Cisco live!

January 29 - February 2, 2018 · Barcelona

BRKSEC-2342

Branch Router Security

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

Cisco live!

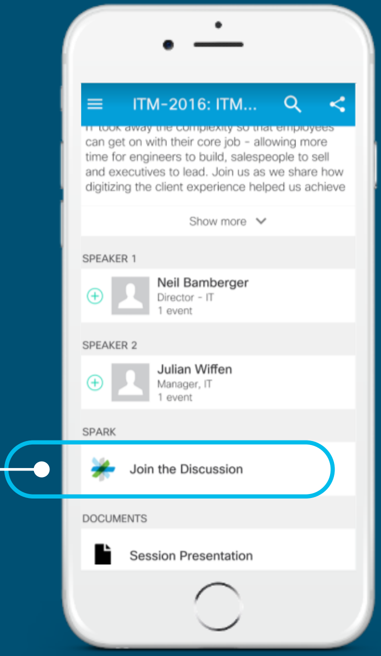
Cisco Spark

Questions?

Use Cisco Spark to communicate with the speaker after the session

How

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



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

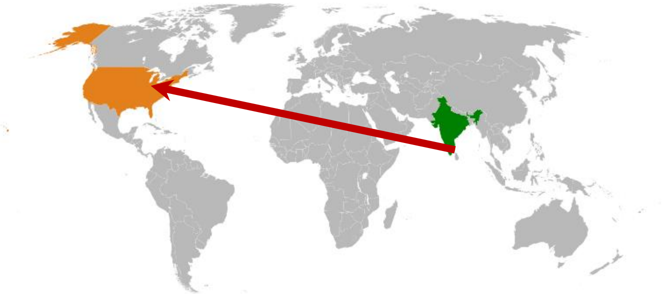
Session Presentation

cs.co/ciscolivebot# BRKSEC-2342

Cisco live!

About me

- BS in Electrical and Electronics Engineering
- Cisco Technical Assistance Center
  - Firewall and VPN technology groups
- CCIE #35505, Security
- Technical Marketing Engineer
- Adjunct professor at University of Cincinnati
- Areas of expertise
  - IOS and IOS-XE security features
  - Security solutions



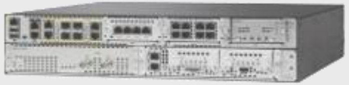
Agenda

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

Branch Router - Freedom of Choice ISR 4K and ISRv

Traditional

Physical Router

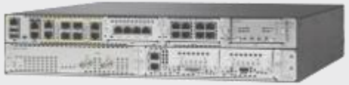


Cisco® 4000 Series ISR

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

- WAN, comprehensive security, wired and wireless access in a single, high-performance platform.
- 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
- Cisco 800 series not affected by Cisco 1100

IWAN & Cisco SD WAN ready

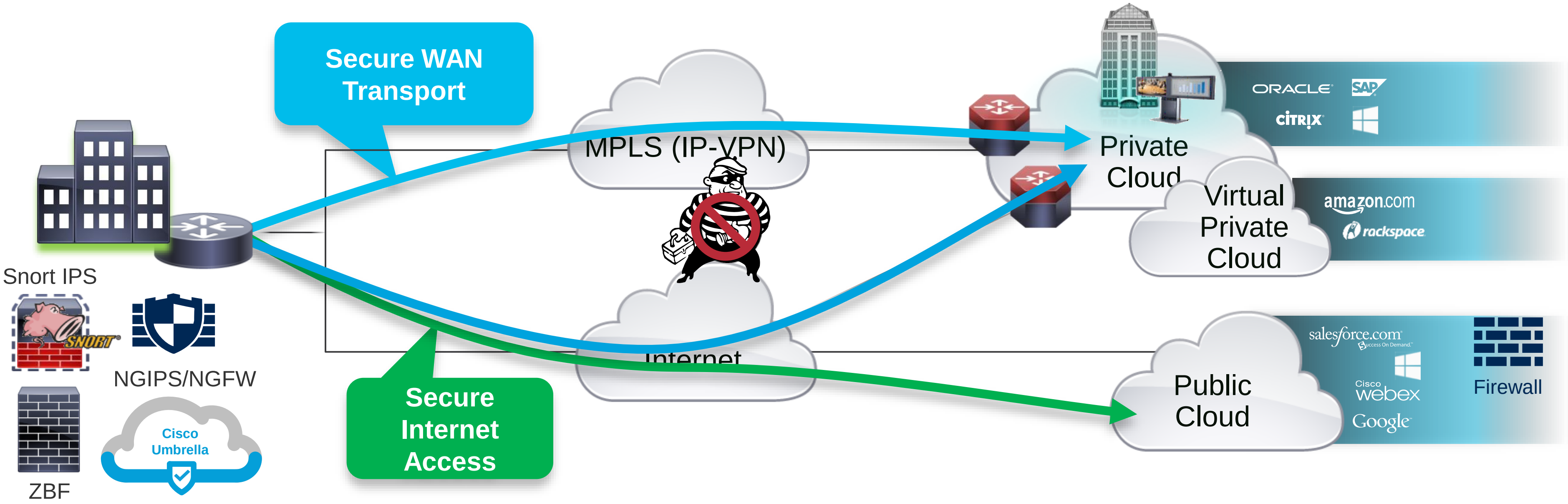
Unprecedented Security ZBF, Cisco Umbrella, ETA, State of the art Cyberthreat protection

Mobility Express

LTE Advanced

Programmability

Securing the network and users



Two areas of concern

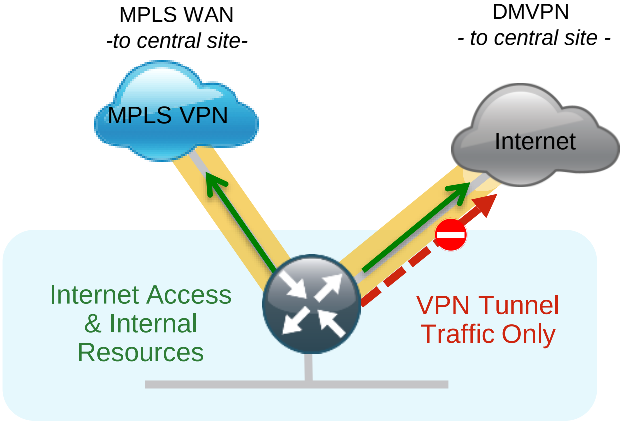
1. **Protecting the network from outside threats with data privacy over provider networks**
2. **Protecting user access to Public Cloud and Internet services; malware, privacy, phishing,…**

Central versus Direct Internet Access

Central Internet Access

- Sub-optimal access to cloud based resources
- All traffic traverses the VPN Tunnel

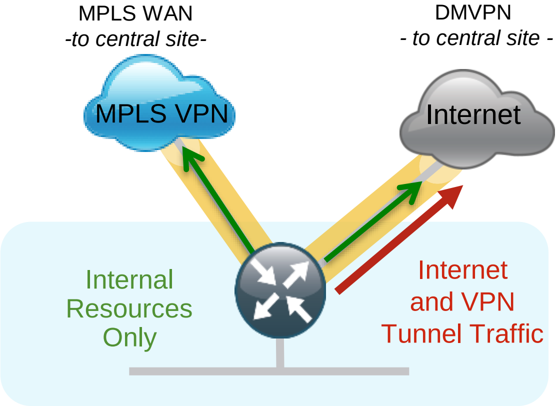
```
RS230#sh ip route
Gateway of last resort is 10.10.34.1 to network 0.0.0.0
D*EX  0.0.0.0/0 [170/2561280] via 10.4.34.1, 1w1d, Tunnel10
```



Direct Internet Access

- Optimal access to cloud based resources
- Only Internal traffic traverses the VPN Tunnel

```
RS250#sh ip route
Gateway of last resort is 172.18.100.129 to network 0.0.0.0
S*    0.0.0.0/0 [15/0] via 172.18.100.129
```



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

Common Use cases

- Provide local Internet access for Guest users
- Provide local Internet access for Employees

Challenges

- Management of many Internet Edges
- Security policy enforcement

Zone Based Firewall

Zone Based Firewall – Benefits and Requirements

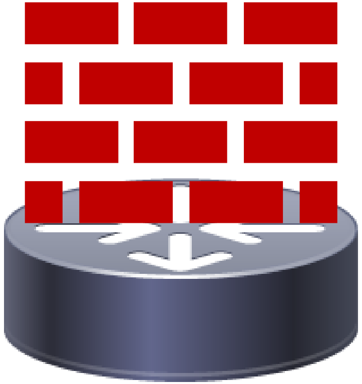
Benefits

- 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

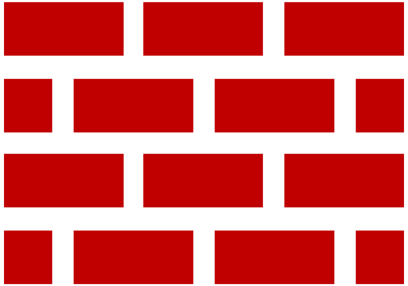
Zone Based Firewall



PCI – Payment Card Industry

Zone Based Firewall

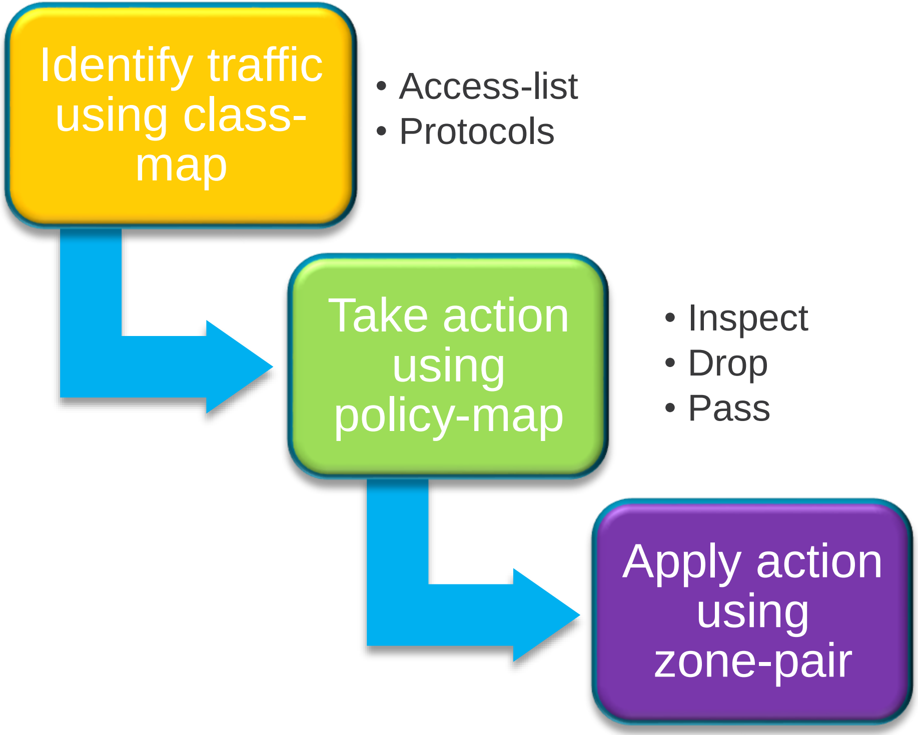
- Custom Zone
- default zone
  - “default” security zone for all INSIDE interfaces
  - default zone has always been in IOS-XE
  - default zone support on ISR-G2 is from 15.6(1)T
- Self Zone



Firewall

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

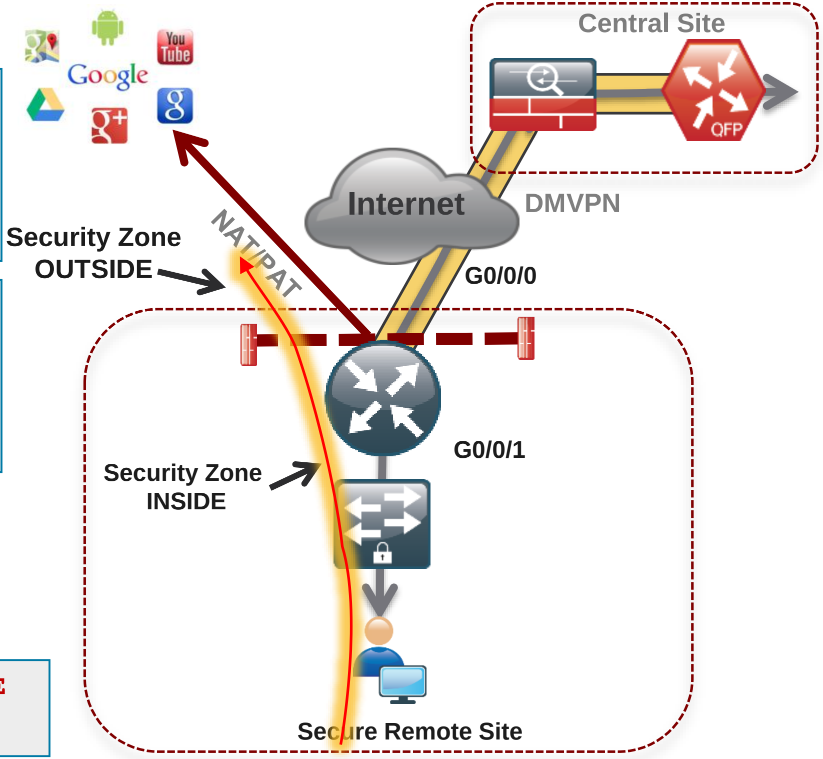
```
zone security INSIDE
zone security OUTSIDE
```

```
class-map type inspect match-any INSIDE-TO-OUTSIDE-CLASS
 match protocol ftp
 match protocol tcp
 match 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

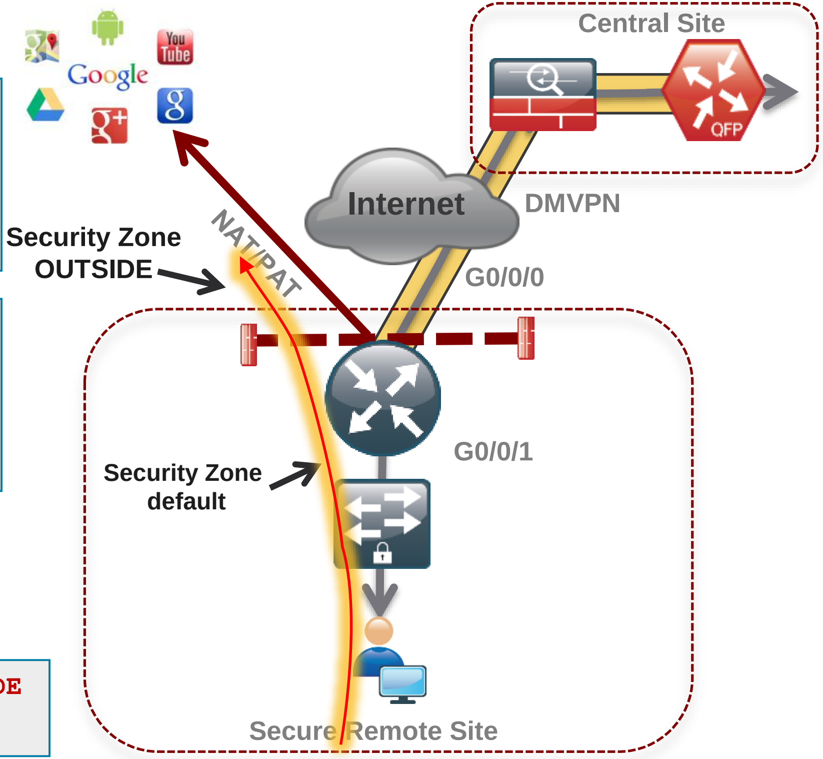
```
zone security default
zone security OUTSIDE
```

