Cisco Support Community

Expert Series Webcast

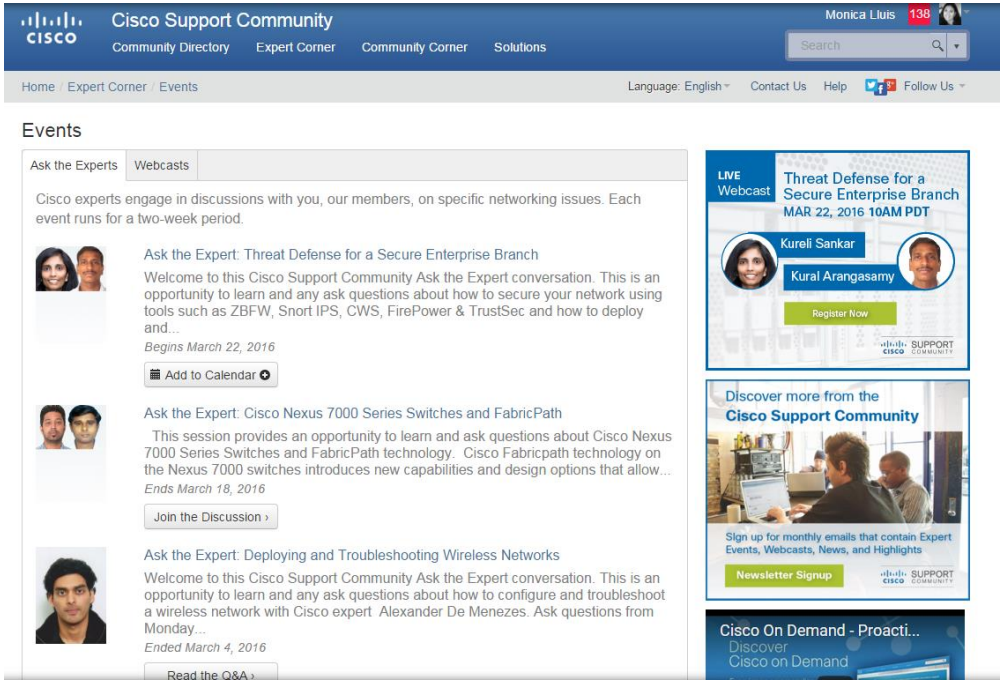
Threat Defense for a Secure Enterprise Branch

Kureli Sankar, TME, CCIE Security #35505
Kural Arangasamy, TME

March 22, 2016

Upcoming Events

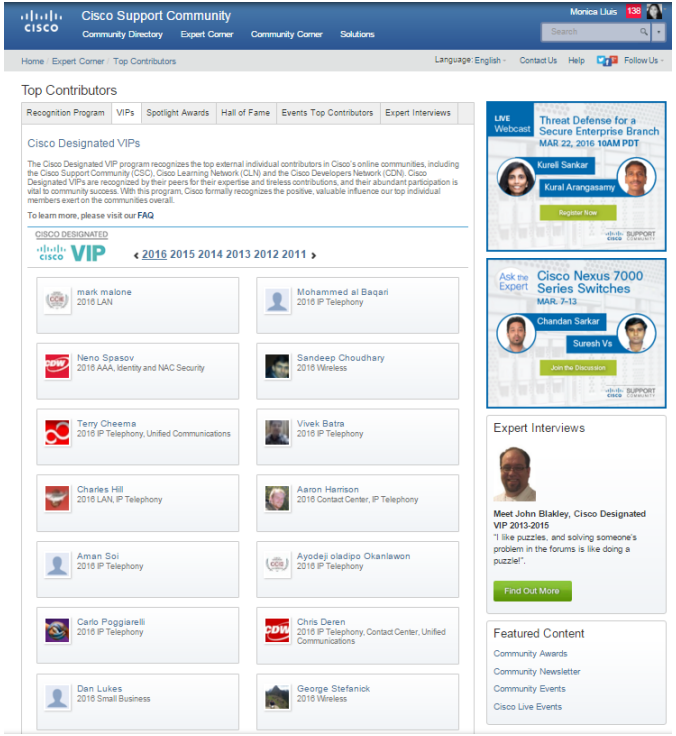
https://supportforums.cisco.com/expert-corner/events



Become an Event Top Contributor

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

If you want to host an event, send an email to csc-events@external.cisco.com



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

Kureli Sankar

TME, Enterprise Infrastructure and Solutions Group
CCIE Security # 35505

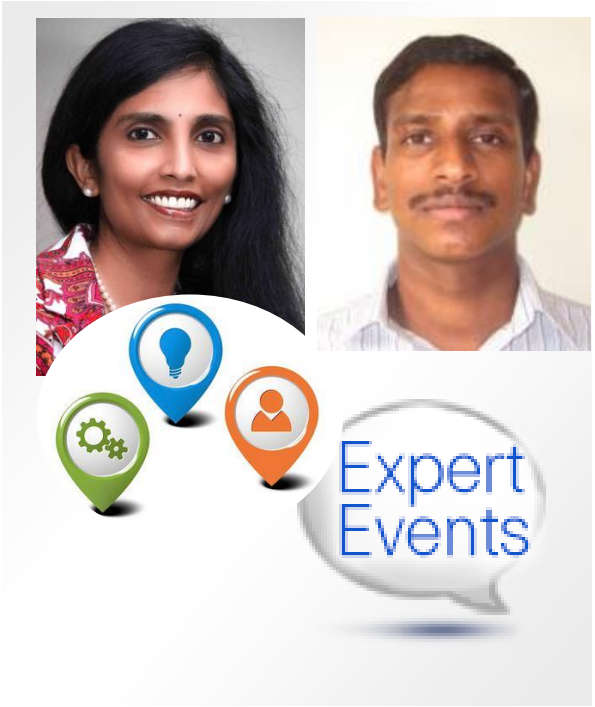
Kural Arangasamy

TME, Enterprise Infrastructure and Solutions Group

Ask the Expert Event following the Webcast

Now through April 1st

https://supportforums.cisco.com/discussion/12753631/ask-expert-threat-defense-secure-enterprise-branch



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/12936416/webcas-slidest-threat-defense-secure-enterprise-branch

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

Threat Defense for a Secure Enterprise Branch

Kureli Sankar, TME, CCIE Security #35505

Kural Arangasamy, TME

March 22, 2016

Agenda

- Security Features
  - Zone Based Firewall
  - Snort IPS
  - CWS
  - FirePOWER
- Demo

Polling Question 1

How important is Branch Threat Defense in your opinion?

A. Very important
B. Important
C. Somewhat important
D. Not important at all

Digitization is Happening at the Branch

More Users

80%

Of employee and customers are served in branch offices*

More Devices

73%

Growth in mobile devices from 2014–2018**

More Apps

20–50%

Increase in Enterprise bandwidth per year through 2018**

"By 2016, **30%** of advanced targeted threats–up from less than **5%** today–will specifically target **branch offices** as an entry point."

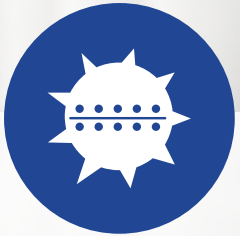
Changes at the Branch Lead to Security Challenges

Increased Threat Surface Area

Mobile, Cloud, IoT, DIA

Increased Threat Sophistication

Average time to discover 80 days*



Increased Complexity for Mitigation

Average time to resolve 123 days

*Ponemon Institute Study
**Gartner, Forecast Analysis: Worldwide Enterprise Network Services, Q2 2014 Update
*** Gartner: "Bring Branch Office Network Security Up to the Enterprise Standard, Jeremy D'Hoinne, 26 April. 2013.

The Approach to Securing Your Branch – Threat Centric Security

Secure Connectivity

Advanced Threat Defense

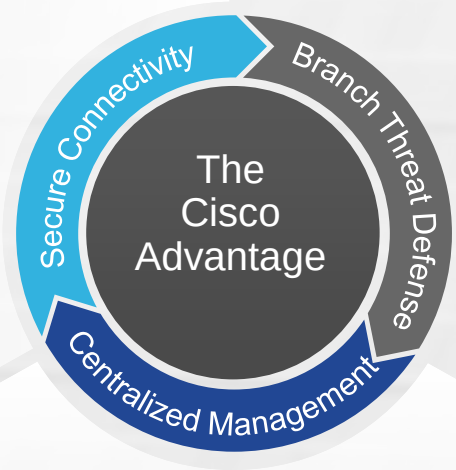
Centralized Policy Management

Visibility & Defense Across the Entire Attack Continuum

Cisco’s Branch Security Solution

Secure Connectivity

- Dynamic Multipoint VPN (DMVPN)
- SSL VPN
- AnyConnect and SSL VPN
- Site to Site IPsec
- NaaS/NaaE
- IWAN



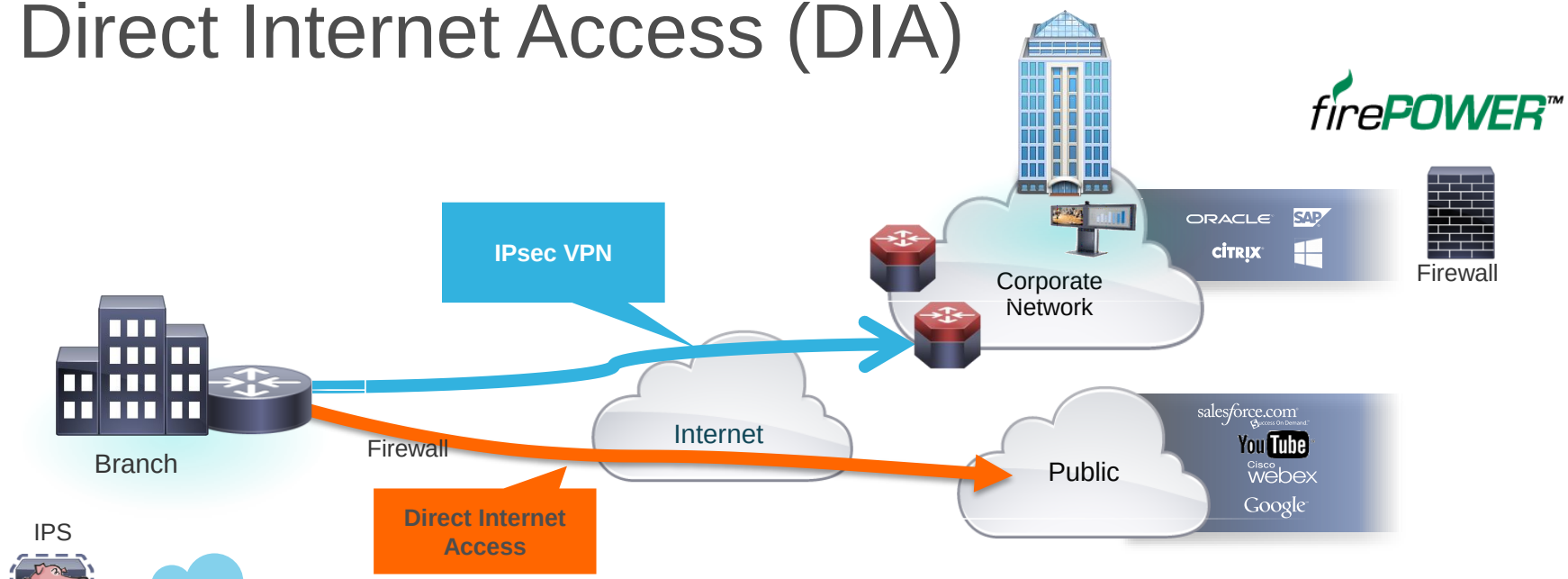
Branch Threat Defense

- Cisco IOS Zone-Based Firewall
- Snort IPS
- FirePOWER threat defense
- Cloud Web Security (CWS)

Centralized Policy and Management

- APIC-EM
- Cisco Prime
- FireSIGHT Management Center

Direct Internet Access (DIA)

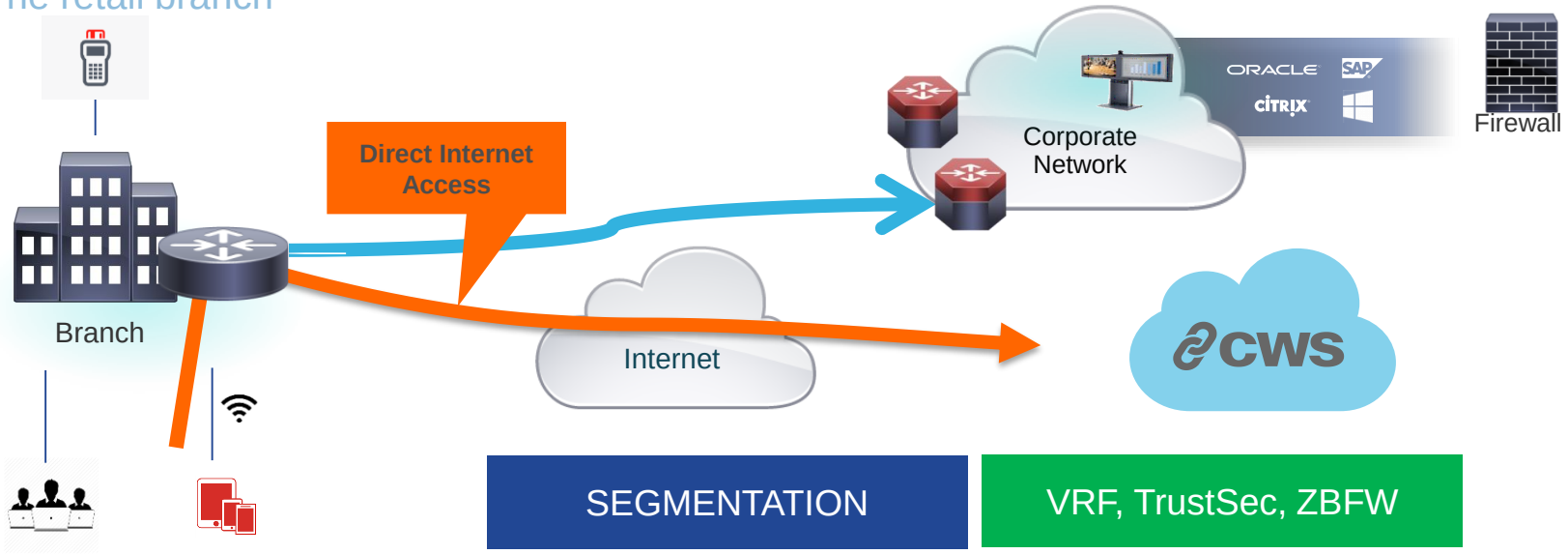


- Secure WAN transport
- Leverage local Internet path
- Threat Detection techniques
- Improve application performance
- Reduced WAN bandwidth consumption

cisco

Direct Internet Access

The retail branch



SEGMENTATION	VRF, TrustSec, ZBFW
PCI COMPLIANCE	ZBFW, SNORT IPS
GUEST WEB ACCESS	CWS

Agenda

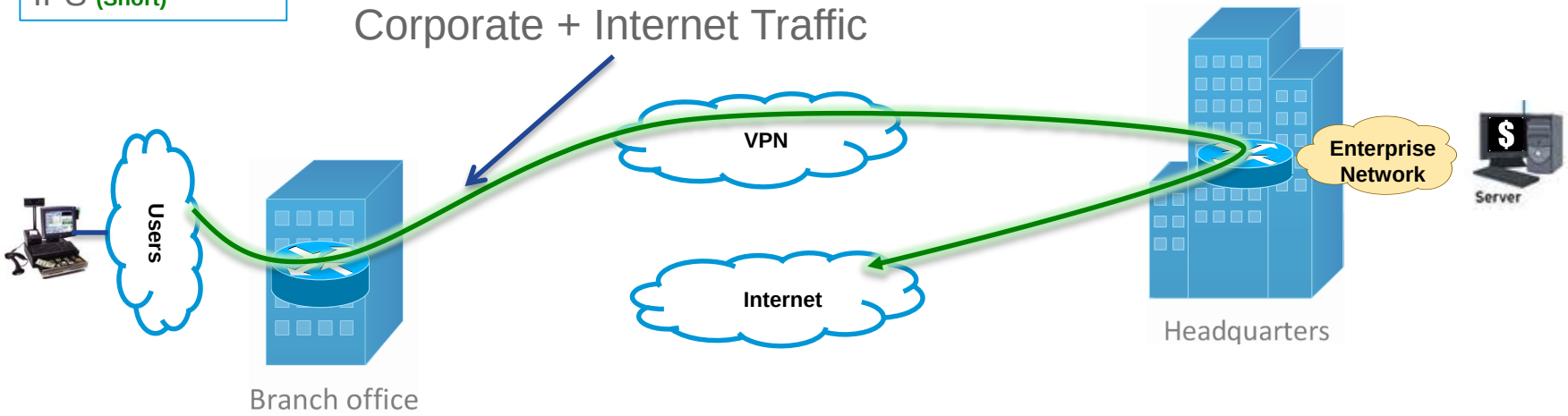
- Security Features
  - Zone Based Firewall
  - Snort IPS
  - CWS
  - FirePOWER
- Demo

