



# 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 2<sup>nd</sup> – May 13<sup>th</sup>

<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 10<sup>th</sup> – May 20<sup>th</sup>

<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/1jll93B>

Participate in Expert  
Programs with Cisco.  
Apply today to join  
the Experts Bureau.

Apply Today



**Cisco Support Community**  
Community Directory Expert Corner Community Corner Solutions

Home Expert Corner Top Contributors Language: English Contact Us Help Follow Us

**Top Contributors**

Recognition Program VIPs Spotlight Awards Hall of Fame Events Top Contributors Expert Interviews

**Cisco Designated VIPs**

The Cisco Designated VIP program recognizes the top external individual contributors in Cisco's online communities, including the Cisco Support Community (CSC), Cisco Learning Network (CLN) and the Cisco Developers Network (CDN). Cisco Designated VIPs are recognized by their peers for their expertise and tireless contributions, and their abundant participation is vital to community success. With this program, Cisco formally recognizes the positive, valuable influence our top individual members exert on the communities overall. To learn more, please visit our [FAQ](#)

**CISCO DESIGNATED VIP** < 2016 2015 2014 2013 2012 2011 >

<b>Aaron Harrison</b> 2016 IP Telephony	<b>Aman Sci</b> 2016 IP Telephony
<b>Ayodeji Oladipo Okanlawon</b> 2016 IP Telephony	<b>Carlo Poggiarelli</b> 2016 IP Telephony
<b>Chris Deren</b> 2016 IP Telephony, Contact Center, Unified Communications	<b>Dan Lukes</b> 2016 Small Business
<b>George Stefanick</b> 2016 Wireless	<b>Jon Marshall</b> 2016 LAN, WAN, Firewalling
<b>Jonathan Schulenberg</b> 2016 IP Telephony	<b>Karsten Iwen</b> 2016 Firewalling, VPN

**Cisco Support Community**  
Directory Expert Corner Solutions Community Corner

Home Experts Bureau Top Contributors Leaderboards Knowledge Sharing Voting results Panelizer Hierarchy

**Experts Bureau**

Use the Cisco Experts Bureau to find, connect, and follow recognized Subject Matter Experts and the programs they participate in regularly. The Experts Bureau comprises Cisco employees as well as Partners and Customers who have contributed to, or been selected for knowledge sharing programs on the Cisco Support Community, such as Webcasts, Ask the Expert Events, Facebook Forums, Tech-Talks, Meetups, and Blogs.

If you have interest in participating, apply online through this [simple form](#). After applying, a member of the Cisco Support Community team will be in contact with additional details.



<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

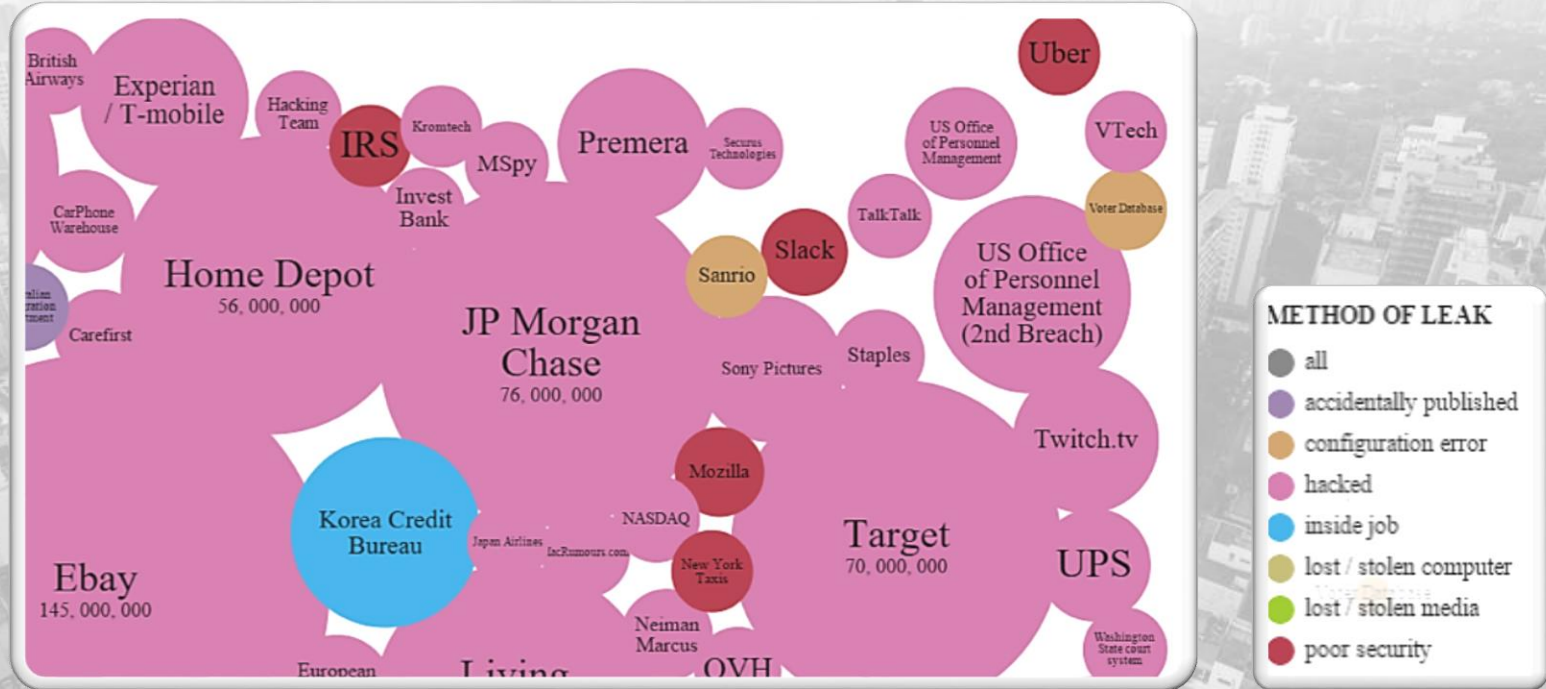
There is a multi-billion dollar global industry targeting your prized assets

