

CISCO *Live!*

Let's go

#CiscoLive



The bridge to possible

A Bird's-eye View of the Secure Firewall Health

Arati Avhad, Director of Engineering
Gayathri Nagarajan, Engineering Product Manager

BRKSEC-2094

CISCO *Live!*

#CiscoLive

Your speakers throughout this Secure Firewall journey



Arati Avhad
Director of Engineering,
Cloud and Network Security
NGFW - Snort, EVE, ZTNA, Observability
aavhad@cisco.com

Passion - Women's Soccer
Creating a level playing field



Your speakers throughout this Secure Firewall journey



Gayathri Nagarajan

Engineering Product Manager

Network Security Management Portfolio
gayathna@cisco.com



Also, a classical dancer & home farmer



Cisco Webex App

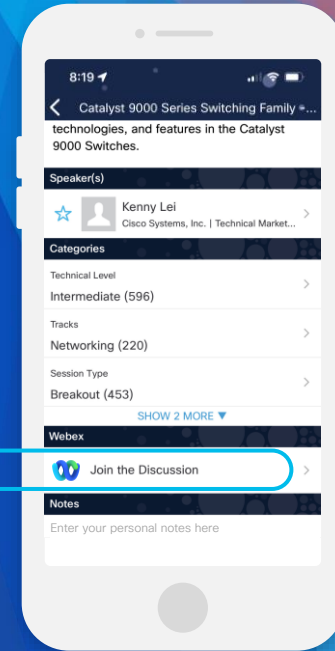
Questions?

Use Cisco Webex App to chat with the speaker after the session

How

- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until June 9, 2023.



<https://cislive.ciscoevents.com/cislivebot/#BRKSEC-2094>

Join at
slido.com
#3885 729

 Passcode: **clus2023**



What is in it for YOU?



Modernize your day-to-day job with Health Monitoring system



Proactively tackle critical incidents in your network



Customize health monitoring by correlating existing health metrics



Consume health metrics into your own monitoring framework

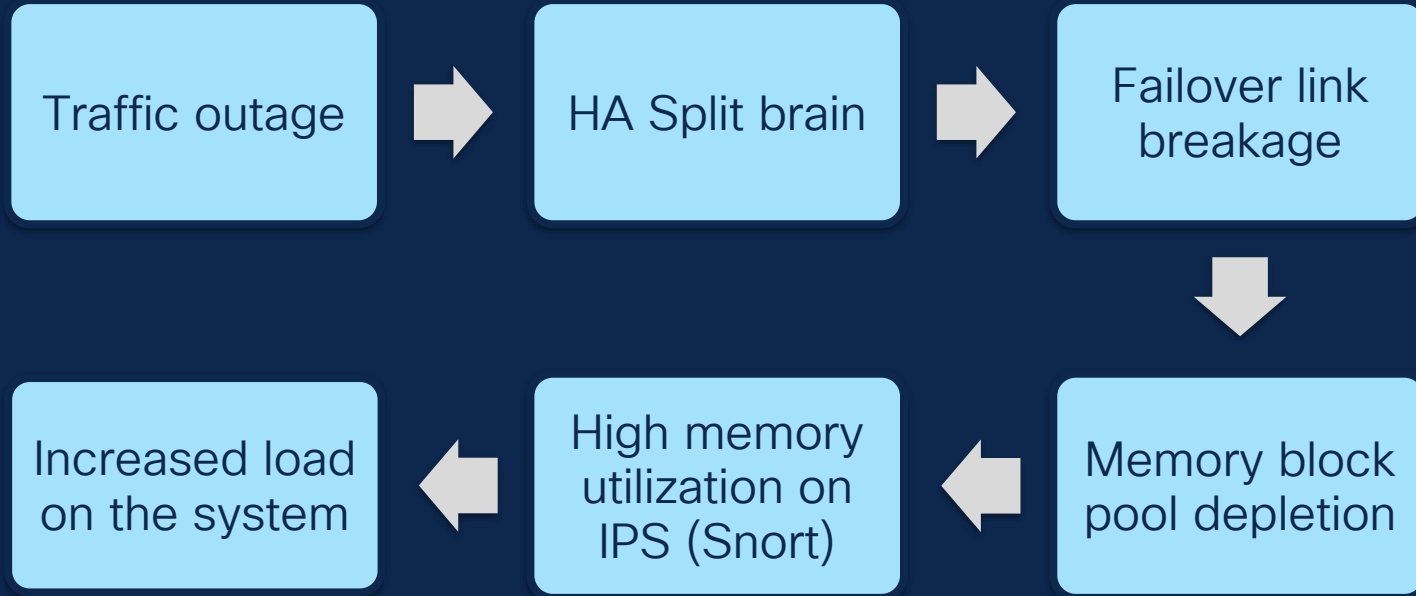
Agenda

- Health Monitoring 101
- The Big Bang Clustering Theory Simplified
- Processing Mystical Elephant Flows
- VPN Network Insights

