CISCO

IMAGINE

INTUITIVE

Cisco live!

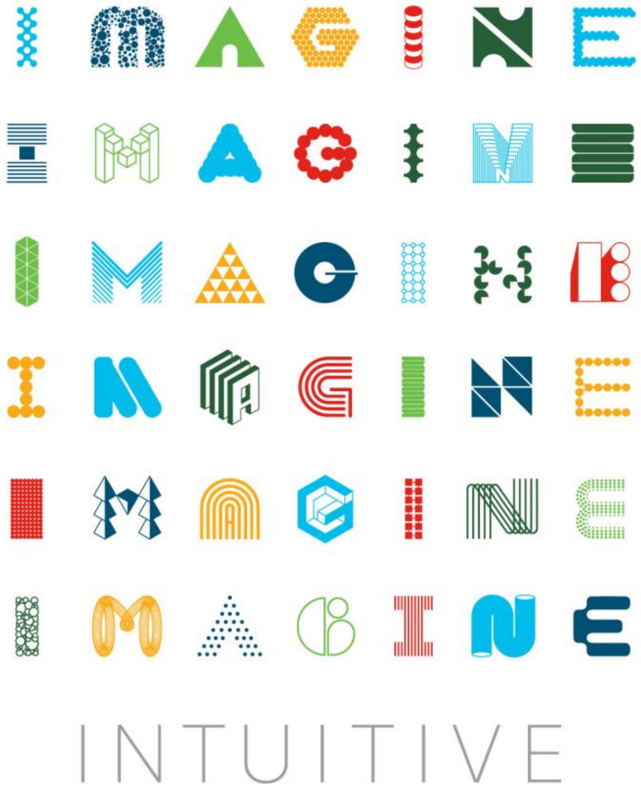
June 10-14, 2018 · Orlando, FL

#CLUS

Branch Router Security

BRKSEC-2342

Kureli Sankar, Technical Marketing Engineer
CCIE Security #35505
Kureli@cisco.com



Agenda

- Zone Based Firewall
- Snort IPS
- Cisco Umbrella Integration (OpenDNS)
- Firepower Threat Defense for ISR
- Encrypted Traffic Analytics (ETA)

Cisco Webex Teams

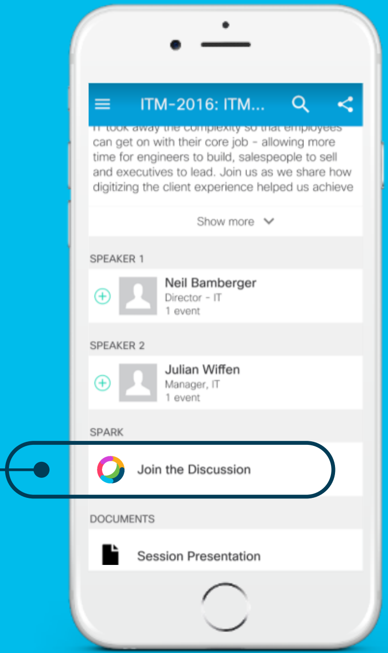
Questions?

Use Cisco Webex Teams (formerly Cisco Spark)
to chat with the speaker after the session

How

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

Webex Teams will be moderated
by the speaker until June 18, 2018.



ITM-2016: ITM...

IT took away the complexity so that employees can get on with their core job - allowing more time for engineers to build, salespeople to sell and executives to lead. Join us as we share how digitizing the client experience helped us achieve

Show more

SPEAKER 1

Neil Bamberger
Director - IT
1 event

SPEAKER 2

Julian Wiffen
Manager, IT
1 event

SPARK

Join the Discussion

DOCUMENTS

Session Presentation

cs.co/ciscolivebot# BRKSEC-2342

Session Abstract

In this session attendees will learn how to deploy the following security features on a Cisco Router:

1. Zone Based Firewall (ZBF)
2. Snort IPS
3. Cisco Umbrella (OpenDNS)
4. Firepower Threat Defense for ISR
5. Encrypted Traffic Analytics (ETA)

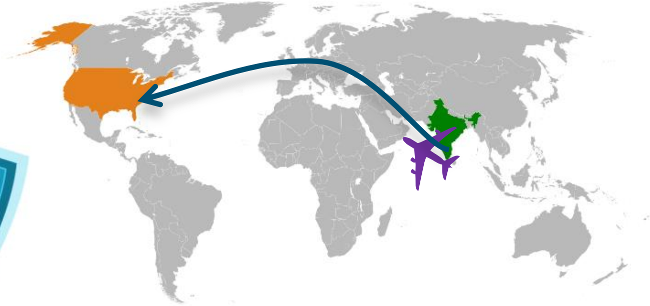
About me

- BS in Electrical and Electronics Engineering
- 2006 – 2013 TAC Engineer
  - CCIE Security #35505
- 2013 – Present TME
- Areas of expertise
  - IOS and IOS-XE security features
  - Security solutions
- 2018 – Distinguished Speaker Cisco Live (EUR and ANZ)

CISCO CERTIFIED CCIE SECURITY

# 35505

NITT

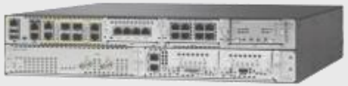


Distinguished Speaker Cisco live!

Branch Router - Freedom of Choice ISR 4K and ISRv

Traditional

Physical Router

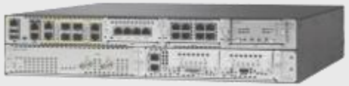


Cisco® 4000 Series ISR

Centralized services
Fixed integrated services
Conservative

Enterprise NFV

Physical Router Virtual Services



4000 Series ISR +
UCS® E-Series

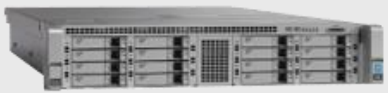
Upgradable hardware
Deterministic routing performance

Virtual Router Virtual Services

Enterprise Network Compute System (ENCS)

Elastic routing and services
Router / Server Hybrid

Virtual Router Virtual Services



UCS C-Series

Elastic routing and services
Performance
Early adopter

Cisco ONE™

Access to Ongoing Innovation

License Portability

Investment Protection

Branch Router - Freedom of Choice ISR 1K

- High performance WAN, comprehensive security, wired and wireless access
- IOS XE - Same code base as ISR 4000 (No UC tech package on 1100)
- Unshaped throughput for non-crypto traffic. IPsec Crypto throughput shaped at 50, 150 & 250Mbps depending on license level and platform
- HSEC license unlocks shaper for crypto
- Cisco 800 series not affected by Cisco 1100

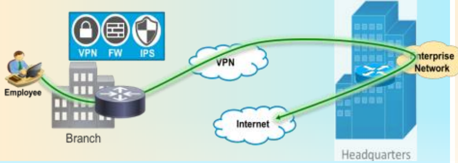
IWAN & Cisco SD WAN ready	Unprecedented Security ZBF, Cisco Umbrella, ETA, State of the art Cyberthreat protection	Mobility Express	LTE Advanced	Programmability

Direct Internet Access – Use Cases

Customer Intent

I need to protect my sensitive data (card holder data, patient data) against data breaches before, during and after a transaction.

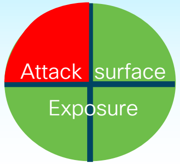
Compliance



IPsec VPN

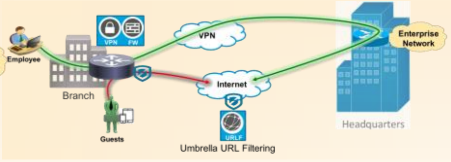
Zone Based Firewall

Snort IPS



I need to protect my company against liability and prevent guest users from disrupting my network when browsing the internet via guest wi-fi.

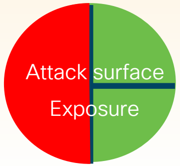
Guest Access



IPsec VPN

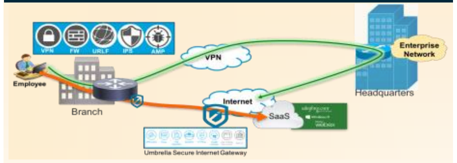
Zone Based Firewall

URL Filtering



I want to reduce expenses and provide better user experience for cloud apps. If I open up my branch office to the internet I increase the attack surface and I need to protect my network.

Direct Cloud Access

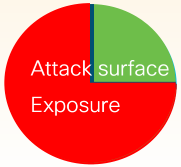


IPsec VPN

Zone Based Firewall

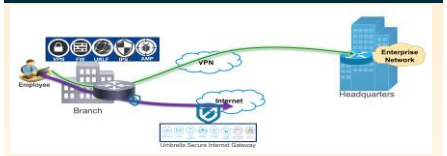
Snort IPS

Umbrella (Cloud SIG)



I want to leverage the local internet path for all internet traffic; I need to protect myself against potential threats coming into my network.

Direct Internet Access

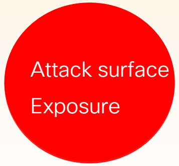


IPsec VPN

Zone Based Firewall

Snort IPS

Umbrella (Cloud SIG)



Direct Internet Access (DIA)

Benefits

- Offload Internet traffic from private WAN link – Save costs
- Optimal access to nearest resources
- Improved performance of private and public applications

Challenges

- Management of many Internet Edges
- Security policy enforcement

Zone Based Firewall

Zone Based Firewall – Benefits and Requirements

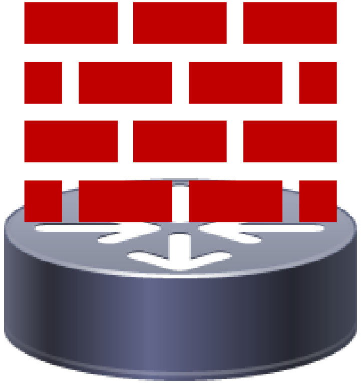
Benefits

- Helps meet PCI * compliance
- Stateful firewall built into ISR and ISRv branch routers
- VLAN Segmentation
- Supports VRF

Requirements

- SEC-K9 license
- XE 3.9 and above on ISR 4K
- XE 16.6.1 and above on ISR 1K
- XE 16.8.1 and above on ISRv

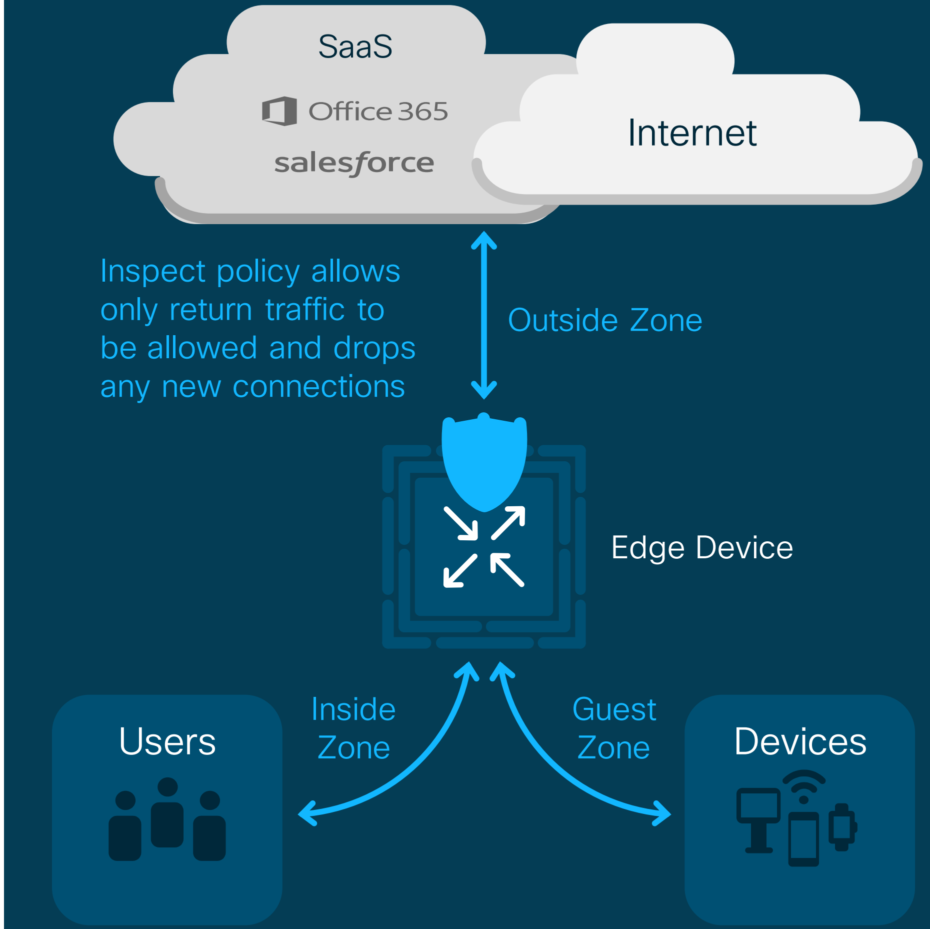
Zone Based Firewall



* PCI – Payment Card Industry

Zone Based Firewall

- Custom Zone
- default zone
  - “default” security zone for all INSIDE interfaces
  - default zone has always been in IOS-XE
  - default zone support on ISR-G2 is from 15.6(1)T
- Self Zone



SaaS

Office 365

salesforce

Internet

Inspect policy allows only return traffic to be allowed and drops any new connections

Outside Zone

Edge Device

Inside Zone

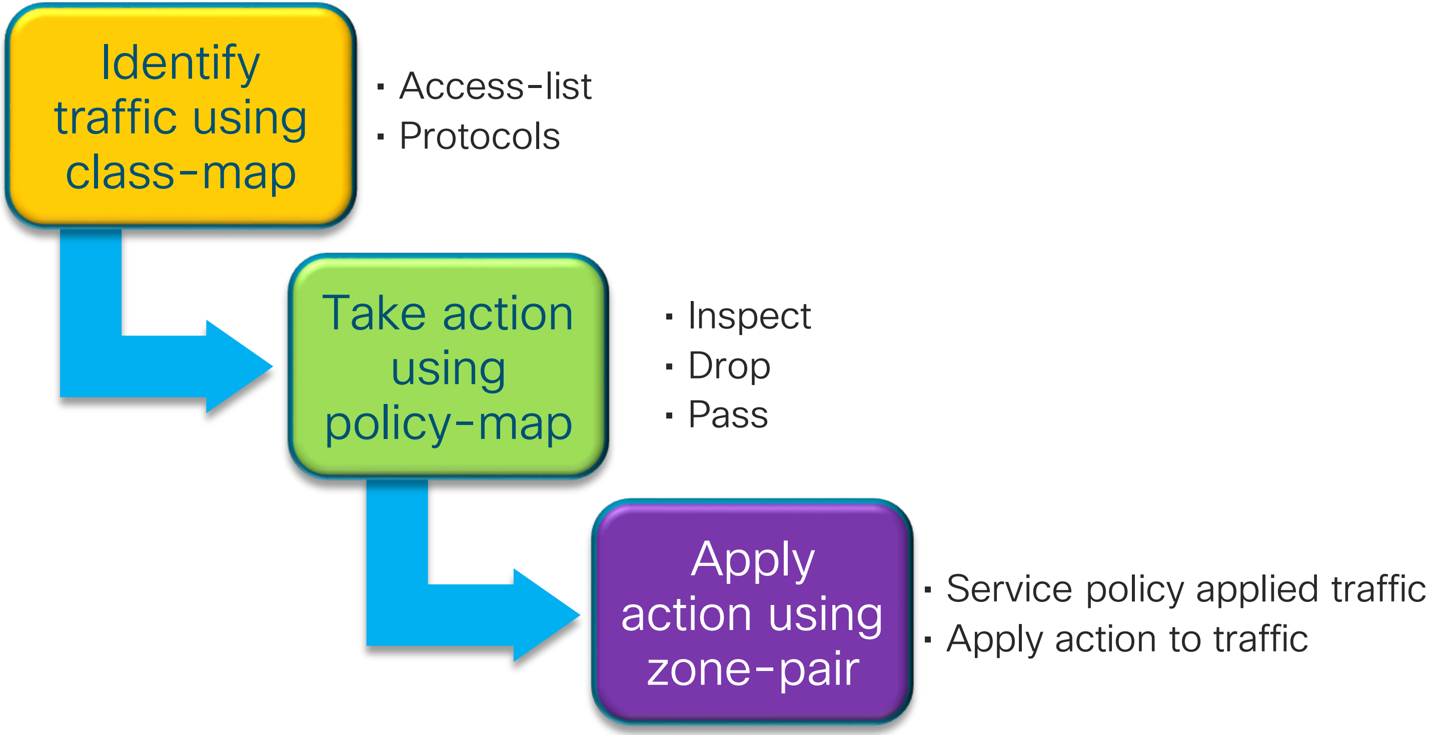
Guest Zone

Users

Devices

Zone Based Firewall

Configuration Theory – directional, different policy based on packet direction



Identify traffic using class-map

- Access-list
- Protocols

Take action using policy-map

- Inspect
- Drop
- Pass

Apply action using zone-pair

- Service policy applied traffic
- Apply action to traffic

Zone Based Firewall - Custom Zone

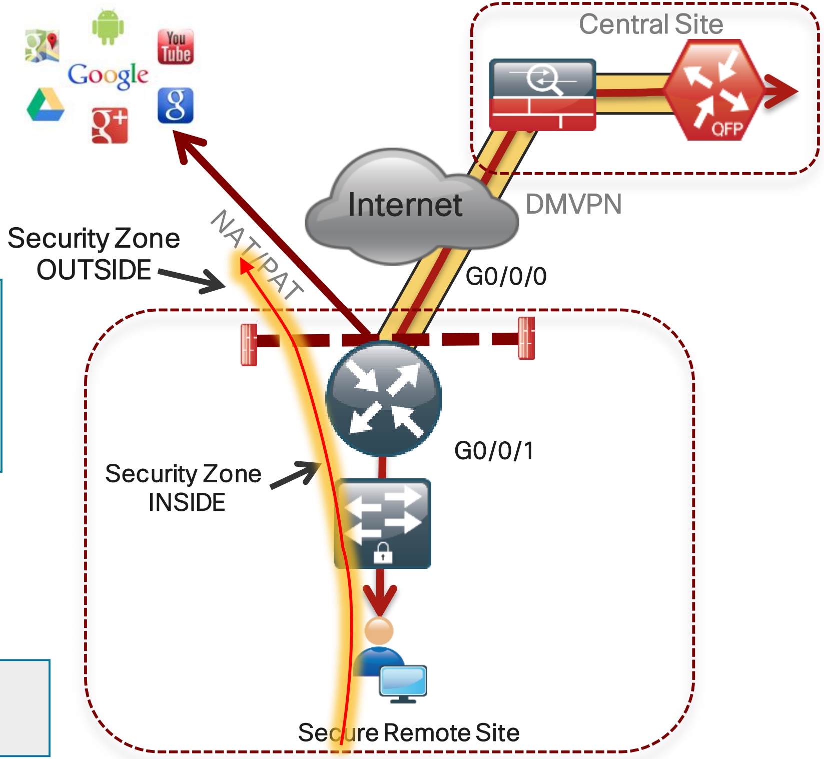
```
zone security INSIDE
zone security OUTSIDE
```

```
class-map type inspect match-any INSIDE-TO-OUTSIDE-CLASS
 match protocol ftp             |
 match protocol tcp             |    match access-group name
 match protocol udp             |
 match protocol icmp            |
```

```
policy-map type inspect INSIDE-TO-OUTSIDE-POLICY
 class type inspect INSIDE-TO-OUTSIDE-CLASS
  inspect
 class class-default
  drop
```

```
Interface G0/0/0
 zone security OUTSIDE
Interface G0/0/1
 Zone security INSIDE
```

```
zone-pair security IN_OUT source INSIDE destination OUTSIDE
 service-policy type inspect INSIDE-TO-OUTSIDE-POLICY
```



Zone Based Firewall – Default Zone

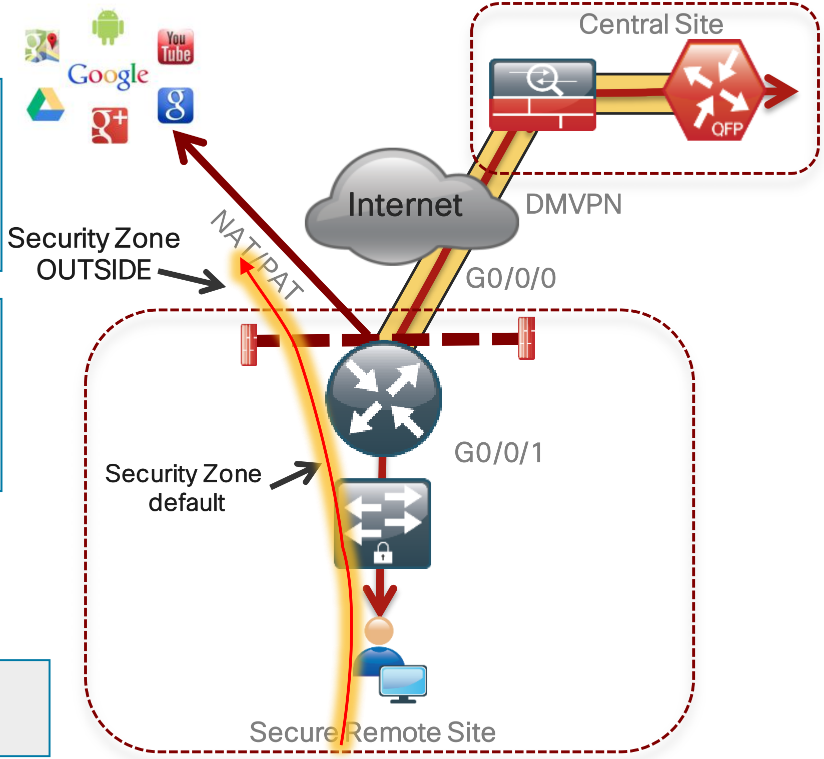
```
zone security default
zone security OUTSIDE
```

```
class-map type inspect match-any INSIDE-TO-OUTSIDE-CLASS
 match protocol ftp
 match protocol tcp                         match access-group name
 match protocol udp
 match protocol icmp
```

```
policy-map type inspect INSIDE-TO-OUTSIDE-POLICY
 class type inspect INSIDE-TO-OUTSIDE-CLASS
  inspect
 class class-default
  drop
```

```
Interface G0/0/0
 zone security OUTSIDE
```

```
zone-pair security IN_OUT source default destination OUTSIDE
 service-policy type inspect INSIDE-TO-OUTSIDE-POLICY
```

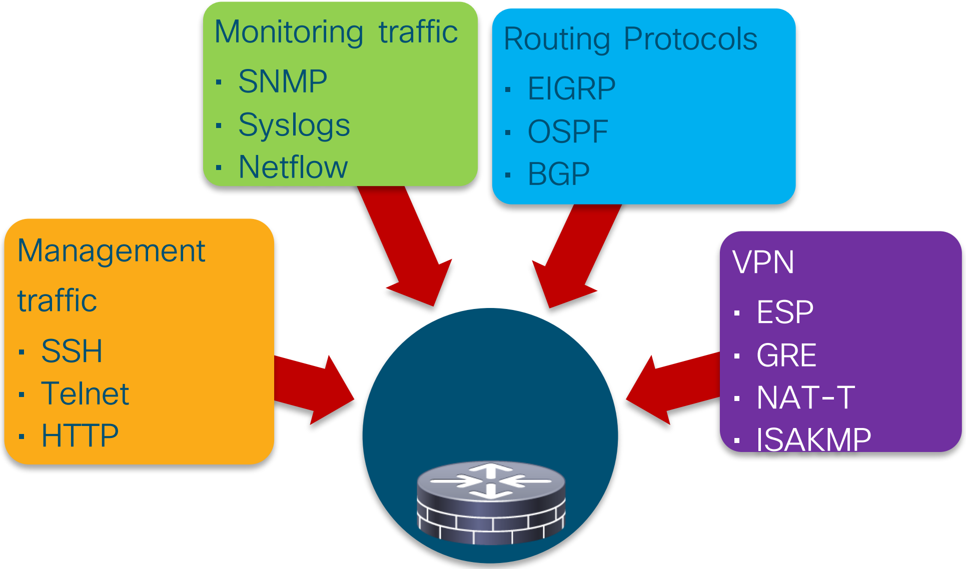


Zone Based Firewall – Self Zone

- Pre-defined zone member
  - Protects traffic TO and FROM router
  - Traffic sourced or destined to router
  - Excludes THROUGH the box NAT traffic

