Cisco Support Community

Expert Series Webcast

Performance Troubleshooting on Firepower

Aastha Bhardwaj, CCIE Security

John Bennion

April 27, 2016

Upcoming Events Cisco Support Community Expert Series Webcast

Catalyst 2960-X and 2960-XR Switches Overview, Configuration, and Troubleshooting

Register here :
https://supportforums.cisco.com/event/12982566/webcast-catalyst-2960-x-and-2960-xr-switches-overview-configuration-and

Roopa R
Technical Leader

Ask the Expert Events

- Troubleshooting Crashes in the Adaptive Security Appliances (ASA) – May 2nd – May 13th

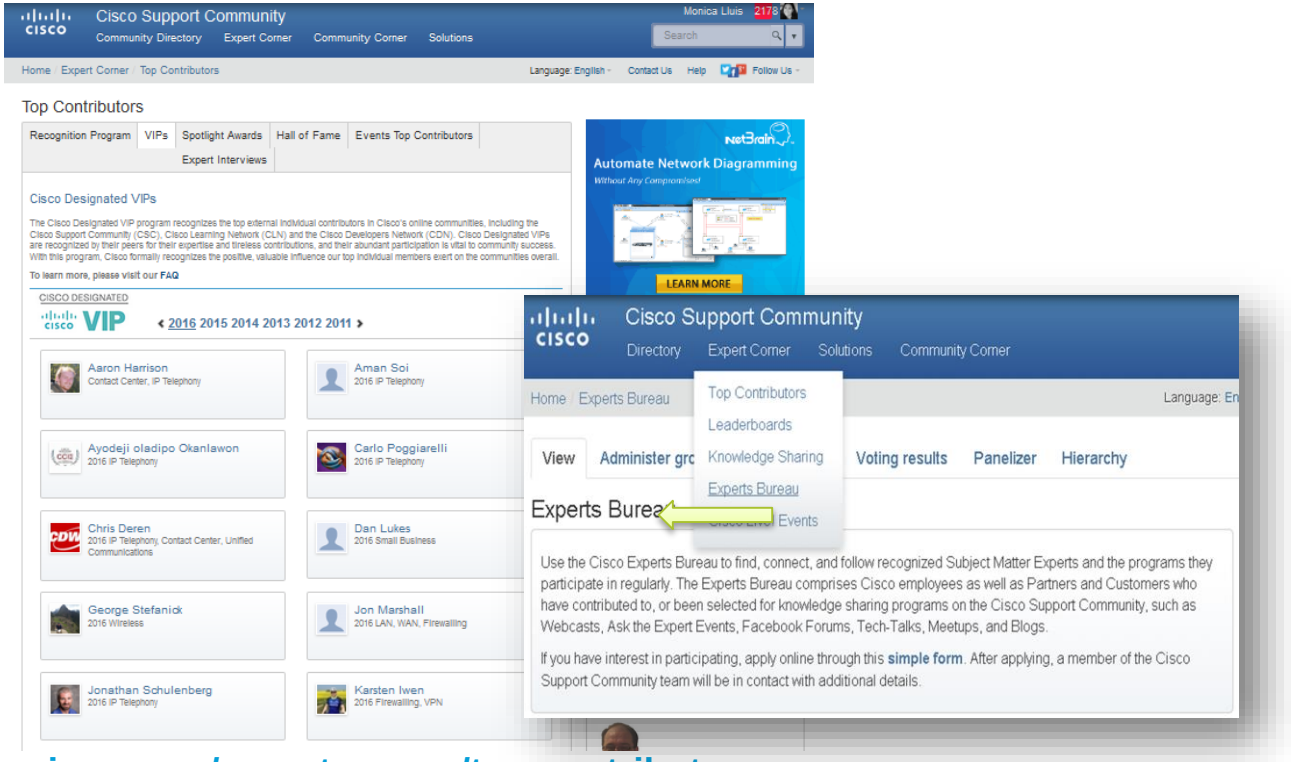
https://supportforums.cisco.com/discussion/12982461/ask-expert-troubleshooting-crashes-adaptive-security-appliances-asa

- Catalyst 2960-X and 2960-XR Switches Overview, Configuration, and Troubleshooting – May 10th – May 20th

https://supportforums.cisco.com/discussion/12982571/ask-expert-catalyst-2960-x-and-2960-xr-switches-overview-configuration-and

Become an Event Top Contributor

Participate in Live Interactive Technical Events and much more
http://bit.ly/1jlI93B



https://supportforums.cisco.com/expert-corner/top-contributors

Rate Content

Encourage and acknowledge people who generously share their time and expertise

Now your ratings on documents, videos, and blogs count give points to the authors!!!

So, when you contribute and receive ratings you now get the points in your profile.

Help us to recognize the quality content in the community and make your searches easier. Rate content in the community.

https://supportforums.cisco.com/blog/154746

Cisco Support Community Expert Series Webcast

Aastha Bhardwaj

CSE, CCIE Security #46900

John Bennion

CSE, Cisco TAC

Question Managers

Pramod Chandrashekar

Manager Engineering

Ask the Expert Event following the Webcast

Now through May 6th

https://supportforums.cisco.com/discussion/12959061/ask-expert-performance-troubleshooting-cisco-firepower

Join the discussion for these Ask The Expert Events:
http://bit.ly/events-webinar

Thank You For Joining Us Today!

If you would like a copy of the presentation slides, click the PDF file link in the chat box on the right or go to:

https://supportforums.cisco.com/document/13009016/webcast-slides-performance-troubleshooting-cisco-firepower

Submit Your Questions Now!

Use the Q & A panel to submit your questions and the panel of experts will respond.

Please take a moment to complete the survey at the end of the webcast

Cisco Support Community

Expert Series Webcast

Performance Troubleshooting on Firepower

Aastha Bhardwaj, CCIE Security

John Bennion

April 27, 2016

Agenda

- Firepower Overview
- Life of a packet
- Use-Case Scenarios
- Factors Impacting Performance
- Performance troubleshooting
- Best Practices
- QnA

Polling Question 1

How does Firepower protect your network ?