Health Monitoring 101

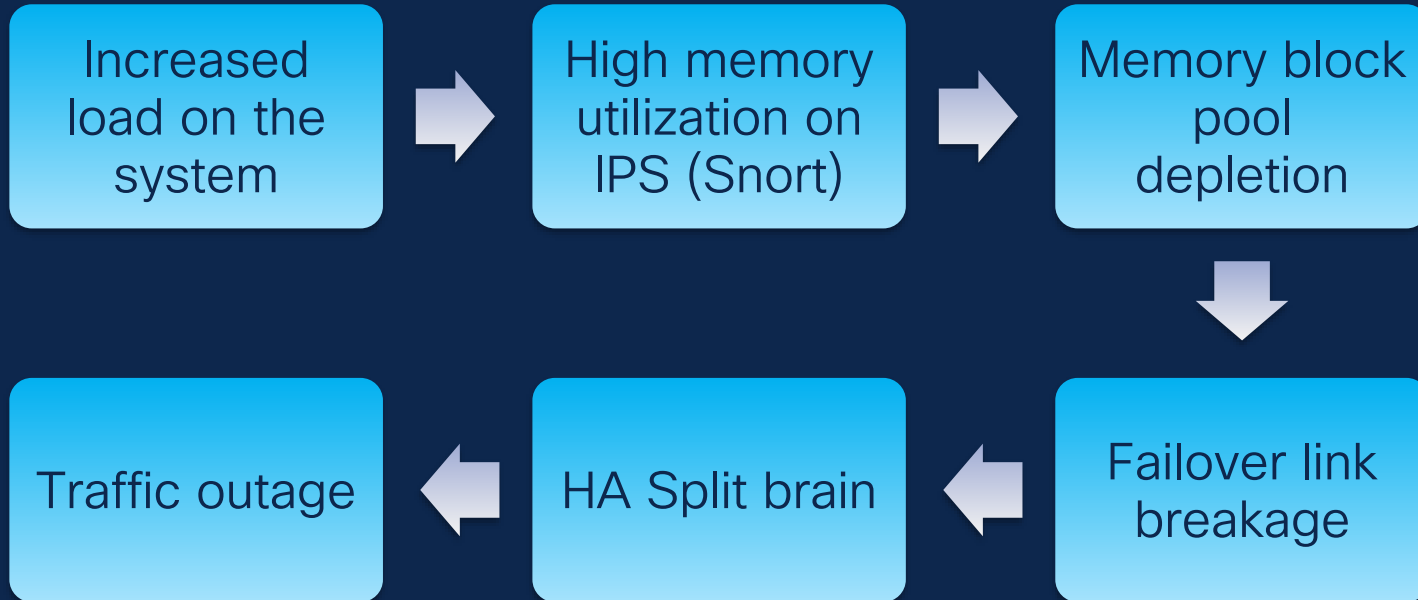
Healthcare System Outage

NIK's incident analysis steps for the 2hr 45min outage



Healthcare System Outage

The actual sequence of events that led to the outage

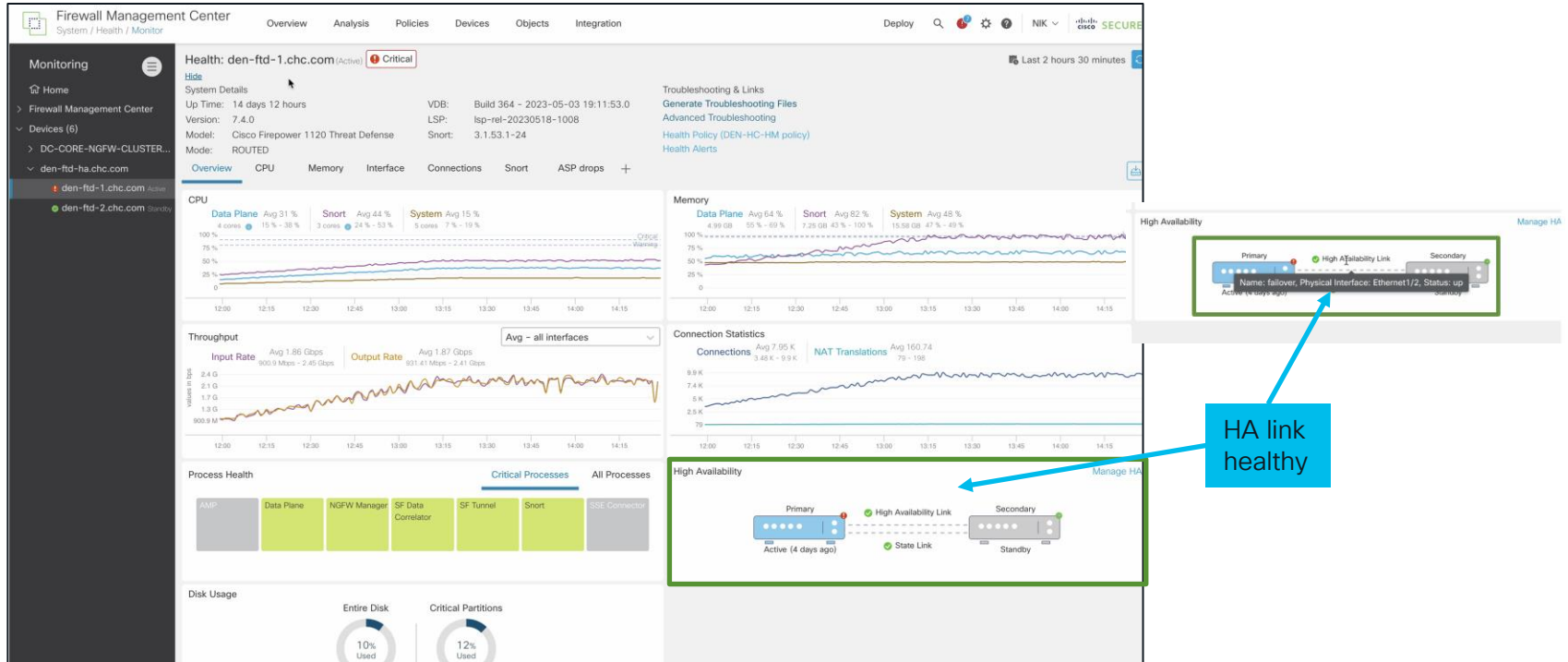


Demo

- How NIK can leverage Health Monitoring Dashboard to avoid outage

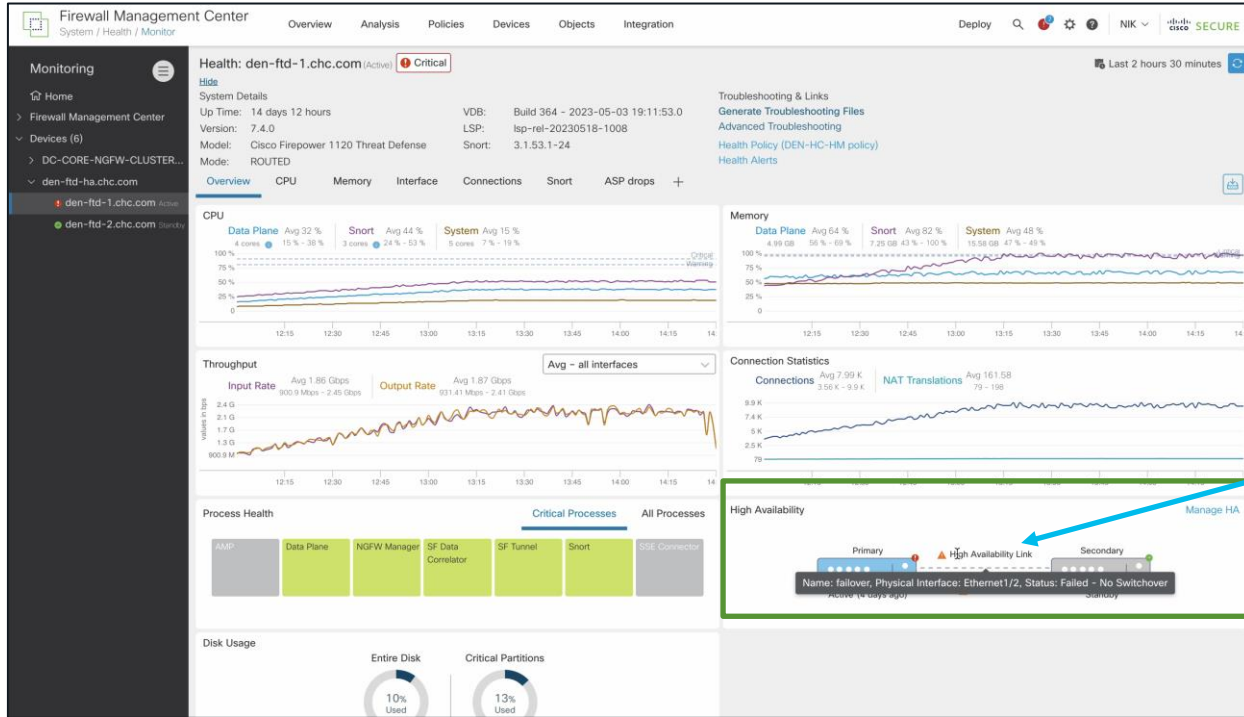
Healthcare System Outage

FTD HA Dashboard - Overview



Healthcare System Outage

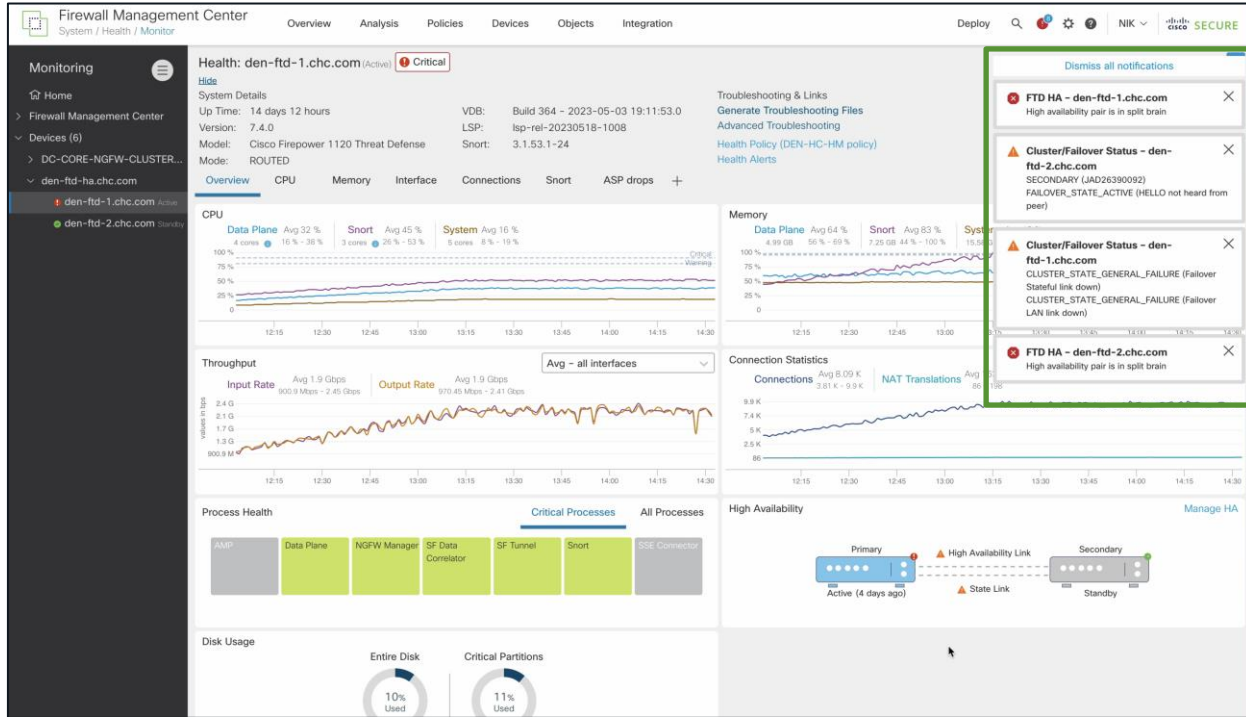
FTD HA Dashboard - Overview



HA link broken

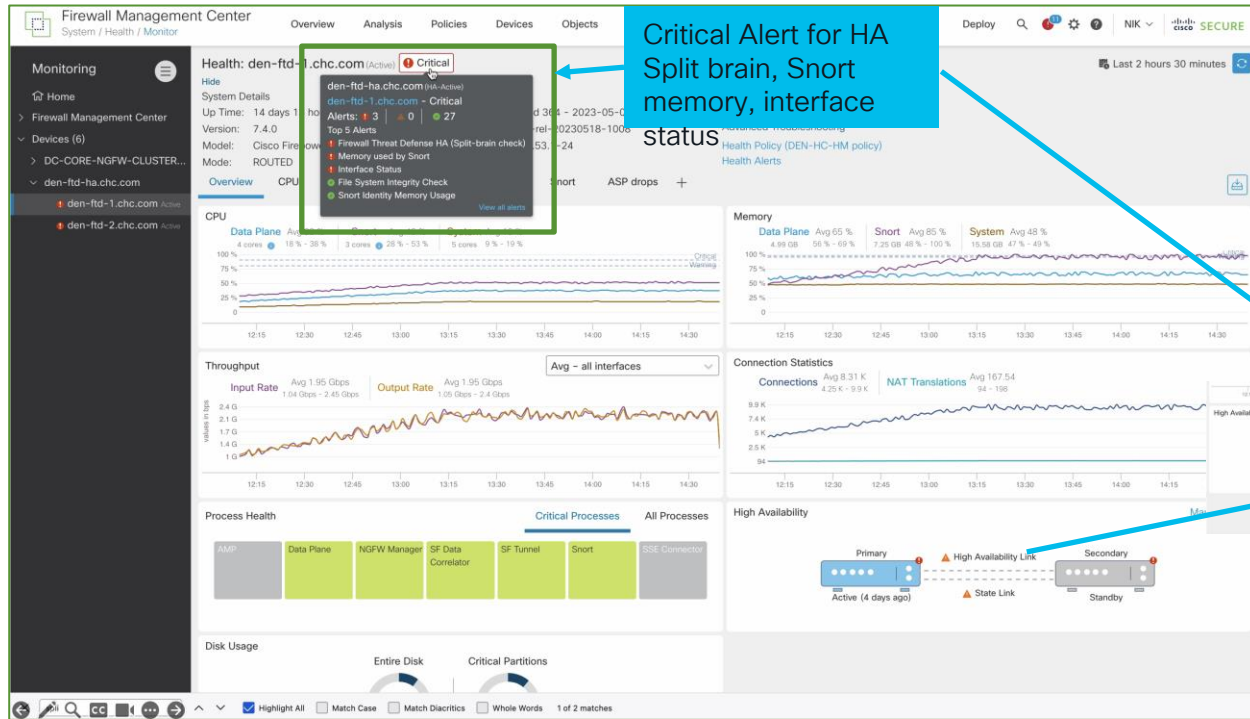
Healthcare System Outage

FTD HA Dashboard - Overview



Healthcare System Outage

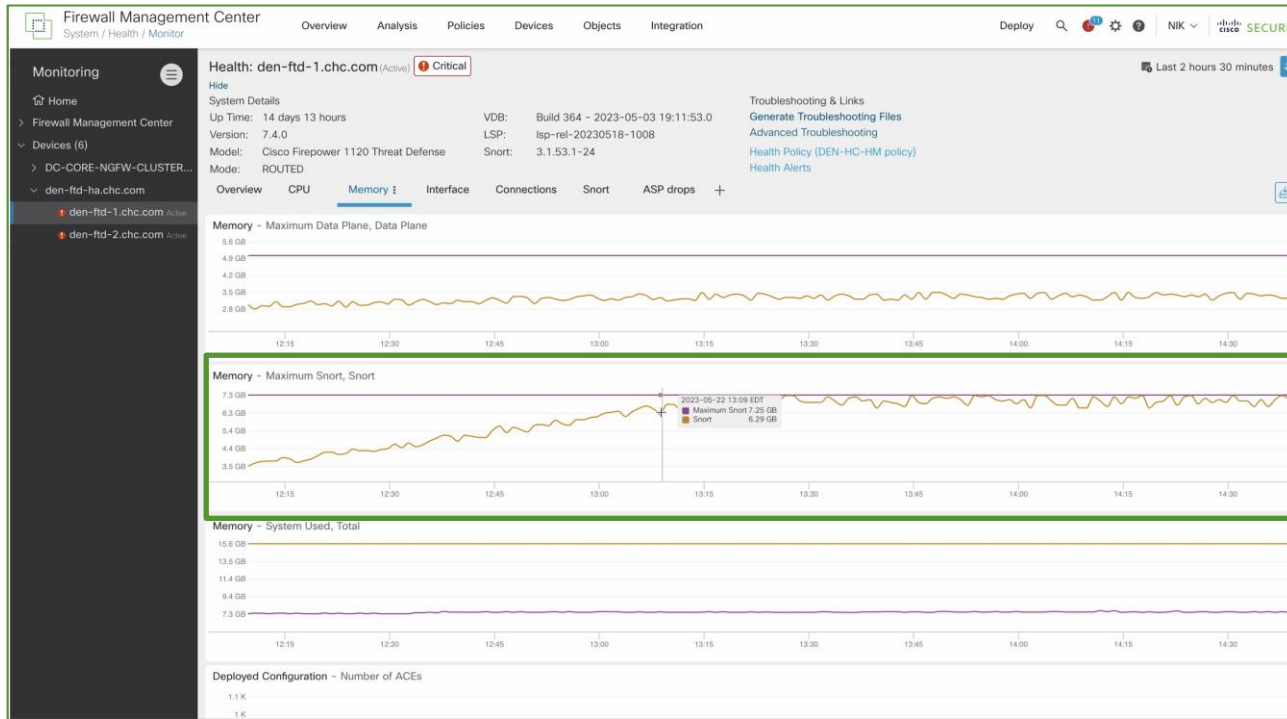
FTD HA Dashboard - Overview



Critical Alert for HA Split brain, Snort memory, interface status

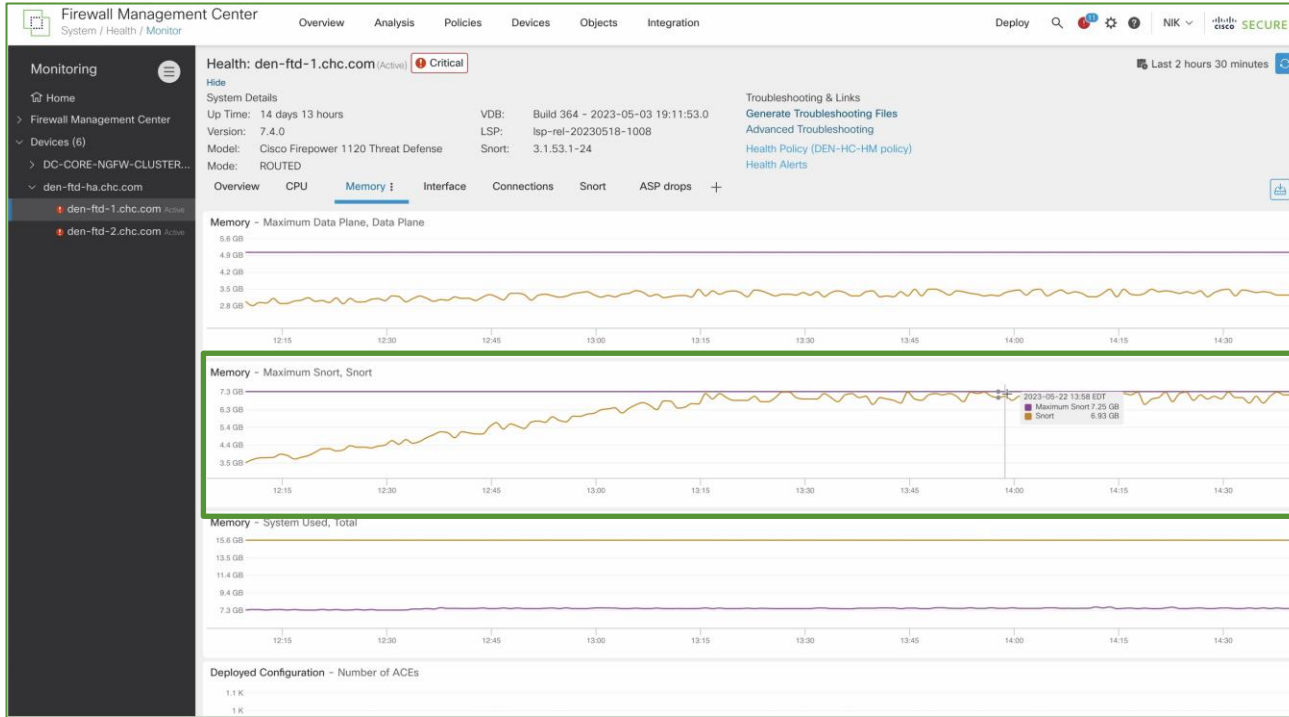
Healthcare System Outage

FTD HA Dashboard – Memory growth 3 hours prior to the split brain



Healthcare System Outage

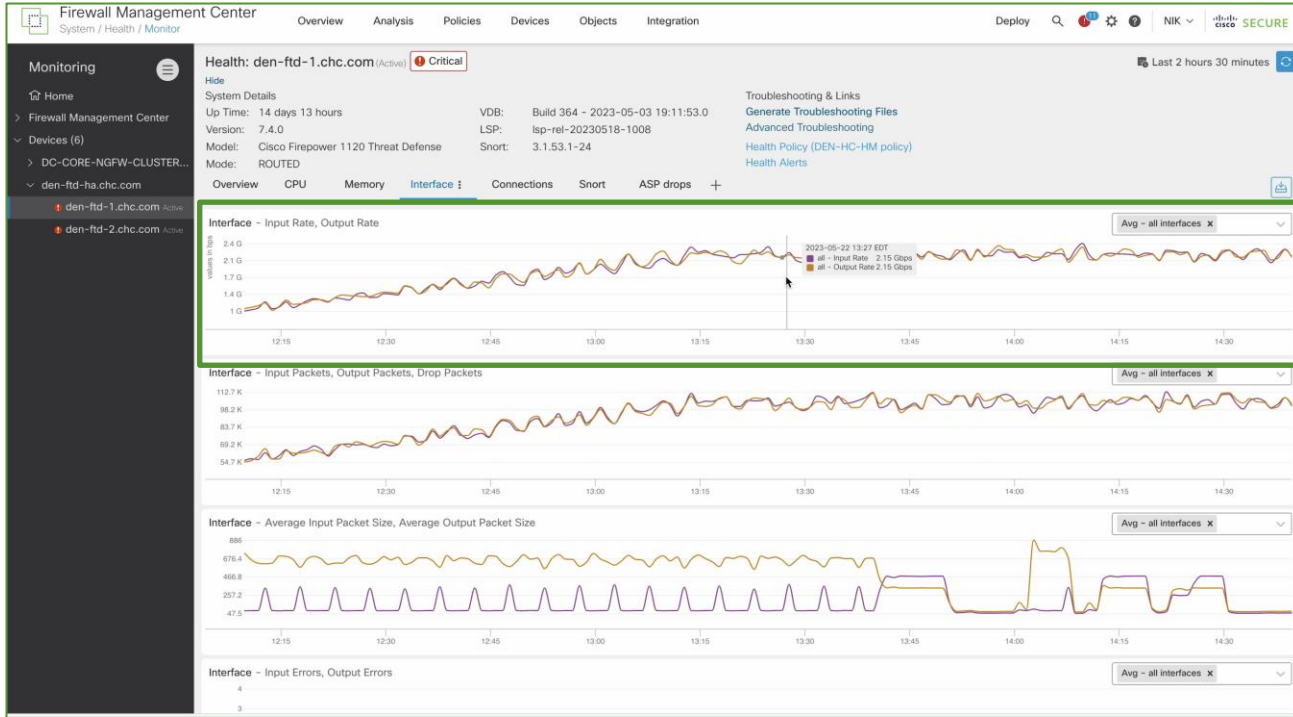
FTD HA Dashboard - Memory growth closer to the maximum threshold



Snort
memory
utilization
trend

Healthcare System Outage

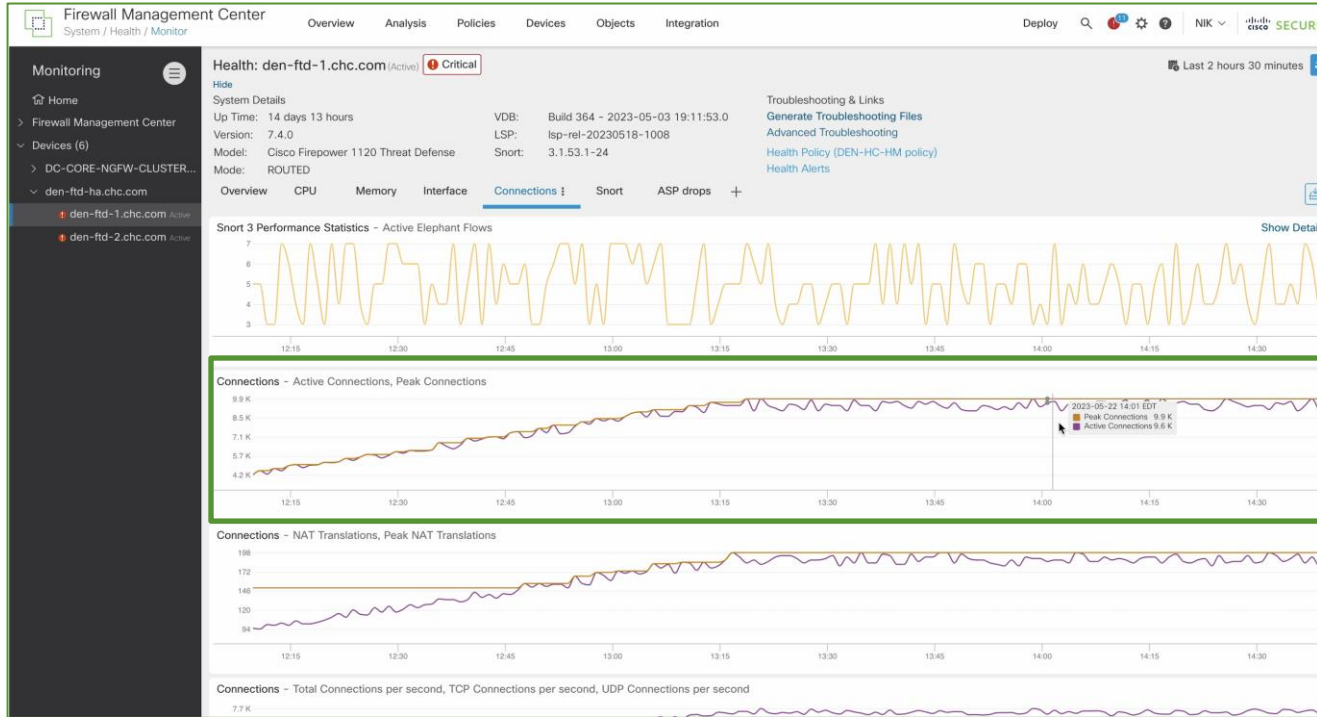
FTD HA Dashboard – Interface input output rate growing closer to the maximum limits



Interface input/output rate trend

Healthcare System Outage

FTD HA Dashboard - Connections



Connections Active / Peak trend

Healthcare System Outage

2 hour 45 minutes outage can come down to 0 minutes if you monitor:

CPU and Memory – Data plane, Snort, Systems

Connections – Active Connections

Throughput – Interface Input rate, Output rate

Snort Process Health

HA link status

How to Monitor Critical Processes in Secure Firewall

1

Understand system processes or parameters you can monitor

2

Configure a Health policy and alerts

3

Learn trends in your network

4

Take proactive steps before problem strikes

Health Monitoring System In Secure Firewall

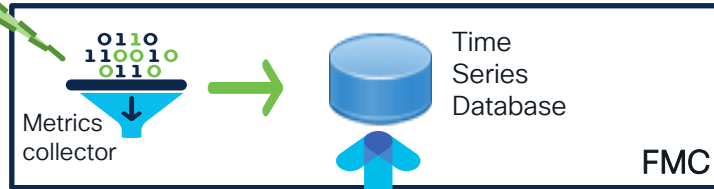
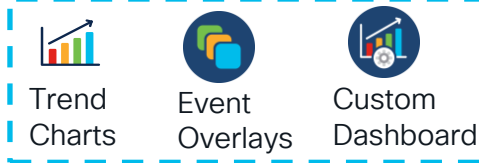
Integrations

Types of metrics
Utilization
Saturation
Error

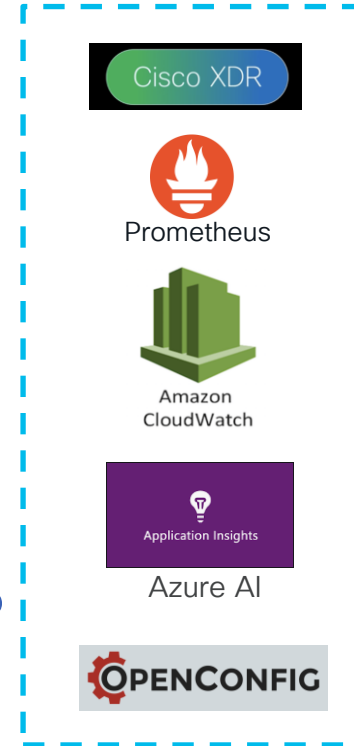
FMC APIs



FMC UI



FTD APIs

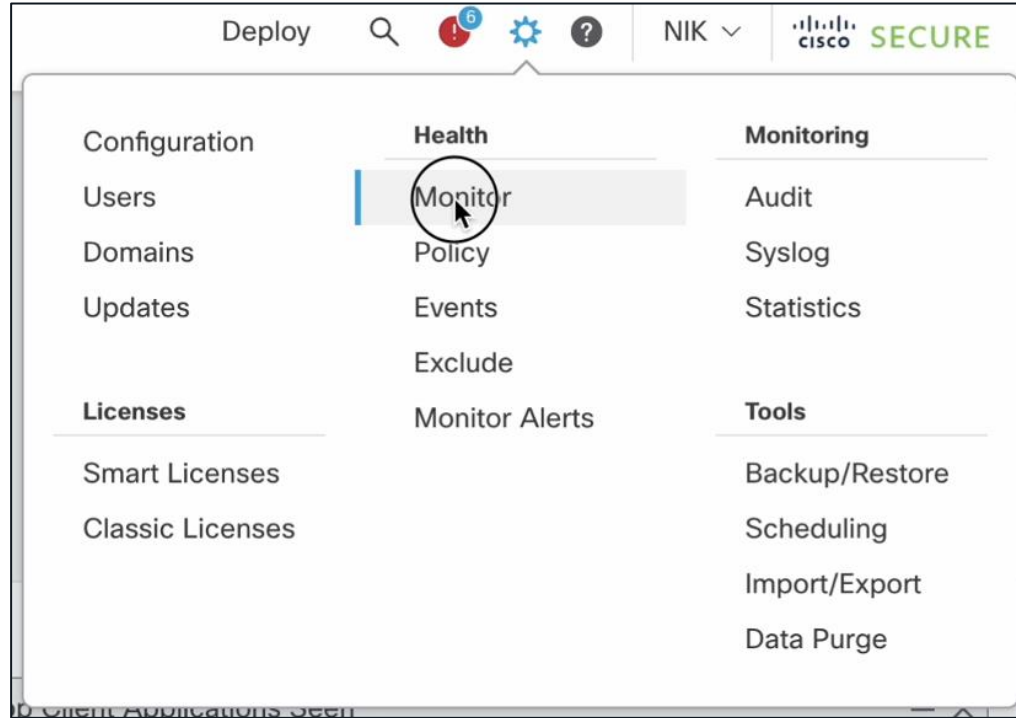


Demo

- Health Monitoring System Overview
- FMC Dashboard
- FTD Dashboard
- Create Health Policy

Health Monitoring Dashboard

System >> Health >> Monitor



Health Monitoring Dashboard

Device list

Alerts and Visual representation of devices

The screenshot displays the Cisco Firepower Management Center (FMC) Health Monitoring Dashboard. The interface includes a navigation menu on the left, a top navigation bar with tabs for Overview, Analysis, Policies, Devices, Objects, and Integration, and a main content area. The 'Devices' tab is selected, showing a 'Health Status' summary and a table of devices.