```
class-map type inspect match-any INSIDE-TO-OUTSIDE-CLASS
 match protocol ftp
 match protocol tcp
 match 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
```

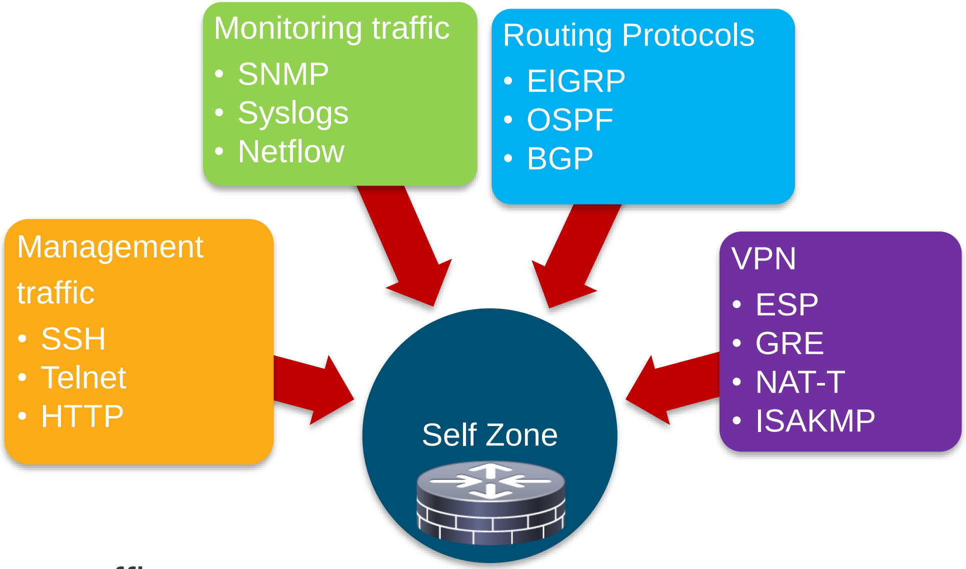


Zone Based Firewall – Self Zone

- 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

- Use 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

Self Zone

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

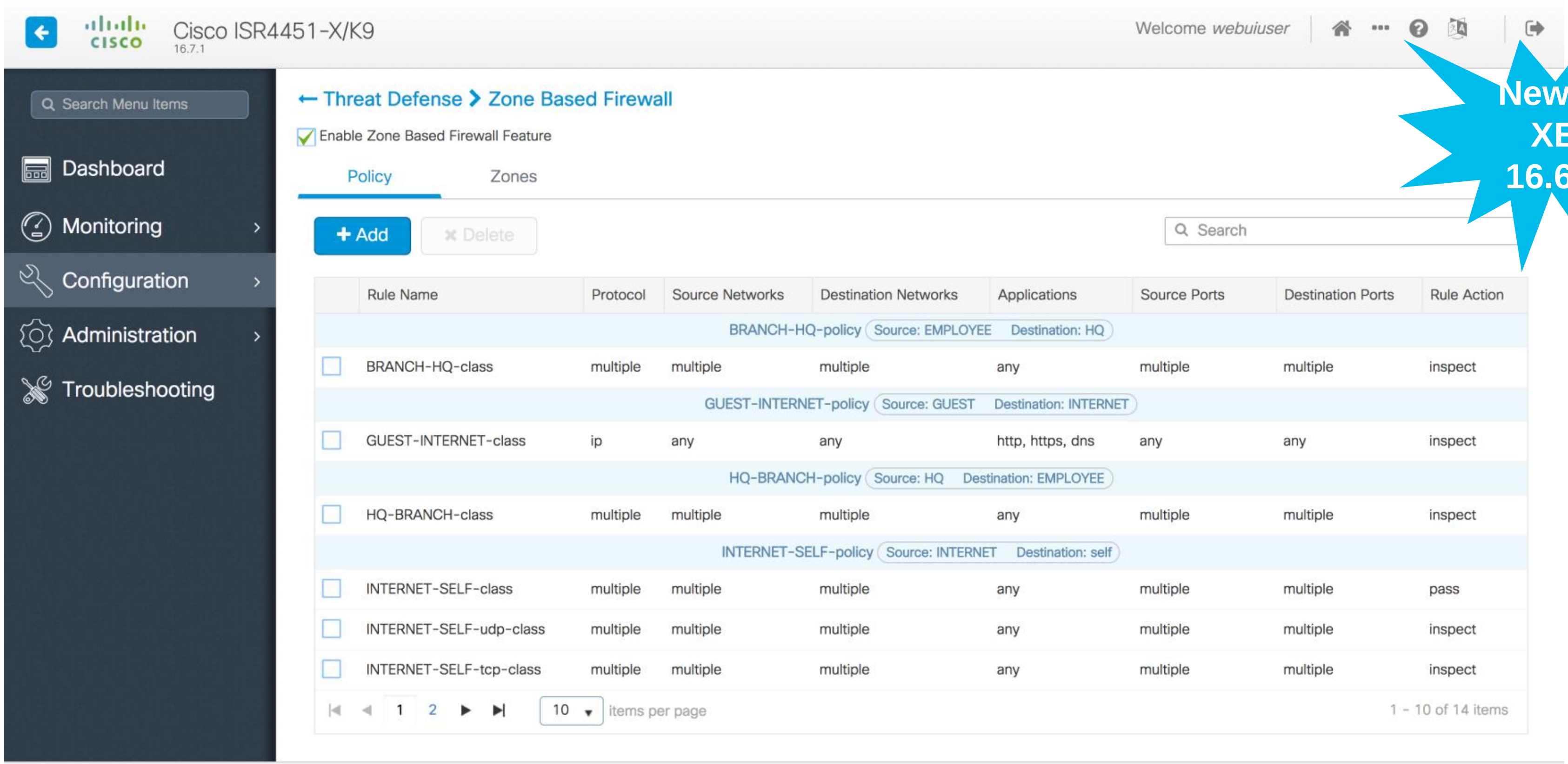
```
ip access-list extended ACL-RTR-OUT
 permit udp any host y.y.y.y eq 4500
 permit udp any host y.y.y.y eq isakmp
 permit icmp any host y.y.y.y
```

