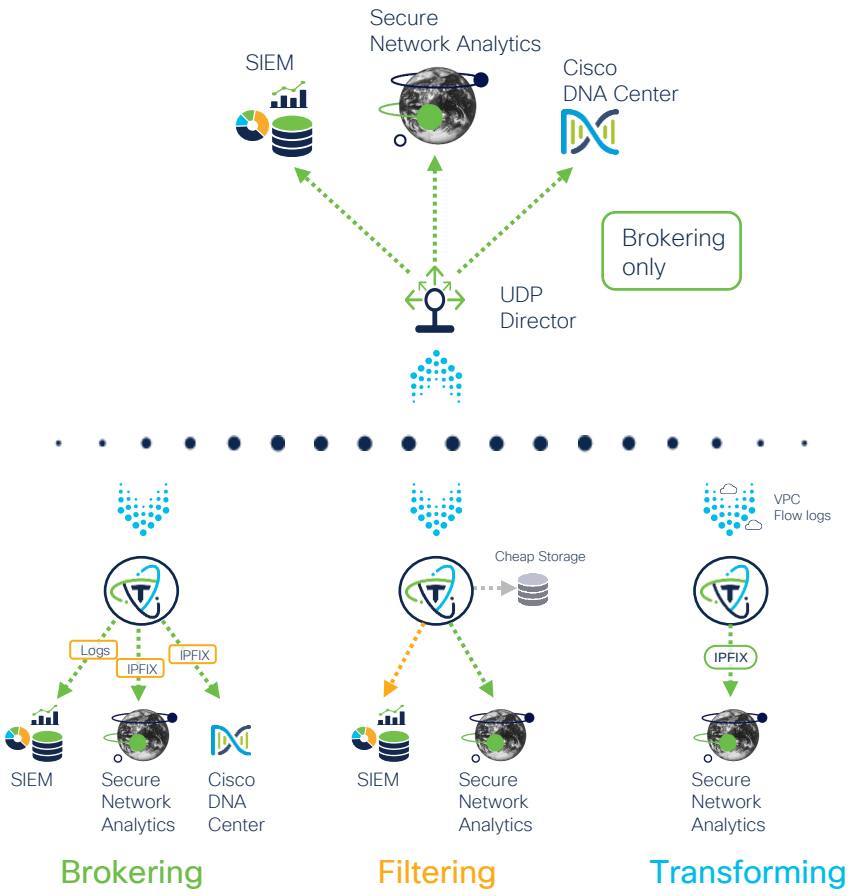
- HA Configurations are supported for Cisco Telemetry Broker
  - Simply scale more brokering nodes to provide for resiliency
  - HA Broker nodes will operate in standby mode until their associated active node goes down
  - Broker nodes can be geo-distributed with the manager centralized
- Broker nodes operating in standby mode will not process any telemetry and will not incur any additional licensing cost



Transitions

Migrating from a UDPD

- Cisco Telemetry Broker improves upon the successful feature set of the UDP Director
  - CTB improves performance, simplicity, and offers new feature functionality
- Cisco Telemetry Broker can use an existing configuration file from UDPD to seamlessly integrate existing forwarding rules
- Device architectures are different
  - Account for the addition of Brokering Nodes in an existing design
  - Account for new licensing model



Data Store Transition

No need for forklift upgrades to achieve success!

2

Hardware generations supported 4K and 5K

Re-use

Managers
Flow Collectors
Flow Sensors

Upgrade Software

to reap the benefits of a Data Store architecture

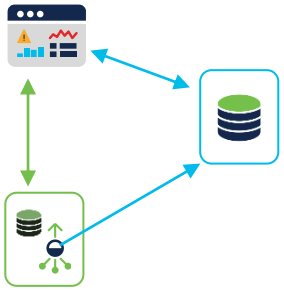
No other vendor in the market supports this model

Transitioning to Data Store

Today

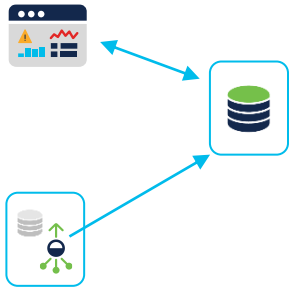
- FC 4210 DDS
- FC 5210 DDS
- FC 4200 DDS
- FC 5200 DDS

Transition State



- Data Store is added to the existing deployment
- Upgrade existing FC (engine) to send new telemetry to the Data Store
- The FC (DB) will stay in existing format
- Manager communicates with the Data Store to run reports and flow searches for recently ingested telemetry
- Manager queries FC (DB) for older reports and searches

End State



- After FC (DB) retention time has expired, DB portion is decommissioned
- SMC no longer queries FC (DB)
- For virt FC, and FC42xx/FC43xx FC (DB) resources are returned to system to optimize FC performance (up to three times faster)

Not the 5K DB Node

Transition Steps

Transition Setup

- From the Manager web UI
  - Step 1: Create a Data Store domain
  - Step 2: Setup sync between non-Data Store domain to Data Store domain
  - Step 3: Sync the domains

Initiate Transition

- From the Manager CLI (SystemConfig as root)
  - Step 4 – Add the data node(s) to Central Manager
  - Step 5 – Enable SSH on the Data Store
  - Step 6 – Initialize the Data Store
  - Step 7 – Pick the flow collector and domain for transitioning
  - Step 8 – Acknowledge the flow collector transition

Monitor Transition

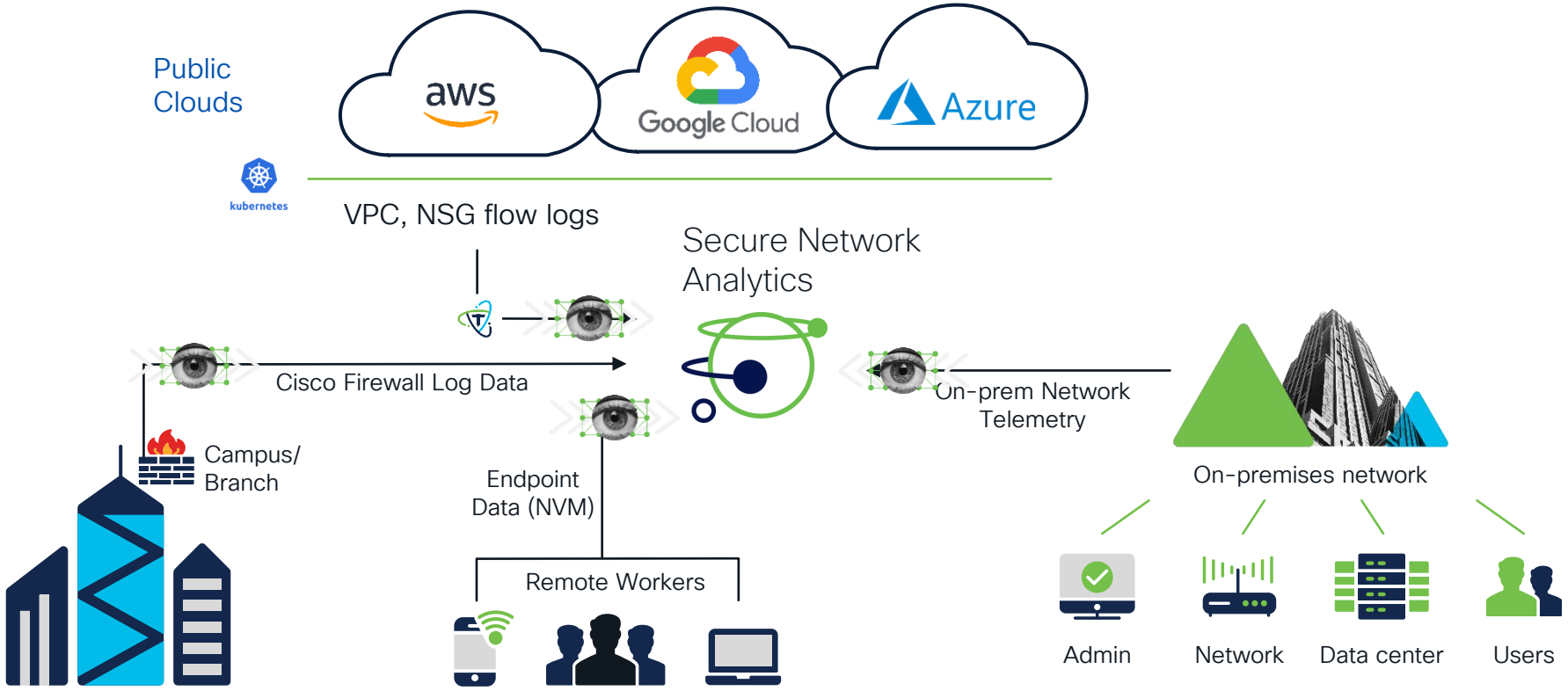
- From the Manager web UI
  - Central Manager>Inventory tab will show a transition flag (Data Store Transition) next to the flow collector
  - Central Manager>Data Store tab will show “Oldest Record (days ago)” for NetFlow, NVM and Firewall logs.
  - Once there is 30 days for each then the transition can be completed

Complete Transition

- From the Manager CLI (SystemConfig as root)
  - Step 9 – Select Data Store then Complete Transition and then the flow collector to transition
  - Step 10 – Acknowledge to complete the transition (note all old data on the flow collector will be deleted)