- Two differences
  - Pre-defined and available for use
  - Explicit allow compared to explicit deny

- Used to protect management and control plane traffic



Monitoring traffic
- SNMP
- Syslogs
- Netflow

Routing Protocols
- EIGRP
- OSPF
- BGP

Management traffic
- SSH
- Telnet
- HTTP

VPN
- ESP
- GRE
- NAT-T
- ISAKMP

Zone Based Firewall

Self Zone inbound - DMVPN tunnel inbound to the router itself

```
ip access-list extended ACL-RTR-IN
 permit udp host y.y.y.y any eq 4500
 permit udp host y.y.y.y any any eq isakmp
 permit icmp host x.x.x.x any echo
 permit icmp host x.x.x.x any echo-reply
 permit icmp any any ttl-exceeded
 permit icmp any any port-unreachable
 permit udp any any range 33434 33463 ttl eq 1
```

```
ip access-list extended ESP-IN
 permit esp any any

ip access-list extended DHCP-IN
 permit udp any eq bootps any eq bootpc

ip access-list extended GRE-IN
 permit gre host x.x.x.x any
```

```
class-map type inspect match-any INSPECT-ACL-IN-CLASS
 match access-group name ACL-RTR-IN

class-map type inspect match-any PASS-ACL-IN-CLASS
 match access-group name ESP-IN
 match access-group name DHCP-IN
 match access-group name GRE-IN

policy-map type inspect ACL-IN-POLICY
 class type inspect INSPECT-ACL-IN-CLASS
  inspect
 class type inspect PASS-ACL-IN-CLASS
   pass
 class class-default
   drop
```

```
zone-pair security TO-ROUTER source OUTSIDE destination self
  service-policy type inspect ACL-IN-POLICY
```

Zone Based Firewall

Self Zone outbound – DMVPN tunnel traffic from the router itself

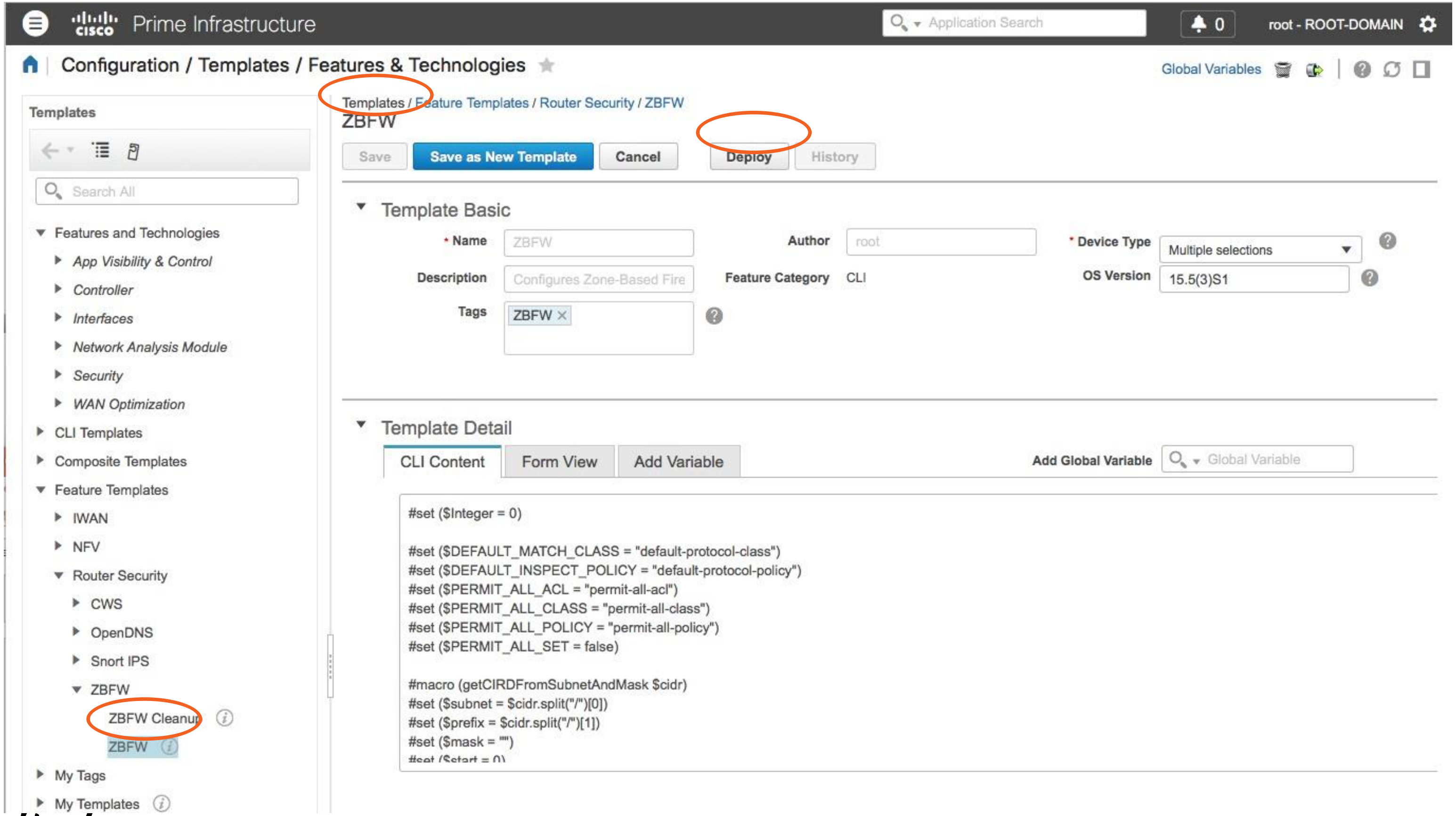
```
ip access-list extended ACL-RTR-OUT
 permit udp any host y.y.y.y eq 4500
 permit udp any host y.y.y.y eq isakmp
 permit icmp any host y.y.y.y
```

```
ip access-list extended ESP-OUT
 permit esp any host y.y.y.y

ip access-list extended DHCP-OUT
 permit udp any eq bootpc any eq bootps
```

```
class-map type inspect match-any INSPECT-ACL-OUT-CLASS
 match access-group name ACL-RTR-OUT

class-map type inspect match-any PASS-ACL-OUT-CLASS
 match access-group name ESP-OUT
 match access-group name DHCP-OUT

 policy-map type inspect ACL-OUT-POLICY
  class type inspect INSPECT-ACL-OUT-CLASS
   inspect
 class type inspect PASS-ACL-OUT-CLASS
   pass
 class class-default
   drop
```

```
zone-pair security FROM-ROUTER source self destination OUTSIDE
 service-policy type inspect ACL-OUT-POLICY
```

Zone Based Firewall – Provisioning (Prime Infrastructure)



Name: ZBFW

Author: root

Device Type: Multiple selections

Description: Configures Zone-Based Fire

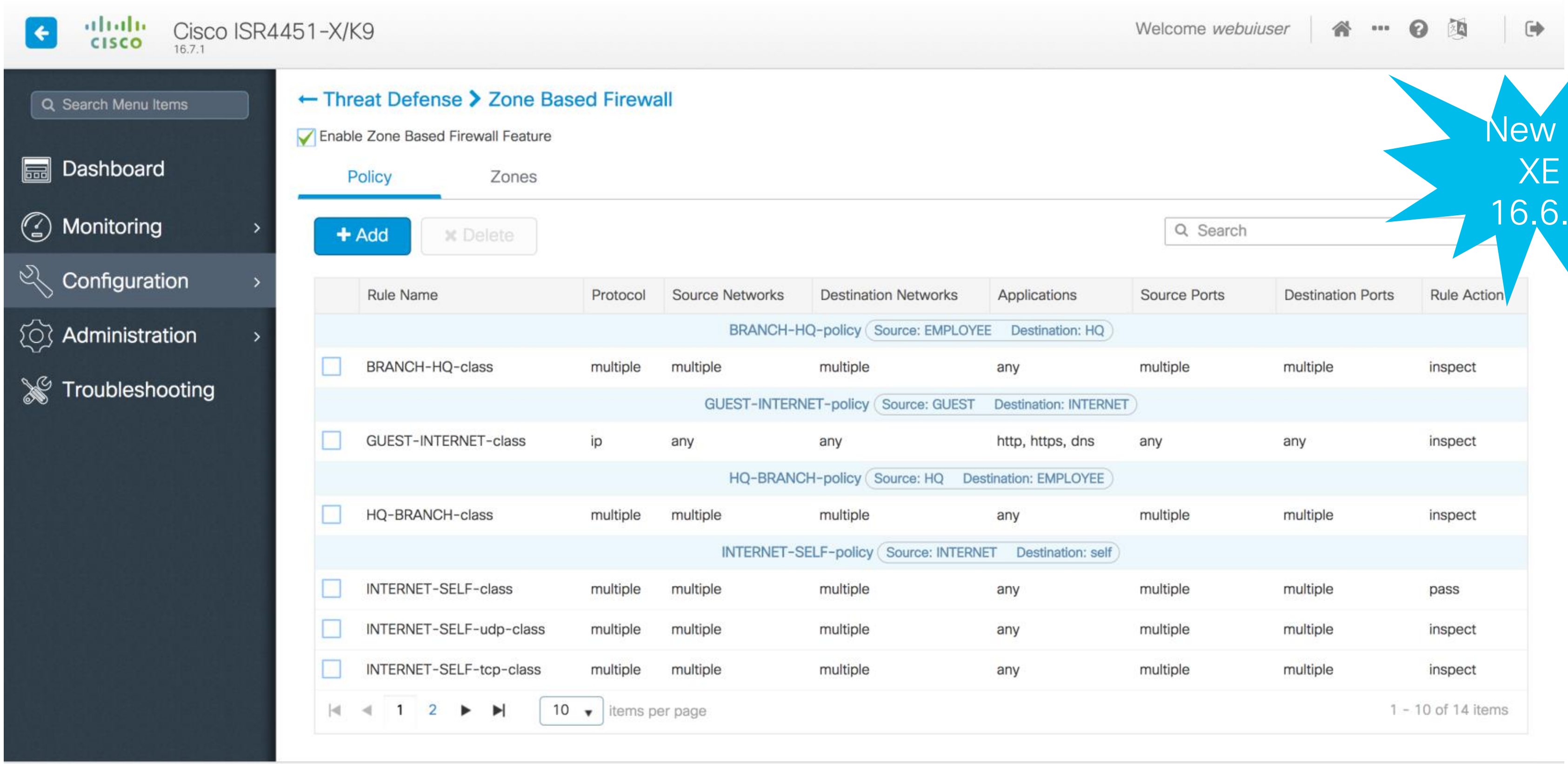
Feature Category: CLI

OS Version: 15.5(3)S1

Tags: ZBFW

```
#set ($Integer = 0)

#set ($DEFAULT_MATCH_CLASS = "default-protocol-class")
#set ($DEFAULT_INSPECT_POLICY = "default-protocol-policy")
#set ($PERMIT_ALL_ACL = "permit-all-acl")
#set ($PERMIT_ALL_CLASS = "permit-all-class")
#set ($PERMIT_ALL_POLICY = "permit-all-policy")
#set ($PERMIT_ALL_SET = false)

#macro (getCIRDFromSubnetAndMask $cidr)
#set ($subnet = $cidr.split("/")[0])
#set ($prefix = $cidr.split("/")[1])
#set ($mask = "")
#set ($start = 0)
```

On-box WebUI - Zone Based Firewall



☑ Enable Zone Based Firewall Feature

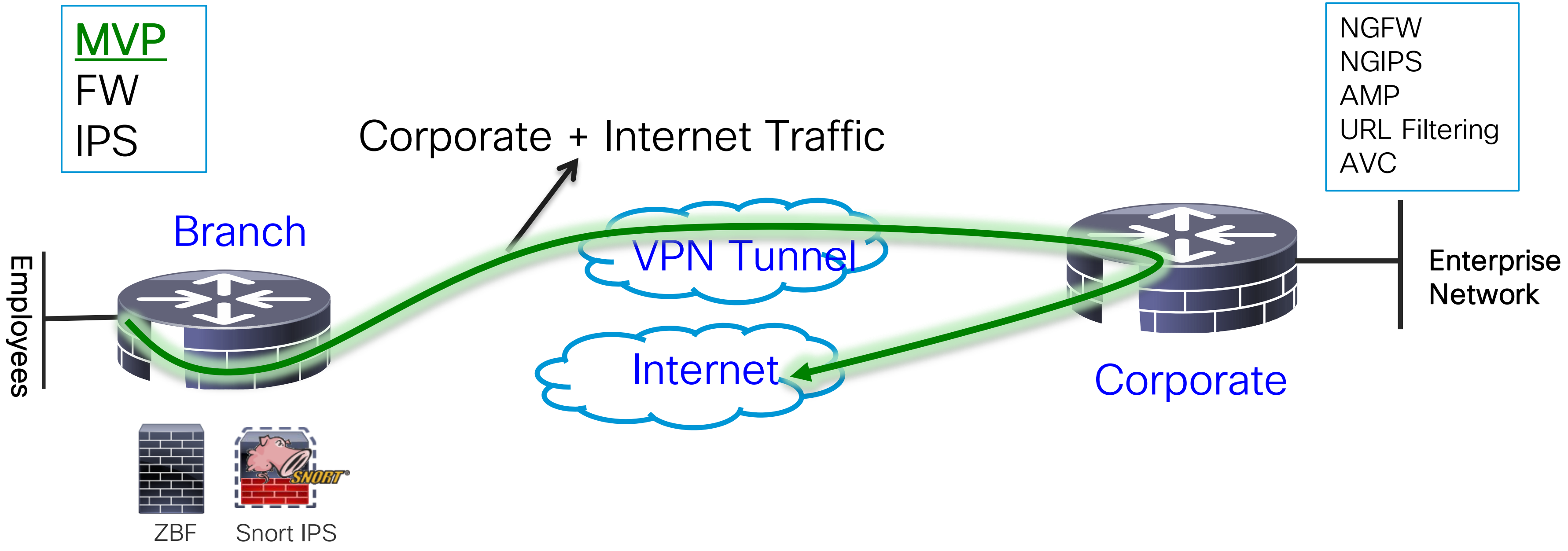
	Rule Name	Protocol	Source Networks	Destination Networks	Applications	Source Ports	Destination Ports	Rule Action
	BRANCH-HQ-policy (Source: EMPLOYEE Destination: HQ)							
□	BRANCH-HQ-class	multiple	multiple	multiple	any	multiple	multiple	inspect
	GUEST-INTERNET-policy (Source: GUEST Destination: INTERNET)							
□	GUEST-INTERNET-class	ip	any	any	http, https, dns	any	any	inspect
	HQ-BRANCH-policy (Source: HQ Destination: EMPLOYEE)							
□	HQ-BRANCH-class	multiple	multiple	multiple	any	multiple	multiple	inspect
	INTERNET-SELF-policy (Source: INTERNET Destination: self)							
□	INTERNET-SELF-class	multiple	multiple	multiple	any	multiple	multiple	pass
□	INTERNET-SELF-udp-class	multiple	multiple	multiple	any	multiple	multiple	inspect
□	INTERNET-SELF-tcp-class	multiple	multiple	multiple	any	multiple	multiple	inspect

1 2 | 10 items per page | 1 - 10 of 14 items

New in XE 16.6.1

Snort IPS

Snort IPS Use Case: Meet PCI Compliance



Value Prop

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

Examples:
Retail stores
Hospitals / Pharmacies

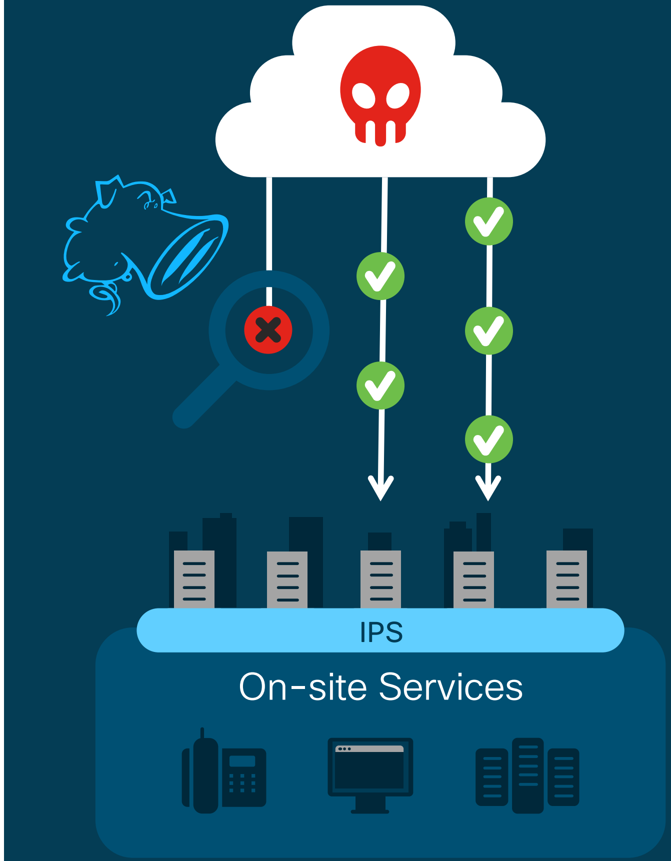
Snort IPS - Appendix

For Your Reference

- 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
- TCO – Total Cost of Ownership
- ASD – Automated Software Delivery

Snort IPS – What is it?

- Lightweight IPS/IDS
- Over 4 million downloads
- 500,000 registered users
- Most widely deployed IPS in the world



Snort IPS – Benefits and Requirements

Benefits

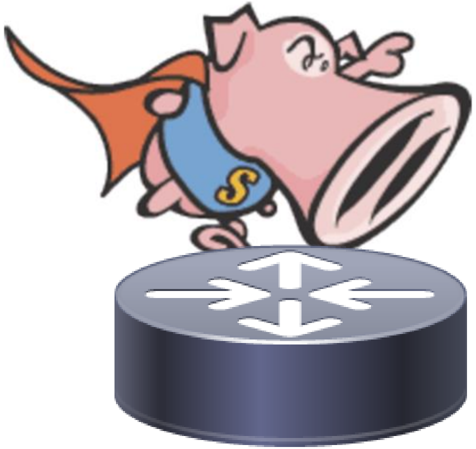
- Helps meet PCI* compliance.
- Threat protection built into ISR and ISRv branch routers
- Complements ISR Integrated Security
- Lightweight IPS solution with low TCO* and automated signature updates
- Supports VRF (16.6)

Requirements

- SEC-K9 license
- 4 GB memory upgrade
- XE 3.16.1 and above on ISR
- XE 16.8.1 and above on ISRv
- Subscription (1Yr, 3Yr)
- Monitoring via 3-rd party

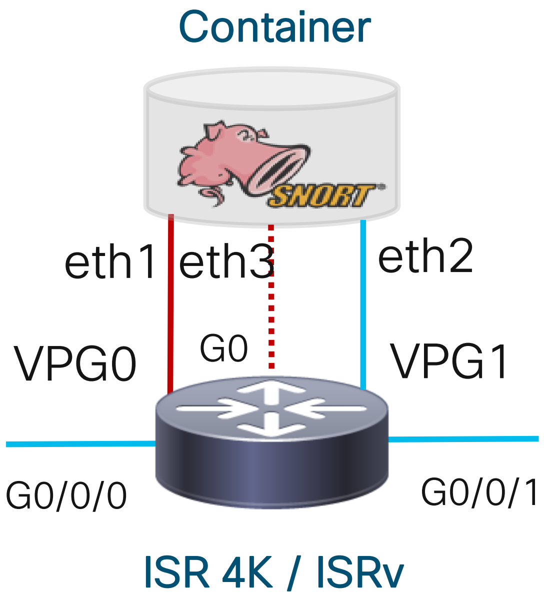
splunk>

SNORT IPS



* PCI – Payment Card Industry * TCO – Total Cost of Ownership

Snort IPS Configuration –Virtual Service Networking



Purpose of the VPGs

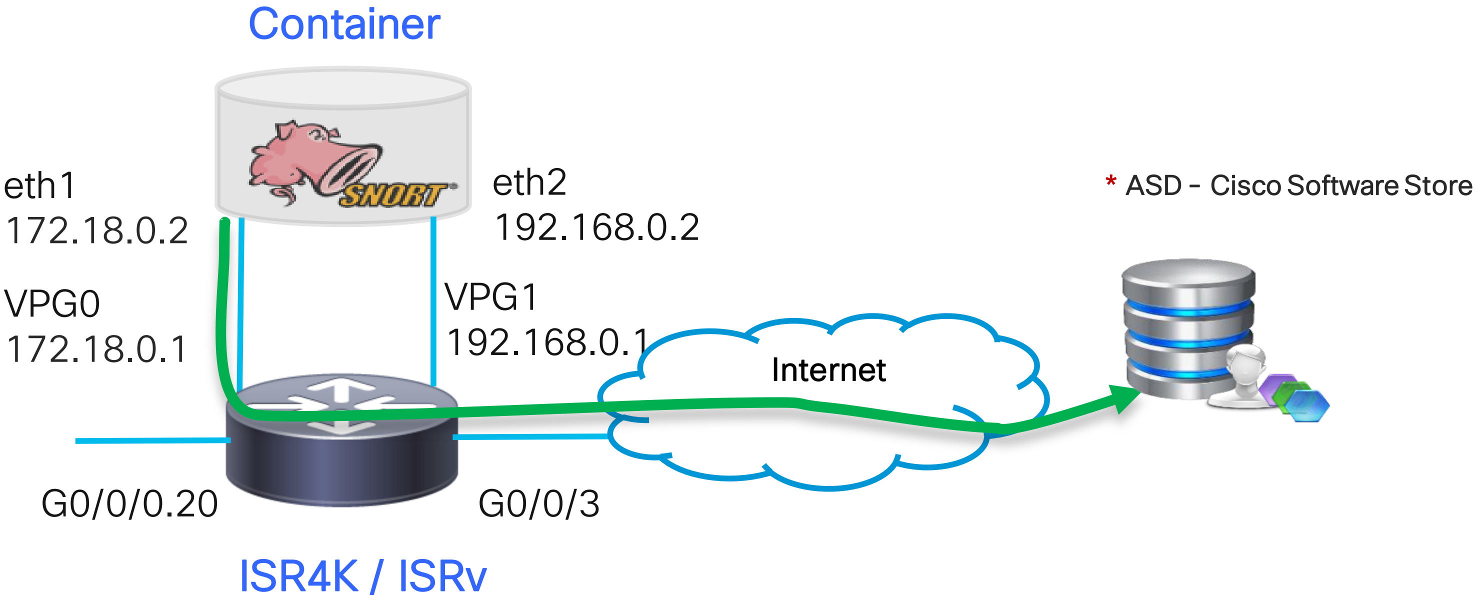
- VPG1 <==> eth2 (data plane)
- VPG0 <==> eth1 (Container Management *)

[OR]

