



Cisco Support Community Expert Series Webcast

FirePOWER Threat Defense for Integrated Services Routers (ISR)

Kureli Sankar, CCIE Security

July 8, 2015

Ask the Expert Events – Active

Now through July 17th

Cisco Unified Computing System Upgrade Best Practices with Payal Bhaduri. Learn and ask questions about UCS architecture and the complete firmware upgrade procedure which would help customers/partners to maintain and operate the UCS environment.

FoIP on CUBE and Gateway's using T.38, protocol based passthrough and modem passthrough hosted by Cisco Experts, Pawan Srivastava and Kaustubh Inamdar



Join the discussion for these Ask The Expert Events:

<http://bit.ly/events-webinar>

Become an Event Top Contributor

Participate in Live Interactive Technical Events and much more

<http://bit.ly/1jll93B>



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 < 2015 2014 2013 2012 2011 >

 Aman Soi 2015 IP Telephony	 Anthony Holloway 2015 Contact Center
 Ayodeji otadipo Okantawon 2015 IP Telephony	 Carlo Poggiarelli 2015 IP Telephony
 Chris Deren 2015 IP Telephony	 Dan Lukes 2015 Small Business, Voice
 Gergely Szabo 2015 Contact Center	 John Blakley 2015 LAN, WAN

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.

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

Kureli Sankar,
CCIE Security #35505

- Today's first featured expert is Kureli Sankar, a former TAC engineer in the firewall team and now a technical marketing engineer responsible for security features on Cisco's IOS and XE products.
- Ask your questions now in the Q&A window



Meet Your Question Managers

Hai Bo Ma



Aston AuYeung



Ask the Expert Event following the Webcast

Now through July 17, 2015

Kureli Sankar will be continuing the discussion in an Ask the Expert event. So if you have more questions, please visit the Expert Corner > Events on the Cisco Support Community

<https://supportforums.cisco.com/discussion/12550411/ask-expert-firepower-threat-defense-integrated-services-routers-isr>



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/12542991/webcast-slidesfirepower-threat-defense-integrated-services-routers-isr>





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



FirePOWER Threat Defense for Integrated Services Routers (ISR)

Cisco Support Community Expert Series Webcast

Kureli Sankar,

CCIE Security #35505

Technical Marketing Engineer

July 8, 2015

Agenda

- Company Introduction
- What is FirePOWER
- Why do we need FirePOWER
- IDS VS IPS
- Cisco FirePOWER Threat Defense for ISR overview
- Branch in a box Security with FirePOWER
 - Important Features
 - Functions
 - Configurations
- Resources

Polling Question 1

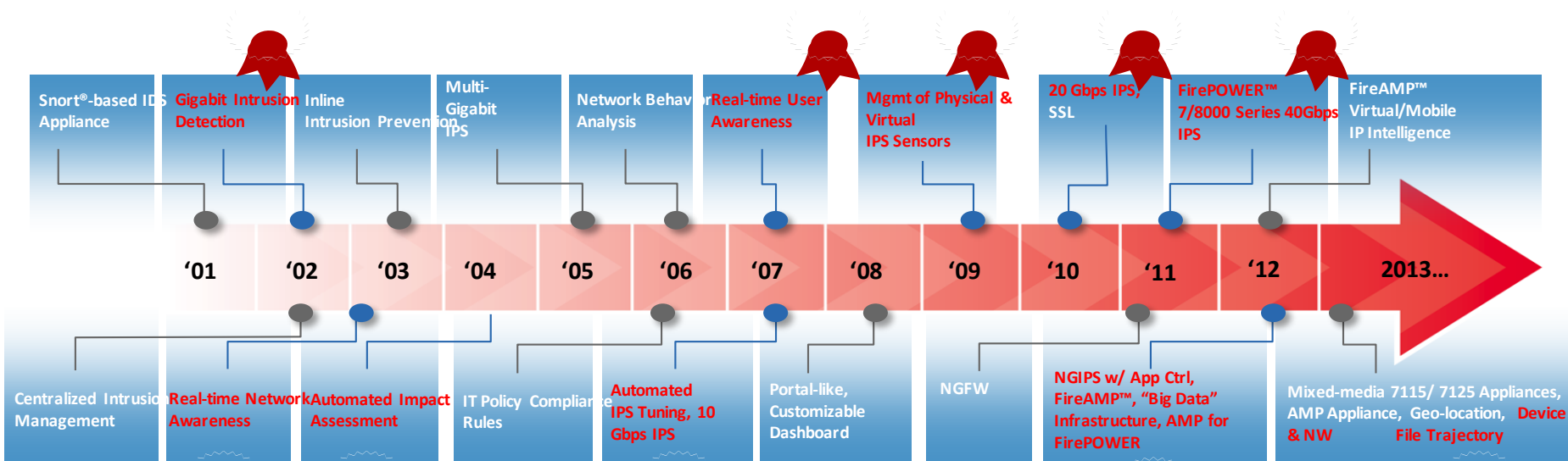
Why are the reasons for your company to invest in Threat Defense Solution?

1. Fear of data breach.
2. To provide a safe internet browsing experience for our users.
3. To protect all our assets from getting infected with malicious Trojans, SpyWare and other attacks.
4. Strictly for PCI and other compliance sake only

Company Introduction

- Acquired Sourcefire in October 2013 for \$2.7B
- Five months after acquisition
 - AMP technology enhances Cisco's ESA, WSA and CWS products
 - Four new FirePOWER appliances introduced (up to 60Gbps)
 - OpenAppID program launched
- Eight months after
 - New AMP features including NGIPS-integrated IoCs and cloud-based sandboxing
- Threat-centric NGFW launched in September 2014

Sourcefire Innovation

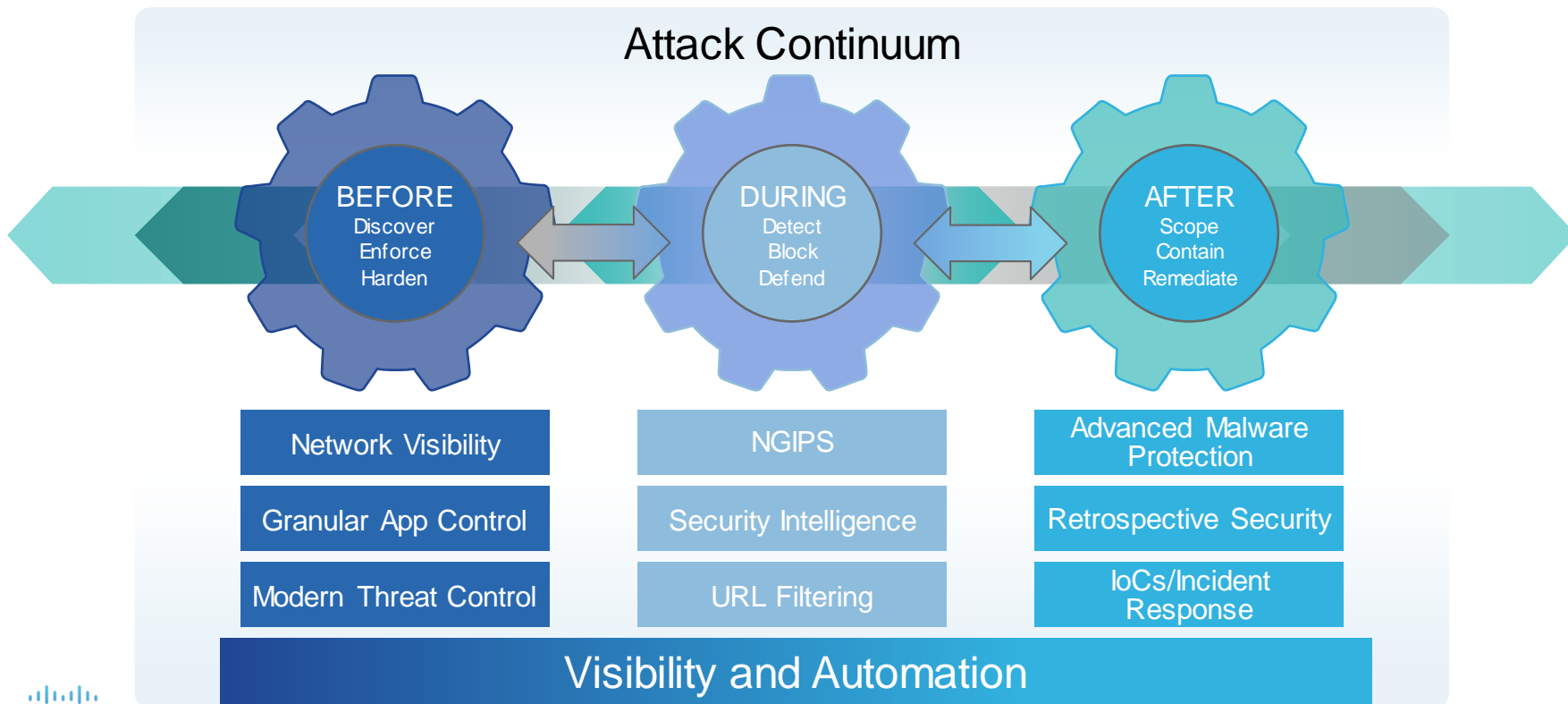


52 Patents Awarded or Pending

World-Class Vulnerability Research Team (VRT™)