A. File inspection

B. Intrusion Prevention

C. Detection of known malicious sites

D. All of the above

Firepower Overview

Security Challenges in the Digital Economy

Maintaining Security and Compliance as business models change (Agility)

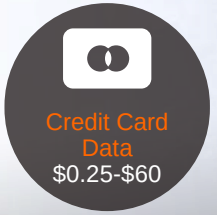
Staying ahead in a very dynamic threat landscape

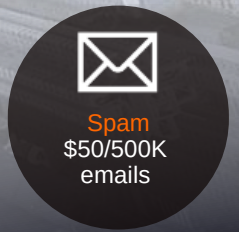
Reducing complexity and fragmentation of security solutions

Digital Disruption Drives the Hacker Economy

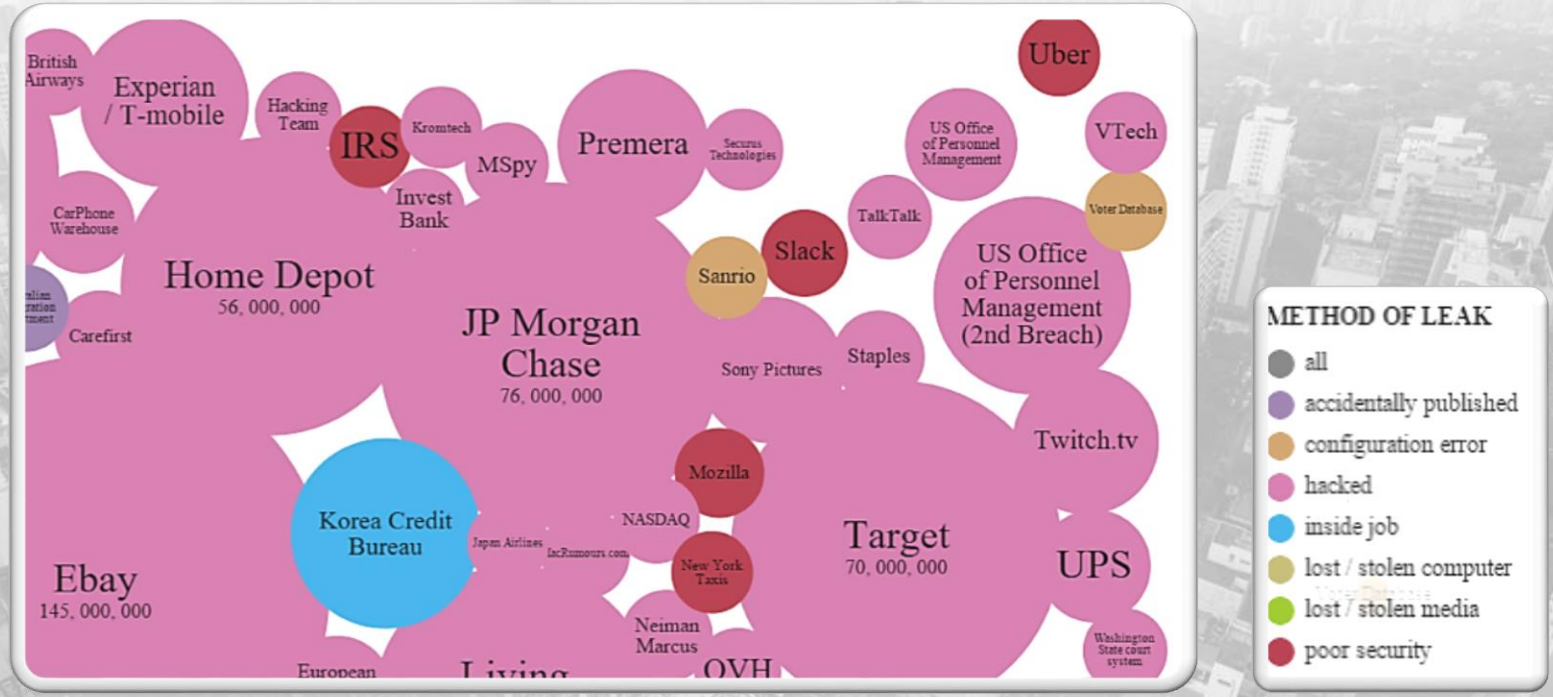
There is a multi-billion dollar global industry targeting your prized assets