```
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
```

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

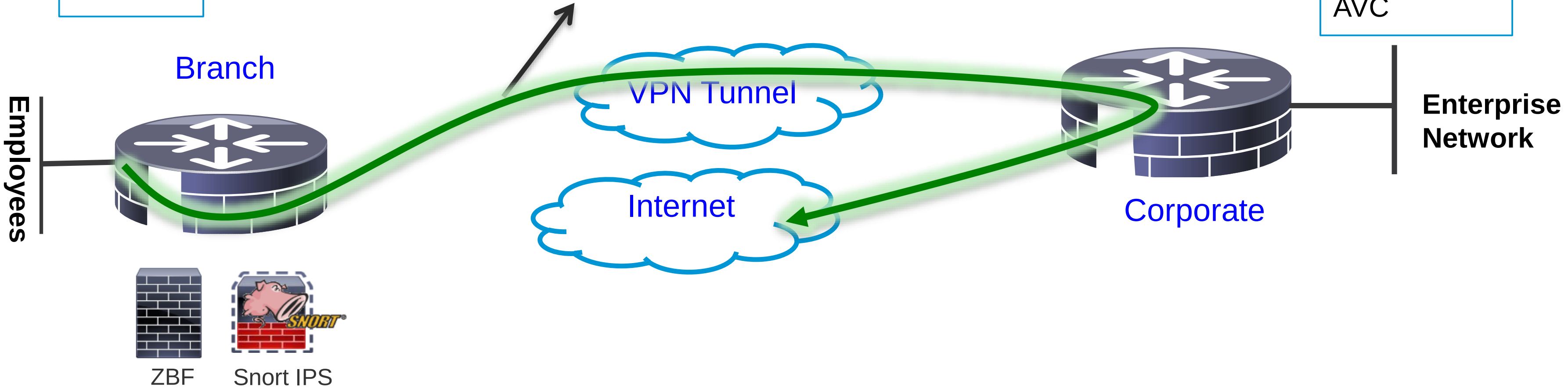
New in XE 16.6.1

Snort IPS

Snort IPS Use Case: Meet PCI Compliance

MVP
FW
IPS

NGFW
NGIPS
AMP
URL Filtering
AVC



Value Prop

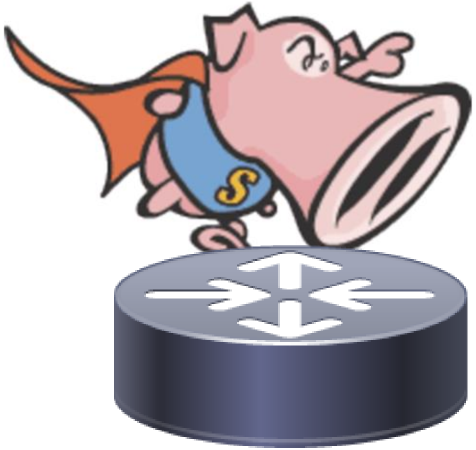
- Best of Routing & Security at Head Quarters
- Good Enough Security at the Branch to Meet Compliance
- Advanced Behavior Analysis at the Head-end

Examples:
Retail stores
Hospitals / Pharmacies

Snort IPS – What is it?

- Lightweight IPS/IDS with low TCO and automated signature updates
- Over 4 million downloads
- 500,000 registered users
- Widely deployed IPS in the world

SNORT IPS



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

Snort IPS – Benefits and Requirements

Benefits

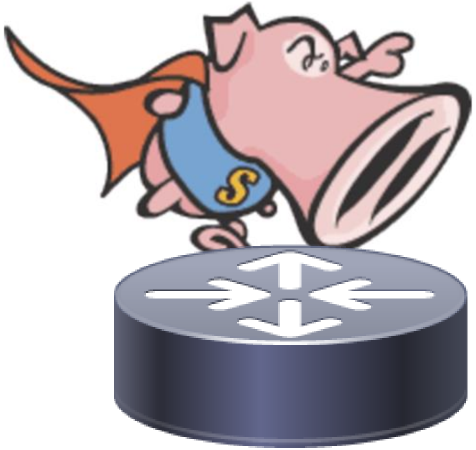
- Helps meet PCI* compliance.
- Threat protection built into ISR and ISRv branch routers
- Complements ISR Integrated Security
- Lightweight IPS solution with low TCO* and automated signature updates
- Supports VRF (16.6)

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 or 5Yr)
- Monitoring via 3-rd party

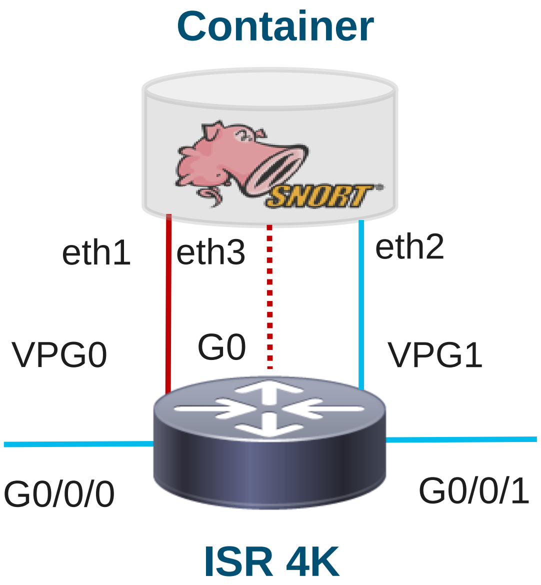
splunk>

SNORT IPS



PCI – Payment Card Industry TCO – Total Cost of Ownership

Snort IPS Configuration –Virtual Service Networking



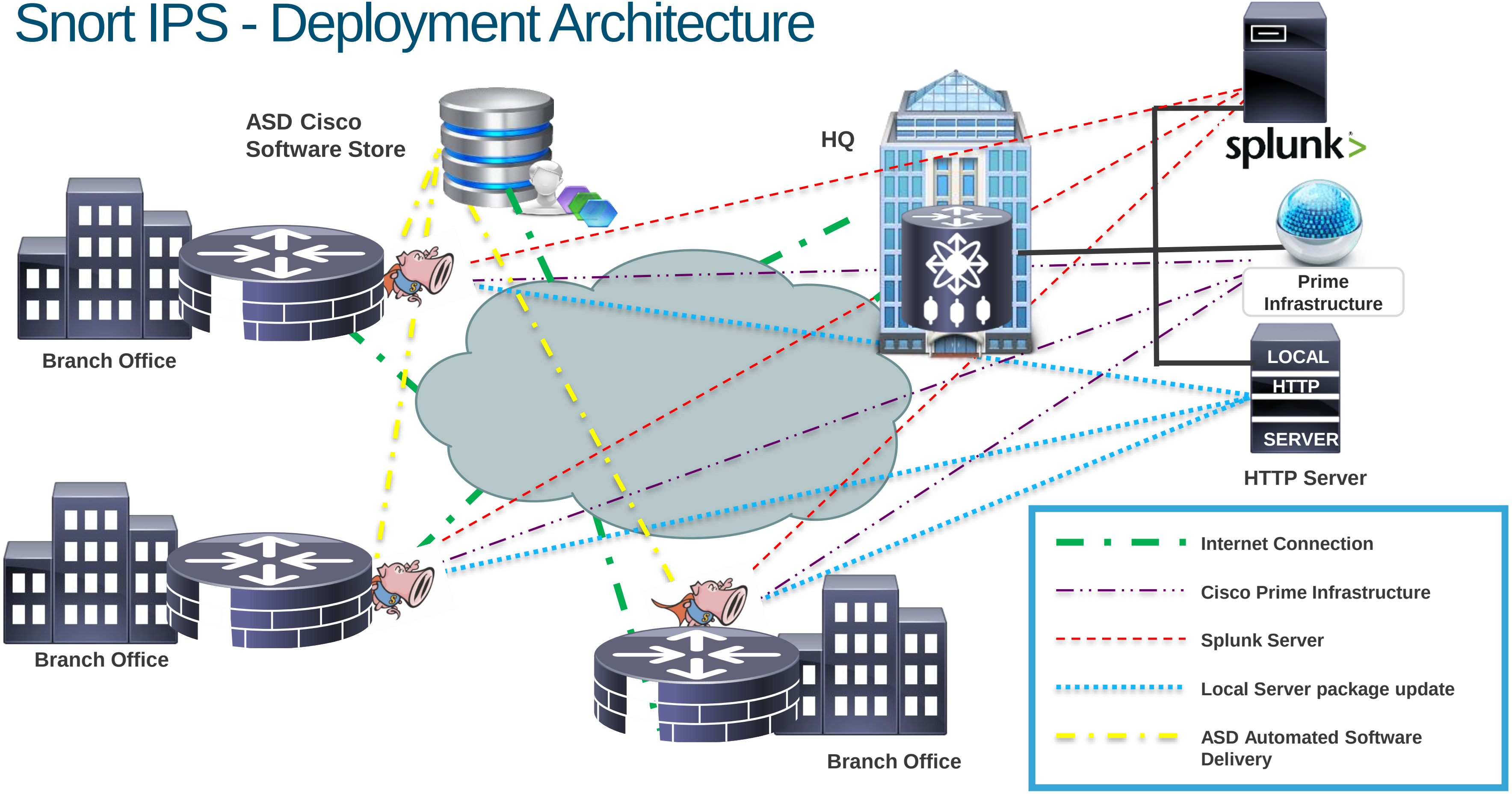
Purpose of the VPGs

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

    [OR]

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

Snort IPS - Deployment Architecture



- Internet Connection
- Cisco Prime Infrastructure
- Splunk Server
- Local Server package update
- ASD Automated Software Delivery

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)

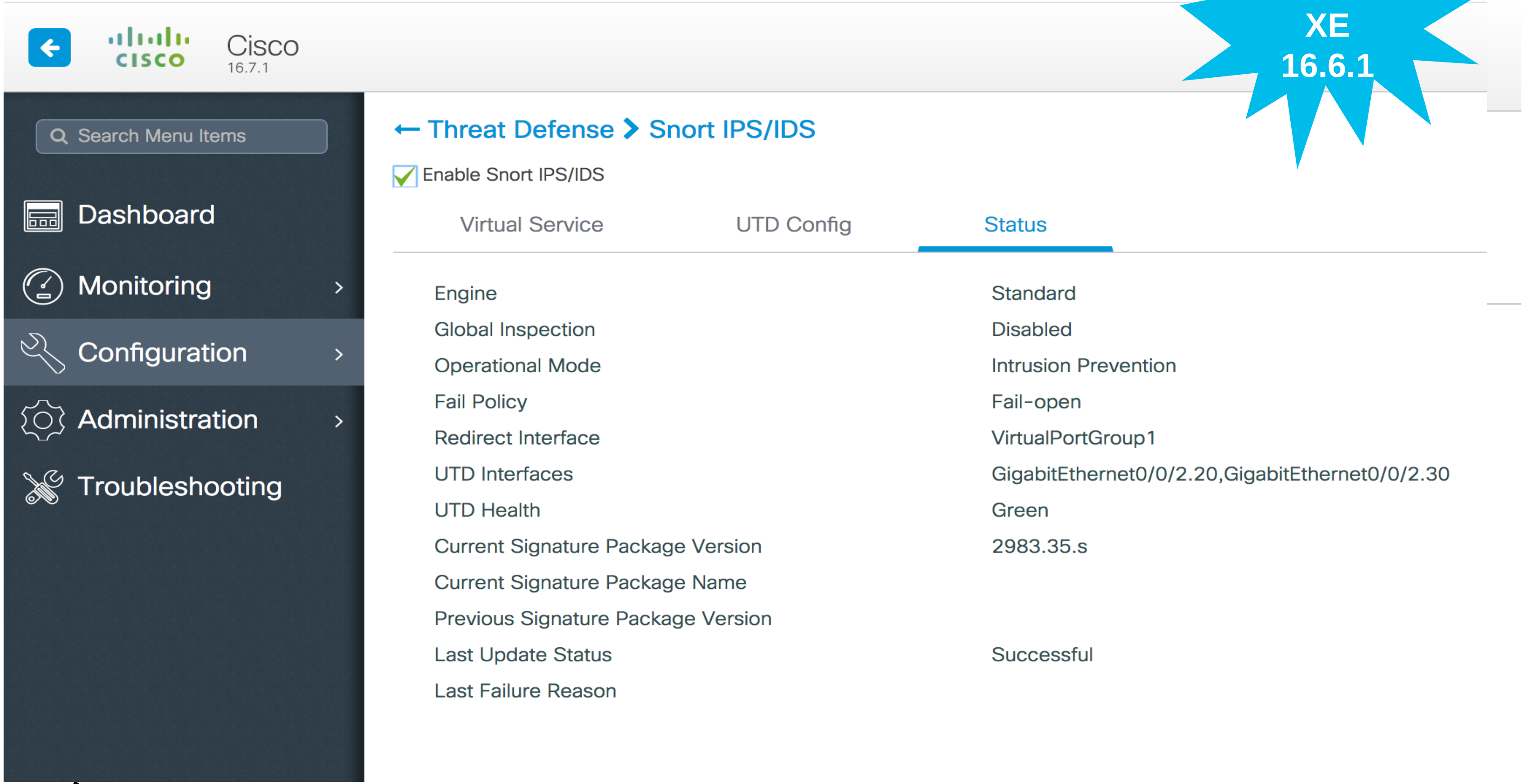
```
utd
all-interfaces
engine standard
 fail close
```

Step 6 Whitelisting (optional)

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

On-box WebUI - Snort IPS/IDS

NEW in XE 16.6.1



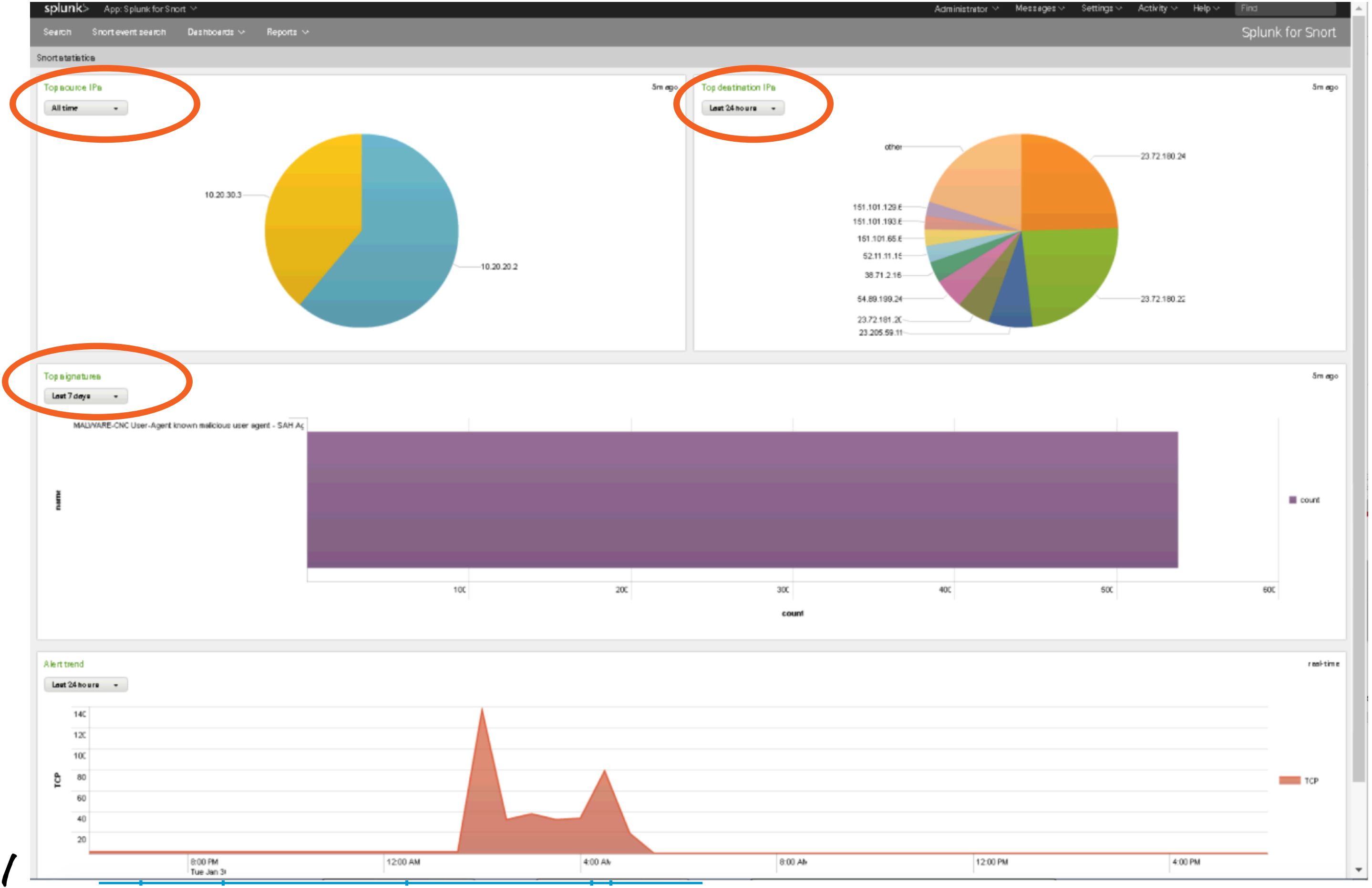
← Threat Defense > Snort IPS/IDS

☑ 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)



For Your Reference

Snort IPS - Resources

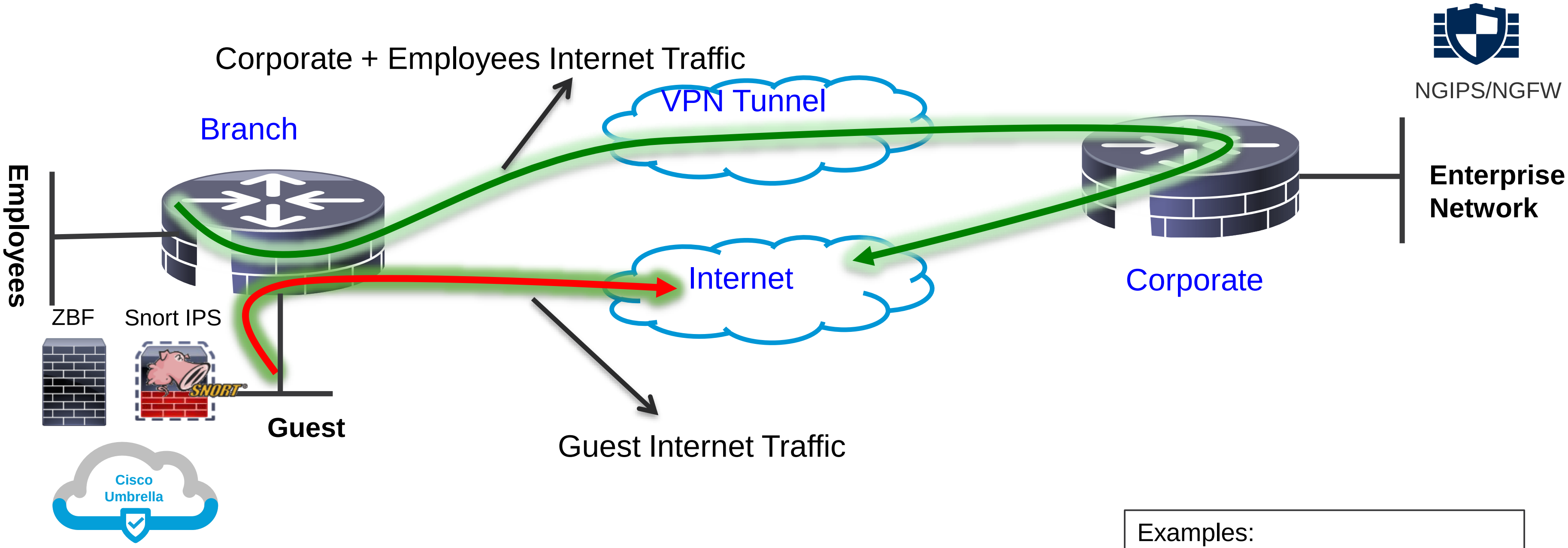
At-A-Glance
http://www.cisco.com/c/dam/en/us/products/collateral/security/router-security/at-a-glance-c45-735895.pdf

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

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

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 Powered IPS provides basic intrusion protection
- Corporate devices reach Internet via HQ

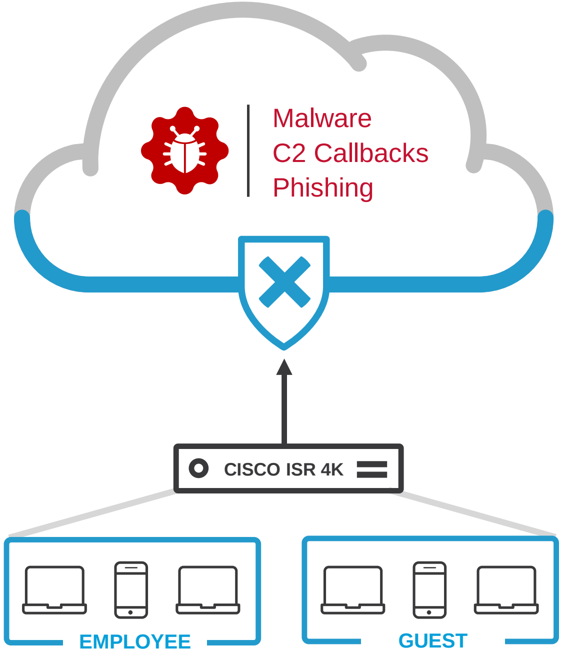
Examples:
Retail stores / Auto Dealerships
Hospitals / Pharmacies
Financials
Schools / Universities

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)
- 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

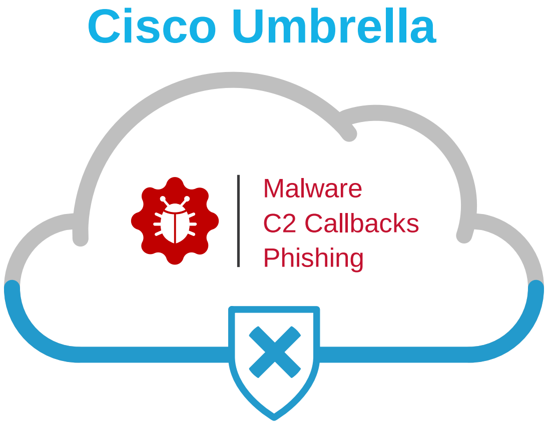
Cisco Umbrella Integration – Benefits and Requirements

Benefits

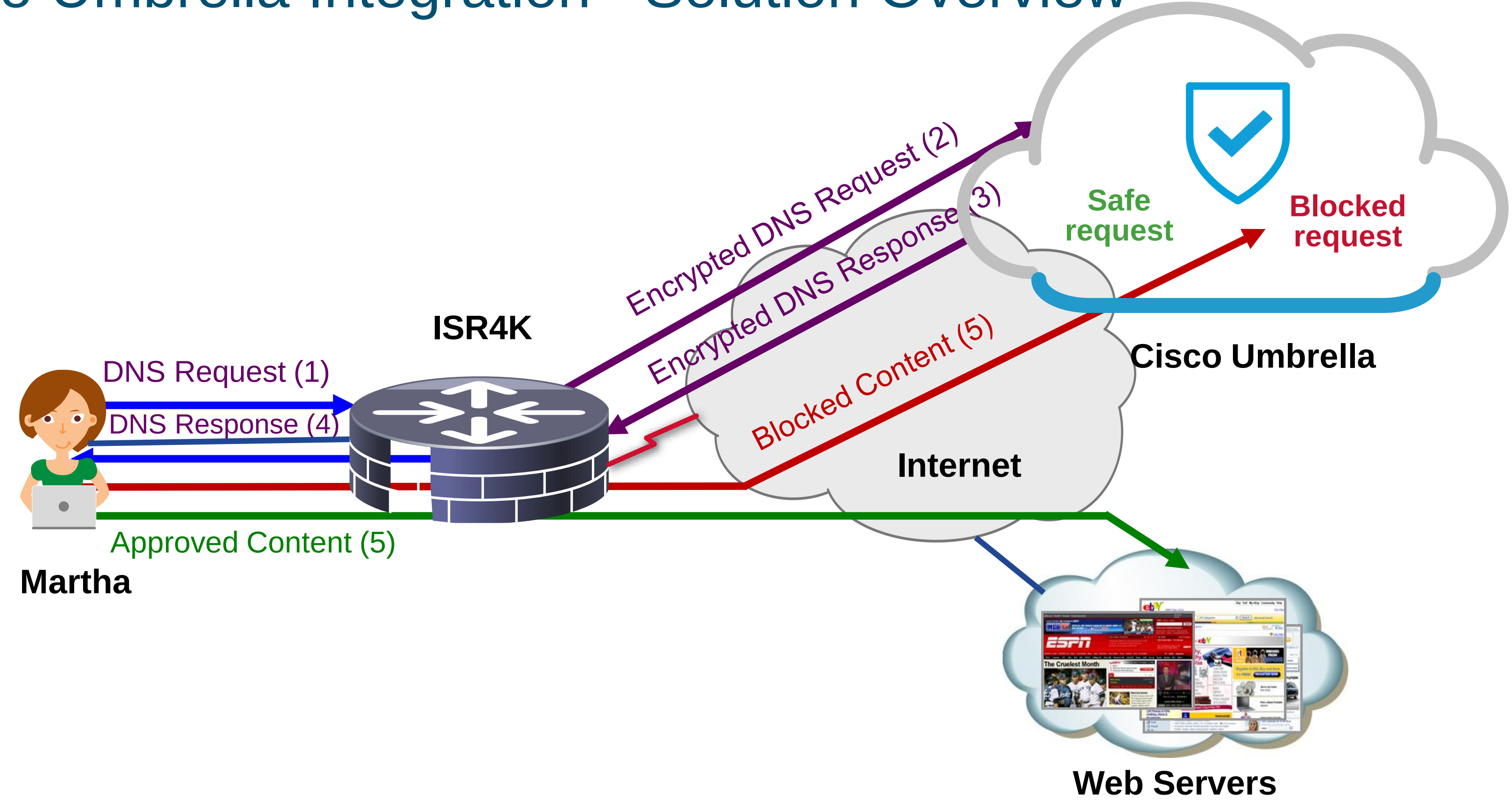
- DNS layer protection
- No need to look within HTTP or HTTPS packets
- Complements ISR Integrated Security
- Configure policies based on ’tags’ per interface
- Supports VRF

Requirements

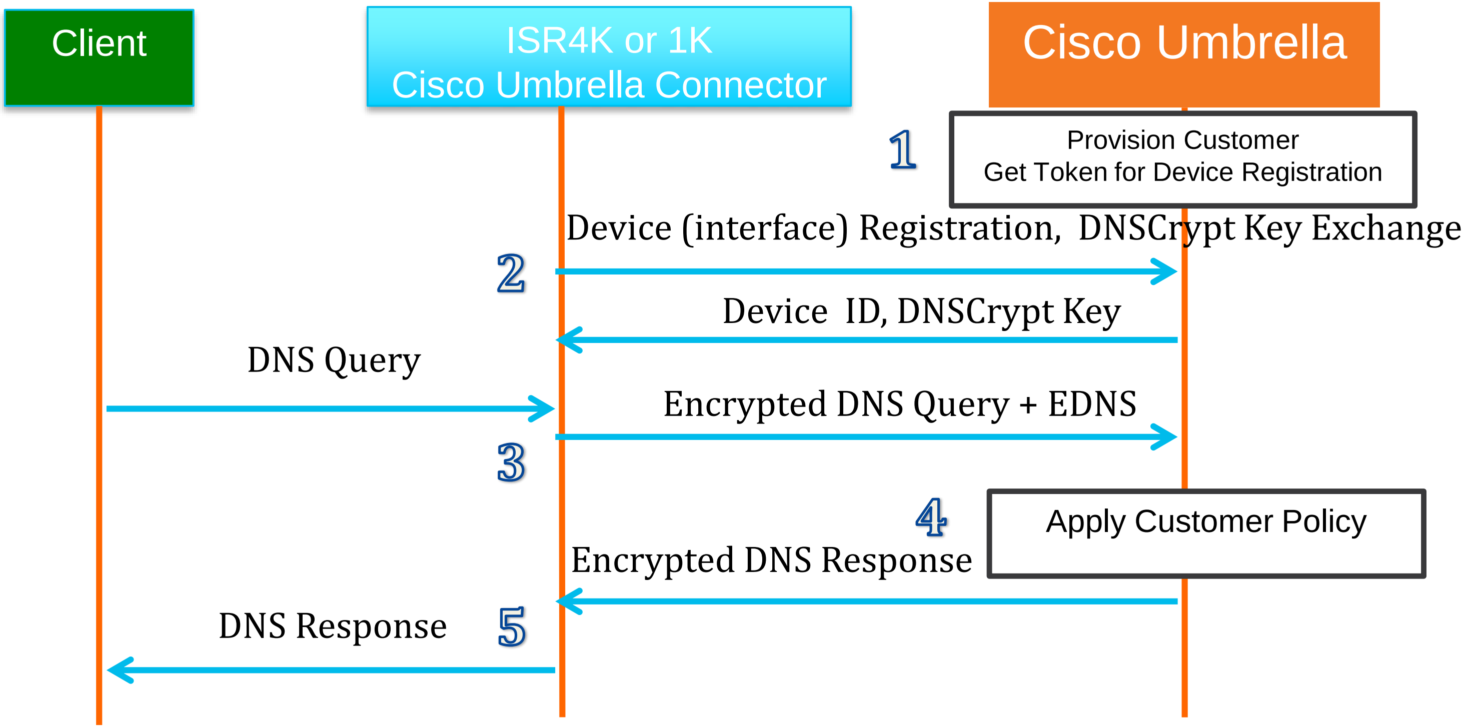
- Provision to get token ID and portal login
- SEC-K9 license
- XE 16.3 and above on ISR 4K series routers
- XE 16.8.1 and above on ISRv and ISR 1K series routers
- Per device subscription
- Monitoring and Reporting via Umbrella Portal



Cisco Umbrella Integration - Solution Overview

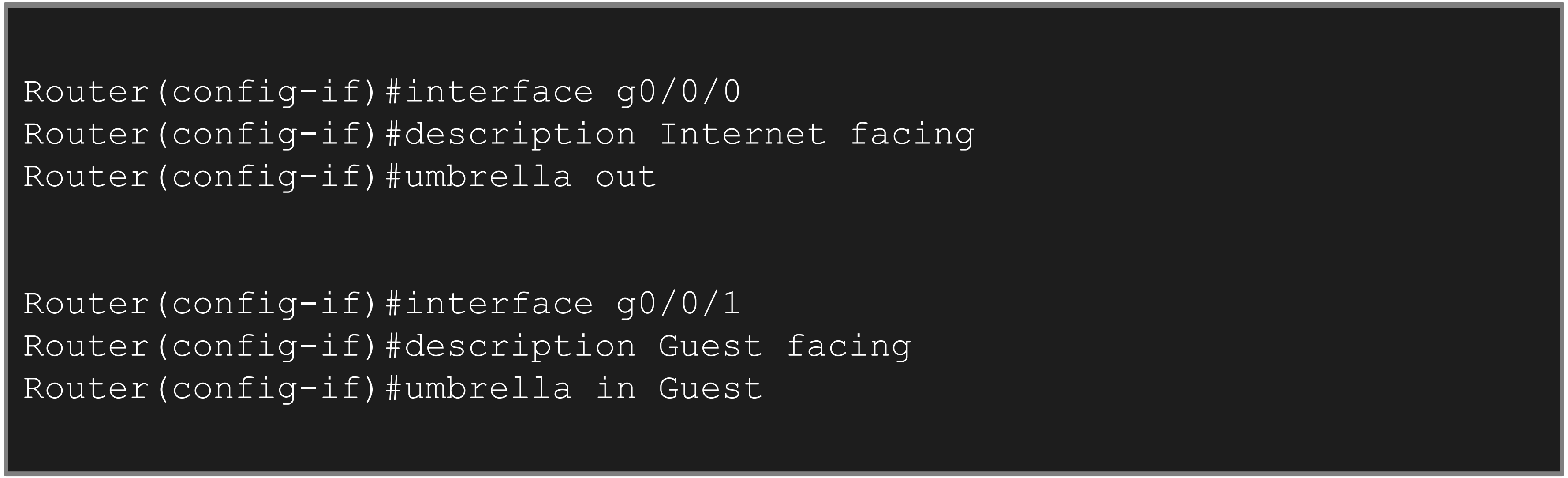


Cisco Umbrella Integration - Packet Flow with DNSCrypt



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
```