What is FirePOWER

Integrated Threat Defense Across the Attack Continuum



Cisco FireSIGHT Brings Unprecedented Network Visibility

Threats
Users
Web Applications
Application Protocols
File Transfers
Malware
Command & Control Servers
Client Applications
Network Servers
Operating Systems
Routers & Switches
Mobile Devices
Printers
VoIP Phones
Virtual Machines

	Threats	Users	Web Applications	Application Protocols	File Transfers	Malware	Command & Control Servers	Client Applications	Network Servers	Operating Systems	Routers & Switches	Mobile Devices	Printers	VoIP Phones	Virtual Machines
FirePOWER NGIPS	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Typical IPS	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Typical NGFW	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗

Automated, Integrated Threat Defense

Superior Protection for Entire Attack Continuum



Context
and Threat
Correlation



Dynamic
Security
Control



Multi-vector
Correlation



Retrospective
Security

Automated, Integrated Threat Defense

Superior Protection for Entire Attack Continuum



Context
and Threat
Correlation



Dynamic
Security
Control



Multi-vector
Correlation



Retrospective
Security

Automated, Integrated Threat Defense

Superior Protection for Entire Attack Continuum



Context
and Threat
Correlation



Dynamic
Security
Control



Multi-vector
Correlation



Retrospective
Security

Automated, Integrated Threat Defense

Superior Protection for Entire Attack Continuum



Context
and Threat
Correlation



Dynamic
Security
Control



Multi-vector
Correlation



Retrospective
Security

Polling Question 2

What do you consider important with any product?

1. Ease of configuration
2. Ease of management
3. Excellent Alerting and Reporting capability
4. All of the above

Why do we need FirePOWER

Enterprise Challenges



Digital Displays



Omni-channel Apps



SaaS Enterprise Apps



Guest WiFi



HD Video



Online Training



Social Media



OS Updates



Mobile Apps



BRANCH

MORE USERS

80%

Of employee and customers are served in branch offices*

MORE DEVICES

73%

Growth in in mobile devices from 2014 - 2018**

MORE APPS

20-50%

Increase in Enterprise bandwidth per year through 2018**

MORE THREATS

30%

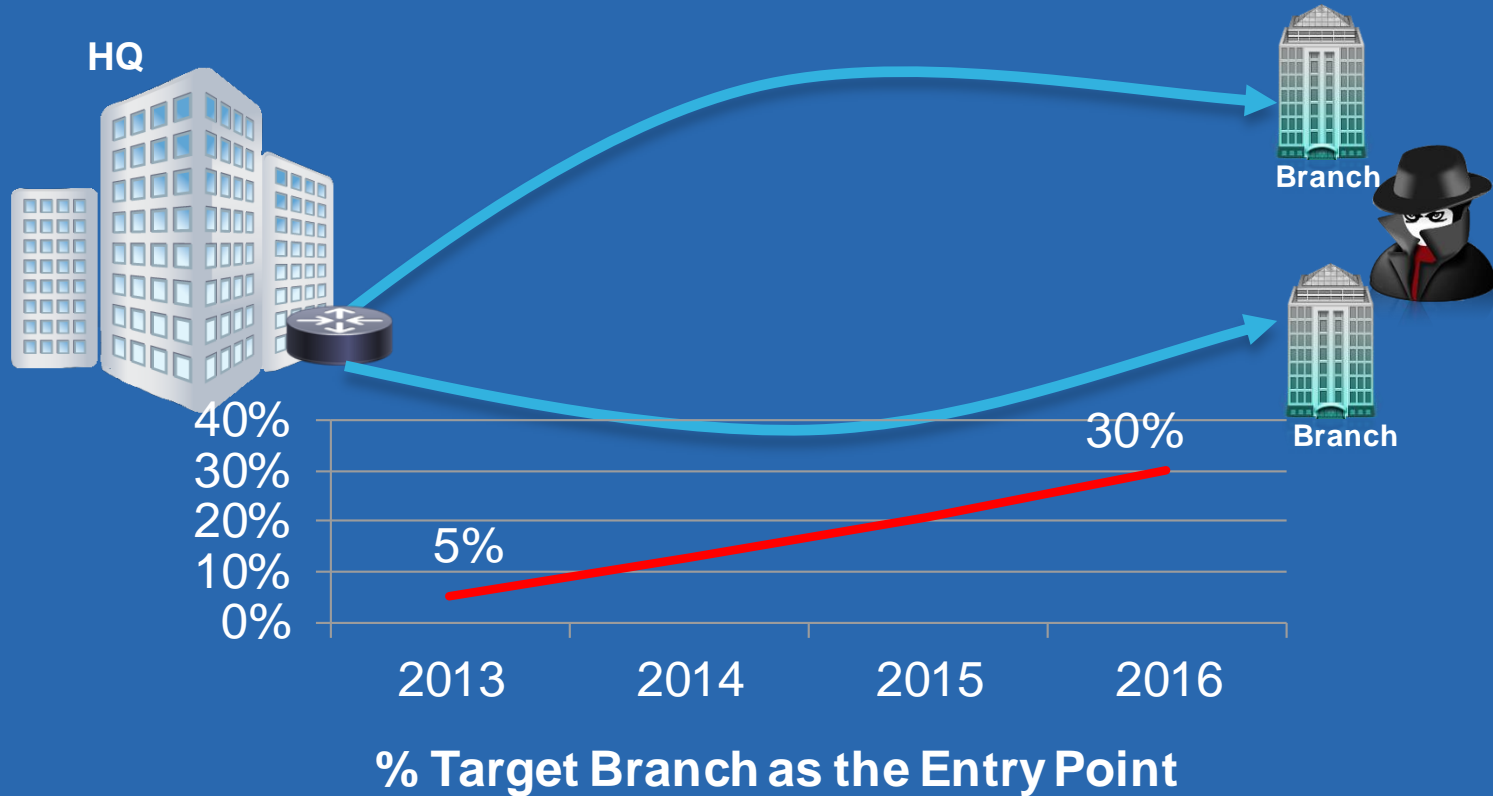
Of advanced threats will target branch offices by 2016 (up from 5%) **

*Tech Target, Branch Office Growth Demands New Devices., 2013

**Gartner, Forecast Analysis: Worldwide Enterprise Network Services, Q2 2014 Update

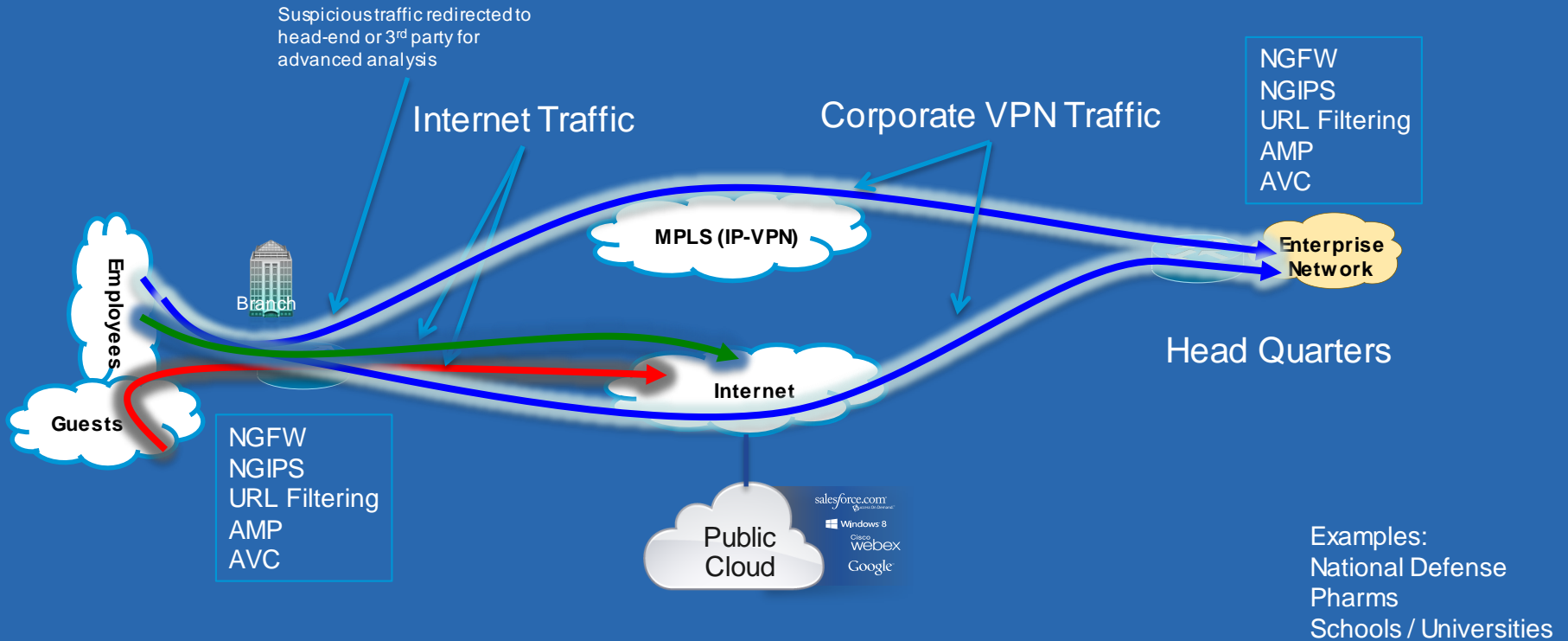
*** Gartner, "Bring Branch Office Network Security Up to the Enterprise Standard," JeremyD'Hoinne, 26 April, 2013.