\$450 Billion  
to  
**\$1 Trillion**



Malware  
Development  
\$2500  
(commercial  
malware)

# Dangerous Times: World's biggest data breaches





# SECURITY EVERYWHERE

## Attack Continuum

Before

During

After



Endpoint



Branch



Edge



Campus



Data  
Center



Cloud



Operational  
Technology



Services



# The Problem with Legacy Next-Generation Firewalls

Focus on the Apps...

00 01000111 0100 111001 CITRIX® 010 01000 01000 111010

00 01000111 0100 1110101001 [f] 111 0011 101001 110011

100 0111100 011 101 [S] 01 1000111010011101 1000111

01000 01000111 0100 [e] 000111010011101 10001110100

0111100 011 1010011101 1 1 [M] 1100 011 101001111 01

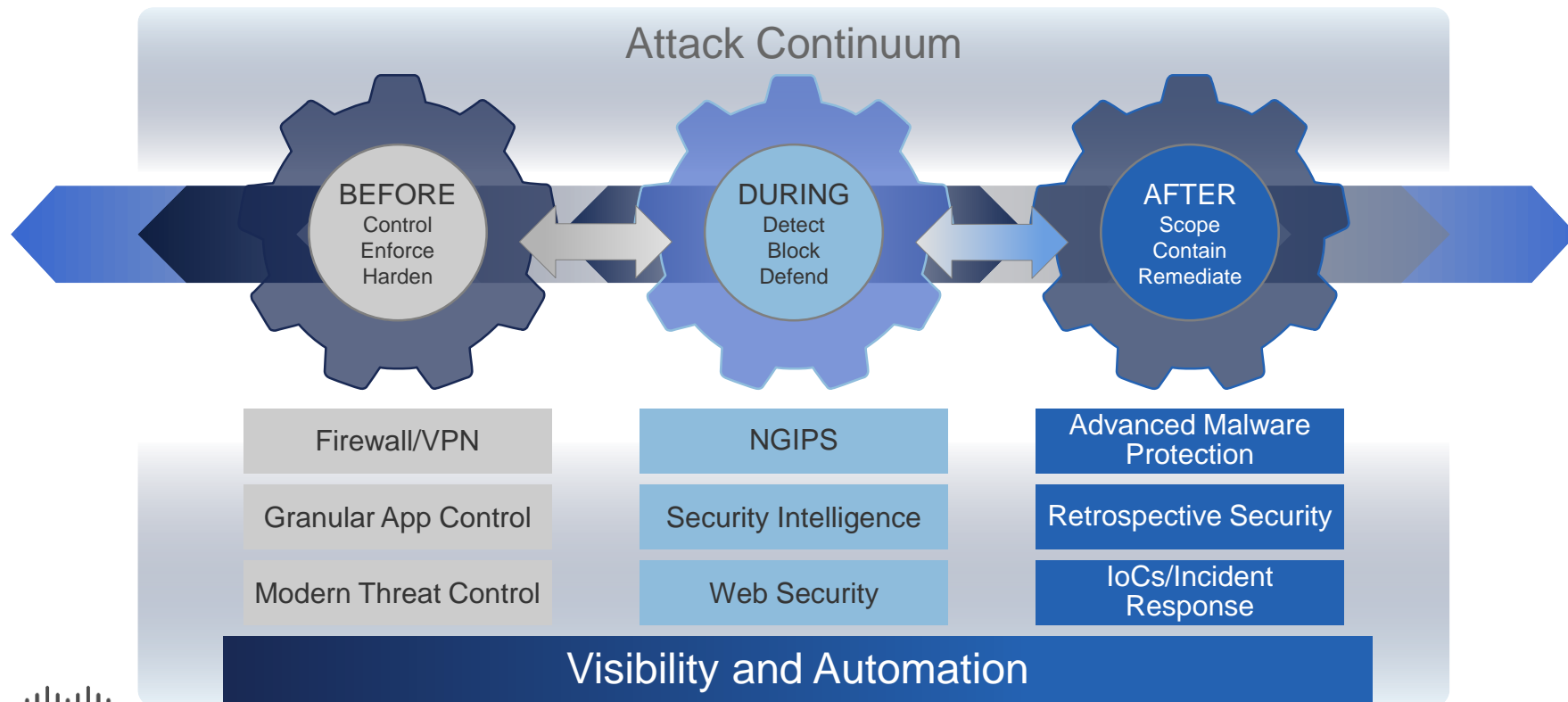


...But Miss the Threat



Legacy NGFWs can reduce attack surface area but advanced malware often evades security controls.