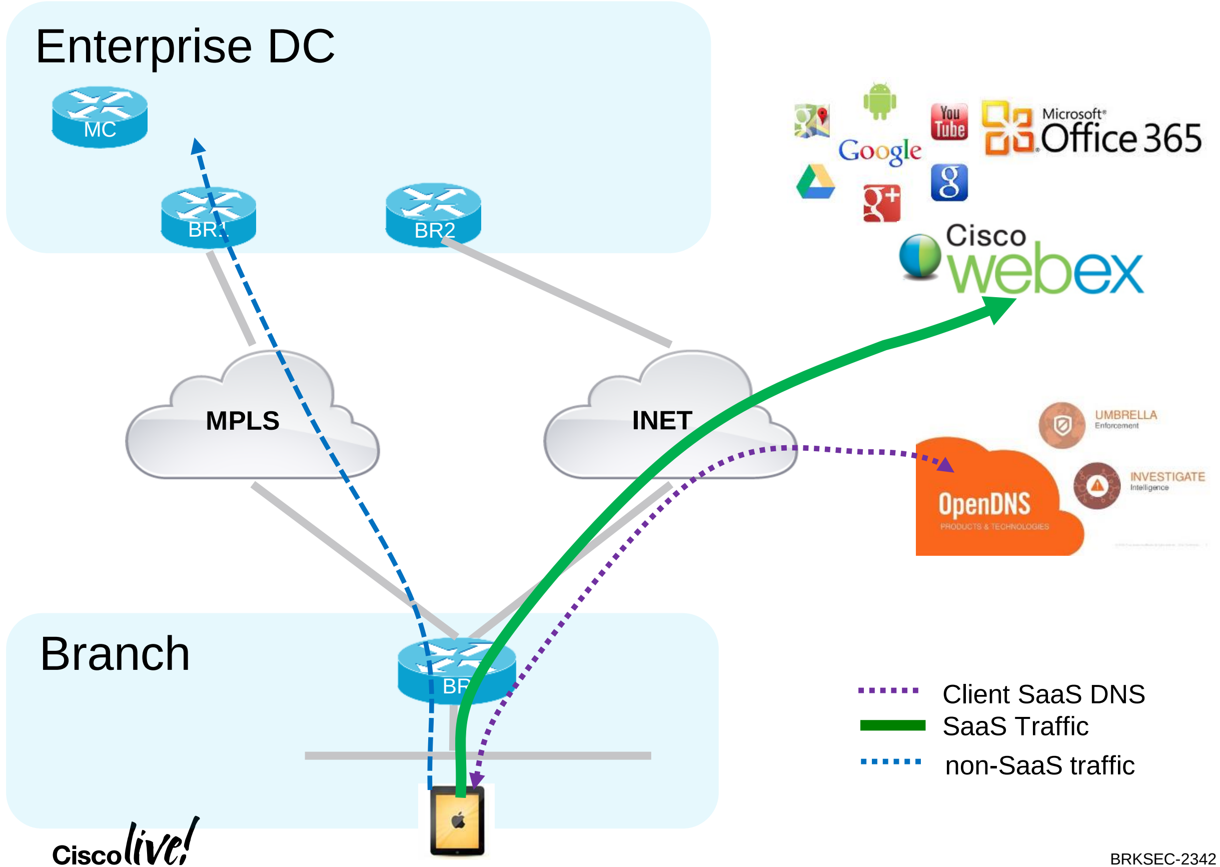
Step 2 Configure local domain (optional) and token

```
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 DCAed)

- 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 – IWAN Direct Cloud Access use case

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 – IWAN Direct Cloud Access use case

Step 2 PfR - Hub MC