Use Cases

Use Case	Vertical	Security Requirements	Technology
PCI and Regulatory Compliance	Retail, Healthcare, Financial, Government	FW, IPS, Content Filtering (optional)	ZBFW, Snort IDS/IPS, CWS
Guest Users Internet Access	Retail, Healthcare, Hospitality	FW, Web Security, IPS (optional)	ZBFW, Snort IDS/IPS, CWS

Use Case: Secure Branch to Meet Compliance Needs

MVP
FW **(ZBFW)**
IPS **(Snort)**



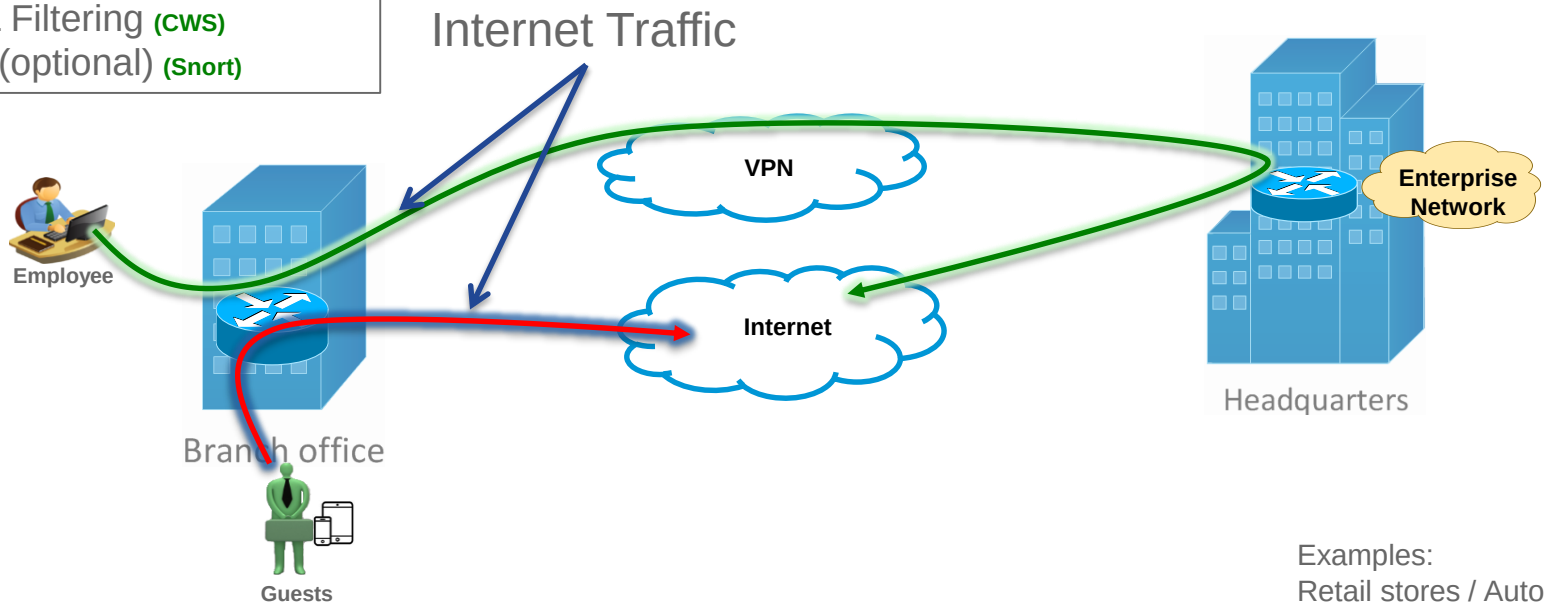
Value Prop

- Best of Routing & Security at Head Quarters
- Good Enough Security at the Branch to Meet Compliance
- Snort IPS at the Branch
- Advanced Behavior Analysis at the Head-end

Examples:
Retail stores
Hospitals / Pharmacies

Use Case: Secure Branch Guest Internet Access

MVP
FW/NGFW **(ZBFW)**
URL Filtering **(CWS)**
IPS (optional) **(Snort)**



Value Prop

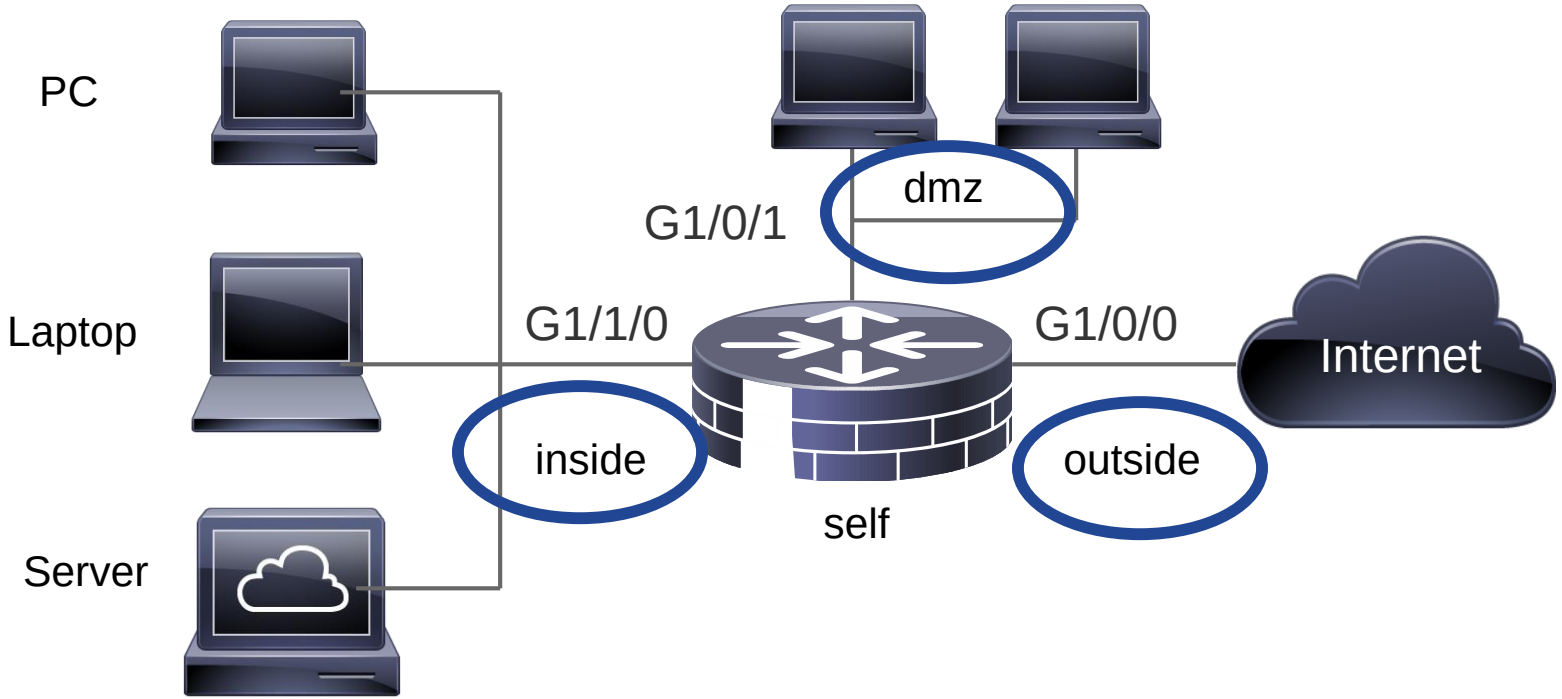
- Best of Routing & Security at Head Quarters
- Good Enough Security at the Branch to Restrict Guest Access
- Advanced Behavior Analysis at the Head-end

Examples:
Retail stores / Auto Dealerships
Hospitals / Pharmacies
Financials
Schools / Universities

Zone Based Firewall

- Segmentation
- Stateful Firewall
- DoS Mitigation
- Resource Management

Zone Based Firewall



23

Step.1 Classify traffic

```
class-map type inspect match-any in-to-out-class
  match protocol ftp
  match protocol tcp
  match protocol udp
!
```

Step.2 Define actions in Policy map

```
policy-map type inspect in-to-out-pol
 class type inspect in-to-out-class
   inspect
 !
 class type inspect class-default
  drop log → logging is optional
```

Step.3 Define Security Zones

```
zone security inside
zone security outside
!
Interface GigabitEthernet 1/0/0
  Description ***connect-to-Internet***
  Zone-member security outside
!
Interface GigabitEthernet 1/1/0
  Description ***connect-to-private***
  Zone-member security inside
```

Step.4 Define inter-Zone Rules

```
Zone-pair security inside-to-outside source inside destination
outside
 service-policy type inspect in-to-out-pol
```


24

Appendix

- ZBF – Zone Based Firewall
- DMZ – Demilitarized Zone
- DoS – Denial Of Service

ZBF - Resources

ZE SYN cookie configuration guide:
http://www.cisco.com/en/US/docs/ios-xml/ios/sec_data_zbf/configuration/xe-3s/asr1000/conf-fw-tcp-syn-cookie.html

XE - Zone Based Firewall configuration guide:
http://www.cisco.com/en/US/docs/ios-xml/ios/sec_data_zbf/configuration/xe-3s/asr1000/sec-zone-pol-fw.html

IOS - Zone Based Firewall configuration guide:
http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_zbf/configuration/15-mt/sec-data-zbf-15-mt-book.html

ISR TCP intercept configuration guide:
http://www.cisco.com/en/US/docs/ios/sec_data_plane/configuration/guide/sec_cfg_tcp_intercpt.html

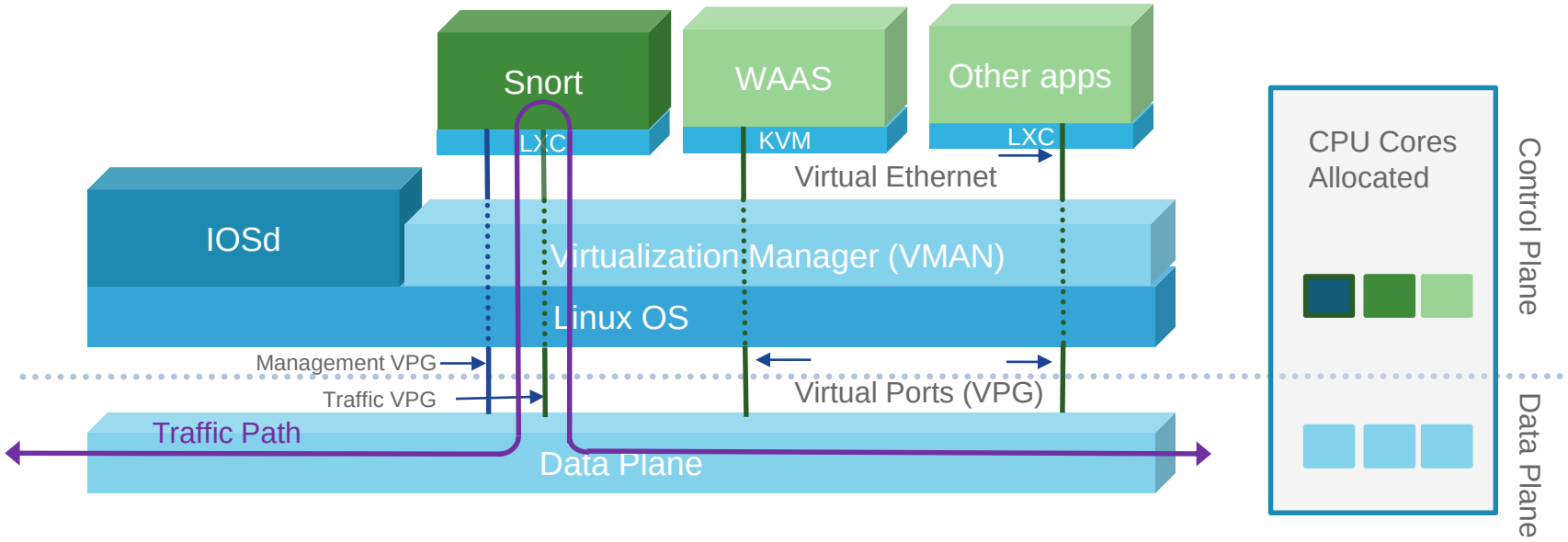
Snort IPS/IDS on ISR-4K

Snort IPS

- Over 4 million downloads
- 500,000 registered users
- Widely deployed IPS in the world

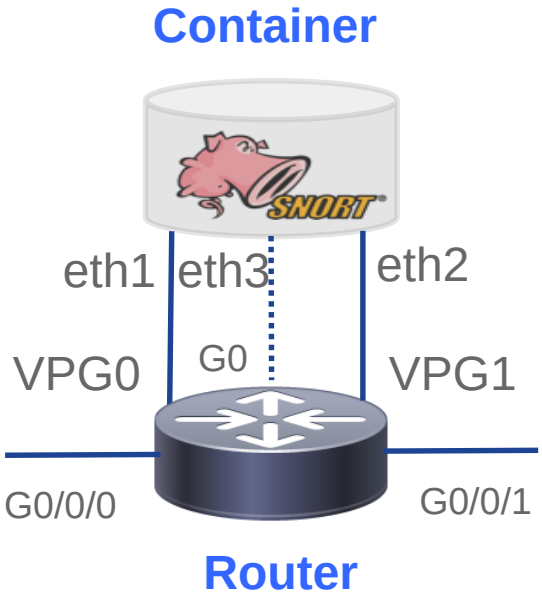
- Help meet PCI compliance mandate at the Branch Office
- Threat protection built into ISR 4000 branch routers
- Complement ISR 4000 Integrated Security
- Lightweight Threat Defense with low TCO and automated signature updates
- splunk> monitoring available

Snort IPS – Container Architecture



- Snort IPS runs on a Linux Container using control plane resources
- Traffic is punted to Snort Container using Virtual Port Group interface
- Reserved CPU and memory for Snort process enables deterministic performance