# 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

# Cisco NGFW Product Family

Performance and Scalability

ASA 5506H-X  
ASA 5506W-X  
ASA 5506-X



ASA 5508-X



SMB & Distributed Enterprise



ASA 5516-X

ASA 5525-X



ASA 5545-X



ASA 5555-X

Commercial & Enterprise



ASA 5585:  
SSP10  
SSP20  
SSP40  
SSP60

Data Center, High Performance Computing, Service Provider

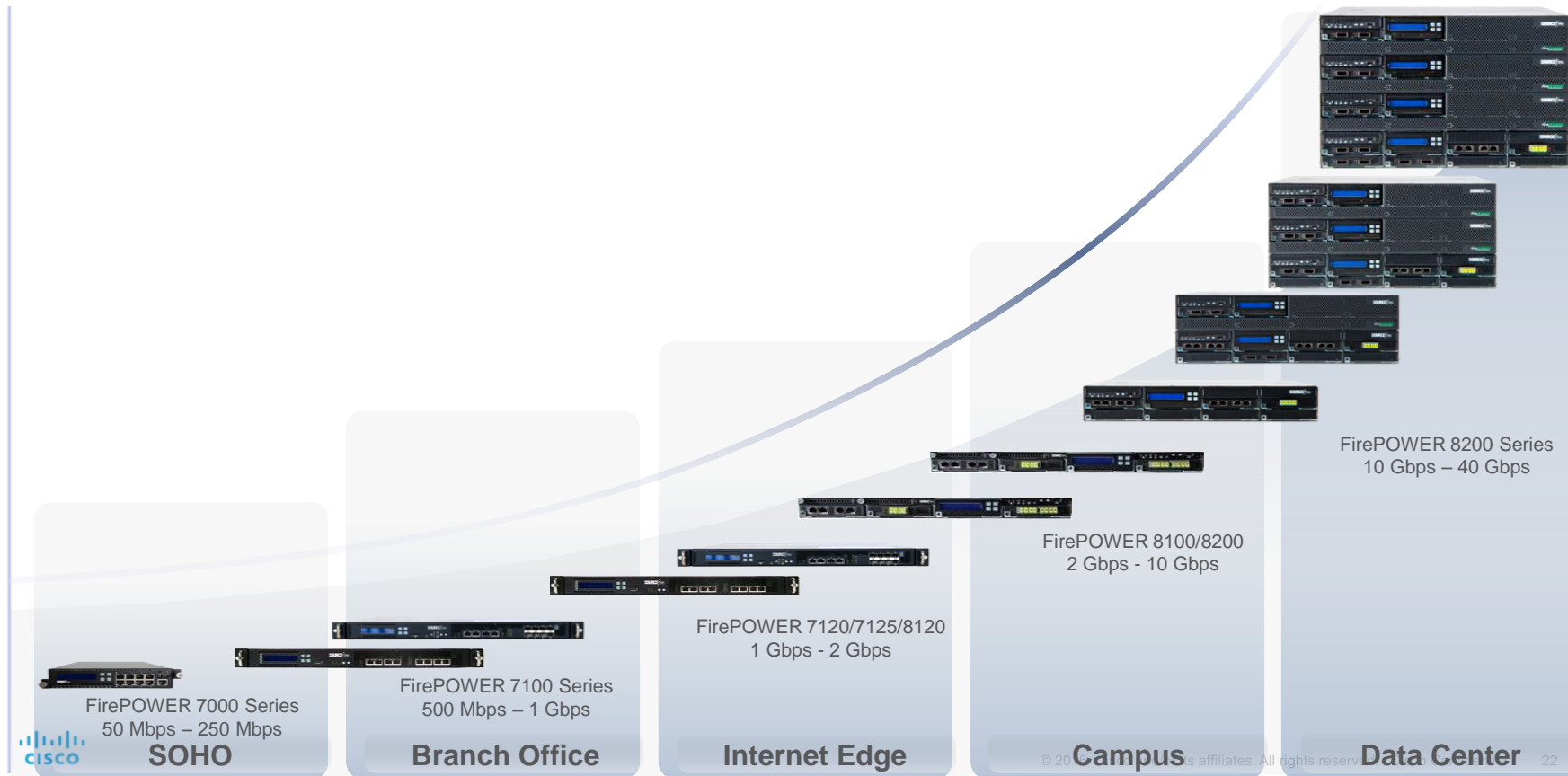


Firepower  
4100



Firepower  
9300

# 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	<b>Firepower Management Center Virtual</b> 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		