Health Status Summary:

- 8 total
- 4 critical
- 0 warnings
- 3 normal
- 1 disabled

Device List Table:

Device	Version	Model
FMC_Active		
FMC_Standby		
bgl-cisco-ngfw-1.dcbu.com	7.4.0	Cisco Firepower 9000 Series SM-40 Threat Defense
bgl-cisco-ngfw-2.dcbu.com	7.4.0	Cisco Firepower 9000 Series SM-40 Threat Defense
bgl-cisco-ngfw-3.dcbu.com	7.4.0	Cisco Firepower 9000 Series SM-40 Threat Defense
bgl-cisco-ngfw-4.dcbu.com	7.4.0	Cisco Firepower 9000 Series SM-40 Threat Defense
den-ftd-1.chc.com	7.4.0	Cisco Firepower 1120 Threat Defense
den-ftd-2.chc.com	7.4.0	Cisco Firepower 1120 Threat Defense

Health Monitoring Dashboard

Device List

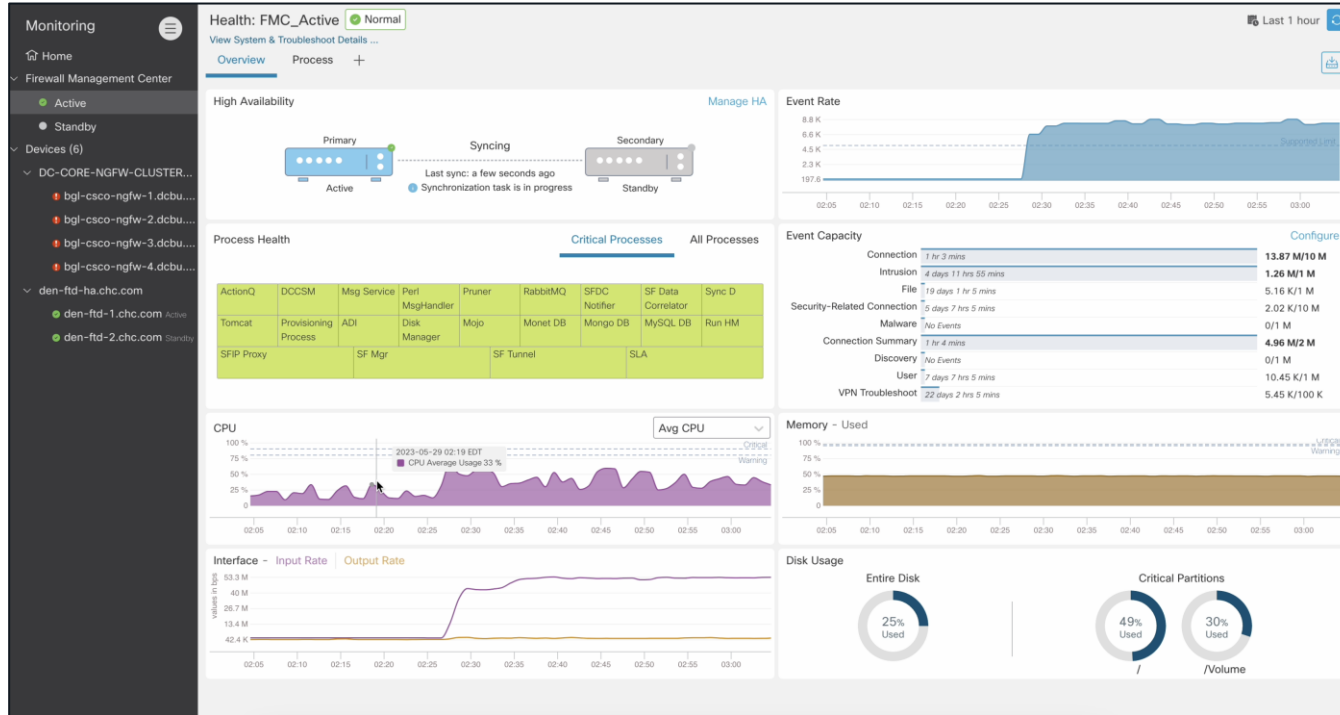
FMC Process List

The screenshot displays the Health Monitoring Dashboard interface. At the top, the 'Health Status' section shows 8 total devices, with 4 critical, 0 warnings, 3 normal, and 1 disabled. A search bar is available for filtering by device name. Below this, the 'Firewall Management Center' and 'Devices' sections are visible. The 'Devices' section contains a table with columns for Device, Version, and Model. The first device, 'FMC_Active', is expanded to show a detailed 'FMC Process List' on the left. This list includes several status items, all marked as successful (green dots): AMP for Endpoints Status (Process is running correctly), AMP for Firepower Status (Successfully connected to cloud), Appliance Heartbeat (All appliances are sending heartbeats correctly), CPU Usage (Average usage is 45.88%), Database (Integrity Checks are passed), and Discovery Host Limit (License is valid). On the right side of the table, for the 'FMC_Active' row, there are 'Export' and 'Run All' buttons. A tooltip is visible over the 'Export' button, indicating the option to 'Export alerts in CSV format'. The table lists several other devices, including 'FMC_Standby' and multiple 'bgl-csco-ngfw' devices, along with their versions and models.

Device	Version	Model
▼ FMC_Active	7.4.0	Secure Firewall Management Center for VMware
▶ FMC_Standby	7.4.0	Secure Firewall Management Center for VMware
▶ bgl-csco-ngfw-1.dcbu.com	7.4.0	Cisco Firepower 9000 Series SM-40 Threat Defense
▶ bgl-csco-ngfw-2.dcbu.com Control	7.4.0	Cisco Firepower 9000 Series SM-40 Threat Defense
▶ bgl-csco-ngfw-3.dcbu.com	7.4.0	Cisco Firepower 9000 Series SM-40 Threat Defense
▶ bgl-csco-ngfw-4.dcbu.com	7.4.0	Cisco Firepower 9000 Series SM-40 Threat Defense
▶ den-ftd-1.chc.com Active	7.4.0	Cisco Firepower 1120 Threat Defense
▶ den-ftd-2.chc.com Standby	7.4.0	Cisco Firepower 1120 Threat Defense

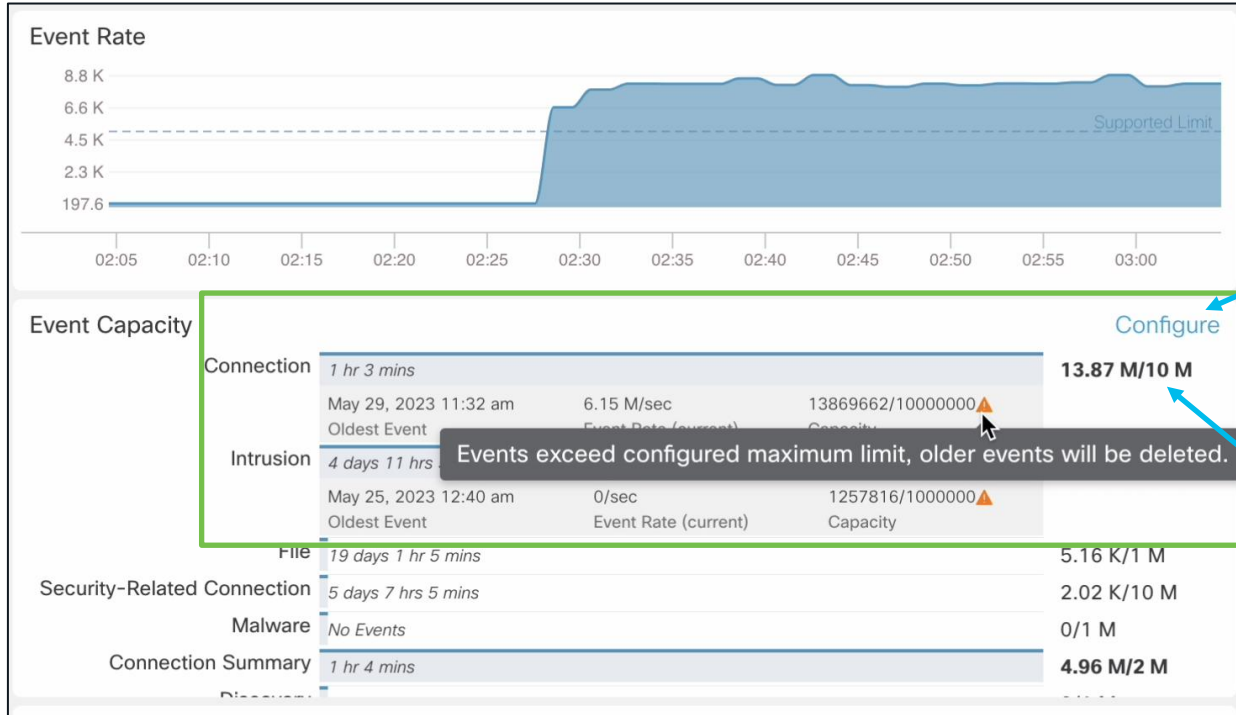
Health Monitoring Dashboard

FMC HA Overview Dashboard



Health Monitoring Dashboard

Event Capacity

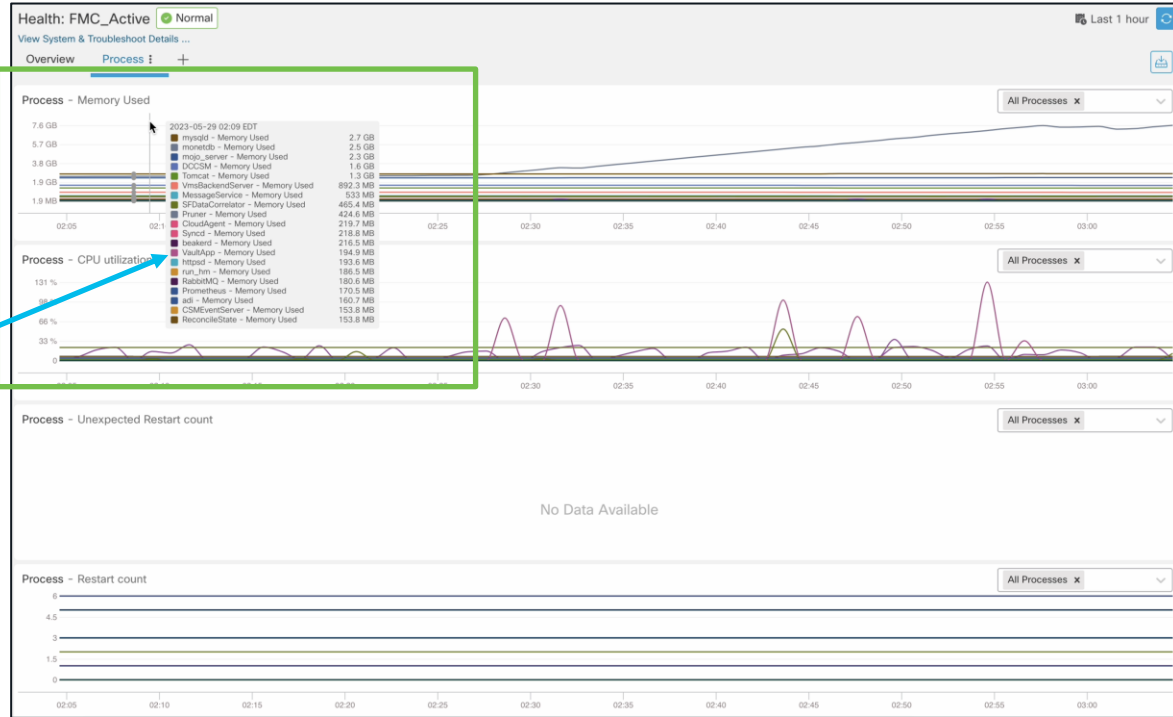


Configure capacity per event type

Event Capacity consumed vs configured

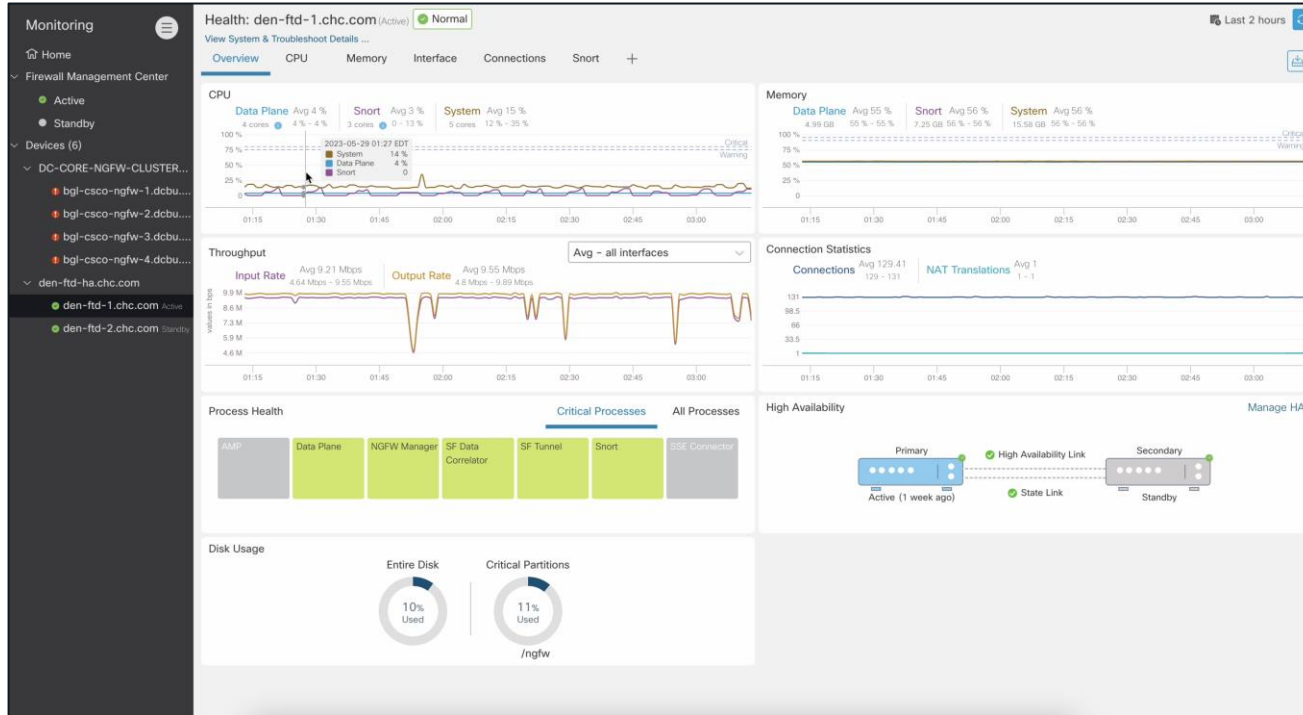
Health Monitoring Dashboard

FMC Processes Dashboard



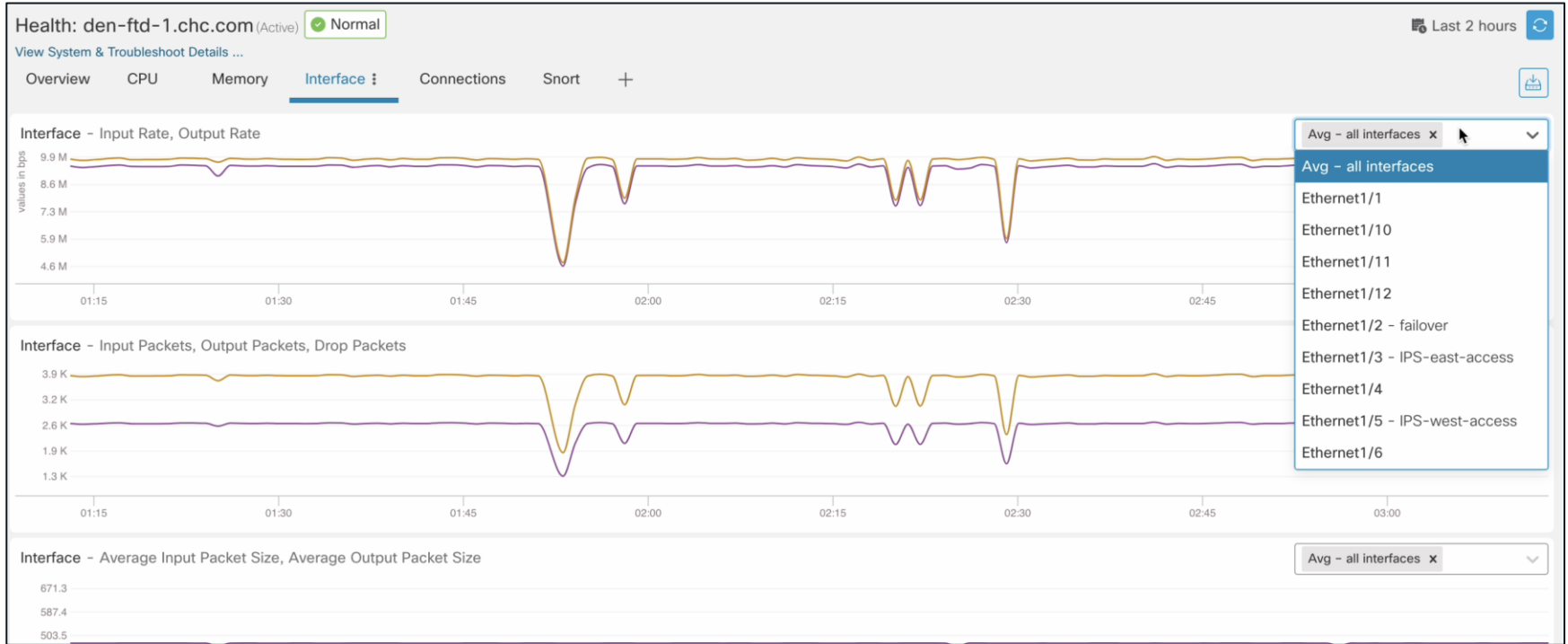
Health Monitoring Dashboard

FTD HA Overview Dashboard



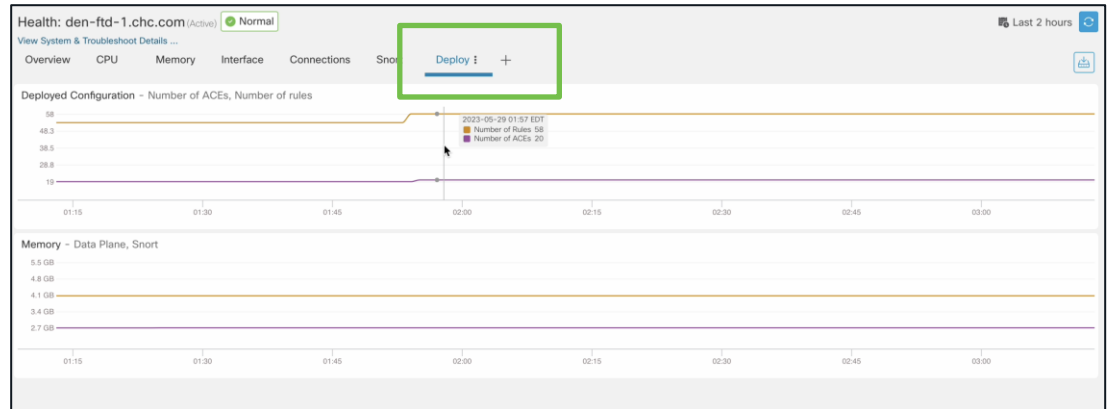
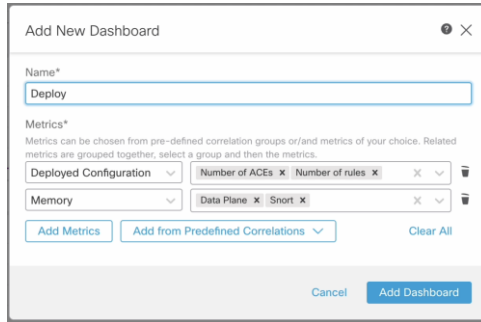
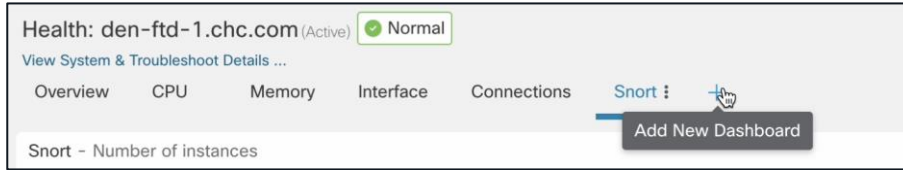
Health Monitoring Dashboard