$450 Billion
to
$1 Trillion



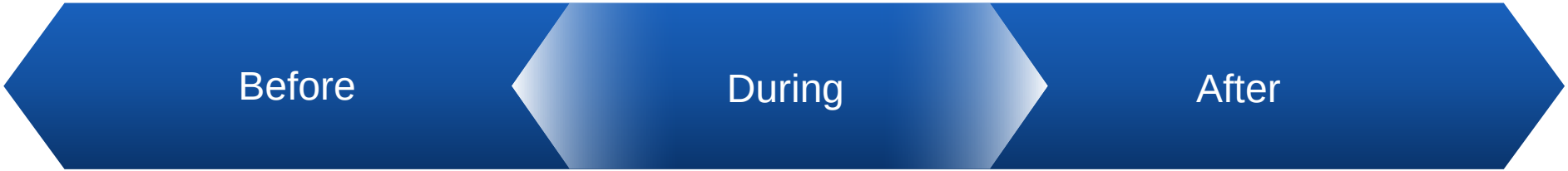


Dangerous Times: World's biggest data breaches



SECURITY EVERYWHERE

Attack Continuum




Endpoint


Branch


Edge


Campus


Data Center

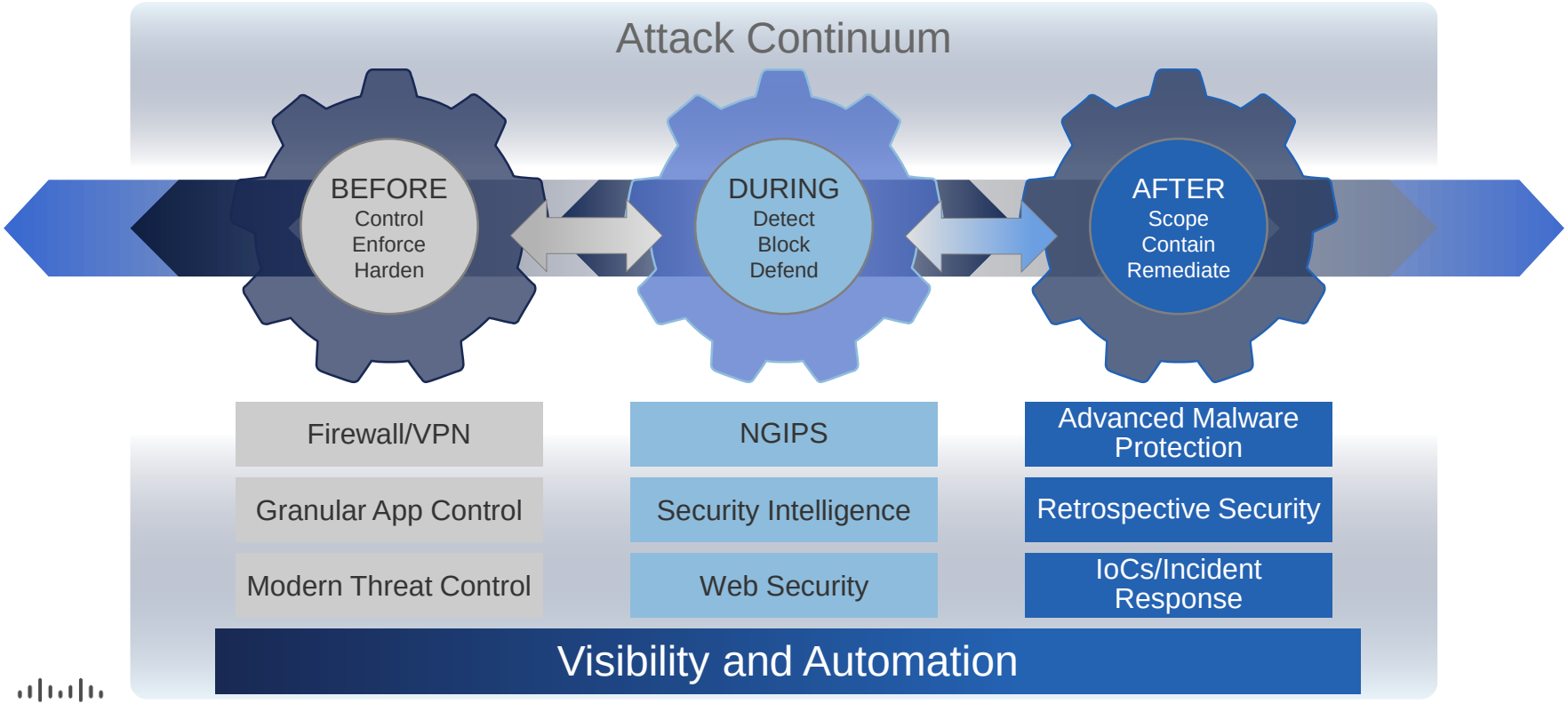

Cloud


Operational Technology


Services


The Problem with Legacy Next-Generation Firewalls

Integrated Threat Defense Across the Attack Continuum



Cisco NGFW Platforms

New Appliances

FTD on Firepower 4100 and Firepower 9300

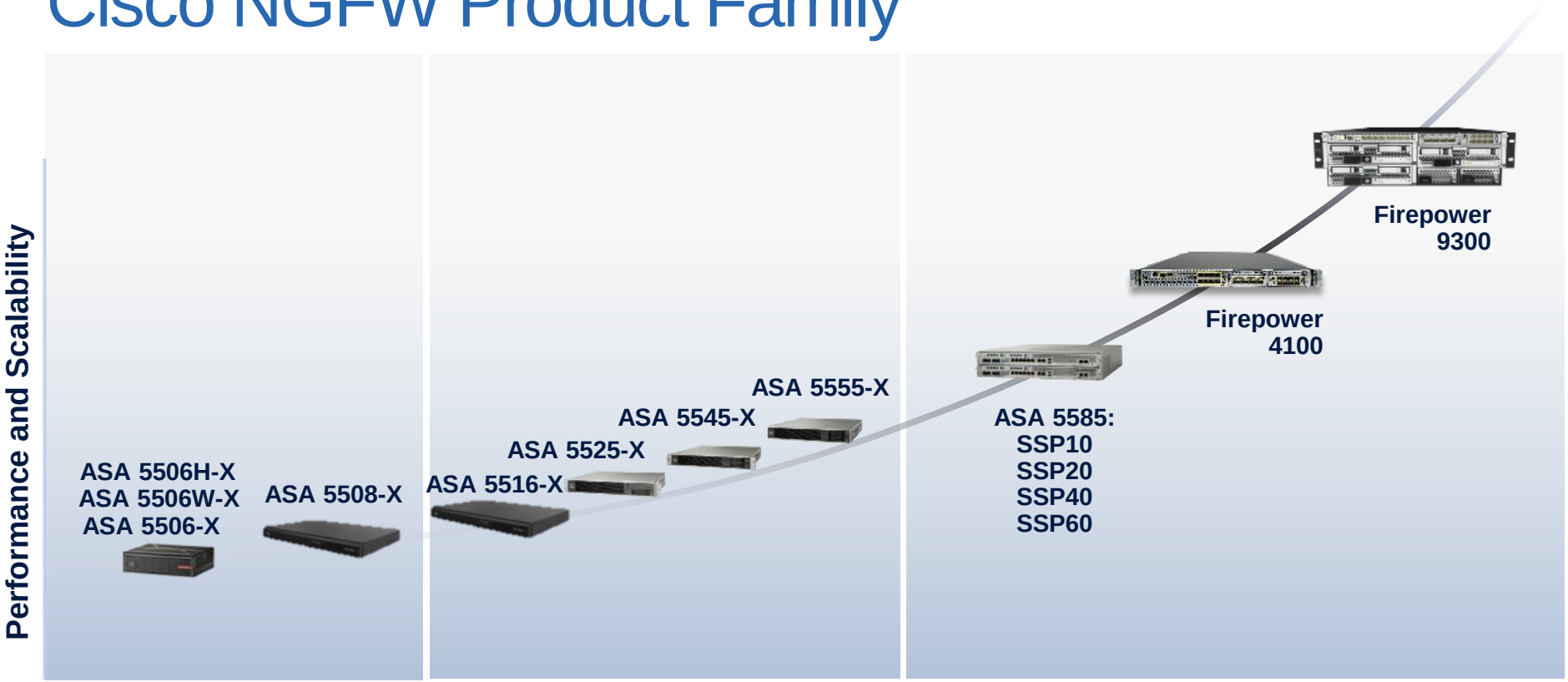
FTD or Firepower Services on ASA 5500-X*