POINT OF ATTACK – Advanced Targeted Threats

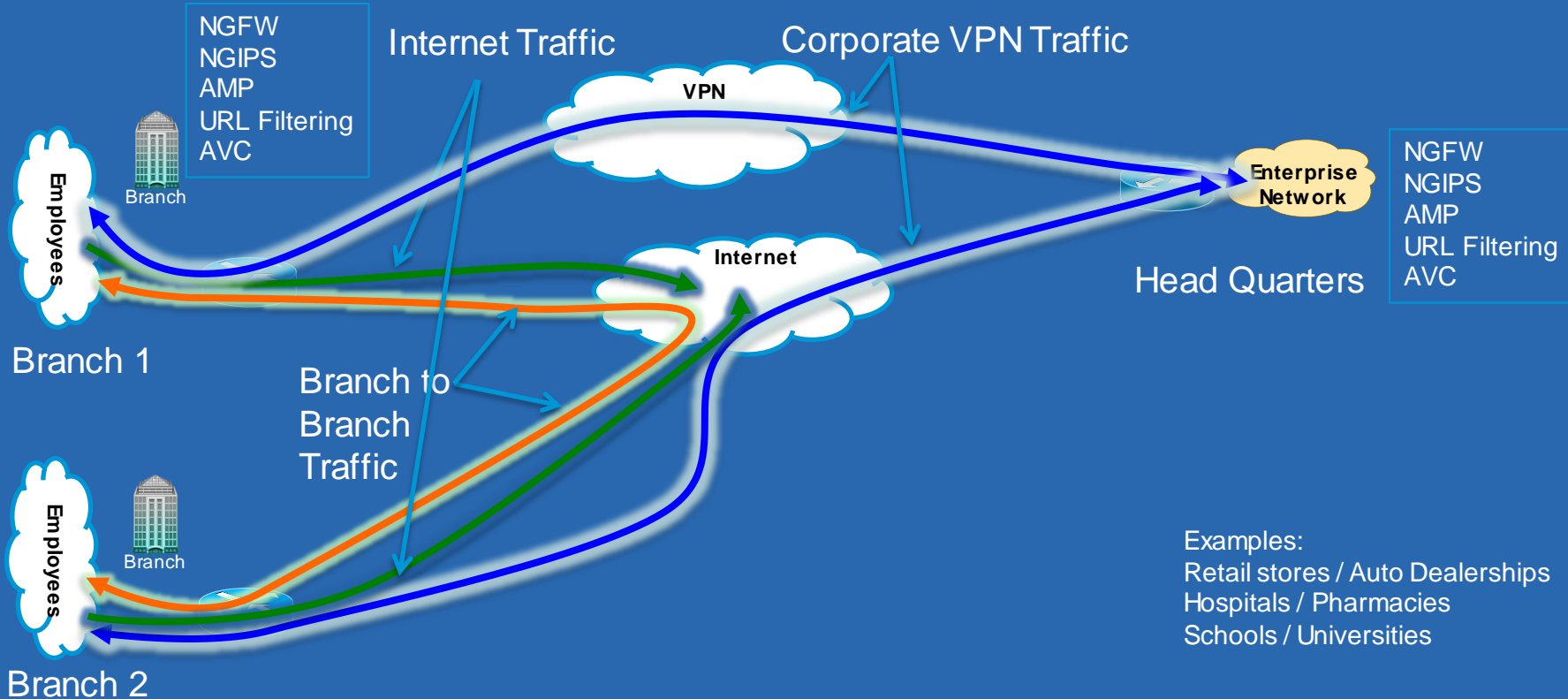


* Gartner: "Bring Branch Office Network Security Up to the Enterprise Standard", April 2013

Use Case 1: Secure Branch Direct Internet Access (DIA)



Use Case 2: Secure Branch to Secure Branch Direct Access



IDS VS IPS

Cisco FirePOWER Threat Defense for ISR

- IDS – Intrusion Detection System
- IPS – Intrusion Prevention System

Polling Question 3

Do you have
FirePOWER/Fire
SIGHT deployed
in your
environment?

Yes, I am using ASA FirePOWER for inspection.

2. Yes, I am using ISR FirePOWER for inspection.

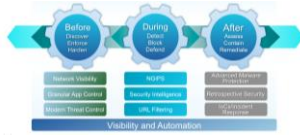
3. No, but I am planning to use ISR FirePOWER for inspection.

4. No, I am not planning to implement IPS, AMP and URL filtering.

Cisco FirePOWER Threat Defense for ISR overview

Cisco FirePOWER Threat Defense for ISR

FirePOWER Threat Defense



+

AppX + Security License



UCS-E Series



ISR 4000 Series



OR

ISR G2 Series

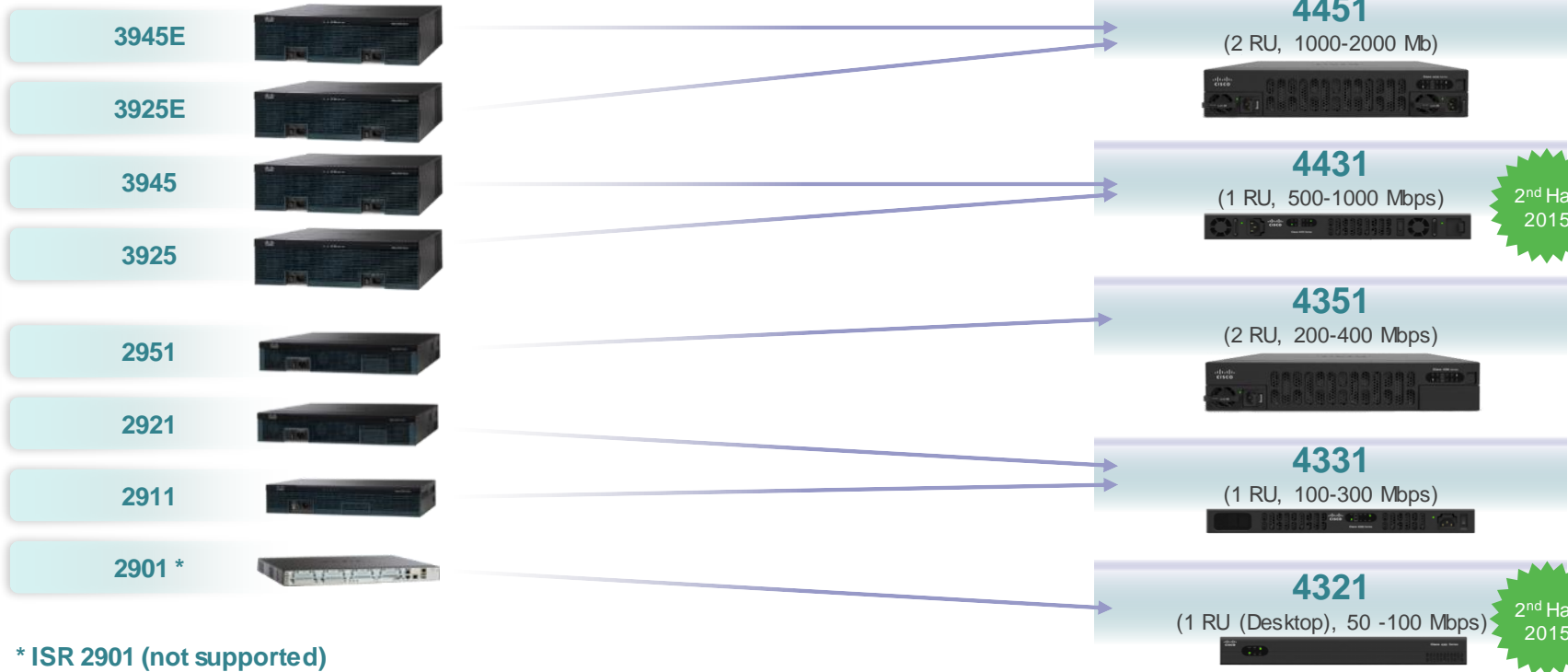


Free Up Valuable Square Footage

Generate More Revenue \$\$\$

FirePOWER for Cisco ISR 4000 and G2 Series

Branch consolidation



* ISR 2901 (not supported)



Application services

UCS E-Series Portfolio

Scalability

Network Compute Engines

Cisco UCS-EN120S



- **Cores:** 2
- **RAM:** 4-16GB (2 DIMMs)
- **HDD:** 2 hard-drives, available in 2 SAS and SATA options

Servers

Cisco UCS-E140S



- **Cores:** 4
- **RAM:** 8-16GB (2 DIMMs)
- **HDD:** 2 hard-drives, available in 3 SSD, SAS and SATA options