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

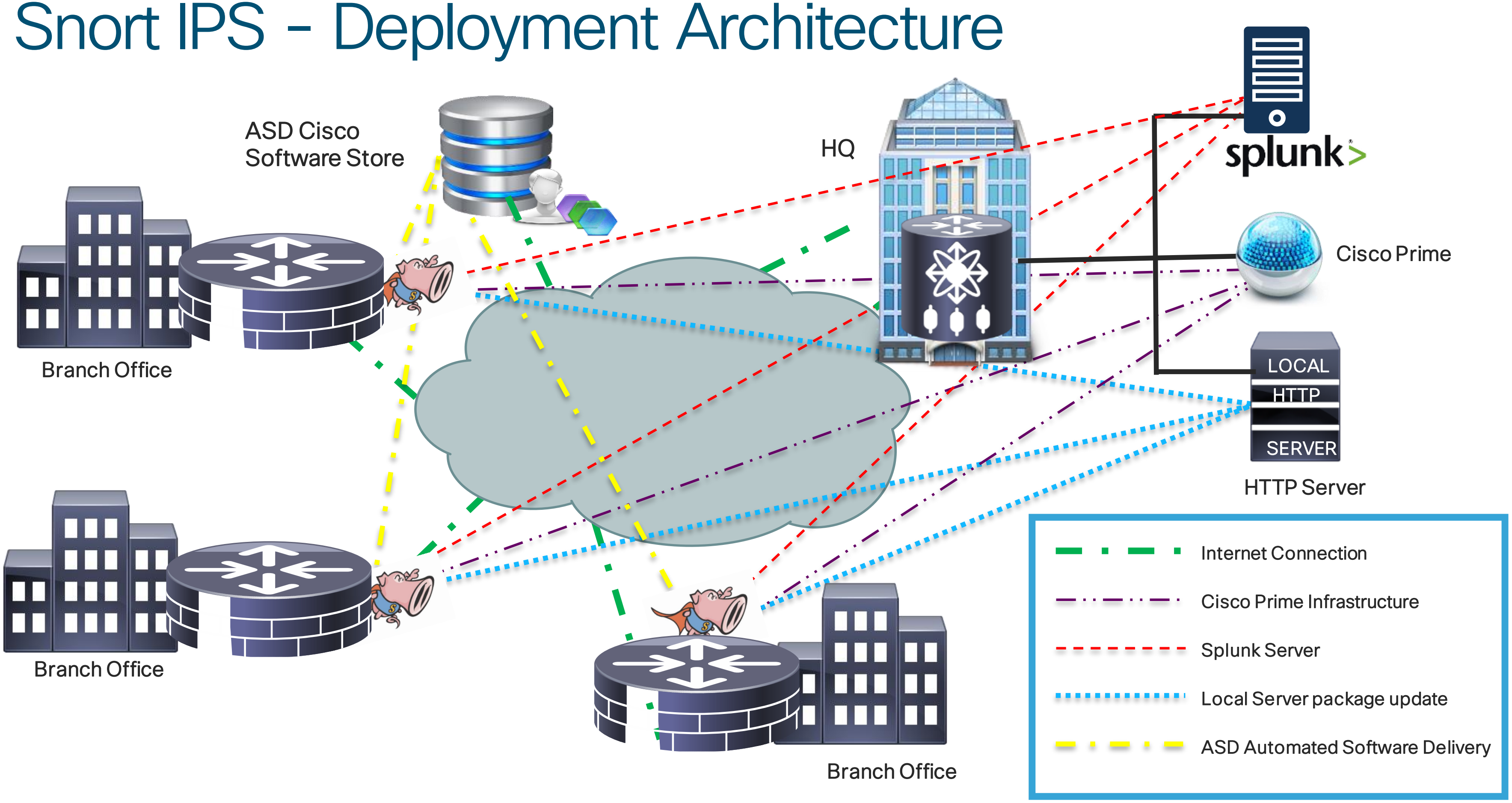
* Proper NAT and/or Routing has to be provided for VPG0 to reach the internet

Snort IPS – Update signature package

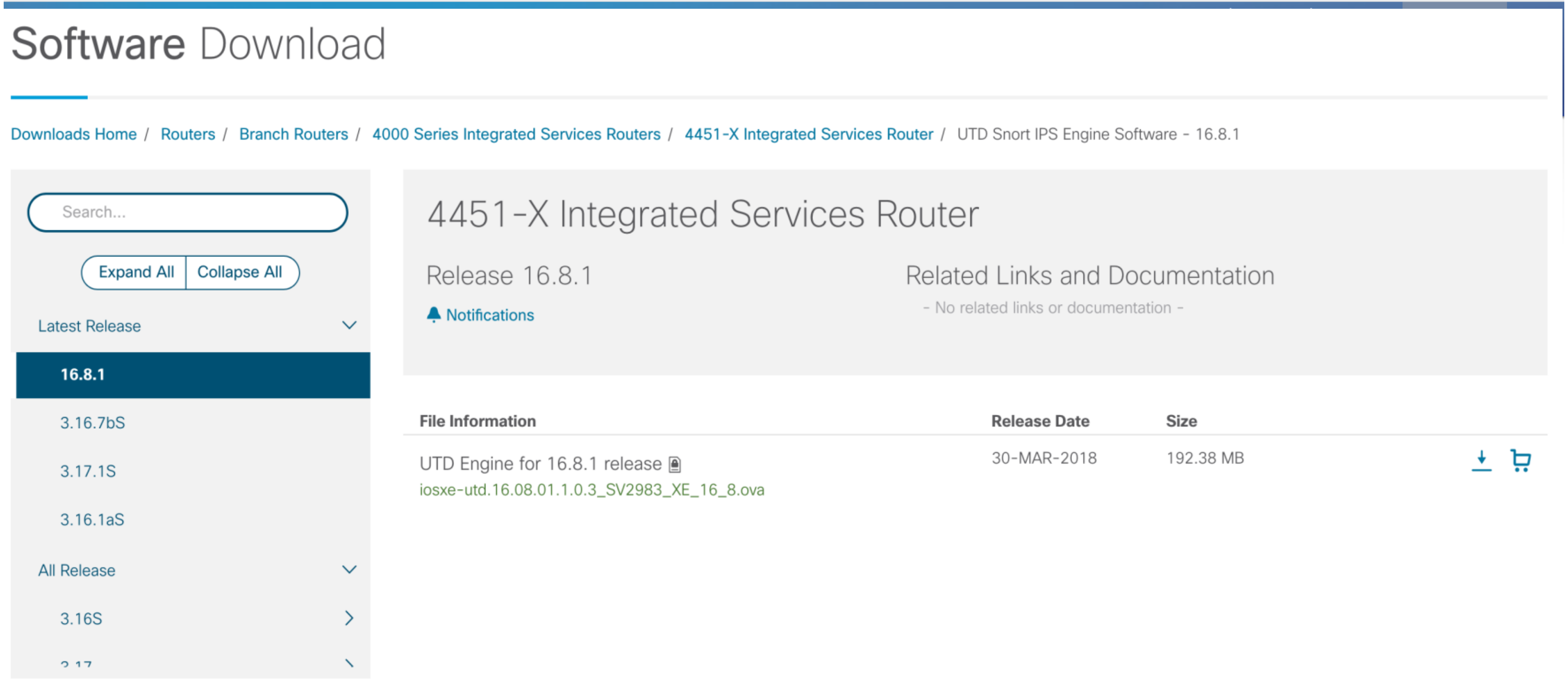


* ASD – Automated Software Delivery

Snort IPS - Deployment Architecture



Snort IPS – Download matching IOS-XE and Snort IPS Engine ova



Software Download

Downloads Home / Routers / Branch Routers / 4000 Series Integrated Services Routers / 4451-X Integrated Services Router / UTD Snort IPS Engine Software - 16.8.1

4451-X Integrated Services Router

Release 16.8.1

Notifications

Related Links and Documentation

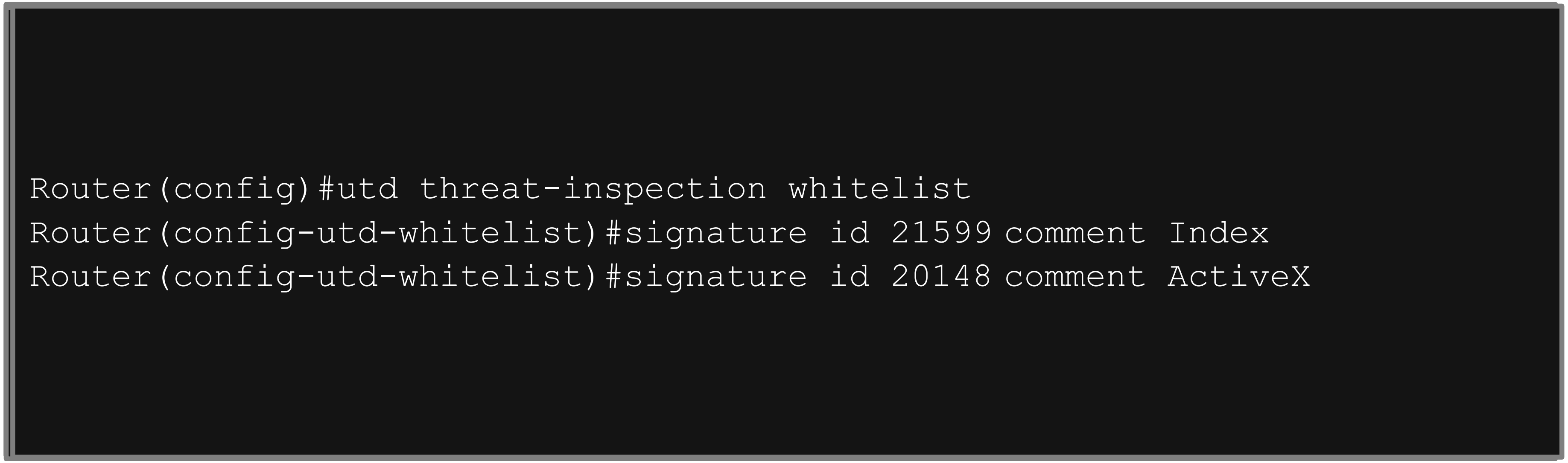
- No related links or documentation -

File Information	Release Date	Size
UTD Engine for 16.8.1 release iosxe-utd.16.08.01.1.0.3_SV2983_XE_16_8.ova	30-MAR-2018	192.38 MB

https://software.cisco.com/download/type.html?mdfid=284389362&catid=null

Snort IPS – Configuration

Step 6 – Whitelisting (Optional)



```
Router(config)#utd threat-inspection whitelist
Router(config-utd-whitelist)#signature id 21599 comment Index
Router(config-utd-whitelist)#signature id 20148 comment ActiveX
```

Snort IPS – Configuration

Step 1 Configure virtual service

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

Step 2 Configure Port Groups

```
interface VirtualPortGroup0
  description Management interface
  ip address 172.18.21.1 255.255.255.252
Interface VirtualPortGroup1
  description Data interface
  ip address 192.168.0.1 255.255.255.252
```

Step 3 Activate virtual service and configure

```
virtual-service myips
  vnic gateway VirtualPortGroup0
    guest ip address 172.18.21.2
  vnic gateway VirtualPortGroup1
    guest ip address 192.168.0.2
  activate
```

Step 4 Configuring UTD (service plane)

```
utd engine standard
 threat-inspection
  threat protection (protection-ips, detection-ids)
  policy security (balanced, connectivity)
  logging server 10.12.5.55 syslog level warning
   signature update server cisco username <blah>
   signature update occur-at daily 0 0
    whitelist
```

Step 5 Enabling UTD (data plane)

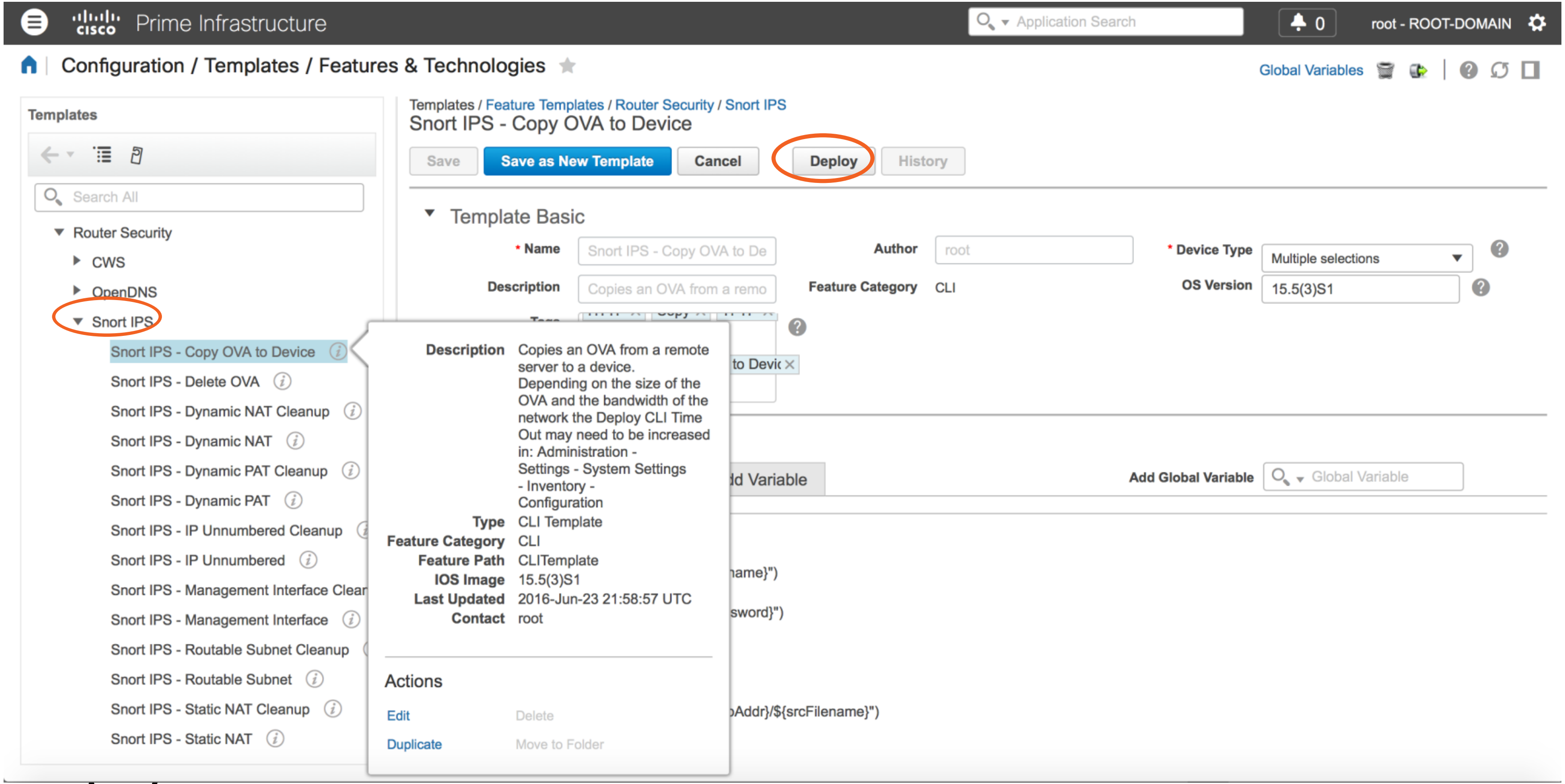
```
utd
all-interfaces
engine standard
 fail close
```

```
interface G0/0/2.20
  utd enable
```

Step 6 Whitelisting (optional)

```
utd threat-inspection whitelist
  signature id 21599 comment Index
  signature id 20148 comment ActiveX
```

Snort IPS – Provisioning (Prime Infrastructure 3.1 and above)


Prime Infrastructure
Application Search
0
root - ROOT-DOMAIN
Configuration / Templates / Features & Technologies
Global Variables
Templates
Search All
Router Security
CWS
OpenDNS
Snort IPS
Snort IPS - Copy OVA to Device
Snort IPS - Delete OVA
Snort IPS - Dynamic NAT Cleanup
Snort IPS - Dynamic NAT
Snort IPS - Dynamic PAT Cleanup
Snort IPS - Dynamic PAT
Snort IPS - IP Unnumbered Cleanup
Snort IPS - IP Unnumbered
Snort IPS - Management Interface Clear
Snort IPS - Management Interface
Snort IPS - Routable Subnet Cleanup
Snort IPS - Routable Subnet
Snort IPS - Static NAT Cleanup
Snort IPS - Static NAT
Templates / Feature Templates / Router Security / Snort IPS
Snort IPS - Copy OVA to Device
Save
Save as New Template
Cancel
Deploy
History
Template Basic

* Name	Snort IPS - Copy OVA to De	Author	root	* Device Type	Multiple selections
Description	Copies an OVA from a remo	Feature Category	CLI	OS Version	15.5(3)S1

to Devic ×

ld Variable

Add Global Variable: Global Variable

ame}")

sword}")

Addr}/${srcFilename}")

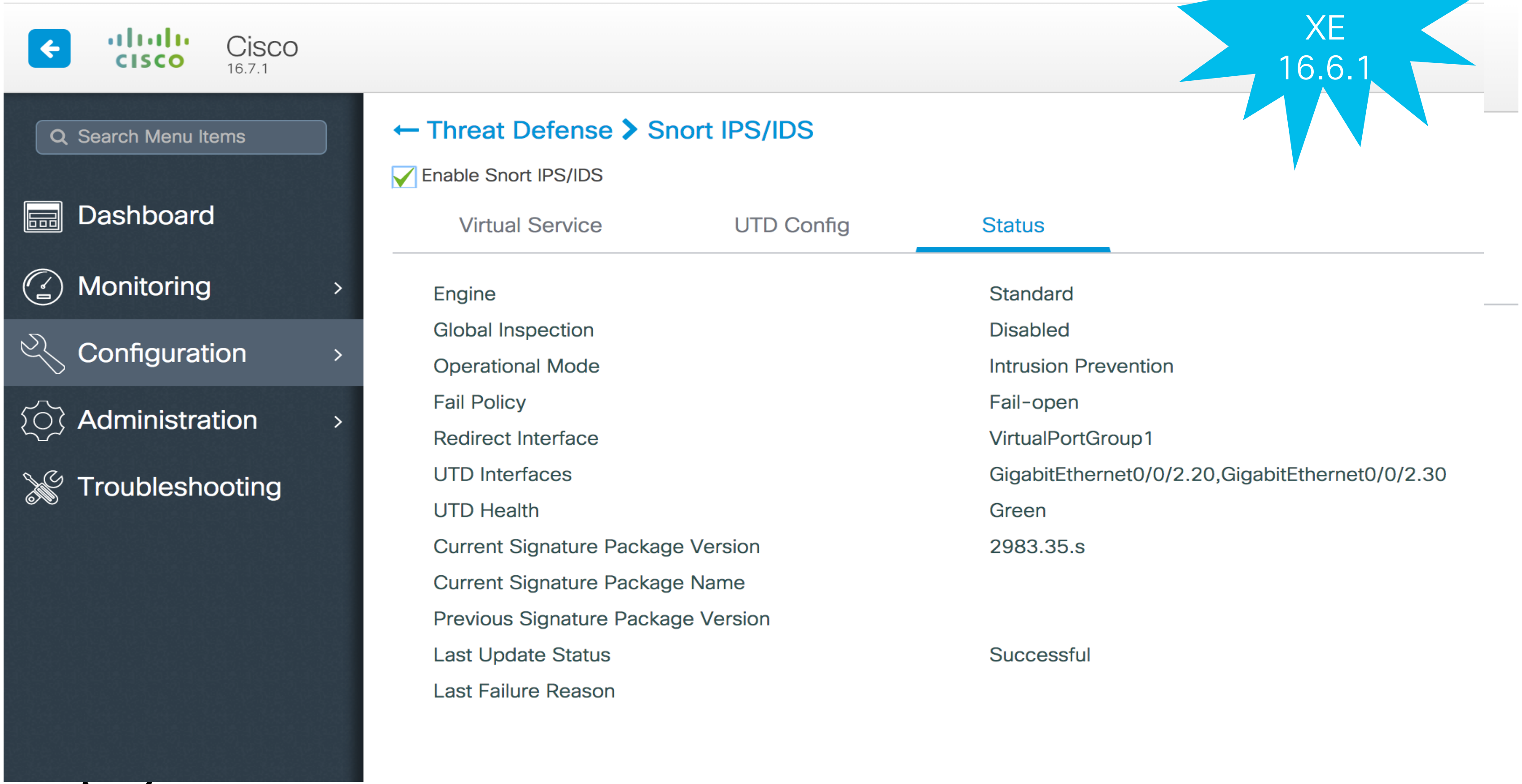
Description	Copies an OVA from a remote server to a device. Depending on the size of the OVA and the bandwidth of the network the Deploy CLI Time Out may need to be increased in: Administration - Settings - System Settings - Inventory - Configuration
Type	CLI Template
Feature Category	CLI
Feature Path	CLITemplate
IOS Image	15.5(3)S1
Last Updated	2016-Jun-23 21:58:57 UTC
Contact	root

Actions

Edit · Delete · Duplicate · Move to Folder

On-box WebUI - Snort IPS/IDS

NEW in XE 16.6.1



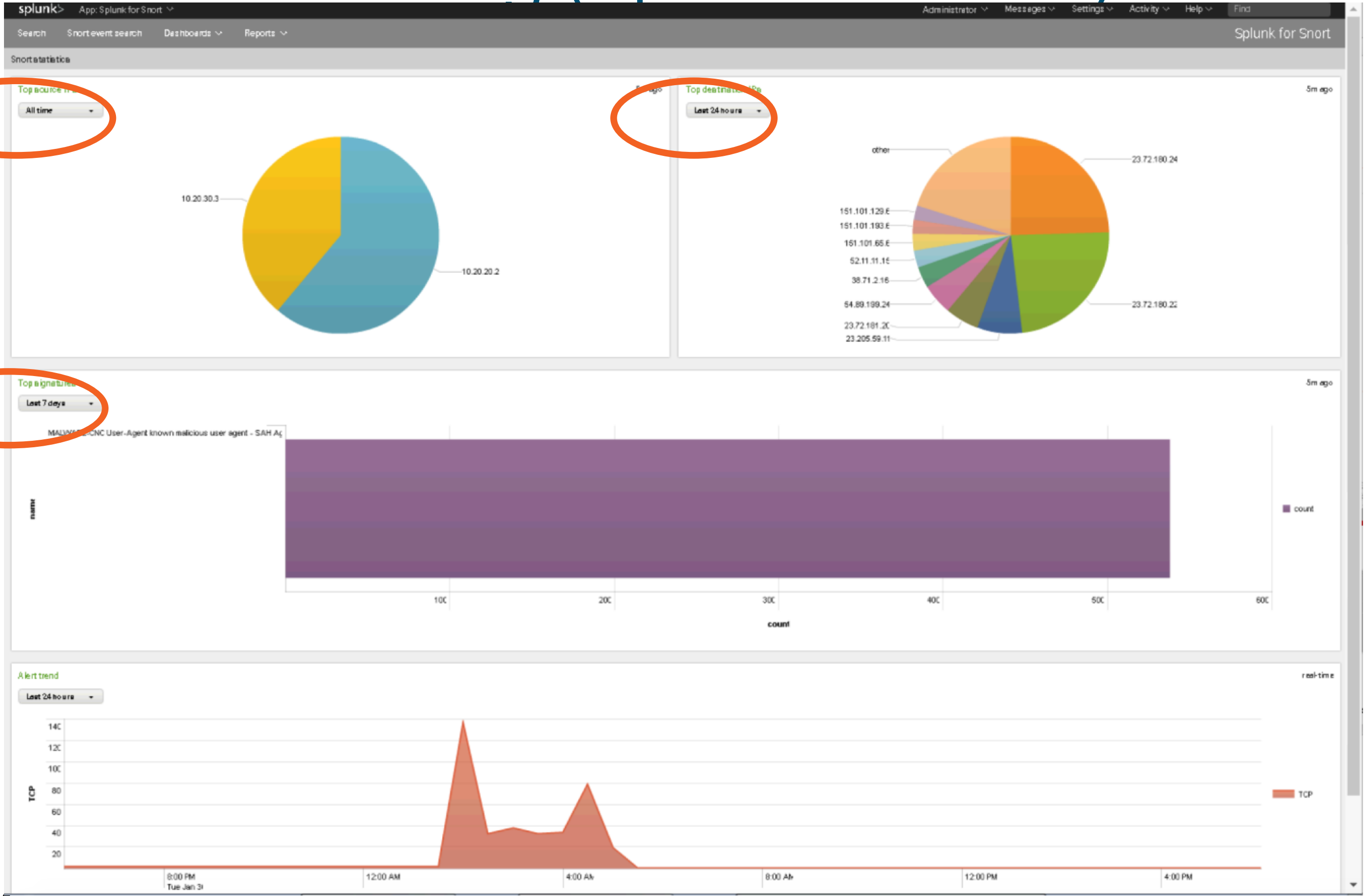
← Threat Defense > Snort IPS/IDS

☑ Enable Snort IPS/IDS

Virtual Service | UTD Config | **Status**

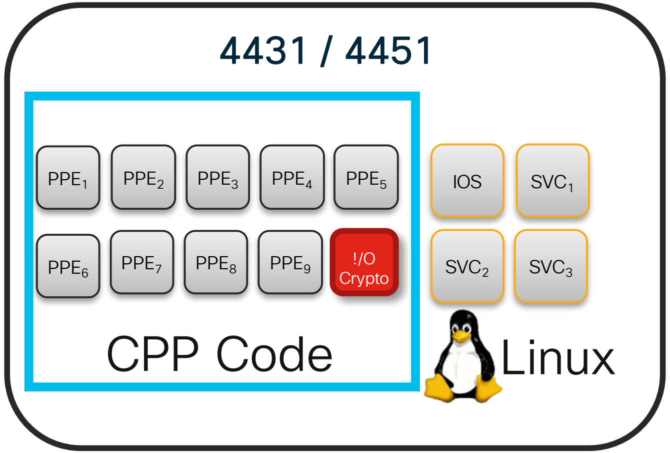
Engine	Standard
Global Inspection	Disabled
Operational Mode	Intrusion Prevention
Fail Policy	Fail-open
Redirect Interface	VirtualPortGroup1
UTD Interfaces	GigabitEthernet0/0/2.20,GigabitEthernet0/0/2.30
UTD Health	Green
Current Signature Package Version	2983.35.s
Current Signature Package Name	
Previous Signature Package Version	
Last Update Status	Successful
Last Failure Reason	