Firepower Services on ASA 5585-X

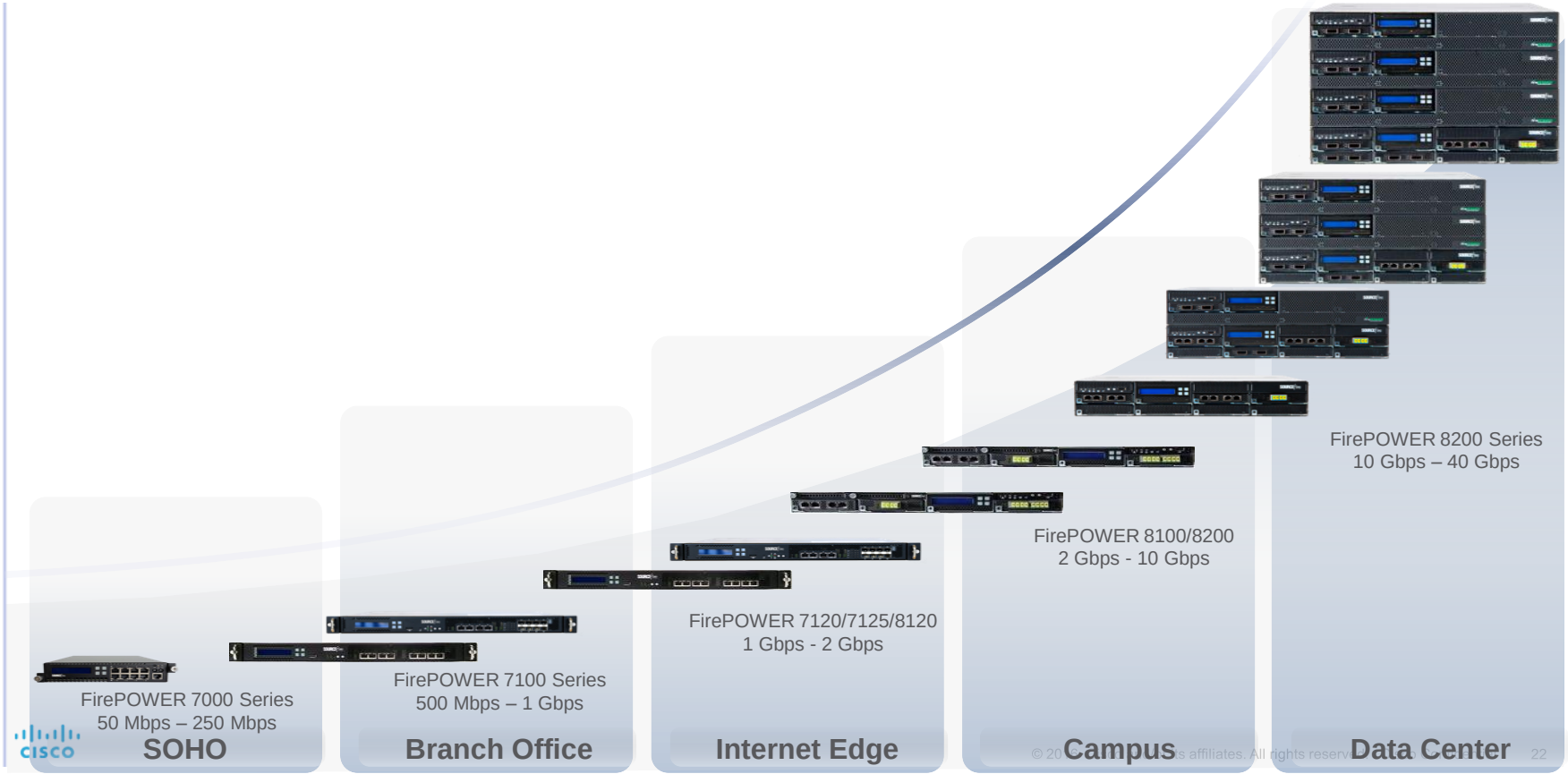
All* Managed by Firepower Management Center

*5585-X management avail 2H ’16 (pre-commit date)
*Excluding 5512-X and 5515-X due to hardware limitations

Cisco NGFW Product Family



Platforms and Places in the Network



Firepower Management Center Sizing Guidance

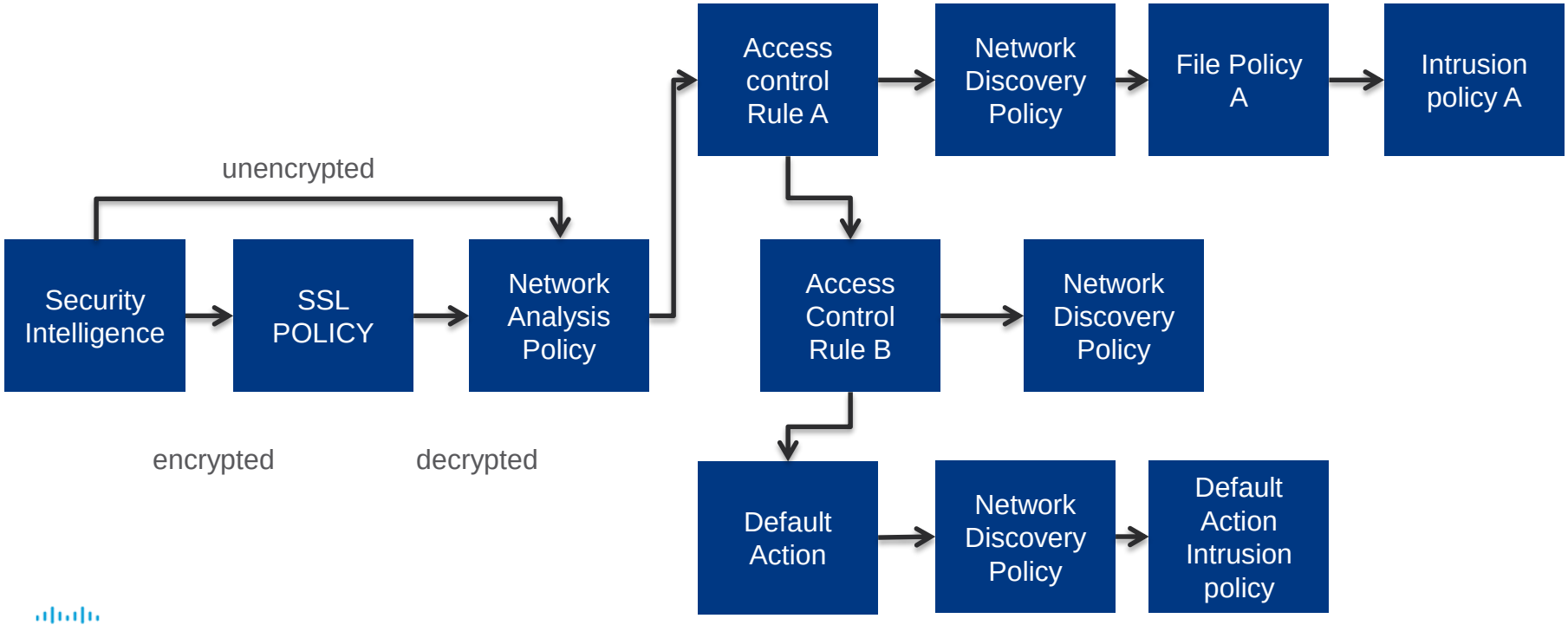
	750 FS750-K9	2000 FS2000-K9	4000 FS4000-K9	Virtual FS-VMW-SW-K9	Virtual FS-VMW-2-SW-K9 FS-VMW-10-SW-K9
Max. Devices Managed*	10	70	300	Firepower Management Center Virtual Up to 25 Managed Devices	The 2 and 10 device Virtual FMC SKUs are promotional offers for managing Firepower Services and Firepower Threat Defense only on ASA5500-X series appliances
Event Storage	100 GB	1.8TB	4.8TB		
Max. Network Map (hosts / users)	2K/2K	150K/150K	600K/600K		
Events per Sec (EPS)	2,000	12,000	20,000		