Snort Configuration –Virtual Service Networking



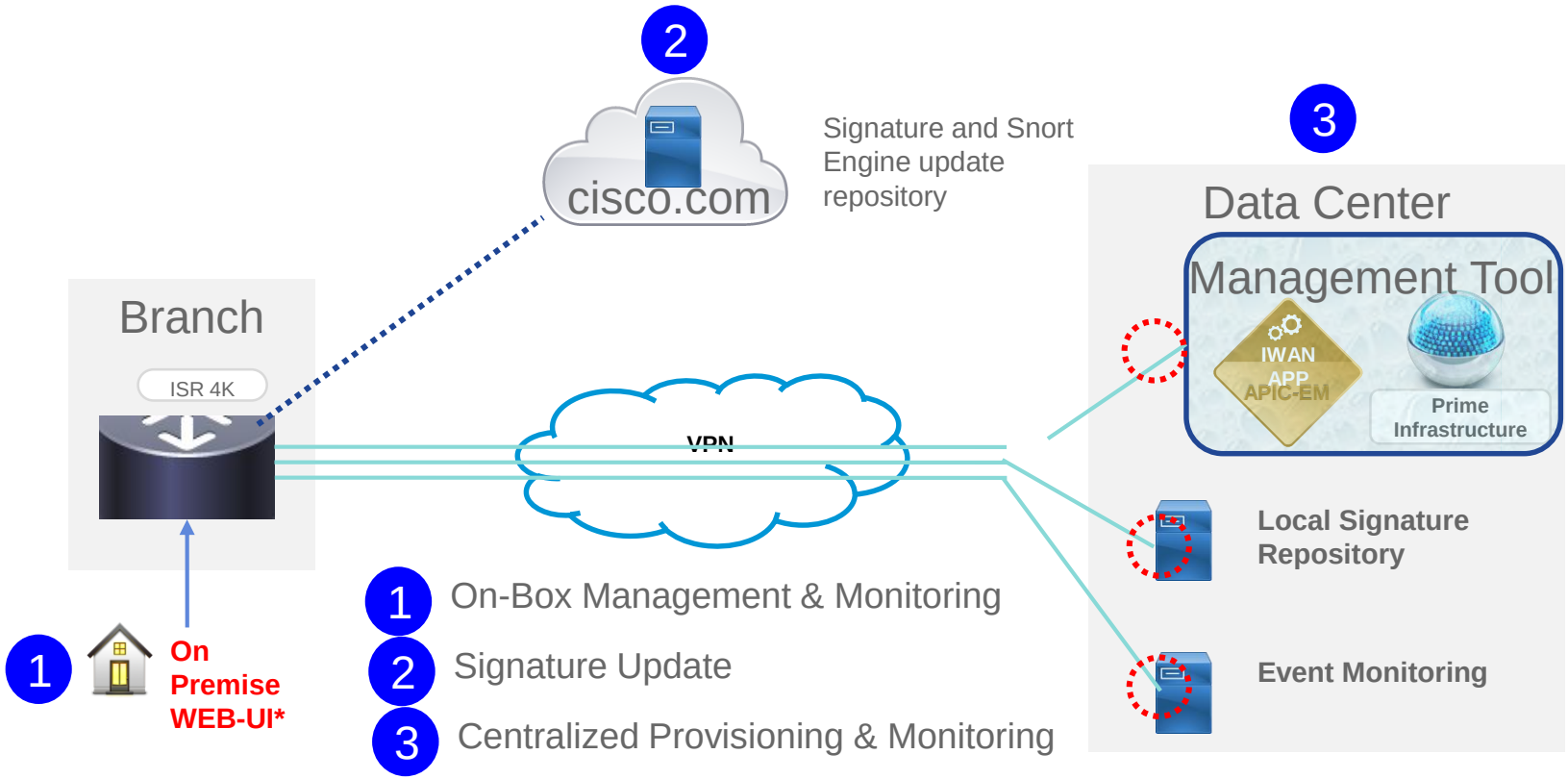
- VPGs to communicate between container and data plane
- VPG1 <==> eth2 (data plane)

- VPG0 <==> eth1 (management)

[OR]

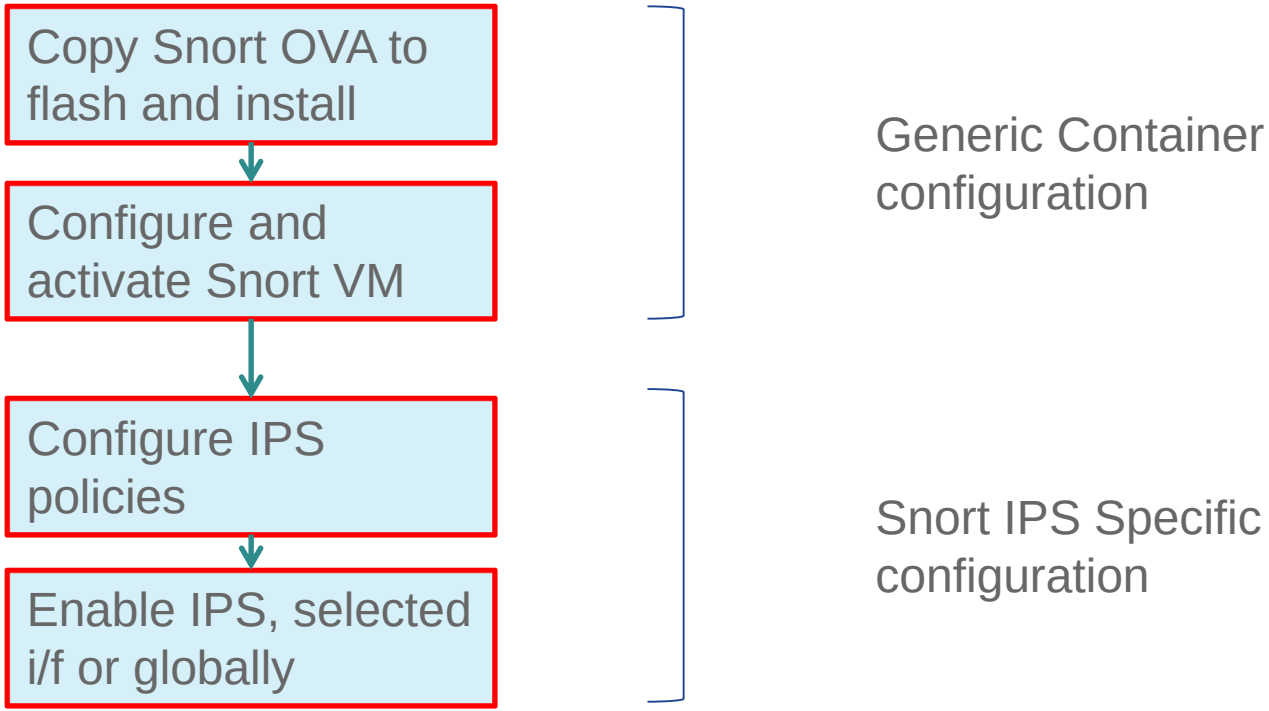
- eth3 can be mapped to dedicated mgmt port G0 of the router

Snort IPS – Management & Monitoring



* Web UI will be available in a future release

Snort IPS – Configuration Steps



Configuration – Virtual Service Activation

Exec Mode:

```
virtual-service install name myips package flash:ios-snort.ova
```

Install virtual service

Config Mode:

```
interface VirtualPortGroup0
  ip address 10.0.1.1 255.255.255.252
interface VirtualPortGroup1
  ip address 192.0.2.1 255.255.255.252
```

Configure Virtual Interfaces

Config Mode:

```
virtual-service myips
 profile high
 vnic gateway VirtualPortGroup0
  guest ip address 10.0.1.2
 vnic gateway VirtualPortGroup1
  guest ip address 192.0.2.2
 activate
```

Configure Virtual Service Interfaces and activate the service

Configuration – IPS Policies

IPS Policy Configuration

```
utd engine standard
 threat protection
 policy security
 signature update server cisco username <uname> password <paswd>
 signature update occur-at daily 0 0
 logging server 10.0.20.20 syslog level warning
```

Enable IPS

```
utd
 engine standard
 all-interfaces
interface GigabitEthernet0/0/0
 utd enable
```

Snort - Community vs Subscriber Rule Set

1. Memory – 8 G RAM
2. License – SEC-K9
3. Subscription
4. Container OVA installation
5. Container service activation
6. Enabling IPS/IDS
7. Enable Snort configuration
8. Reporting
9. Signature updates
10. Ability to whitelist

	Community Rule Set	**Subscriber Rule Set**
Pricing	free	paid
Number of rules	3000+	30,000+
Coverage in advance of exploits	No	Yes
Signature availability	30 days later	Fastest access to Talos signature updates
Snort Engine “Latest-1” compatibility	90 days only	
SLA	No	
Level 3 support	No	Bugzilla

Snort – Troubleshooting Commands

show virtual-service list
show utd engine standard config
show virtual-service detail
show platform hardware qfp active feature utd stats
show platform hardware qfp active feature utd config
show platform hardware qfp active feature utd stat divert

Snort – Debug Commands

debug platform packet copy packet out size 2048
debug platform packet-trace enable
debug platform packet-trace packet 64 circular fia-trace

Note: Conditional debugging needs to be enabled along with packet tracing

debug platform condition interface g0/0/0 both
debug platform condition start

Note: Optionally the utd debugging can be enabled along with packet tracing
debug platform condition feature utd dataplane submode divert level info

Appendix

- VPG – Virtual Port Group
- DIA – Direct Internet Access
- CSR - Cloud Services Router
- WL – White Listing
- OVA – Open Virtual Appliance
- UTD – Unified Threat Defense
- APIC-EM – Application Policy Infrastructure Controller – Enterprise Module
- IWAN – Intelligent WAN

Snort IPS/IDS - Resources

At-A-Glance

http://www.cisco.com/c/dam/en/us/products/collateral/security/router-security/at-a-glance-c45-735895.pdf

Data Sheet

http://www.cisco.com/c/en/us/products/collateral/security/router-security/datasheet-c78-736114.html

Agenda

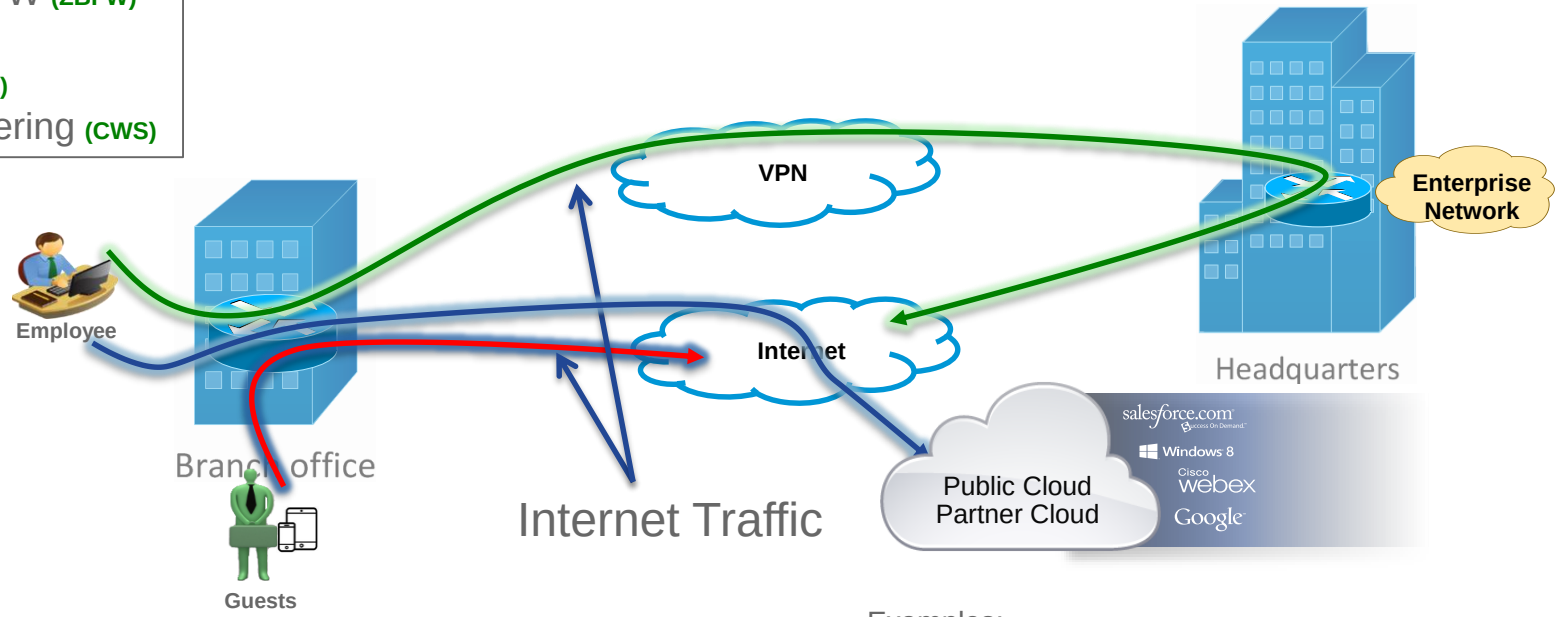
- Security Features
  - Zone Based Firewall
  - Snort IPS
  - CWS
  - FirePOWER
- Demo

Use Cases

Use Case	Vertical	Security requirements	Security Technology
Guest Users Internet Access	Retail, Healthcare, Public Sector	FW, Web Security, IPS (optional)	ZBF, CWS and Snort IDS/IPS
Partial Direct Internet Access (Public Cloud, Partner Sites)	Retail, Healthcare, Manufacturing	FW, Web Security, IPS	ZBF, CWS, Snort IDS/IPS **[OR]** ZBF and FirePOWER Threat Defense

Use Case: Secure Branch Public Cloud / Partner Access

MVP
FW/NGFW **(ZBFW)**
DBR
IPS **(Snort)**
URL Filtering **(CWS)**



Value Prop

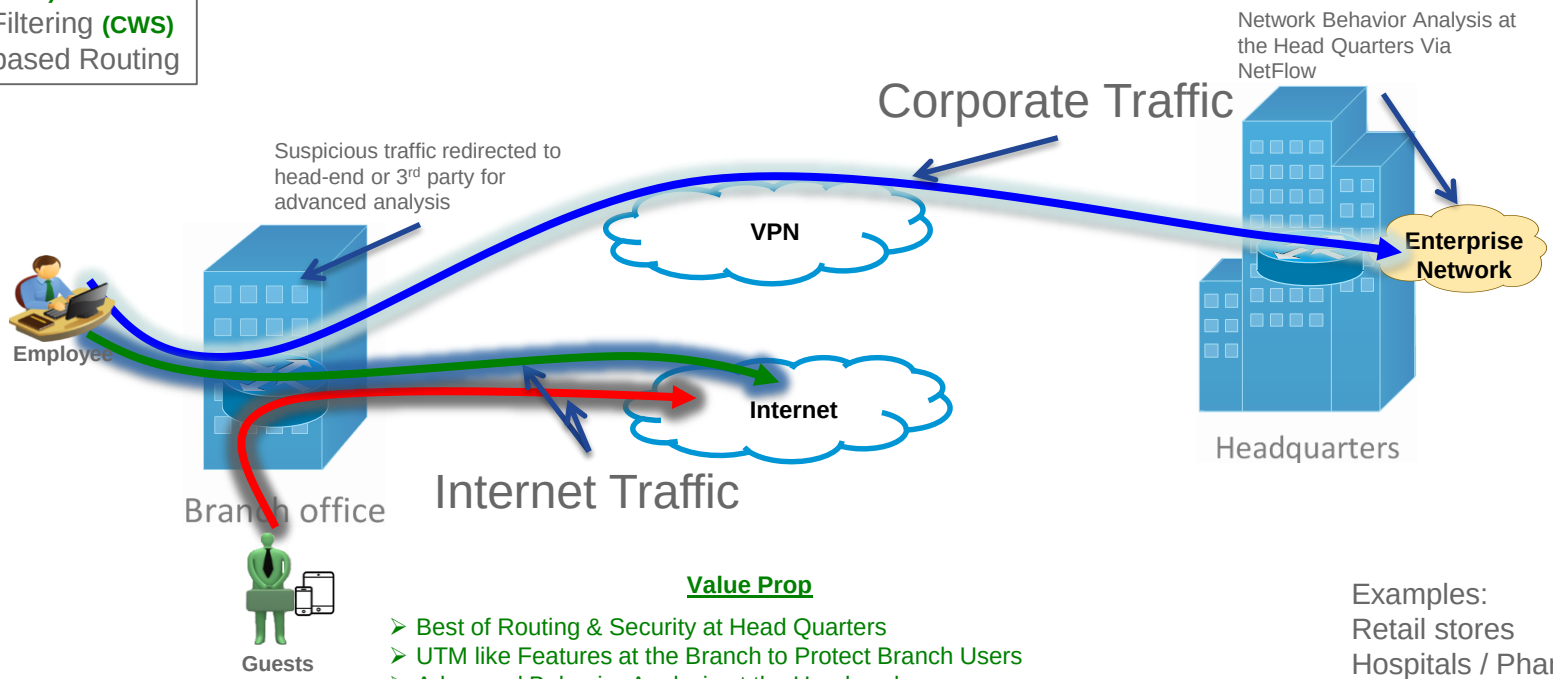
- Domain Based Routing, routes only the cloud specific traffic directly
- ZBFW provides pinholes for return traffic from cloud services
- CWS provides additional protection from cloud services
- Additional security services if needed (CWS AMP, CTA etc.)