```
domain IWAN
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 IWAN
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 DAC-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 6 Enable Umbrella “in” with DCA

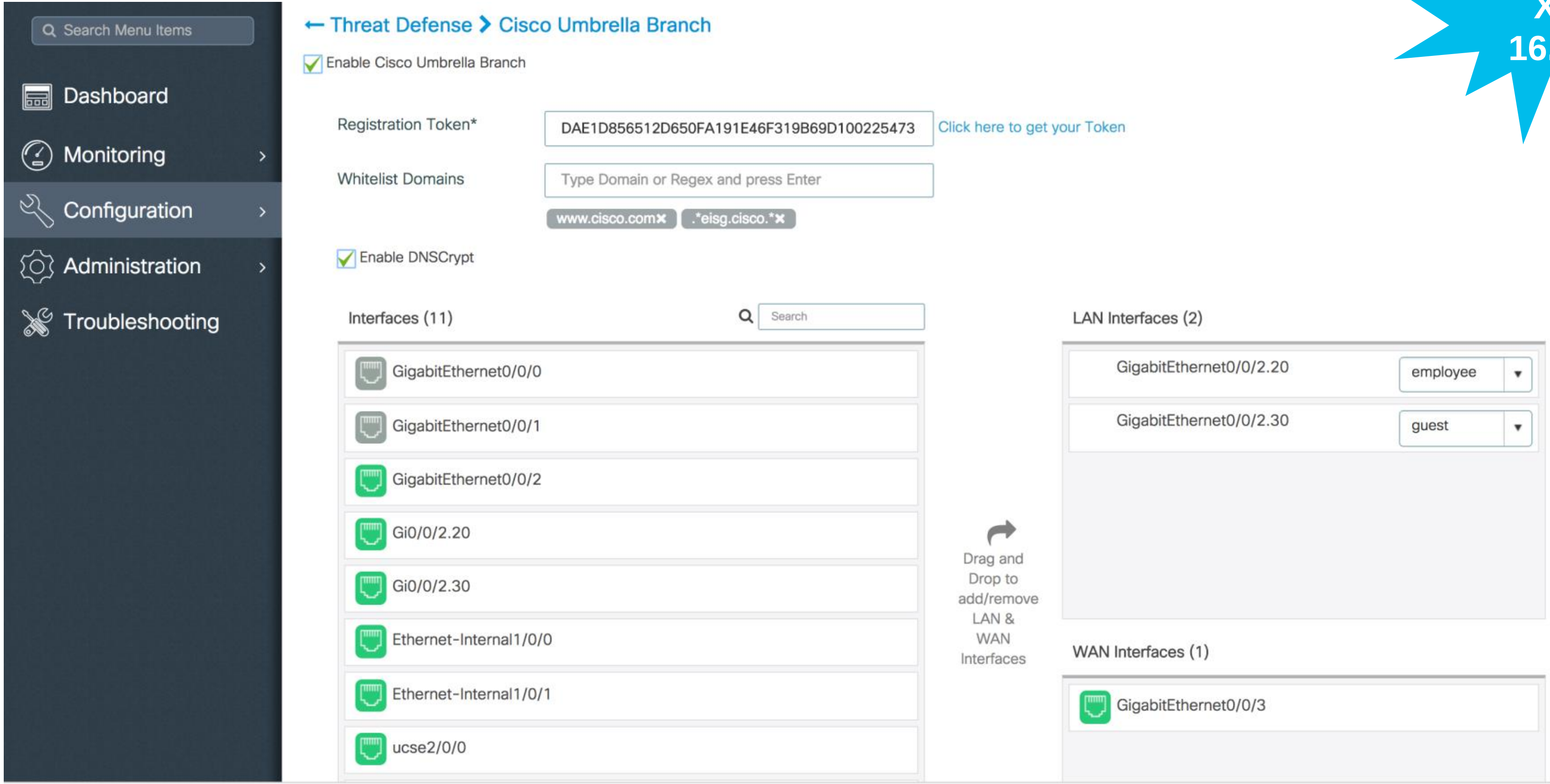
```
interface g0/0/1
 umbrella in direct-cloud-access DCA-list-PMAP
```

Step 7 Enable Umbrella “out”

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

On-box WebUI - Cisco Umbrella

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

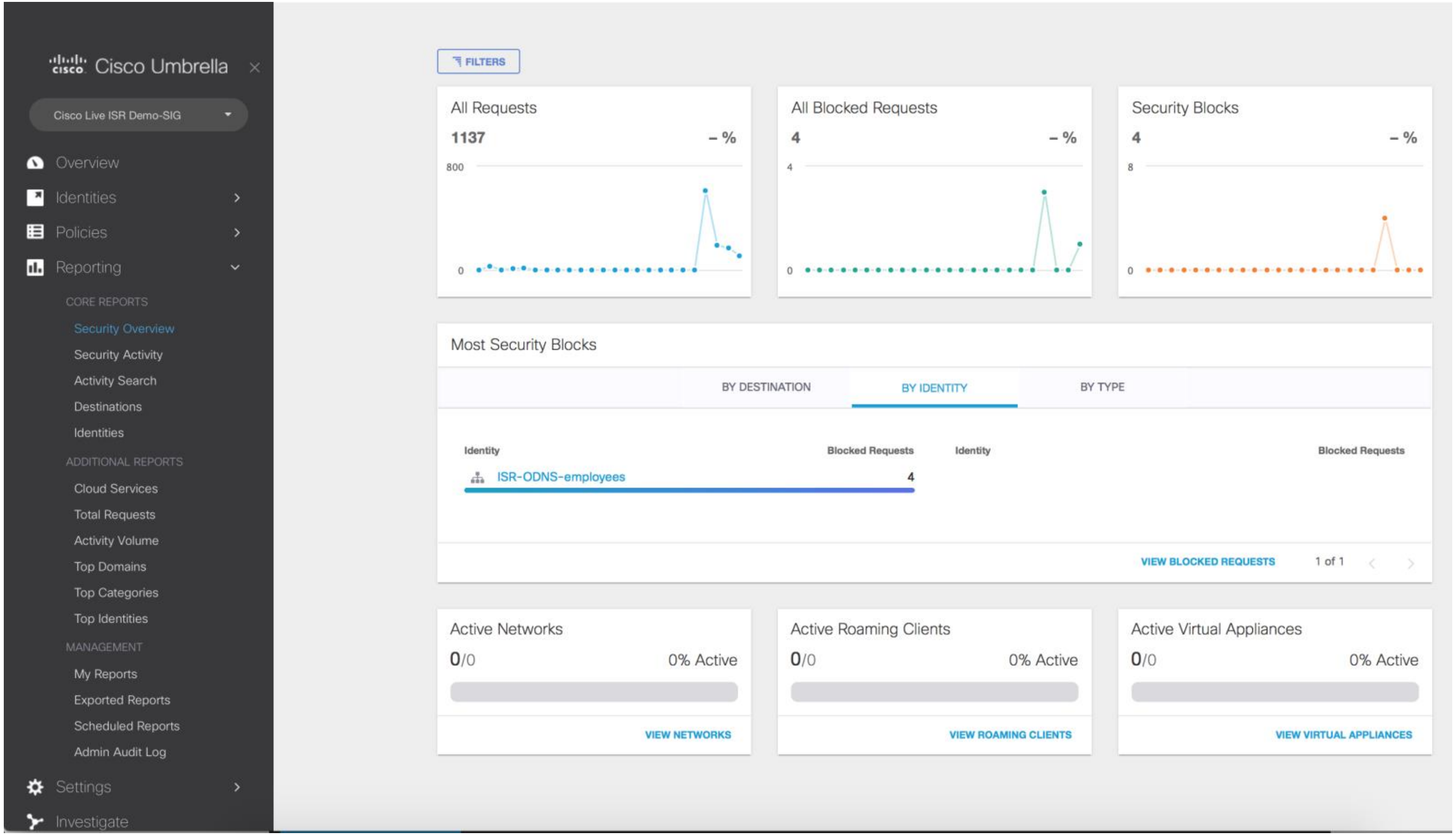
LAN Interfaces (2)

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

WAN Interfaces (1)

- GigabitEthernet0/0/3

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		

1 of 1

Active Networks
0/0 0% Active

Active Roaming Clients
0/0 0% Active

Active Virtual Appliances
0/0 0% Active

For Your Reference

Cisco Umbrella - Resources

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

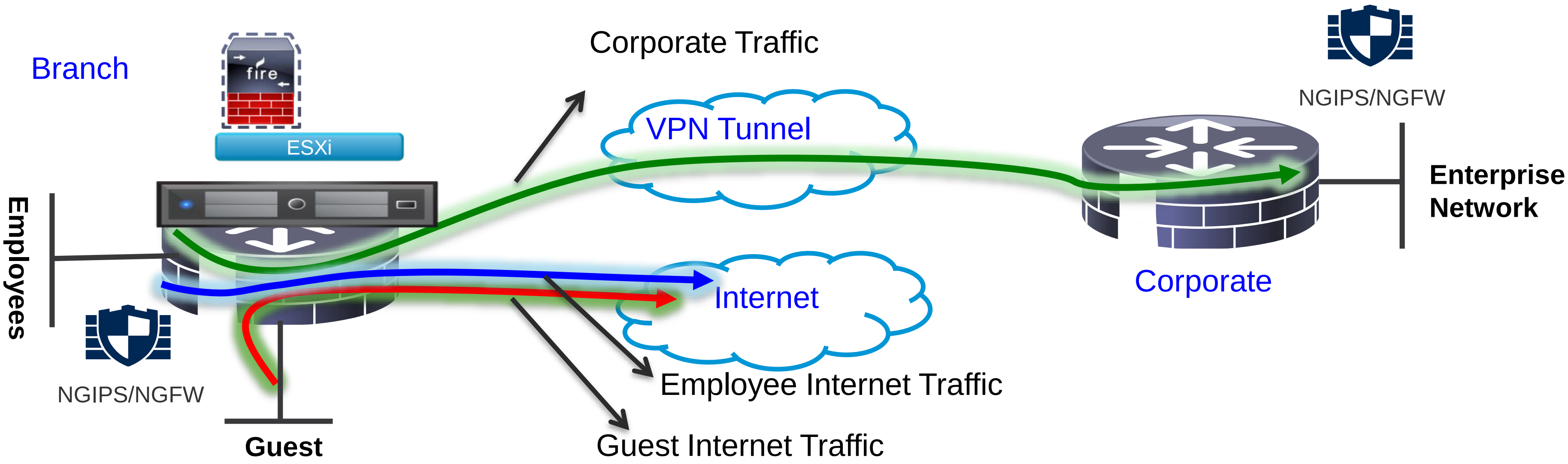
Cisco Umbrella Configuration Guide:
http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_utd/configuration/xe-16/sec-data-umbrella-branch-xe-16-book/sec-data-umbrella-bran.html

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

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.)