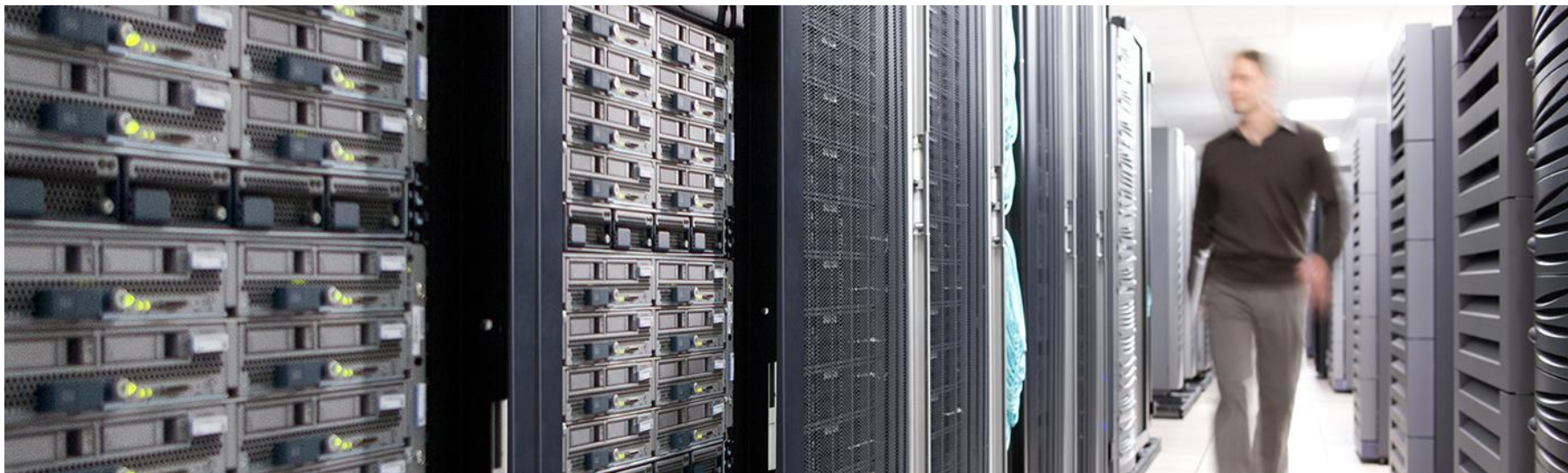
\* Max number of devices is dependent upon sensor type and event rate