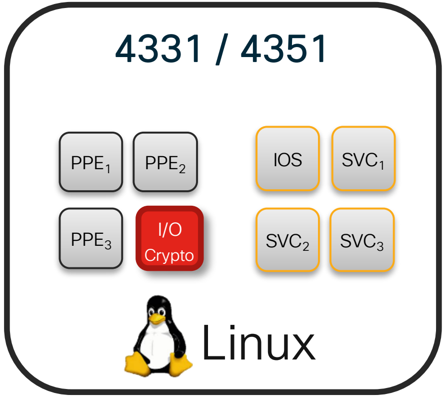
Snort IPS – Monitoring (Splunk for Snort)

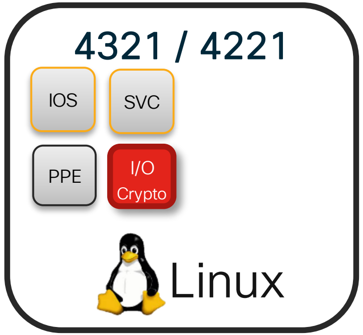


https://splunkbase.splunk.com/app/340/

Snort IPS – Profile Configuration







	PPE Cores Without Performance License	PPE Cores With Performance License
4221	1 x PPE + 1 x I/O	No change
4321	1 x PPE + 1 x I/O	No change
4331	2 x PPE + 1 x I/O	3 x PPE + 1 x I/O
4351	2 x PPE + 1 x I/O	3 x PPE + 1 x I/O
4431	3 x PPE + 1 x I/O	5 x PPE + 1 x I/O
4451	5 x PPE + 1 x I/O	9 x PPE + 1 x I/O

	Total No of CP Cores	Low Profile % of CPU	Medium Profile % of CPU	High Profile % of CPU
4221	2	50%	_	_
4321	2	50%	_	_
4331	4	25%	50%	75%
4351	4	25%	50%	75%
4431	4 (8)	25%	50%	75%
4451	4 (8)	25%	50%	75%

Snort IPS - ISR 4400 Performance (16.3.5)

For Your Reference

Platform	Profile	Avg Throughput	Avg CPS	Snort CPU	Snort Memory% (MB)
ISR-4451	High	485 Mbps	3235	93%	5.2% (845MB)
	Medium	300 Mbps	2020	91%	5.2% (845MB)
	Low	165 Mbps	1107	92%	5.2% (845MB)
ISR4431	High	265 Mbps	1760	93%	5.2% (845MB)
	Medium	130 Mbps	870	91%	5.2% (845MB)
	Low	80 Mbps	540	90%	5.2% (845MB)

Snort IPS - ISR 4300 Performance (16.3.5)

For Your Reference

Platform	Profile	Avg Throughput	Avg CPS	Snort CPU	Snort Memory% (MB)
ISR4351	High	275 Mbps	1836	93%	5.1% (829MB)
	Medium	180 Mbps	1218	91%	5.2% (845MB)
	Low	100 Mbps	668	92%	5.1% (829MB)
ISR4331	High	190 Mbps	1250	80%	5.2% (829MB)
	Medium	160 Mbps	1070	92%	5.2% (829MB)
	Low	80 Mbps	550	91%	5.2% (829MB)
ISR4321	Low	88 Mbps	590	90%	8.2% (656MB)

Snort IPS - ISR 4200 Performance (16.6.2)

For Your Reference

Platform	Profile	Avg Throughput	Avg CPS	Snort CPU	Snort Memory% (MB)
ISR4221	Low	70 Mbps	460	96%	20%

Snort IPS - ISRv Performance (16.8)

For Your Reference

Platform	Profile	Avg Throughput	Avg CPS	Snort CPU	Snort Memory% (MB)
ENCS 5412	Low	120 Mbps	831	91%	13%
ENCS 5408	Low	230 Mbps	1600	96%	9.9%

Snort IPS - Resources

For Your Reference

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

Snort IPS Deployment Guide
http://www.cisco.com/c/en/us/products/collateral/security/router-security/guide-c07-736629.html

Snort IPS – Guides

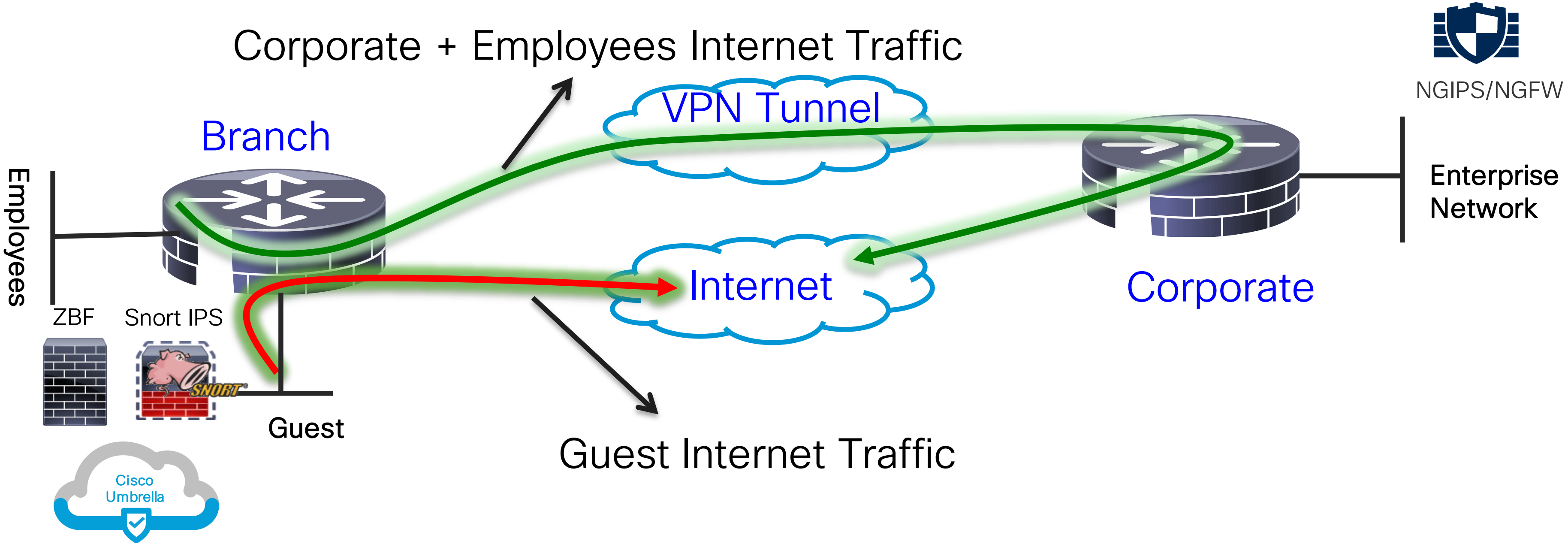
For Your Reference

Step-By-Step Guide
https://supportforums.cisco.com/t5/security-documents/snort-ips-on-isr-isrv-and-csr-step-by-step-configuration/ta-p/3369186

Troubleshooting Guide
https://supportforums.cisco.com/t5/security-documents/snort-ip-on-isr-isrv-and-csr-troubleshooting/ta-p/3369225

Cisco Umbrella Integration (OpenDNS)

Use Case: Guest Internet Access



- ➢ VLAN separation, guest and employees network are separated
- ➢ ZBFW blocks guest to employees traffic and vice versa
- ➢ Cisco Umbrella provides content filtering and policy enforcement
- ➢ Snort IPS provides basic intrusion protection
- ➢ Corporate devices reach Internet via HQ

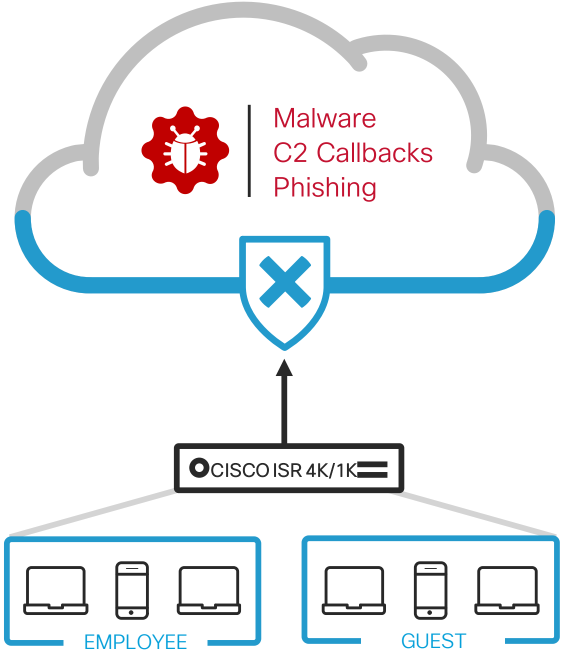
Examples:
Retail stores / Auto Dealerships
Hospitals / Pharmacies
Financials
Schools / Universities

Cisco Umbrella Integration

For Your Reference

- Token - Token is ONLY used for Device Registration and obtain Origin ID
- Origin ID – Device ID. Good until someone deletes that Network Device Identity from the dashboard
- EDNS – Extension mechanisms for DNS
- CFT – Common Flow Table
- PTR – Pointer Record
- DNSCrypt – Protocol that authenticates communications between a DNS client and a DNS resolver
- FQDN – Fully Qualified Domain Name
- API – Application Programming Interface
- ReST API – Representational State Transfer API
- FMAN – Forwarding Manager
- CPP – Cisco Packet Processor (external name is Quantum Flow Processor)
- CFT – Common Flow Table
- Phishing - The fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.

Cisco Umbrella Integration



DNS is the first step in internet connections and is used by all devices

Protect against malware, phishing and C2 callbacks

Enable domain filtering

Create policies for different network segments (e.g. employees and guests)

Review deployment and research incidents using reports

Umbrella Integration – Benefits and Requirements

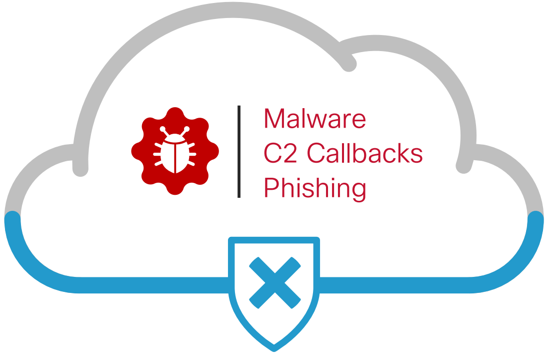
Benefits

- DNS layer protection
- No need to look within HTTP or HTTPS packets
- Complements ISR Integrated Security
- Configure per interface policies
- Supports HTTPS decryption
- Intelligent Proxy
- Supports VRF

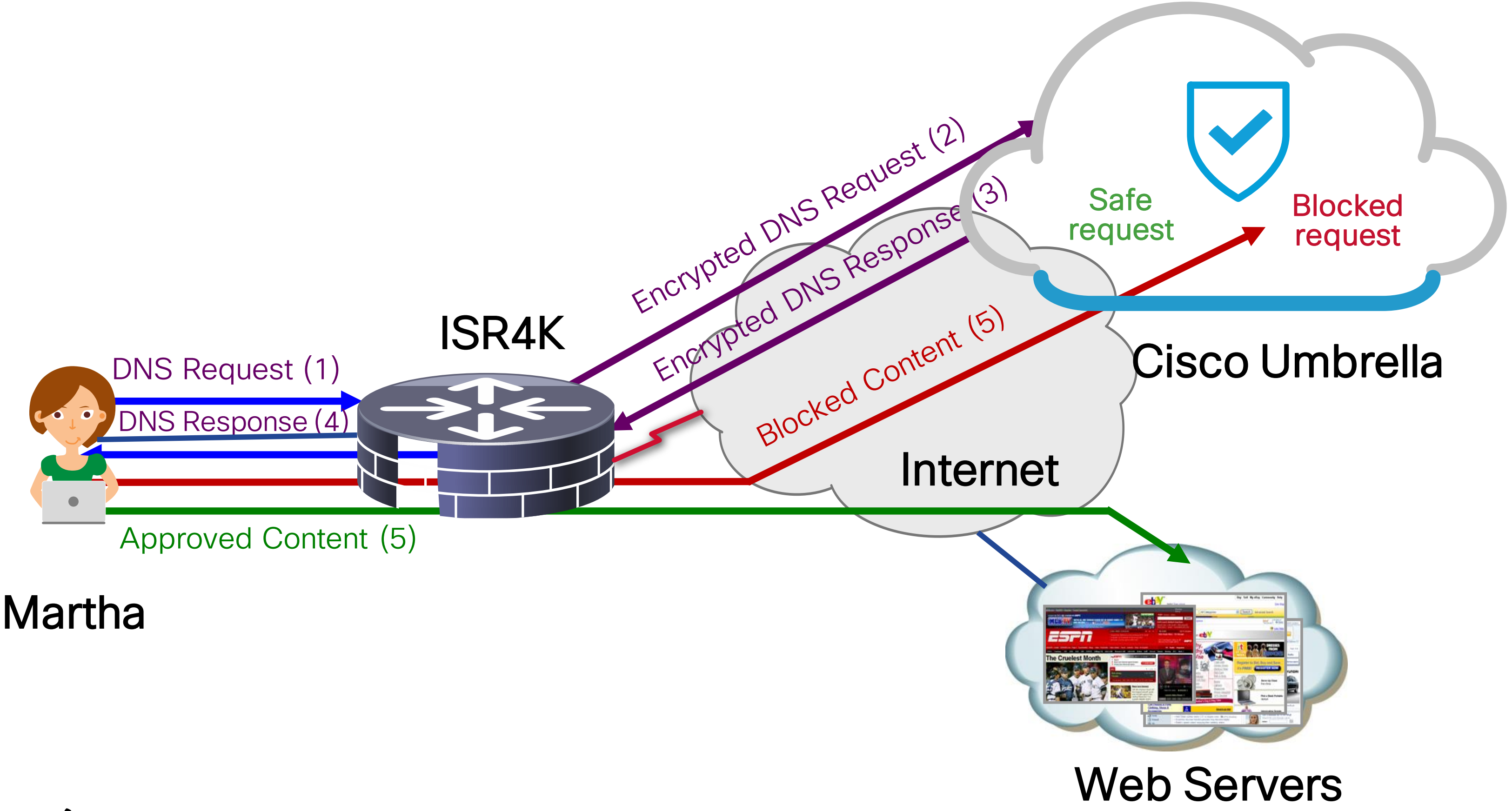
Requirements

- Provision to get token ID and portal login
- SEC-K9 license
- XE 16.3 and above on ISR 4K series routers
- XE 16.8.1 and above on ISRv and ISR 1K series routers
- Per device subscription
- Monitoring and Reporting via Umbrella Portal