Cisco UCS-E160D



- **Cores:** 6
- **RAM:** 8-48GB (3 DIMMs)
- **HDD:** 3 hard-drives, available in SSD, SAS and SATA options

Cisco UCS-E180D



- **Cores:** 8
- **RAM:** 8-48GB (3 DIMMs)
- **HDD:** 3 hard-drives, available in SSD, SAS and SATA options

Platform Support:

- Cisco ISR G2 Series
 - ISR 2900
 - ISR 3900
- Cisco ISR 4000 Series*
 - ISR 4331
 - ISR 4351
 - ISR 4451

* ISR 4321 and 4431 (coming 2nd Half 2015)

Cisco ISR with FirePOWER Services UCS-E Modules Platforms Support

ISR 4K Platform	ISR 4321 *	ISR 4331	ISR 4351	ISR 4431 *	ISR 4451
UCSE 180D	No	No	Yes	No	Yes
UCSE 160D	No	No	Yes	No	Yes
UCSE 140S	No	Yes	Yes	No	Yes
UCSE 120S	No	Yes	Yes	No	Yes

ISR G2 Platform	ISR 2911	ISR 2921	ISR 3925	ISR 3925E	ISR 3945	ISR 3945E
UCSE 180D	No	No	Yes	Yes	Yes	Yes
UCSE 160D	No	No	Yes	Yes	Yes	Yes
UCSE 140S	Yes	Yes	Yes	Yes	Yes	Yes
UCSE 120S	Yes	Yes	Yes	Yes	Yes	Yes

* ISR 4K routers will support NIMs when released in Aug 2015

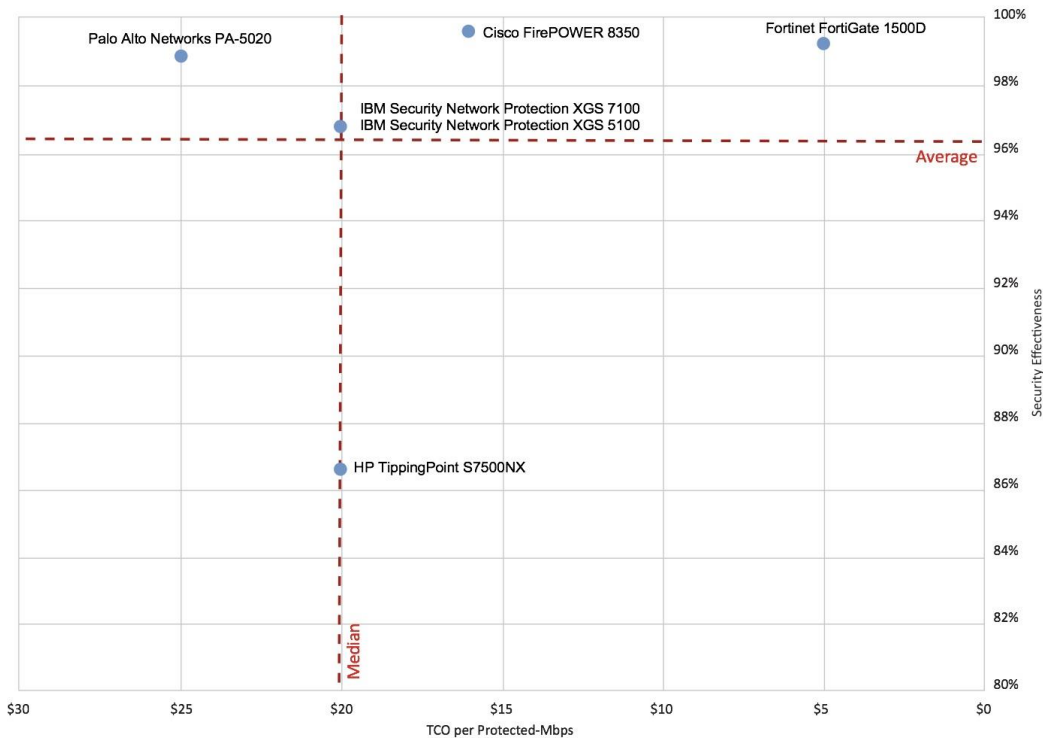
NSS Labs 2015 NGIPS Testing Released

Cisco FirePOWER the Leader in Efficacy (Again)

Cisco is still the highest tested @ 99.5%

Lower TCO at ~ \$17.00

NSS Labs Next Generation Intrusion Prevention System (NGIPS) Security Value Map™



Source: NSS Labs 2015

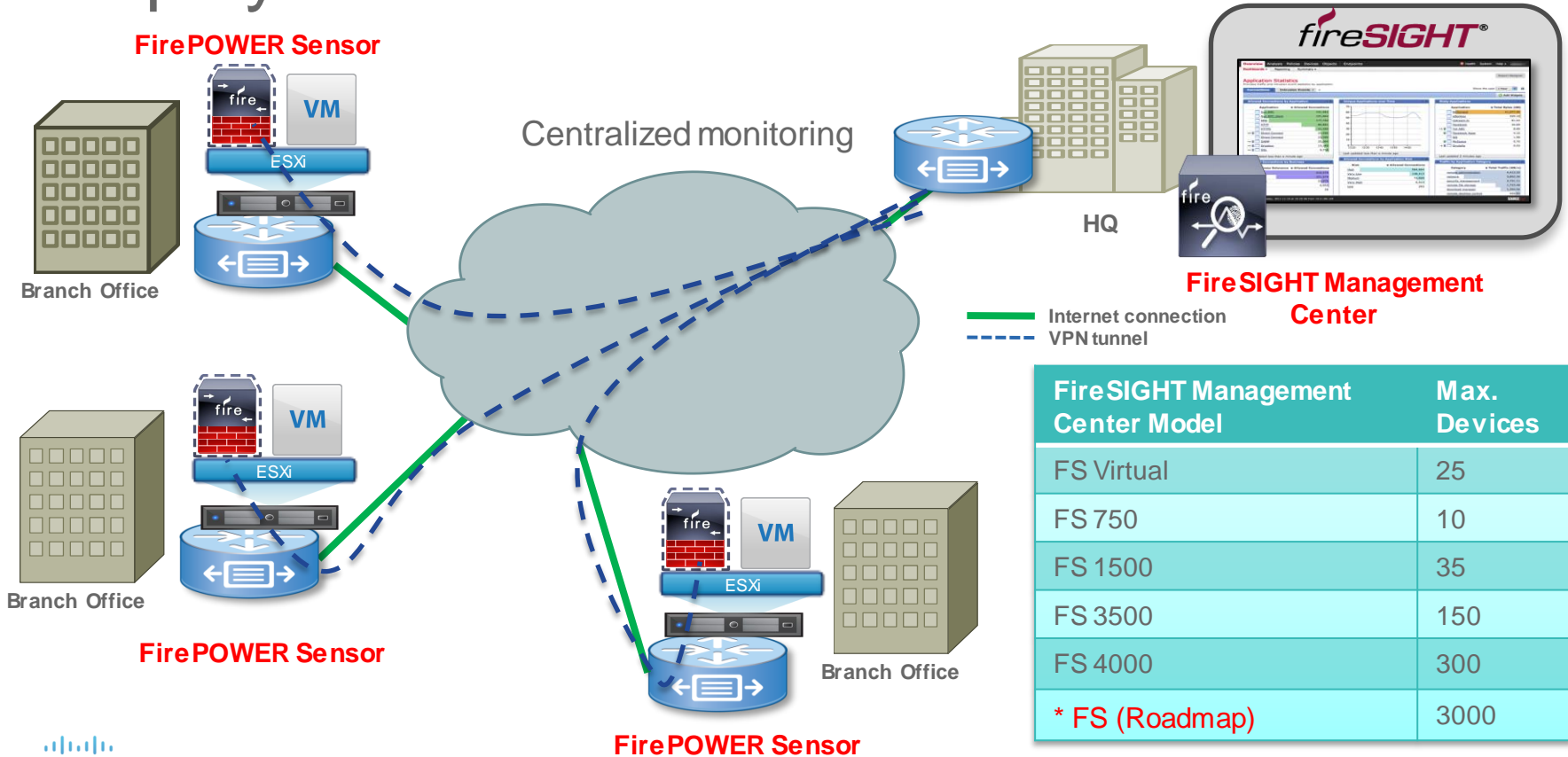


Branch in a box Security with FirePOWER

Cisco FirePOWER Threat Defense for ISR - IDS

- IOS-XE data-plane pushes packets to SF Sensor for analysis
- IOS-XE CLI used to create service & configure redirection (global or per-interface)
- SF Sensor CLI used to setup sensor and link to FireSIGHT Management
- SF FireSIGHT used to link sensor and configure policies