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>

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

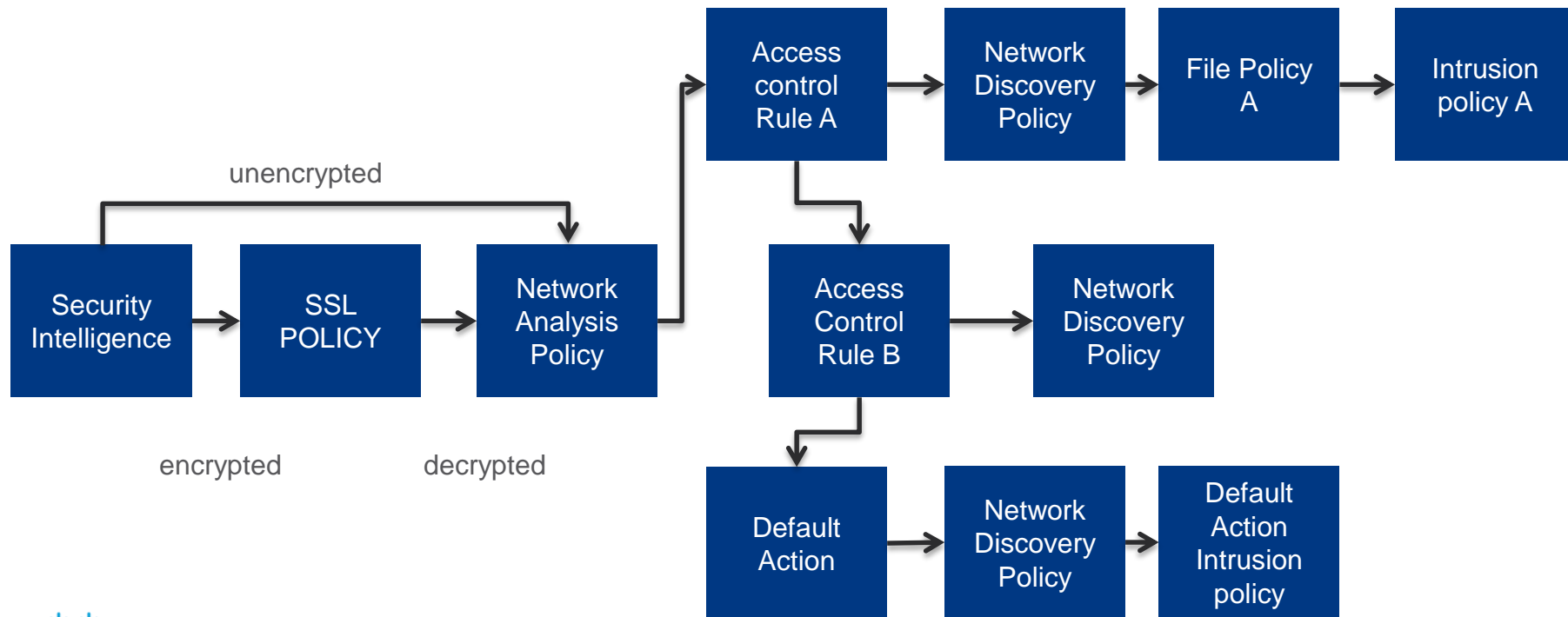
23



# Life of a packet



# Packet Flow



# Polling Question 2

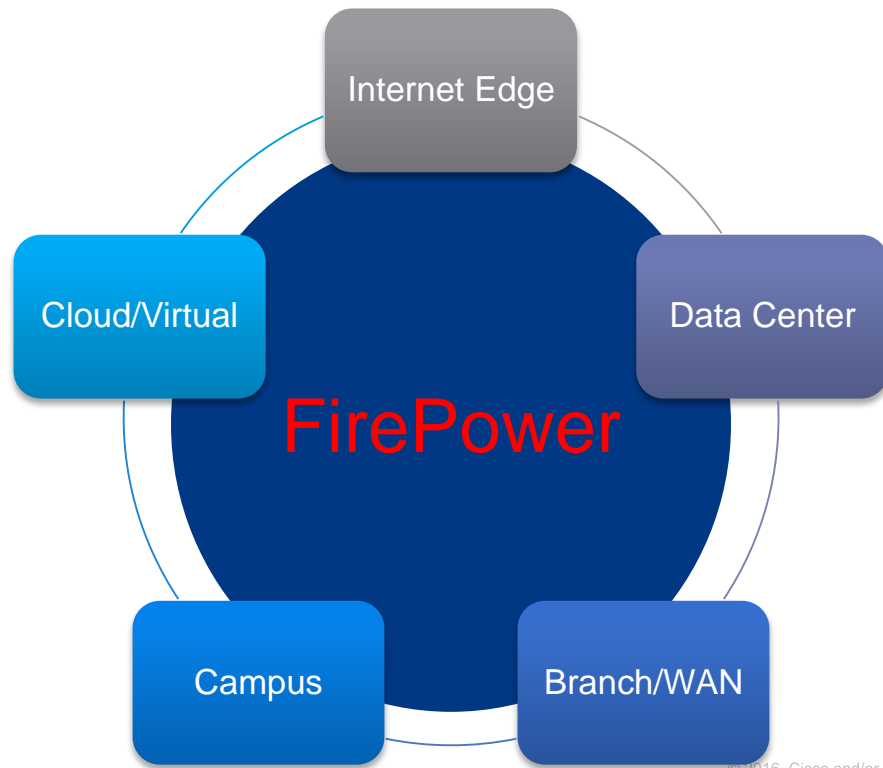
**Which policy will a packet be inspected against First ?**