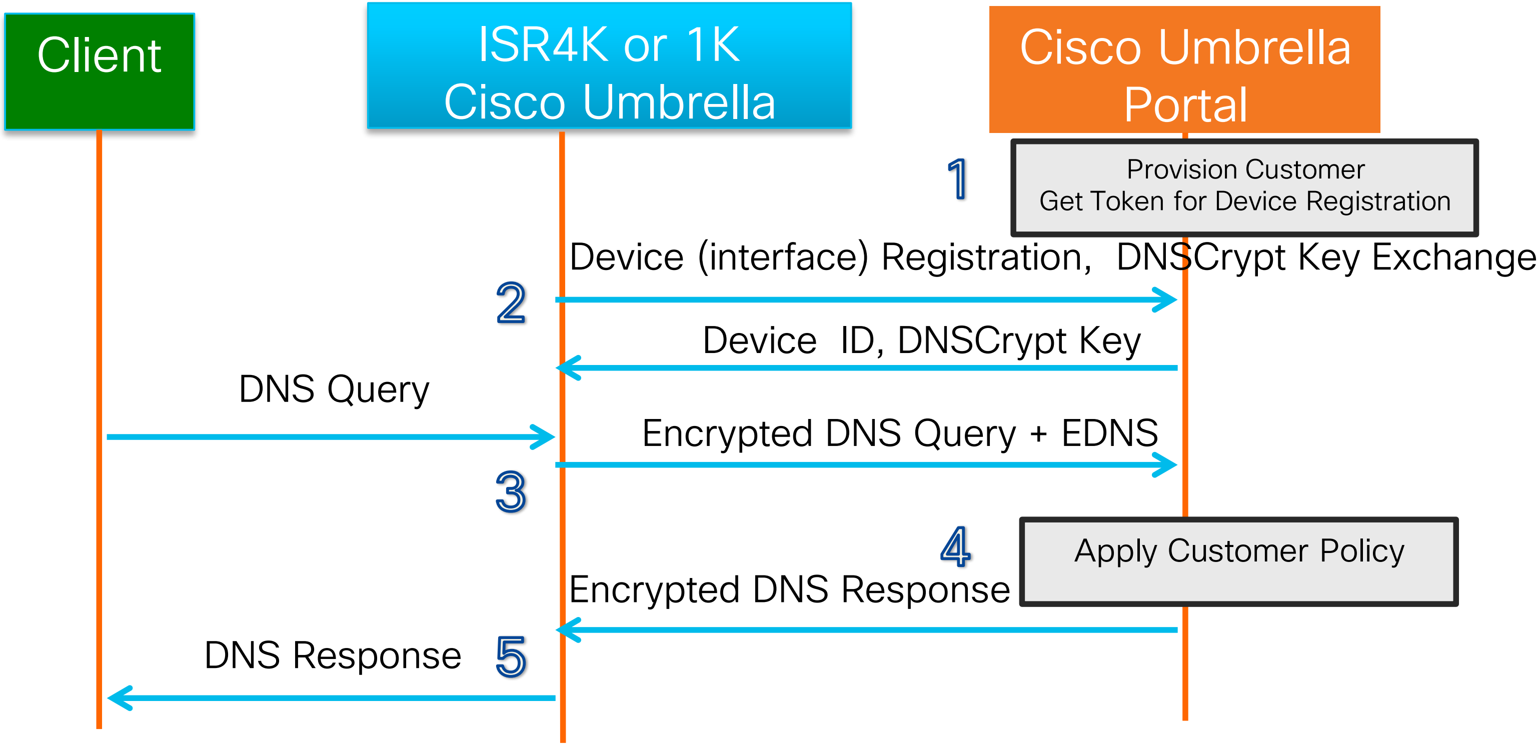
Cisco Umbrella



Cisco Umbrella Integration - Solution Overview



Cisco Umbrella Integration – Packet Flow with DNSCrypt



Client

ISR4K or 1K Cisco Umbrella

Cisco Umbrella Portal

1 Provision Customer
Get Token for Device Registration

2 Device (interface) Registration, DNSCrypt Key Exchange

Device ID, DNSCrypt Key

DNS Query

Encrypted DNS Query + EDNS

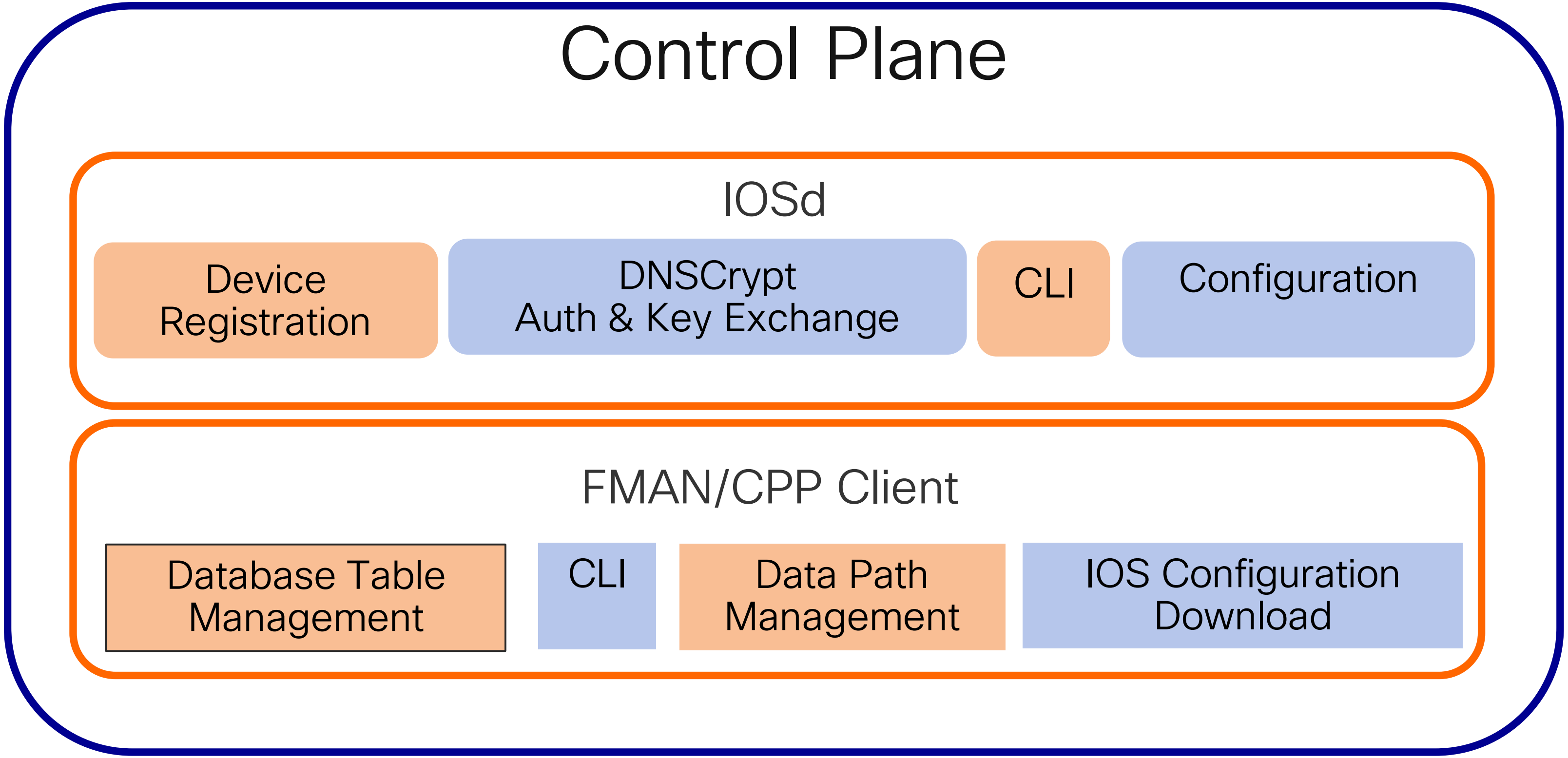
3

4 Apply Customer Policy

Encrypted DNS Response

5 DNS Response

Cisco Umbrella – Software Architecture



Control Plane

IOSd

Device Registration

DNSCrypt Auth & Key Exchange

CLI

Configuration

FMAN/CPP Client

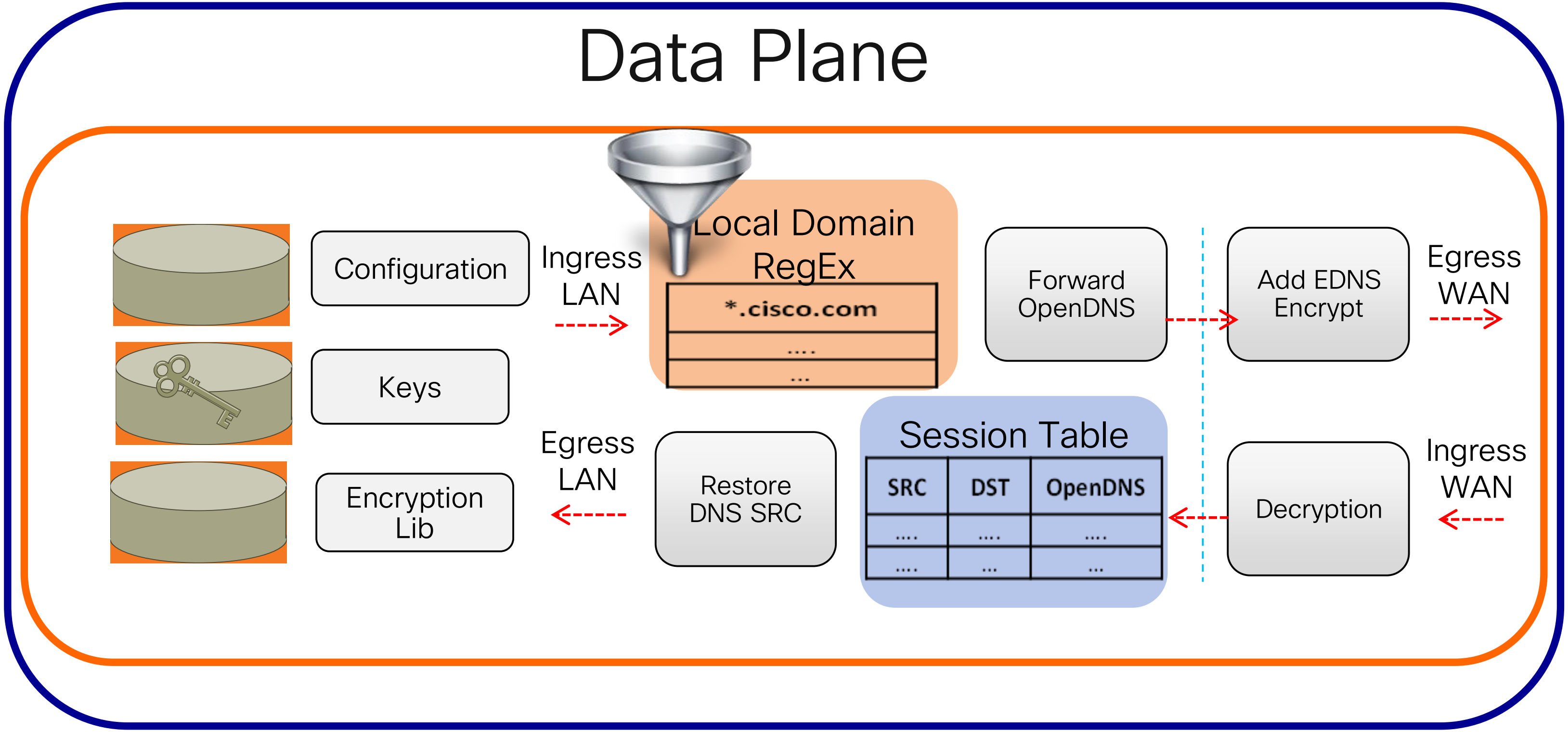
Database Table Management

CLI

Data Path Management

IOS Configuration Download

Cisco Umbrella – Software Architecture



Local Domain RegEx
*.cisco.com
….
…

Session Table

SRC	DST	OpenDNS
….	….	….
….	…	…

Cisco Umbrella Integration – Configuration

Step 3 – Enable Cisco Umbrella “out” and “in” with a tag

```
Router(config-if)#interface g0/0/0
Router(config-if)#description Internet facing
Router(config-if)#umbrella out


Router(config-if)#interface g0/0/1
Router(config-if)#description Guest facing
Router(config-if)#umbrella in Guest
```

https://www.digicert.com/CACerts/DigiCertSecureServerCA.crt - Certificate URL
http://www.cisco.com/security/pki/trs/ios_core.p7b - Certificate URL PKCS7 (p7b) format

“opendns” command has been changed to “umbrella” starting 16.6.1

Cisco Umbrella – Configuration

Step 1 Certificate import (mandatory for device registration via https)

```
Router(config)#crypto pki trustpool import terminal
% Enter PEM-formatted CA certificate.
% End with a blank line or "quit" on a line by itself.
30820494 3082037C A0030201 02021001
FDA3EB6E CA75C888 438B724B
....
quit
```

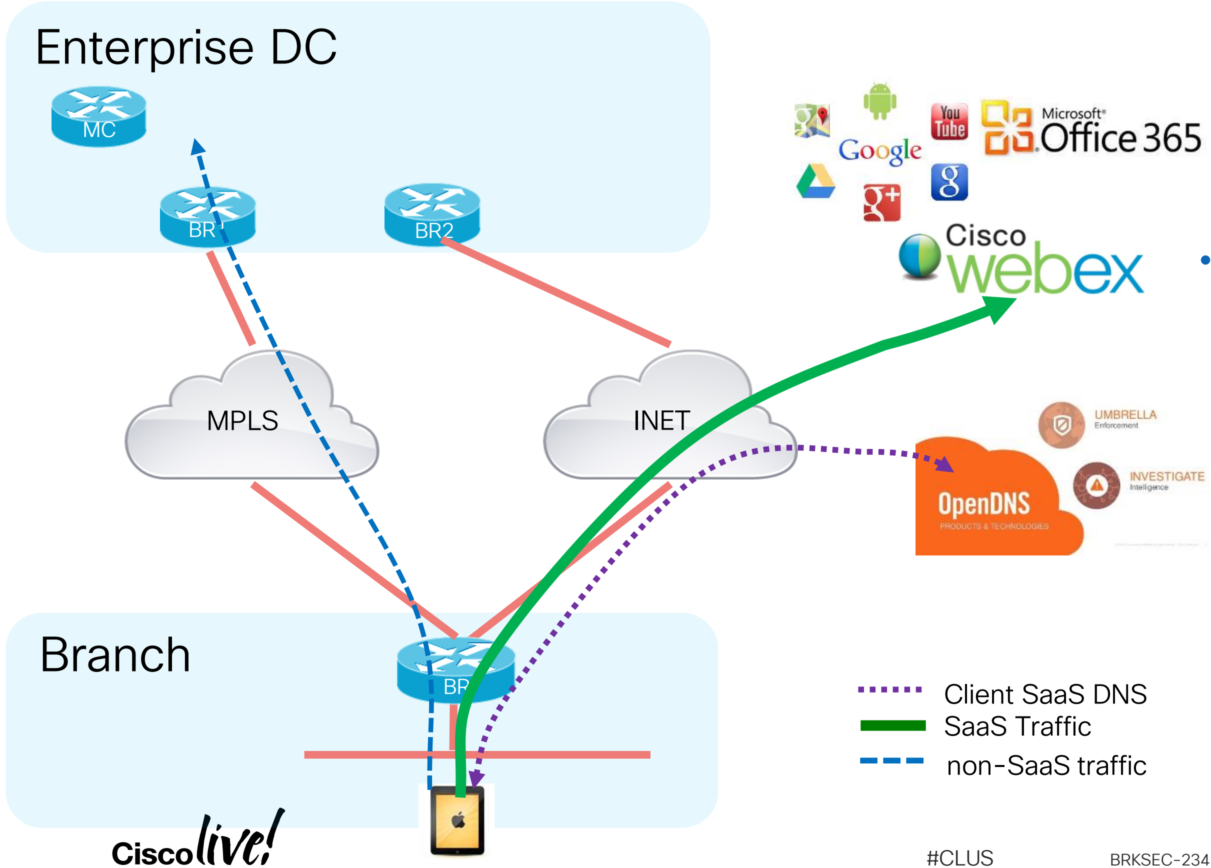
Step 2 Configure local domain (optional) and token

```
parameter-map type regex dns_bypass
pattern www.cisco.com
pattern .*eisg.cisco.*

Router(config)#parameter-map type umbrella
global
Router(config-profile)#token 562D3C7FF844001C70E7
0F32C32FEC26991C2B562D3C7FF844001C70E7
Router(config-profile)#local-domain dns_bypass
```

Step 3 Enable OpenDNS “out” and “in” with a tag

```
Router(config-if)#interface g0/0/0
Router(config-if)#description Internet facing
Router(config-if)#umbrella out
Router(config-if)#interface g0/0/1
Router(config-if)#description Guest facing
Router(config-if)#umbrella in Guest
```

Cisco Umbrella Integration - Direct Cloud Access



- Value Proposition

Cost down by elimination of SaaS apps backhaul to DC

Improved SaaS apps performance &security(Umbrella inspection and only SaaS DCA-ed)

Building blocks

NBAR: 1st packet classification and App visibility
SLA: Path performance measurement
PfR: Path selection and control
ODNS: location proximity(ODNS account not mandatory, can use a different DNS server)

Cisco Umbrella Integration – Direct Cloud Access

Requirements

- NBAR
- DNS traffic must traverse the ISR
- PfR
- XE 16.8.1 and above on ISR 4K series router

Step 1 Certificate import (mandatory for router registration via https)

```
Router(config)#crypto pki trustpool import terminal
% Enter PEM-formatted CA certificate.
% End with a blank line or "quit" on a line by itself.
30820494 3082037C A0030201 02021001
FDA3EB6E CA75C888 438B724B
....
8FAB492E 9D3B9334 281F78CE 94EAC7BD
D3C96D1C DE5C32F3
quit
```

https://www.digicert.com/CACerts/DigiCertSecureServerCA.crt - Certificate URL
http://www.cisco.com/security/pki/trs/ios_core.p7b - Certificate URL PKCS7 (p7b) format

Cisco Umbrella Integration - Direct Cloud Access

Step 2 PfR - Hub MC

```
domain DCA
 vrf default
  master hub
  class DCA sequence 4
    match application amazon-web-services custom
               priority 1 one-way-delay threshold 500
    path-preference DCA2 fallback DCA1 next-fallback INET
  class DCA sequence 5
    match app-group ms-cloud-group policy custom
              priority 1 one-way-delay threshold 500
     path-preference DCA2 fallback DCA1 next-fallback INET
```

Step 3 PfR - Branch MC/BR (Single BR site)

```
domain DCA
master branch
  domain-map
      application ms-cloud-group domain
          http://www.office.com      dscp af21
      application amazon-web-services domain
          http://www.amazonaws.com dscp af21
```

Step 4 NBAR - Branch

```
class-map match-any DCA-list-CMAP
   match protocol attribute application-group ms-cloud-group
   match protocol amazon-web-services
policy-map type umbrella DCA-list-PMAP
   class DCA-list-CMAP
        direct-cloud-access
```

Cisco Umbrella Configuration – Direct Cloud Access

Step 5 Configure parameter-map with token

```
parameter-map type umbrella global
 token 0F32C32FEC26991C2B562D3C001C70E7
```

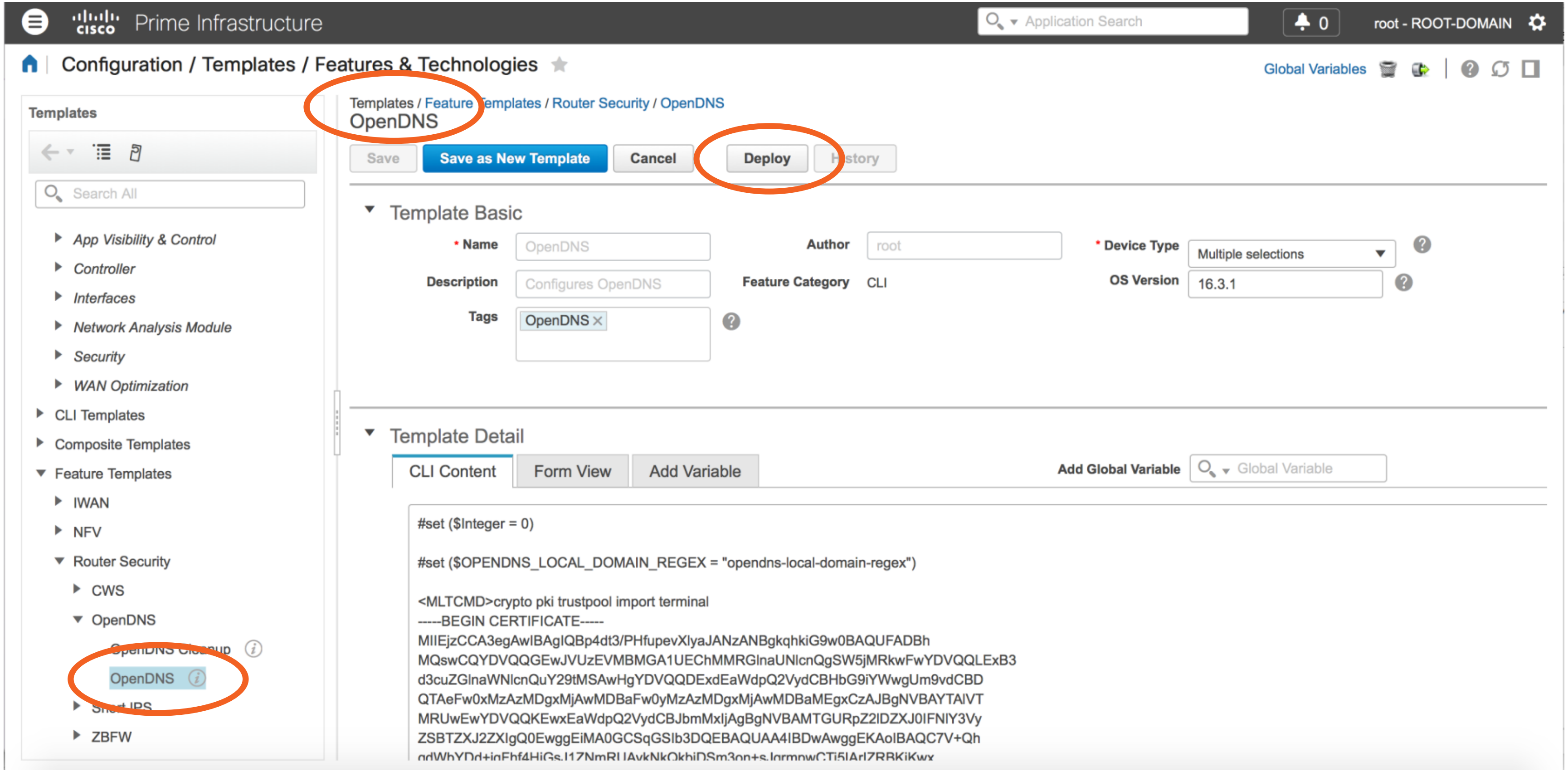
Step 7 Enable Umbrella “out”

```
interface g0/0/0
 domain path DCA1 direct-cloud-access
 umbrella out
```

Step 6 Enable Umbrella “in” with DCA

```
interface g0/0/1
 umbrella in direct-cloud-access DCA-list-PMAP
```

Cisco Umbrella – Provisioning (Prime Infrastructure 3.1 and above)



OpenDNS

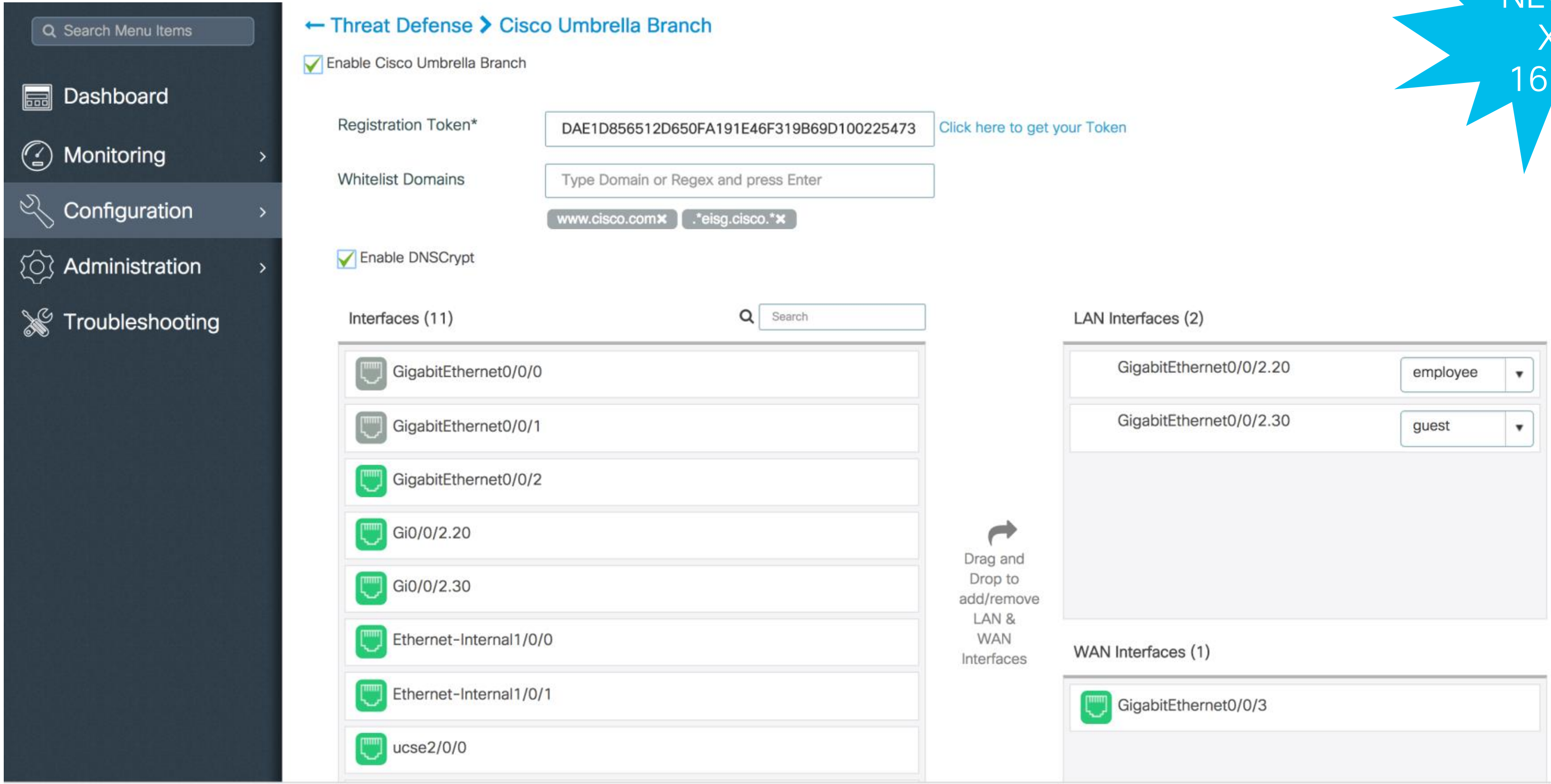
Template Basic

* Name	OpenDNS	Author	root	* Device Type	Multiple selections
Description	Configures OpenDNS	Feature Category	CLI	OS Version	16.3.1
Tags	OpenDNS ×				

```
#set ($Integer = 0)

#set ($OPENDNS_LOCAL_DOMAIN_REGEX = "opendns-local-domain-regex")

<MLTCMD>crypto pki trustpool import terminal
-----BEGIN CERTIFICATE-----
MIIEjzCCA3egAwIBAgIQBp4dt3/PHfupevXlyaJANzANBgkqhkiG9w0BAQUFADBh
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNlcnQuY29tMSAwHgYDVQQDExdEaWdpQ2VydCBHbG9iYWwgUm9vdCBD
QTAeFw0xMzAzMDgxMjAwMDBaFw0yMzAzMDgxMjAwMDBaMEgxCzAJBgNVBAYTAlVT
MRUwEwYDVQQKEwxEaWdpQ2VydCBJbmMxIjAgBgNVBAMTGURpZ2lDZXJ0IFNIY3Vy
ZSBTZXJ2ZXIgQ0EwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC7V+Qh
qdWbYDd+iqFhf4HiGsJ1ZNmRUAvkNkQkbiDSm3on+sJormpwCTi5lArlZRBKiKwx
```

On-box WebUI - Cisco Umbrella Integration

NEW in XE 16.6.1



← Threat Defense › Cisco Umbrella Branch

☑ Enable Cisco Umbrella Branch

Registration Token* DAE1D856512D650FA191E46F319B69D100225473 Click here to get your Token

Whitelist Domains Type Domain or Regex and press Enter

www.cisco.com✖ .*eisg.cisco.*✖

☑ Enable DNSCrypt

Interfaces (11)

- GigabitEthernet0/0/0
- GigabitEthernet0/0/1
- GigabitEthernet0/0/2
- Gi0/0/2.20
- Gi0/0/2.30
- Ethernet-Internal1/0/0
- Ethernet-Internal1/0/1
- ucse2/0/0

Drag and Drop to add/remove LAN & WAN Interfaces

LAN Interfaces (2)

GigabitEthernet0/0/2.20	employee ▾
GigabitEthernet0/0/2.30	guest ▾

WAN Interfaces (1)