* Max number of devices is dependent upon sensor type and event rate

Firepower Threat Defense requires a Firepower Management Center appliance running software version 6.0 or higher. Most supported FireSIGHT Management Center appliances can be upgraded to software version 6.0 or higher, including the 750 (Rev 2), the 1500 (Rev 2), 2000, 3500, and 4000. The 750 (Rev 2) and 1500 (Rev 2) will require memory upgrades before upgrading the software to 6.0 or higher. Please reference the following URL for more information: http://www.cisco.com/c/en/us/support/docs/field-notices/640/fn64077.html

Life of a packet

Packet Flow



Polling Question 2

Which policy will a packet be inspected against First ?

A. SSL policy

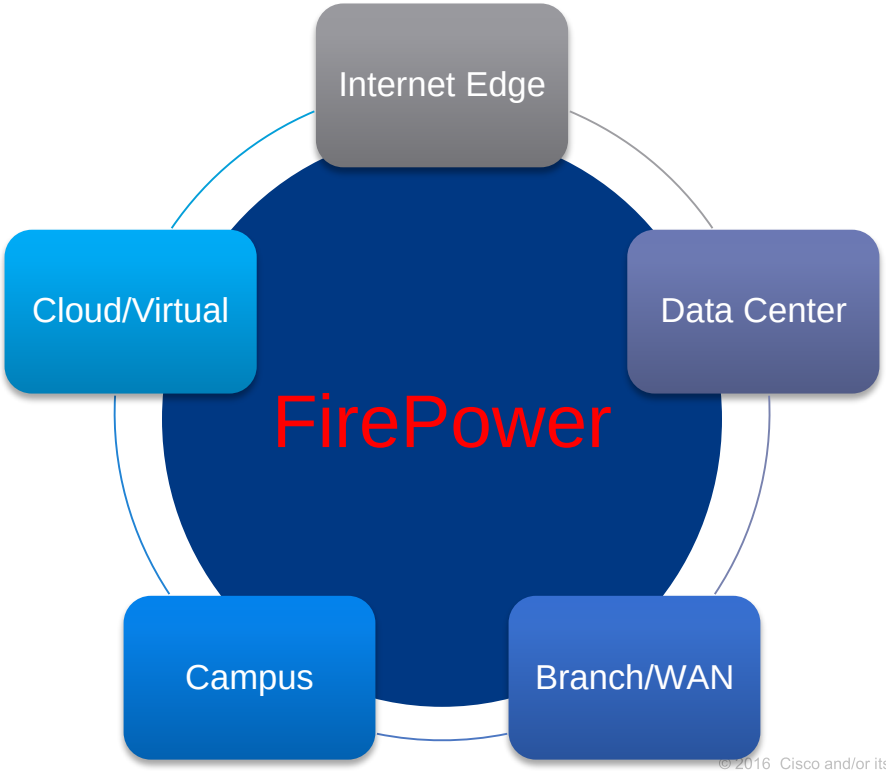
B. Intrusion policy

C. Security Intelligence policy

D. File inspection

Use-Case Scenarios

Locations



Security Features/Compliance

WWW

URL Filtering

Next-Generation
Intrusion Prevention

Advanced Malware
Protection

PCI DSS COMPLIANT

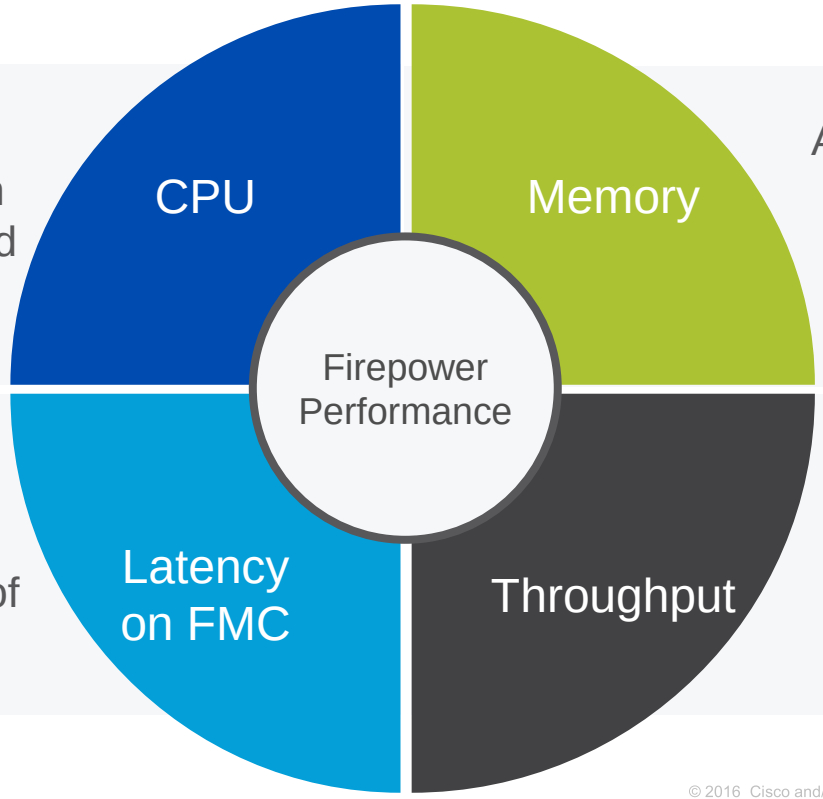
FISMA
FEDERAL INFORMATION SECURITY MANAGEMENT ACT

HIPAA

SARBANES-OXLEY ACT (SOX)
COMPLIANCE

Factors Impacting Performance

Performance Factors



- Elephant flows
- Oversubscription
- Features enabled
- Number of rules
- Packet Size