FTD HA Interfaces Dashboard – View metrics for all interfaces or specific one



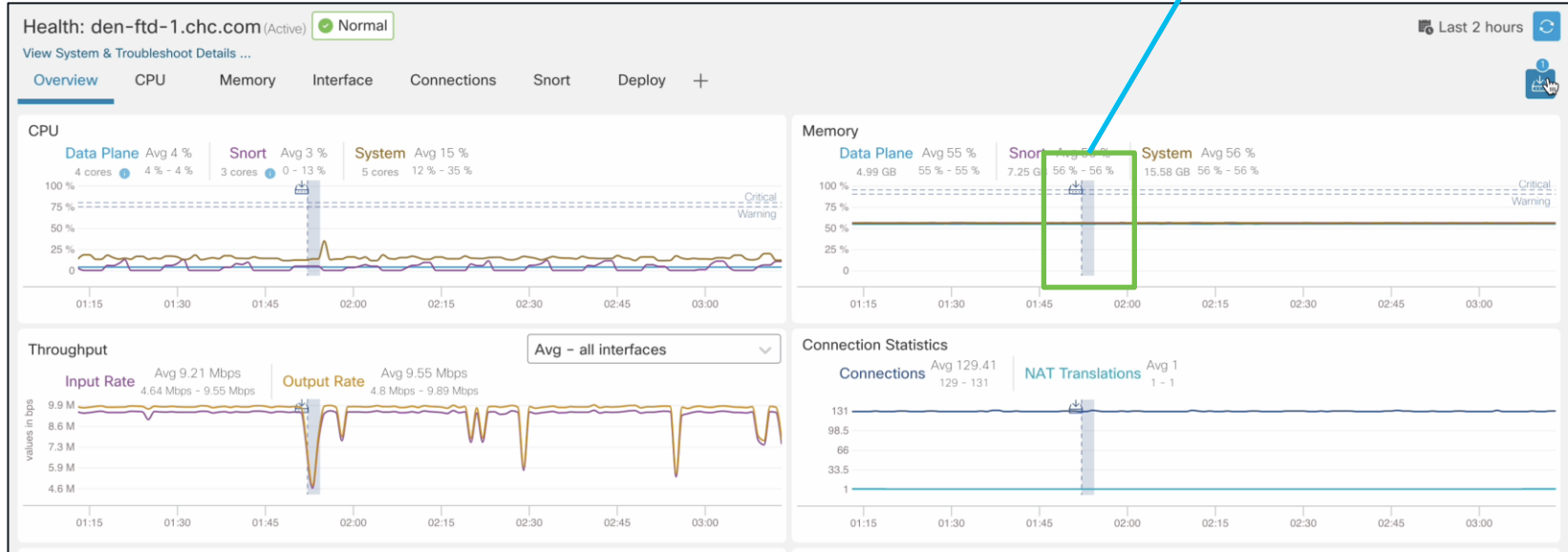
Health Monitoring Dashboard

Add Custom Dashboard – Name the dashboard and Select metrics



Health Monitoring Dashboard

Event overlay – Resource Utilization at the time of De



Health Monitoring Dashboard

Systems and Troubleshooting Panel, Select time range for trend

Health: den-ftd-1.chc.com (Active) Normal

[View System & Troubleshooting Details ...](#)

Overview CPU Memory Interface Connections Snort Deploy :

Health: den-ftd-1.chc.com (Active) Normal

[Hide](#)

System Details		Troubleshooting & Links
Up Time: 21 days 1 hour	VDB: Build 364 - 2023-05-03 19:11:53.0	Generate Troubleshooting Files
Version: 7.4.0	LSP: lsp-rel-20230524-1503	Advanced Troubleshooting
Model: Cisco Firepower 1120 Threat Defense	Snort: 3.1.53.1-24	Health Policy ()
Mode: ROUTED		Health Alerts

Overview CPU Memory Interface Connections Snort Deploy :

Last 2 hours

Fixed Time Range Sliding Time Range

Show the last

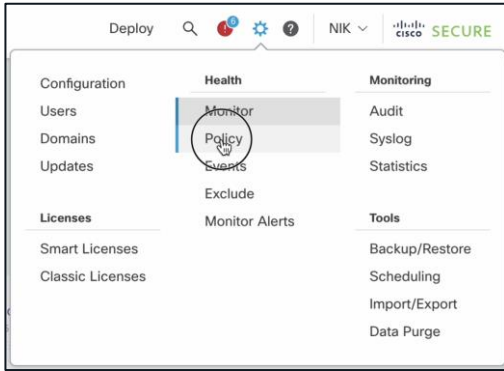
2 hours

Select last: 5 minutes, 30 minutes, 1 hour, 6 hours, 1 day, 2 weeks, 1 month

Apply

Health Monitoring Dashboard

Create Health Policy



The screenshot shows the 'Create Health Policy' dialog box. It contains the following fields:

- Name* (text input field)
- Base Policy* (dropdown menu with 'Select...' option)
- Description (text input field)

Buttons: Cancel, Save

Health Policy List

The screenshot shows the Health Policy List table. The table has the following columns: Policy Name, Domain, Applied To, and Last Modified. The table contains the following data:

Policy Name	Domain	Applied To	Last Modified
BLR-DCBU-HM policy Cluster FTD policy	Global	4 devices	2023-05-22 12:28:23 Last modified by arati
DEN-HC-HM policy Initial Health Policy	Global	0 devices	2023-05-22 12:32:49 Last modified by arati
Initial_Health_Policy 2023-05-18 07:42:14 Initial Health Policy	Global	0 devices	2023-05-22 12:38:16 Last modified by admin
DC-TEST-HM-Policy	Global	0 devices	2023-05-24 07:05:32 Last modified by NIK

Health Monitoring Dashboard

Configure Dashboards and Thresholds

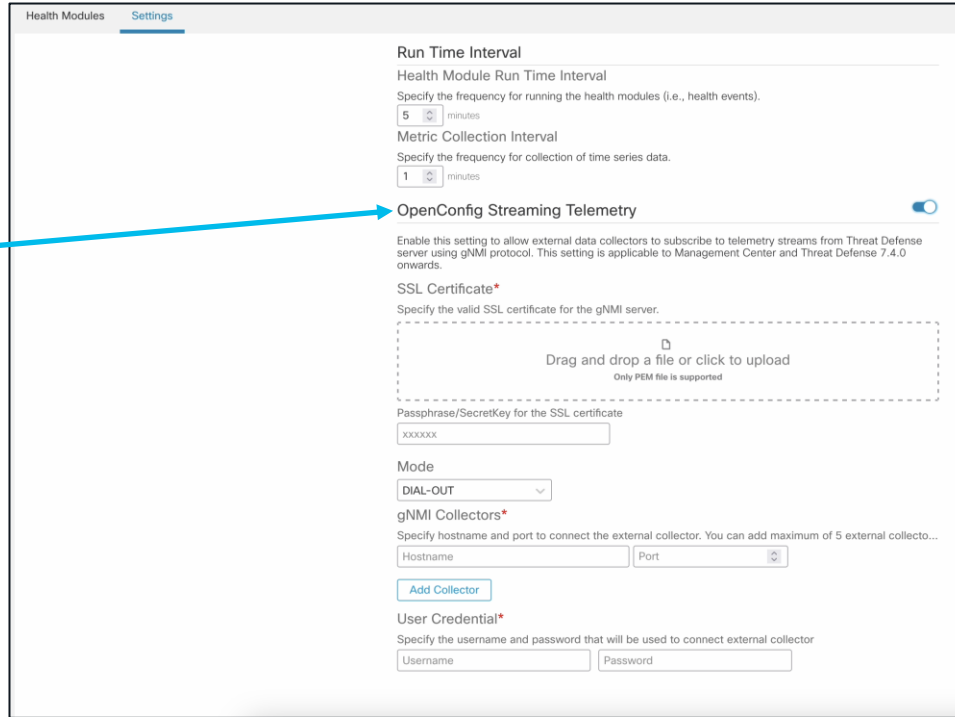
The screenshot displays the configuration interface for the 'CLUS-IT-HM Policy'. The interface is organized into several sections:

- Health Modules:** A sidebar on the left lists various monitoring modules, each with a toggle switch. Enabled modules include: Firewall Threat Defense Platform Faults, Hardware Alarms, Power Supply, CPU Usage (per core), Data Plane Statistics, ASP Drop, Connection Statistics, Flow Offload Statistics, Routing Statistics, and XTLS Counters.
- Settings:** A central area where specific thresholds and configurations are set for each module. For example:
 - Disk:** Disk Status, Disk Usage (Warning: 85%, Critical: 90%), and Warning Threshold (secondary HD) (Warning: 97%, Critical: 99%).
 - High Availability:** Cluster/HA Failure Status and Firewall Threat Defense HA (Split-brain check).
 - Integration:** SSE Connection Status.
 - Malware:** AMP Connection Status, AMP Threat Grid Connectivity, and Local Malware Analysis.
 - Memory:** Memory Usage (Warning: 95%, Critical: 97%), Memory Usage Data Plane (Warning: 80%, Critical: 90%), and Memory Usage Snort (Warning: 80%, Critical: 90%).
- Policy Assignments & Deploy:** A right-hand section for managing policy assignments, including:
 - Processes:** Critical Process Statistics and Process Status.
 - Snort:** Automatic Application Bypass, Configuration Resource Utilization, Intrusion and File Event Rate (Warning Event Rate: 30, Critical Event Rate: 50), Snort Identify Memory Usage (Critical threshold: 80%), Snort Reconfiguring Detection, Snort Statistics, and Snort3 Statistics.
 - Threat Data Updates:** Threat Data Updates on Devices (Warning alert after: 1 hour, Critical alert after: 24 hours).
 - Time Synchronization:** NTP Statistics.
 - VPN:** VPN Statistics.

Health Monitoring Dashboard

Health Policy Settings

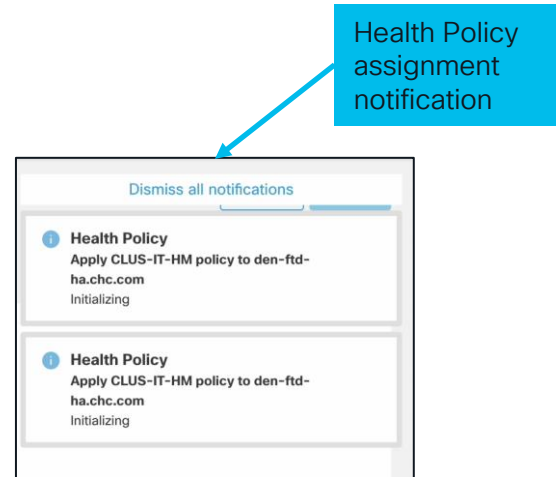
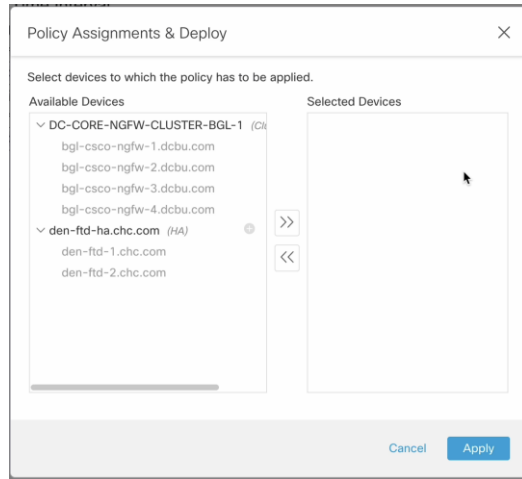
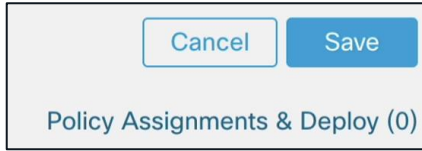
Configure OpenConfig Streaming Telemetry



The screenshot shows the 'Settings' tab for 'Health Modules'. It includes sections for 'Run Time Interval' (set to 5 minutes), 'Metric Collection Interval' (set to 1 minute), and 'OpenConfig Streaming Telemetry' (enabled). Below this are fields for 'SSL Certificate' (with a file upload area), 'Passphrase/SecretKey for the SSL certificate' (masked as 'xxxxxx'), 'Mode' (set to 'DIAL-OUT'), and 'gNMI Collectors*' (with fields for 'Hostname' and 'Port'). At the bottom, there is a 'User Credential*' section with 'Username' and 'Password' fields.

Health Monitoring Dashboard

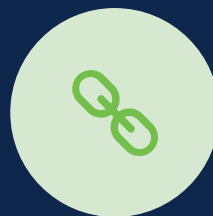
Save, Assign and Deploy Health Policy



Why You Should Use The Health Monitoring System?



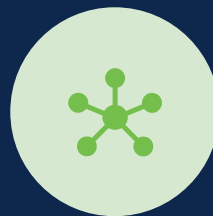
Easy to use



Extensible



Advance
Correlation



Integrations



The bridge to possible

The Big Bang Clustering Theory Simplified

CISCO *Live!*

#CiscoLive



Optimize Cluster Performance using Health Monitoring

Network Administrator NIK's Journey into:
Enhanced Cluster dashboard to optimize performance of the cluster and minimize traffic drops in a network

Cluster Performance Optimization with Health Monitoring



Monitoring of load distribution across nodes



Visibility of Cluster Control Link throughput



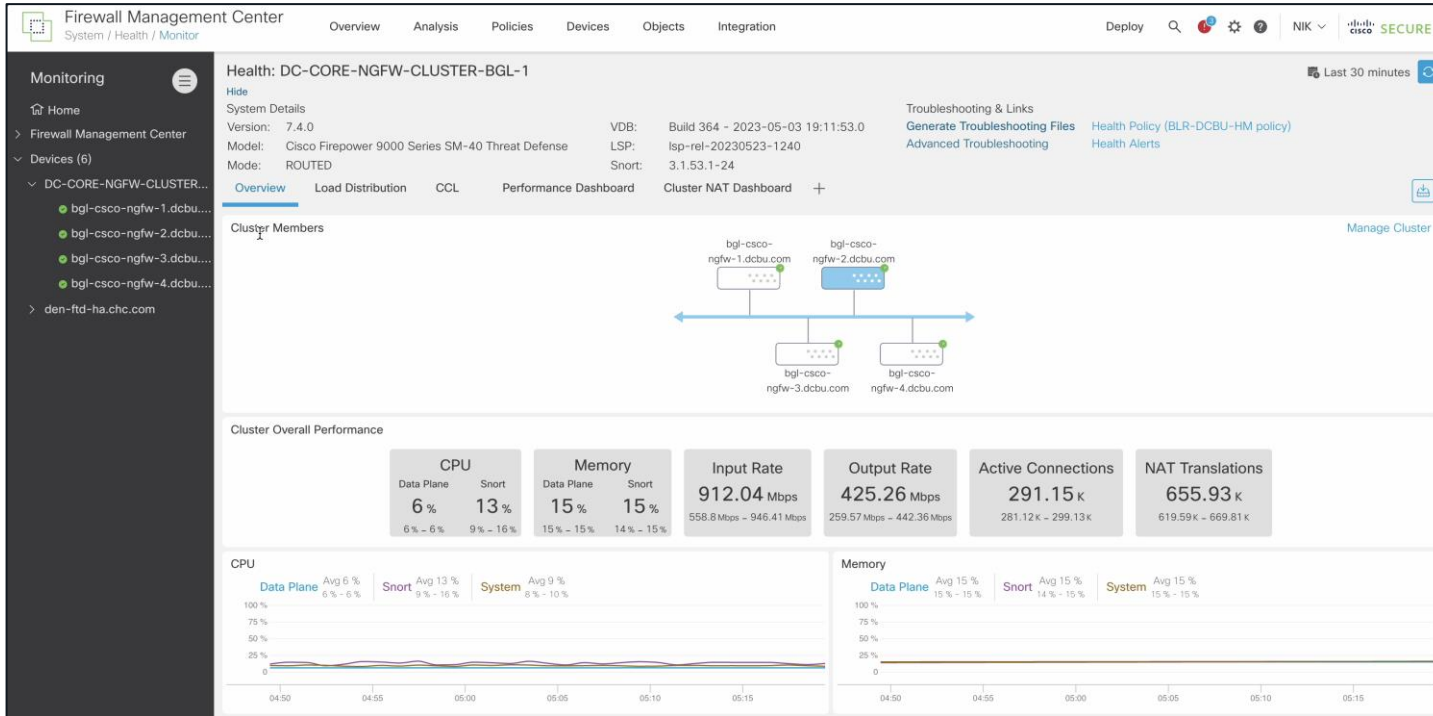
Indications on evolving bandwidth needs

Demo

- Cluster Node Imbalance Monitoring and Remediation

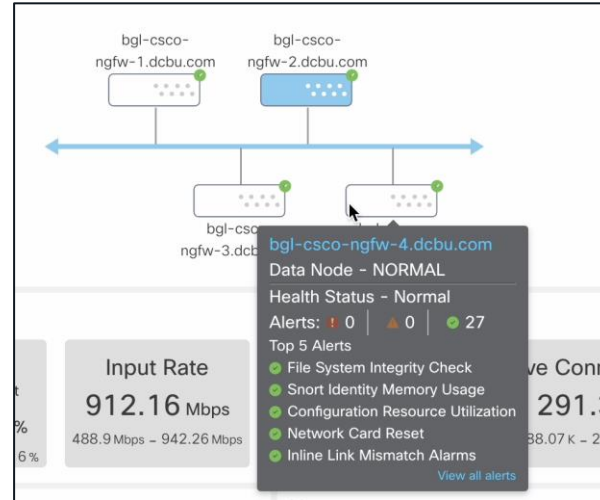
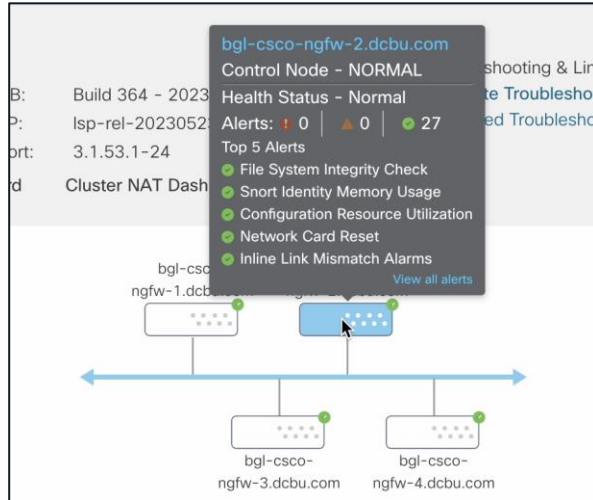
FTD Cluster Dashboard