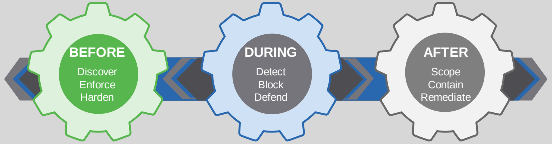
Firepower Threat Defense for ISR - Appendix

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



Network Visibility	NGIPS	Advanced Malware Protection
Granular App Control	Security Intelligence	Retrospective Security
Modern Threat Control	URL Filtering	IoCs/Incident Response

Visibility and Automation

+

AppX + Security License

Cisco UCS®

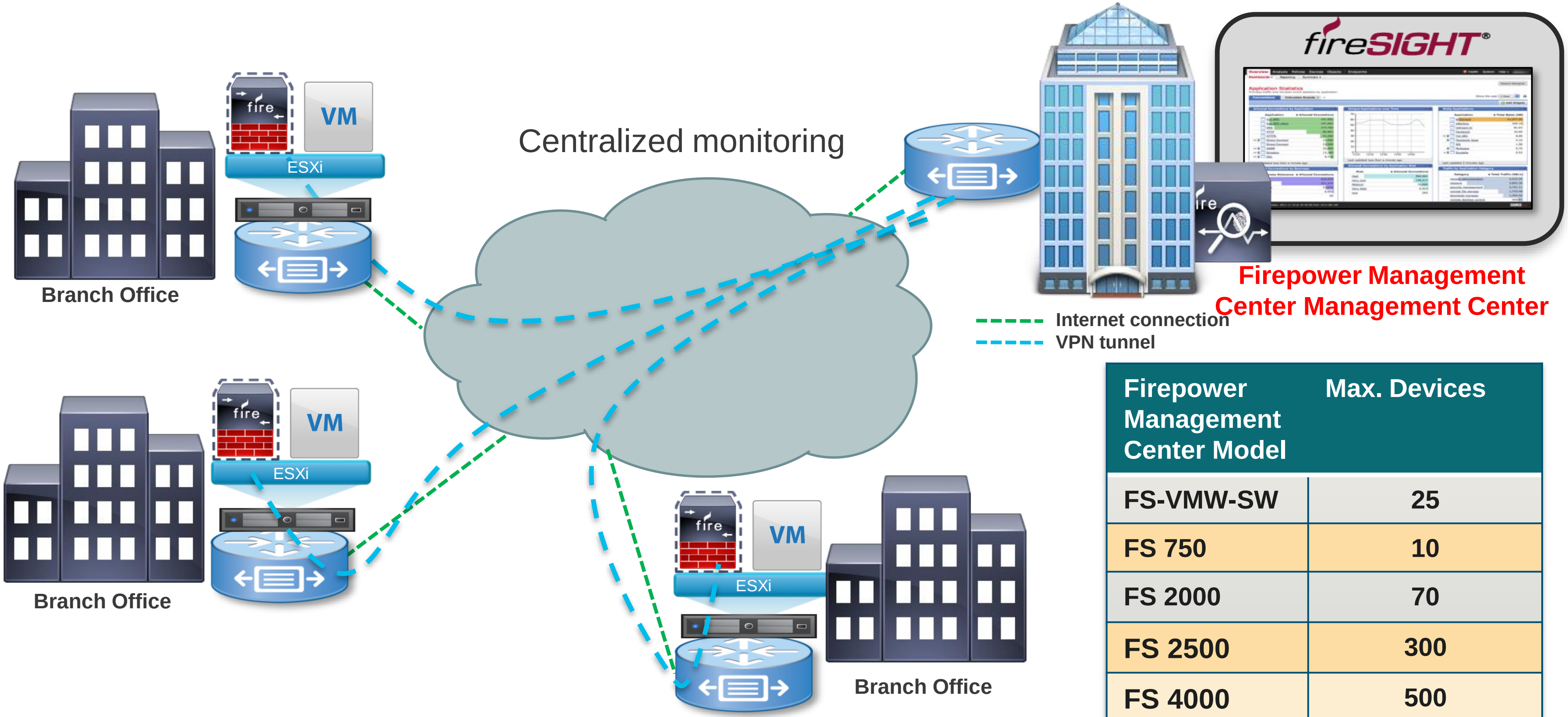
Cisco® 4000 Series ISR

OR

Cisco ISR G2 Series

Free Up Valuable Square Footage Generate More Revenue $$$

Firepower Threat Defense - Deployment Architecture



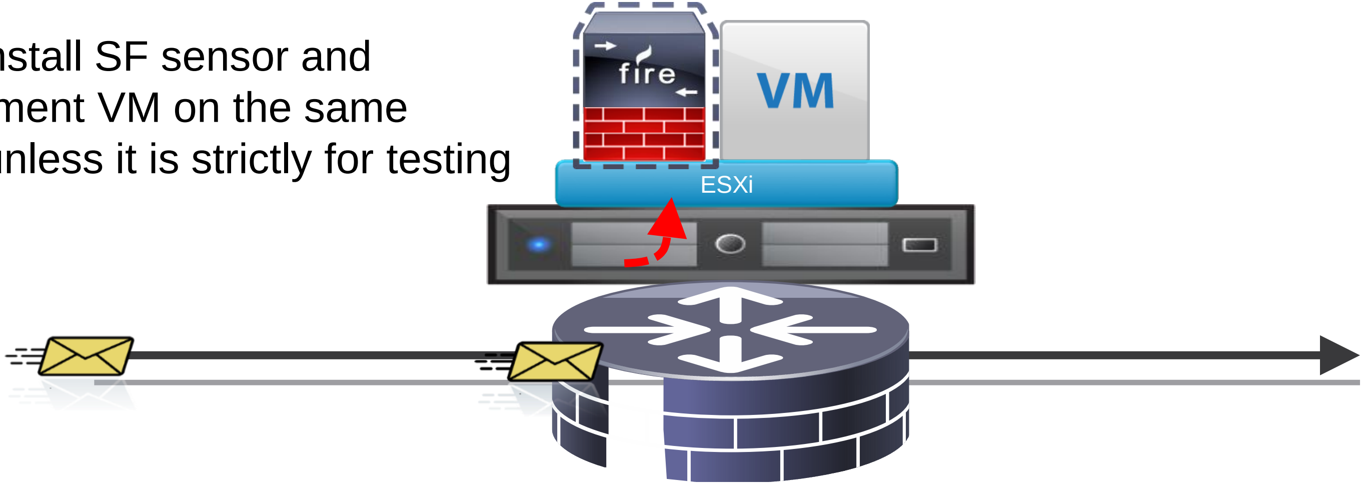
Firepower Management Center Model	Max. Devices
FS-VMW-SW	25
FS 750	10
FS 2000	70
FS 2500	300
FS 4000	500
FS 4500	750

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

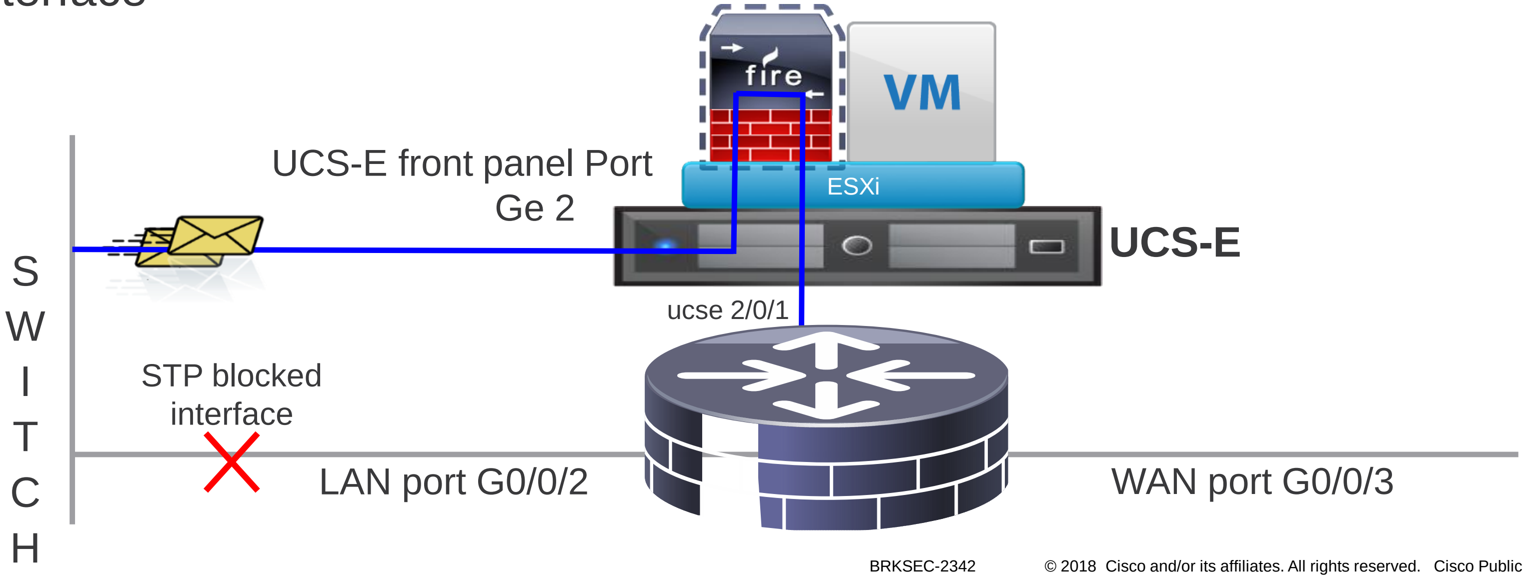
Configuration Steps

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
```

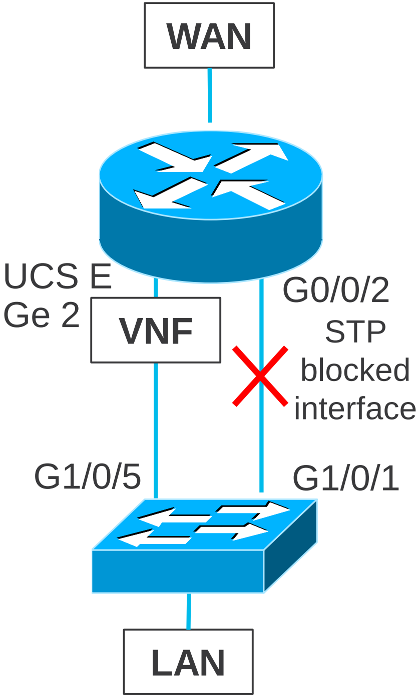
Firepower Threat Defense for ISR - IPS using BDI

- 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
```