Deployment Architecture



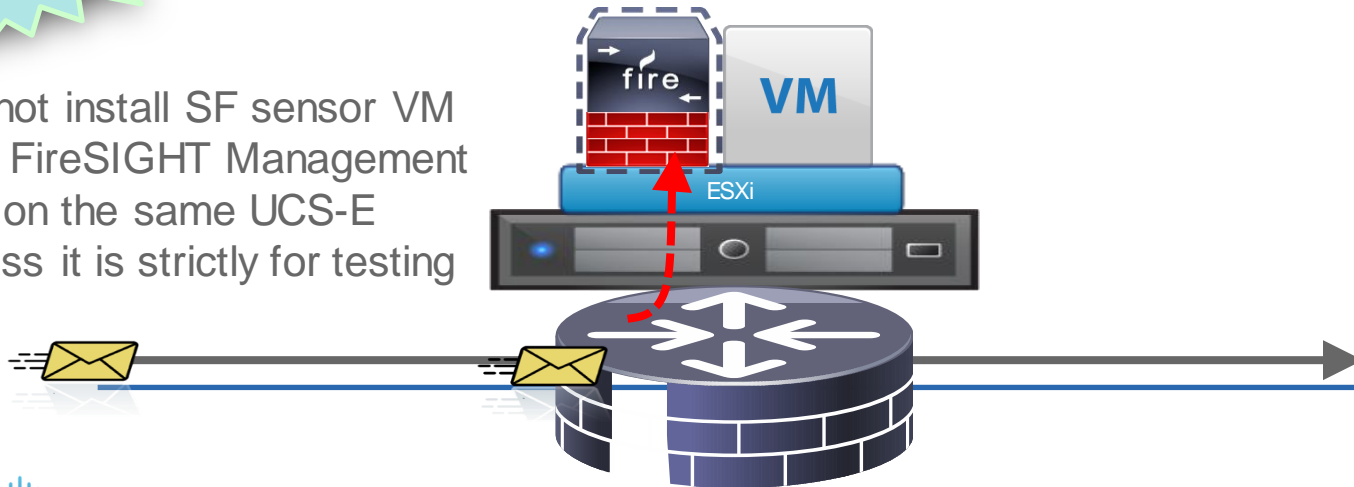
FireSIGHT Management Center Model	Max. Devices
FS Virtual	25
FS 750	10
FS 1500	35
FS 3500	150
FS 4000	300
* FS (Roadmap)	3000

Cisco FirePOWER Threat Defense for ISR- IDS

- Host the Sensor on the UCS-E
- Replicate and push all the traffic to be inspected to the Sensor
- FirePOWER sensor examines traffic

Caution

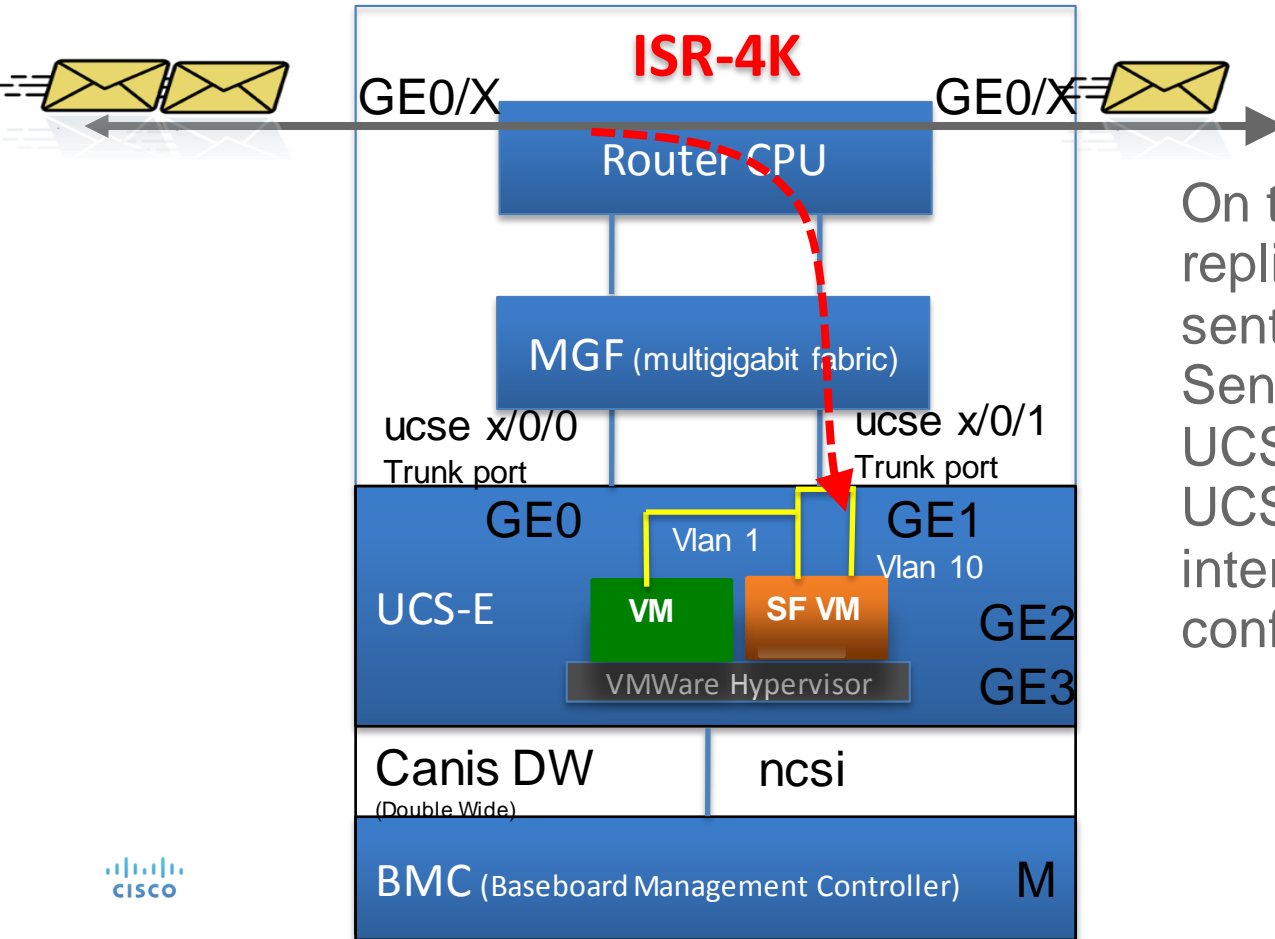
Do not install SF sensor VM and FireSIGHT Management VM on the same UCS-E unless it is strictly for testing



Cisco FirePOWER Threat Defense for ISR – ISR G2 side limitation

- Multicast is not supported
- IPV6 traffic is not supported
- With NAT apply UTD* on the inside NAT interface
- When IP traffic export is enabled, delay is incurred due to RITE *
 - UTD – Unified Threat Defense
 - RITE – Router IP Traffic Export

IDS packet flow on ISR 4K



On the ISR-4K, the replicated traffic can be sent to SourceFire Virtual Sensor using either UCSEx/0/0 interface or UCSEx/0/1 interface, both interfaces can be configured as trunk ports

Cisco FirePOWER Threat Defense for ISR

ISR 4K side limitation

- Multicast is not supported
- IPV6 traffic is not supported
- With NAT apply UTD on the inside NAT

Cisco FirePOWER Threat Defense for ISR— Configuration Steps

- Configure CIMC
- Install ESXi on UCS-E
- Install Vsphere Client
- Spin Sourcefire sensor VM
- Configure vswitches on ESXi
- Deploy FireSIGHT as a VM
- ADD sensor VM to FireSIGHT
- Apply license to FireSIGHT (IPS&Apps, AMP and URL)
- Configure UCS-E (backplane) interface on the router
- Configure UTD to replicate traffic to the sensor

Cisco FirePOWER Threat Defense for ISR— Configuration Steps

Configure CIMC

```
unknown# scope cimc
unknown /cimc # scope network
unknown /cimc/network # set dhcp-enabled no
unknown /cimc/network *# set dns-use-dhcp no
unknown /cimc/network *# set mode dedicated --->mode dedicated when MGMT port is used
unknown /cimc/network *# set v4-addr 172.16.1.8
unknown /cimc/network *# set v4-netmask 255.255.255.0
unknown /cimc/network *# set v4-gateway 172.16.1.1
unknown /cimc/network *# set preferred-dns-server 64.102.6.247
unknown /cimc/network *# set hostname kusankar-4451-UCS-E
unknown /cimc/network *# commit -----> make sure to commit to save the changes
```