Examples:
Retail Stores Accessing Supplier Websites
Hospital / Pharmacy Accessing Insurance websites
Cloud Based Enterprise Services (webex, salesforce etc.)

Use Case: Secure Branch Direct Internet Access

Integrated Cloud-based Threat Defense

MVP
NGFW **(ZBFW)**
IPS **(Snort)**
URL Filtering **(CWS)**
SGT based Routing



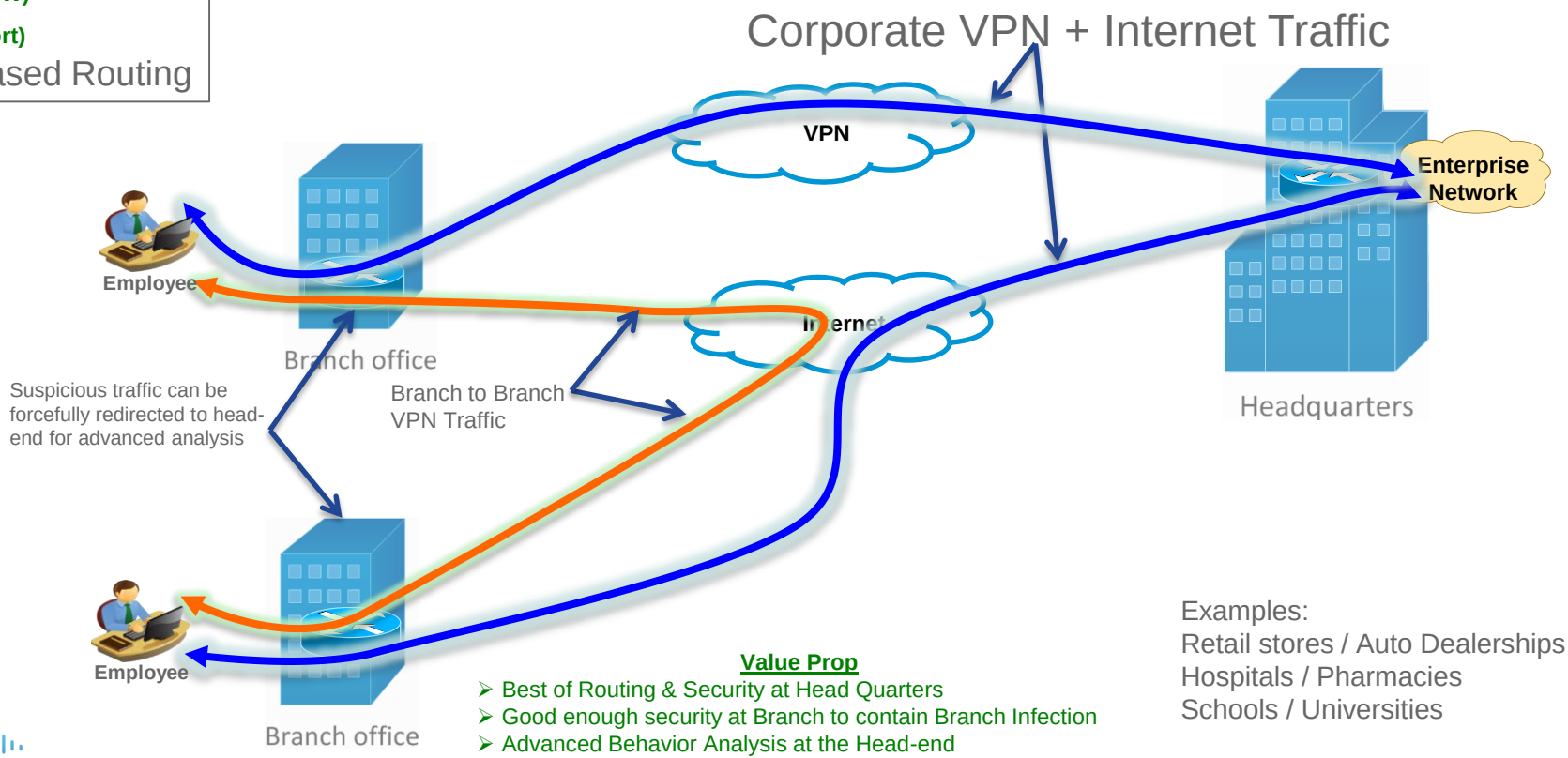
Value Prop

- Best of Routing & Security at Head Quarters
- UTM like Features at the Branch to Protect Branch Users
- Advanced Behavior Analysis at the Head-end
- Advanced dynamic routing at Branch to reroute suspicious users

Examples:
Retail stores
Hospitals / Pharmacies
Schools / Universities

Use Case: Branch to Branch Direct Access

MVP
FW **(ZBFW)**
IPS **(Snort)**
SGT based Routing



Value Prop

- Best of Routing & Security at Head Quarters
- Good enough security at Branch to contain Branch Infection
- Advanced Behavior Analysis at the Head-end

Examples:
Retail stores / Auto Dealerships
Hospitals / Pharmacies
Schools / Universities

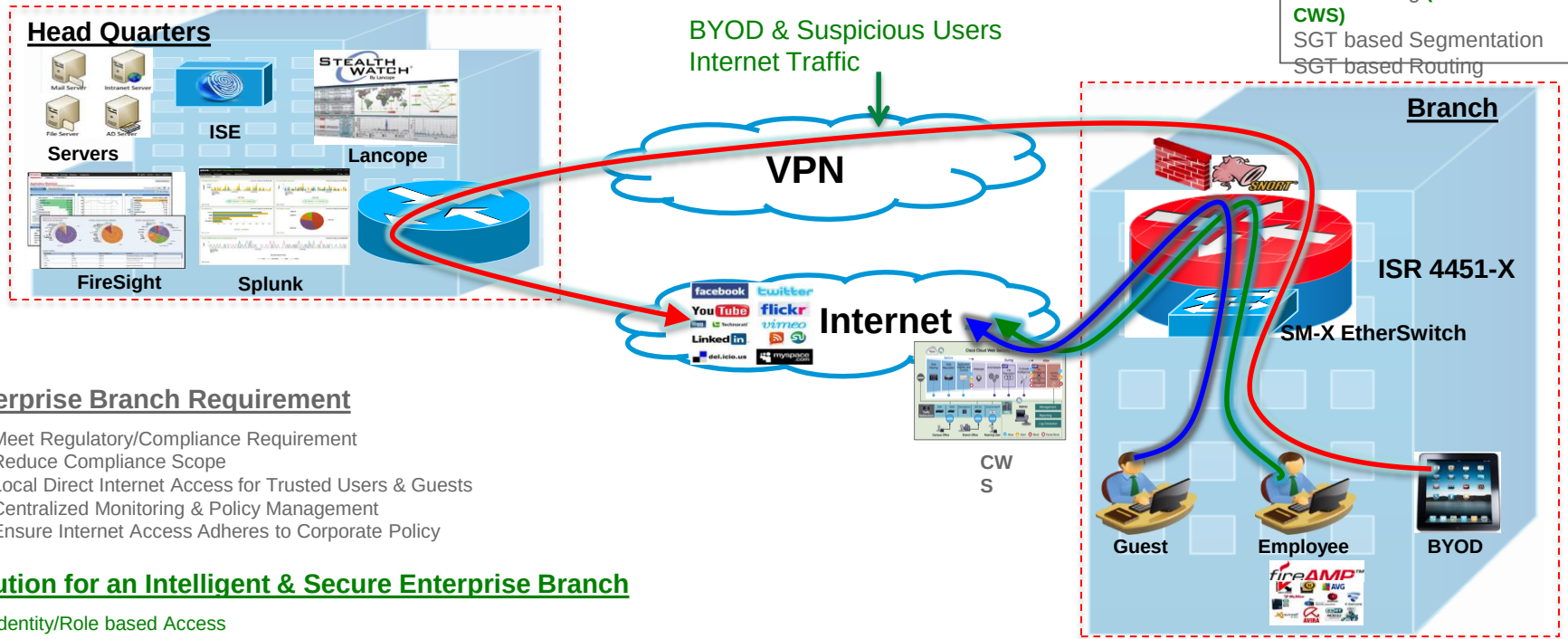
Advanced Architecture

Use Case: Context Aware Threat Defense for an Enterprise Branch

Network as a Sensor (NaaS) / Enforcer (NaaE), TrustSec, ZBFW, FirePOWER or Snort IPS, CWS

MVP
FW/NGFW **(ZBFW, FirePower)**
IPS **(Snort or FirePower)**
URL Filtering **(FirePower or CWS)**
SGT based Segmentation
SGT based Routing

Non-Compliant Devices & Suspicious Users Internet Traffic Redirection to HQ



Enterprise Branch Requirement

- Meet Regulatory/Compliance Requirement
- Reduce Compliance Scope
- Local Direct Internet Access for Trusted Users & Guests
- Centralized Monitoring & Policy Management
- Ensure Internet Access Adheres to Corporate Policy

Solution for an Intelligent & Secure Enterprise Branch

- Identity/Role based Access
- Segmentation & Security Policy Enforcement
- Advanced Flow Analytics
- Security Event Monitoring
- Policy based Traffic Redirect and QoS Management

Polling Question 2

What comes to your mind when we talk about BTD?
(check all that applies)

A. Regulatory compliance (ex. PCI-DSS)

B. Guest Internet Access

C. Public Cloud Access (ex. office 365, salesforce)

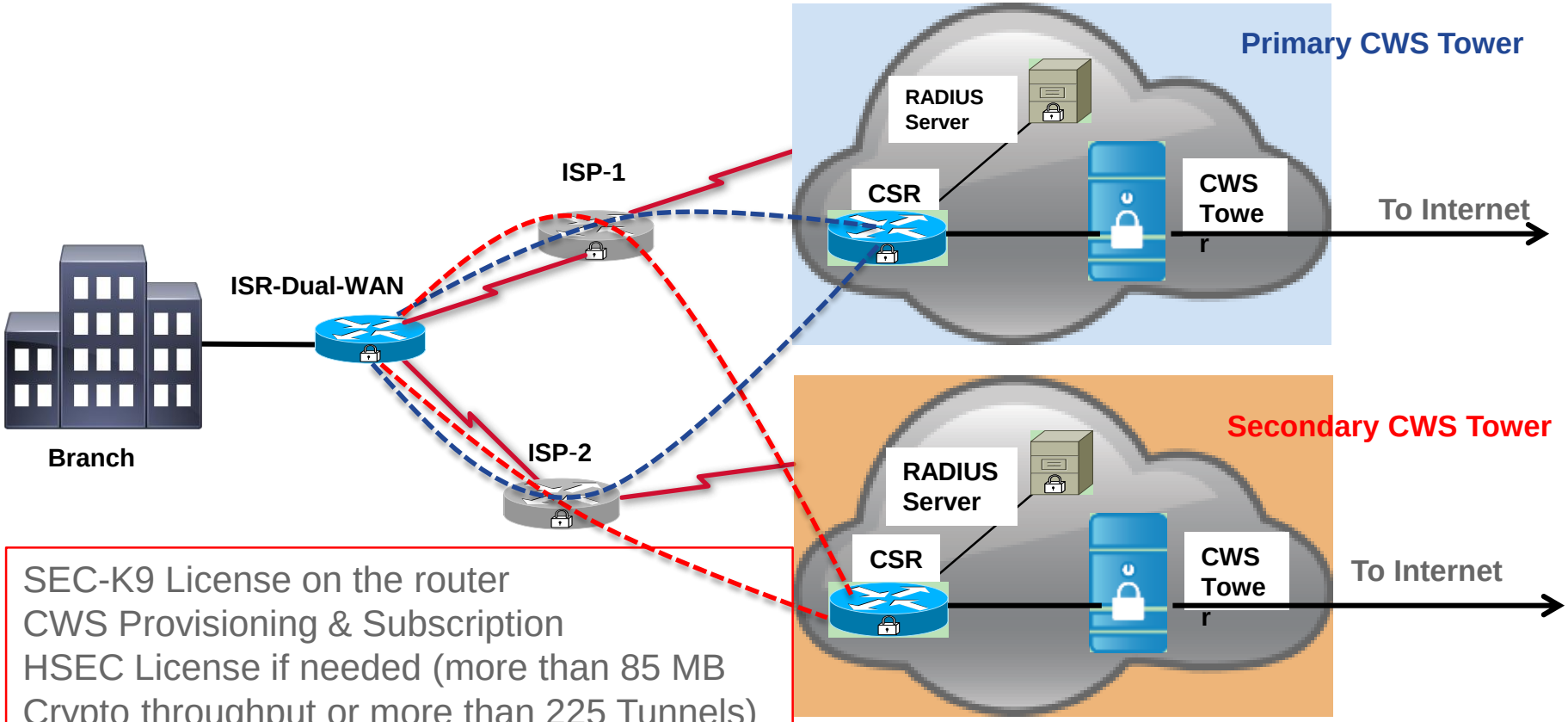
D. BYOD

Agenda

- Security Features
  - Zone Based Firewall
  - Snort IPS
  - CWS
  - FirePOWER
- Demo