Cluster Overview



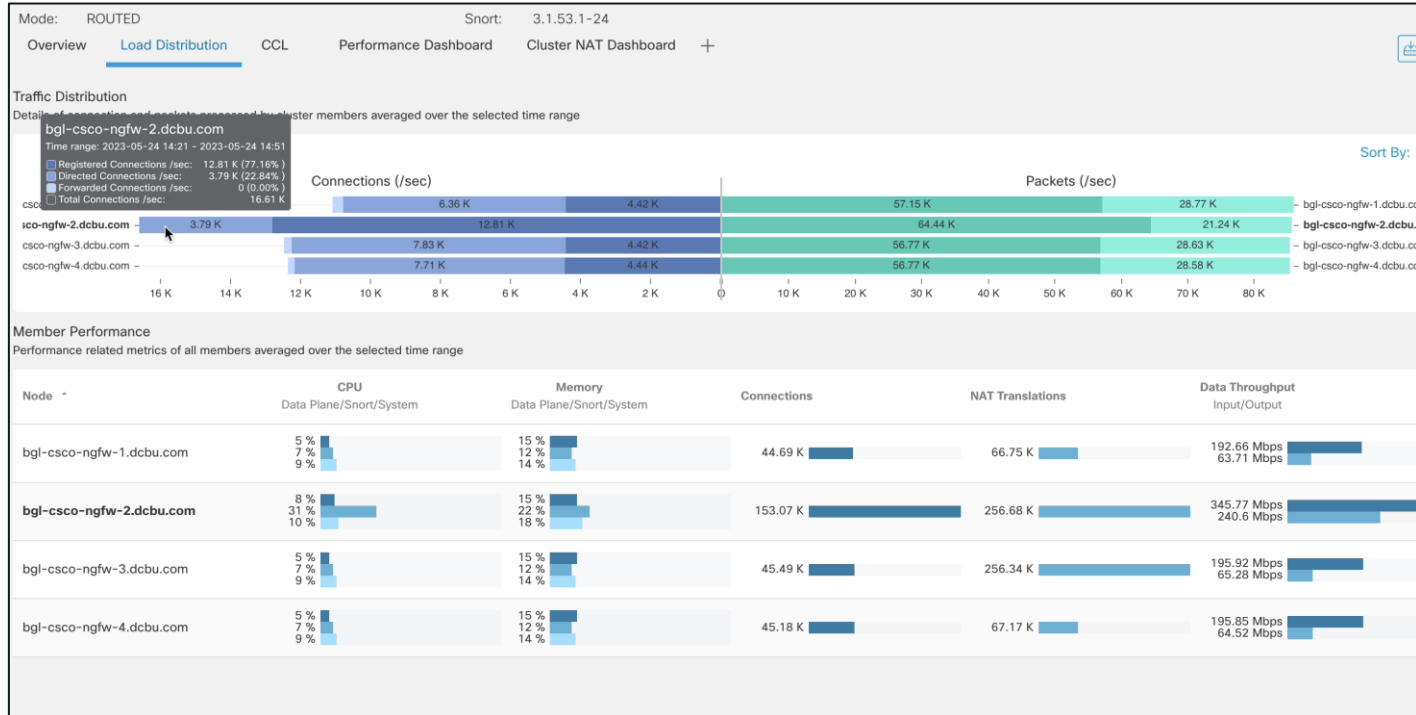
FTD Cluster Dashboard

Details of cluster nodes



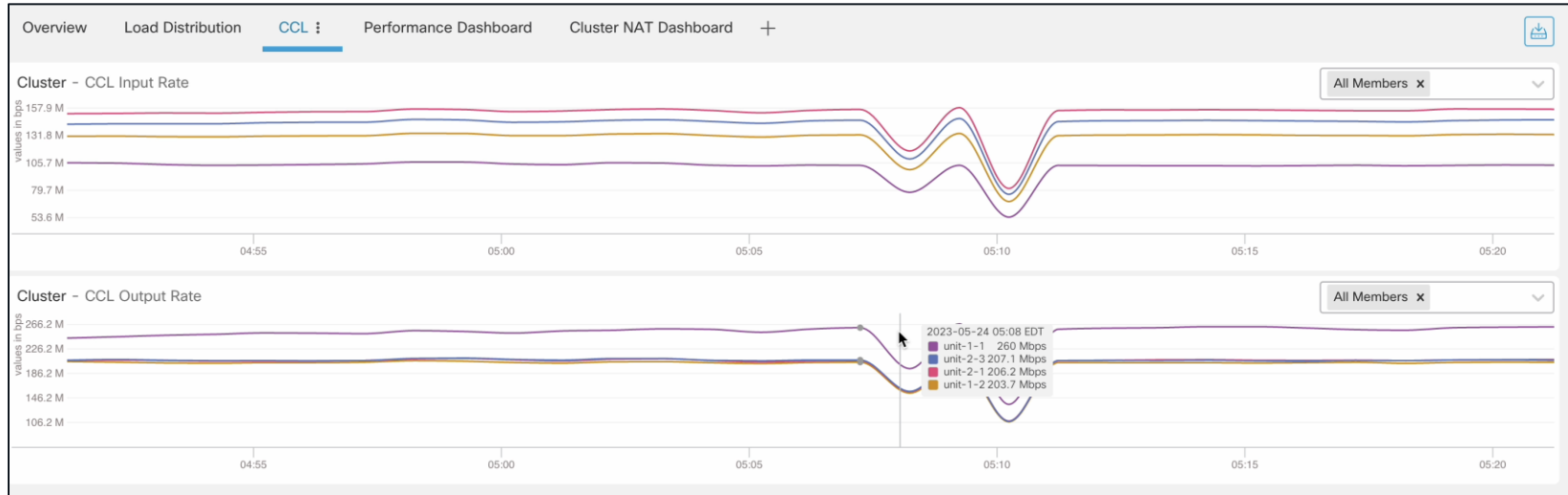
FTD Cluster Dashboard

Load imbalanced across nodes – Control node getting most traffic



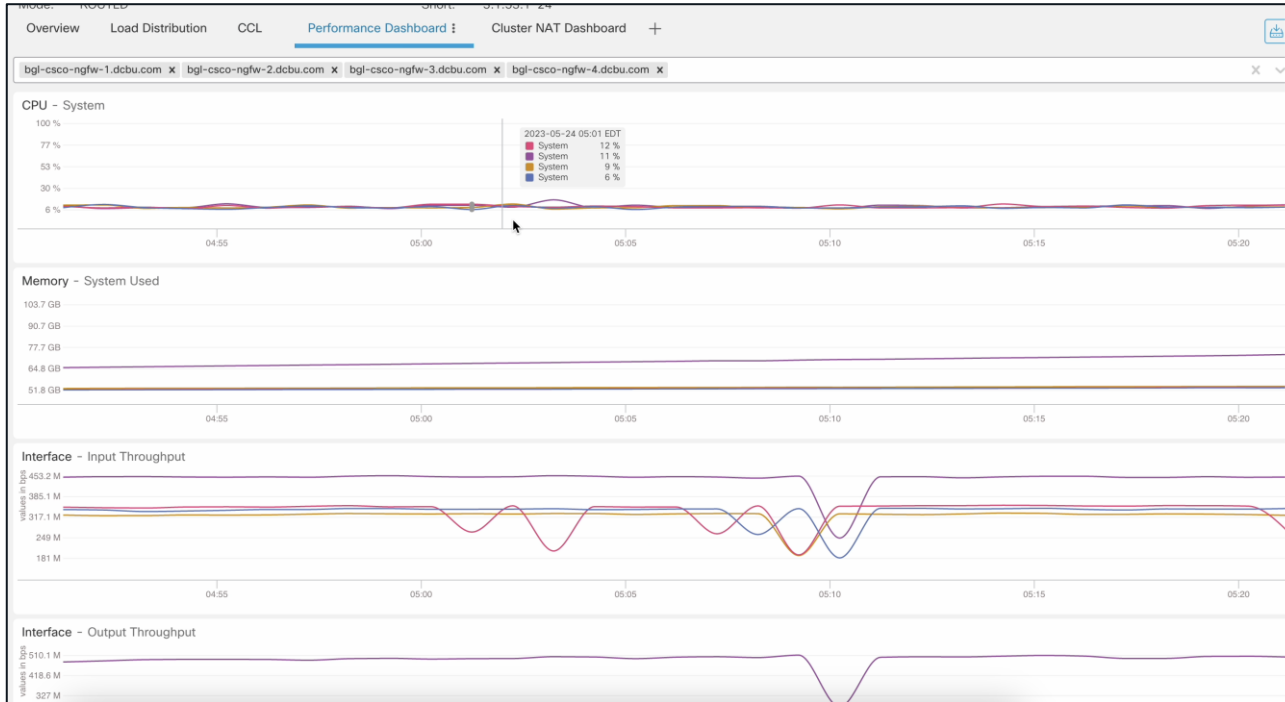
FTD Cluster Dashboard

Cluster Control Link (CCL) Health



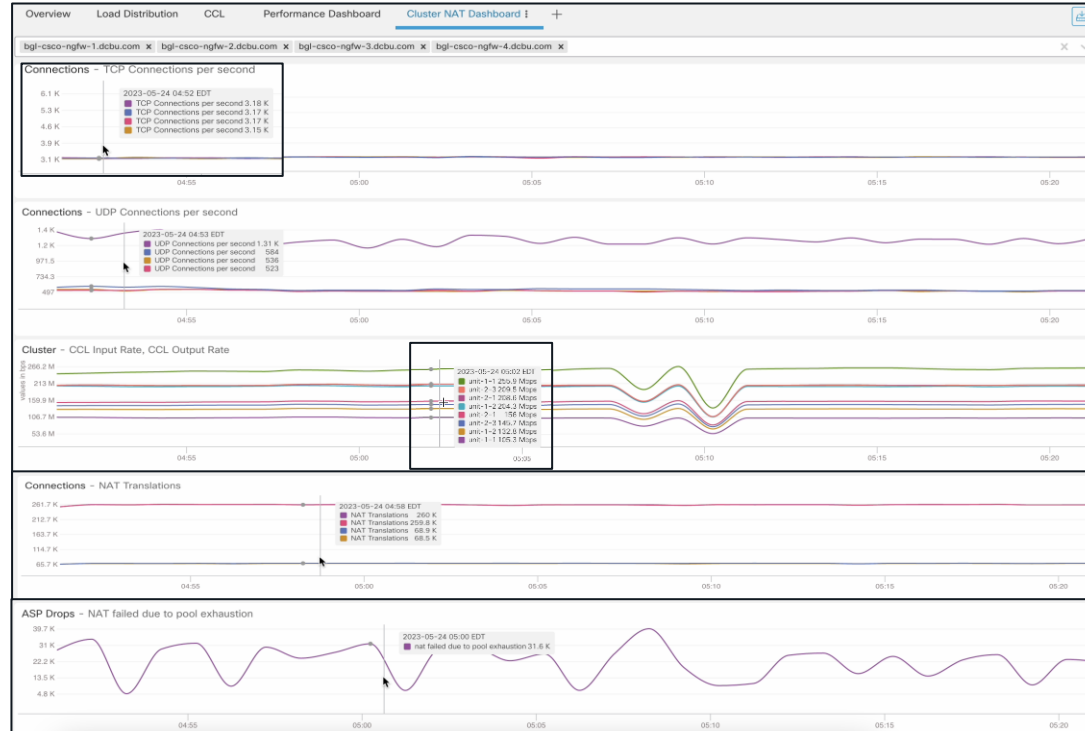
FTD Cluster Dashboard

Cluster Performance – CPU, Memory, Interface throughput



FTD Cluster Dashboard

Custom Dashboard – UDP traffic, NAT Translations unevenly distributed across nodes

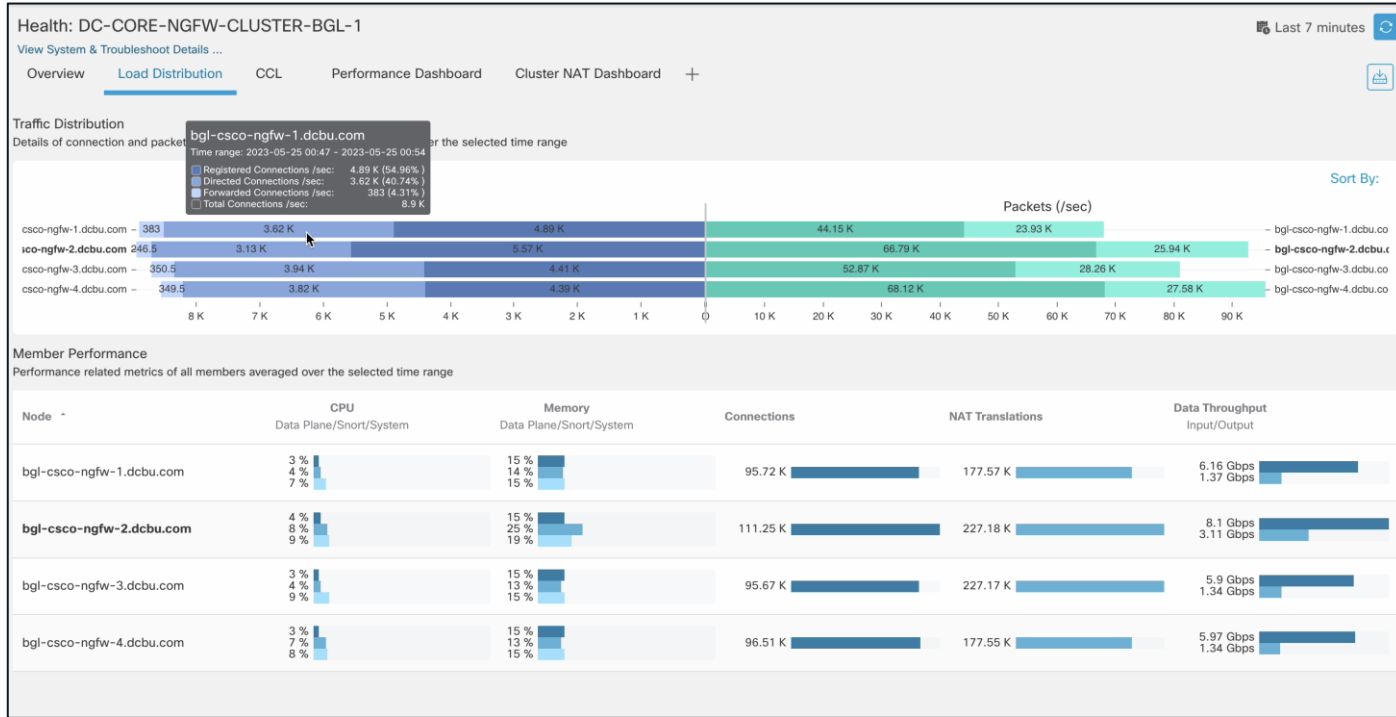


Remediation of Cluster Node Imbalance

- Cross check the load balancing algorithm on connected switches/routers
- Ensure an equal number of blades in each chassis in a multi-chassis cluster
- Enable per-session PAT for required traffic

FTD Cluster Dashboard

Load balanced across cluster nodes after remediation



FTD Cluster Dashboard

UDP traffic, NAT translations evenly distributed after remediation



Cluster Capacity Planning with Health Monitoring

Network Administrator NIK's Journey into:
Leveraging Cluster dashboard to
understand changing bandwidth needs

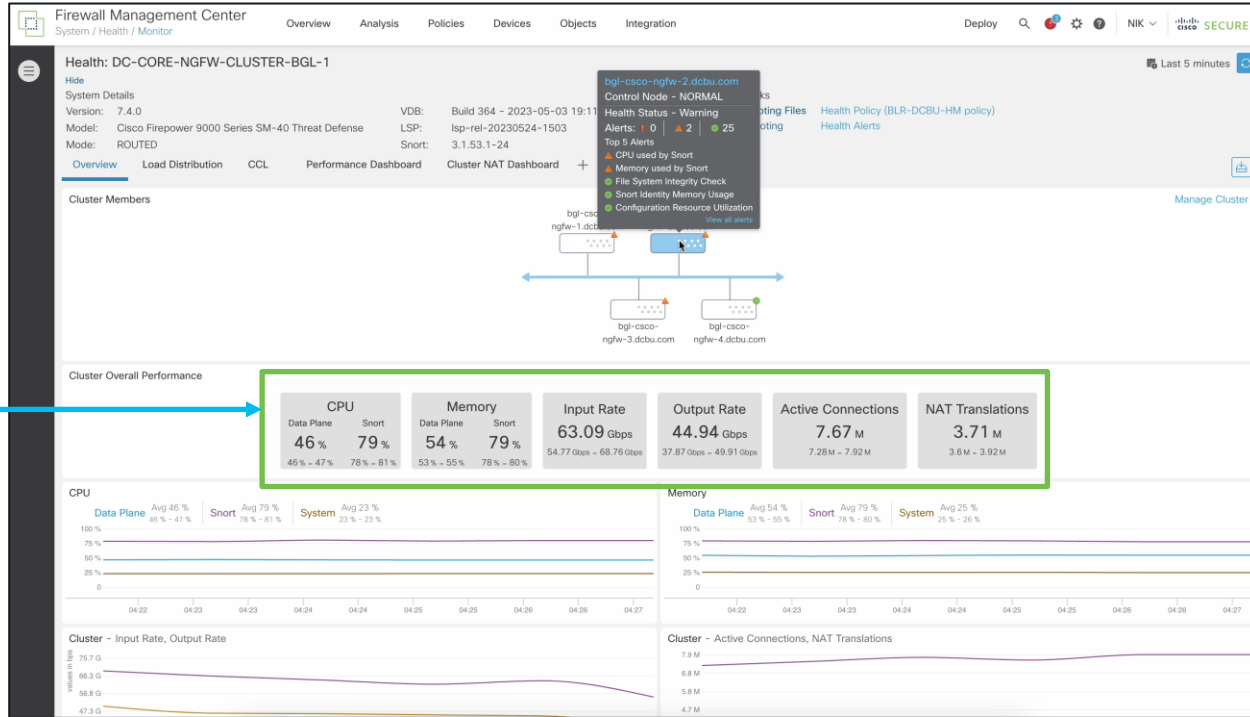
Cluster Capacity

The growing bandwidth need

Dataplane
CPU/Memory
growth is one
indication of
growing
bandwidth needs

4 node cluster of
SM-40 has
capacity of 120G

Input/Output rate
total is getting
closer to 120G



Cluster Monitoring

To optimize cluster performance and avoid traffic drops proactively NIK can monitor:

Cluster Members Status

Cluster Performance Panel

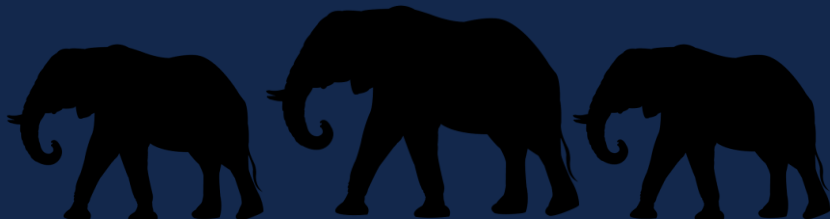
Load Distribution Across Nodes

CCL Usage

Custom Dashboard- ASP Drops, TCP and UDP Connections, NAT translations



The bridge to possible



Processing Mystical Elephant Flows



Processing Mystical Elephant flows

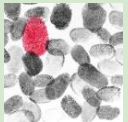
Network Administrator NIK's Journey into

- Optimize with Elephant Flow Detection, Visibility, and Remediation for your data centre.
- Improved Infrastructure services using Elephant flow detection, Visibility and remediation