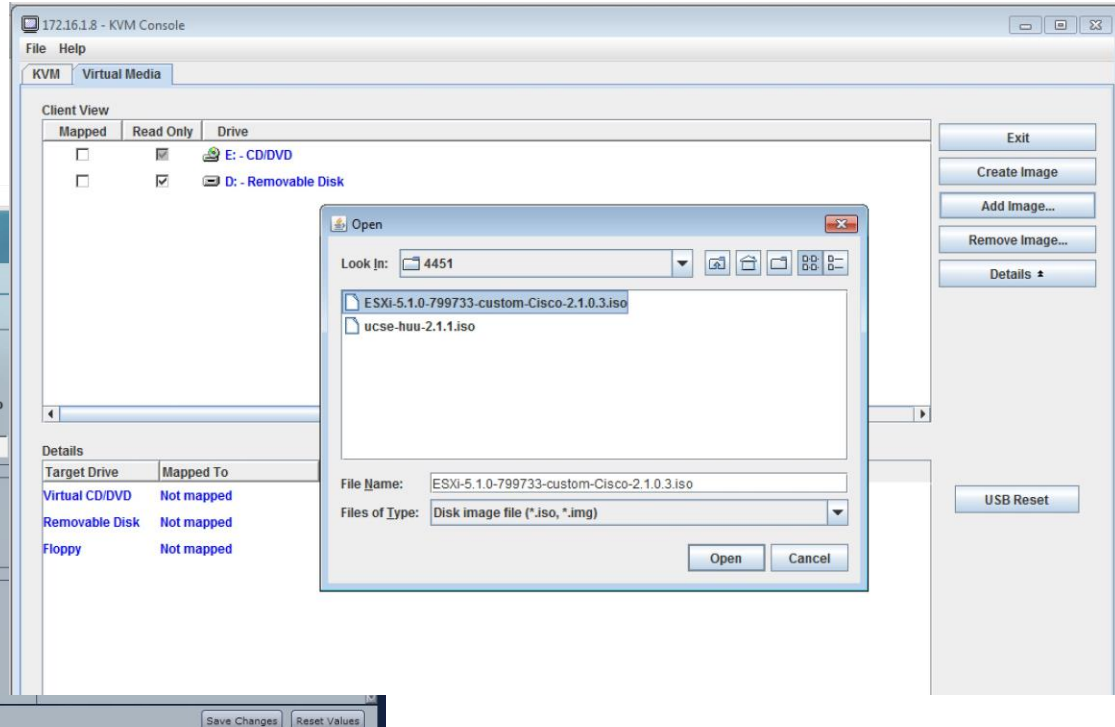
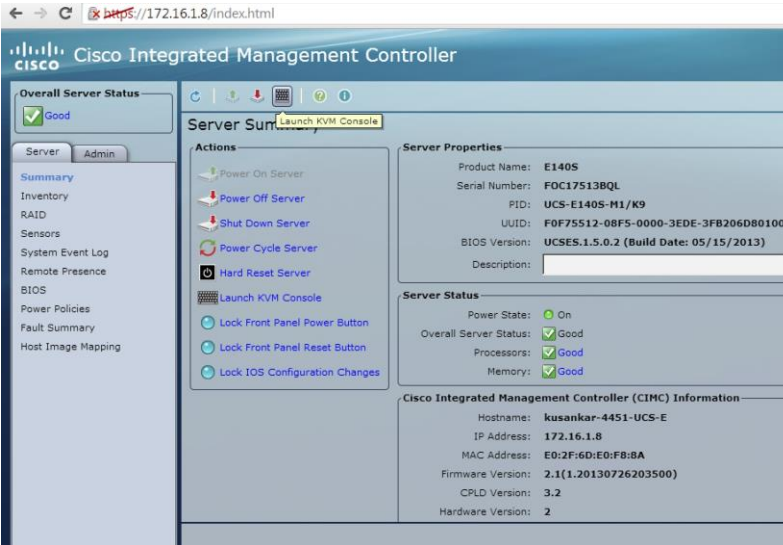
Make sure to use the right command to session into CIMC from the router

```
ISR-4K#hw-module subslot 2/0 session imc
```

```
ISR-G2#ucse subslot 1/0 session imc
```

Cisco FirePOWER Threat Defense for ISR— Configuration Steps

Install ESXi on UCS-E



Cisco FirePOWER Threat Defense for ISR— Configuration Steps

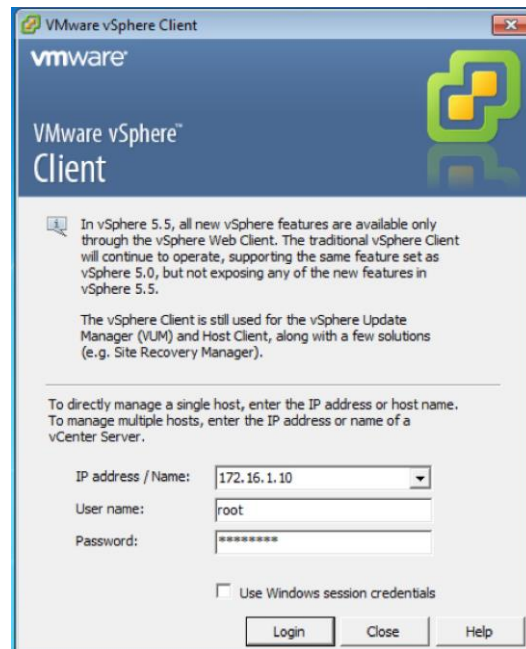
Install Vsphere Client

Double-Wide UCS-E – 4 interfaces

- First highest MAC address is the Gig 3 interface
- Second highest MAC address interface is Gig 2 interface
- The other two are internal ucse interfaces

Single-Wide UCS-E – 3 interfaces

- Highest MAC address interface is Gig 2 interface
- The other two are internal ucse interfaces.

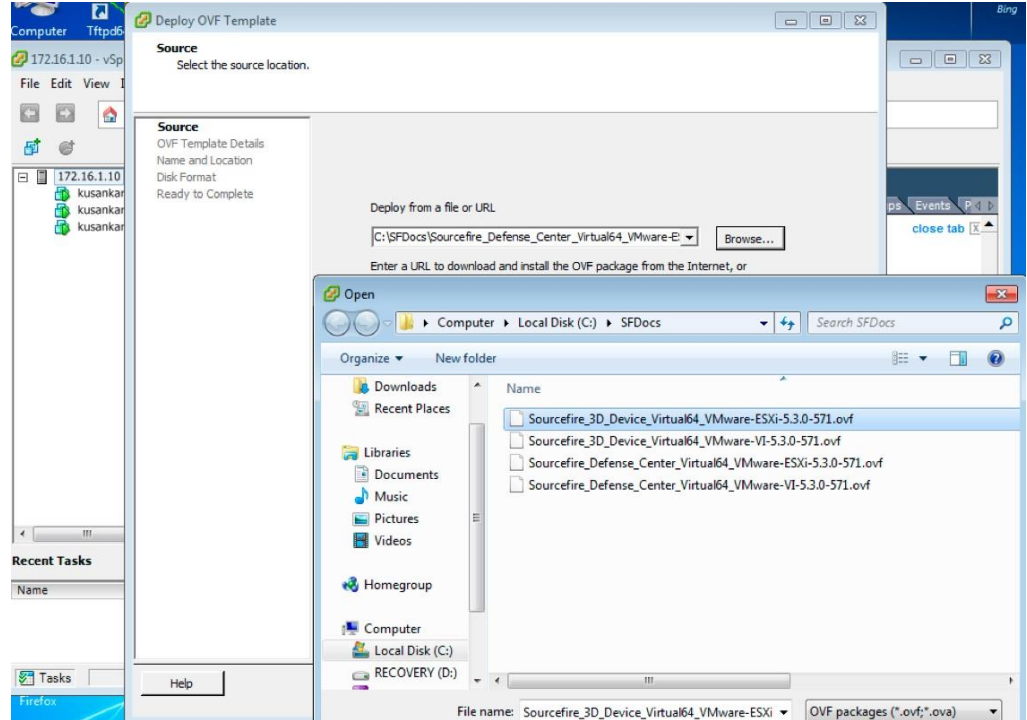


Cisco FirePOWER Threat Defense for ISR— Configuration Steps

Spin Sensor OVF

Download image
from here:

https://support.sourcefire.com/sections/1/sub_sections/54#5-3-virtual-appliances



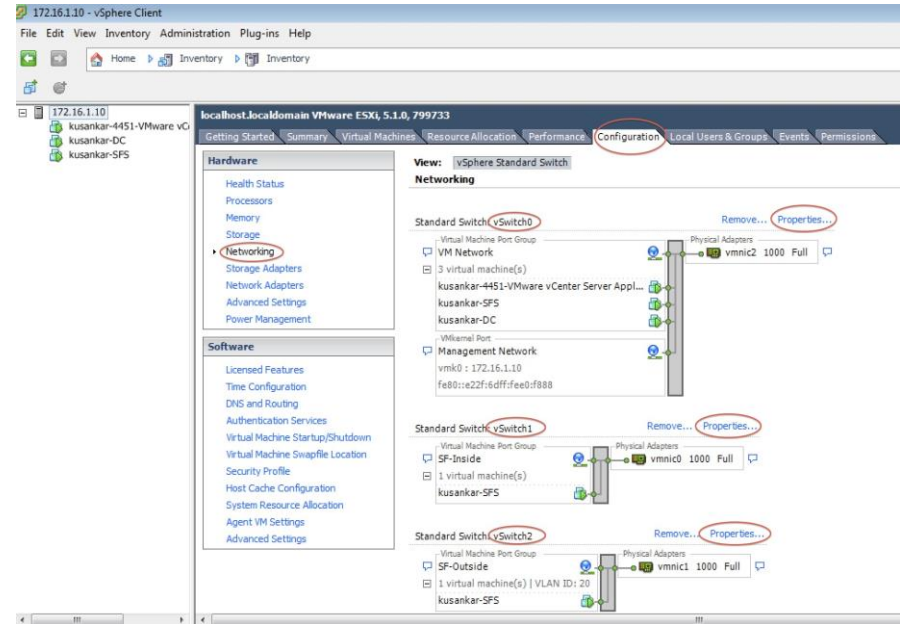
Cisco FirePOWER Threat Defense for ISR— Configuration Steps

Configure vswitches on ESXi

Both UCS-E interfaces on the ISR4K are trunk ports.