- GigabitEthernet0/0/3

Cisco Umbrella Integration – Performance Numbers

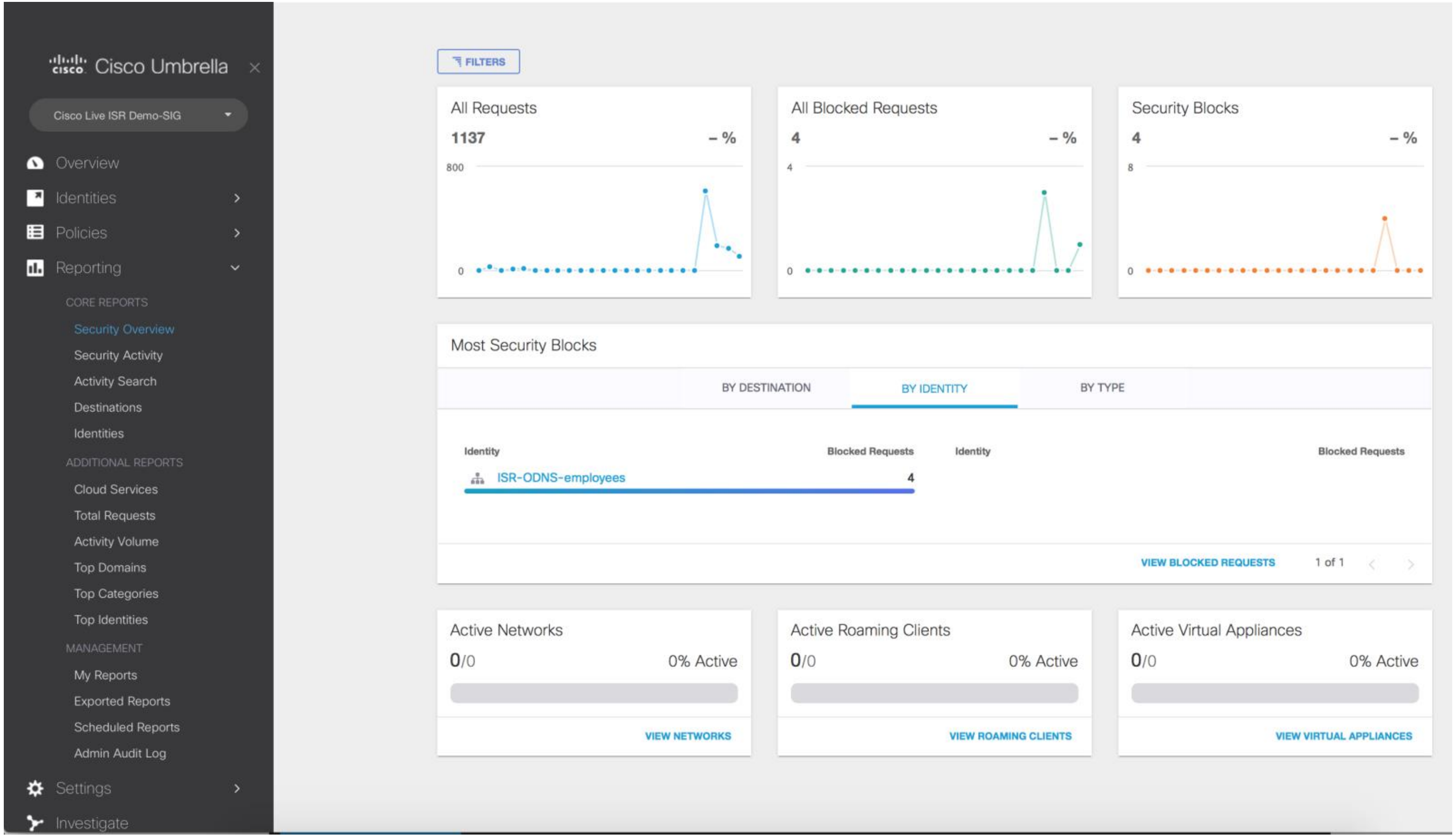
For Your Reference

Platform	Max Throughput License	Profile	Data Plane Throughput(Mbps)	CPU Utilization(%)
ISR 4451	1Gbps	EMIX	990	21
		EMIX with DNSCRYPT	920	60
		Plain DNS	350	66 *
		Plain DNSCRYPT	205	99
ISR4321	100Mbps	EMIX	94	25
		EMIX with DNSCRYPT	65	71
		Plain DNS	100	100
		Plain DNSCRYPT	61	100
ISRv	1Gbps	EMIX	830	15
		EMIX with DNSCRYPT	810	22
		Plain DNS	230	54 **
		Plain DNSCRYPT	70	99

* Could not reach max CPU because CFT cap of 250K was reached
** Could not reach max CPU because CFT cap of 50K was reached

EMIX Profile: HTTP 50%, FTP 12%, IMAP 13%, SMTP 15% DNS 10%
Objective set in IxLoad: 100 Simulated Users

Cisco Umbrella – Monitoring and Reporting Using Umbrella Portal



All Requests 1137 – %

All Blocked Requests 4 – %

Security Blocks 4 – %

Most Security Blocks

Identity	Blocked Requests	Identity	Blocked Requests
ISR-ODNS-employees	4		

Active Networks 0/0 0% Active

Active Roaming Clients 0/0 0% Active

Active Virtual Appliances 0/0 0% Active

Cisco Umbrella Integration - Resources

For Your Reference

At-A-Glance (AAG):
http://www.cisco.com/c/dam/en/us/products/collateral/security/router-security/at-a-glance-c45-737403.pdf

Frequently Asked Questions (FAQ):
https://www.cisco.com/c/dam/en/us/products/collateral/security/firewalls/td-umbrella-faqs.pdf

Cisco Umbrella Configuration Guide:
http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_utd/configuration/xe-16/sec-data-umbrella-branch-xe-16-book/sec-data-umbrella-bran.html

CWS EOL announcement:
http://www.cisco.com/c/en/us/products/collateral/security/cloud-web-security/eos-eol-notice-c51-738257.html

Cisco Umbrella Video:
https://youtu.be/CGeLQTWKaPQ

Cisco Umbrella Integration - Guides

For Your Reference

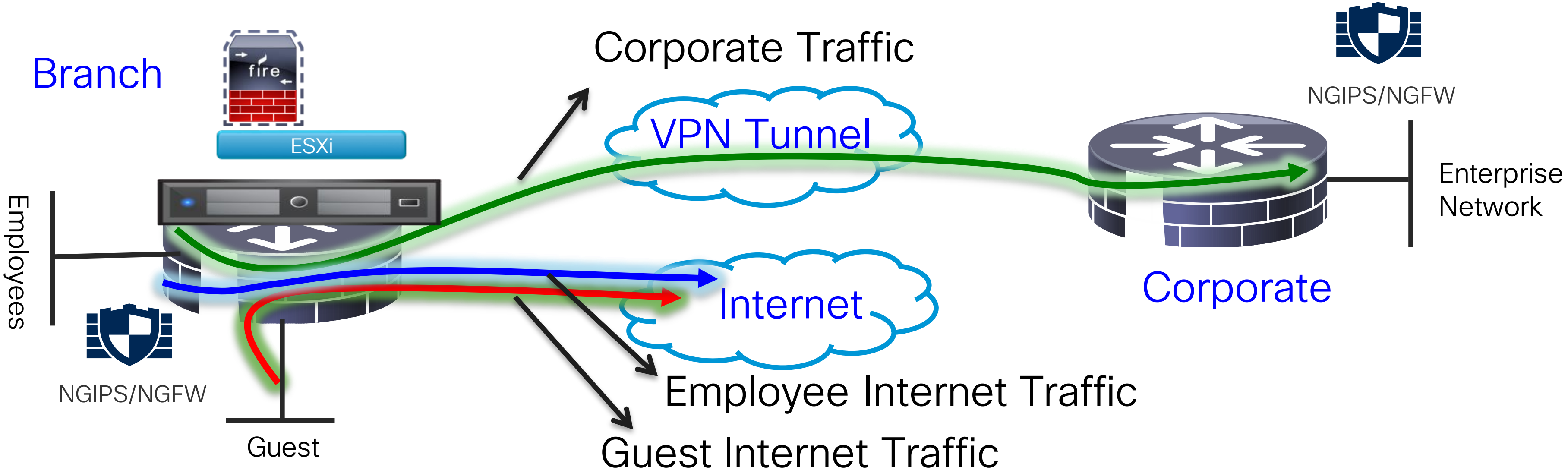
Cisco Umbrella Integration on ISR – Troubleshooting Guide
https://supportforums.cisco.com/t5/security-documents/cisco-umbrella-opendns-troubleshooting/ta-p/3165759

Cisco Umbrella Integration on ISR – Step-By-Step Guide

https://supportforums.cisco.com/t5/security-documents/isr-4k-1k-umbrella-integration-opendns-step-by-step/ta-p/3399077

Firepower Threat Defense for ISR

Use Case: Full DIA



- VLAN separation, guest and employees network are separated
- Firepower URL Filtering provides web reputation and category based filtering
- Corporate and Guest devices reach Internet directly from the Branch
- Firepower provides FW, URL-F, IPS, AVC and AMP

Examples:
Retail stores accessing Supplier websites
Hospital / Pharmacy accessing Insurance websites
Cloud based enterprise service (webex, salesforce etc.)

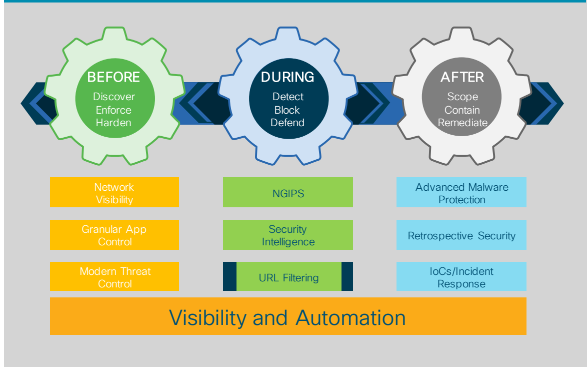
Firepower Threat Defense for ISR - Appendix

For Your Reference

- UTD – Unified Threat defense
- RITE – Router IP traffic export feature
- BDI - Bridge domain interface
- VPG – Virtual Port Group
- CIMC – Cisco Integrated Management Controller
- UCS – Unified Computing System
- QFP – Quantum Flow Processor
- UCS-E : Unified computing system – Express (Blade servers for ISR routers)
- AMP – Advance Malware Protection

Cisco Firepower Threat Defense for ISR

Firepower Threat Defense



BEFORE
Discover
Enforce
Harden

DURING
Detect
Block
Defend

AFTER
Scope
Contain
Remediate

Network Visibility

Granular App Control

Modern Threat Control

NGIPS

Security Intelligence

URL Filtering

Advanced Malware Protection

Retrospective Security

IoCs/Incident Response

Visibility and Automation

+

AppX + Security License

Cisco UCS®

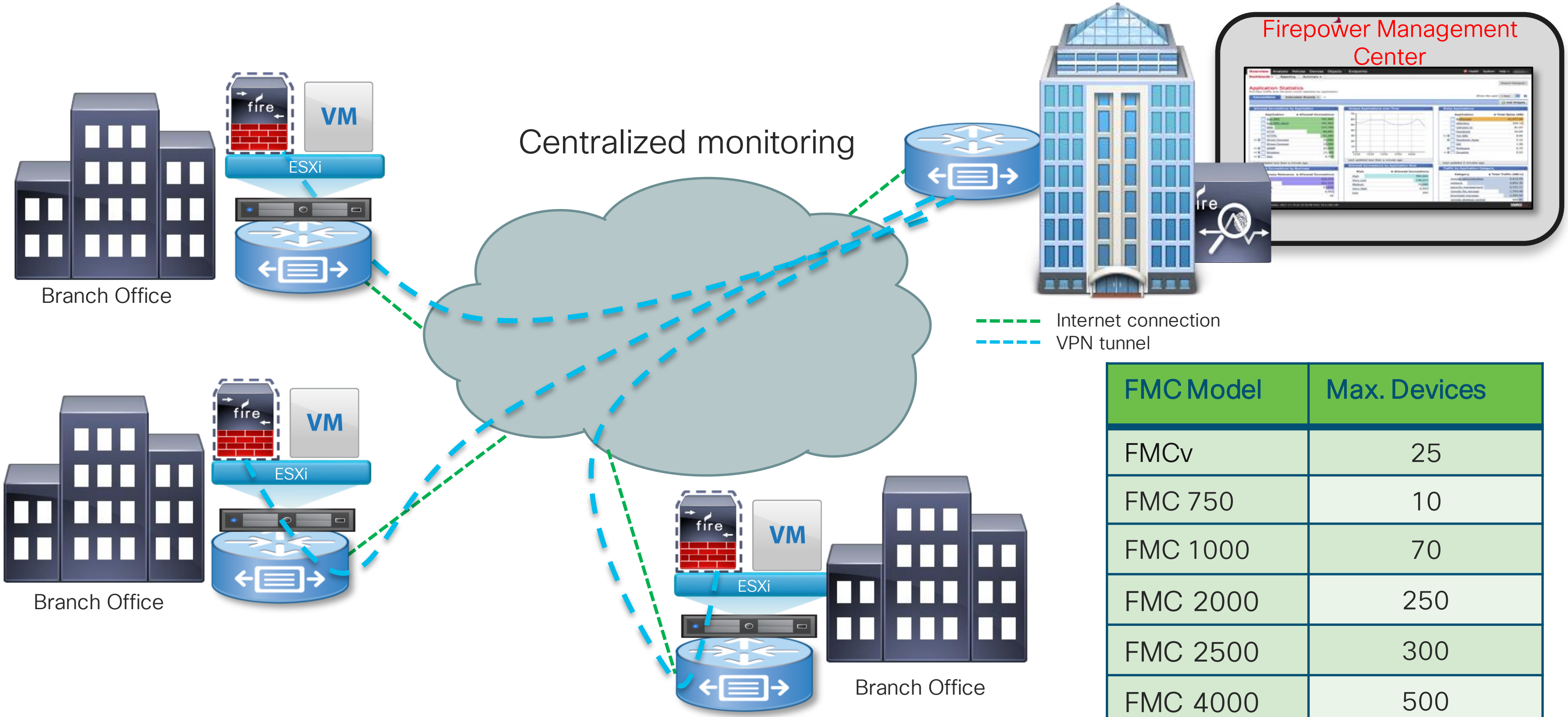
Cisco® 4000 Series ISR

OR

Cisco ISR G2 Series

Free Up Valuable Square Footage Generate More Revenue $$$

Firepower Threat Defense - Deployment Architecture

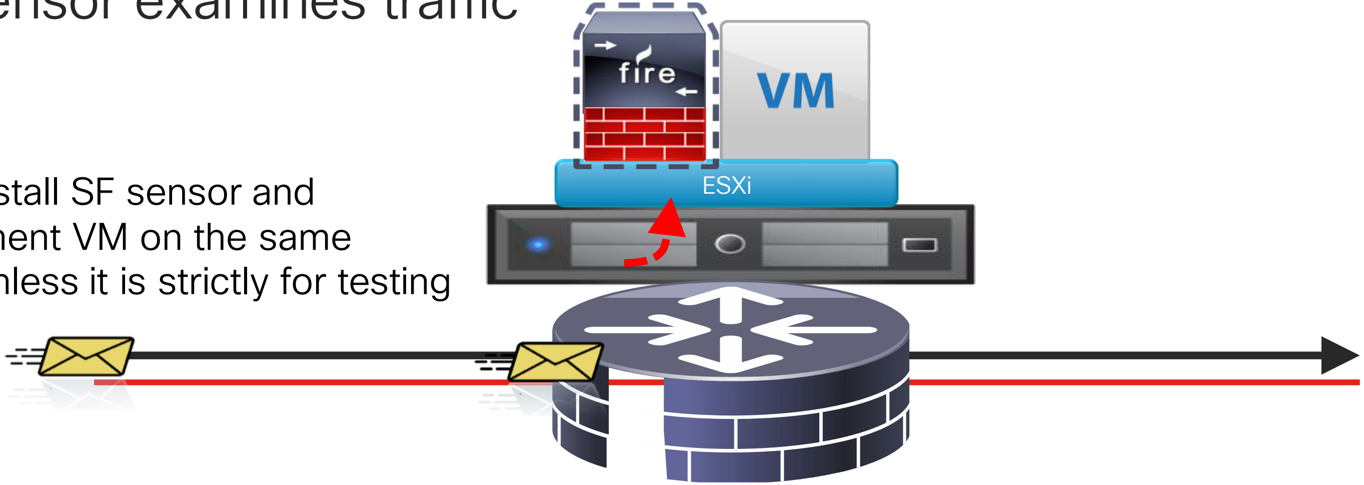


FMC Model	Max. Devices
FMCv	25
FMC 750	10
FMC 1000	70
FMC 2000	250
FMC 2500	300
FMC 4000	500
FMC 4500	750

https://www.cisco.com/c/en/us/products/collateral/security/firesight-management-center/datasheet-c78-736775.html?cachemode=refresh

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



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

Cisco Firepower Threat Defense for ISR G2 – IDS

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 4K – IDS

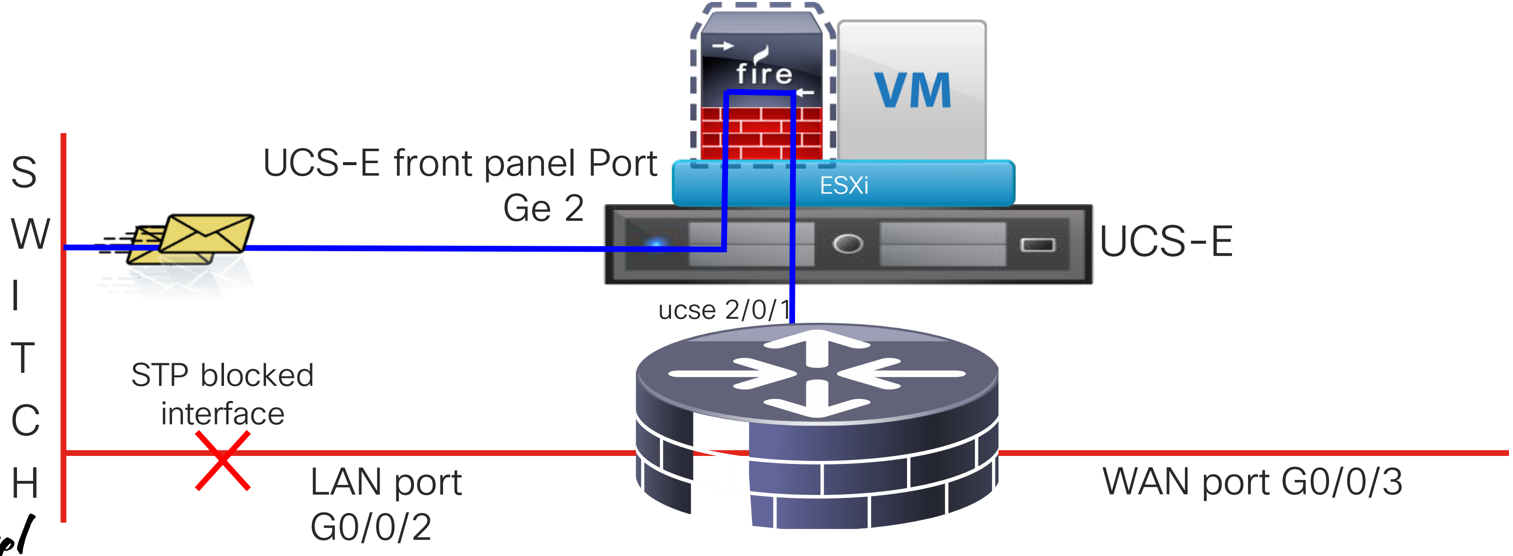
Configuration Steps

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

```
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
```

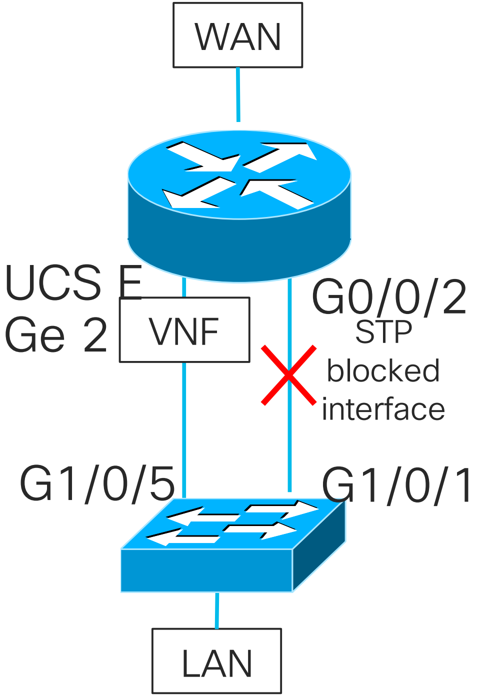
Firepower Threat Defense for ISR - IPS using BDI

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



Firepower Threat Defense for ISR - IPS using BDI

Switch Config



Enable Rapid Spanning Tree on the Switch

```
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 20,30 hello-time 1
spanning-tree vlan 20,30 forward-time 4
```

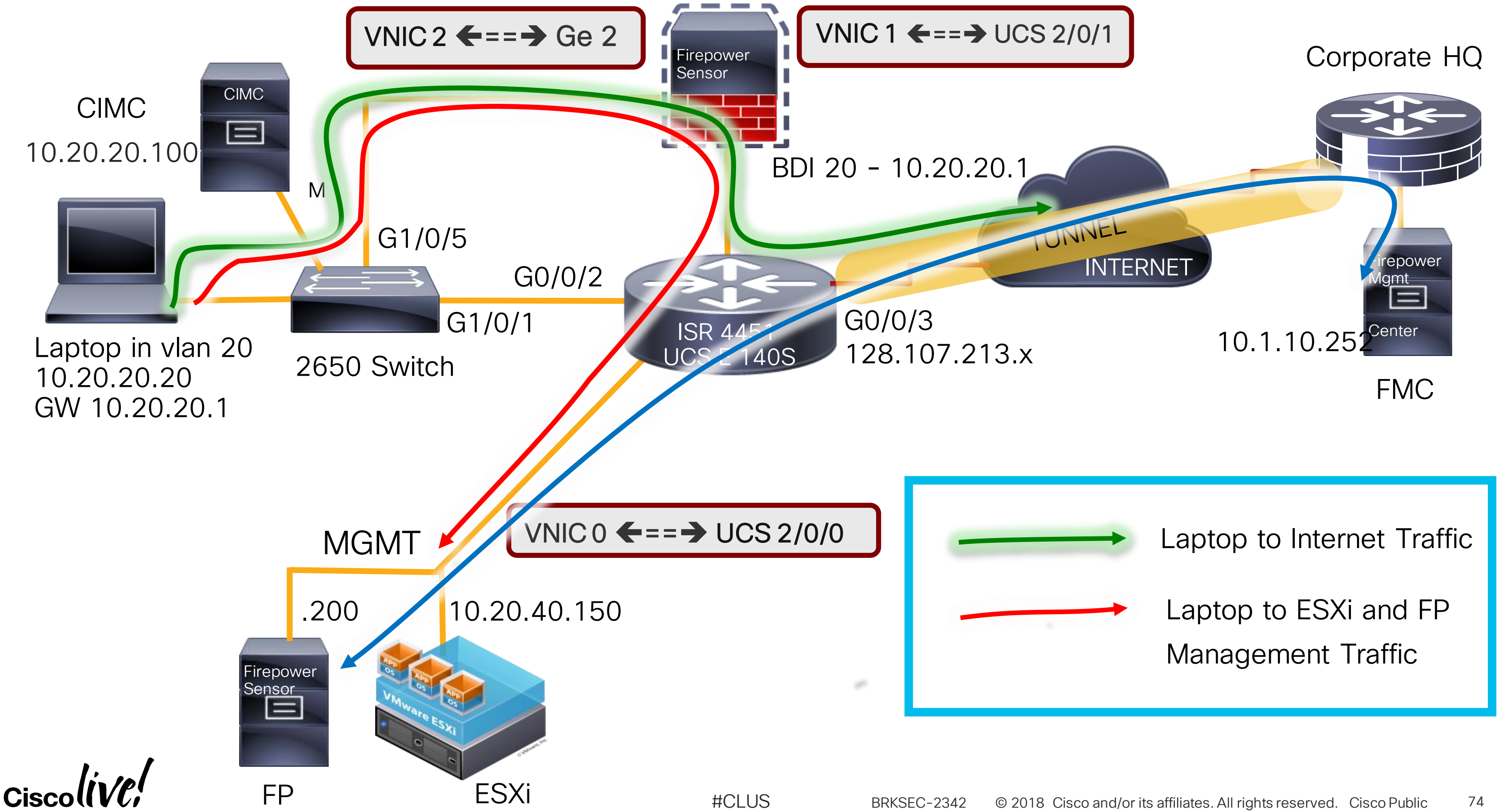
Port connected to the routers G0/0/2 Port

```
interface GigabitEthernet1/0/1
 description connected to ISR-4451 G0/0/2
 switchport trunk allowed vlan 20,30
 switchport mode trunk
 spanning-tree cost 100
```

Port connected to the UCS-E Front Panel Ge 2 Port

```
interface GigabitEthernet1/0/5
 description Connected to Ge 2 port on the UCS-E Blade
 switchport trunk allowed vlan 20,30
 switchport mode trunk
 spanning-tree cost 10
```

Firepower Threat Defense for ISR – NGIPSv using BDI



🟩 Laptop to Internet Traffic

🟥 Laptop to ESXi and FP Management Traffic

Firepower Threat Defense for ISR - IPS using BDI

Router Config

vNIC2 Inside

UCS E Front Panel Port

```
interface GigabitEthernet0/0/2
 no ip address
 negotiation auto

 service instance 20 ethernet
  encapsulation dot1q 20
  rewrite ingress tag pop 1 symmetric
  bridge-domain 20
```

STP blocked interface For vlan 20

Firepower

Fail-Open Addition

vNIC1 Outside

```
interface ucse2/0/1
 no ip address
 negotiation auto
 switchport mode trunk

service instance 20 ethernet
  encapsulation dot1q 20
  rewrite ingress tag pop 1 symmetric
  bridge-domain 20

interface BDI20
 ip address 10.20.20.1 255.255.255.0
 ip nat inside
```

```
interface GigabitEthernet0/0/3
 ip address 128.107.213.x 255.255.255.0
 ip nat outside
```

Firepower Threat Defense for ISR - IPS using BDI

Router Config

Inside Interface Configuration no ip address here. BDI interface has the IP address

```
interface GigabitEthernet0/0/2
 no ip address

 service instance 20 ethernet
  encapsulation dot1q 20
  rewrite ingress tag pop 1 symmetric
  bridge-domain 100

 service instance 30 ethernet
  encapsulation dot1q 30
  rewrite ingress tag pop 1 symmetric
  bridge-domain 30
```

This interface is to route management traffic to ESXi and Firepower Sensor (notice the static routes)

```
interface ucse2/0/0
 ip address 10.20.40.1 255.255.255.0
 switchport mode trunk
```

```
interface ucse2/0/1
 no ip address
 switchport mode trunk
 service instance 20 ethernet
  encapsulation dot1q 20
  rewrite ingress tag pop 1 symmetric
  bridge-domain 20

 service instance 30 ethernet
  encapsulation dot1q 30
  rewrite ingress tag pop 1 symmetric
  bridge-domain 30
```

BDI Interface to terminate vlan 20 and 30 outside FP sensor

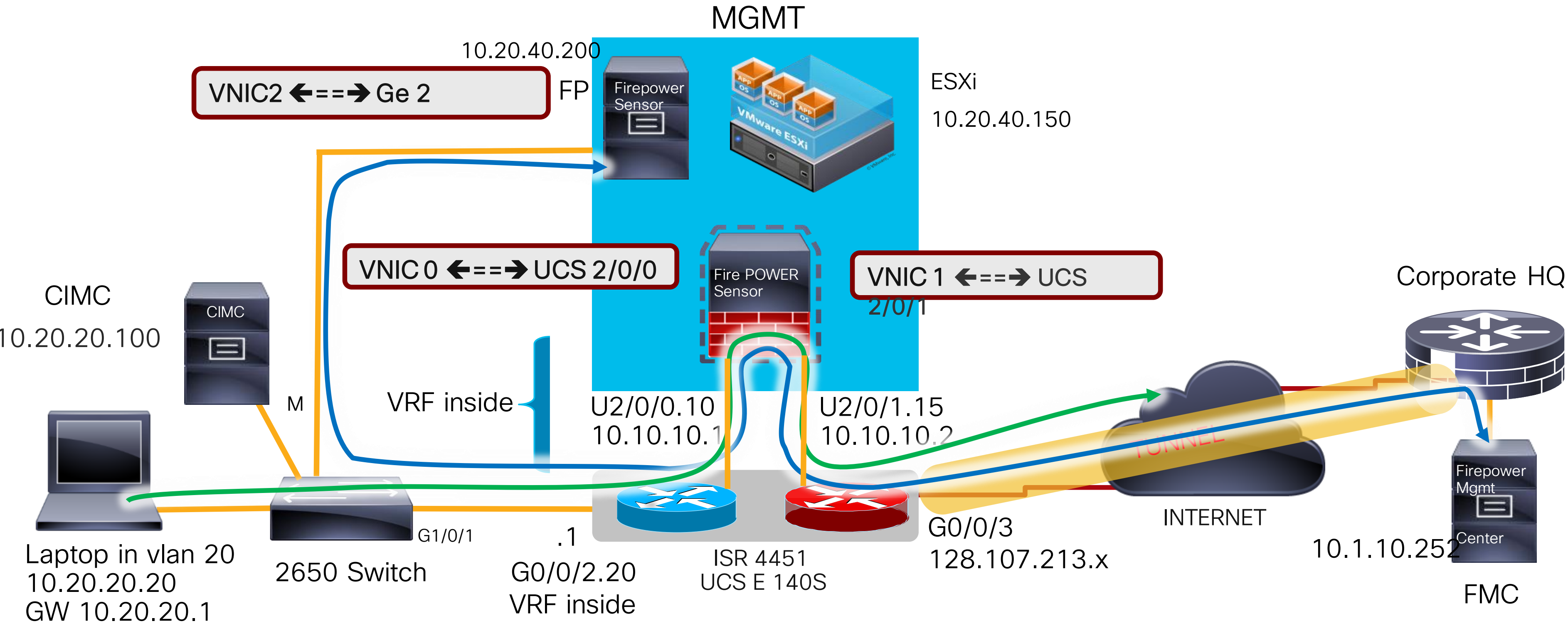
```
interface BDI20
 ip address 10.20.20.1 255.255.255.0

interface BDI30
 ip address 10.20.30.1 255.255.255.0
```

Route statements for FP-Sensor and ESXi management

```
ip route 10.20.40.150 255.255.255.255 ucse 2/0/0
ip route 10.20.40.200 255.255.255.255 ucse 2/0/0
```

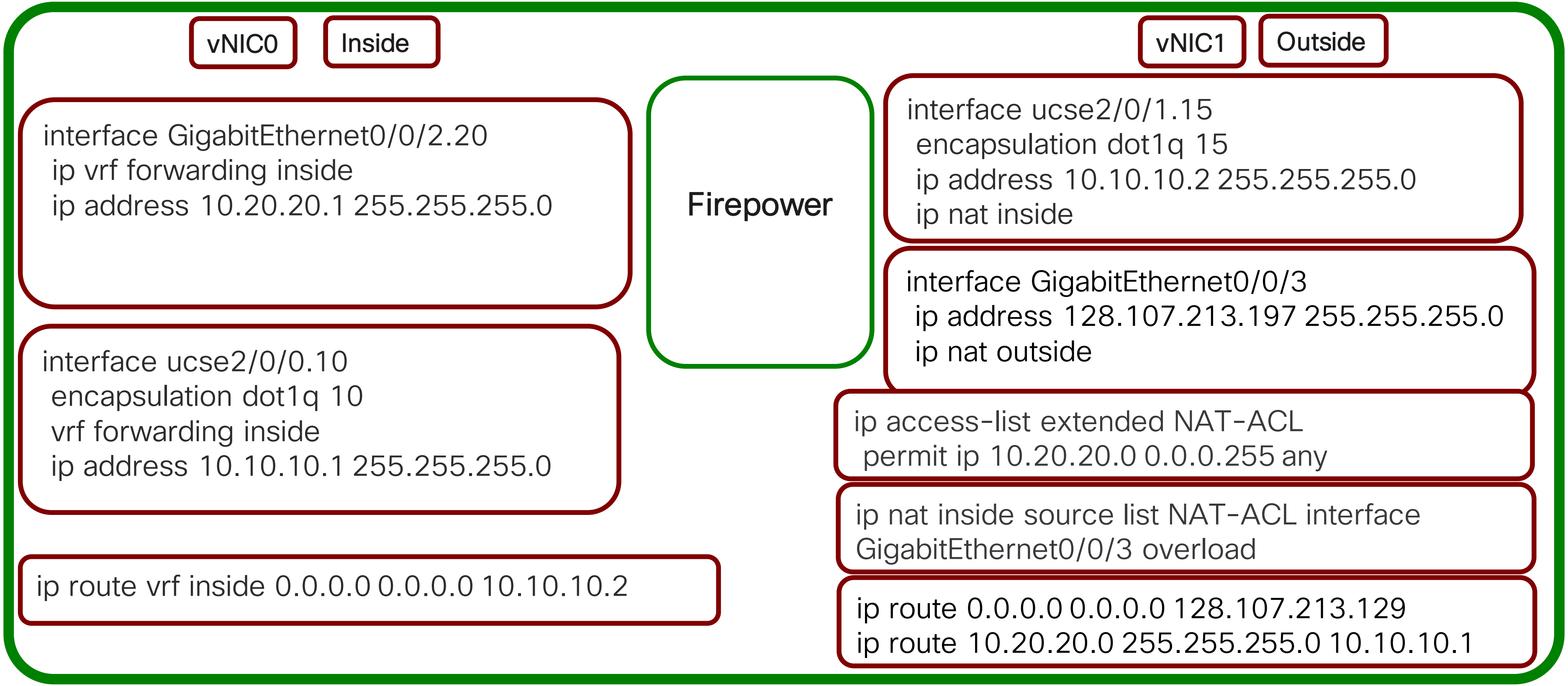
IPS inline with VRF

Firepower Threat Defense for ISR – NGIPSv using VRF



http://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-e-series-servers/white-paper-c11-739289.html#_Toc486544453

Firepower Threat Defense for ISR – IPS using VRF



```
interface GigabitEthernet0/0/2.20
 ip vrf forwarding inside
 ip address 10.20.20.1 255.255.255.0
```

```
interface ucse2/0/0.10
 encapsulation dot1q 10
 vrf forwarding inside
 ip address 10.10.10.1 255.255.255.0
```

```
ip route vrf inside 0.0.0.0 0.0.0.0 10.10.10.2
```

```
interface ucse2/0/1.15
 encapsulation dot1q 15
 ip address 10.10.10.2 255.255.255.0
 ip nat inside
```

```
interface GigabitEthernet0/0/3
 ip address 128.107.213.197 255.255.255.0
 ip nat outside
```

```
ip access-list extended NAT-ACL
 permit ip 10.20.20.0 0.0.0.255 any
```

```
ip nat inside source list NAT-ACL interface
GigabitEthernet0/0/3 overload
```

```
ip route 0.0.0.0 0.0.0.0 128.107.213.129
ip route 10.20.20.0 255.255.255.0 10.10.10.1
```

Firepower Threat Defense for ISR – IPS using VRF

Optional Fail Open

```
ip sla 1
 icmp-echo 10.10.10.2 source-ip 10.10.10.1
 vrf inside
 threshold 500
 timeout 1000
 frequency 2
!
ip sla schedule 1 life forever start-time now
!
track 1 ip sla 1
 delay down 3
```

```
event manager applet ipsla_ping-down
 event syslog pattern "1 ip sla 1 state Up -> Down"
 action 1.0 cli command "enable"
 action 1.5 cli command "config term"
 action 2.0 cli command "interface g0/0/2.20"
 action 2.5 cli command "no ip vrf forwarding"
 action 2.6 cli command "ip address 10.20.20.1 255.255.255.0"
 action 2.7 cli command "ip nat inside"
 action 2.8 cli command "zone security EMPLOYEE"
 action 3.1 cli command "write mem"

event manager applet ipsla_ping-down
event syslog pattern "1 ip sla 1 state Up -> Down"
action 1.0 cli command "enable"
action 1.5 cli command "config term"
action 2.0 cli command "interface g0/0/2.20"
action 2.5 cli command "ip vrf forwarding inside"
action 2.6 cli command "ip address 10.20.20.1 255.255.255.0"
action 2.7 cli command "no ip nat inside"
action 2.8 cli command "no zone security EMPLOYEE"
action 3.1 cli command "write mem"
```

Cisco Firepower Threat Defense for ISR – IPS using VRF

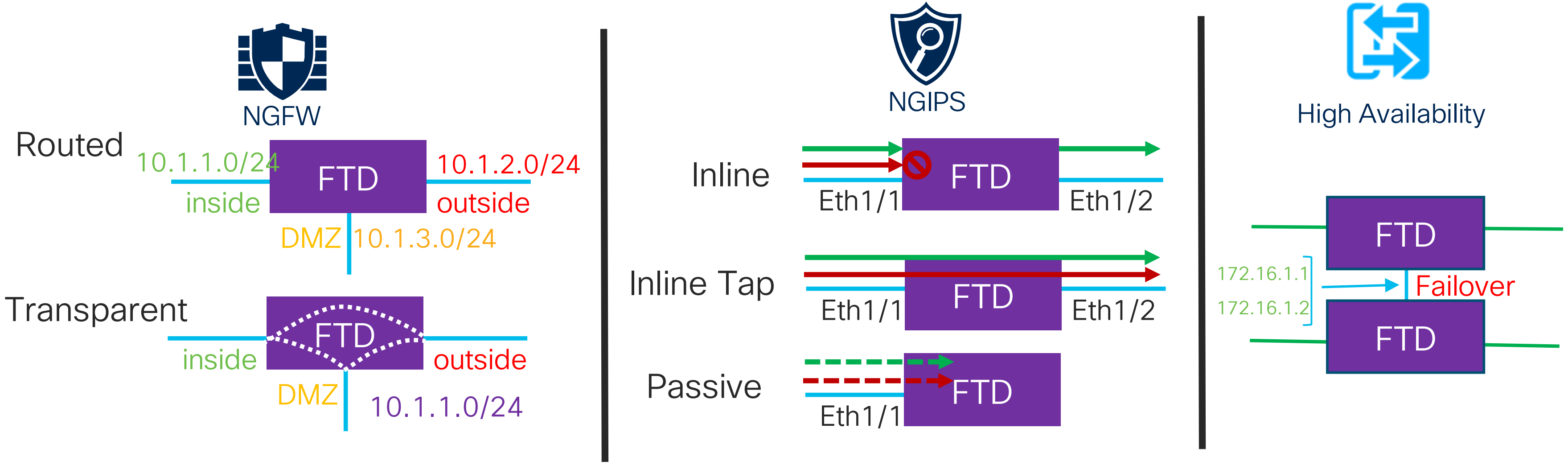
Optional Fail Open

```
event manager applet ipsla_ping-down
 event syslog pattern "1 ip sla 1 state Up -> Down"
 action 1.0 cli command "enable"
 action 1.5 cli command "config term"
 action 2.0 cli command "interface g0/0/2.20"
 action 2.5 cli command "no ip vrf forwarding"
 action 2.6 cli command "ip address 10.20.20.1 255.255.255.0"
 action 2.7 cli command "ip nat inside"
 action 2.8 cli command "zone security EMPLOYEE"
 action 3.0 cli command "interface g0/0/2"
 action 3.1 cli command "no ip vrf forwarding"
 action 3.2 cli command "ip address 10.20.40.1 255.255.255.0"
 action 3.3 cli command "ip nat inside"
 action 3.4 cli command "zone security EMPLOYEE"
 action 3.5 cli command "interface t1"
 action 3.6 cli command "no ip vrf forwarding"
 action 3.7 cli command "ip address 10.1.20.3  255.255.255.0"
 action 3.8 cli command "zone security EMPLOYEE"
 action 3.9 cli command "write mem"
```

```
event manager applet ipsla_ping-up
 event syslog pattern "1 ip sla 1 state Down -> Up"
 action 1.0 cli command "enable"
 action 1.5 cli command "config term"
 action 2.0 cli command "interface g0/0/2.20"
 action 2.5 cli command "ip vrf forwarding inside"
 action 2.6 cli command "ip address 10.20.20.1  255.255.255.0"
 action 2.7 cli command "no ip nat inside"
 action 2.8 cli command "no zone security EMPLOYEE"
 action 3.1 cli command "interface g0/0/2"
 action 3.2 cli command "ip vrf forwarding inside"
 action 3.3 cli command "ip address 10.20.40.1  255.255.255.0"
 action 3.4 cli command "no ip nat inside"
 action 3.5 cli command "no zone security EMPLOYEE"
 action 3.6 cli command "interface t1"
 action 3.7 cli command "ip vrf forwarding inside"
 action 3.8 cli command "ip address 10.1.20.3  255.255.255.0"
 action 3.9 cli command "no zone security EMPLOYEE"
 action 4.0 cli command "write mem"
```

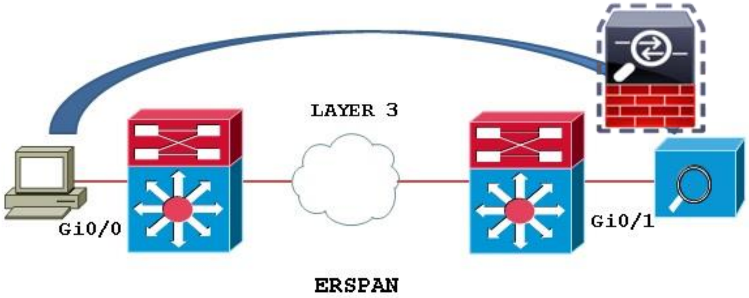
NGFWv Deployment Modes

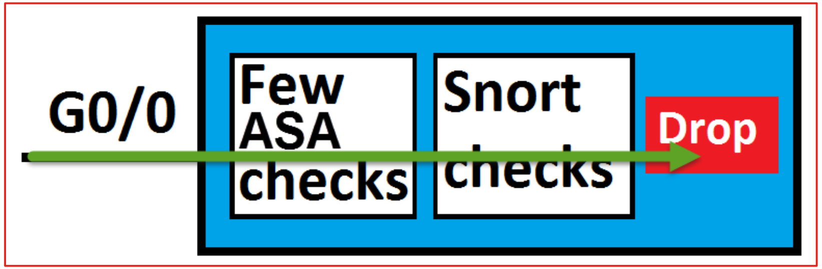
- FTD is both NGFW and NGIPS on different network interfaces
  - NGFW inherits operational modes from ASA and adds FirePOWER features
  - NGIPS operates as standalone FirePOWER with limited ASA data plane functionality



Interface Mode: ERSPAN

- L3 interface operating as a sniffer
- Allow you to monitor traffic from source port distributed over multiple switches
- Uses GRE to encapsulate the traffic from source to destination
- Available only in Routed Deployment modes
- Few ASA engine and Full Snort engine checks to a copy of the actual traffic.



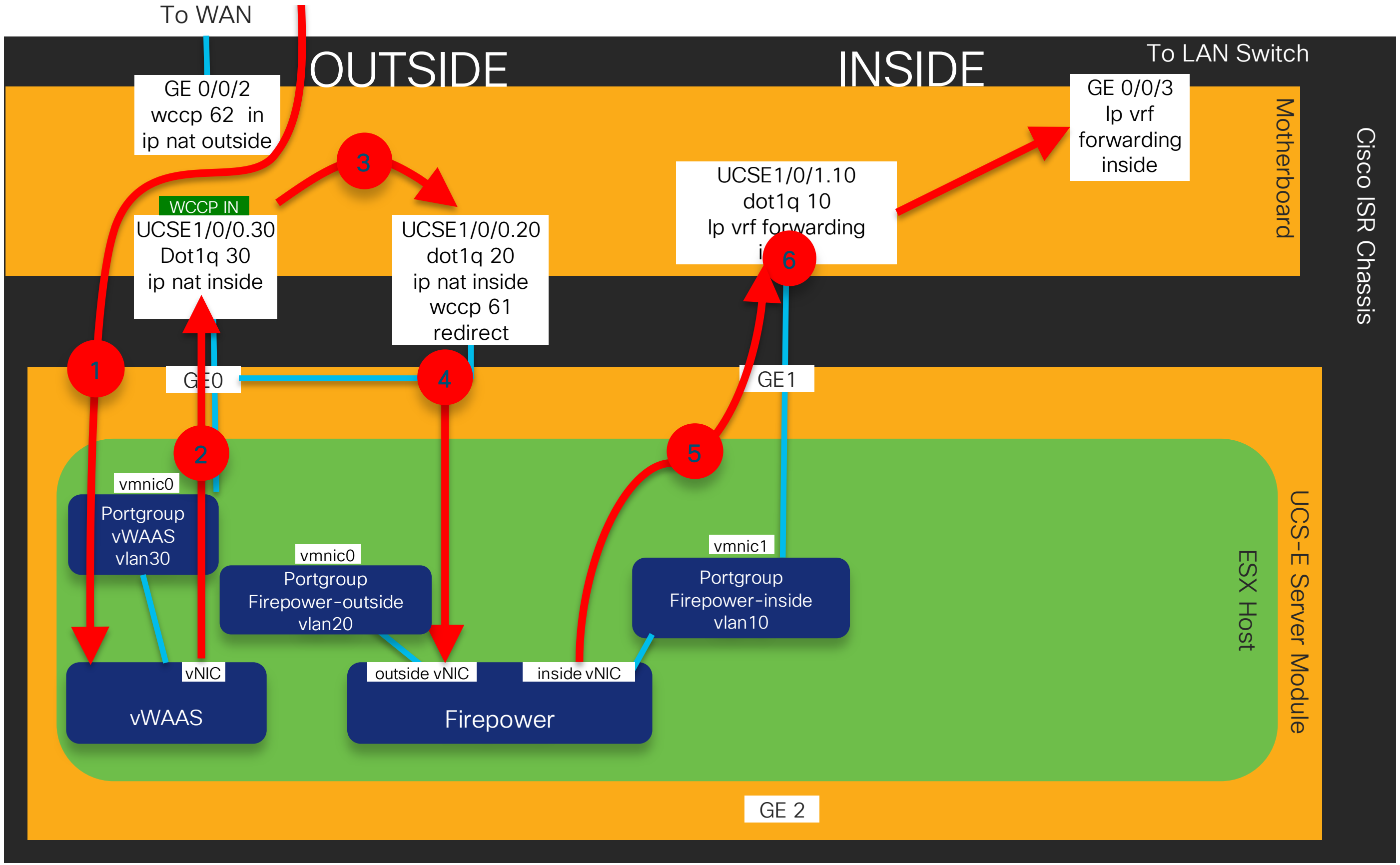


Cisco NGFWv HA on two UCS-E in the same ISR Router

Deployment Use Cases Tested

NGFWv Modes	UCS-E VNF Stitching Modes	Failures Tested with HA
NGFW Routed Mode	Between Internal and External Interfaces	Device level failure
NGFW Transparent mode	Between Internal Interfaces	Interface level failure
NGIPS Inline Interface Mode	Between External Interfaces	
NGIPS Passive mode		
NGIPS ERSPAN mode (only in Routed mode)		

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

Firepower Threat Defense for ISR - Resources

For Your Reference

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/sec-data-fpwr-utd.html

Router Security – Firepower Threat Defense for ISR

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

Cisco NGFWv Data Sheet

https://www.cisco.com/c/en/us/products/collateral/security/firepower-ngfw/datasheet-c78-736661.html

Cisco NGFWv for VMware Deployment Quick Start Guide

https://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/VMware/ftdv/ftdv-VMware-qsg.htm

Firepower Threat Defense for ISR - Resources

For Your Reference

Cisco UCS E-Series Deployment White Paper
https://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-e-series-servers/white-paper-c11-738013.html#_Toc465916728

Deployment Examples: Cisco UCS E-Series Integration with Passive and Inline Services on ESXi White Paper
https://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-e-series-servers/white-paper-c11-739289.html

Firepower Management Center Configuration Guide
https://www.cisco.com/c/en/us/td/docs/security/firepower/622/configuration/guide/fpmc-config-guide-v622.html

Configuration Examples and Technotes
https://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-configuration-examples-list.html

Firepower Threat Defense show commands
https://www.cisco.com/c/en/us/td/docs/security/firepower/command_ref/b_Command_Reference_for_Firepower_Threat_Defense/s_5.html

Firepower Threat Defense for ISR - Guides

For Your Reference

Firepower Threat Defense for ISR 4K & G2 - IPS inline mode using UCS-E front panel port
https://supportforums.cisco.com/document/13016901/firepower-threat-defense-isr-ips-using-front-panel-port-ucs-e

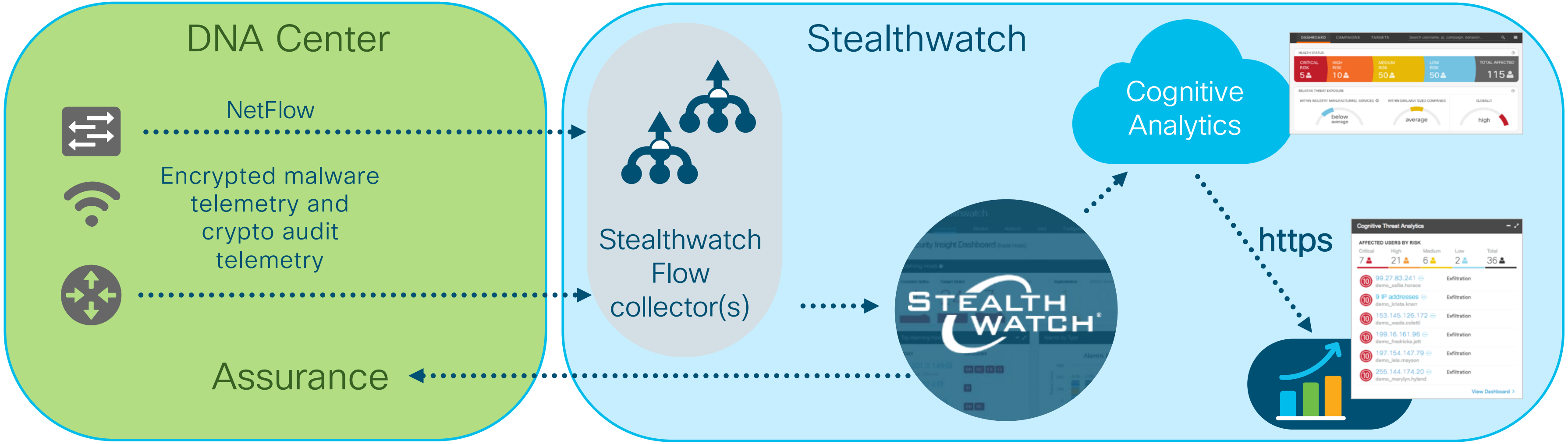
Firepower Threat Defense for ISR 4K & G2 - IPS inline mode using VRF method
https://supportforums.cisco.com/document/13050311/firepower-threat-defense-isr-4k-g2-ips-inline-mode-using-vrf-method

NGFWv Support Documentation
https://supportforums.cisco.com/t5/security-documents/firepower-threat-defense-ngfwv-on-ucs-e-series-blade-on-isr-4k/ta-p/3215394

https://supportforums.cisco.com/t5/security-documents/firepower-threat-defense-ngfwv-on-ucs-e-series-blade-on-isr-4k/ta-p/3215375

Encrypted Traffic Analytics (ETA)

Finding malicious activity in encrypted traffic


DNA Center
NetFlow
Encrypted malware telemetry and crypto audit telemetry
Assurance
Stealthwatch
Stealthwatch Flow collector(s)
STEALTHWATCH
Cognitive Analytics
https
Cognitive Threat Analytics
AFFECTED USERS BY RISK

Cisco's unique hardware and software architecture

Enhanced NetFlow with Encrypted Traffic Analytics from Cisco's newest routers and switches

Stealthwatch enhanced analytics and machine learning reduces threat investigation time

Global-to-local knowledge correlation results in higher precision of threat findings

Encrypted Traffic Analytics – Benefits and Requirements

Benefits

Identifies malware in encrypted traffic

Crypto audit

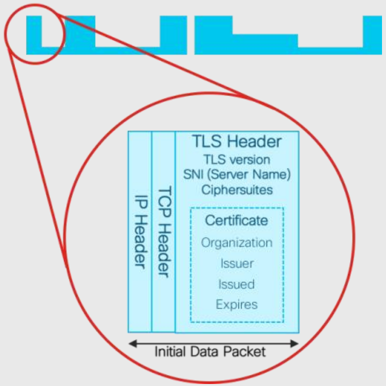
Requirements

- SEC-K9 license
- XE 16.6.2 and above on ASR, ISR 4K, 1K, ISRv and CSR
- Stealthwatch Management
- Supports VRF (16.8.1)

How do we inspect encrypted traffic?

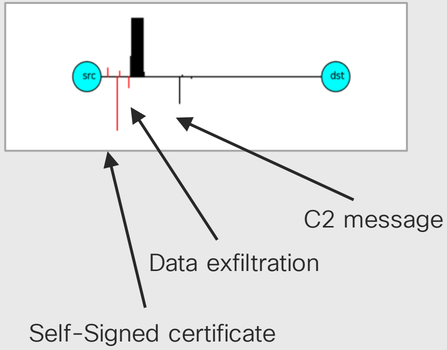
Initial Data Packet

Make the most of the unencrypted fields



Sequence of Packet Lengths and Times

Identify the content type through the size and timing of packets



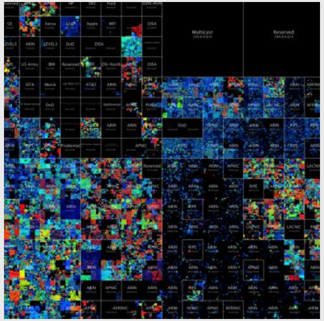
C2 message

Data exfiltration

Self-Signed certificate

Threat Intelligence Map

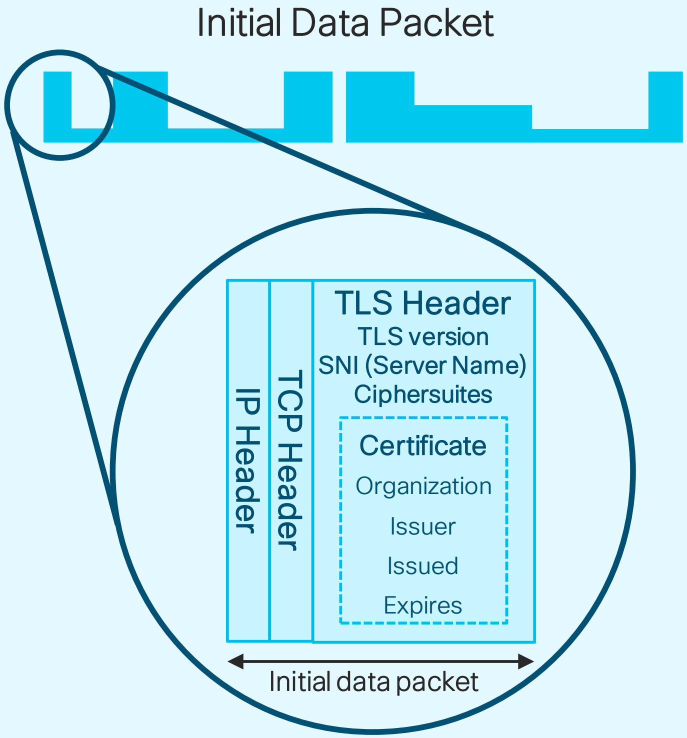
Who's who of the Internet's dark side



Broad behavioral information about the servers on the Internet.

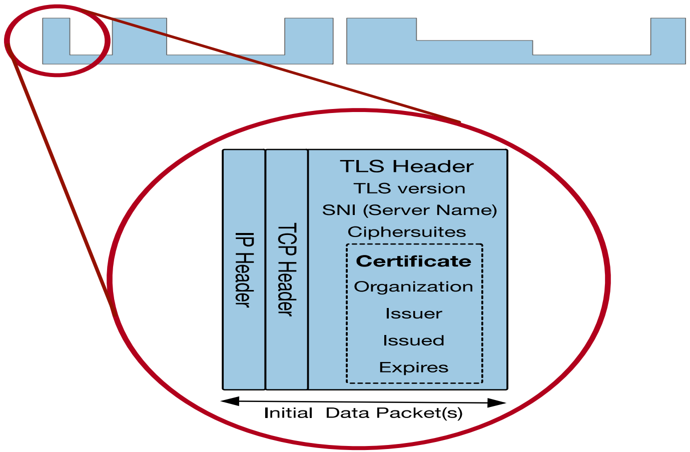
Encrypted Traffic Analytics - Initial Data Packet (IDP)

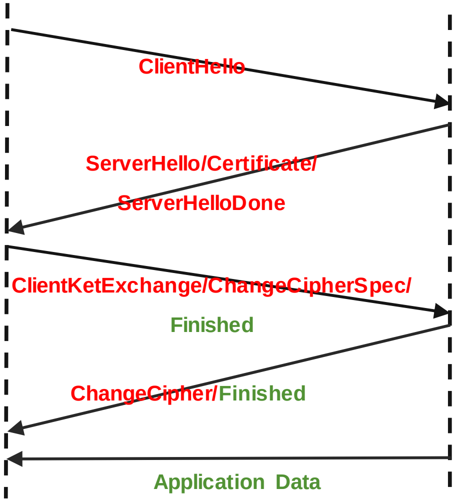
- HTTPS header contains several information-rich fields.
- Server name provides domain information.
- Crypto information educates us on client and server behavior and application identity.
- Certificate information is similar to **whois** information for a domain.
- And much more can be understood when we combine the information with global data.



Encrypted Traffic Analytics - Initial Data Packet

Initial Data Packet





Client: I support crypto

Server: I support that crypto, and I'm me

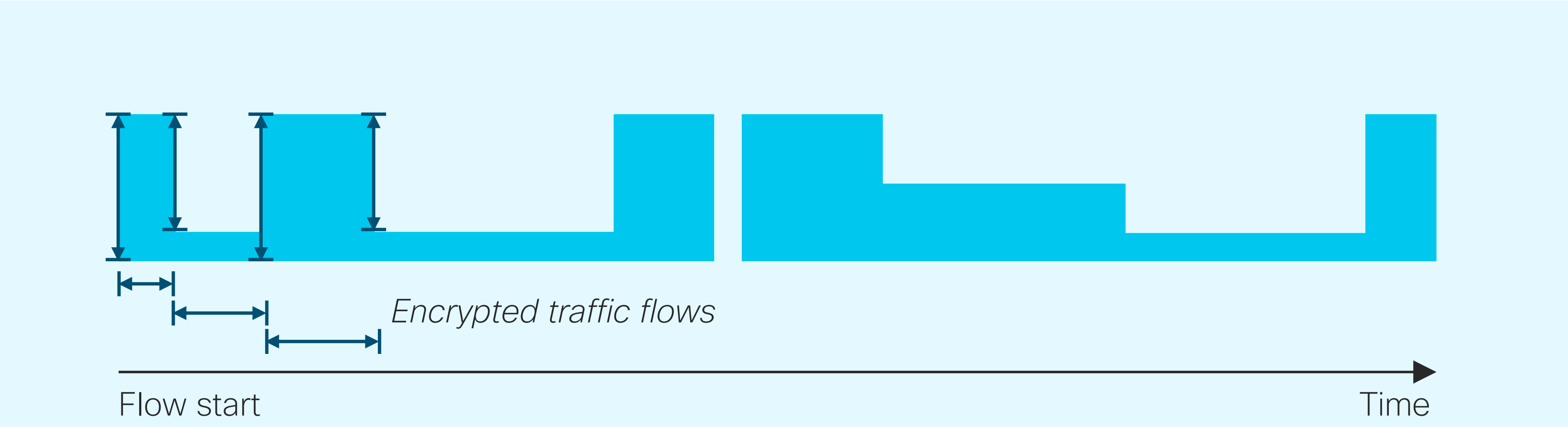
Client: Take this secret and let's encrypt

Server: Your secret looks good, let's encrypt

Client/Server: encrypted data

TLS field (in Client Hello)	Inference
Offered Cypher suites	Browsers prefer heavy weight and more secure encryption algorithms, Mobile applications prefer efficient encryption
Extensions	

ETA - Sequence of Packet Lengths and Times (SPLT)



- Size and timing of the first packets allow us to estimate the type of data inside the encrypted channel.
- We can distinguish video, web, API calls, voice, and other data types from one another and characterize the source within the class.

Encrypted Traffic Analytics – Configuration

Step 2 – Enable ETA under the interfaces

```
Router(config)#interface GigabitEthernet0/0/2.20
Router(config-subif)#et-analytics enable

Router(config)#interface GigabitEthernet0/0/2.30
Router(config-subif)#et-analytics enable
```

Encrypted Traffic Analytics – Configuration

Step 1 Step 1 – Configure ETA with an optional whitelist access-list

```
Router (config)#ip access-list extended 101
Router(config-ext-nacl)# permit ip host 10.20.20.2 any
Router(config-ext-nacl)# permit ip any host 10.20.20.2

Router(config)#et-analytics
Router(config-et-analytics)#ip flow-export destination 10.1.10.200 2055
Router(config-et-analytics)#whitelist acl 101
```

Step 2 Enable ETA under the interfaces

```
Router(config)#interface GigabitEthernet0/0/2.20
Router(config-subif)#et-analytics enable

Router(config)#interface GigabitEthernet0/0/2.30
Router(config-subif)#et-analytics enable
```

Encrypted Traffic Analytics - Performance & Scale

For Your Reference

Platform	Platform Throughput	Recommended FPS*
ISR 4451	1 Gbps	7,500
ISR 4431	500 Mbps	3,500
ISR 4351	200 Mbps	1,500
ISR 4331	100 Mbps	750
ISR 4321	50 Mbps	350
ISR 4221	35 Mbps	250
ISR 1100	Up to 350 Mbps	250
ISRv	1 Gbps	7,500
CSR1000v	2.5 Gbps	19,000
RP2/ESP20	20 Gbps	20,000
RP2/ESP40	40 Gbps	40,000
RP2/ESP100 & ESP 200	100 Gbps	60,000
ASR1001-X / 1002-X	20 Gbps / 36 Gbps	20,000
ASR1001-HX / 1002-HX	60 Gbps / 100 Gbps	60,000

* HTTP/HTTPS Unidirectional New Flows Per Second

WAN Bandwidth Utilization for ETA Records export: 10 to 15% of Platform throughput

Records Exported: IDP (~1400 Bytes) + SPLT (~150 Bytes) + TLS (~900 Bytes) = ~20 Kbits

Encrypted Traffic Analytics (ETA) - Resources

For Your Reference

- Encrypted Traffic Analytics (ETA)

https://www.cisco.com/c/en/us/solutions/enterprise-networks/enterprise-network-security/eta.html

- ETA Configuration Guide for Routers

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/netflow/configuration/xe-16-6/nf-xe-16-6-book/encrypted-traffic-analytics.html

- Cognitive Analytics

https://cognitive.cisco.com

- Stealthwatch and CTA Configuration Guide

https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/cta/configuration/SW_6_9_1_Stealthwatch_and_CTA_Configuration_Guide_DV_1_6.pdf

- Detecting Encrypted Traffic Malware Traffic (Without Decryption) blog

https://blogs.cisco.com/security/detecting-encrypted-malware-traffic-without-decryption

- Cisco Validated Design (CVD) Guide for ETA Deployment

https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Campus/CVD-Encrypted-Traffic-Analytics-Deployment-Guide-2017DEC.pdf

Troubleshooting

For Your Reference

- CWS Tunnel Connector on ISR 4K – Troubleshooting
  https://supportforums.cisco.com/document/12945581/cws-tunnel-connector-isr-4k-troubleshooting
- Firepower Threat Defense for ISR – Troubleshooting
  https://supportforums.cisco.com/document/13078621/troubleshooting-firepower-threat-defense-isr
- Cisco Umbrella (OpenDNS) – Troubleshooting
  https://supportforums.cisco.com/document/13229216/cisco-umbrella-opendns-troubleshooting
- Packet Tracer
  http://www.cisco.com/c/en/us/support/docs/content-networking/adaptive-session-redundancy-asr/117858-technote-asr-00.html
- TAC Troubleshooting Tools
  http://www.cisco.com/c/en/us/support/web/tools-catalog.html

Summary

Feature	Description
ZBF	Build a comprehensive, scalable security solution to protect user services. Provides stateful firewall and segmentation. Supports VRF and SGT.
Snort IPS	Snort IPS is the most widely deployed Intrusion Prevention System in the world with more than 4 million downloads. The Snort IPS feature enables Intrusion Prevention System (IPS) or Intrusion Detection System (IDS) for branch offices on ISR 4K routers. Snort monitors network traffic and analyzes against a defined rule set. Supports VRF.
Cisco Umbrella Integration	Cisco Umbrella Integration offers easy-to-manage DNS-layer content filtering based on categories as well as reputation that can be configured in three simple steps. It prevents branch users and guests from accessing inappropriate content and known malicious sites that might contain malware and other security risks. Supports VRF
Firepower	Firepower Threat Defense offers IPS/AVC, URL Filtering and AMP (Advanced Malware Protection). This is a one box solution that is supported on UCS E-Series blades on both ISR G2 as well as ISR 4K routers. Intrusion Detection is accomplished using AppNav redirection/replication and Intrusion Prevention is accomplished either via front panel port on the UCS-E or using VRF method.
ETA	Detecting malicious content in encrypted packets without having to decrypt them.

Summary

Zone Based Firewall

- ISR G2 and 4K Series Routers
- ISR 1K Series Routers
- ISRv
- ASR
- CSR

Snort IPS

- ISR 4K Series Routers
- ISRv
- CSR

Cisco Umbrella

- ISR 4K Series Routers
- ISR 1K Series Routers

Firepower Threat Defense

- ISR G2 and ISR 4K Series Routers with UCS E-Series Blades
- ENCS

ETA

- ISR 4K Series Routers
- ISR 1K Series Routers
- ISRv
- ASR
- CSR

Router-security@cisco.com

Cisco Webex Teams

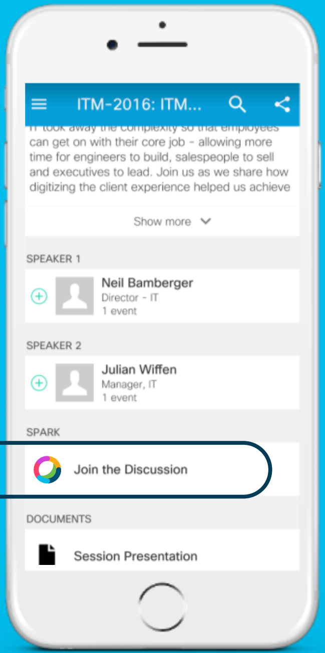
Questions?

Use Cisco Webex Teams (formerly Cisco Spark) to chat with the speaker after the session

How

1. Find this session in the Cisco Events App
2. Click “Join the Discussion”
3. Install Webex Teams or go directly to the team space
4. Enter messages/questions in the team space

Webex Teams will be moderated by the speaker until June 18, 2018.



ITM-2016: ITM...

IT took away the complexity so that employees can get on with their core job - allowing more time for engineers to build, salespeople to sell and executives to lead. Join us as we share how digitizing the client experience helped us achieve

Show more

SPEAKER 1

Neil Bamberger
Director - IT
1 event

SPEAKER 2

Julian Wiffen
Manager, IT
1 event

SPARK

Join the Discussion

DOCUMENTS

Session Presentation

cs.co/ciscolivebot# BRKSEC-2342

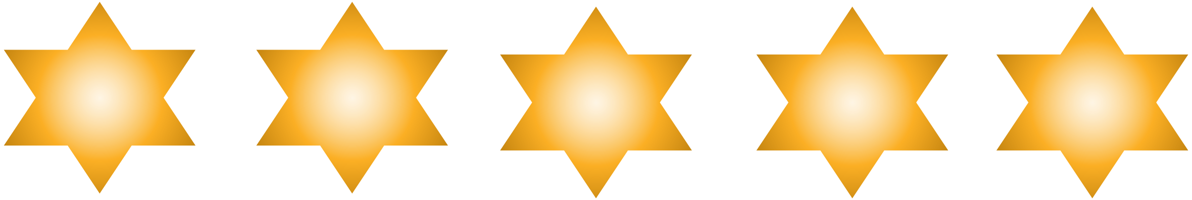
Complete your online session evaluation

Give us your feedback to be entered into a Daily Survey Drawing.

Complete your session surveys through the Cisco Live mobile app or on www.CiscoLive.com/us.

Don't forget: Cisco Live sessions will be available for viewing on demand after the event at www.CiscoLive.com/Online.

Complete your online session evaluation



Continue your education

- Demos in the Cisco campus
- Walk-in self-paced labs
- Meet the engineer 1:1 meetings
- Related sessions

Continue Your Education

Related sessions

BRKSEC-2446 Endpoint Security, Your Last Line of Defense
Aaron Woland 90 min Breakout

BRKSEC-3557 Advanced Security Integration, Tips
Aaron Woland, 90 min Breakout

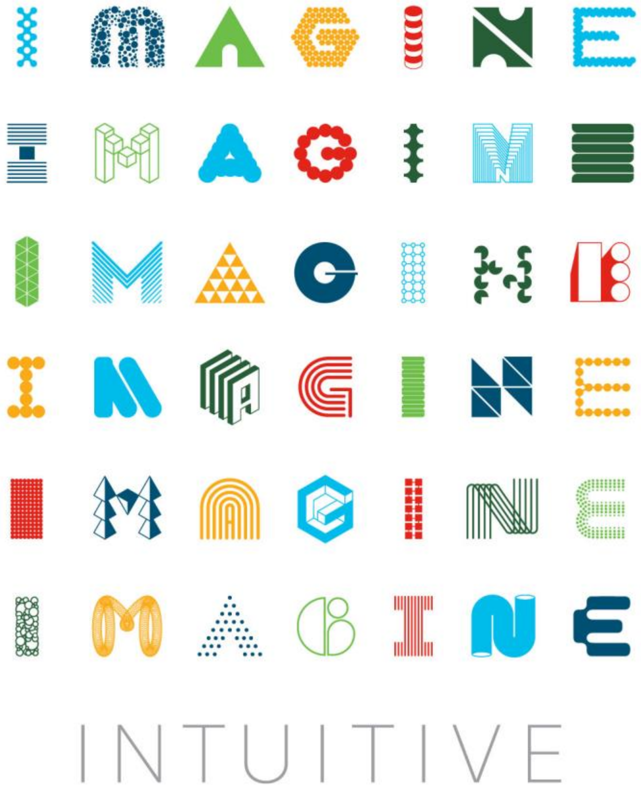
BRKSEC-1980 Introducing Cisco Umbrella for Cloud Based Threat Protection
Jonny Noble, 90 min Breakout

PSOSEC-1102 The Secure Branch in a Direct to Internet Era
Joe Aronow, 60 min

BRKSEC-1008 Simple Hacking Tools for your Network
Jerry Lin, 90 min Breakout

Q & A

Thank you


IMAGINE
IMAGINE
IMAGINE
IMAGINE
IMAGINE
IMAGINE
INTUITIVE

cisco

IMAGINE

INTUITIVE