Telemetry Ingest and Analytics

Multi-telemetry ingest and visibility



Netflow Required Fields

The fields that SNA requires to ingest flow are:

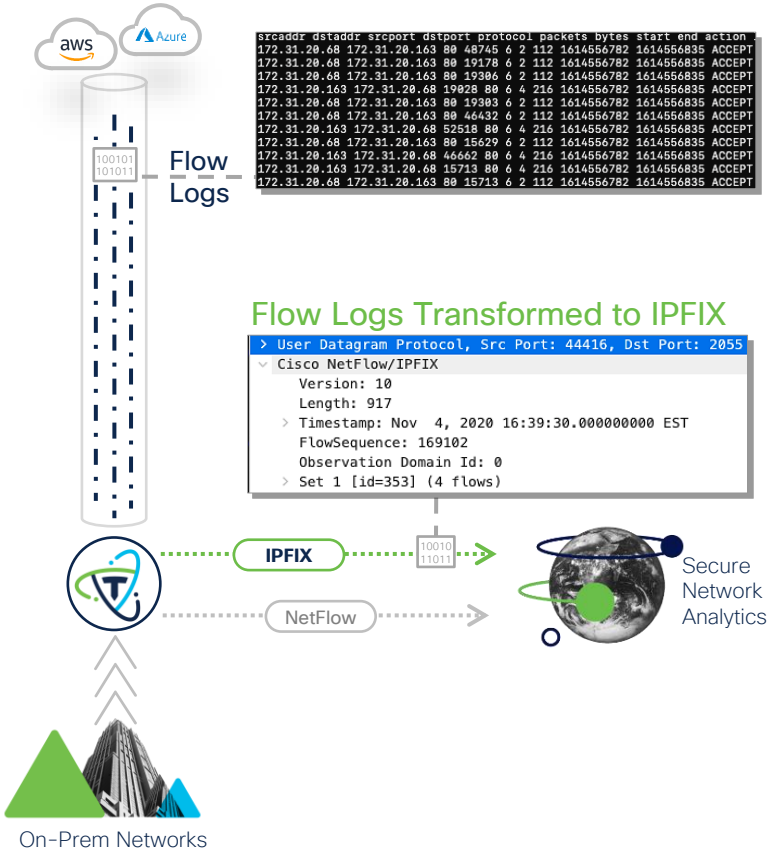
Field	NetFlow Element ID	Configuration Example	Required Field?
NF_F_PROTOCOL	4	match ipv4 protocol	**Yes, Key Field**
NF_F_SRC_ADDR_IPV4	8	match ipv4 source address	**Yes, Key Field**
NF_F_DST_ADDR_IPV4	12	match ipv4 destination address	**Yes, Key Field**
NF_F_L4_SRC_PORT	7	match transport source-port	**Yes, Key Field**
NF_F_L4_DST_PORT	11	match transport destination-port	**Yes, Key Field**
INPUT_SNMP	10	match interface input	**Yes, Key Field**
SRC_TOS	5	match ipv4 tos	**Yes, Key Field**
OUTPUT_SNMP	14	collect interface output	**Yes, Key Field**
NF_F_IN_BYTES	1	collect counter bytes	**Yes, Key Field**
NF_F_IN_PKTS	2	collect counter packets	**Yes, Key Field**
NF_F_LAST_SWITCHED	21	collect timestamp sys-uptime first	**Required; for calculating duration**
NF_F_FIRST_SWITCHED	22	collect timestamp sys-uptime last	**Required; for calculating duration**
NF_F_TCP_FLAGS			

Netflow Required Fields

ETA Fields	ETA Fields	ETA Fields	ETA Fields
	44940	ipv4 idp	This is Initial Data Packet; used for crypto audit
	44941	ipv4 splt	SPLT - Sequence of Packet Lengths and Times ; malware detection
	44944		ETA Byte Distribution; malware detection
NBAR Data	**NBAR Data**	**NBAR Data**	**NBAR Data**
	12235	match application name	NBAR application data
	45003	match application name	NBAR application data
Additional Fields	**Additional Fields**	**Additional Fields**	**Additional Fields**
initiatorOctets	231	collect connection initiator	This field is useful to determine the flow initiator
natEvent	230		Without this field we cannot get firewall events for the flow (denied, accepted, etc)

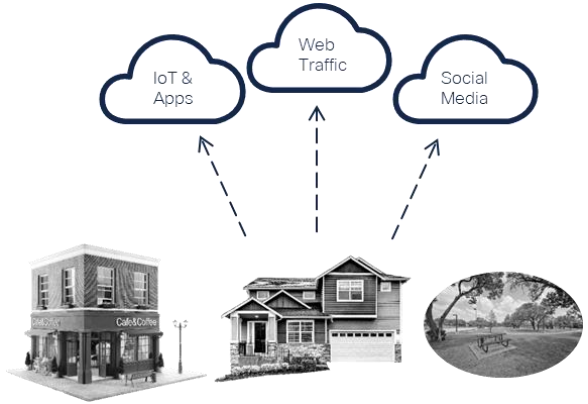
VPC Flow Logs to IPFIX

- Cloud Flow Logs from AWS and Azure provide insight into the activities of hosts residing within cloud environments
- Meta data from Flow Logs centers around the network activity, similar to IPFIX/NetFlow
  - There are 25 total fields provided in Flow Logs
  - Fields provide insight to network metadata as well as metadata associated with the VPC/NSG
- CTB pulls Flow Logs from AWS S3 buckets and Azure BLOB storage via secure HTTPS connections and transforms the telemetry to IPFIX
  - Once the VPC flow is transformed it is then forwarded to consumers



Complete and continuous remote worker visibility

The Cisco Secure Client (AnyConnect Secure Mobility Client) caches all network traffic telemetry records, even when users are not using a VPN



- On-network flows (collected when VPN connected) – real time
  - When user connects to VPN all stored NVM flow data is sent to the Flow Collector
  - Can be configured for burst or chunks and adjustable cache size
  - Detections are carried out on the NVM flows (Behavioral, Customer Security Events and Converged Analytics)
  - Note a flow search does not show NVM specific fields

- Off-network flows (collected when VPN not connected) – cached late arriving
  - Can view the historical NVM flow data using the NVM endpoint traffic reports in Report Builder
  - No detections are applied to off-network traffic

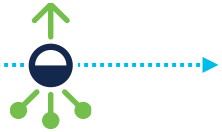
```
nvm_to_flow_cache
nvm_filter_untrusted_flows
```

No Endpoint VM Since 7.3

Recap of all NVM telemetry records retained

User Endpoints with AnyConnect Secure Mobility Client

Flow Collector



Data Store

NVM Telemetry

- Session
- Interface
- User
- OS
- Process

Session
Start Time*
End Time*
Source IP*
Source Port*
Destination IP*
Destination Port*
Bytes Sent*
Bytes Received*
Packet Count* (derived)
Protocol*

Interface
Interface Info UID
Interface Index
Interface Type
Interface Name
Interface Details List
Interface Mac Addr.

User
UDID
User
User Account Type
Agent Version
Virtual Station Name
OS Name
OS Version
OS Edition
System Manufacturer
System Type

Process
Process Account*
Process Account Type
Process ID
Process Name*
Process Hash*
Process Path
Process Args
Parent Process ID
Parent Process Account
Process Account
Parent Process Name*
Parent Process Hash*
Parent Process Path
Parent Process Args
Host Name
DNS Suffix
Module Name List
Module Hash List
Parent Process Name
Parent Process Hash

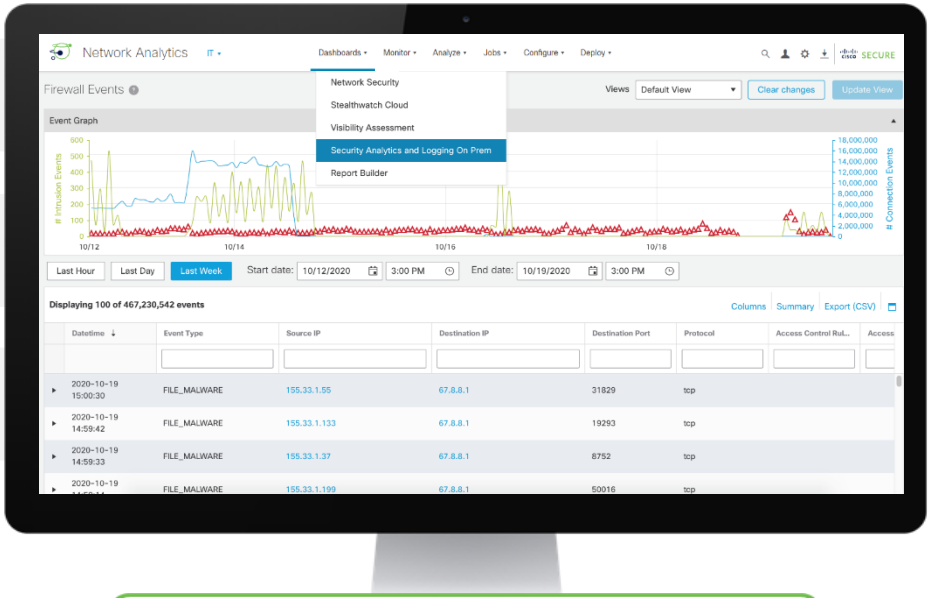
* NVM telemetry records available within non-Data Store deployments