UCS-E 120S and 140S, have 3 Network Adaptors + Mgmt Port
vmnic0 is mapped to UCSEx/0/0 on the router backplane
vmnic1 is mapped to UCSEx/0/1 on the router backplane
vmnic2 is mapped to UCS-E front plane GE2 interface
front-panel management (M) port can only be used for CIMC

UCS-E 140D, 160D, and 180D have 4 Network Adaptors:
vmnic0 is mapped to UCSEx/0/0 on the router backplane
vmnic1 is mapped to UCSEx/0/1 on the router backplane
vmnic2 is mapped to UCS-E front plane GE2 interface
vmnic3 is mapped to UCS-E front plane GE3 interface
front-panel management (M) port can only be used for CIMC



Cisco FirePOWER Threat Defense for ISR— Configuration Steps

Spin FireSIGHT Manager VM

Download image from here:

https://support.sourcefire.com/sections/1/sub_sections/54#5-3-1-virtual-appliances

```
login as: admin
Using keyboard-interactive authentication.
Password:
Last login: Tue May 27 23:59:46 2014

Copyright 2001-2013, Sourcefire, Inc. All rights reserved. Sourcefire is
a registered trademark of Sourcefire, Inc. All other trademarks are
property of their respective owners.

Sourcefire Linux OS v5.3.0 (build 52)
Sourcefire Virtual Defense Center 64bit v5.3.0 (build 571)

admin@Sourcefire3D:~$ sudo su
Password:

root@Sourcefire3D:/var/home/admin# cd /usr/local/sf/bin
root@Sourcefire3D:/usr/local/sf/bin# ./configure-network

Do you wish to configure IPv4? (y or n) y

Management IP address?      172.16.1.9
Management netmask?        255.255.255.0
Management default gateway? 172.16.1.1

Are these settings correct? (y or n) y

Do you wish to configure IPv6? (y or n) n
Updated network configuration.
Updated comms. channel configuration.
Please go to https://172.16.1.9/ or https://[]/ to finish installation.
```

Cisco FirePOWER Threat Defense for ISR— Configuration Steps

ADD sensor VM to FireSIGHT

ADD FireSIGHT to Sensor VM

The screenshot shows the Cisco FirePOWER web interface. The 'Devices' tab is selected in the top navigation bar. A modal dialog titled 'Add Device' is open. The 'Host' field contains '172.16.1.6', the 'Registration Key' is 'cisco123', the 'Group' is set to 'None', and the 'Access Control Policy' is 'Default Access Control'. Below these fields, there is a 'Licensing' section with checkboxes for 'Protection', 'Control', 'Malware', 'URL Filtering', and 'VPN', all of which are currently unchecked. At the bottom of the dialog, there is an 'Advanced' section that is collapsed. The 'Register' button is highlighted in blue, and the 'Cancel' button is in grey.

```
> configure manager add 172.16.1.9 cisco123  
Manager successfully configured.
```

Cisco FirePOWER Threat Defense for ISR— Configuration Steps

Apply license to FireSIGHT (IPS-Apps, AMP and URL)

The screenshot displays the Cisco FirePOWER Threat Defense configuration interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', and 'FireAMP'. The 'System' tab is selected, and the 'Licenses' sub-tab is active. A red arrow points to the 'Add New License' button in the top right corner. The main content area shows the 'Add Feature License' form. The 'License Key' field contains the value '66:00:0C:29:B8:09:80'. A red arrow points to this field. The 'License' field contains a long alphanumeric string representing the license key. Below the license key, there are three buttons: 'Get License', 'Verify License', and 'Submit License'. The 'Submit License' button is highlighted with a red circle. Below the buttons, there is a note: 'If your web browser cannot access the Internet, you must switch to a host with Internet access and navigate to <https://keyserver.sourcefire.com>. Using the license key, 66:00:0C:29:B8:09:80, follow the on-screen instructions to generate a license.' At the bottom of the form, there is a 'Return to License Page' button.

Cisco FirePOWER Threat Defense for ISR— Configuration Steps

Configure UCS-E (backplane) interface on the router - ISR-G2

```
utd
ids redirect interface Vlan10
ids 000c.2923.abdc (mac address of the sensor interface) ←
!
interface ucse1/0
no ip address
imc ip address 10.122.160.173 255.255.255.128 default-gateway 10.122.160.129
imc access-port dedicated
!
interface ucse1/1
description Internal switch interface connected to Service Module
switchport mode trunk
no ip address
```

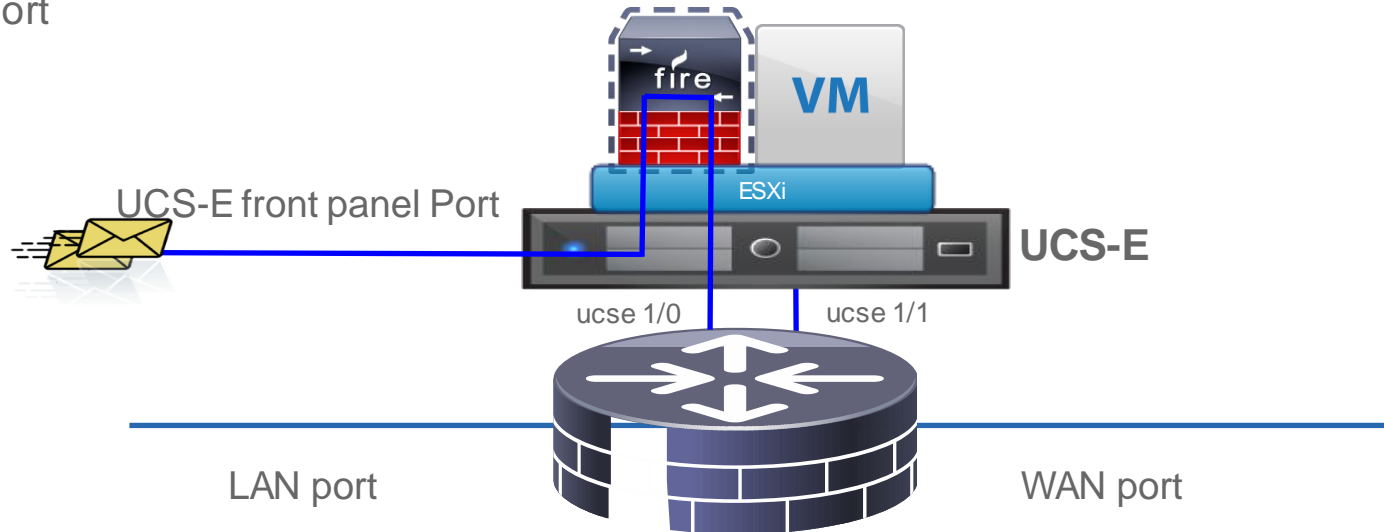
Cisco FirePOWER Threat Defense for ISR— Configuration Steps

Configure UCS-E (backplane) interface on the router – ISR 4K

```
interface ucse2/0/0
  no ip address
  no negotiation auto
  switchport mode trunk
  service instance 1
    ethernet encapsulation untagged bridge-domain 1
  !
interface BDI1
  ip unnumbered GigabitEthernet0/0/1
end
!
utd
  mode ids-global ids
  redirect interface BDI1
```

Cisco FirePOWER Threat Defense for ISR- IPS

- Host the Sensor on the UCS-E
- IPS is in inline mode
- Packets ingress via the UCS-E front panel port
- SF sensor examines traffic; allowed packets egress the WAN interface



Cisco FirePOWER Threat Defense for ISR-IPS using Front Panel Ports

- LAN to WAN traffic that needs to be inspected arrive on the front panel port of the UCS-E blade. Allowed packet upon Source Fire sensor inspection, egress out via the backplane and out the WAN interface.
- WAN to LAN traffic ingress on router's WAN interface, forwarded to the backplane, get inspected by Source Fire and egress out the front panel port on the UCS-E.
- Fail-Open can be achieved with a second connection between the router's interface and the switch.

Cisco FireSIGHT Provides Unmatched Visibility for Accurate Threat Detection and Adaptive Defense

The screenshot displays the Cisco FireSIGHT interface with several overlapping windows. On the left, a 'CATEGORIES' sidebar lists various threat types: Threats, Users, Web Applications, File Transfers, Malware, Command & Control, Client Applications, Network Servers, Operating Systems, Routers & Switches, Mobile Devices, Printers, VoIP Phones, and Virtual Machines. Each category has a corresponding red label box.

The main area shows a 'Network Information' window with a pie chart titled 'Operating Systems'. The chart is divided into segments for various OSes, with 'Unix 8.1' being the largest. Other OSes listed include AIX 5.x, 5L 5.x, Windows Phone 7.5, Chromium 3701.81.2, Mac OSX 10.8, 1....8.3, Android 2.3.5, and Android 2.3.3, ... 4.4.