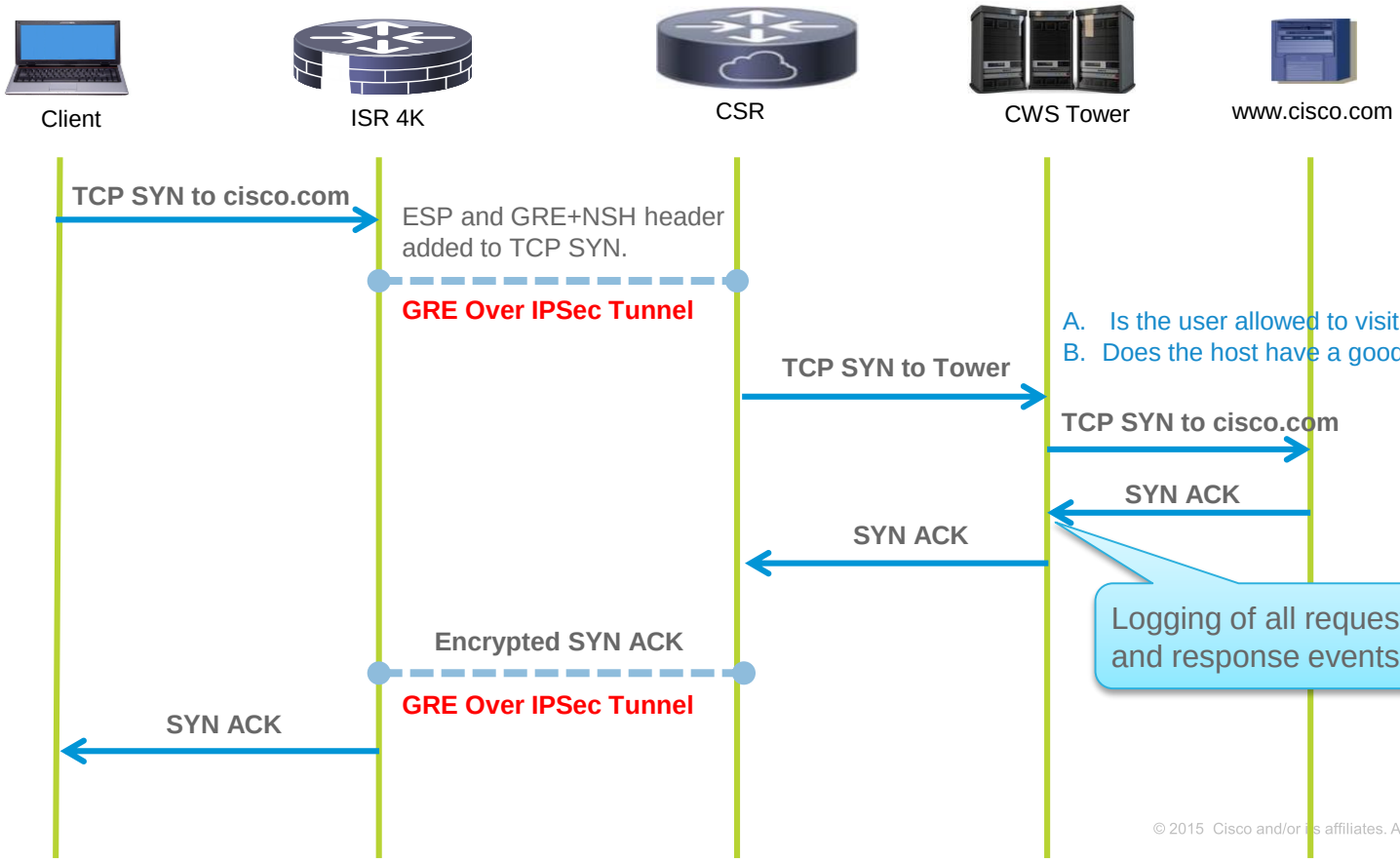
CWS (Cloud Web Security) on ISR-4K

CWS – Tunnel Based Redirection

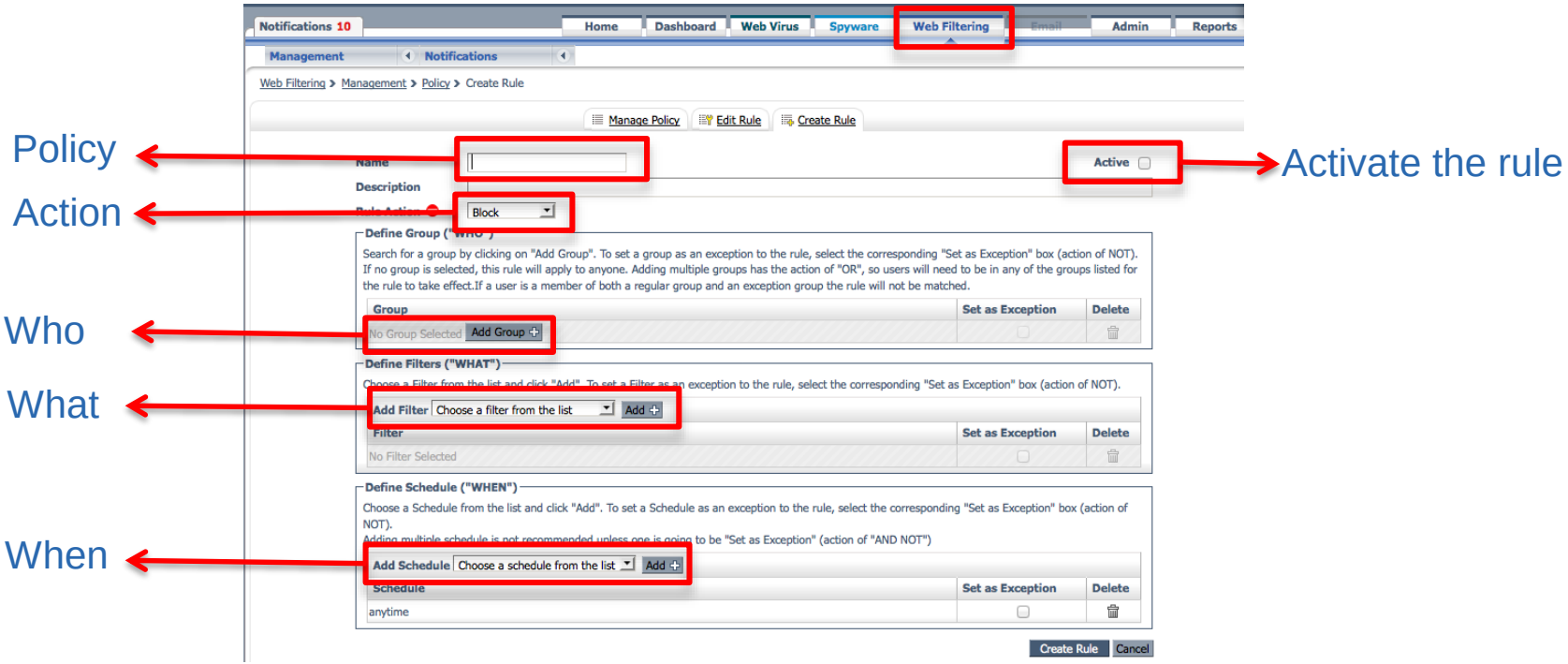


SEC-K9 License on the router
CWS Provisioning & Subscription
HSEC License if needed (more than 85 MB Crypto throughput or more than 225 Tunnels)

CWS – Tunnel Based Redirection Packet Flow



CWS: Policy creation on CWS portal



CWS - Tunnel Based Redirection Configuration

Step. 1 Import Certificate

```
Router(config)#crypto pki trustpoint cws-trustpoint
Router(ca-trustpoint)#revocation-check none
Router(ca-trustpoint)#enrollment terminal
Router(ca-trustpoint)#exit
Router(config)#cry pki authenticate cws-trustpoint
```

Step.2 Define a redirect list

```
Router(config)#access-list 80 per 10.10.20.0 0.0.0.255
```

Step.3 Define a whitelist (optional)

```
Router(config)#ip access-list extended cws-whitelist
Router(config-ext-nacl)#permit ip any 10.0.0.0 0.255.255.255
Router(config-ext-nacl)#permit ip any 172.16.0.0 0.15.255.255
Router(config-ext-nacl)#permit ip any 192.168.0.0 0.0.255.255
```

Step.4 Parameter Map

```
Router(config)#parameter-map type cws-tunnel global
Router(config-profile)# primary
Router(config-cws-pri)#  tower ipv4 108.171.130.255
Router(config-cws-pri)# secondary
Router(config-cws-sec)#  tower ipv4 108.171.133.254
Router(config-cws-sec)# license 0
947D9DC0781B425AED0BB0B30C345321
Router(config-profile)# redirect-list 80
Router(config-profile)# whitelist
Router(config-cws-tun-wl)#acl name cws-whitelist
Router(config-cws-tun-wl)#download interval 10
```

Step.5 Apply CWS OUT

```
Router(config)#int g0/0/2
Router(config-if)#cws-tunnel out tunnel-number 60
```

Step.6 Apply CWS IN

```
Router(config)#int g0/0/1
Router(config-if)#cws-tunnel in
```


61

CWS - Proxy VS Tunnel Connector

Features	Proxy ISR-G2 (IOS)	Tunnel ISR-4K (XE)
Redirection	Proxy	Tunnel
Telemetry	Yes	No (March 2016)
Tower Pooling	Yes	Through Tunnel Keepalives
MetaData	X-Scansafe Headers	NSH (Network Services Headers)
Whitelisitng	ACL & HTTP Headers Based	ACL & Domain Based
Authentication	Yes	No (March 2016)
Default User-Group	Yes	No

CWS – Resources

External – CCO Page: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_cws/configuration/xe-3s/sec-data-cws-xe-3s-book.html

CWS Tunnel Connector Step by Step: https://supportforums.cisco.com/document/12713171/isr-cws-tunnel-based-redirection-step-step-configuration

Appendix

- CWS – Cloud Web Security
- IWAN – Intelligent WAN
- CSR - Cloud Services Router
- RRI – Reverse Route Injection
- L4F – Layer 4 Forwarding
- AMP – Advance Malware Protection
- WL – White Listing

Polling Question 3

Are you interested in all integrated single box solution to provide FW, URL filtering, Advance Malware Protection and IPS/AVC?

A. Yes, I prefer single box

B. No, I prefer different boxes to do each job

Agenda

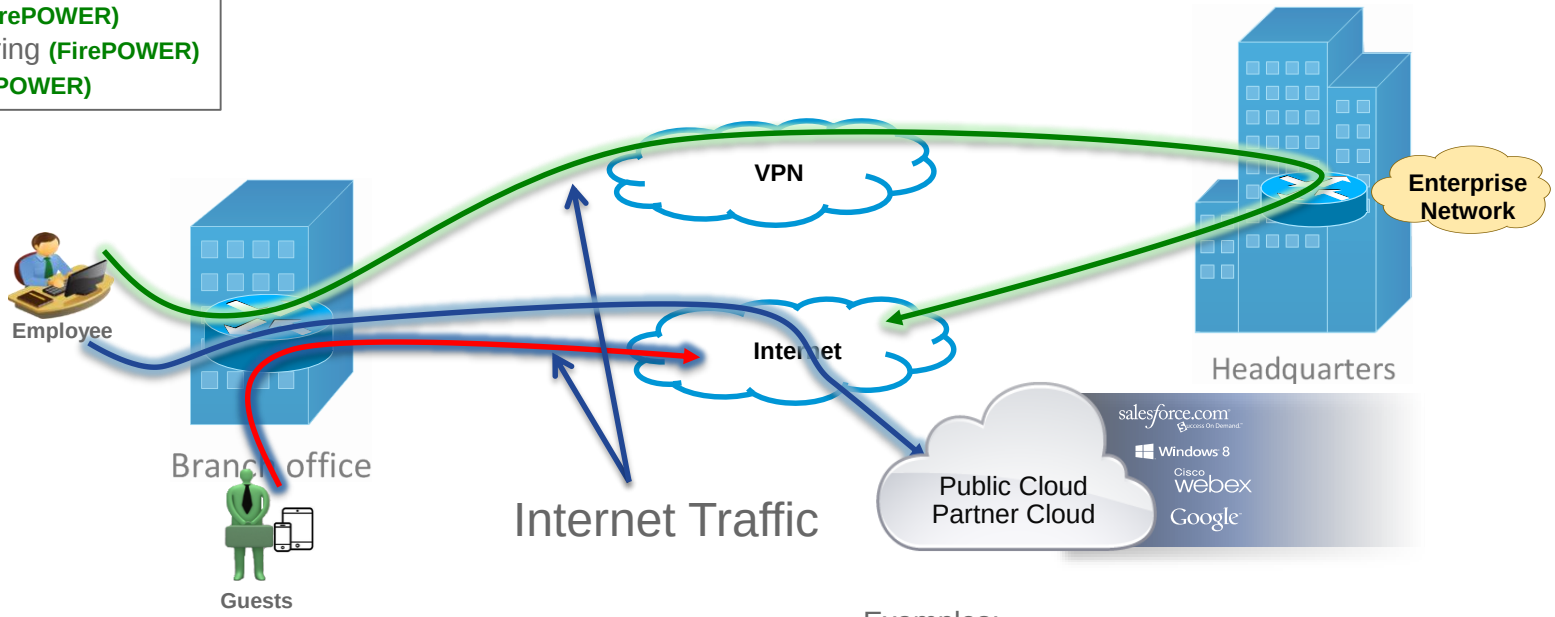
- Security Features
  - Zone Based Firewall
  - Snort IPS
  - CWS
  - FirePOWER
- Demo

Use Cases

Use Case	Vertical	Security Requirements	Technology
Partial Direct Internet Access (Public Cloud, Partner Sites)	Retail, Healthcare, Manufacturing	FW, Web Security, IPS	Snort IDS/IPS, CWS (Identity Policies) or FirePOWER Threat Defense
Full Direct Internet Access	Retail, Healthcare, Manufacturing	FW, Web Security, IPS, Malware Protection, AVC	FirePOWER Threat Defense

Use Case: Secure Branch Public Cloud / Partner Access

MVP
NGFW **(ZBFW, FirePOWER)**
NGIPS **(FirePOWER)**
URL Filtering **(FirePOWER)**
AMP **(FirePOWER)**



Value Prop

- Domain Based Routing, routes only the cloud specific traffic directly
- ZBFW provides pinholes for return traffic from cloud services
- CWS provides additional protection from cloud services
- Additional security services if needed (CWS AMP, CTA etc.)

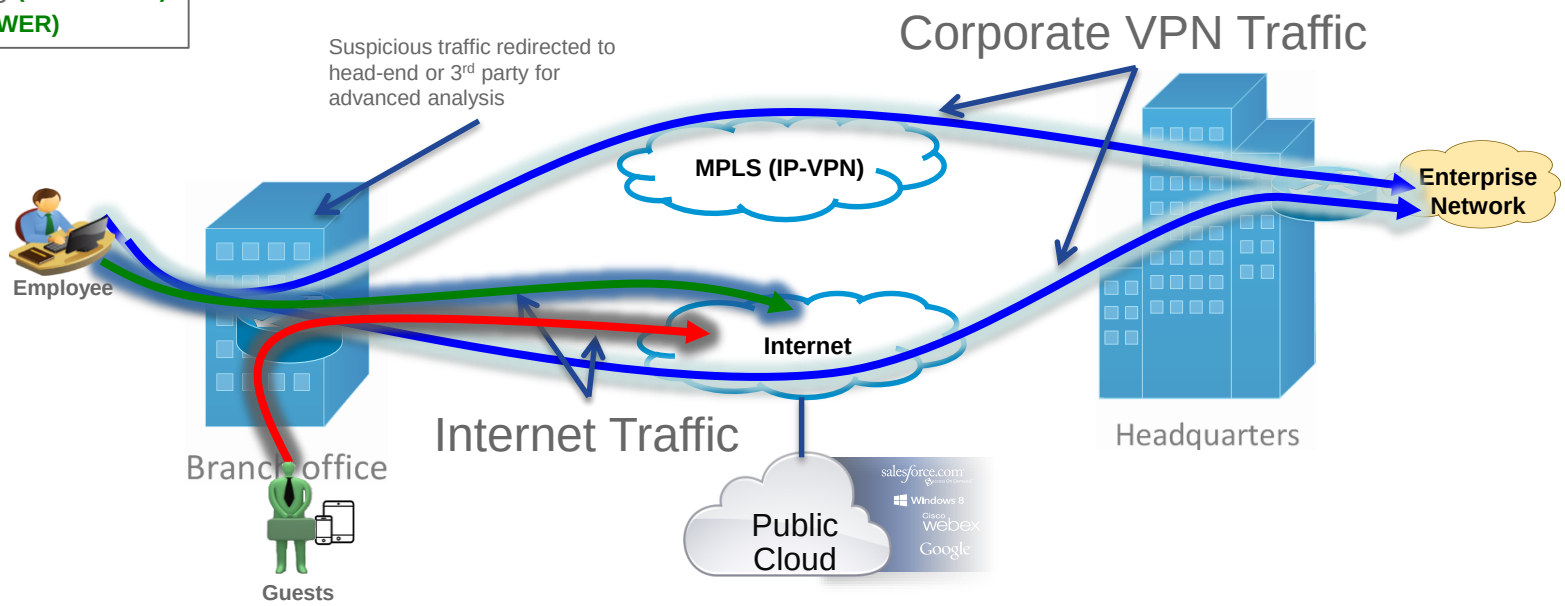
Examples:
Retail Stores Accessing Supplier Websites
Hospital / Pharmacy Accessing Insurance websites
Cloud Based Enterprise Services (webex, salesforce etc.)