Efficiently tame Elephant flows along with NIK using FMC

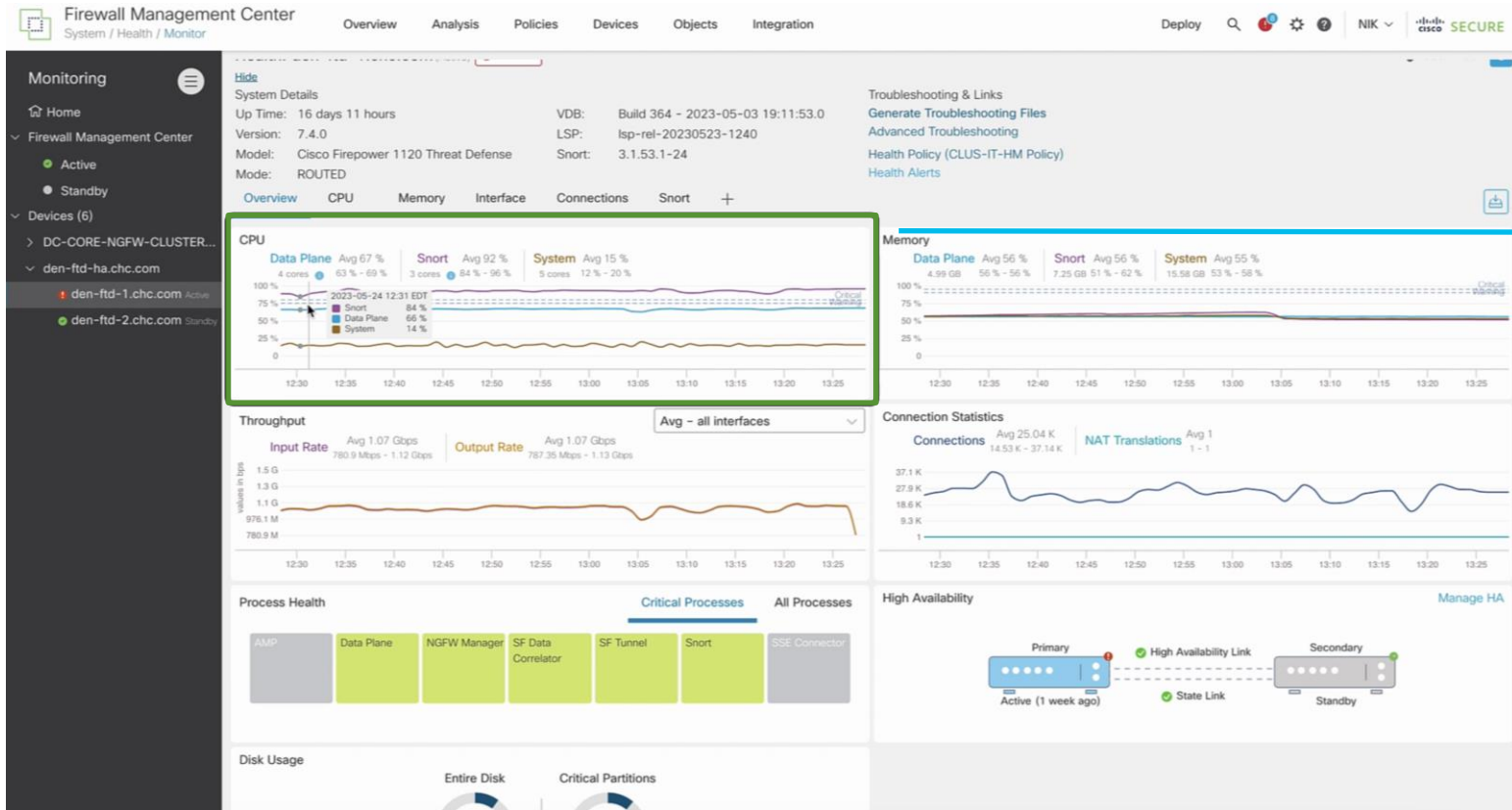


Elephant flow detection and Visibility



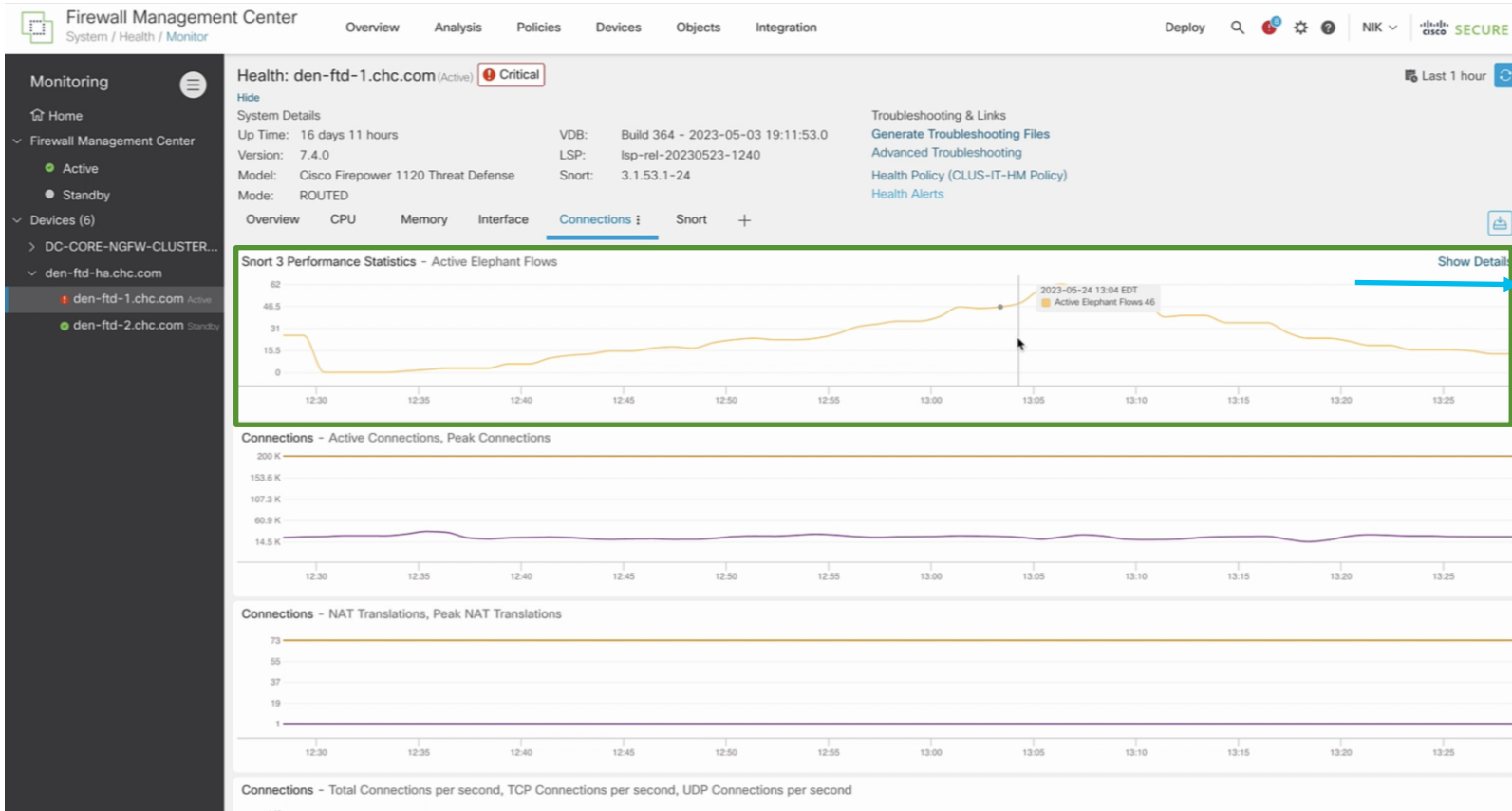
Analyse, Remediate by Bypass/ Throttle, or Exempt Elephant Flows

Elephant Flow Detection & Visibility



Monitor your Snort CPU

Elephant Flow Detection & Visibility



Monitor active elephant flows

Elephant Flow Detection & Visibility

The screenshot displays the Cisco Firewall Management Center (FMC) interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', and 'Integration'. The main content area shows the health of 'den-ftd-1.chc.com' with a 'Critical' status. Below this, there are tabs for 'Overview', 'CPU', 'Memory', 'Interface', 'Connections', and 'Snort'. The 'Connections' tab is active, showing 'Elephant Flow' monitoring. A summary bar indicates 'Number of Elephant Flows: 173' and 'CPU Utilization (%) : Avg: 50.16 Min: 41.89 Max: 58.05'. A blue arrow points from this summary bar to a callout box on the right that says 'Monitor trends into elephant flow'. Below the summary bar is a horizontal bar chart showing various flows over time, with labels such as '30.23.2.37:1027 - 20.2...' and '30.23.2.121:1026 - 20.23.1.1:443 - TCP'.

Monitor trends into elephant flow

Elephant Flow Detection & Visibility

Firewall Management Center
System / Health / Monitor

Overview Analysis Policies Devices Objects Integration Deploy 🔍 ⚙️ 🔄 NIK ✓ CISCO SECURE

Monitoring ☰

- Home
- Firewall Management Center
 - Active
 - Standby
- Devices (6)
 - DC-CORE-NGFW-CLUSTER...
 - den-ftd-ha.chc.com
 - den-ftd-1.chc.com Active
 - den-ftd-2.chc.com Standby

Health: den-ftd-1.chc.com (Active) Critical Last 1 hour ↻

Hide

System Details

Up Time: 16 days 11 hours VDB: Build 364 - 2023-05-03 19:11:53.0
Version: 7.4.0 LSP: lsp-rel-20230523-1240
Model: Cisco Firepower 1120 Threat Defense Snort: 3.1.53.1-24
Mode: ROUTED

Troubleshooting & Links
[Generate Troubleshooting Files](#)
[Advanced Troubleshooting](#)
[Health Policy \(CLUS-IT-HM Policy\)](#)
[Health Alerts](#)

Overview CPU Memory Interface Connections Snort +

Elephant Flow Hide Details

Number of Elephant Flows: 173 CPU Utilization (%) : Avg: 50.16 Min: 41.89 Max: 58.05

30.23.2.30:1026 - 20.2...
30.23.2.121:1026 - 20.23.1.1:443 - TCP

Source	Destination	Protocol	CPU Utilization (%)	Duration
30.23.2.121 : 1026	20.23.1.1 : 443	TCP	Avg:47.26 Min:33 Max:70	Completed (18 min+)

100%
75%
50%
25%
0

12:30 12:35 12:40 12:45 12:50 12:55 13:00 13:05 13:10 13:15 13:20 13:25

30.23.2.146:1035 - 20.23.1.1:443 - TCP
30.23.2.109:1028 - 20.23.1.1:443 - TCP
30.23.2.88:1033 - 20.23.1.1:443 - TCP
30.23.2.50:1033 - 20.23.1.1:443 - TCP
30.23.2.104:1028 - 20.23.1.1:443 - TCP
30.23.2.12:1035 - 20.23.1.1:443 - TCP
30.23.2.39:1028 - 20.23.1.1:443 - TCP

Drill down into each connection

Elephant Flow Detection & Visibility

Firewall Management Center
Analysis / Connections / Events

Overview Analysis Policies Devices Objects Integration Deploy 🔍 ⚙️ ? NIK 🔒 Cisco SECURE

Bookmark This Page | Reporting | Dashboard | View Bookmarks | Search

Connection Events (switch workflow)

No Search Constraints [\(Edit Search\)](#) II 2023-05-

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

Jump to...

<input type="checkbox"/>	↓ First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code	Application Protocol	Client	Web App	
▼	<input type="checkbox"/> 2023-05-24 13:30:00	2023-05-24 13:30:00	Allow		30.23.2.22	USA	20.23.1.108	NLD	LAN-ZONE		1044 / tcp	443 (https) / tcp				
▼	<input type="checkbox"/> 2023-05-24 13:30:00	2023-05-24 13:30:00	Allow		1.1.124.0	JPN	1.2.125.208	CHN			47727 / tcp	40630 / tcp	eDonkey	eDonkey		
▼	<input type="checkbox"/> 2023-05-24 13:30:00	2023-05-24 13:30:00	Allow		30.23.2.7	USA	20.23.1.102	NLD	LAN-ZONE		1047 / tcp	443 (https) / tcp				
▼	<input type="checkbox"/> 2023-05-24 13:30:00	2023-05-24 13:30:00	Allow		1.1.141.173	THA	1.2.136.60	THA			36859 / udp	53 (domain) / udp	DNS	DNS		
▼	<input type="checkbox"/> 2023-05-24 13:30:00	2023-05-24 13:30:00	Allow		1.1.4.95	CHN	1.2.25.89	CHN			7887 / tcp	80 (http) / tcp	HTTP	BitTorrent	BitTorrent	http://Tracker/announce?peer
▼	<input type="checkbox"/> 2023-05-24 13:30:00	2023-05-24 13:30:00	Allow		1.1.92.204	JPN	1.2.94.204	CHN			26241 / tcp	5190 / tcp	Unknown			
▼	<input type="checkbox"/> 2023-05-24 13:30:00	2023-05-24 13:30:00	Allow		1.1.58.153	CHN	1.2.136.171	THA			17381 / tcp	62591 / tcp				
▼	<input type="checkbox"/> 2023-05-24 13:30:00	2023-05-24 13:30:00	Allow		1.1.235.87	THA	1.2.97.88	CHN			54393 / tcp	5190 / tcp	Unknown			
▼	<input type="checkbox"/> 2023-05-24 13:30:00	2023-05-24 13:30:00	Allow		1.1.151.93	THA	1.2.128.221	THA			14862 / tcp	10892 / tcp	eDonkey	eDonkey		
▼	<input type="checkbox"/> 2023-05-24 13:30:00	2023-05-24 13:30:00	Allow		30.23.2.4	USA	20.23.1.101	NLD	LAN-ZONE		1048 / tcp	443 (https) / tcp				
▼	<input type="checkbox"/> 2023-05-24 13:30:00	2023-05-24 13:30:00	Allow		1.1.161.97	THA	1.2.163.82	THA			7857 / tcp	49602 / tcp				
▼	<input type="checkbox"/> 2023-05-24 13:30:00	2023-05-24 13:30:00	Allow		30.23.2.14	USA	20.23.1.105	NLD	LAN-ZONE		1048 / tcp	443 (https) / tcp				
▼	<input type="checkbox"/> 2023-05-24 13:30:00	2023-05-24 13:30:00	Allow		1.1.79.177	JPN	1.2.230.27	THA			57693 / tcp	2049 / tcp	NFS	NFS client		
▼	<input type="checkbox"/> 2023-05-24 13:30:00	2023-05-24 13:30:00	Allow		1.1.68.139	JPN	1.2.243.100	THA			20180 / tcp	4239 / tcp	eDonkey	eDonkey		
▼	<input type="checkbox"/> 2023-05-24 13:30:00	2023-05-24 13:30:00	Allow		1.1.67.75	JPN	1.2.241.134	THA			19881 / tcp	5190 / tcp	Unknown			
▼	<input type="checkbox"/> 2023-05-24 13:30:00	2023-05-24 13:30:00	Allow		1.1.65.24	JPN	1.2.247.82	THA			19392 / tcp	22 (ssh) / tcp	SSH	PuTTY		
▼	<input type="checkbox"/> 2023-05-24 13:30:00	2023-05-24 13:30:00	Allow		1.1.1.230	AUS	1.2.183.210	THA			3020 / tcp	51185 / tcp	eDonkey	eDonkey		
▼	<input type="checkbox"/> 2023-05-24 13:30:00	2023-05-24 13:30:00	Allow		1.1.68.139	JPN	1.2.225.215	THA			59142 / tcp	1162 / tcp	eDonkey	eDonkey		
▼	<input type="checkbox"/> 2023-05-24 13:30:00	2023-05-24 13:30:00	Allow		1.1.1.230	AUS	1.2.18.82	CHN			43899 / tcp	46407 / tcp	eDonkey	eDonkey		

- Predefined Searches
- Elephant Flows
- Malicious URLs
- Possible Database Access
- Risky Applications with Low Business Relevance
- Standard HTTP
- Standard Mail
- Standard SSL

Use predefined search



Elephant Flow Detection & Visibility

Bookmark This Page | Reporting | Dashboard | View Bookmarks | Search Predefined Searches ▾

Connection Events [\(switch workflow\)](#) || 2023-05-24 11:55:22 - 2023-05-24 13:30:08
Expanding

Search Constraints [\(Edit Search Save Search\)](#)

Connections with Application Details Table View of Connection Events

Jump to...

<input type="checkbox"/>	↓ First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code	Application Protocol	Client	Web Application	URL	URL Category	URL Reputation
▼ <input type="checkbox"/>	2023-05-24 13:28:35		Allow	Elephant Flow	30.23.2.7	USA	20.23.1.102	NLD	LAN-ZONE		1049 / tcp	443 (https) / tcp	HTTP	Web browser	WebEx	http://index.html		
▼ <input type="checkbox"/>	2023-05-24 13:28:22		Allow	Elephant Flow	30.23.2.20	USA	20.23.1.107	NLD	LAN-ZONE		1048 / tcp	443 (https) / tcp	HTTP	Web browser	WebEx	http://index.html		
▼ <input type="checkbox"/>	2023-05-24 13:27:50		Allow	Elephant Flow	30.23.2.8	USA	20.23.1.103	NLD	LAN-ZONE		1049 / tcp	443 (https) / tcp	HTTP	Web browser	WebEx	http://index.html		
▼ <input type="checkbox"/>	2023-05-24 13:27:44		Allow	Elephant Flow	30.23.2.19	USA	20.23.1.107	NLD	LAN-ZONE		1049 / tcp	443 (https) / tcp	HTTP	Web browser	WebEx	http://index.html		
▼ <input type="checkbox"/>	2023-05-24 13:27:29		Allow	Elephant Flow	30.23.2.14	USA	20.23.1.105	NLD	LAN-ZONE		1050 / tcp	443 (https) / tcp	HTTP	Web browser	WebEx	http://index.html		
▼ <input type="checkbox"/>	2023-05-24 13:27:20		Allow	Elephant Flow	30.23.2.19	USA	20.23.1.107	NLD	LAN-ZONE		1048 / tcp	443 (https) / tcp	HTTP	Web browser	WebEx	http://index.html		
▼ <input type="checkbox"/>	2023-05-24 13:27:09		Allow	Elephant Flow	30.23.2.7	USA	20.23.1.102	NLD	LAN-ZONE		1048 / tcp	443 (https) / tcp	HTTP	Web browser	WebEx	http://index.html		
▼ <input type="checkbox"/>	2023-05-24 13:27:05		Allow	Elephant Flow	30.23.2.20	USA	20.23.1.107	NLD	LAN-ZONE		1047 / tcp	443 (https) / tcp	HTTP	Web browser	WebEx	http://index.html		
▼ <input type="checkbox"/>	2023-05-24 13:27:05		Allow	Elephant Flow	30.23.2.24	USA	20.23.1.109	NLD	LAN-ZONE		1049 / tcp	443 (https) / tcp	HTTP	Web browser	WebEx	http://index.html		
▼ <input type="checkbox"/>	2023-05-24 13:27:03		Allow	Elephant Flow	30.23.2.3	USA	20.23.1.101	NLD	LAN-ZONE		1048 / tcp	443 (https) / tcp	HTTP	Web browser	WebEx	http://index.html		
▼ <input type="checkbox"/>	2023-05-24 13:26:55		Allow	Elephant Flow	30.23.2.11	USA	20.23.1.104	NLD	LAN-ZONE		1047 / tcp	443 (https) / tcp	HTTP	Web browser	WebEx	http://index.html		
▼ <input type="checkbox"/>	2023-05-24 13:26:33		Allow	Elephant Flow	30.23.2.10	USA	20.23.1.103	NLD	LAN-ZONE		1047 / tcp	443 (https) / tcp	HTTP	Web browser	WebEx	http://index.html		
▼ <input type="checkbox"/>	2023-05-24 13:26:33		Allow	Elephant Flow	30.23.2.4	USA	20.23.1.101	NLD	LAN-ZONE		1049 / tcp	443 (https) / tcp	HTTP	Web browser	WebEx	http://index.html		
▼ <input type="checkbox"/>	2023-05-24 13:26:28		Allow	Elephant Flow	30.23.2.5	USA	20.23.1.101	NLD	LAN-ZONE		1048 / tcp	443 (https) / tcp	HTTP	Web browser	WebEx	http://index.html		
▼ <input type="checkbox"/>	2023-05-24 13:25:59		Allow	Elephant Flow	30.23.2.22	USA	20.23.1.108	NLD	LAN-ZONE		1047 / tcp	443 (https) / tcp	HTTP	Web browser	WebEx	http://index.html		
▼ <input type="checkbox"/>	2023-05-24 13:25:35		Allow	Elephant Flow	30.23.2.1	USA	20.23.1.100	NLD	LAN-ZONE		1046 / tcp	443 (https) / tcp	HTTP	Web browser	WebEx	http://index.html		
▼ <input type="checkbox"/>	2023-05-24 13:24:53		Allow	Elephant Flow	30.23.2.25	USA	20.23.1.109	NLD	LAN-ZONE		1048 / tcp	443 (https) / tcp	HTTP	Web browser	WebEx	http://index.html		
▼ <input type="checkbox"/>	2023-05-24 13:24:02		Allow	Elephant Flow	30.23.2.15	USA	20.23.1.105	NLD	LAN-ZONE		1048 / tcp	443 (https) / tcp	HTTP	Web browser	WebEx	http://index.html		
▼ <input type="checkbox"/>	2023-05-24 13:23:46		Allow	Elephant Flow	30.23.2.13	USA	20.23.1.104	NLD	LAN-ZONE		1046 / tcp	443 (https) / tcp	HTTP	Web browser	WebEx	http://index.html		

Elephant flows

Elephant Flow Detection & Visibility

Connections with Application Details Table View of Connection Events

Jump to...