Below the pie chart, a table titled 'Operating Systems (2)' provides details for two entries:

Vendor	Product	Version
Linux	Linux	2.6
Google	Android	2.2, 2.3.4, 2.3.7

Another pie chart below shows 'Linux 4.10 ppc', 'Linux 6.3, 6.4', 'Linux 11.x, 12....3.04', and 'Linux 2.6' as segments, with 'Unix 9.0' also visible.

In the background, a table with columns 'Classification', 'Priority', and 'Event' is partially visible, showing entries like 'Privilege Gain' with 'high' priority and '7' event count.

FireSIGHT Management Center

Single console for event, policy, and configuration management

The screenshot displays the FireSIGHT Management Center interface. The top navigation bar includes tabs for Overview, Analysis, Policies, and Devices. The main content area is titled "Local > User Management" and contains sub-tabs for Users, User Roles, and Login Authentication. The "User Roles" tab is active, showing a form for configuring a user role. The form includes fields for Name and Description, and two sections for permissions: "Menu-Based Permissions" and "System Permissions".

Menu-Based Permissions

- Policies
 - Access Control
 - Access Control List
 - Modify Access Control Policy
 - Modify Administrator Rules
 - Modify Root Rules
 - Apply Intrusion Policies
 - Intrusion
 - Intrusion Policy
 - Modify Intrusion Policy
 - Rule Editor

System Permissions

- External Database Access
- Set this role to escalate to: Administrator

Buttons for Save and Cancel are located at the bottom of the form.

Sourcefire-provided



FireSIGHT - URL Filtering

- Dozens of Content Categories
- URLs Categorized by Risk

Editing Rule - Web Block List

The screenshot shows the configuration interface for a 'Web Block List' rule. At the top, the rule name is 'Web Block List', it is 'Enabled', and the action is 'Block'. Below this are tabs for 'Zones', 'Networks', 'VLAN Tags', 'Users', 'Applications', 'Services', 'URLs', 'Policy', 'Logging', and 'Comments'. The 'URLs' tab is active, showing three main sections: 'Categories and URLs', 'Reputations', and 'Selected URLs'. The 'Categories and URLs' section has a search bar and a list of categories including 'Any', 'Abortion', 'Abused Drugs', 'Adult and Pornography', 'Alcohol and Tobacco', 'Auctions', 'Bot Nets', 'Business and Economy', 'CDNs', 'Computer and Internet Info', and 'Computer and Internet Security'. The 'Reputations' section has a search bar and a list of risk levels: 'Any', '5 - Well known', '4 - Benign sites', '3 - Benign sites with security risks', '2 - Suspicious sites', and '1 - High risk'. An 'Add to Rule' button is located between the 'Reputations' and 'Selected URLs' sections. The 'Selected URLs' section has a search bar and a list of categories including 'Adult and Pornography (Any Reputation)', 'Bot Nets (Any Reputation)', 'Confirmed SPAM Sources (Any Reputation)', 'Gambling (Any Reputation)', 'Keyloggers and Monitoring (Any Reputation)', 'Malware Sites (Any Reputation)', 'Marijuana (Any Reputation)', 'Nudity (Any Reputation)', 'Open HTTP Proxies (Any Reputation)', 'Parked Domains (Any Reputation)', and 'Pay to Surf (Any Reputation)'. At the bottom right, there are 'Save' and 'Cancel' buttons.

FireSIGHT - AMP

Overview **Analysis** Policies Devices Objects FireAMP Health System Help admin

Context Explorer Connections Intrusions **Files > Network File Trajectory** Hosts Users Vulnerabilities Correlation Custom Search

Network File Trajectory for 0517f034...588e1374

File SHA-256 0517f034...588e1374

File Name [WindowsMediaInstaller.exe](#)

File Type MSEXE

File Category [Executables](#)

Current Disposition Malware

Threat Score ●●● High

First Seen 2013-12-06 10:57:13 on [10.4.10.183](#)

Last Seen 2013-12-06 18:17:27 on [10.4.10.183](#)

Event Count 7

Seen On 4 hosts

Seen On Breakdown 2 senders → 3 receivers

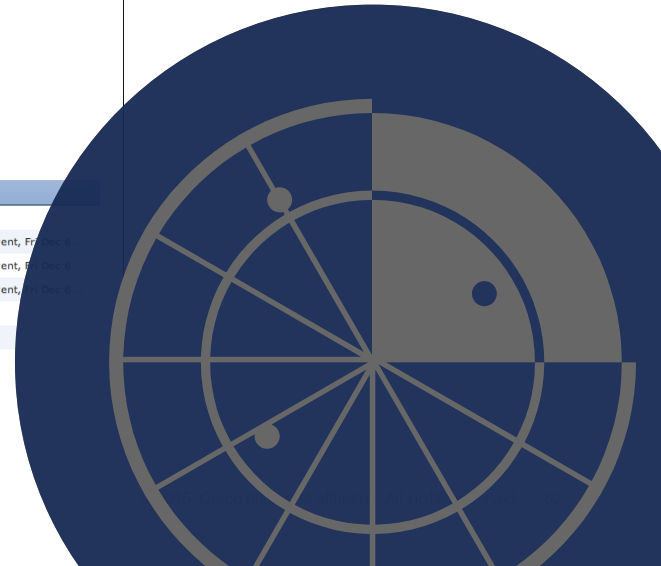
Trajectory

Events Transfer Block Create Move Execute Scan Retrospective Quarantine

Dispositions Unknown Malware Clean Custom Unavailable

Events

Time	Event Type	Sending IP	Receiving IP	File Name	Disp...	Action	Protocol	Client	Web Ap...	Description
2013-12-06 10:57:13	Retrospectiv...				Malwa...					
2013-12-06 17:40:28	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller...	Unkn...	Malware Cloud L...	HTTP	Firefox		Retrospective Event, F...
2013-12-06 18:06:03	Transfer	10.5.11.8	10.3.4.51	WindowsMediaInstaller...	Unkn...		NetBIOS...			Retrospective Event, T...
2013-12-06 18:10:03	Transfer	10.5.11.8	10.5.60.66	WindowsMediaInstaller...	Unkn...		NetBIOS...			Retrospective Event, T...
2013-12-06 18:14:10	Retrospectiv...				Malwa...					
2013-12-06 18:14:23	File Quaranti...		10.5.11.8	WindowsMediaInstaller...	Malwa...					
2013-12-06 18:17:27	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller...	Malwa...	Malware Block	HTTP	Firefox		



Network File Trajectory for 0517f034...588e1374

File SHA-256 0517f034...588e1374

File Name [WindowsMediaInstaller.exe](#)

File Type [MSEXE](#)

File Category [Executables](#)

Current Disposition Malware

Threat Score High

First Seen 2013-12-06 10:57:13 on [10.4.10.183](#)

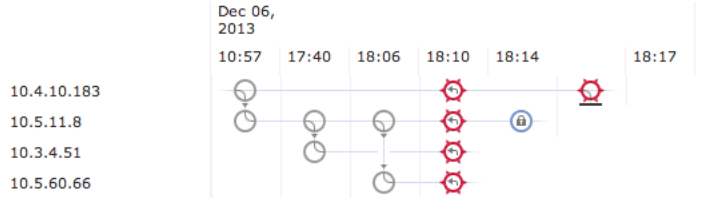
Last Seen 2013-12-06 18:17:27 on [10.4.10.183](#)

Event Count 7

Seen On 4 hosts

Seen On Breakdown 2 senders → 3 receivers

Trajectory



Events Transfer Block Create Move Execute Scan Retrospective Quarantine

Dispositions Unknown Malware Clean Custom Unavailable

Events

Time	Event Type	Sending IP	Receiving IP	File Name	Disp...	Action	Protocol	Client	Web Ap...	Description
2013-12-06 10:57:13	Retrospectiv...				Malwa...					
2013-12-06 17:40:28	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Unkn...	Malware Cloud L...	HTTP	Firefox		Retrospective Event, Fri Dec 6 ...
2013-12-06 18:06:03	Transfer	10.5.11.8	10.3.4.51	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:10:03	Transfer	10.5.11.8	10.5.60.66	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:14:10	Retrospectiv...				Malwa...					
2013-12-06 18:14:23	File Quaranti...		10.5.11.8	WindowsMediaInstaller....	Malwa...					
2013-12-06 18:17:27	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Malwa...	Malware Block	HTTP	Firefox		

Polling Question 4

How important it
is to enable
HTTPS
inspection/
decryption?

1. No. It is not. HTTPS is secure
2. Yes. HTTPS connections are secure, NOT safe
3. HTTPS traffic does not discriminate against malicious or compromised servers

Resources

Resources

- Router Security – FirePOWER Threat Defense for ISR

<http://www.cisco.com/c/en/us/products/security/router-security/firepower-threat-defense-isr.html>

- Configuration Guide - FirePOWER Threat Defense for ISR

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_utd/configuration/xs-3s/sec-data-utd-xe-3s-book.html#concept_0AC4C1AE8D714F1C9533FD3B383EC8AF



Submit Your Questions Now!

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

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>



Please take a moment to complete the survey

Thank you for Your Time!



CISCO

TOMORROW starts here.