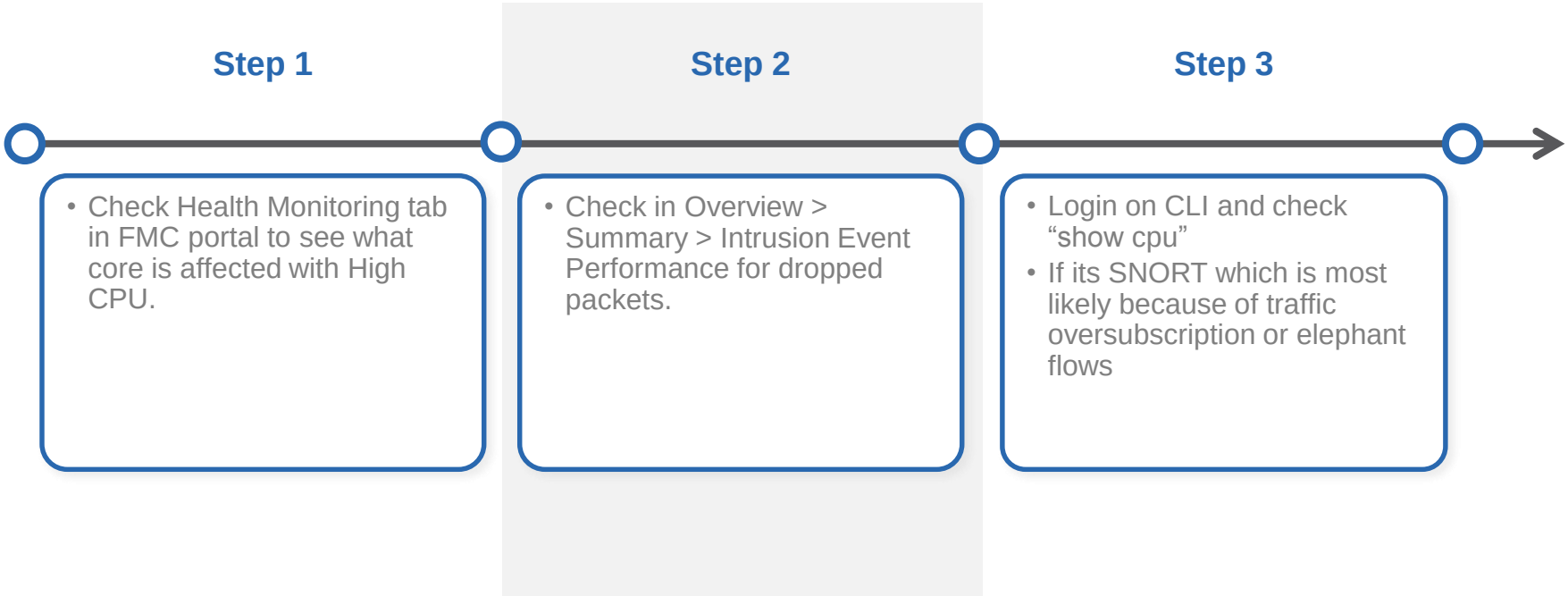
- Asynchronous traffic
- Memory Leak
- Number of rules

- Custom widgets
- Large numbers of Write events

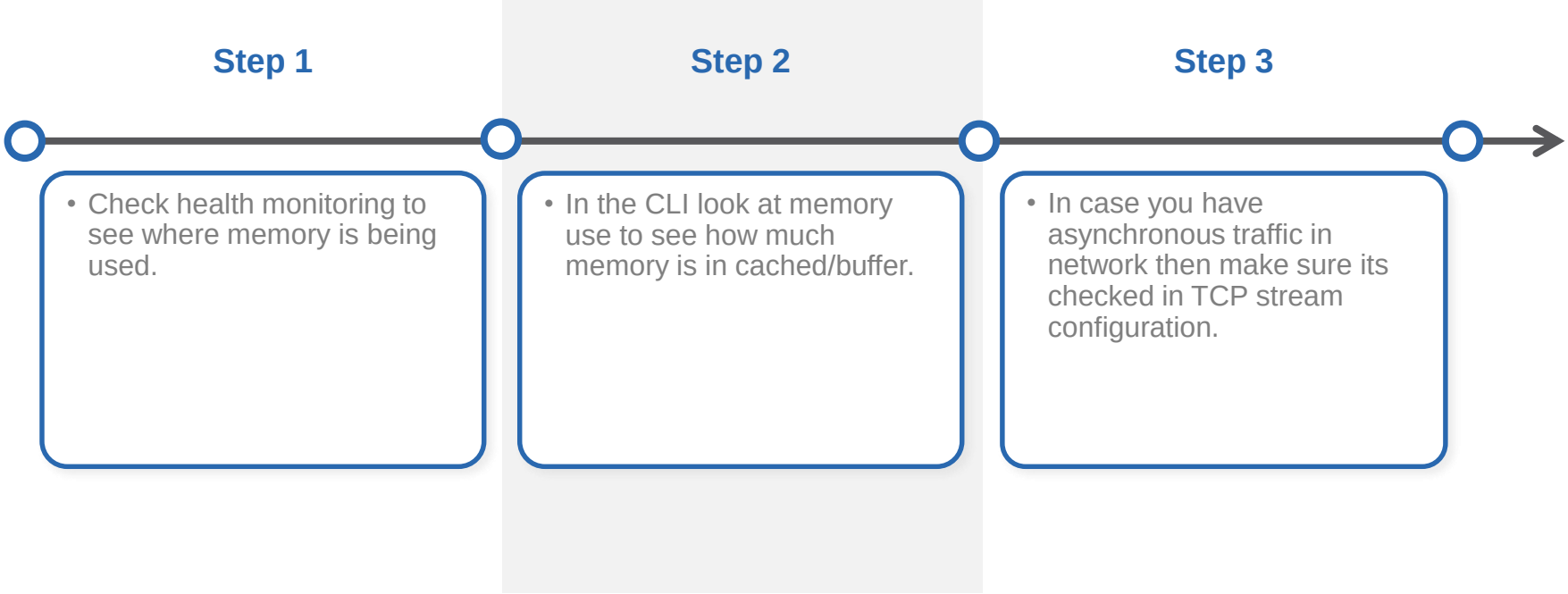
- Over-Subscription
- Type of Traffic
- Inspections enabled
- Elephant flows