	<input type="checkbox"/>	↓ First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code	Application Protocol	Client	Web Application	URL	URL Category	URL Reputation
▼	<input type="checkbox"/>	2023-05-24 13:28:35		Allow	Elephant Flow	30.23.2.7	USA	20.23.1.102	NLD	LAN-ZONE		1049 / tcp	443 (https) / tcp	HTTP	Web browser	WebEx	http://index.html		
▼	<input type="checkbox"/>	2023-05-24 13:28:22		Allow	Elephant Flow	30.23.2.20	USA	20.23.1.107	NLD	LAN-ZONE		1048 / tcp	443 (https) / tcp	HTTP	Web browser	WebEx	http://index.html		
▼	<input type="checkbox"/>	2023-05-24 13:27:50		Allow	Elephant Flow	30.23.2.8	USA	20.23.1.103	NLD	LAN-ZONE		1049 / tcp	443 (https) / tcp	HTTP	Web browser	WebEx	http://index.html		
▼	<input type="checkbox"/>	2023-05-24 13:27:44		Allow	Elephant Flow	30.23.2.19	USA	20.23.1.107	NLD	LAN-ZONE		1049 / tcp	443 (https) / tcp	HTTP	Web browser	WebEx	http://index.html		
▼	<input type="checkbox"/>	2023-05-24 13:27:29		Allow	Elephant Flow	30.23.2.14	USA	20.23.1.105	NLD	LAN-ZONE		1050 / tcp	443 (https) / tcp	HTTP	Web browser	WebEx	http://index.html		
▼	<input type="checkbox"/>	2023-05-24 13:27:20		Allow	Elephant Flow	30.23.2.19	USA	20.23.1.107	NLD	LAN-ZONE		1048 / tcp	443 (https) / tcp	HTTP	Web browser	WebEx	http://index.html		
▼	<input type="checkbox"/>	2023-05-24 13:27:09		Allow	Elephant Flow	30.23.2.7	USA	20.23.1.102	NLD	LAN-ZONE		1048 / tcp	443 (https) / tcp	HTTP	Web browser	WebEx	http://index.html		
▼	<input type="checkbox"/>	2023-05-24 13:27:09		Allow	Elephant Flow	30.23.2.20	USA	20.23.1.107	NLD	LAN-ZONE		1047 / tcp	443 (https) / tcp	HTTP	Web browser	WebEx	http://index.html		
▼	<input type="checkbox"/>	2023-05-24 13:27:05		Allow	Elephant Flow	30.23.2.24	USA	20.23.1.109	NLD	LAN-ZONE		1049 / tcp	443 (https) / tcp	HTTP	Web browser	WebEx	http://index.html		
▼	<input type="checkbox"/>	2023-05-24 13:27:03		Allow	Elephant Flow	30.23.2.3	USA	20.23.1.101	NLD	LAN-ZONE		1048 / tcp	443 (https) / tcp	HTTP	Web browser	WebEx	http://index.html		
▼	<input type="checkbox"/>	2023-05-24 13:26:55		Allow	Elephant Flow	30.23.2.11	USA	20.23.1.104	NLD	LAN-ZONE		1047 / tcp	443 (https) / tcp	HTTP	Web browser	WebEx	http://index.html		
▼	<input type="checkbox"/>	2023-05-24 13:26:33		Allow	Elephant Flow	30.23.2.10	USA	20.23.1.103	NLD	LAN-ZONE		1047 / tcp	443 (https) / tcp	HTTP	Web browser	WebEx	http://index.html		
▼	<input type="checkbox"/>	2023-05-24 13:26:33		Allow	Elephant Flow	30.23.2.4	USA	20.23.1.101	NLD	LAN-ZONE		1049 / tcp	443 (https) / tcp	HTTP	Web browser	WebEx	http://index.html		
▼	<input type="checkbox"/>	2023-05-24 13:26:28		Allow	Elephant Flow	30.23.2.5	USA	20.23.1.101	NLD	LAN-ZONE		1048 / tcp	443 (https) / tcp	HTTP	Web browser	WebEx	http://index.html		
▼	<input type="checkbox"/>	2023-05-24 13:25:59		Allow	Elephant Flow	30.23.2.22	USA	20.23.1.108	NLD	LAN-ZONE		1047 / tcp	443 (https) / tcp	HTTP	Web browser	WebEx	http://index.html		
▼	<input type="checkbox"/>	2023-05-24 13:25:35		Allow	Elephant Flow	30.23.2.1	USA	20.23.1.100	NLD	LAN-ZONE		1046 / tcp	443 (https) / tcp	HTTP	Web browser	WebEx	http://index.html		
▼	<input type="checkbox"/>	2023-05-24 13:24:53		Allow	Elephant Flow	30.23.2.25	USA	20.23.1.109	NLD	LAN-ZONE		1048 / tcp	443 (https) / tcp	HTTP	Web browser	WebEx	http://index.html		
▼	<input type="checkbox"/>	2023-05-24 13:24:02		Allow	Elephant Flow	30.23.2.15	USA	20.23.1.105	NLD	LAN-ZONE		1048 / tcp	443 (https) / tcp	HTTP	Web browser	WebEx	http://index.html		
▼	<input type="checkbox"/>	2023-05-24 13:23:46		Allow	Elephant Flow	30.23.2.13	USA	20.23.1.104	NLD	LAN-ZONE		1046 / tcp	443 (https) / tcp	HTTP	Web browser	WebEx	http://index.html		
▼	<input type="checkbox"/>	2023-05-24 13:23:46		Allow	Elephant Flow	30.23.2.19	USA	20.23.1.107	NLD	LAN-ZONE		1047 / tcp	443 (https) / tcp	HTTP	Web browser	WebEx	http://index.html		
▼	<input type="checkbox"/>	2023-05-24 13:23:09		Allow	Elephant Flow	30.23.2.23	USA	20.23.1.108	NLD	LAN-ZONE		1048 / tcp	443 (https) / tcp	HTTP	Web browser	WebEx	http://index.html		
▼	<input type="checkbox"/>	2023-05-24 13:23:03		Allow	Elephant Flow	30.23.2.5	USA	20.23.1.101	NLD	LAN-ZONE		1047 / tcp	443 (https) / tcp	HTTP	Web browser	WebEx	http://index.html		
▼	<input type="checkbox"/>	2023-05-24 13:22:56		Allow	Elephant Flow	30.23.2.23	USA	20.23.1.109	NLD	LAN-ZONE		1047 / tcp	443 (https) / tcp	HTTP	Web browser	WebEx	http://index.html		
▼	<input type="checkbox"/>	2023-05-24 13:22:41		Allow	Elephant Flow	30.23.2.5	USA	20.23.1.101	NLD	LAN-ZONE		1046 / tcp	443 (https) / tcp	HTTP	Web browser	WebEx	http://index.html		

Application causing elephant flow is shown

Elephant Flow Detection & Visibility

The screenshot shows the Cisco Firewall Management Center (FMC) interface. The main view is the 'Advanced Settings' for a policy named 'Health Care-DEN Policy'. The 'Advanced Deploy' modal is open, showing a list of applications. The application 'den-ftd-ha.chc.com' is selected, and a blue arrow points from this application to a callout box on the right that says 'Make changes & Deploy'.

Application	Status
<input type="checkbox"/> DC-CORE-NGFW-CLUSTER-BGL-1	Ready for Deployment
<input checked="" type="checkbox"/> den-ftd-ha.chc.com	Ready for Deployment

1 selected | 2 pending

Make changes & Deploy

VPN Network Insights

Unveiling Comprehensive Details
and In-Depth Analysis



VPN Network Insights

Network Administrator NIK's Journey into

- Enhanced Monitoring and Mitigation: Real-time RAVPN Dashboard for Active VPN Sessions and Certificate Management to ensure reliable and secure remote connectivity
- Enhanced Site to Site VPN Monitoring and Troubleshooting with Cisco FMC to manage his multinational company which operates multiple branch offices across different locations.

NIK's Effective RAVPN Management with FMC



Visibility for Security



Visibility for planning your Business needs



Visibility for Troubleshooting



Visibility for proactive Mitigation

RAVPN Monitoring Dashboard – Session View

Firewall Management Center
Overview / Dashboards / Remote Access VPN

Overview Analysis Policies Devices Objects Integration

Deploy 🔍 ⚙️ 👤 admin 🔒 **SECURE**

Refresh every 5 minutes Refresh

Sessions

Select Type: By Device

202 Total Sessions

- CSF-USA (52 / 250)
- CSF-IND (50 / 250)
- CSF-JAPAN (50 / 250)
- CSF-AUS (50 / 250)

Active Sessions

Sessions Legend:
Less than 10
10 to 100
100 to 1000
1000 to 10000

Device Identity Certificates

6 Identity Certificates

- 1 certificate expiring in 1 to 30 days
- 1 certificate is expired

[View Details](#)

Active Sessions (202)

User Name	Assigned IP	Public IP	Login Time	Gateway	Client Application	Client OS	Connection Profile	Group Policy	Actions
user510	192.168.52.150	202.12.101.11	2022-08-05 10:...	CSF-IND		win	VPN-IND	IND-USERS	...
user514	192.168.52.151	202.12.101.15	2022-08-05 10:...	CSF-IND		win	VPN-IND	IND-USERS	...
user513	192.168.52.202	202.12.101.14	2022-08-05 10:...	CSF-IND		win	VPN-IND	IND-USERS	...
user54	192.168.52.203	202.12.101.5	2022-08-05 10:...	CSF-IND		win	VPN-IND	IND-USERS	...
user53	192.168.52.204	202.12.101.4	2022-08-05 10:...	CSF-IND		win	VPN-IND	IND-USERS	...
user539	192.168.52.205	202.12.101.40	2022-08-05 10:...	CSF-IND		win	VPN-IND	IND-USERS	...
user522	192.168.52.206	202.12.101.23	2022-08-05 10:...	CSF-IND		win	VPN-IND	IND-USERS	...

Sessions by Device view

RAVPN Monitoring Dashboard – Global View

Firewall Management Center
Overview / Dashboards / Remote Access VPN

Overview
Analysis
Policies
Devices
Objects
Integration

Deploy
Q
⚙️
🔔
admin ▾

Refresh every 5 minutes ⏸ Refresh

Sessions

Select Type
By Connection Profile

202
Total
Sessions

- VPN-USA (52)
- VPN-IND (50)
- VPN-JAPAN (50)
- VPN-AUS (50)

Active Sessions

+ - Reset

100 to 1000

 1000 to 10000

Active
Sessions by
Geo

Device Identity Certificates

6 Identity Certificates

- ▲ 1 certificate expiring in 1 to 30 days
- 1 certificate is expired

[View Details](#)

Active Sessions (202)

Select...

User Name	Assigned IP	Public IP	Login Time	Gateway	Client Application	Client OS	Connection Profile	Group Policy	Actions
user510	192.168.52.150	202.12.101.11	2022-08-05 10:...	CSF-IND		win	VPN-IND	IND-USERS	...
user514	192.168.52.151	202.12.101.15	2022-08-05 10:...	CSF-IND		win	VPN-IND	IND-USERS	...
user513	192.168.52.202	202.12.101.14	2022-08-05 10:...	CSF-IND		win	VPN-IND	IND-USERS	...
user54	192.168.52.203	202.12.101.5	2022-08-05 10:...	CSF-IND		win	VPN-IND	IND-USERS	...
user53	192.168.52.204	202.12.101.4	2022-08-05 10:...	CSF-IND		win	VPN-IND	IND-USERS	...
user539	192.168.52.205	202.12.101.40	2022-08-05 10:...	CSF-IND		win	VPN-IND	IND-USERS	...
user522	192.168.52.206	202.12.101.23	2022-08-05 10:...	CSF-IND		win	VPN-IND	IND-USERS	...

RAVPN Monitoring Dashboard – Device Identity Certificate

Firewall Management Center
Overview / Dashboards / Remote Access VPN

Overview Analysis Policies Devices Objects Integration

Deploy 🔍 ⚙️ 👤 admin | Cisco **SECURE**

Refresh every 5 minutes Refresh

Sessions

Select Type: By Device

202 Total Sessions

- CSF-USA (52 / 250)
- CSF-IND (50 / 250)
- CSF-JAPAN (50 / 250)
- CSF-AUS (50 / 250)

Active Sessions

Sessions Legend:
Less than 10
10 to 100
100 to 1000
1000 to 10000

Device Identity Certificates

6 Identity Certificates

- ⚠️ 1 certificate expiring in 1 to 30 days
- 🔴 1 certificate is expired

[View Details](#)

Active Sessions (202)

User Name	As...
user510	192.168.52.203	202.12.101.5	2022-08-05 10:...	CSF-IND		win	VPN-IND	IND-USERS	...
user514	192.168.52.151	202.12.101.15	2022-08-05 10:...	CSF-IND		win	VPN-IND	IND-USERS	...
user513	192.168.52.202	202.12.101.14	2022-08-05 10:...	CSF-IND		win	VPN-IND	IND-USERS	...
user54	192.168.52.203	202.12.101.5	2022-08-05 10:...	CSF-IND		win	VPN-IND	IND-USERS	...
user53	192.168.52.204	202.12.101.4	2022-08-05 10:...	CSF-IND		win	VPN-IND	IND-USERS	...
user539	192.168.52.205	202.12.101.40	2022-08-05 10:...	CSF-IND		win	VPN-IND	IND-USERS	...
user522	192.168.52.206	202.12.101.23	2022-08-05 10:...	CSF-IND		win	VPN-IND	IND-USERS	...

Device Identity Certificate which have expired & about to expire

RAVPN Monitoring Dashboard – Terminate Session

Firewall Management Center
Overview / Dashboards / Remote Access VPN

Overview Analysis Policies Devices Objects Integration

Deploy 🔍 ⚙️ 👤 admin 🔒 Cisco SECURE

Refresh every 5 minutes Refresh

Sessions

Select Type: By Device

202 Total Sessions

- CSF-USA (52 / 250)
- CSF-IND (50 / 250)
- CSF-JAPAN (50 / 250)
- CSF-AUS (50 / 250)

Active Sessions

Device Identity Certificates

6 Identity Certificates

- 1 certificate expiring in 1 to 30 days
- 1 certificate is expired

View Details

Active Sessions (202)

User Name	Assigned IP	Public IP	Login Time	Gateway	Client Application	Client OS	Connection Profile	Group Policy	Actions
user992	192.168.55.69	202.12.1.115	2022-08-05 10:...	CSF-USA	Cisco AnyConne	win	VPN-USA	USA-USERS	⋮
user991	192.168.55.68	202.12.1.105	2022-08-05 11:...	CSF-USA	Cisco AnyConne	linux-64			
user89	192.168.53.59	202.12.27.7	2022-08-05 10:...	CSF-JAPAN					
user88	192.168.53.65	202.12.27.9	2022-08-05 10:...	CSF-JAPAN					
user87	192.168.53.101	202.12.27.8	2022-08-05 10:...	CSF-JAPAN					
user86	192.168.53.58	202.12.27.7	2022-08-05 10:...	CSF-JAPAN					
user850	192.168.53.100	202.12.27.51	2022-08-05 10:...	CSF-JAPAN					

Terminate Session

- Terminate session
- Terminate all sessions of user992, on gateway CSF-USA
- Terminate all sessions on gateway CSF-USA

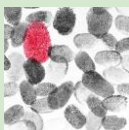
NIK's Effective S2S VPN Management with FMC



Monitor VPN Tunnel Status:

Ensure the continuous and smooth operation of VPN tunnels.

Detect and address any potential disruptions or issues promptly.



Analyze VPN Traffic Flow:

Gain insights into the data traversing through VPN tunnels.

Optimize bandwidth allocation and identify any suspicious activities.