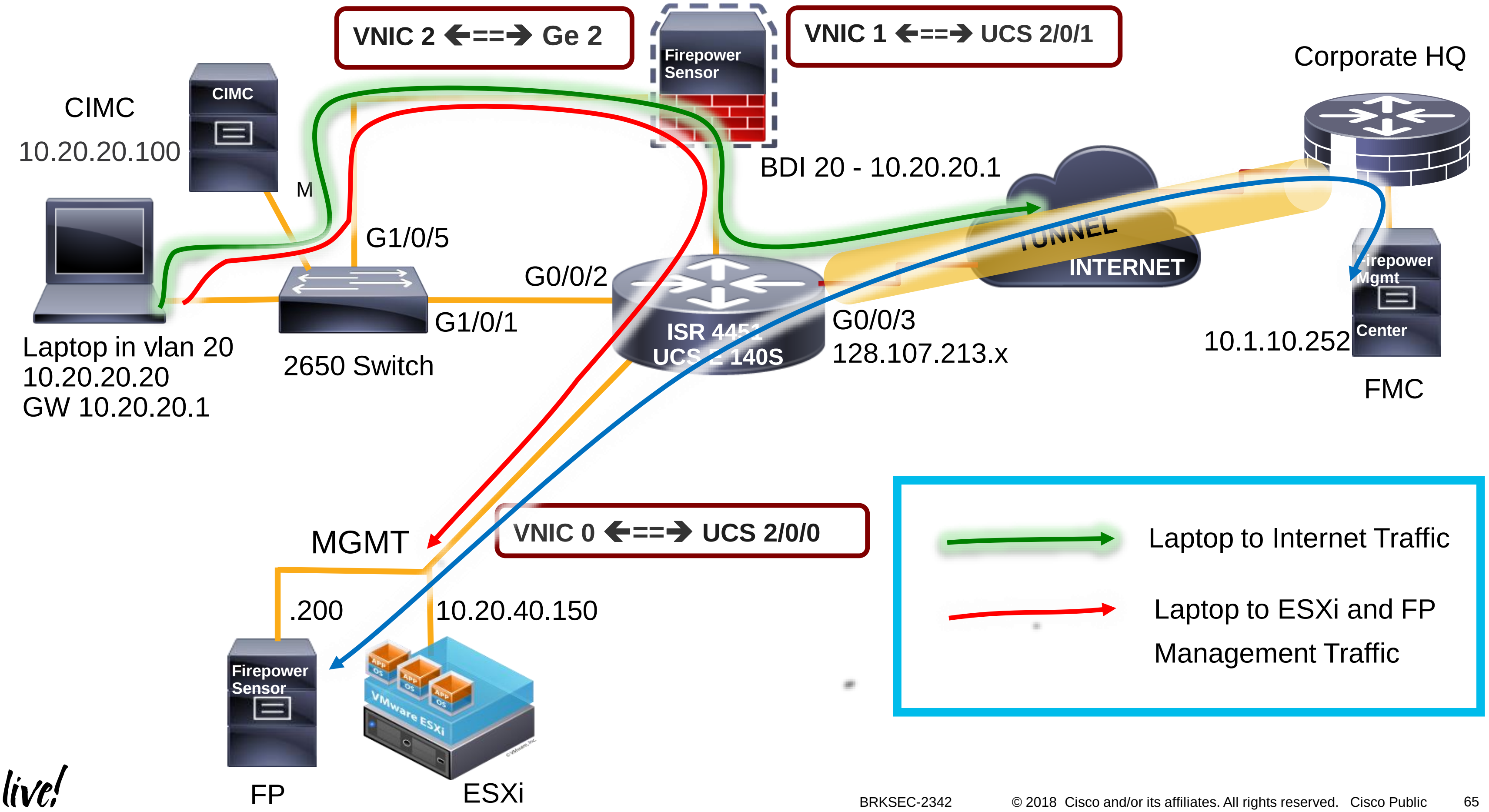
Port connected to the routers G0/0/2 Port

```
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

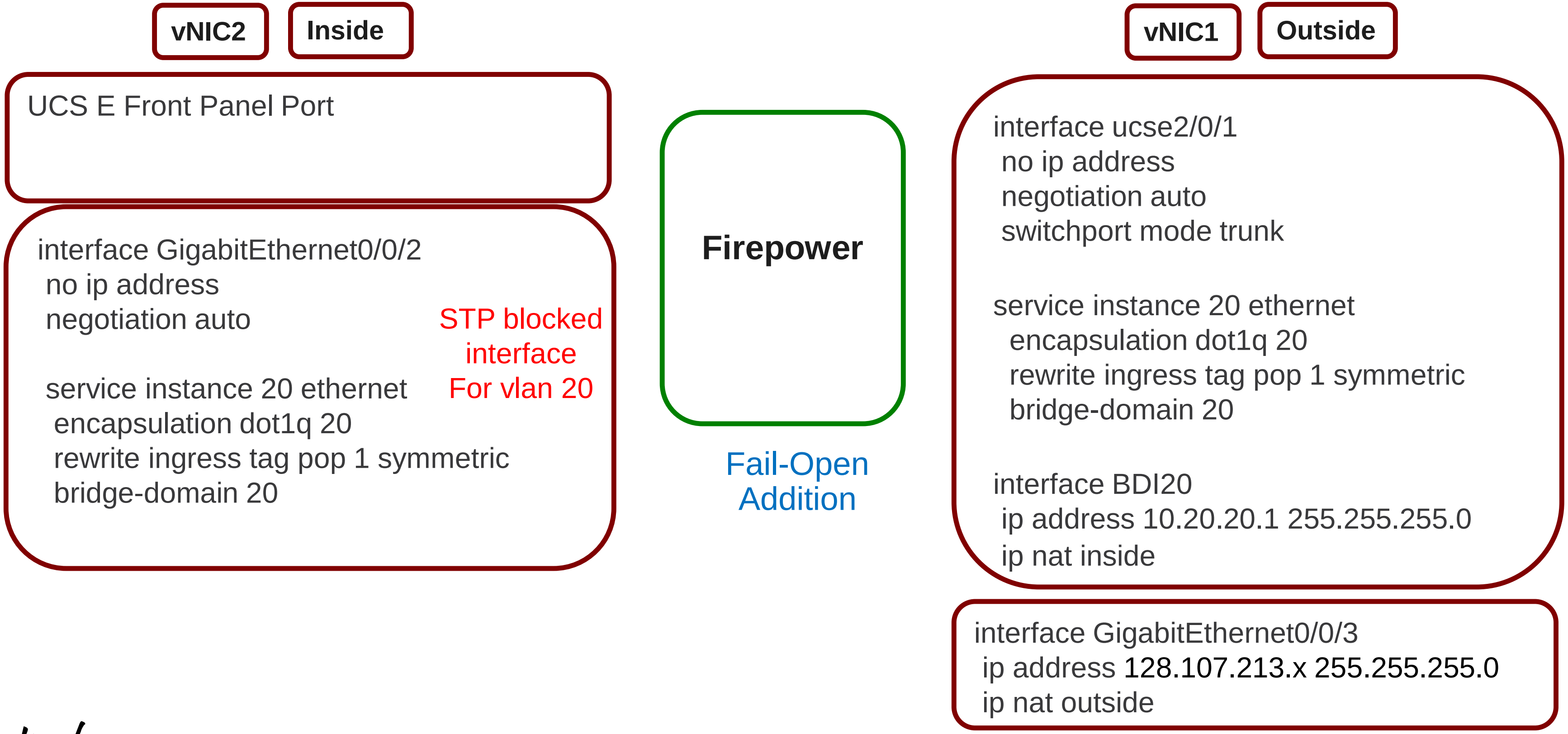
```
interface GigabitEthernet1/0/5
 description Connected to Ge 2 port on the UCS-E Blade
 switchport trunk allowed vlan 20,30
 switchport mode trunk
 spanning-tree cost 10
```

Firepower Threat Defense for ISR – NGIPSv using BDI



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

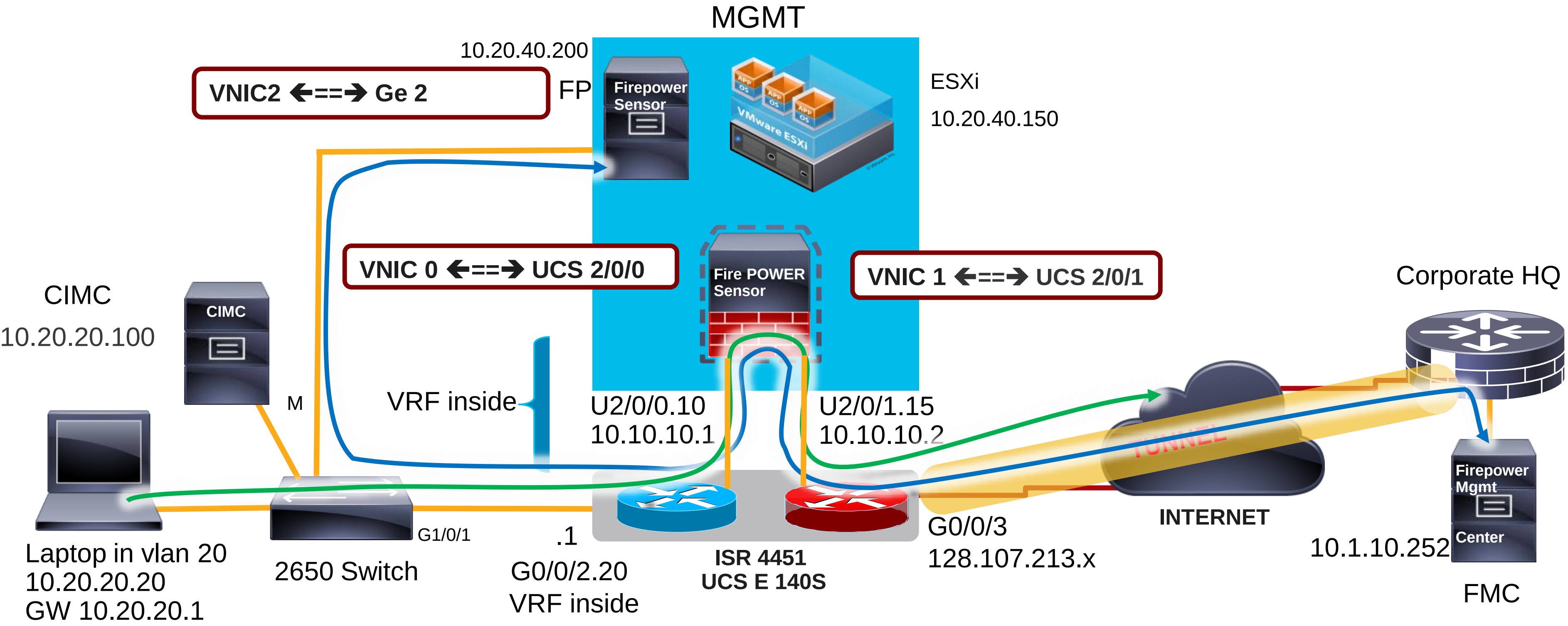
Outside

```
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
```

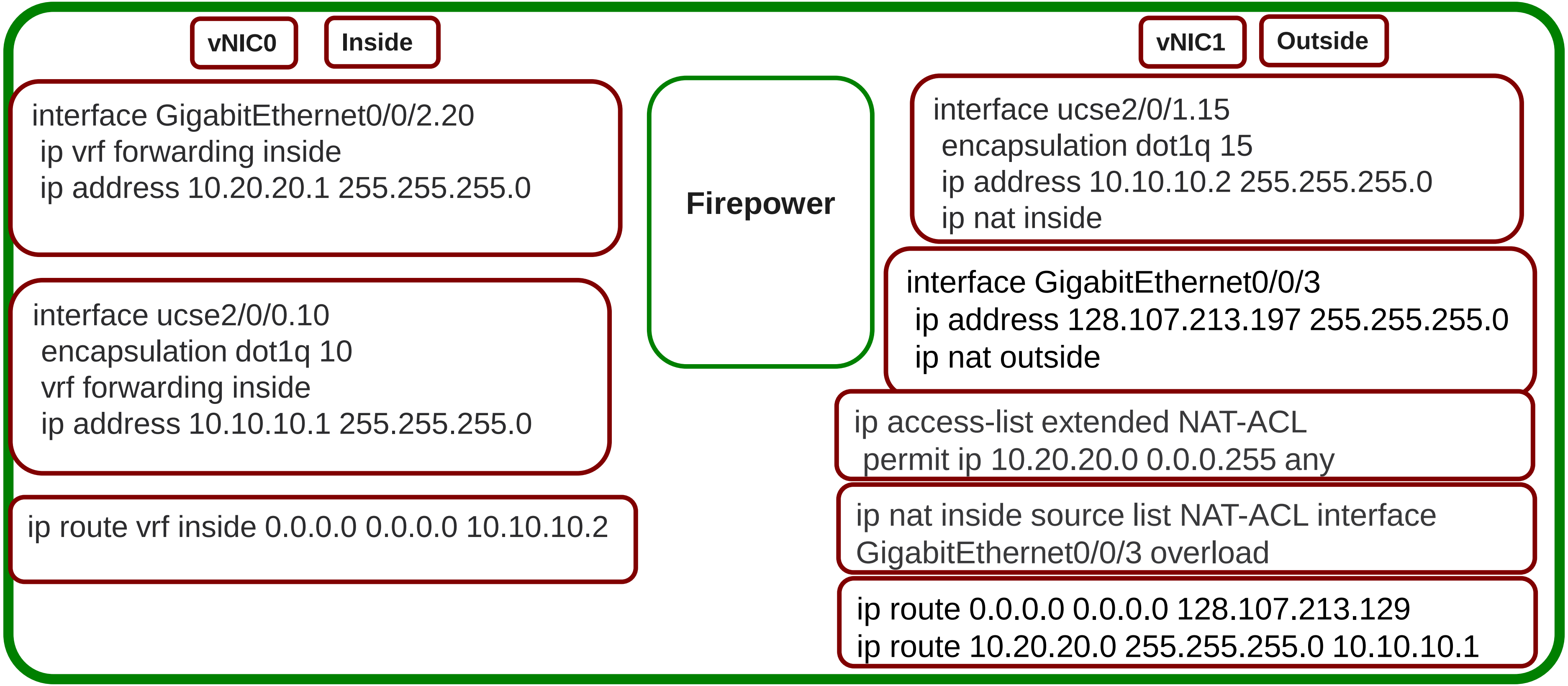
IPS inline with VRF

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



vNIC0 | Inside

```
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
```

Firepower

vNIC1 | Outside

```
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
```

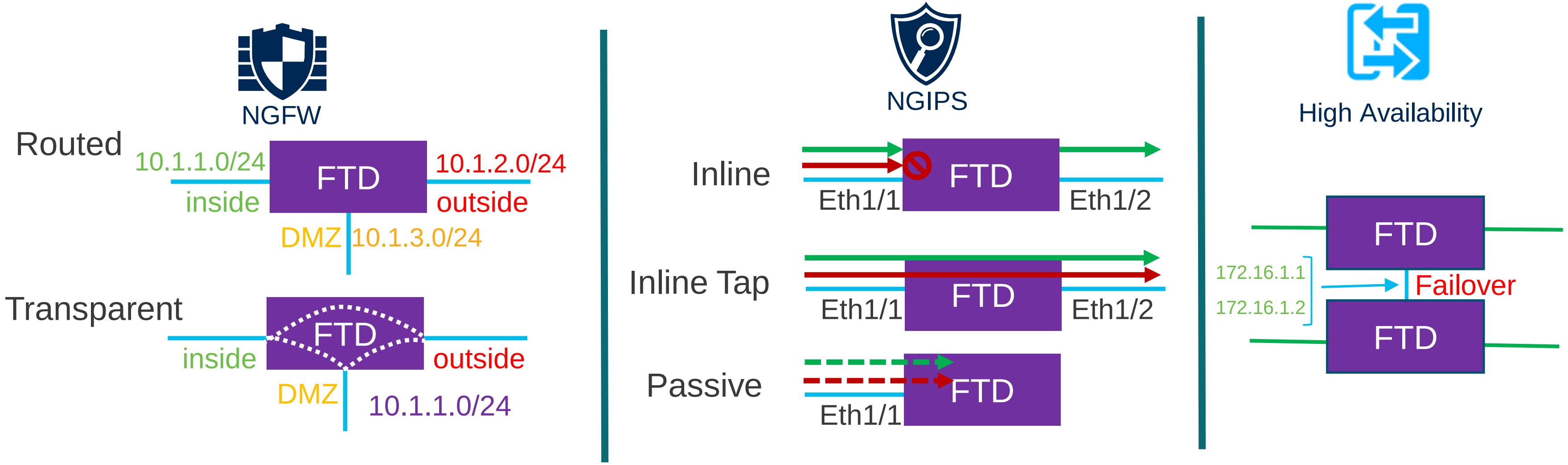
```
ip access-list extended NAT-ACL
 permit ip 10.20.20.0 0.0.0.255 any
```