Use Case: Secure Branch Direct Internet Access

Integrated On-Premise Advanced Threat Defense

MVP

NGFW **(ZBFW, FirePOWER)**
NGIPS **(FirePOWER)**
URL Filtering **(FirePOWER)**
AMP **(FirePOWER)**



Value Prop

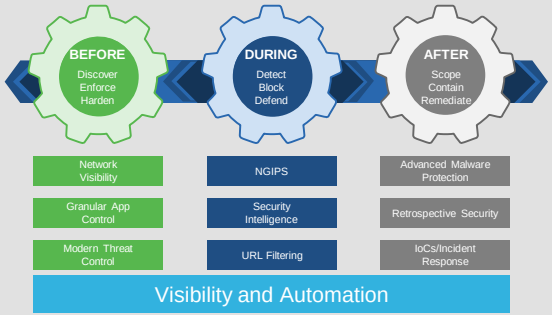
- Best of Routing & Security at Head Quarters and Branch
- Advanced Behavior Analysis at the Head-end

Examples:
Financials

Cisco FirePOWER Threat Defense for ISR

Cisco FirePOWER Threat Defense for ISR

FirePOWER Threat Defense



+

AppX + Security License

Cisco UCS®

Cisco® 4000 Series ISR

OR

Cisco ISR G2 Series

Free Up Valuable Square Footage Generate More Revenue $$$

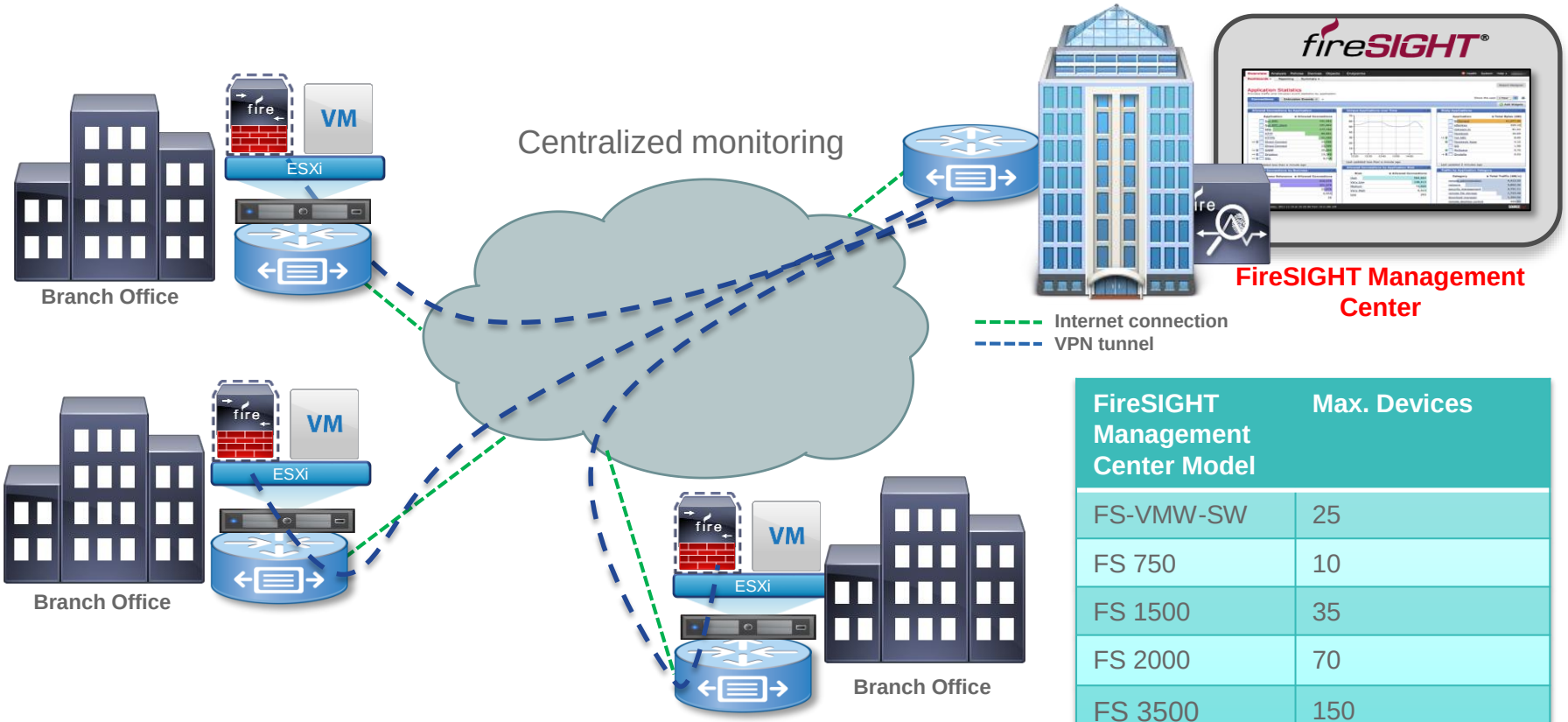
Snort vs FirePOWER Threat Defense for ISR

	Threats	Application visibility and control	Contextual awareness	Impact assessment	Automated IPS tuning	User identities	FireSIGHT
Snort IPS	✓						
FirePOWER IPS and Apps	✓	✓	✓	✓	✓	✓	✓

Snort vs. FirePOWER Threat Defense for ISR

	Snort	FirePOWER
IDS	Yes	Yes
IPS	Yes	Yes
Signature set	Snort	FirePOWER
Application Control and URL Filtering	No	Yes
Next Gen FW	No	Yes
SSL Traffic inspection	No	Yes, with the help of SSL decryption appliance
Advanced Malware Protection	No	Yes
Centralized Management	APIC EM IWAN App (March 2016) Cisco Prime Infrastructure (Nov 2015)	FireSIGHT appliance
Centralized Monitoring	No (third-party tools)	FireSIGHT appliance
Application/Endpoint visibility and profiling	No	Yes
Performance	Less than 1 Gbps	Upto 40 Gbps
Compute required	1 core CPU	4 vCPUs

FirePOWER - Deployment Architecture



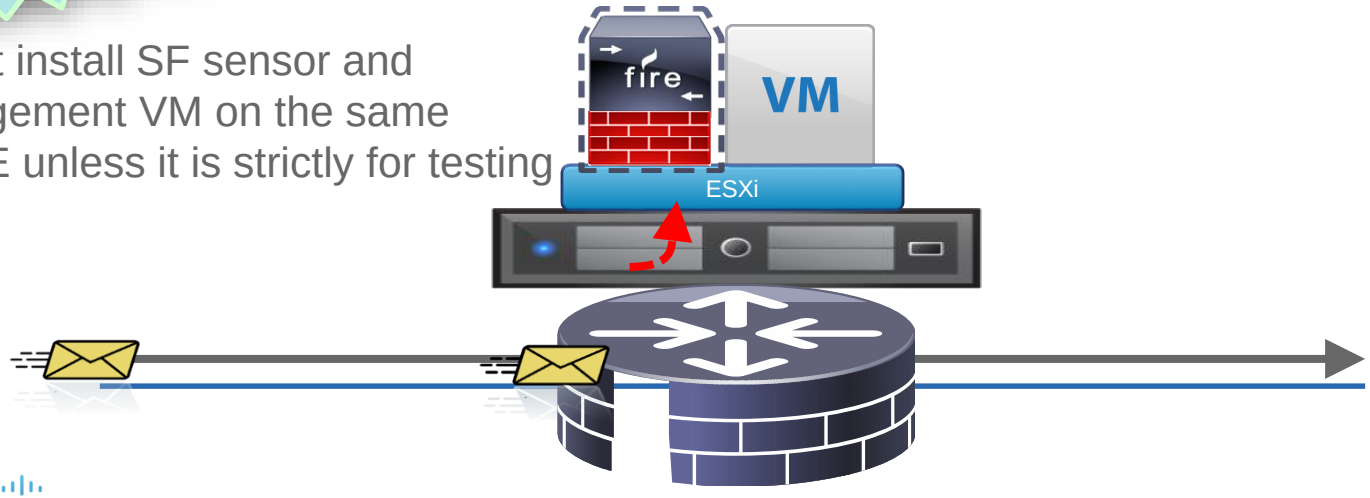
FireSIGHT Management Center Model	Max. Devices
FS-VMW-SW	25
FS 750	10
FS 1500	35
FS 2000	70
FS 3500	150
FS 4000	300

Cisco FirePOWER Threat Defense for ISR - IDS

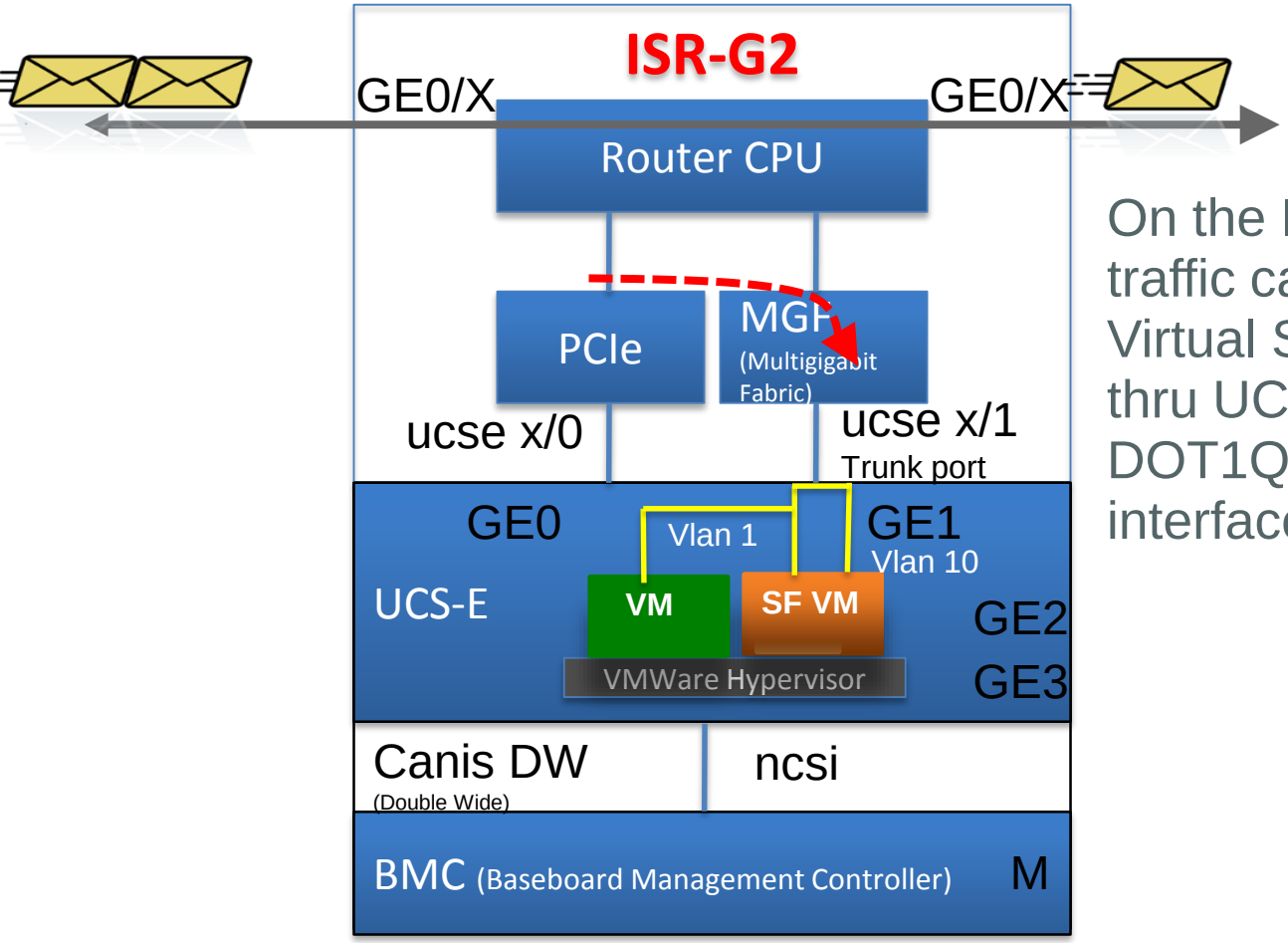
- Host the Sensor on the UCS-E
- Replicate and push all the traffic to be inspected to the Sensor
- SF sensor examines traffic

Only for POC purpose

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

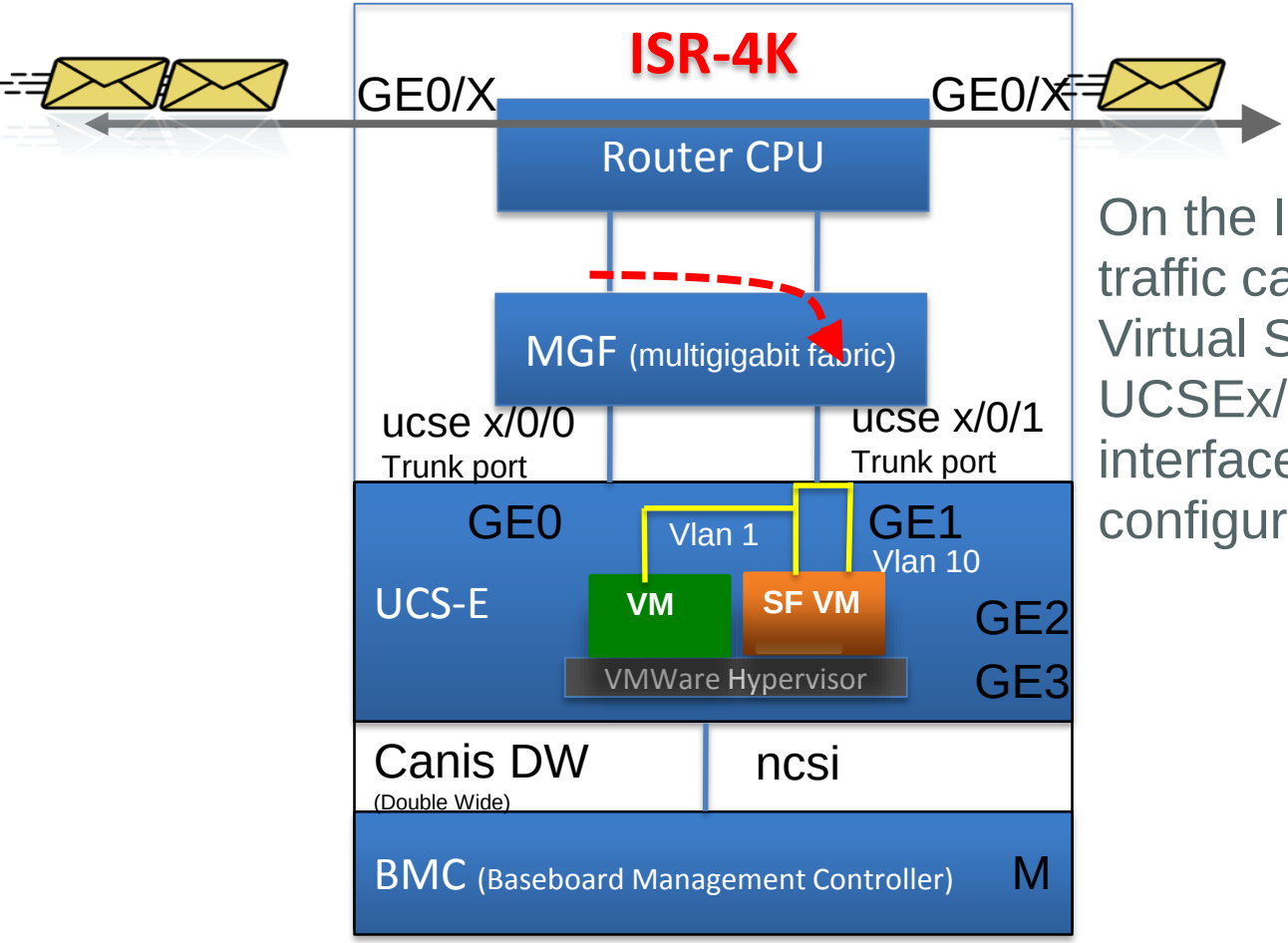


IDS packet flow on ISR G2



On the ISR-G2, the replicated traffic can be sent to SourceFire Virtual Sensor as untagged traffic thru UCSEx/0 interface or as DOT1Q VLAN on UCSEx/1 interface