Store Cisco Firewall logs on premise with Data Store

Cross launch from FMC with context into Secure Analytics and Logging dashboard

Make data available to FMC via APIs for supporting remote query

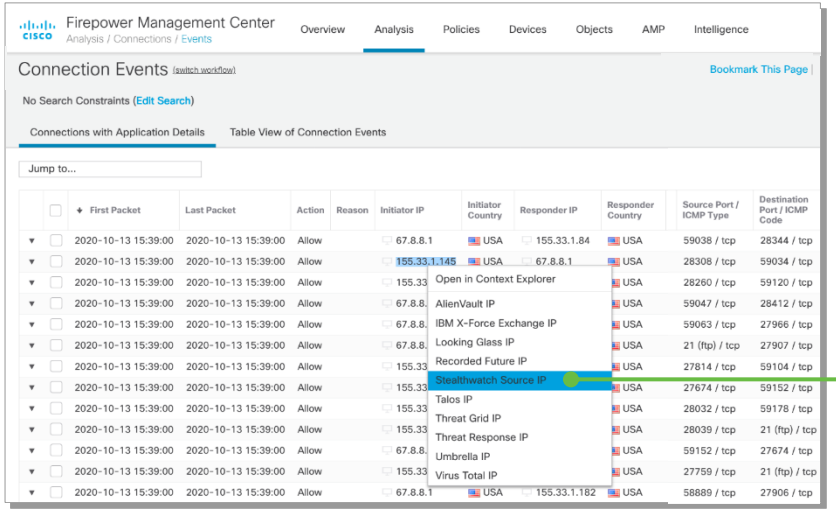
100,000k eps (8.65 Bn/ day) support for +30 days using full data store architecture

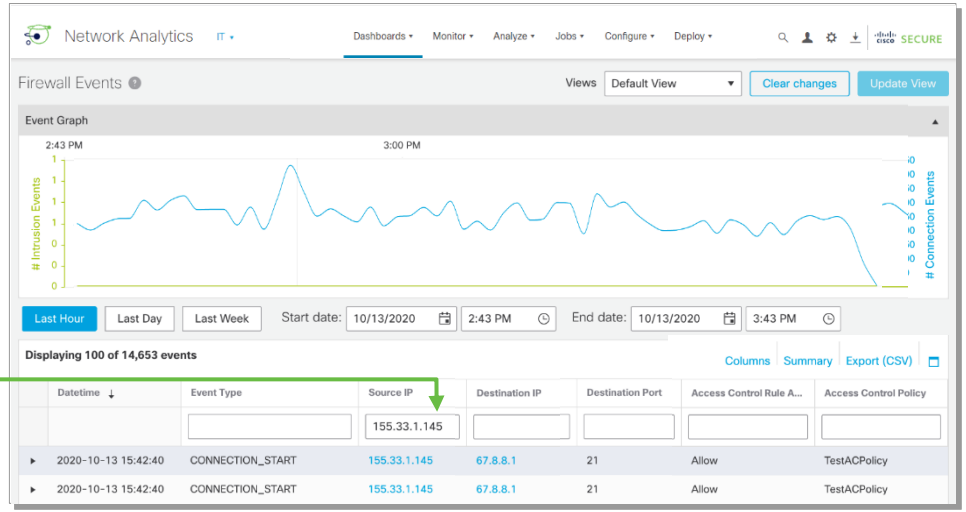


FTD, ASA & FTD-LINA Syslogs within a unified event viewer

FMC pivots directly to the Data Store with enhanced context

- Contextual pivots from Firepower Management Center to the event viewer optimizes SecOps workflows by automatically filtering on events of interest

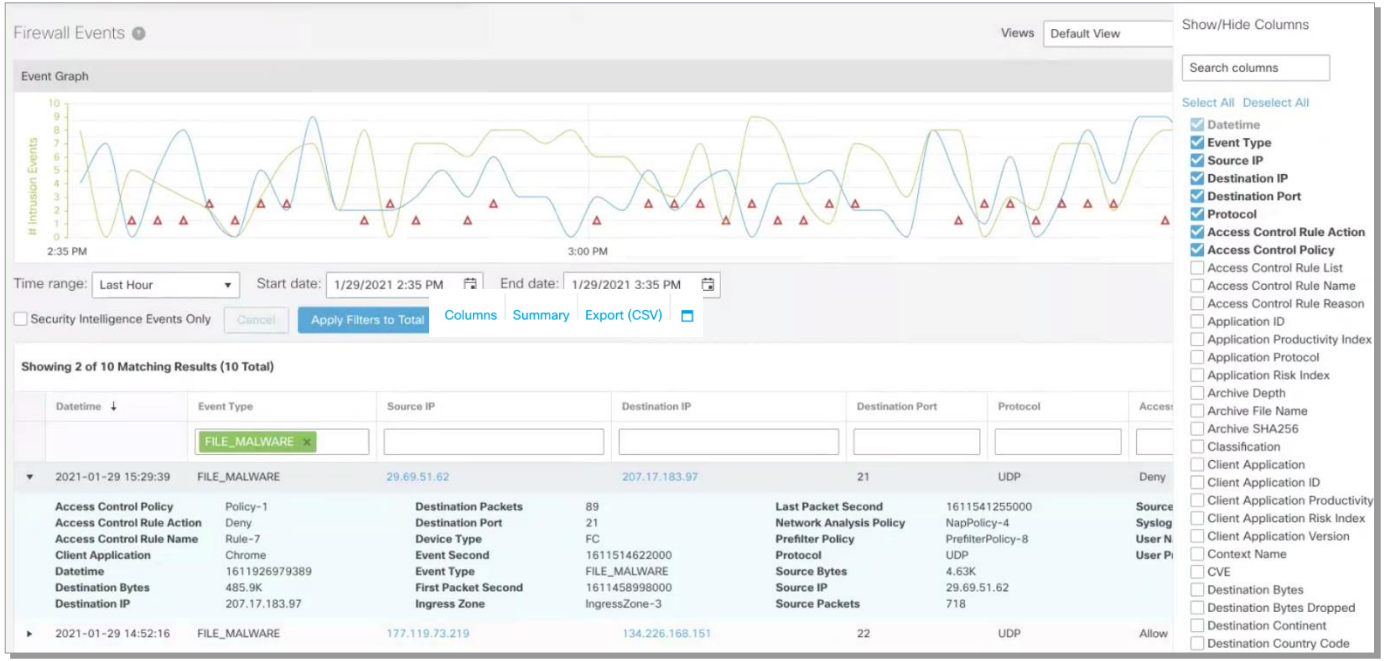




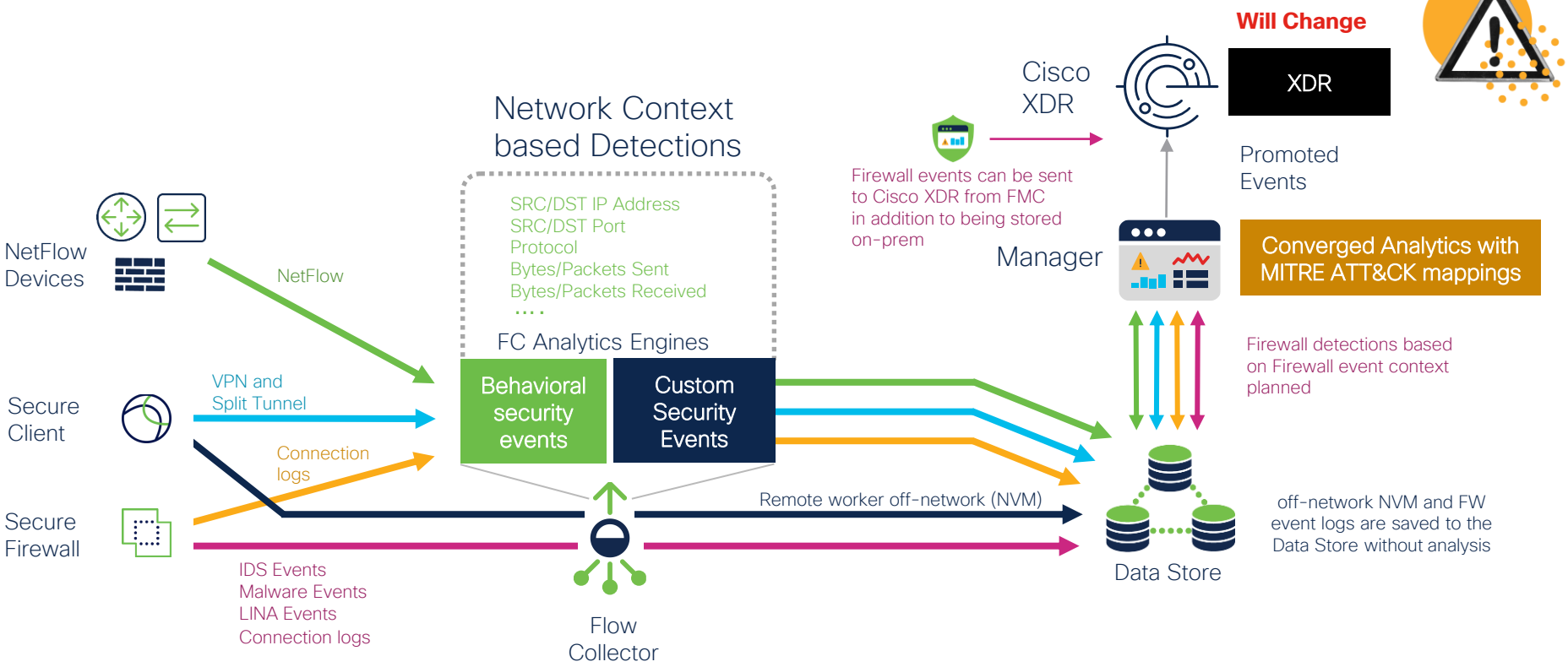
Remote Query API do not support ASA Events

Intelligent viewer provides access to all Firewall data

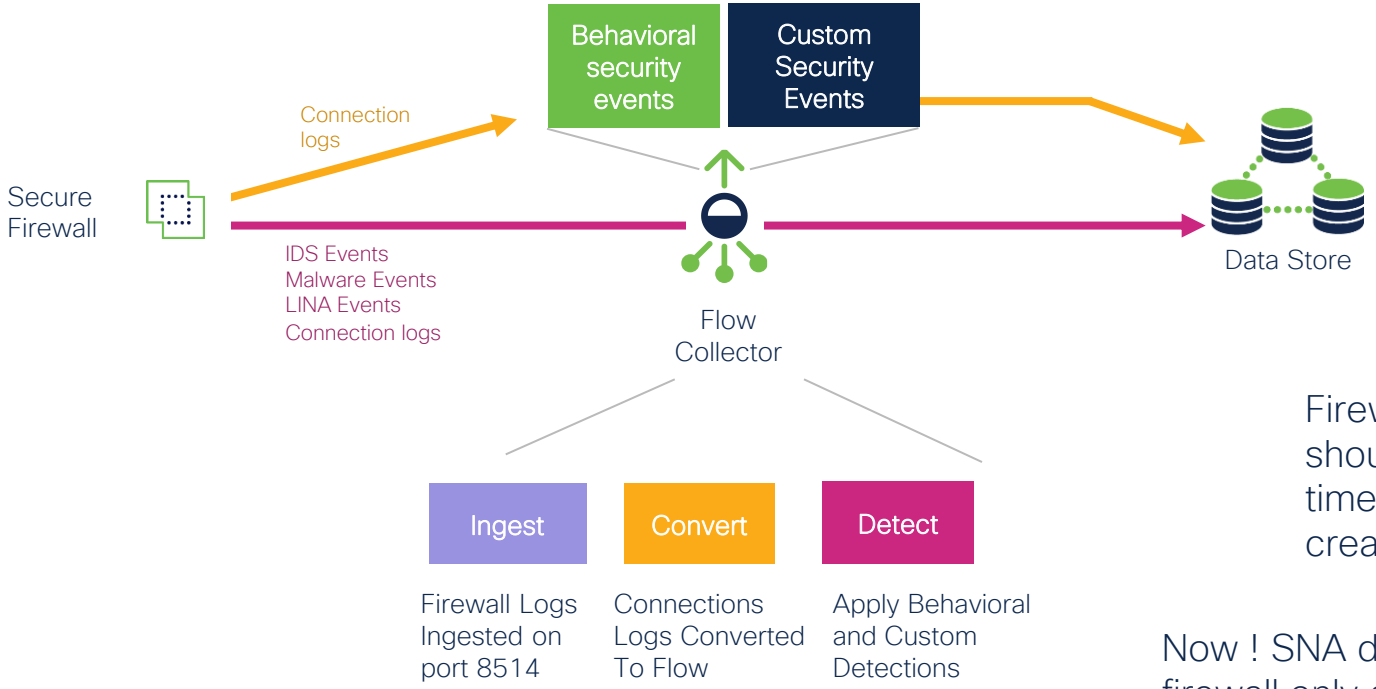
- Select custom timeframes going back across over any retention time
- Filter exclusively on Security Events and use per column filters to quickly isolate data of interest
- Create custom view to tailor content based on columns shown
- Use Summary to identify trends and outliers
- Export any view to CSV for archiving or to further forensic investigations



Secure Network Analytics detection architecture



SNA Firewall Logs Detections



Flows converged from Firewalls logs to Netflow do not count against the FPS license. SAL is licenses per GB/Day already

Firewall Logs from a device should not be sent at the same time with Netflow, that will create wrong ByteCount.

Now ! SNA detections with a firewall only as a telemetry source. (Connection End)

SNA Firewall Logs Detections

Top Security Events for 192.168.157.172

Source (1) Target (0)

Security Event	Count	Concern Index	First Active	Target Host	Target Host Group	Actions
Flow_Denied - 80	1	162	09/25 5:00:56 PM	184.84.3.78 ···	United States	···

DETAILS
--

DESCRIPTION
Flow_Denied - 80: The source host has been rejected by a firewall (such as the Cisco ASA) or other flow-blocking device.

Flow Denied Security Event in SNA triggered on traffic from Firewall Logs

Leverage Analytics to trigger Behavioral Alerts

Customized Alerts with Custom Security Events

Security Events | 192.168.118.54 (1)

All Security Events For 192.168.118.54

Security Event	Count	Concern Index	First Active	Source Host	Source Host Group	Target Host	Target Host Group	Actions
CSE: Alert on Firewall Flow Denied - 443	1	0	09/26 12:54:06 PM	192.168.118.54 ···	Catch All	96.43.146.48 ···	United States	···

DETAILS
--

DESCRIPTION
CSE: Alert on Firewall Flow Denied - 443: When any host within Inside Hosts is denied from talking to any host within Outside Hosts, an alarm is raised.

SNA Firewall logs to Detections Configurations

Configuration

- sal_enable = 1
- sal_to_flow_cache = 0 (default) Put it to 1 to enable conversion
- sal_port = 8514 (default) Ports should not be overlapped with other ports 2055 for Netflow and 2030 for NVM

Troubleshooting

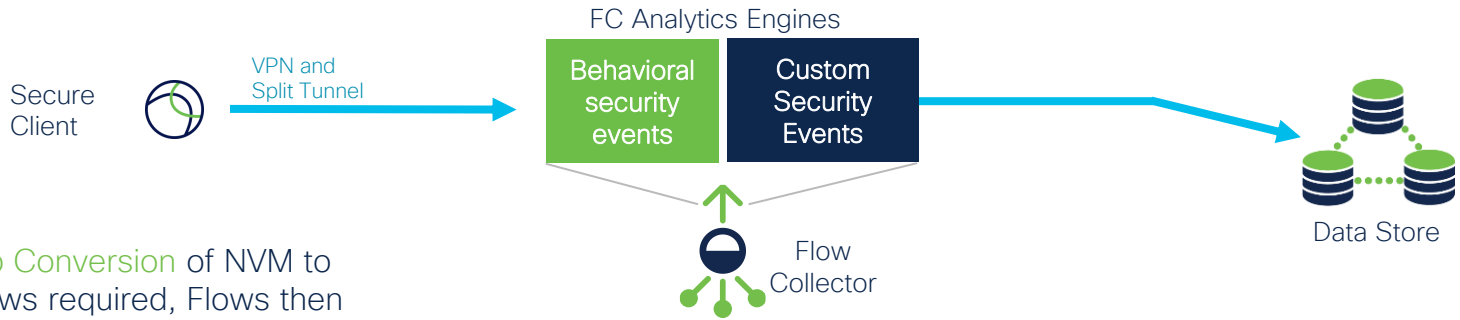
- /lancope/var/sw/today/logs/sw.log

```
05:00:02 S-per-t:        Current sal_event, Input: 0, Decoded: 0, Output: 0, Ignored: 0
05:05:00 S-per-t:        Current sal_event, Input: 3325, Decoded: 3325, Output: 3325,
Ignored: 0, Dropped: 0, To_Flow: 1578 this period
Dropped: 0, To_Flow: 0 this period
05:10:00 S-per-t:        Current sal_event, Input: 4411, Decoded: 4411, Output: 4411,
```

No Pivots are available to FMC

Not Available for DDS

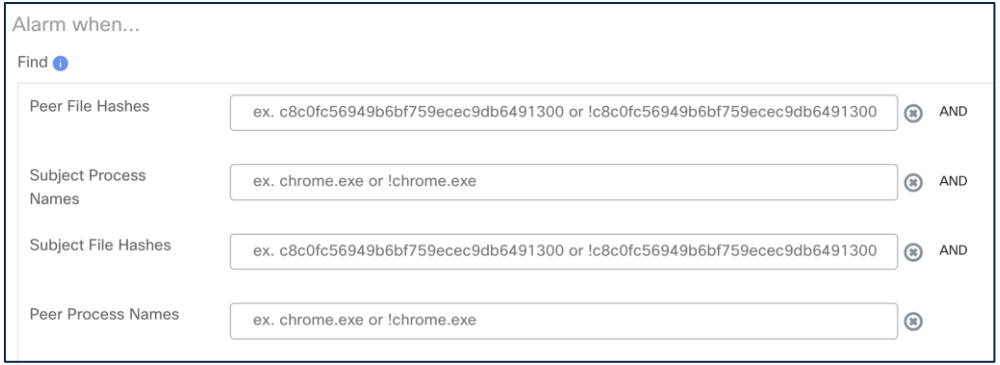
NVM Detections



No Conversion of NVM to flows required, Flows then goes through the detection engine

All Detection from behavioral analytics can be applied including data movement.

One More way to Deploy SNA without having to be restricted to network flow to get detections



Alert on Process Names and Hashes with CSEs in addition to all other data

NVM Detections Configurations

New Install

nvm_enable = 1
nvm_to_flow_cache = 0 (default)
nvm_port = 2030 (default)

NVM flows can be seen in flow search and Report Builder when *nvm_to_flow_cache* is enabled
NVM flows can be seen in only Report Builder when *nvm_to_flow_cache* is not enabled

Troubleshooting

/lancope/var/sw/today/logs/sw.log
/lancope/var/logs/containers/svc-db-ingest.log

New Detections and Alerts in Converged Analytics

4 New Alerts from Secure Cloud Analytics

- LDAP Connection Spike
- Outbound LDAP Spike
- Protocol Forgery
- Repeated Umbrella Sinkhole Communications

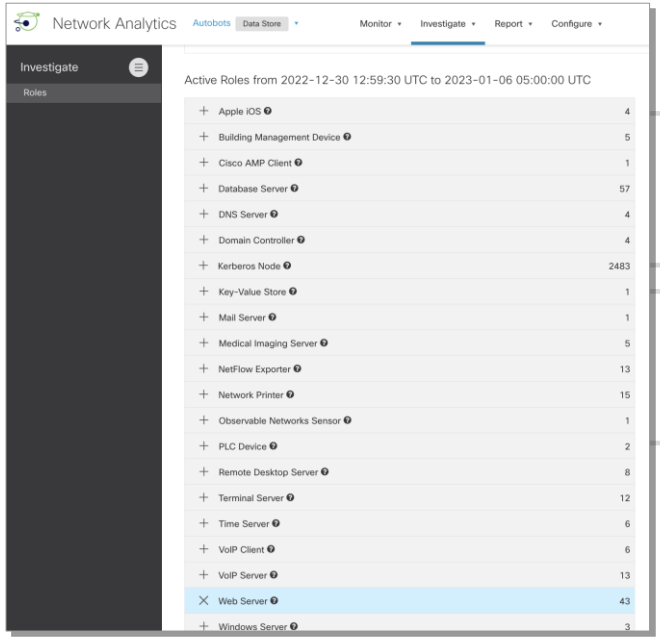
2 New Observations from Secure Cloud Analytics

- ISE Session Started Observation
- Umbrella Sinkhole Hit Observation

Alert Type	MITRE ATT&CK Tacti...	MITRE ATT&CK Te...
Outbound LDAP Connection Spike Device is communicating with a large number of external hosts using an LDAP port. This alert uses the IP Scanner observation and may indicate a possible infected host or an internally-initiated port scan.	Reconnaissance	Active Scanning
Outbound SMB Connection Spike Device is communicating with a large number of external hosts using SMB ports. This alert uses the IP Scanner observation and may indicate a possible infected host or an internally-initiated port scan.	Reconnaissance	Active Scanning
Potential Data Exfiltration Device downloaded data from an internal device that it doesn't communicate with regularly. Shortly after that, the device uploaded a similar amount of data to an external device. This alert uses the Potential Data Forwarding observation and may indicate that sensitive data is compromised.	Exfiltration	Automated Exfiltration
Protocol Forgery Device was observed running a potentially restricted service (such as SSH) on a non-standard port. This alert uses the Bad Protocol Observation and may indicate an evasion of security controls.	Command And Control	Non-Standard Port

Converged Analytics supports redundant Managers

Dynamically maps entities by role



Type based modeling

Functional modeling

Roles include:

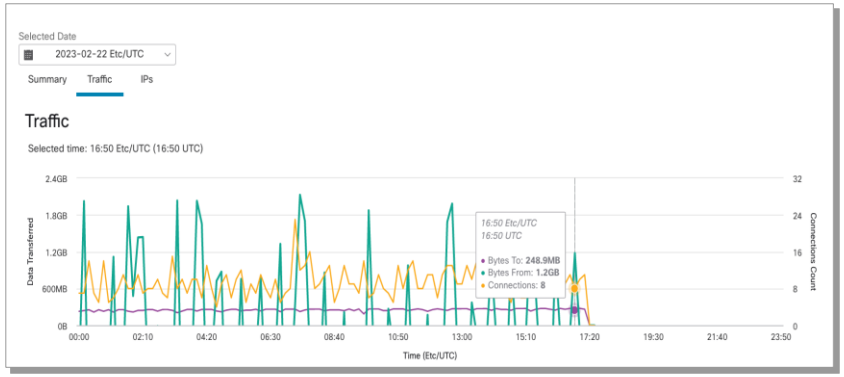
- Android
- Web server
- VoIP client
- Mail server
- Medical imaging client
- Citrix PVS server
- Apple iOS
- Remote desktop server
- DNS server
- Windows workstation
- Wireless LAN controller
- Domain controller

...over **50+** entity roles are supported !

- Automatic role classification available on a new report leveraging the new converged analytics capability
- Roles are available out of the box with no tuning and provide details about devices on the network for investigation and input to detection

Device Report Traffic enhanced with automatic filters

- Select any time on the traffic statistics graph and see results dynamically filtered in the flow table
- Accelerates investigation of traffic anomalies
- Immediately correlates chart events with actual flows attributing to the event



All | Internal | External

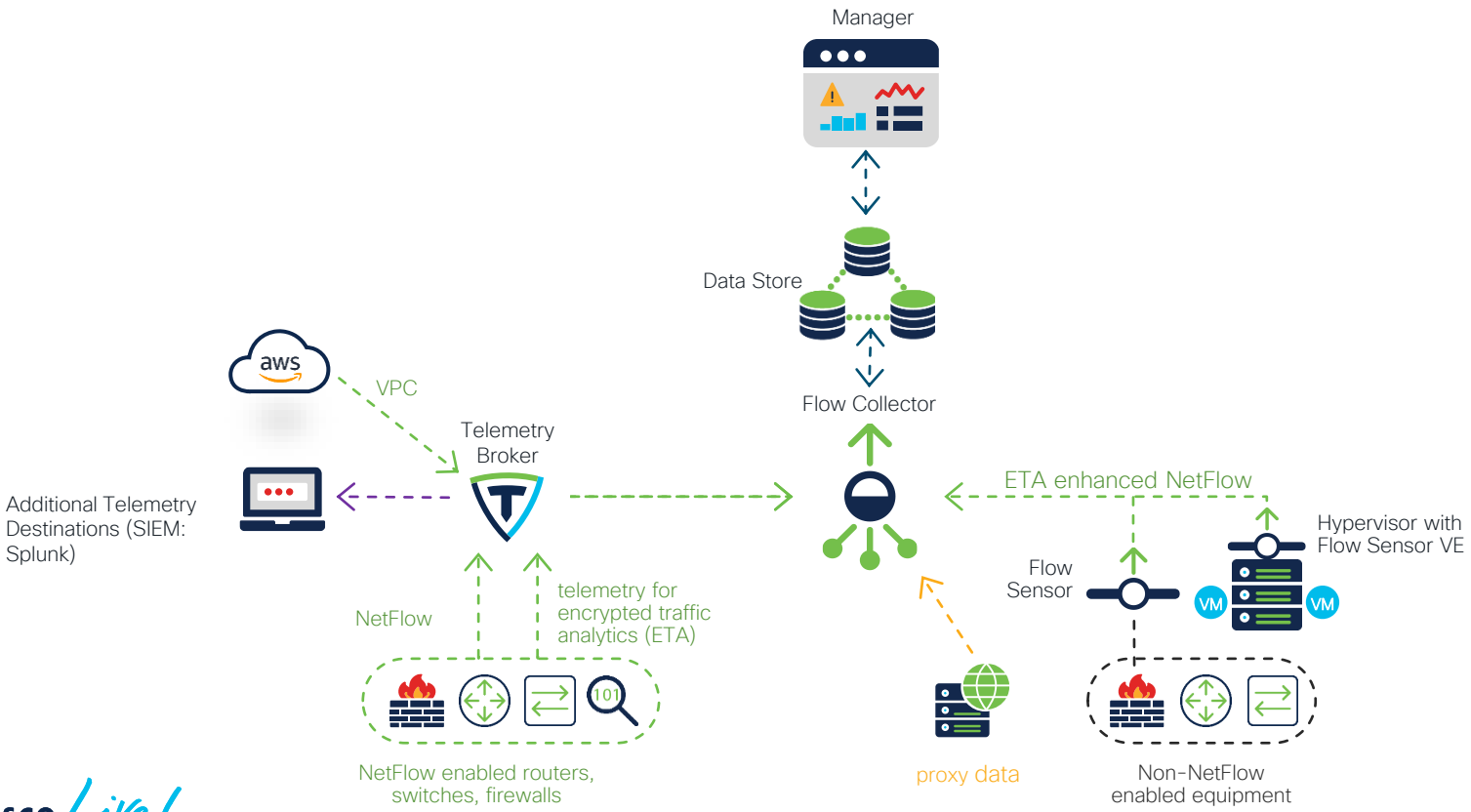
CSV

Connected IP	Hostname/PDNS Record	By...	Bytes...	Bytes ...	First Connection	Last Connection	
20.42.73.154	--	19.5KB	4.1KB	23.6KB	2023-02-22 16:50:00 UTC	2023-02-22 16:50:00 UTC	•••
192.111.4.108	--	17.3KB	10.1KB	27.4KB	2023-02-22 16:50:00 UTC	2023-02-22 16:50:00 UTC	•••
35.232.111.17	--	296B	174B	470B	2023-02-22 16:50:00 UTC	2023-02-22 16:50:00 UTC	•••
192.111.4.116	--	15.2KB	3.2KB	18.4KB	2023-02-22 16:50:00 UTC	2023-02-22 16:50:00 UTC	•••
185.125.190.49	--	294B	174B	468B	2023-02-22 16:50:00 UTC	2023-02-22 16:50:00 UTC	•••

Demo NVM + Firewall Logs + Converged Analytics

Design- Where to get Telemetry

Where To Enabled Telemetry ?



The more you enabled the more you see

Edge Devices at Campus Edge Devices at Branches	Visibility into traffic going through these devices to the internet or to the main data center. Firewalls could provide NAT information
Core Switches	Visibility into traffic going through the core to the Internet or to the DC and Campuses
Access and Distribution	More visibility into user traffic from one VLAN to another or even from port to port

Add A Flow Sensor

At the EDGE

Get Application layer visibility into your internet traffic (URL and APPs)

At the Hypervisor

Visibility into VM traffic and additional network use cases with RTT and SRT

Non Flow Capable Networks

Legacy Networks visibility where flow is not available

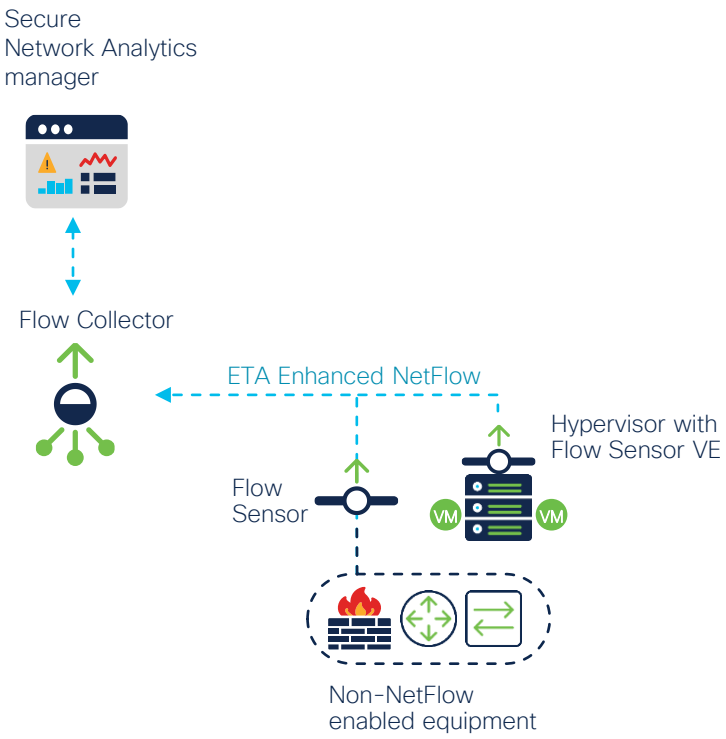
What Can A flow Sensor Do

Virtual or physical appliance that produces telemetry for network infrastructure incapable of generate NetFlow natively

Provides additional security context to enhance Secure Network Analytics security analytics

Additional information gathered

- ETA enhanced NetFlow
- TLS Finger Printing
- Layer 7 application data
- URL information for web traffic
- TCP and ICMP flag details
- RTT (Round trip time)
- SRT (Server response time)
- Retransmissions
- X-Forwarded headers from web load balancers



Visbility at the Endpoint Level

User Endpoints with AnyConnect Secure Mobility Client

Flow Collector

Data Store

NVM Telemetry

- Session
- Interface
- User
- OS
- Process

Start Time*
End Time*
Source IP*
Source Port*
Destination IP*
Destination Port*
Bytes Sent*
Bytes Received*
Packet Count* (derived)
Protocol*

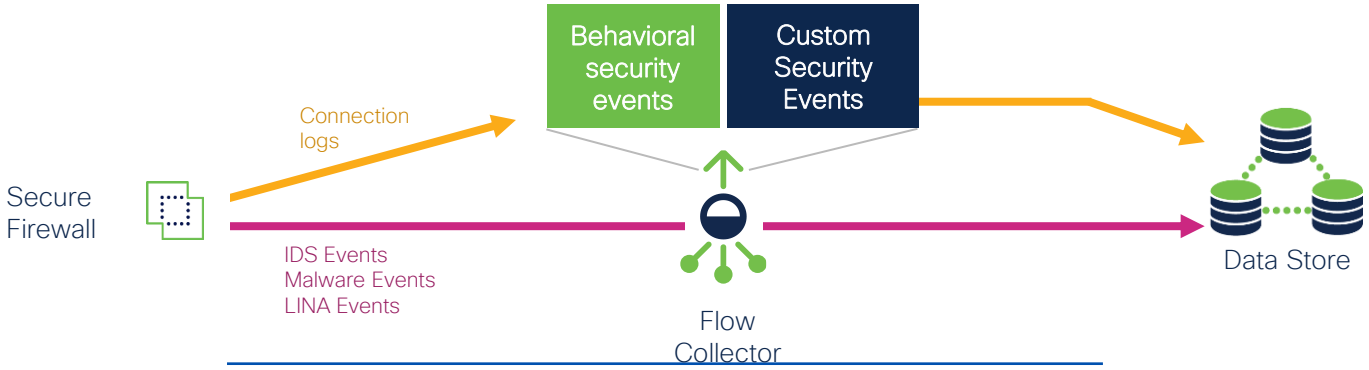
Interface Info UID
Interface Index
Interface Type
Interface Name
Interface Details List
Interface Mac Addr.

UDID
User
User Account Type
Agent Version
Virtual Station Name
OS Name
OS Version
OS Edition
System Manufacturer
System Type

Process Account*
Process Account Type
Process ID
Process Name*
Process Hash*
Process Path
Process Args
Parent Process ID
Parent Process Account
Process Account
Parent Process Name*
Parent Process Hash*
Parent Process Path
Parent Process Args
Host Name
DNS Suffix
Module Name List
Module Hash List
Parent Process Name
Parent Process Hash

* NVM telemetry records available within non-Data Store deployments

Store and Analyse Firewall Logs



Min Supported Version	Notes
FMC 6.7	Older versions are supported but Cross-launch will not be available
FTD 6.4	
SMC 7.3.0	SMC VE or SMC 2210
SAL On Prem 1.0.0	An application needs to be installed separately from the SMC 7.3.0 install

Analyze your Cloud Data by adding CTB

aws

VPC Flow Logs

srcaddr
dstaddr
srcport
dstport
protocol
packets
bytes
start
End
tcp-flags

Cisco Telemetry Broker
Transformation

IPFIX

sourceIPv4Address or sourceIPv6Address
destinationIPv4Address or destinationIPv6Address
sourceTransportPort
destinationTransportPort
protocolIdentifier
packetDeltaCount
octetDeltaCount
flowStartSeconds
flowEndSeconds
tcpControlBits

Secure
Network Analytics

Summarize The Telemetry Design Use Cases

Visibility into traffic going through the Network east West extend it by enabled at other layers

Analyze and Store your firewall logs and NAT information

Get to the endpoint process user and interface level

Get visibility into your cloud environment by leveraging CTB

Design - Most Common Integrations

Secure Network Analytics integrations

Proxy
Web APP, web URL and user info

DNA Center
Automated setup and deployment

Secure Client
Process and endpoint visibility

Identity Services Engine
User identity, device identity, mitigation and response

Secure
Network Analytics

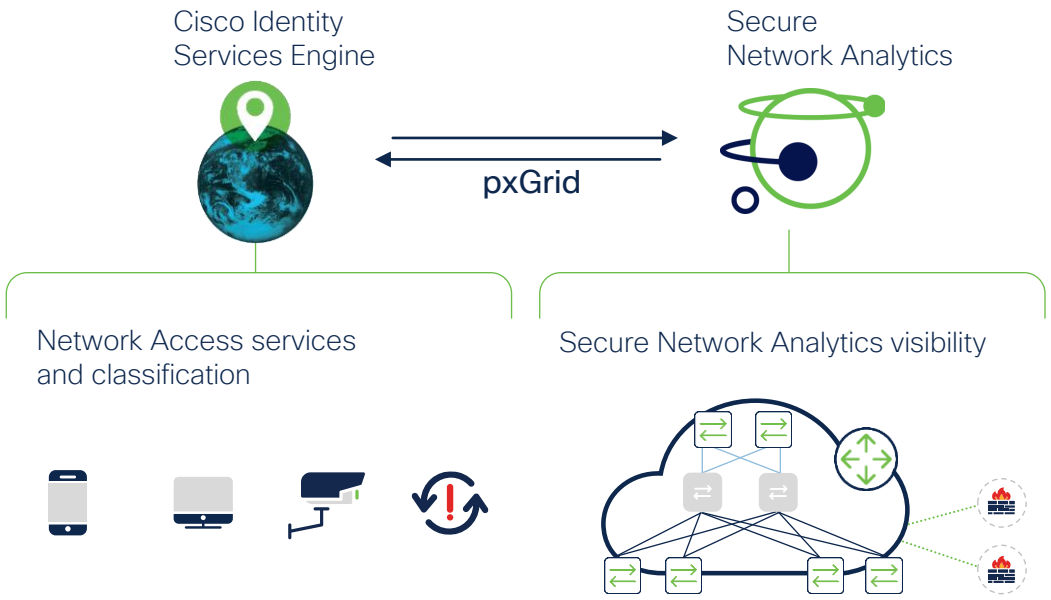
External lookup
Extended analytics, threat investigation

XDR
Threat hunting and response

PAN
Application and user identity

API
Automated and customized configuration and reporting

Secure Network Analytics and network access integration



Secure Network Analytics integrates with ISE to get mitigation capabilities and apply different ANC policies to an endpoint

Device Id	Trustsec name
Domain Id	Last update time
Active	InterfaceDevicePortId
Start active time	InterfaceDeviceIp
Endpoint IP	Vlan
Username	MAC address
SGT Tag	Session ID

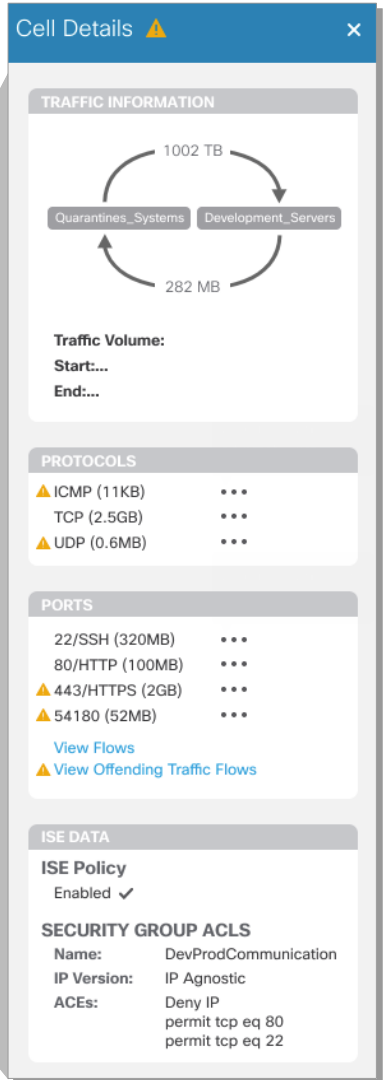
Info from ISE

Secure Network Analytics also integrates with ISE-PIC using pxGrid to get endpoint contextual information

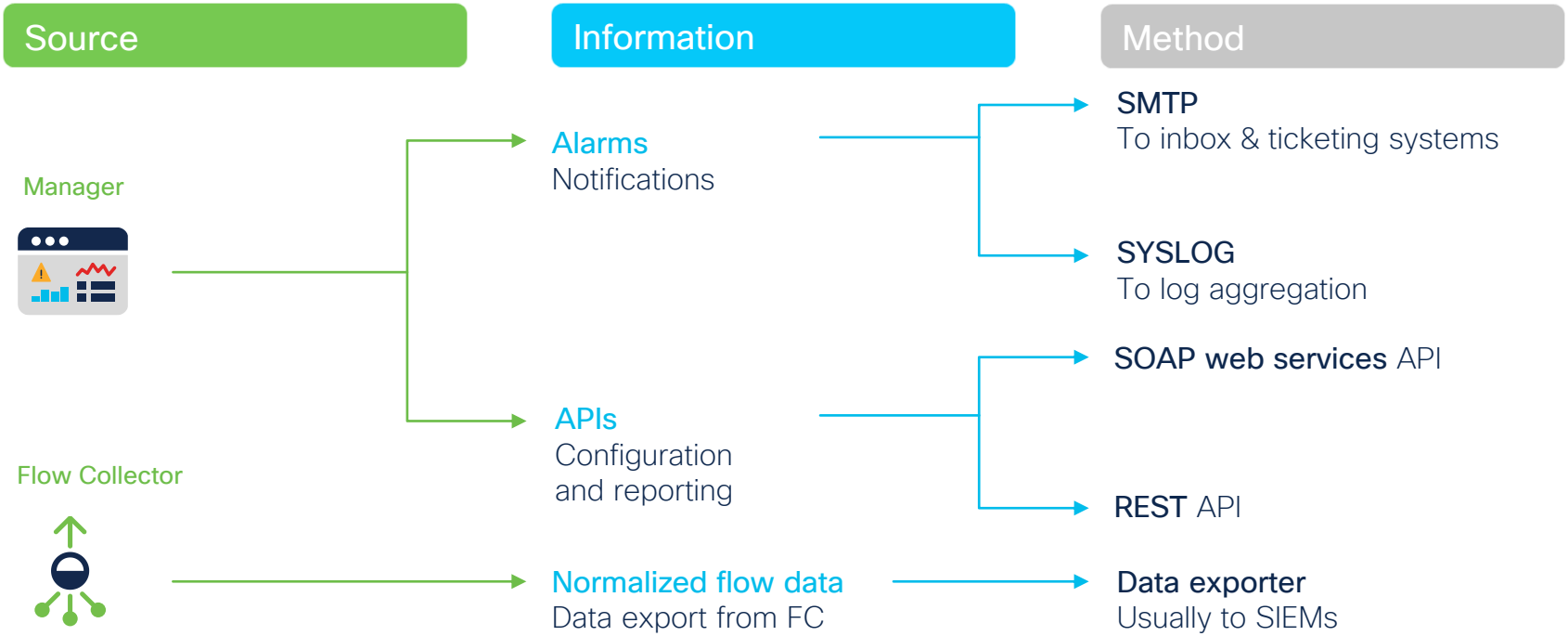
Active	Username
Start active time	Last update time

Info from ISE – PIC

Validate trusted ISE policy is being observed from near real time network telemetry



Secure Network Analytics is a comprehensive data source



Improving on-prem NDR with Cisco XDR

Cross correlation of data

Correlation of NDR findings with other detections mechanisms including EDR based detections, email and others

Impact Analysis

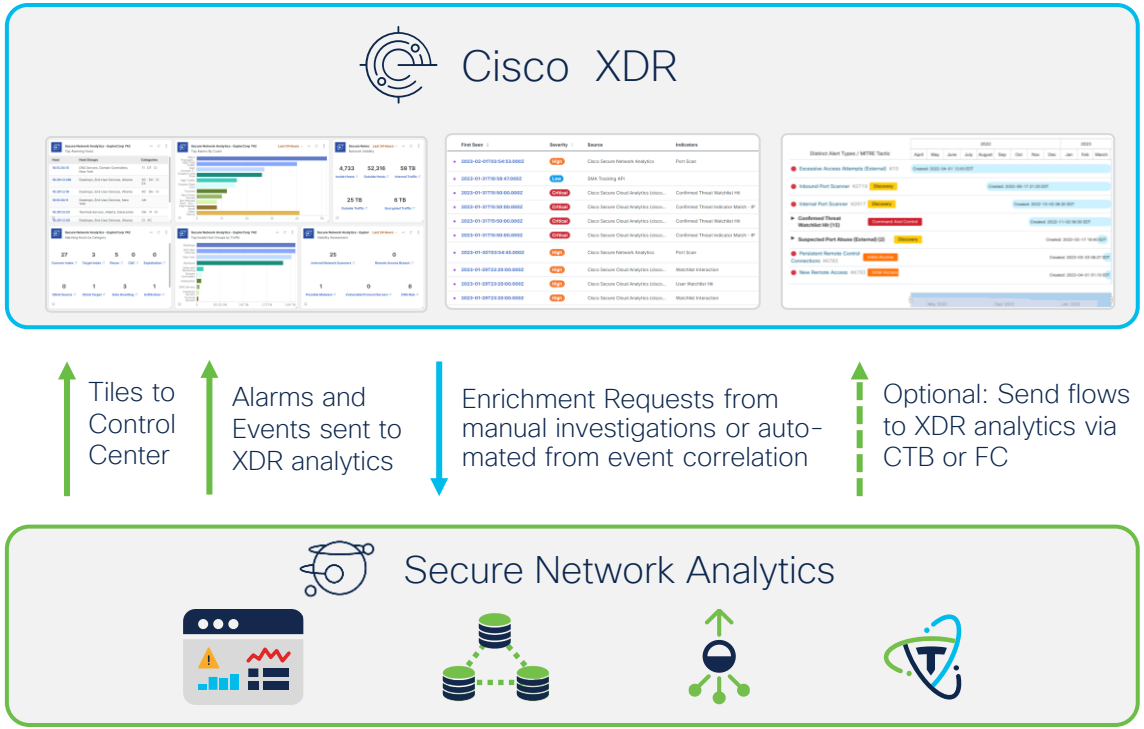
Understand the Impact of an incident leveraging XDR incident Manager