```
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
```

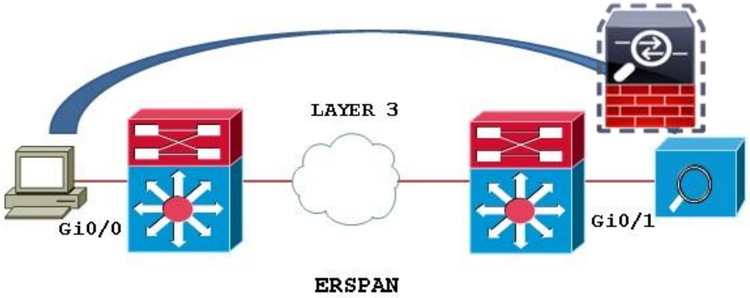
NGFWv Deployment Modes

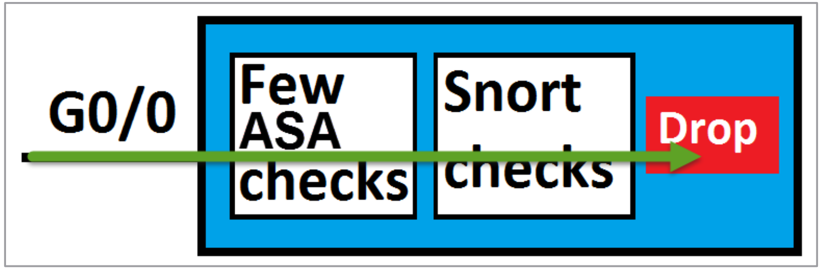
- FTD is both NGFW and NGIPS on different network interfaces
  - NGFW inherits operational modes from ASA and adds FirePOWER features
  - NGIPS operates as standalone FirePOWER with limited ASA data plane functionality



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)		

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

- 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

- UCSE
  http://www.cisco.com/c/en/us/products/servers-unified-computing/ucs-e-series-servers/white-paper-listing.html

Additional 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_Firepo
wer_Threat_Defense/s_5.html

Additional Resources

For Your Reference

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

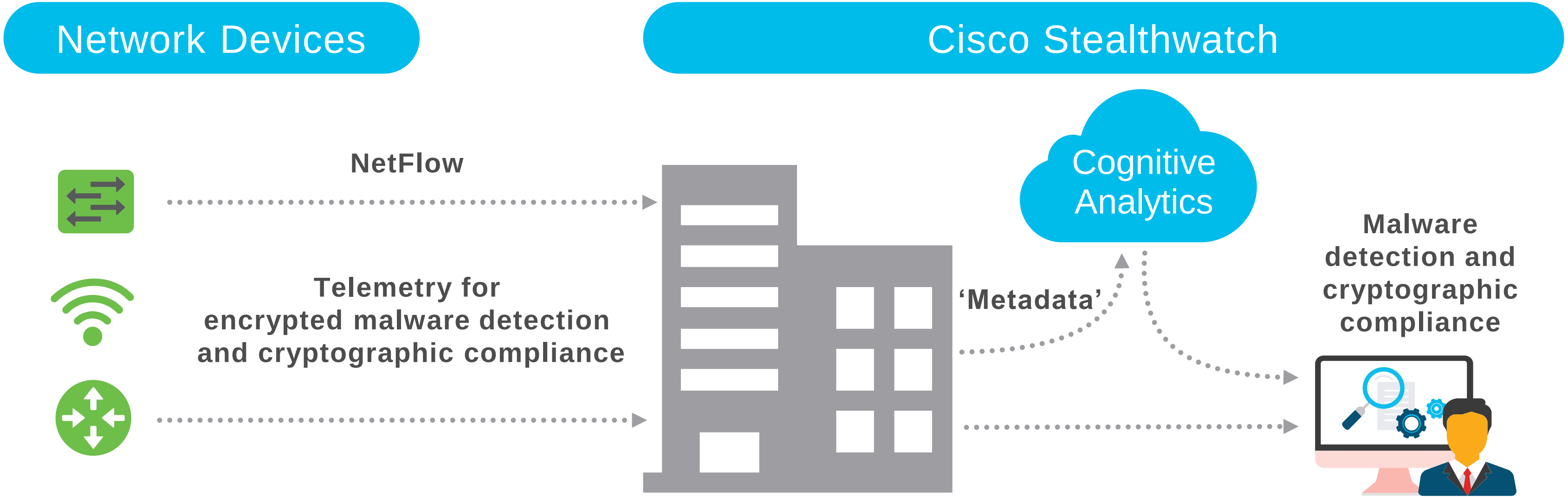
Space Communication protocol standard
https://supportforums.cisco.com/t5/firewalling/asa5520-keepalive-as-ip-protocol-105-scsp/td-p/1442798
http://www.scps.org/

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


Network Devices
Cisco Stealthwatch
NetFlow
Telemetry for encrypted malware detection and cryptographic compliance
Cognitive Analytics
'Metadata'
Malware detection and cryptographic compliance

Leveraged network	Faster investigation	Higher precision	Stronger protection
Enhanced NetFlow from Cisco's cat9k switches and routers	Enhanced analytics and machine learning	Global-to-local knowledge correlation	Continuous Enterprise-wide compliance

Encrypted Traffic Analytics – Benefits and Requirements

Benefits

Identifies malware in encrypted traffic

Crypto audit

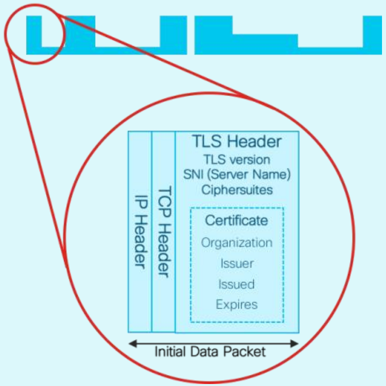
Requirements

- 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?

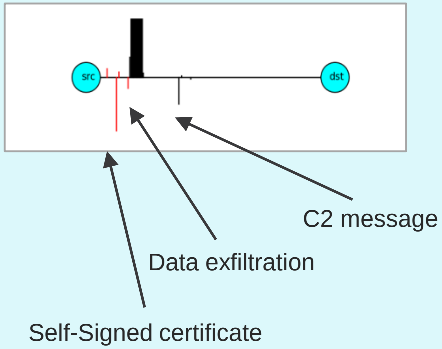
Initial Data Packet

Make the most of the unencrypted fields



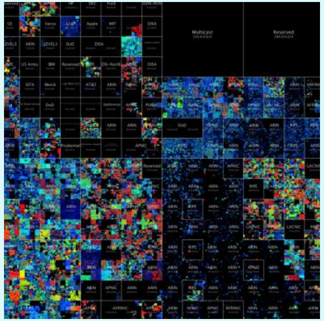
Sequence of Packet Lengths and Times

Identify the content type through the size and timing of packets



Threat Intelligence Map

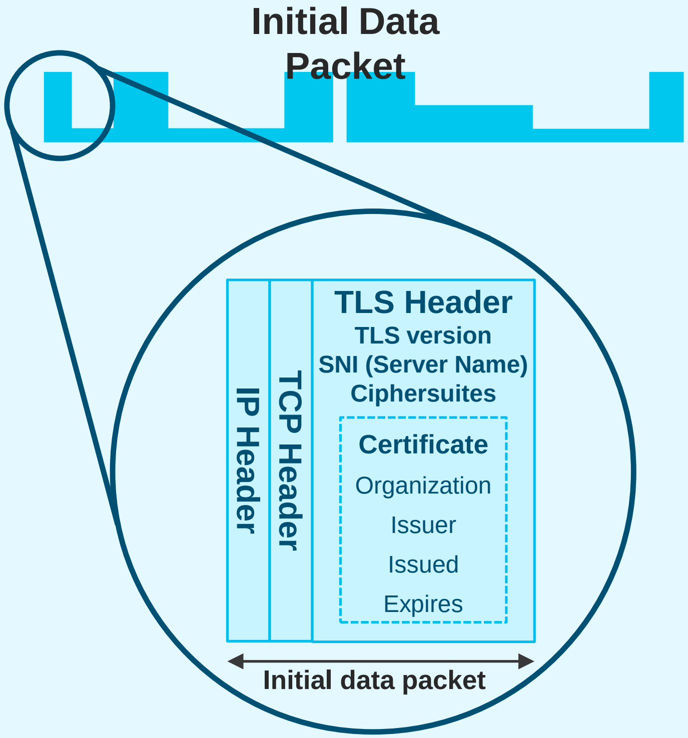
Who's who of the Internet's dark side



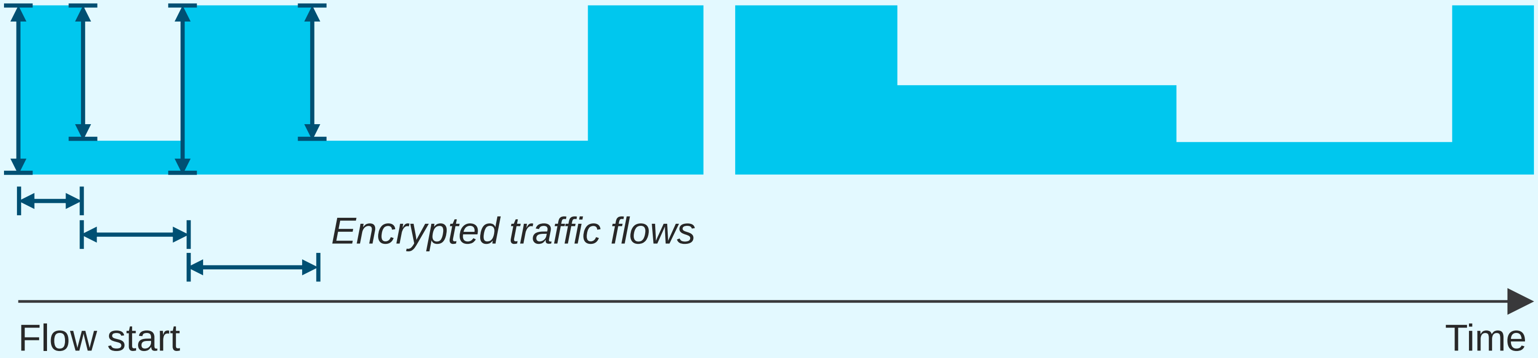
Broad behavioral information about the servers on the Internet.

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.



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

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	Cisco Umbrella Branch 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 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

ZBF

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

Snort IPS

- ISR 4K Series Routers
- ISR 1K 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

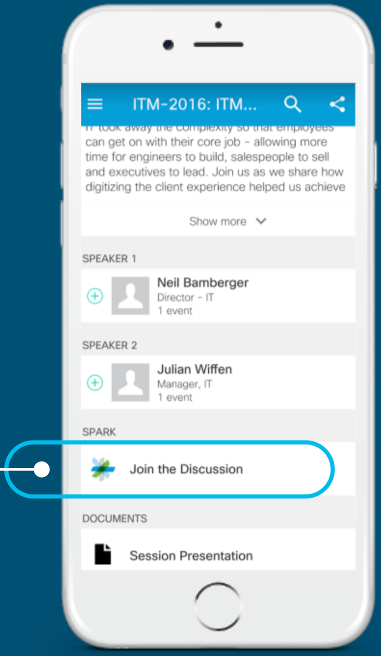
Cisco Spark

Questions?

Use Cisco Spark to communicate with the speaker after the session

How

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



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

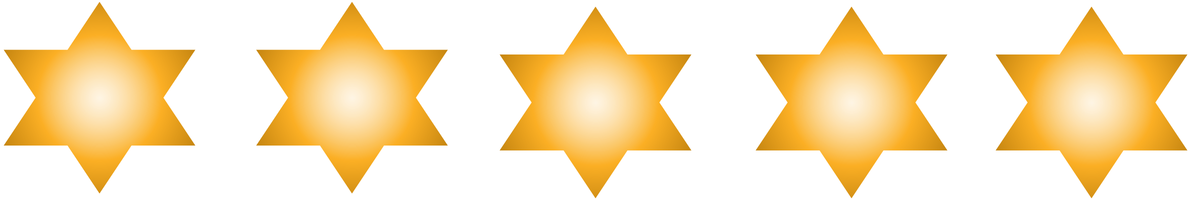
Cisco live!

Complete Your Online Session Evaluation

- Please complete your Online Session Evaluations after each session
- Complete 4 Session Evaluations & the Overall Conference Evaluation (available from Thursday) to receive your Cisco Live T-shirt
- All surveys can be completed via the Cisco Live Mobile App or the Communication Stations

Don’t forget: Cisco Live sessions will be available for viewing on-demand after the event at www.ciscolive.com/global/on-demand-library/.

Complete your online session evaluation



Continue Your Education

- Demos in the Cisco campus
- Walk-in Self-Paced Labs
- Tech Circle
- Meet the Engineer 1:1 meetings

Continue Your Education

Related sessions

BRKSEC-3446 Endpoint Security, Your Last Line of Defense
Aaron Woland 90 min Breakout 01/30/2018 Hall 8.0, Session Room 122 4:45 PM

BRKSEC-2890 AMP Threat Grid integrations with Web, Email and Endpoint Security
Moritz Wenz , Rene Straube , 120 min Breakout 01/30/2018 Hall 8.0, Session Room 129 2:15 PM

BRKSEC-2058 A Deep Dive into using the Firepower Manager
William Young , 90 min Breakout 01/30/2018 Hall 8.0, Session Room 101 4:45 PM

BRKSEC-3015 TLS Decryption on Cisco Security Devices
Tobias Mayer, 120 min Breakout 01/31/2018 Hall 8.0, Session Room 136 9:00 AM

BRKSEC-3014 Security Monitoring with Stealthwatch: The Detailed Walkthrough
Matthew Robertson, 120 min Breakout 01/31/2018 Hall 8.0, Session Room 122 11:30 AM

Continue Your Education

Related sessions

BRKSEC-2998 Cloud Managed Security & SD-WAN from Cisco Meraki
Greg Griessel, 90 min Technical Breakout 01/31/2018 Hall 8.0, Session Room 131 4:30 PM

BRKSEC-2339 How IoT Threat Defense is protecting the promise of the IoT
Mustafa Mustafa, 90 min Breakout 01/31/2018 Hall 8.0, Session Room 120 4:30 PM

BRKSEC-3035 Firepower Platform Deep Dive
Andrew Ossipov, 120 min Breakout 02/01/2018 Hall 8.0, Session Room 123 11:30 AM

BRKSEC-2980 Building an End-End Policy Driven Secure Hybrid Cloud DC Architecture
Brenden Buresh Technical 90 min Breakout 02/01/2018 Hall 8.0, Session Room 122 2:30 PM

BRKSEC-3557 Advanced Security Integration, Tips & Tricks
Aaron Woland Technical 120 min Breakout 02/02/2018 Hall 8.0, Session Room 112 09:00 AM

Q & A

Thank you

You're

iT

Cisco live!