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–
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)
 mode ids-global
!
interface ucse1/1
 description Internal switch interface connected to Service Module
 switchport mode trunk
 no ip address
!
Interface vlan10
 ip address 10.10.10.1 255.255.255.0
```

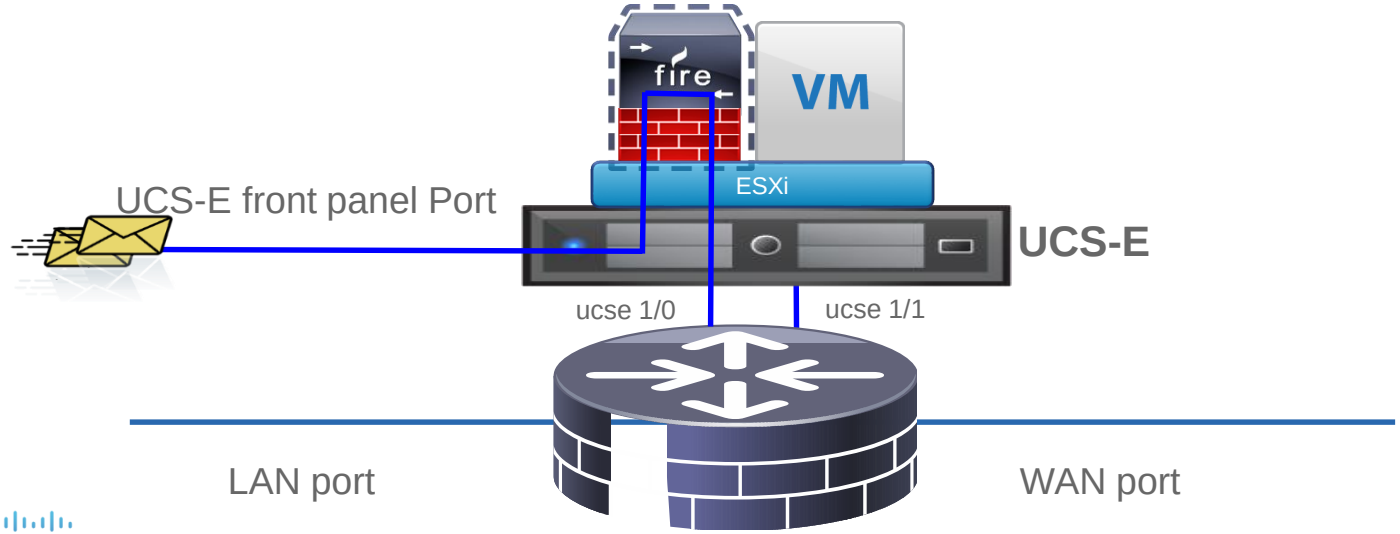
Cisco FirePOWER Threat Defense for ISR–
Configuration Steps

Configure UCS-E (backplane) interface on the router – ISR 4K 3.16.1

```
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
!
utd  (data plane)
 all-interfaces
 redirect interface BDI1
 engine advanced
```

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



Switch Config

```
spanning-tree mode rapid-pvst
 spanning-tree extend system-id
 spanning-tree vlan 10 hello-time 1
 spanning-tree vlan 10 forward-time 4

interface GigabitEthernet3/17
  description connected to UCS-E front panel Ge 2
  switchport
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 10
  switchport mode trunk

 interface GigabitEthernet3/4
  description connected to Router's LAN int g0/0/1
  switchport
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 10
  switchport mode trunk
```

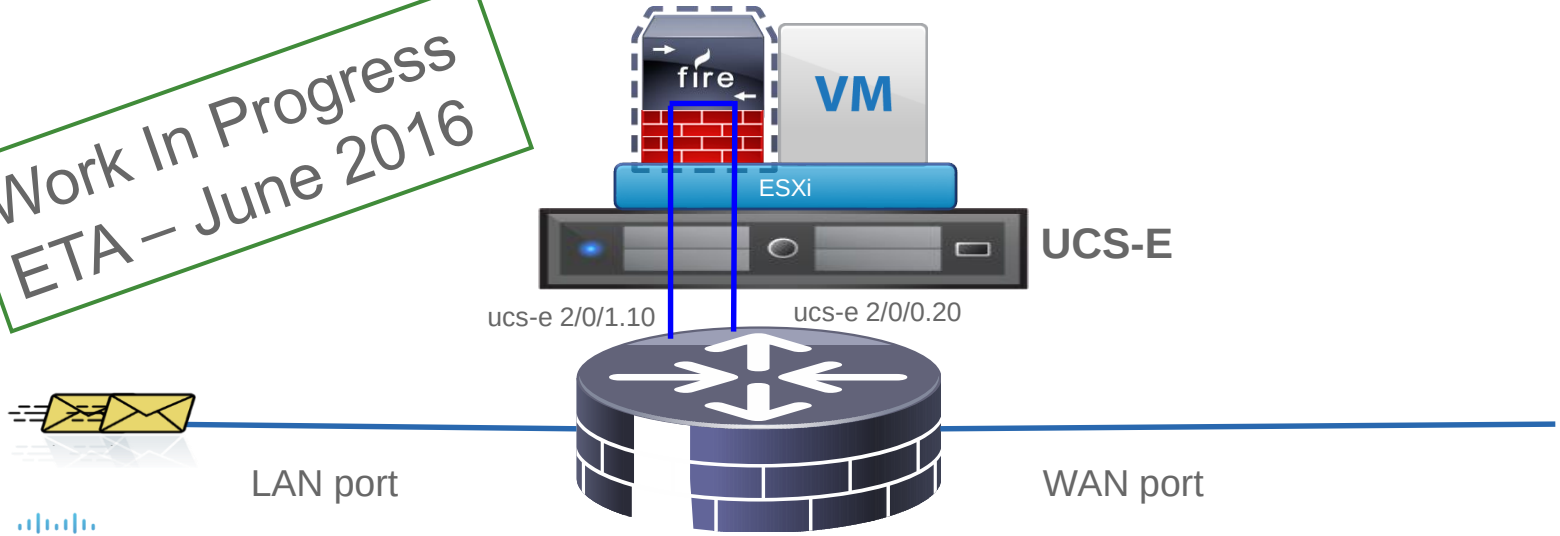
Router Config