Performance Troubleshooting

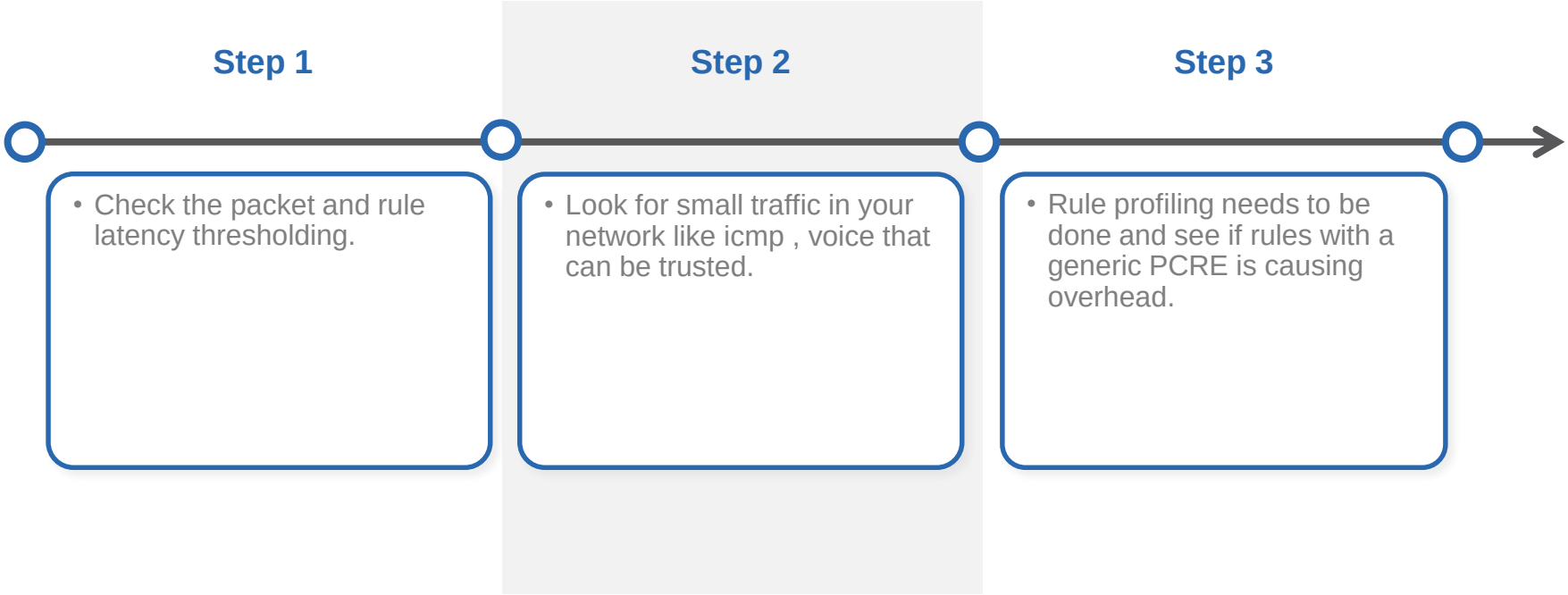
High CPU Troubleshooting



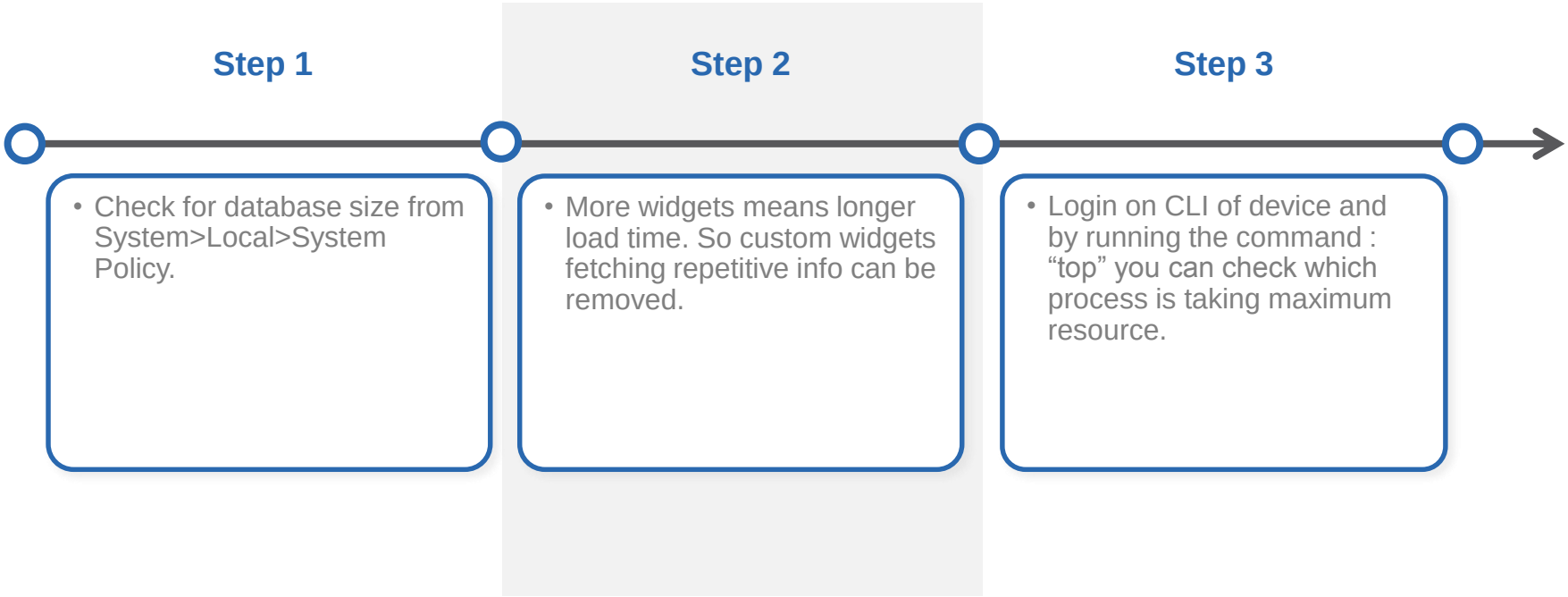
High Memory Troubleshooting



Low Throughput Troubleshooting



Latency on FireSight Management Center



Polling Question 3

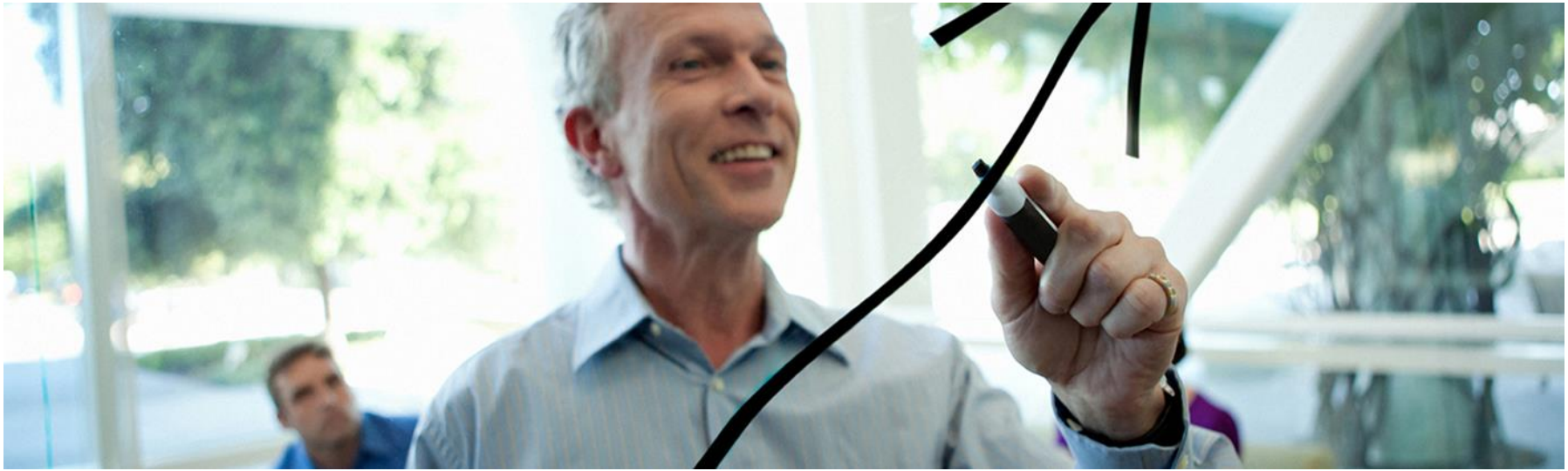
Which of the below options can cause latency on Firesight Management Center ?

A. Logged events

B. Custom widgets

C. Database size

D. All of the above



Best Practices

CPU

1	Trust Known Traffic (Internal network, backup and upload streams)
2	Elephant Flows should be avoided*
3	Avoid discovering 0.0.0.0/0 network

Tip: Test performance impact by changing policy to “BALANCED” mode.

*Please refer Elephant Flow document on CCO for more details.

Memory

1	Validate Asynchronous Traffic and update TCP stream configuration*
2	Check for swap and buffer memory.
3	Trust known traffic to reduce number of active TCP Sessions.

Tip: Memory is not an issue unless traffic is being affected.

*Please refer TCP Stream Configuration document on CCO for more details.

Throughput

1. Trust small packets in your network (like Voice, DNS & ICMP)
2. Rules with generic *PCRE** should be used with caution.
3. Elephant flows (like backup) will contribute to latency.

Tip: Total Throughput = SNORT-1 + SNORT-2 + +++ + SNORT-N

*Perl-Compatible Regular Expression.

Latency on FireSight Management Center

1. Connection event logging should be used with caution.
2. Keep connection event database size* to default value.
3. Avoid un-necessary custom widgets.

Tip: Log either the beginning or the end of the connection, but not both.

Please refer CCO Document for changing Database Size.