Reduce the time to respond

Reducing the time to response leveraging XDR automation and the multi responses capabilities

Extend response capability

Expand NDR response capabilities with multiple technologies through XDR integrations with Cisco and 3rd party technologies



Data Enrichment From SNA to XDR

SecureX Integration Options

- [x] Enable SecureX Security Ribbon and Pivot Menu
- [x] Enable SecureX Dashboard Tiles Service requests
- [x] Enable SecureX Threat Response enrichment requests

Number of TOP Security Events: 100

Period of time (days): 30

Security Events Investigation Configuration Limits

ork Analytics | Severity

Severity	Source	Indicators	Observables
High	Cisco Secure Network Anal...	Suspect Quiet Long Flow	52.32.82.144
High	Cisco Secure Network Anal...	ICMP_Port_Unreach**	
High	Cisco Secure Network Anal...	Addr_Scan/tcp	146.112.63.0
High	Cisco Secure Network Anal...	ICMP_Port_Unreach**	
High	Cisco Secure Network Anal...	Suspect Quiet Long Flow	52.11.170.250
High	Cisco Secure Network Anal...	ICMP_Port_Unreach**	
2023-09-24T18:18:54.00 High	Cisco Secure Network Anal...	Suspect Quiet Long Flow	52.11.170.250
2023-09-24T15:15:00.00 High	Cisco Secure Network Anal...	High Total Traffic	108.62.141.152
2023-09-24T15:15:00.00 High	Cisco Secure Network Anal...	Suspect Data Loss	

Security Events Contribute into XDR investigations

Short description

The source IP has attempted to connect to an excessive number of ports on the target IP.

Long description

Title
The source IP has attempted to connect to an excessive number of ports on the target IP.

Observed Time
2023-09-24T14:33:39Z

Observed By
breach-smc742

Source
192.168.246.115

Target
192.168.249.116

Relations 1

obsidian-WIN10 Connected to flint-WIN10

Indicators 1

Cisco Secure Network Analytics
Port Scan

Events details are sent with relationship indicators for some alerts when available

SNA Alerts to XDR

It came in 7.5 Will Change 7.5.1

456	Heartbeat Connection Count on 10.70.28.171	Cisco Secure ...	1 Month	Unassigned	New
456	Heartbeat Connection Count on 10.70.15.24				New
1000	Remote Access (Geographic) on 10.19.1.22	Cisco Secure ...	1 Month		

Source
Cisco Secure Network Analytics (smc-750-577338-2.lancope.ciscolabs.com)

MITRE | ATT&CK View Details

TA0043: Reconnaissance
TA0042: Resource Development
TA0001: Initial Access
TA0002: Execution
TA0003: Persistence
TA0004: Privilege Escalation
TA0005: Defense Evasion
TA0006: Credential Access
TA0007: Discovery
TA0008: Lateral Movement
TA0009: Collection
TA0011: Command and Control
TA0010: Exfiltration
TA0040: Impact

Remote Access (Geographic) on 10.19.1.22

Priority 1000 Status New

Reported by Cisco Secure Network Analytics (smc-750-577338-2.lancope.ciscolabs.com) 1 month ago

Assigned Unassigned

MITRE

Priority score breakdown

1000 | 100 Detection Risk | 10 Asset Value at Risk

Short description

Device has been accessed from a remote host in a user-supplied watchlisted country. This alert uses the Remote Access observation and may indicate a device is compromised.

Long description

Assets 5

Endpoint

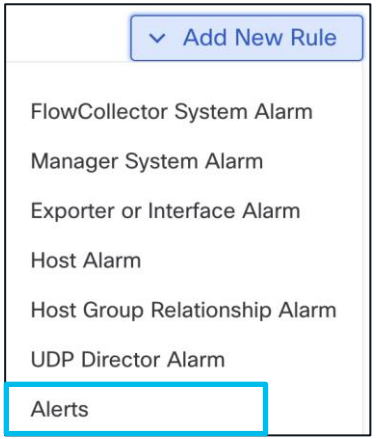
ip-10-19-1-23.us-east-2.compute.i... 27 events

SNA Converged Analytics Alerts Published to XDR Through Response Management

Alerts can trigger incidents and are Mapped with MITRE attack tactics and technique.

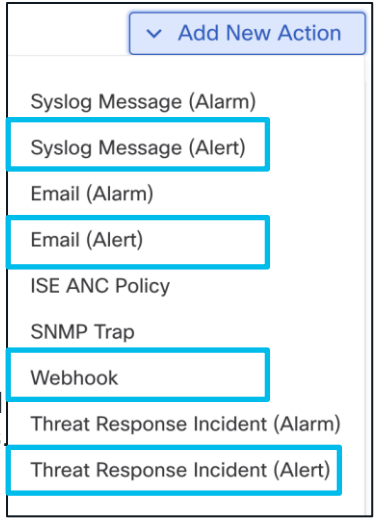
Integration for Response Management

Response Manager Logic



New Alerts option in Response Manger. Converged Analytics needs to be enabled.

New Actions for Converged Analytics Alerts.



Webhooks supported for Alerts (Converged Analytics) and Alarms. Not customizable for either.

Automatic Response

Automate responses by defining rules and applying actions

If **Condition** is met, then trigger **Response**

Rule

What alarms?

Action

What to do with alarms?

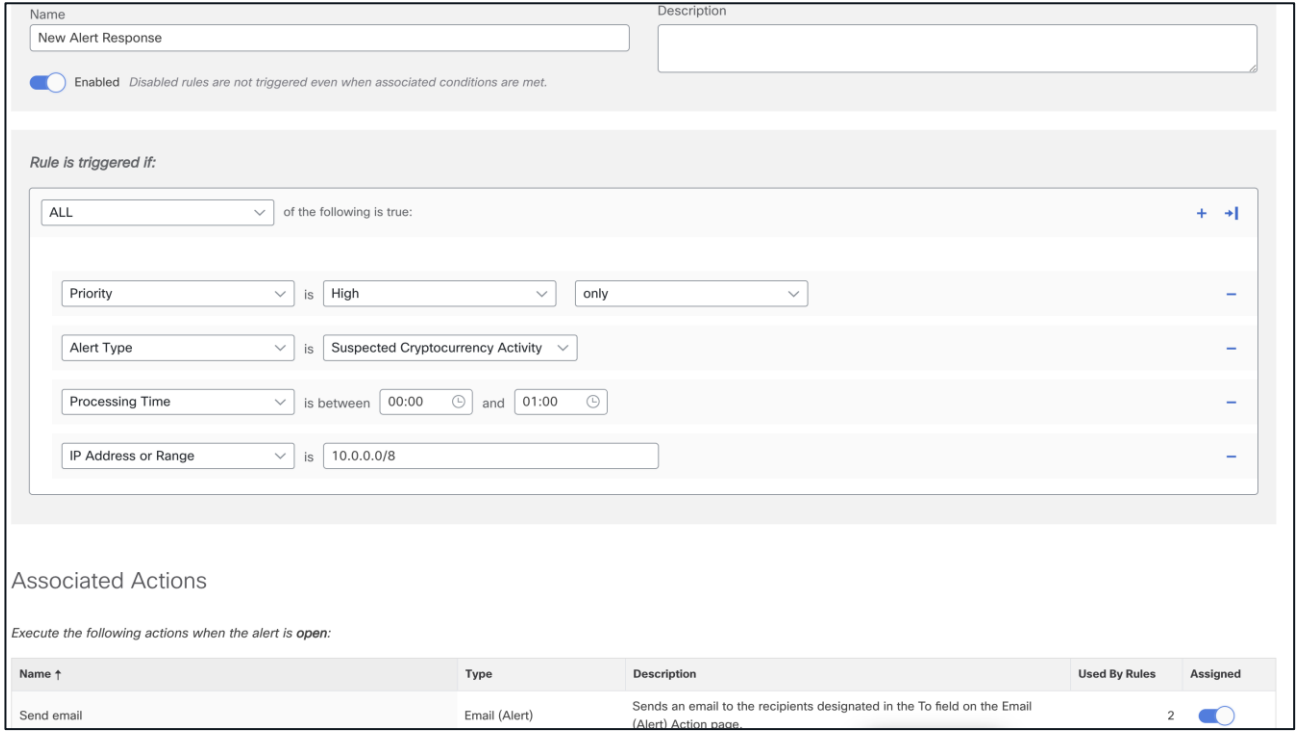
Rules With Flexible Conditions

Define Rules with Multiple Conditions

- Granular control with complex rule triggering conditions

Use Multiple Actions:

- Select 1 or more actions to be executed once rule is matched and alert is open
- Select 1 or more actions to trigger when the alert is closed



Demo XDR and Response Management

SNA Resources

Most Utilized Resources

Secure Analytics Videos
http://cs.co/SecureAnalyticsVideos

Detection:
Secure Analytics Detections Demo playlist

Design Guide:
SNA Data Store Design Guide

FPS Estimator:
FPS Estimator

Training Center:
Secure Network Analytics Training Center - Use Cases

The bridge to possible

Thank you

cisco Live!

cisco Live!

Let's go