- 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



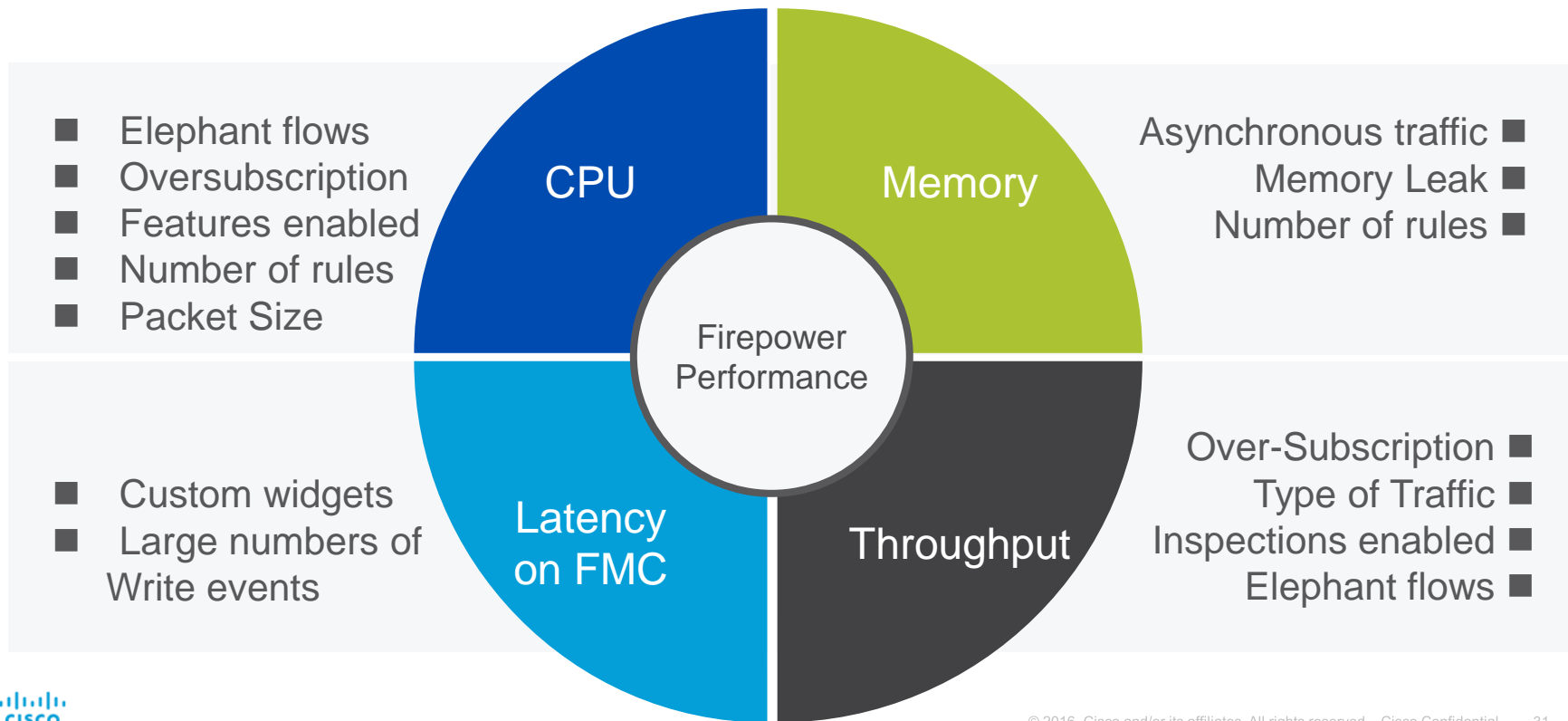
SARBANES-OXLEY ACT (SOX)  
COMPLIANCE





# Factors Impacting Performance

# Performance Factors

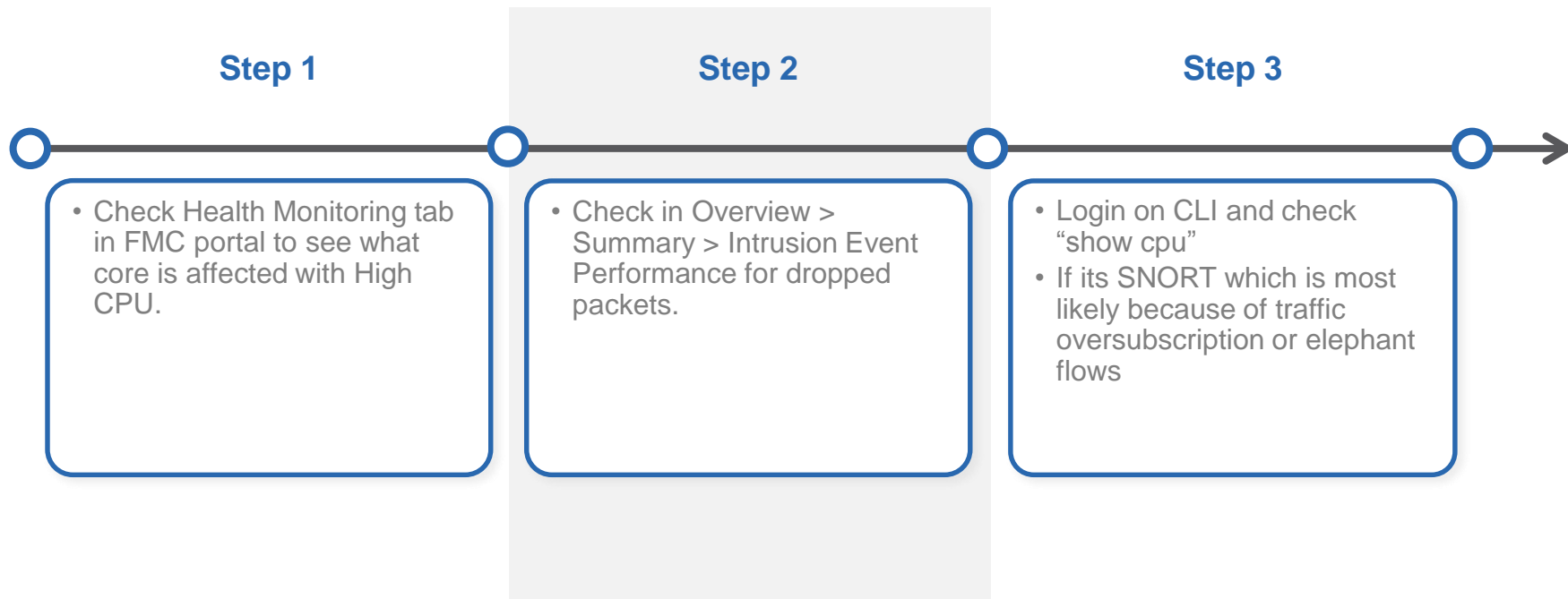




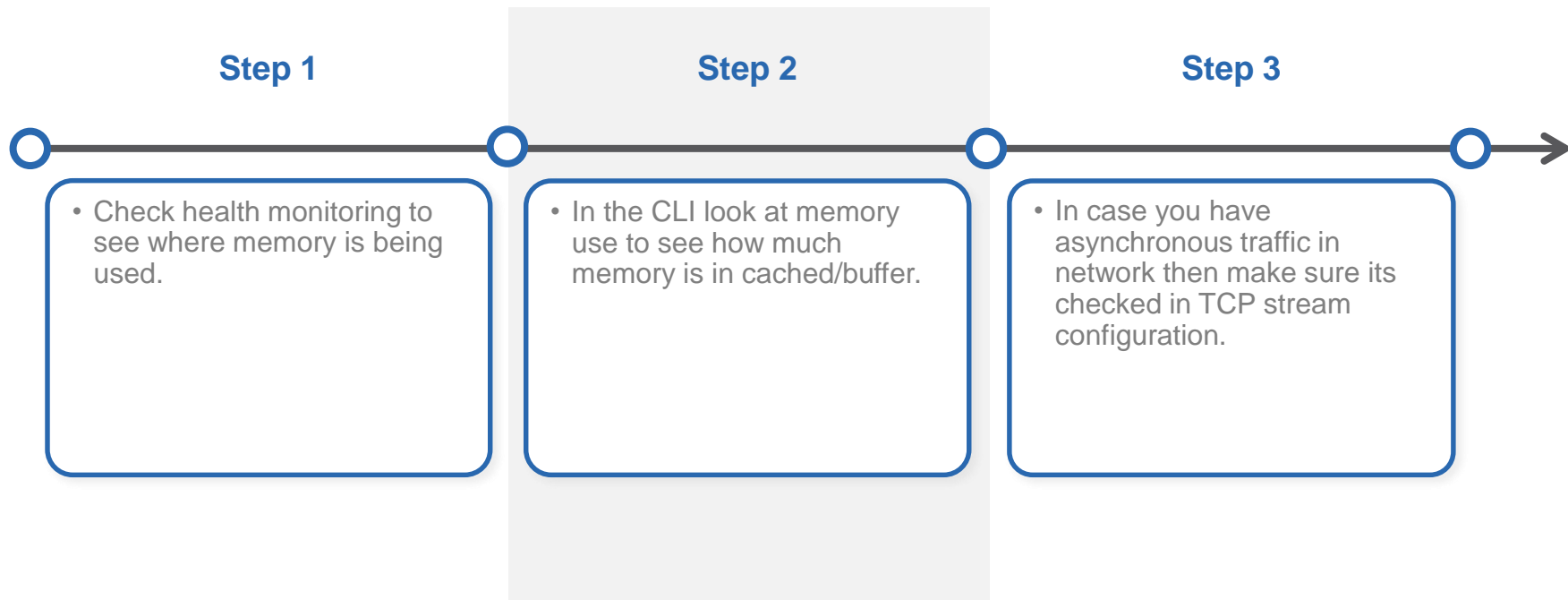
# Performance Troubleshooting



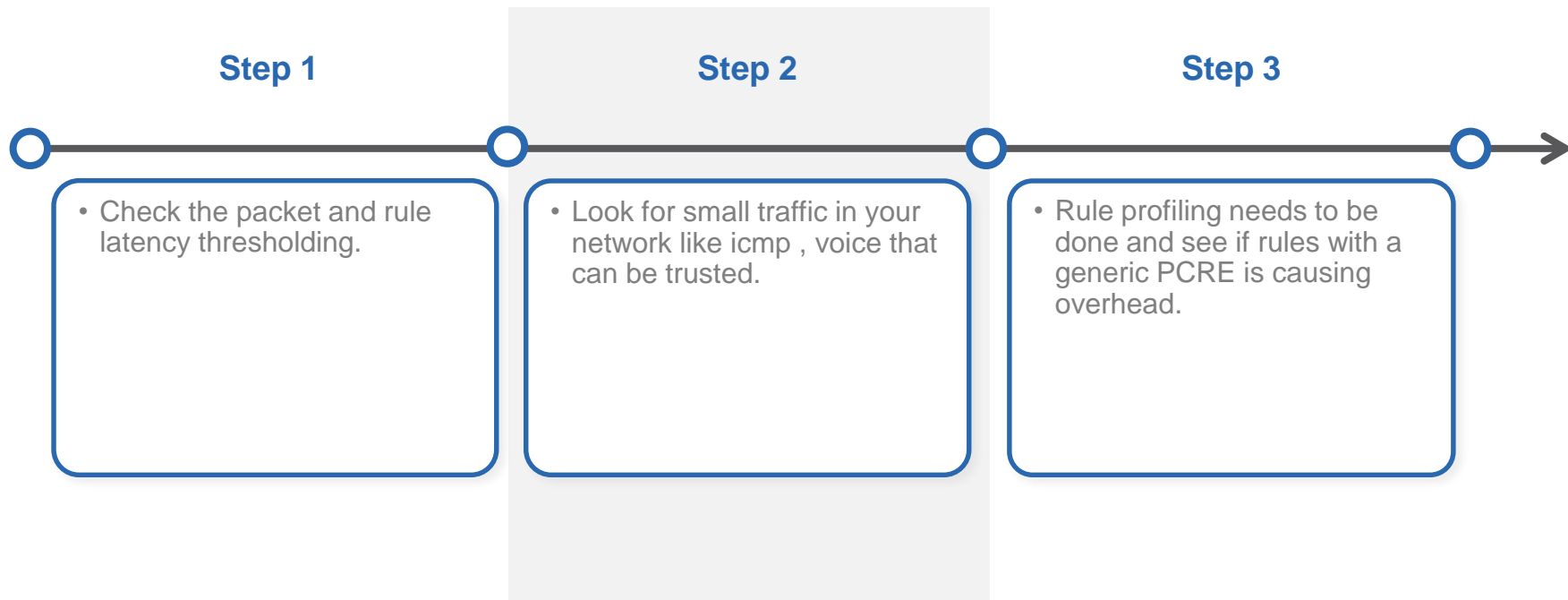