Submit Your Questions Now!

Use the Q & A panel to submit your questions and our expert will respond

Ask the Expert Event following the Webcast

Now through May 6th

https://supportforums.cisco.com/discussion/12959061/ask-expert-performance-troubleshooting-cisco-firepower

Join the discussion for these Ask The Expert Events:
http://bit.ly/events-webinar

Collaborate within our Social Media

Learn About Upcoming Events

Facebook- http://bit.ly/csc-facebook

Twitter- http://bit.ly/csc-twitter

You Tube http://bit.ly/csc-youtube

Google+ http://bit.ly/csc-googleplus

LinkedIn http://bit.ly/csc-linked-in

Instgram http://bit.ly/csc-instagram

Newsletter Subscription
http://bit.ly/csc-newsletter

Cisco has support communities in other languages!

If you speak Spanish, Portuguese, Japanese, Russian or Chinese we invite you to participate and collaborate in your language

Spanish
https://supportforums.cisco.com/community/spanish

Portuguese
https://supportforums.cisco.com/community/portuguese

Japanese
https://supportforums.cisco.com/community/csc-japan

Russian
https://supportforums.cisco.com/community/russian

Chinese
http://www.csc-china.com.cn

More IT Training Videos and Technical Seminars on the Cisco Learning Network

View Upcoming Sessions Schedule
https://cisco.com/go/techseminars

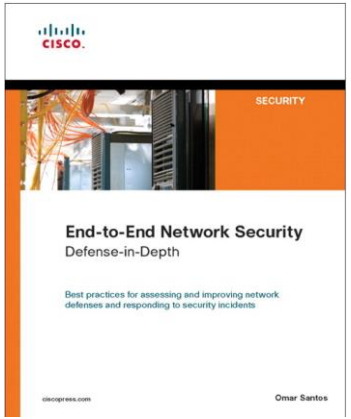
Thank you for participating!

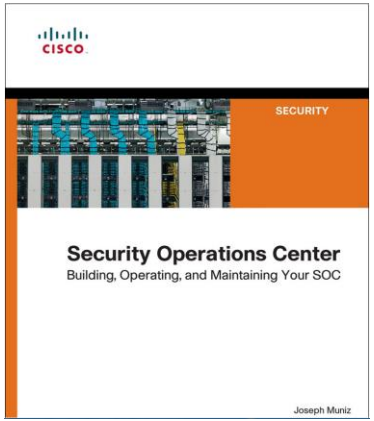
. Redeem your 35% discount offer by entering code: CSC when checking out:

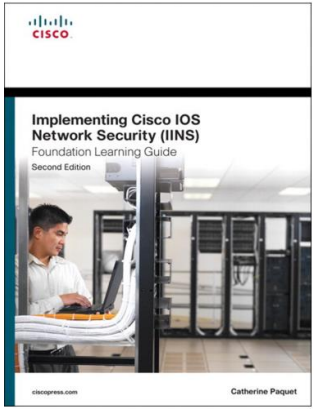
Visit Cisco Press at:

http://bit.ly/csc-ciscopress-2016

Cisco Press







Please take a moment to complete the survey

Thank you for Your Time!


CISCO
TOMORROW starts here.