```
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 10 hello-time 1
spanning-tree vlan 10 forward-time 4
 bridge-domain 1
interface GigabitEthernet0/0/1
  description LAN interface
  no ip address
  negotiation auto
  spanning-tree cost 100
  service instance 10 ethernet
   encapsulation dot1q 10
   rewrite ingress tag pop 1 symmetric
   bridge-domain 10
 interface ucse1/0/1
   switchport mode trunk
   spanning-tree cost 10
  service instance 10 ethernet
   encapsulation dot1q 10
   rewrite ingress tag pop 1 symmetric
   bridge-domain 10
 interface BDI10
  ip address 106.0.0.1 255.255.255.0
```

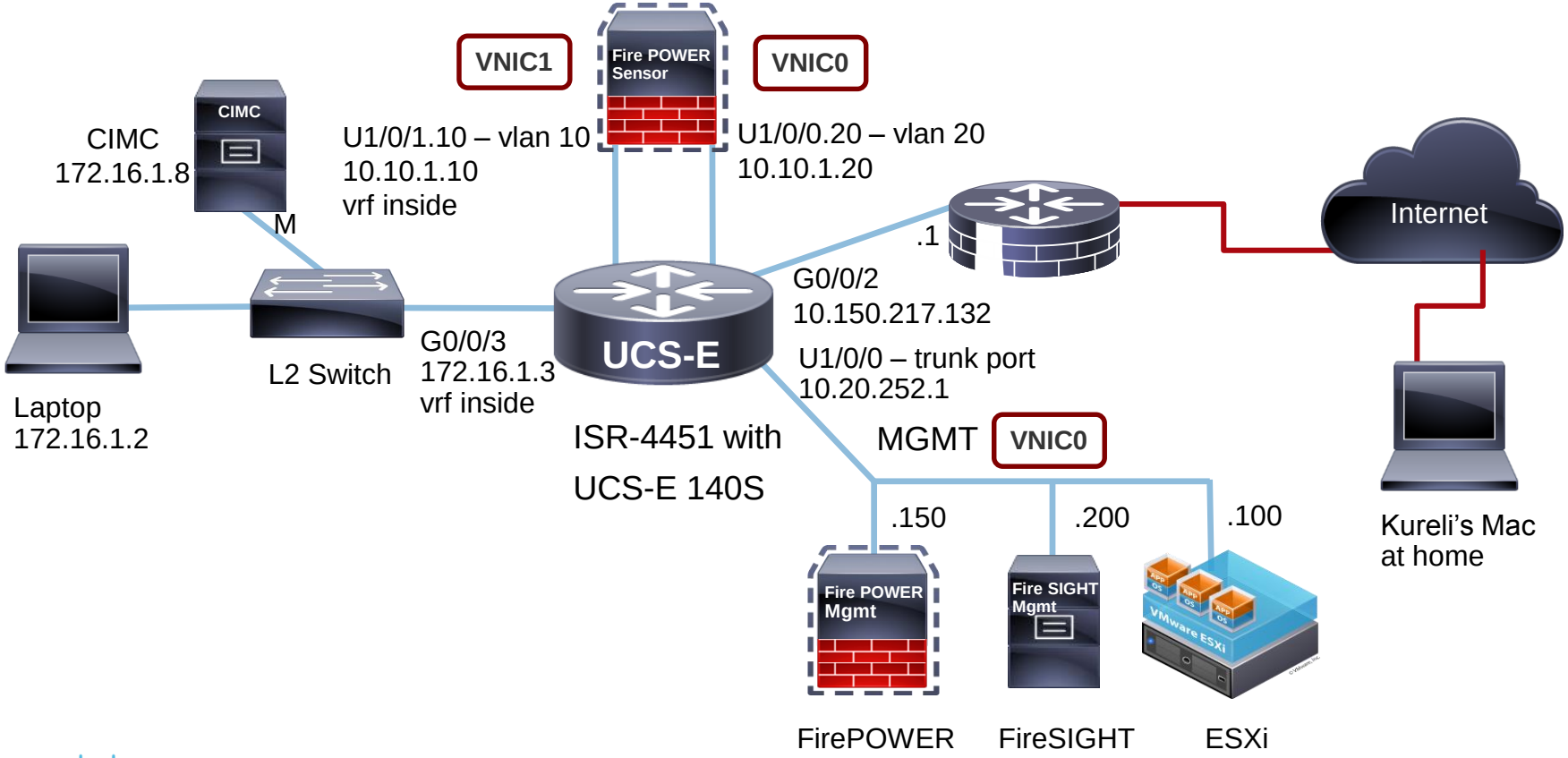
Cisco FirePOWER Threat Defense for ISR- IPS

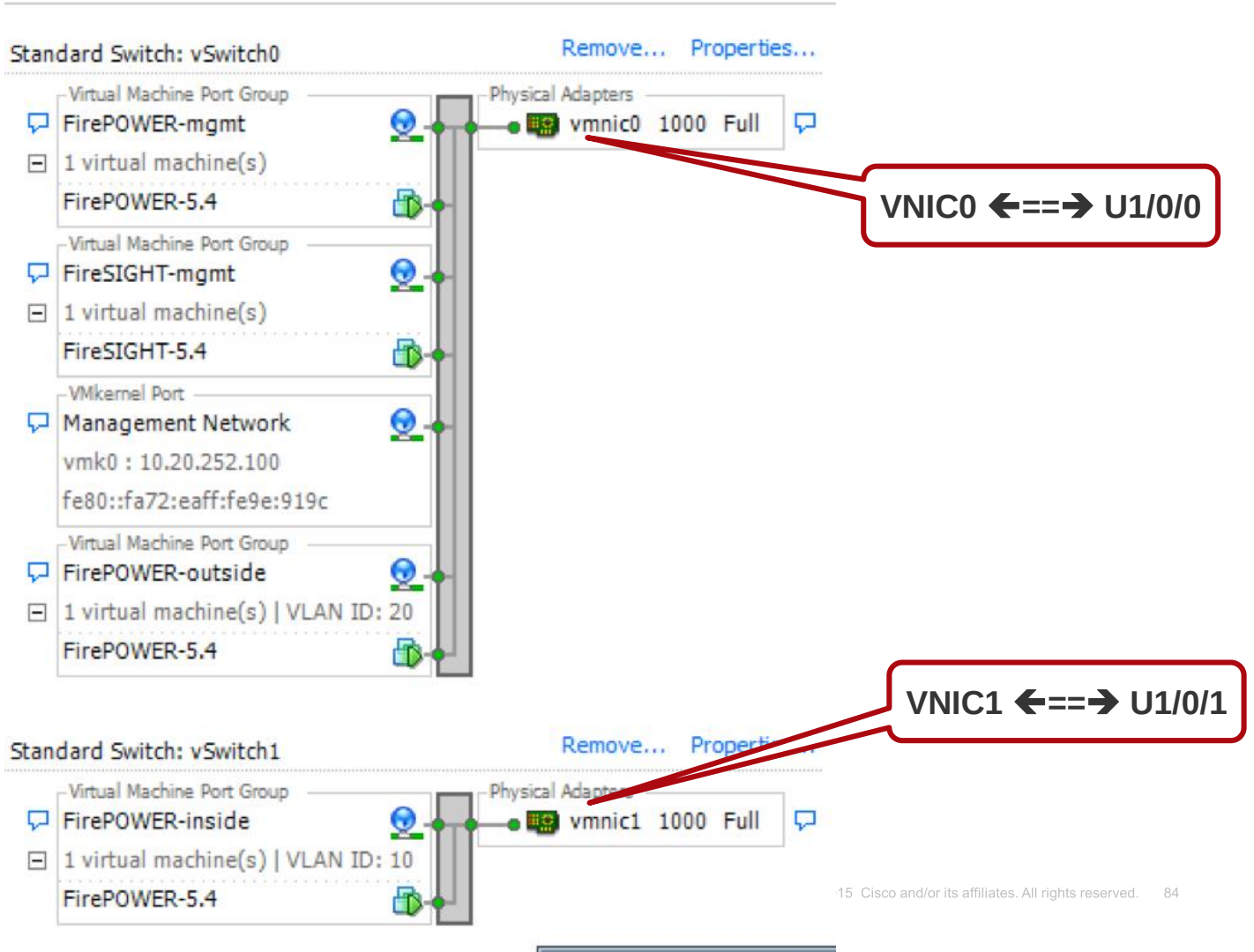
- Host the Sensor on the UCS-E
- IPS is in inline mode
- Packets ingress via the LAN interface of the router
- SF sensor examines traffic; allowed packets egress the WAN interface of the router

Work In Progress
ETA – June 2016

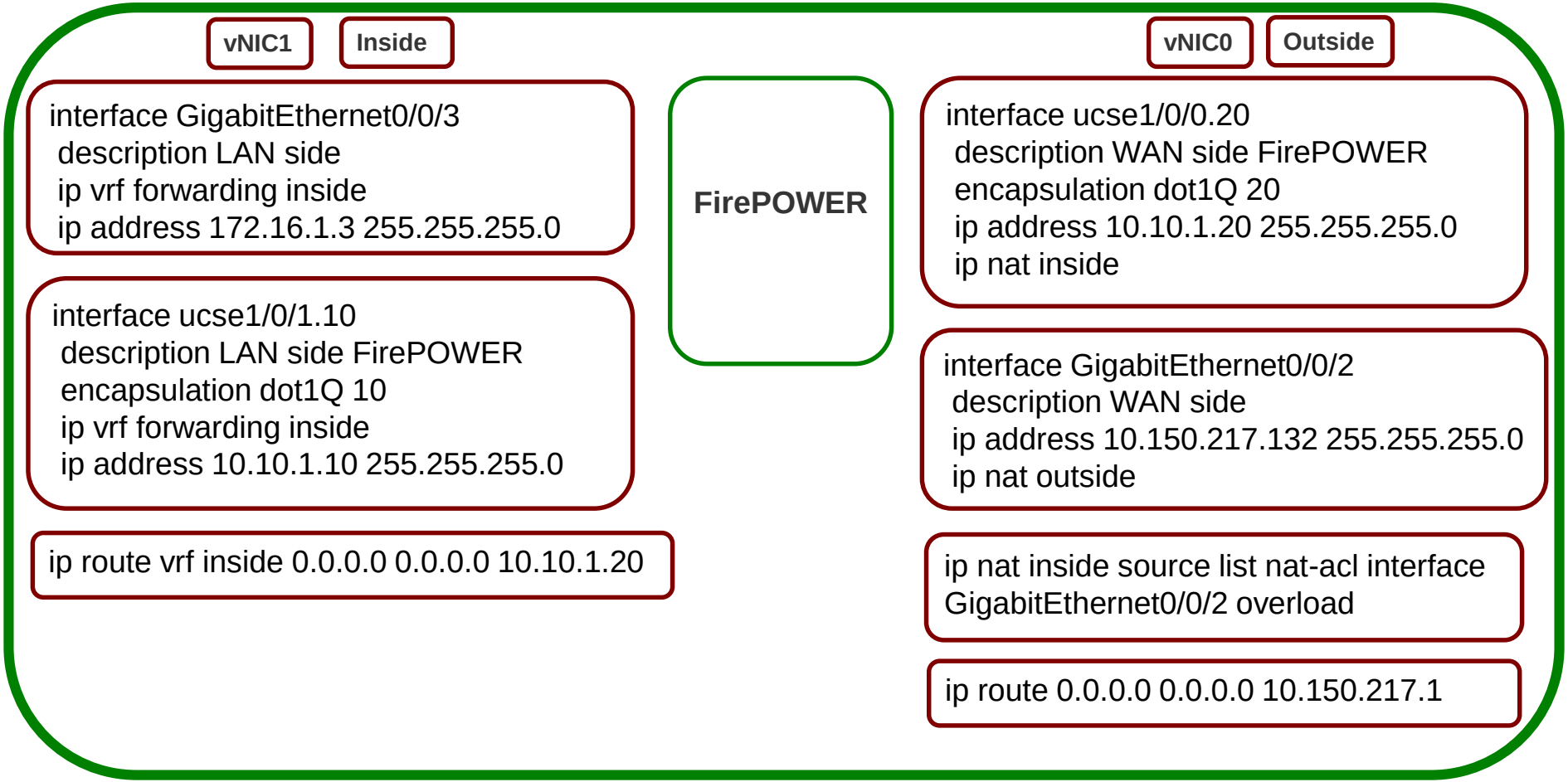


Cisco FirePOWER Threat Defense for ISR - IPS

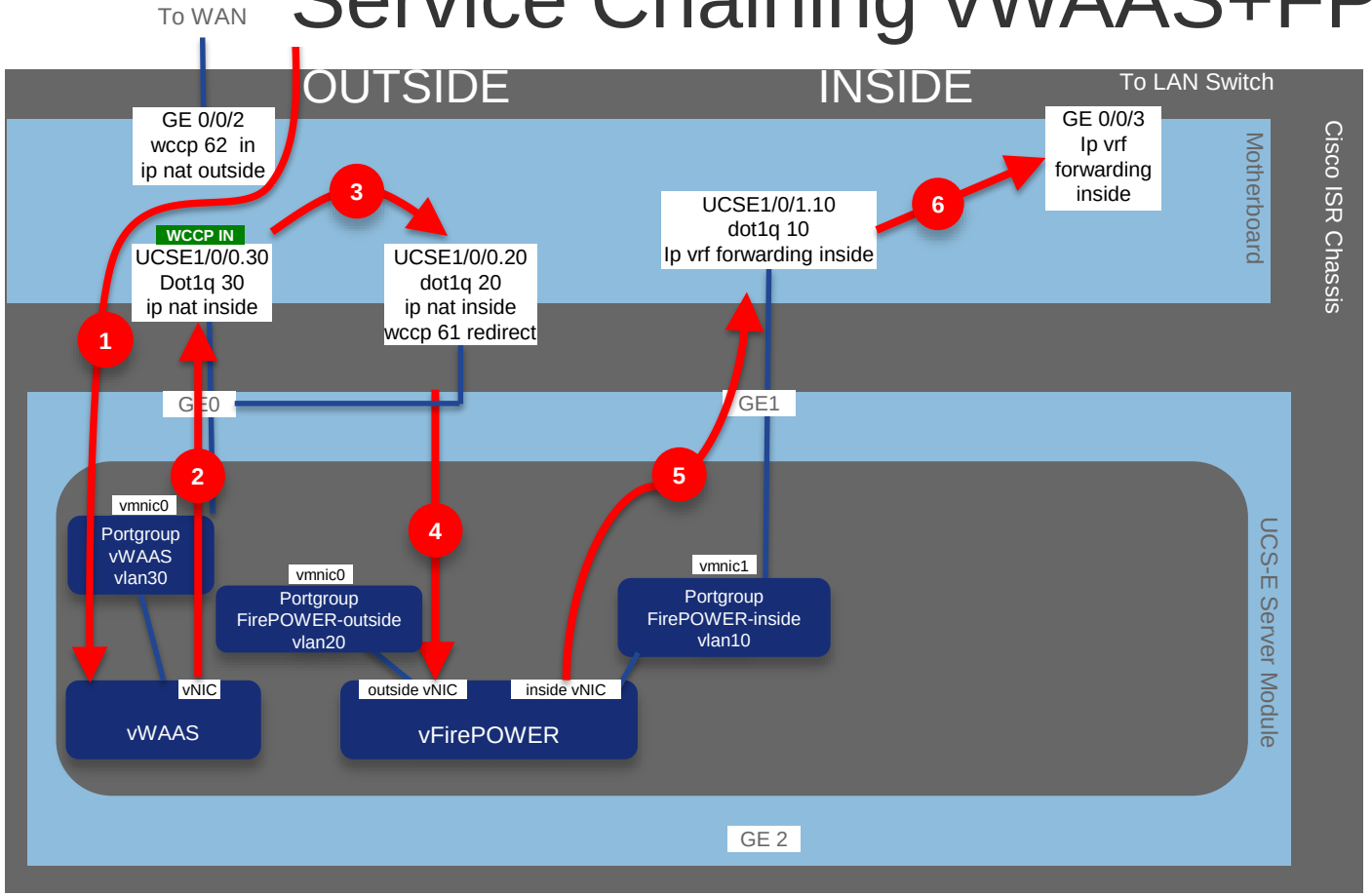




Cisco FirePOWER Threat Defense for ISR - IPS



Service Chaining vWAAS+FP



1. Ingress WAN traffic from the ISR WAN port is redirected to vWAAS on sub-intfc ucse1/0/0.30 running on the UCS-E vmnic0 vlan30
2. vWAAS will redirect traffic back to the ISR router
3. Use standard routing to route traffic from vWAAS to sub-intfc ucse1/0/0.20 to the UCS-E blade
4. Traffic will be routed to the outside interface of the FP VM set to vlan20 on vmnic0 vswitch
5. Traffic is analyzed by the inline IPS service, allowed packets are sent out via the inside interface of the FP VM
6. UCSE1/0/1.10 sub-intfc is placed in “ip vrf inside” to segregate at layer 3 from outside network and traffic is routed to LAN via GE0/0/3 which is also on ip vrf inside

Appendix

- AMP – Advance Malware Protection
- WL – White Listing
- CIMC – Cisco Integrated Management Console
- PI – Prime Infrastructure
- WAAS – Wide Area Application Services
- UCS-E – Unified Computing System
- BDI – Bridge Domain Interface
- IDS – Intrusion Detection System
- IPS – Intrusion Prevention System

FirePOWER - 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/xe-3s/sec-data-utd-xe-3s-book.html#concept_0AC4C1AE8D714F1C9533FD3B383EC8AF

- Router Security – FirePOWER Threat Defense for ISR
  BDM, TDM, Step-by-Step Guides (includes performance numbers)
  Troubleshooting Guide, Ordering Guide, FAQ

http://wwwin.cisco.com/tech/srtg/rbs/security.shtml#tab-vpn=0&ext-comp-1078=1&tab-CWS=0&tab-td=3&tab-fp=0&ext-comp-1077=1

Polling Question 4

What products are you interested in? (Check all that applies)

A. IPS/IDS

B. AVC - Application Visibility and Control

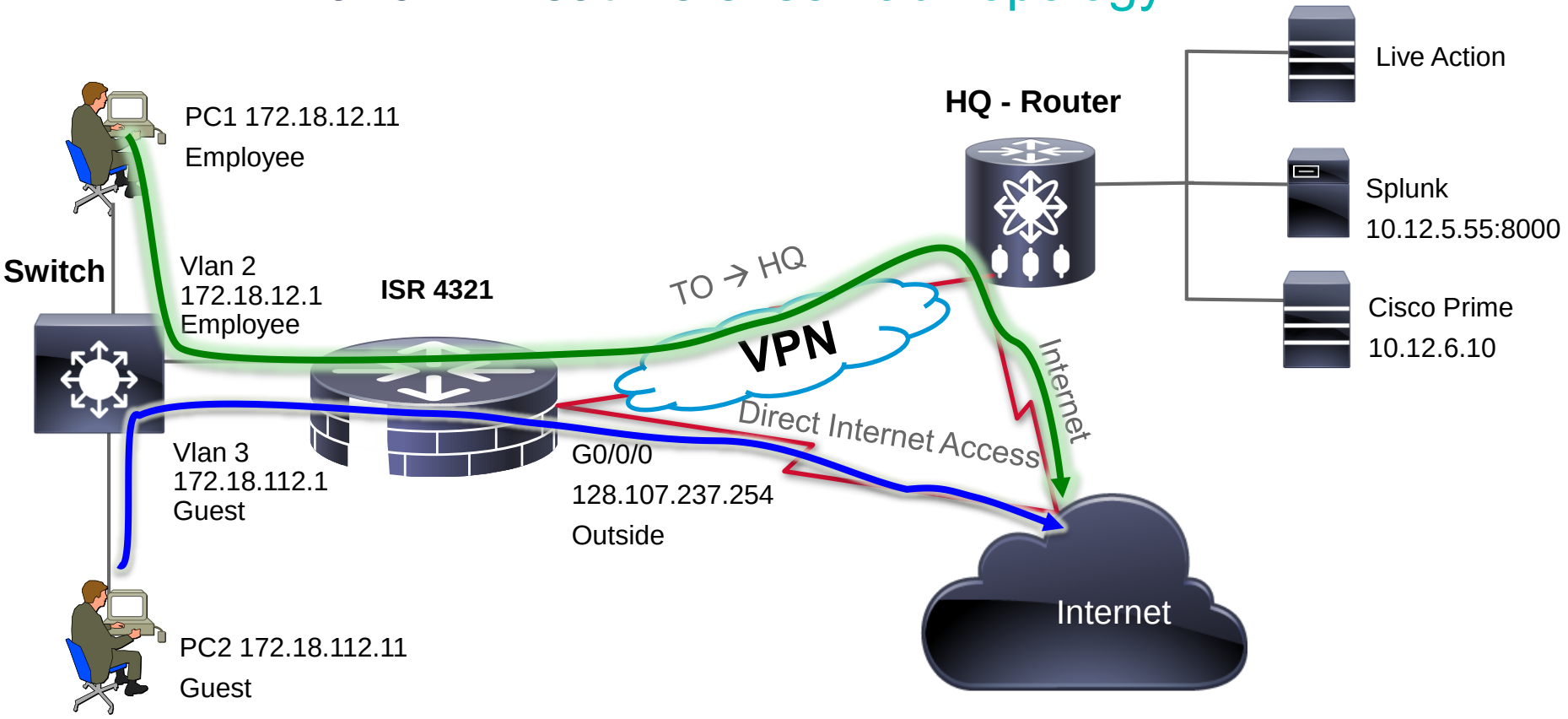
C. URL Filtering solution

D. Advanced Malware Protection

Agenda

- Security Features
  - Snort IPS
  - CWS
  - FirePOWER
  - Zone Based Firewall
- Demo

Branch Threat Defense Lab Topology



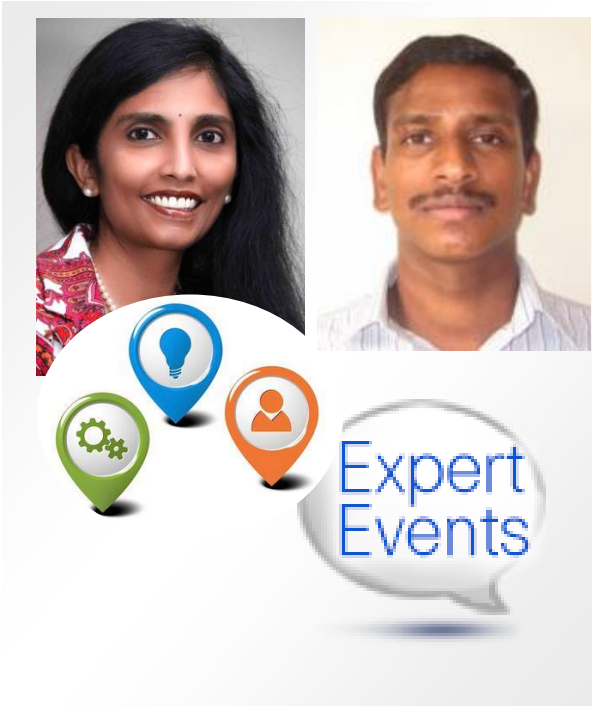
Submit Your Questions Now!

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

Ask the Expert Event following the Webcast

Now through April 1st

https://supportforums.cisco.com/discussion/12753631/ask-expert-threat-defense-secure-enterprise-branch



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

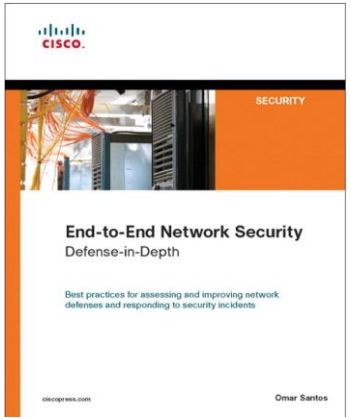
Thank you for participating!

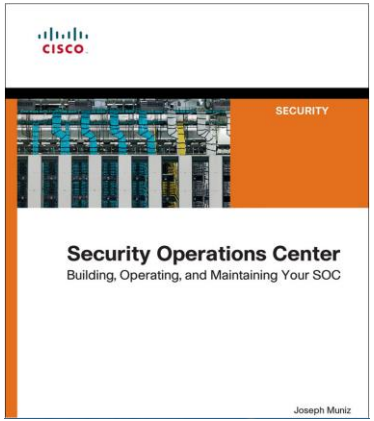
. Redeem your 35% discount offer by entering code: CSC when checking out:

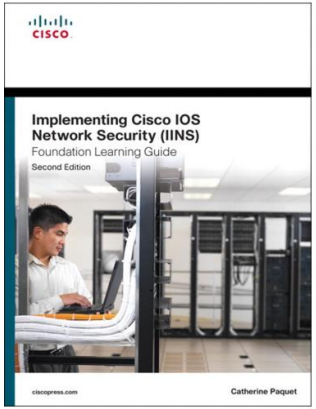
Visit Cisco Press at:

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.