# High CPU Troubleshooting



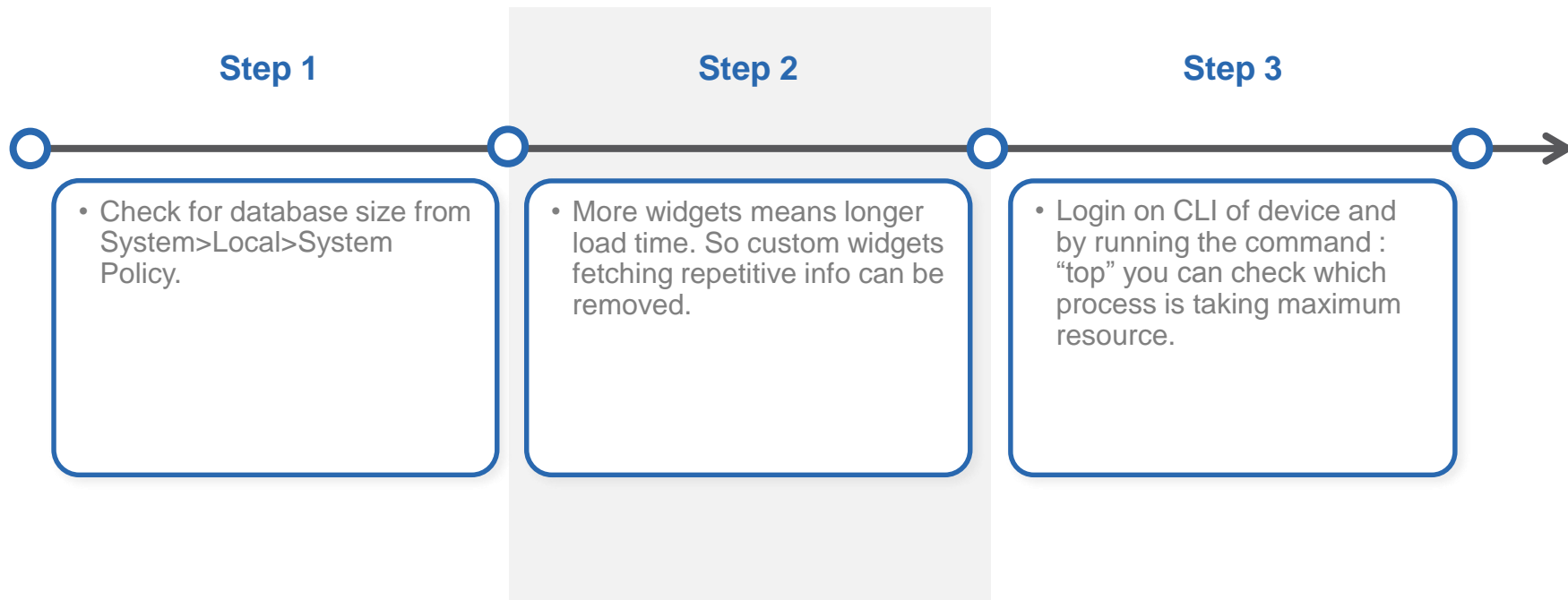
# High Memory Troubleshooting



# Low Throughput Troubleshooting



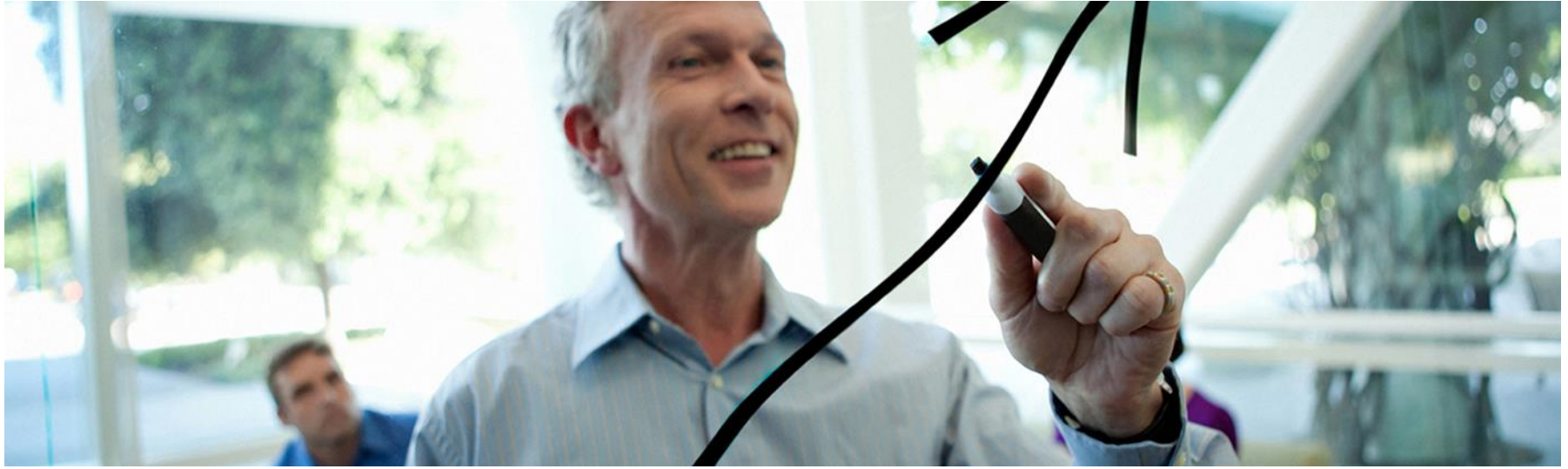
# Latency on FireSight Management Center



# 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.

# 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.



# 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

# 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.



# 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>



Instagram <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>

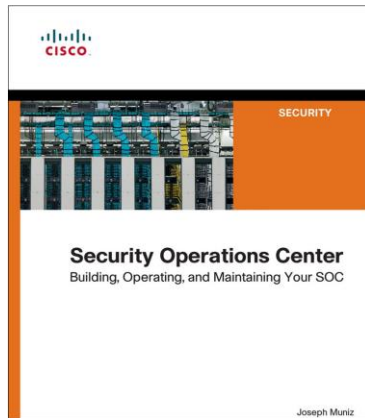
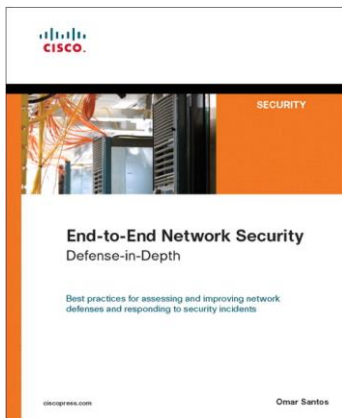
Thank you for participating!

- . 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.*