S2S VPN Monitoring Dashboard

Firewall Management Center
Overview / Dashboards / Site to Site VPN

Overview Analysis Policies Devices Objects Integration

Deploy 🔍 ⚙️ ⓘ Nik 🔒 Cisco SECURE

Select... [X] Refresh Refresh every 5 minutes

Node A	Node B	Topology	Status	Last Updated
Hub-SINGAPORE (VPN IP: 121.1.1.254)	Spoke-2-JAPAN (VPN IP: 121.1.1.2)	hub-spoke	Active	2023-05-23 02:24:59
Hub-SINGAPORE (VPN IP: 120.1.1.1)	Spoke-0-INDIA (VPN IP: 120.1.1.2)	s2s_crypto_map	Active	2023-05-24 01:13:20

100% Active
2 connections

Topology

Name	🔴	🟡	🟢
hub-spoke	0	0	1
s2s_crypto_map	0	0	1

Connections View

Viewing 1-2 of 2

S2S VPN Monitoring Dashboard – Tunnel Information


Firewall Management Center
Overview / Dashboards / Site to Site VPN

Overview Analysis Policies Devices Objects Integration

Deploy 🔍 ⚙️ ? Nik ▾ CISCO SECURE



Select... Refresh Refresh every 5 minutes

Tunnel Summary



100% Active
2 connections

Name	🔴	🟡	🟢
hub-spoke	0	0	1
s2s_crypto_map	0	0	1

Node A	Node B	Topology	Status	Last Updated
 Hub-SINGAPORE (VPN IP: 121.1.1.254)	Spoke-2-JAPAN (VPN IP: 121.1.1.2)	hub-spoke	🟢 Active	2023-05-23 02:24:59
 View full information SINGAPORE (VPN IP: 120.1.1.1)	Spoke-0-INDIA (VPN IP: 120.1.1.2)	s2s_crypto_map	🟢 Active	2023-05-24 01:13:20

View full tunnel details by clicking on the eye icon

Viewing 1-2 of 2

S2S VPN Monitoring Dashboard – General Details

Firewall Management Center
Overview / Dashboards / Site to Site VPN

Overview Analysis Policies Devices Objects Integration Deploy Search Settings Help Nik Cisco SECURE

Select... Refresh Refresh every 5 minutes

Node A	Node B	Topology	Status	Last Updated
Hub-SINGAPORE (VPN IP: 121.1.1.254)	Spoke-2-JAPAN (VPN IP: 121.1.1.2)	hub-spoke	Active	2023-05-23 02:24:59
Hub-SINGAPORE (VPN IP: 120.1.1.1)	Spoke-0-INDIA (VPN IP: 120.1.1.2)	s2s_crypto_map	Active	2023-05-24 01:13:20

Complete tunnel details under General Tab

A: Hub-SINGAPORE ↔ B: Spoke-2-JAPAN
Topology: hub-spoke | Status: Active

General CLI Details Packet Tracer

Topology: hub-spoke
Status: Active
Node A: Hub-SINGAPORE
Node B: Spoke-2-JAPAN
Node A IP: 121.1.1.254
Node B IP: 121.1.1.2
Node A VPN Interface Name: int1
Node B VPN Interface Name: int0
Last Updated: 2023-05-23 02:24:59

Automatic refresh is turned off. Dismiss all

Viewing 1-2 of 2

S2S VPN Monitoring Dashboard – CLI Details

Firewall Management Center
Overview / Dashboards / Site to Site VPN

Overview Analysis Policies Devices Objects Integration Deploy 🔍 ⚙️ 🔄 Nik 🏠 cisco SECURE

Select... Refresh Refresh every 5 minutes

Node A	Node B	Topology	Status	Last Updated
Hub-SINGAPORE (VPN IP: 121.1.1.254)	Spoke-2-JAPAN (VPN IP: 121.1.1.2)	hub-spoke	Active	2023-05-23 02:24:59
Hub-SINGAPORE (VPN IP: 120.1.1.1)	Spoke-0-INDIA (VPN IP: 120.1.1.2)	s2s_crypto_map	Active	2023-05-24 01:13:20

CLI details like show crypto ipsec can be seen here

A: Hub-SINGAPORE ↔ B: Spoke-2-JAPAN
Topology: hub-spoke | Status: Active

General CLI Details Packet Tracer

Refresh Maximize view

Summary

Node A (121.1.1.254/500)	Node B (121.1.1.2/500)
Transmitted: 201.36 KB (206197 B)	Transmitted: 206.35 KB (211298 B)
Received: 266.45 KB (272848 B)	Received: 262.38 KB (268672 B)

Ipssec Security Associations (1)

0.0.0.0/0.0.0.0/0	0.0.0.0/0.0.0.0/0
-------------------	-------------------

Hub-SINGAPORE (VPN Interface IP: 121.1.1.254)

```
show crypto ipsec sa peer 121.1.1.2
peer address: 121.1.1.2
interface: int0_dynamic_vti_1_va4
Crypto map tag: int0_dynamic_vti_1_vtemplate_dyn_map, seq n

Protected vrf (ivrf): Global
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
current_peer: 121.1.1.2
```

Spoke-2-JAPAN (VPN Interface IP: 121.1.1.2)

```
show crypto ipsec sa peer 121.1.1.254
show vpn-sessiondb detail l2l filter ipaddress 121.1.1.1...
```

Automatic refresh is turned off. Dismiss all

Viewing 1-2 of 2

S2S VPN Monitoring Dashboard – Packet Tracer

Firewall Management Center
Overview / Dashboards / Site to Site VPN

Overview Analysis Policies Devices Objects Integration Deploy 🔍 ⚙️ ? Nik ▾ Cisco **SECURE**

Select... Refresh Refresh every 5 minutes

Node A	Node B	Topology	Status	Last Updated
Hub-SINGAPORE (VPN IP: 121.1.1.254)	Spoke-2-JAPAN (VPN IP: 121.1.1.2)	hub-spoke	Active	2023-05-23 02:24:59
Hub-SINGAPORE (VPN IP: 120.1.1.1)	Spoke-0-INDIA (VPN IP: 120.1.1.2)	s2s_crypto_map	Active	2023-05-24 01:13:20

Packet tracer available

A: Hub-SINGAPORE ↔ B: Spoke-2-JAPAN

Topology: hub-spoke | Status: Active

General CLI Details **Packet Tracer**

SELECT TRACE

See Trace Config

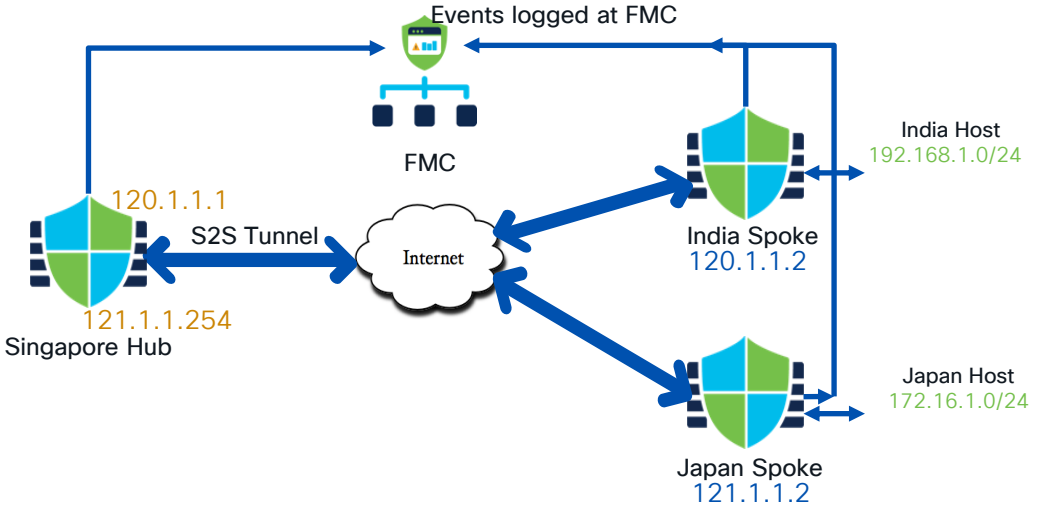
Node A Traces	Node B Traces
✓ → Allow A: In → Out	Not Traced B (Decrypted): Out → In
Not Traced A (Decrypted): In → Out	✓ ← Allow B: Out → In

Viewing 1-2 of 2

Enhancing VPN Security

Advanced Traffic Flow Analysis

Hub and Spoke topology



India Host 192.168.1.2 --- India Spoke 120.1.1.2 --- Singapore Hub 121.1.1.254 --- Japan Spoke 121.1.1.2 --- Japan Host 172.16.1.2

Encrypt Decrypt Encrypt Decrypt

S2S VPN Monitoring Dashboard – Unified Viewer

Firewall Management Center
Analysis / Unified Events

Overview Analysis Policies Devices Objects Integration

Deploy 🔍 ⚙️ 📄 Nik 🔒 cisco SECURE

Search...

Showing all 10 events (📄 10) ⌵

📅 2023-05-24 00:32:34 EDT → 2023-05-24 01:32:34 EDT 1h 🔄 Go Live

Time	Event Type	Action	Reason	Source IP	Destination IP	Source Port / ICMP Type	Destination Port / ICMP Code	...
2023-05-24 01:32:23	🔗 Connection	🟢 Allow		192.168.1.2	172.16.1.2	8 (Echo Reques...	0 (No Co	...
2023-05-24 01:32:21	🔗 Connection	🟢 Allow		172.16.1.2	192.168.1.2	8 (Echo Reques...	0 (No Co	...
2023-05-24 01:29:15	🔗 Connection	🟢 Allow		192.168.1.2	172.16.1.2	8 (Echo Reques...	0 (No Co	...
2023-05-24 01:29:15	🔗 Connection	🟢 Allow		192.168.1.2	172.16.1.2	8 (Echo Reques...	0 (No Co	...
2023-05-24 01:29:13	🔗 Connection	🟢 Allow		192.168.1.2	172.16.1.2	8 (Echo Reques...	0 (No Co	...
2023-05-24 01:29:11	🔗 Connection	🟢 Allow		172.16.1.2	192.168.1.2	8 (Echo Reques...	0 (No Co	...
2023-05-24 01:29:09	🔗 Connection	🟢 Allow		172.16.1.2	192.168.1.2	8 (Echo Reques...	0 (No Co	...
2023-05-24 01:12:02	🔗 Connection	🟢 Allow		192.168.1.2	172.16.1.2	51136 / tcp	22 (ssh)	...
2023-05-24 01:12:02	🔗 Connection	🟢 Allow		192.168.1.2	172.16.1.2	51136 / tcp	22 (ssh) / tcp	...
2023-05-24 01:12:02	🔗 Connection	🟢 Allow		192.168.1.2	172.16.1.2	51136 / tcp	22 (ssh) / tcp	...

Column set

VPN

Deselect 1 filtered · Select default

VPN Action

Revert 8 selected Apply

Select Encrypt Peer, Decrypt Peer and VPN Action

S2S VPN Monitoring Dashboard – Unified Viewer

Firewall Management Center
Analysis / Unified Events

Overview Analysis Policies Devices Objects Integration

Deploy 🔍 ⚙️ ⓘ Nik ▾ SECURE

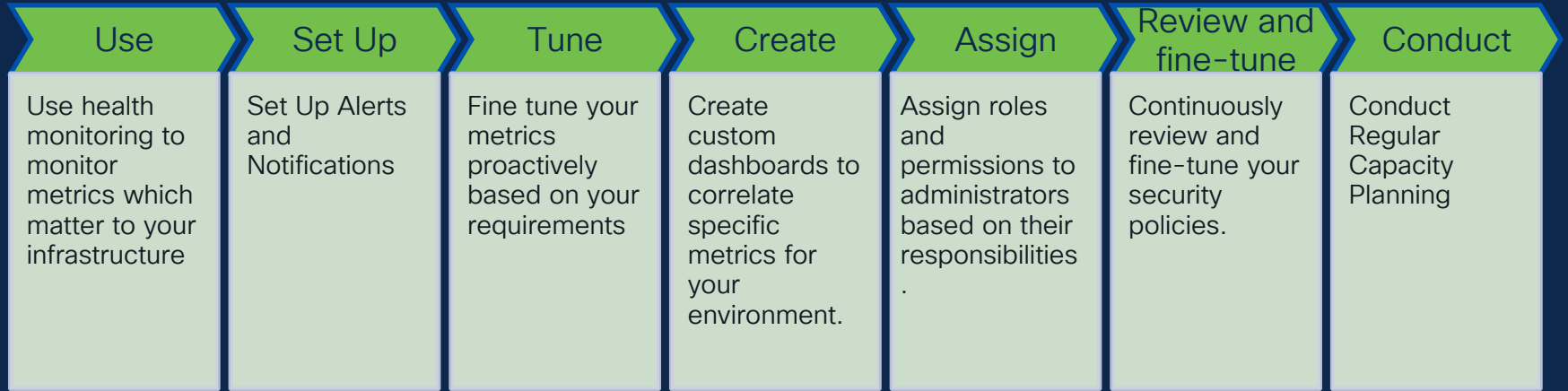
🔍 Search... ☆ × Refresh

Showing 3 events (1/3) 2023-05-24 01:33:18 EDT → 2023-05-24 01:34:04 EDT 1m 16s Live

Time	Event Type	Action	Source IP	Destination IP	Device	Decrypt Peer	Encrypt Peer	VPN Action	
2023-05-24 01:34:13	🔗 Connection	➡ Allow	192.168.1.2	172.16.1.2	Spoke-0-INDIA		120.1.1.1	Encrypt	⋮
2023-05-24 01:34:12	🔗 Connection	➡ Allow	192.168.1.2	172.16.1.2	Hub-SINGAPORE	120.1.1.2	121.1.1.2	VPN Routing	⋮
2023-05-24 01:34:12	🔗 Connection	➡ Allow	192.168.1.2	172.16.1.2	Spoke-2-JAPAN	121.1.1.254		Decrypt	⋮

Complete connection log available

Best Practice Recommendations



What's in the roadmap

A futuristic soldier in a city. The soldier is wearing a dark, armored suit with glowing blue lights on the chest and helmet. The background is a hazy, futuristic cityscape with tall buildings and glowing windows. The text is overlaid on the center of the image.

CISCO SECURE FIREWALL PROTECTED BY ADVANCED HEALTH MONITORING

Fill out your session surveys!



Attendees who fill out a minimum of four session surveys and the overall event survey will get **Cisco Live-branded socks** (while supplies last)!



Attendees will also earn 100 points in the **Cisco Live Challenge** for every survey completed.



These points help you get on the leaderboard and increase your chances of winning daily and grand prizes

References

BRKSEC-2121 Help, My firewall has an issue. How to get a health alert

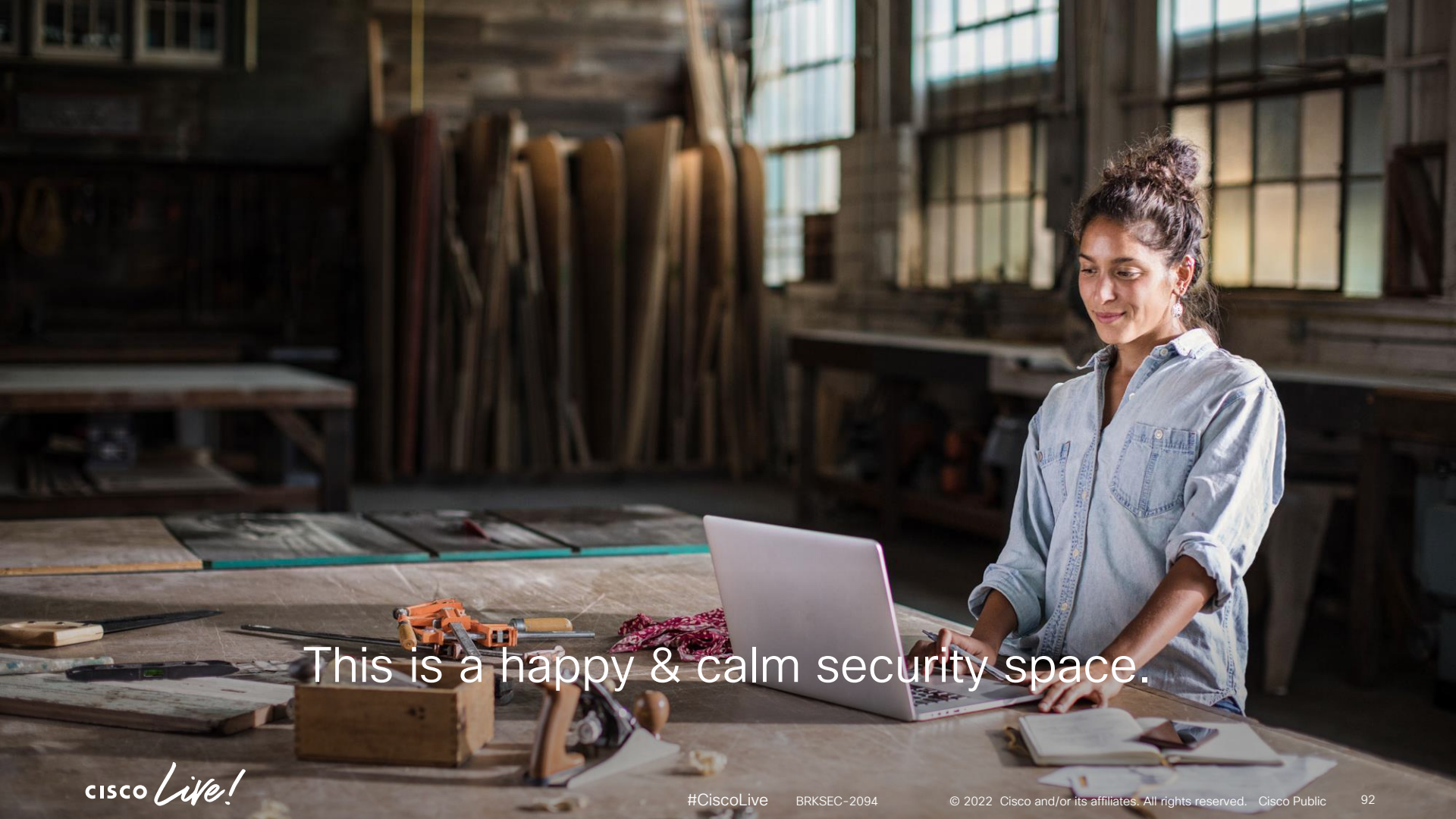
– *By Lucas Cammarata*

Wednesday, Jun 7 | 2:30 PM to 3:30 PM
PDT

Continue your education

CISCO *Live!*

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand



This is a happy & calm security space.

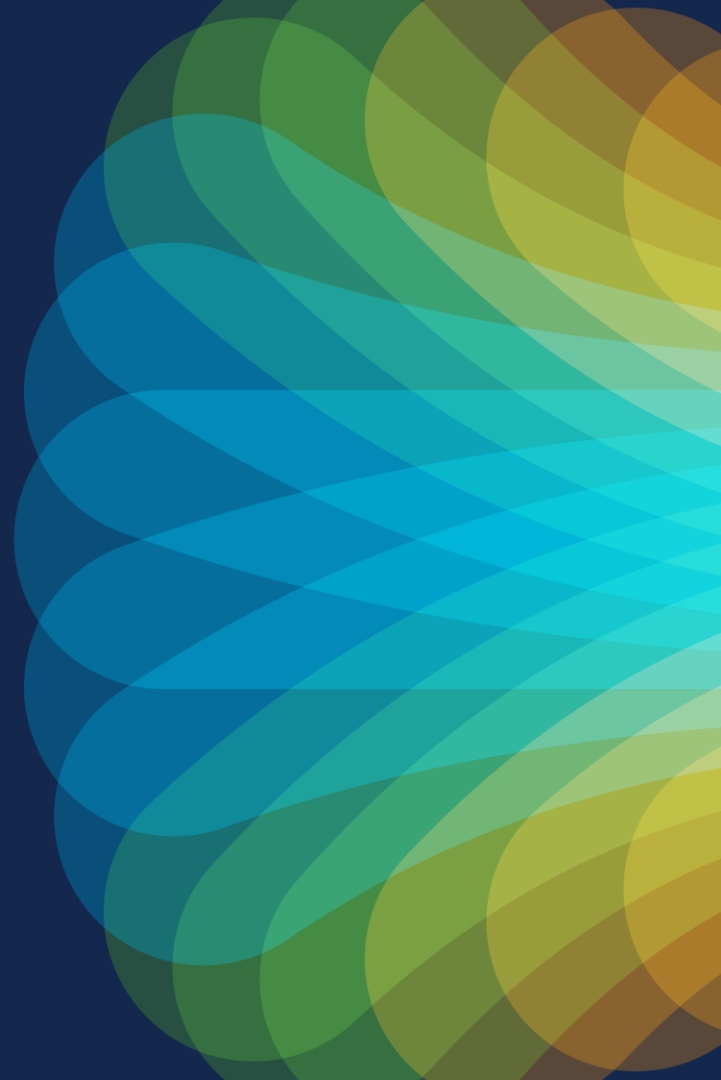


The bridge to possible

Thank you

CISCO *Live!*

#CiscoLive



CISCO *Live!*

Let's go

#CiscoLive

Cisco Live Challenge

Gamify your Cisco Live experience!
Get points for attending this session!

How:

- 1 Open the Cisco Events App.
- 2 Click on 'Cisco Live Challenge' in the side menu.
- 3 Click on View Your Badges at the top.
- 4 Click the + at the bottom of the screen and scan the QR code:

