cisco

Cisco live!

June 25-29, 2017 • Las Vegas, NV

Branch Router Security

Kureli Sankar

Kureli@cisco.com

Technical Marketing Engineer

CCIE Security #35505

BRKSEC-2342

Cisco Spark

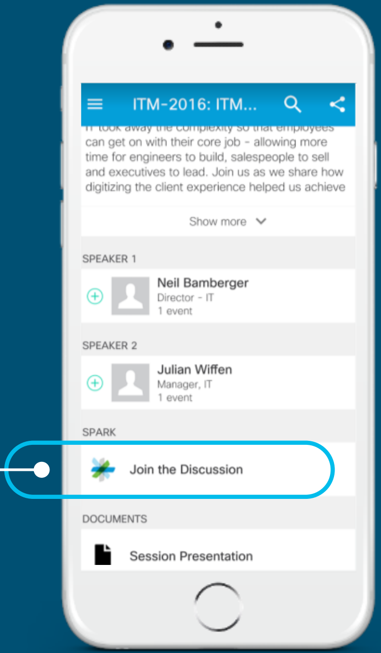
Questions?

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

Cisco Spark spaces will be available until July 3, 2017.



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/clus17/#BRKSEC-2342

Agenda

- **Zone Based Firewall**
- Snort IPS
- Cisco Umbrella (OpenDNS)
- Firepower
- Stealthwatch Learning Network License (SLNL)
- Cloud Web Security (CWS)

Branch Router Security Options

Options available on the ISR 4000 series

ZBFW · Snort IPS · Cisco Umbrella · Firepower · SLNL · CWS

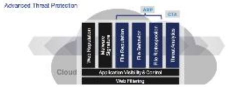
Cisco Trustworthy Systems Levels Enterprise Routing

Protects the Network

SNORT®

Cisco Umbrella Branch

CWS



Firepower

Intrusion Prevention
(Subscription)
Firepower Management Center
Advanced Malware Protection
(Subscription)
WWW
URL Filtering
(Subscription)
Application Visibility & Control
Built-in Network Profiling
Identity-Policy Control & VPN

Stealthwatch Learning Network License

TALOS

ISE

Branch

ISR

Manager

Packet Analysis

Platform Integrity

- Secure Boot
- Image Signing
- Counterfeit Protections
- Hardware Trust Anchor
- Runtime Defenses
- OS Validation
- Modern Crypto
- Secure Device Onboarding

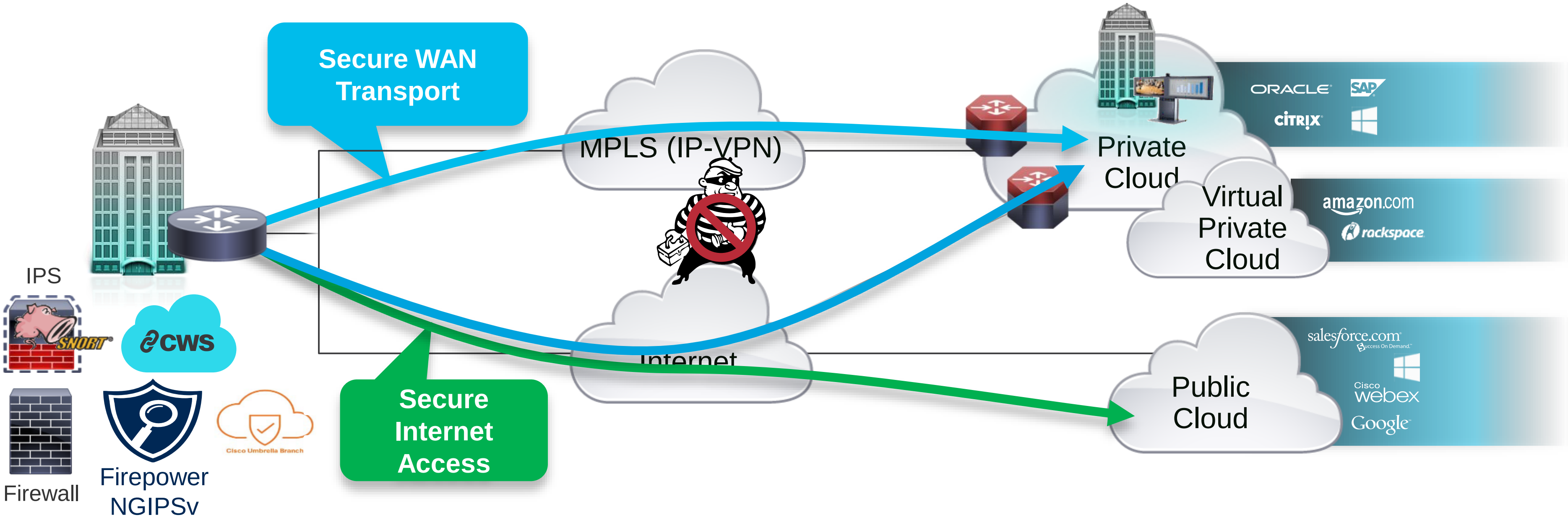
Security Culture

- Supply Chain Management
- Open Source Registration
- Security Training
- Threat Modeling
- Product Security Baseline
- PSIRT Advisories

Learn more: BRKARC-1010 “Protecting the Device: Cisco Trustworthy Systems & Embedded Security”

Secure Connectivity

Securing the network and users



Two areas of concern

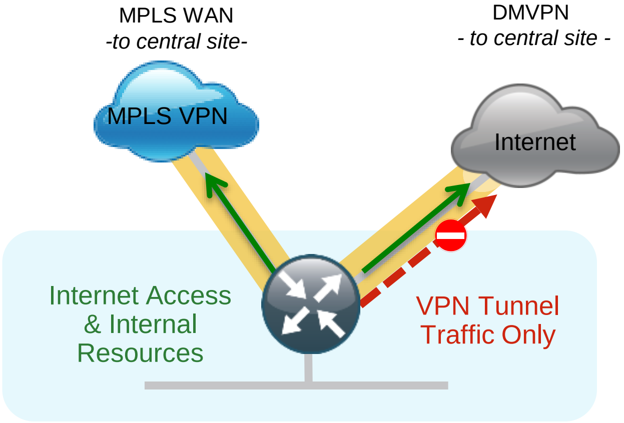
1. **Protecting the network from outside threats with data privacy over provider networks**
2. **Protecting user access to Public Cloud and Internet services; malware, privacy, phishing,…**

Central versus Direct Internet Access

Central Internet Access

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

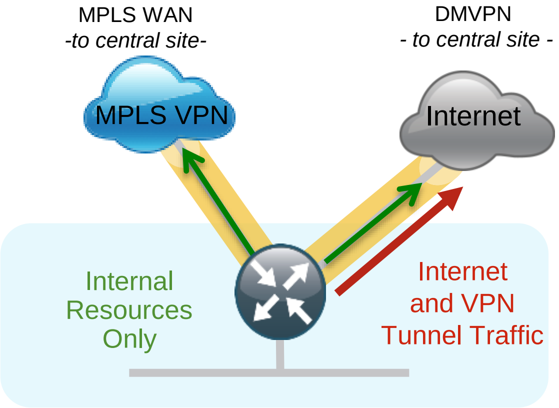
```
RS230#sh ip route
Gateway of last resort is 10.10.34.1 to network 0.0.0.0
D*EX  0.0.0.0/0 [170/2561280] via 10.4.34.1, 1w1d, Tunnel10
```



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

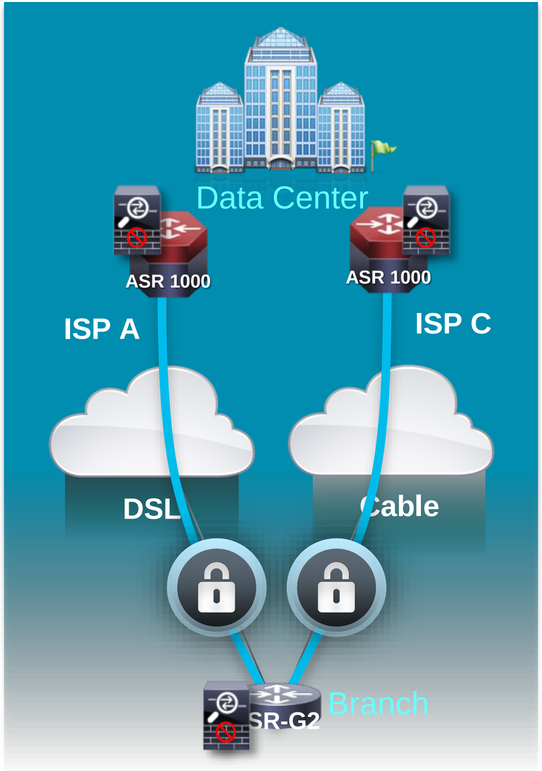
- Provide local Internet access for Guest users
- Provide local Internet access for Employees

Challenges

- Management of many Internet Edges
- Security policy enforcement

Securing DIA – Zone Based Firewall

- Control the Perimeter:
  - External and internal protection: internal network is no longer trusted
  - Protocol anomaly detection and stateful inspection
- Communicate Securely:
  - Call flow awareness (SIP, SCCP, H323)
  - Prevent DoS attacks
- Flexible:
  - Split Tunnel-Branch/Remote Office/Store/Clinic
  - Network segmentation and addresses regulatory compliances
- Integrated:
  - No need for additional devices, expenses and power
  - Works with other Cisco Services: Firepower, Umbrella Branch, CWS and Snort IPS



Zone Based Firewall

- Custom zone
- default zone
- “default” security zone for all INSIDE interfaces
- Default Zone in IOS-XE, first support on ISR-G2 with 15.6(1)T.
- Self Zone

Zone Based Firewall

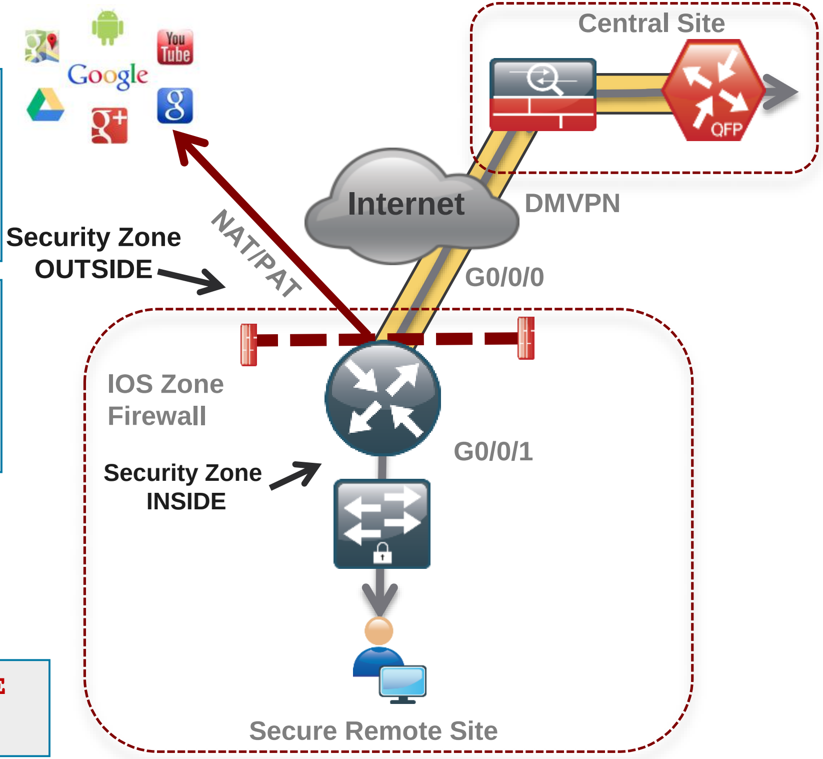
```
zone security INSIDE
zone security OUTSIDE
```

```
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

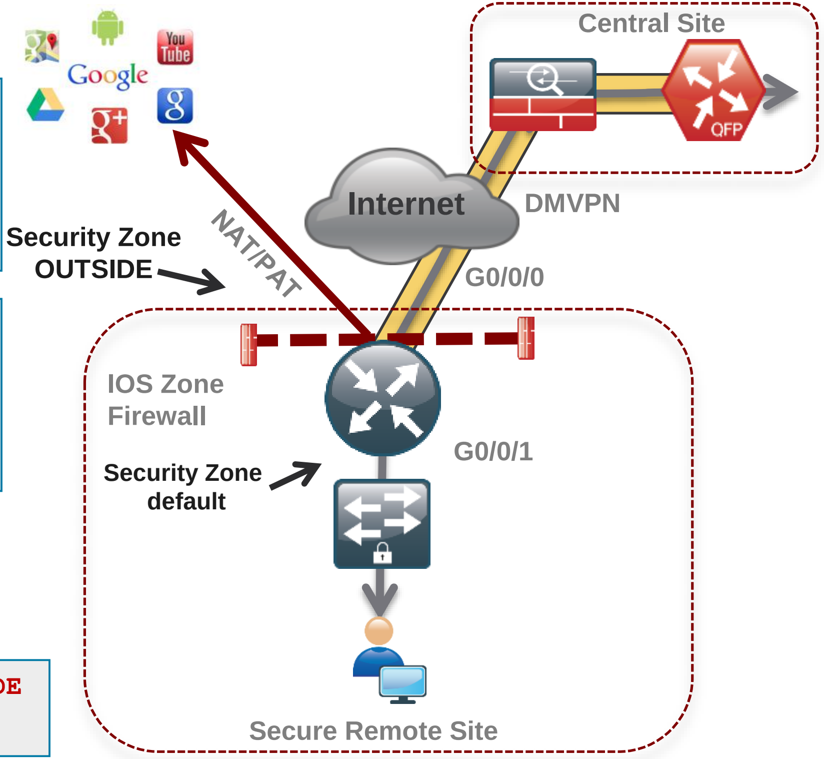
```
zone security default
zone security OUTSIDE
```

```
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 inbound - DMVPN tunnel inbound to the router itself

```
ip access-list extended ACL-RTR-IN
 permit udp any any eq non500-isakmp
 permit udp any any eq isakmp
 permit icmp any any echo
 permit icmp any 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 any 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

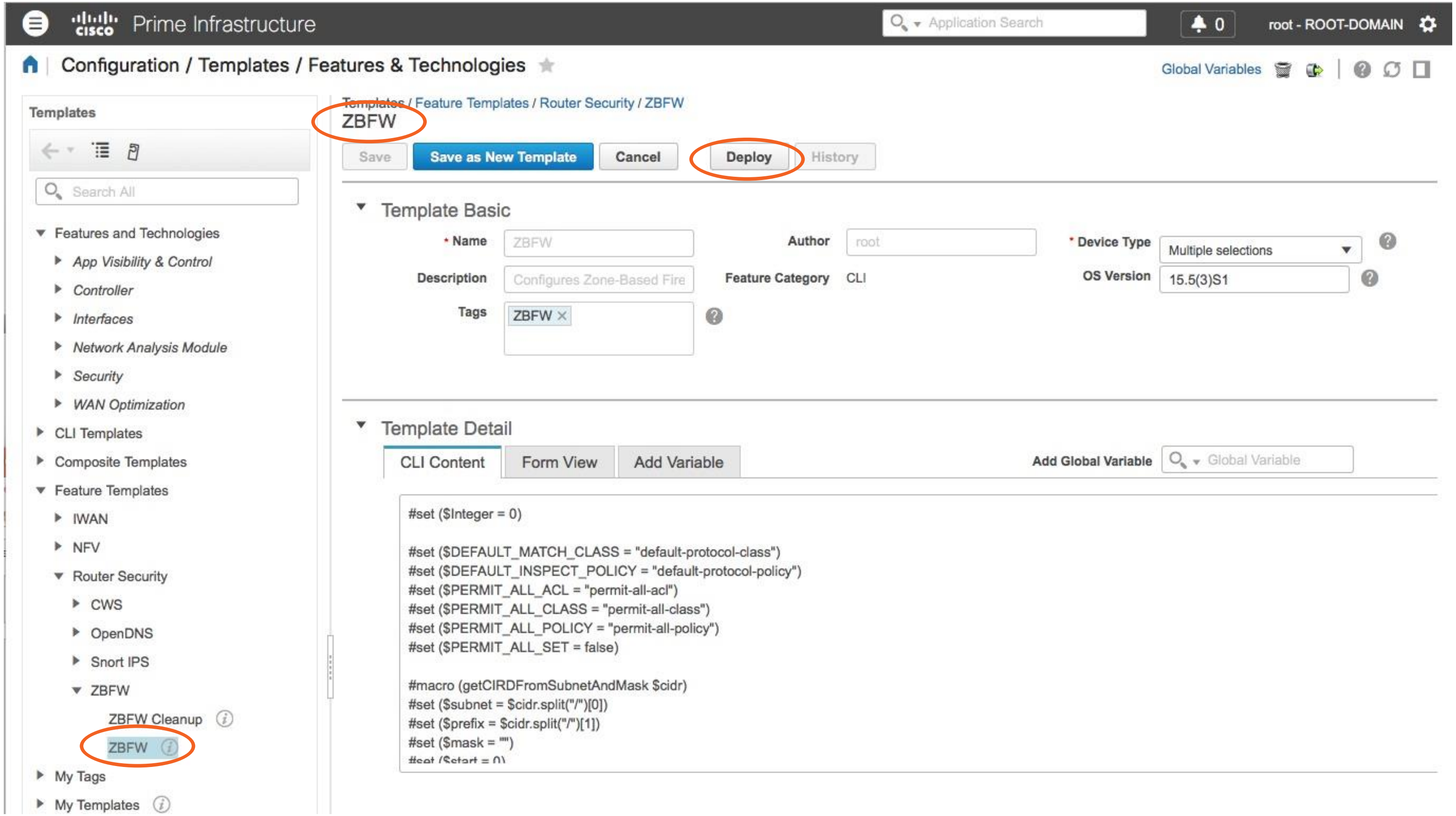
```
ip access-list extended ACL-RTR-OUT
permit udp any any eq non500-isakmp
permit udp any any eq isakmp
permit icmp any any
```

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

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)



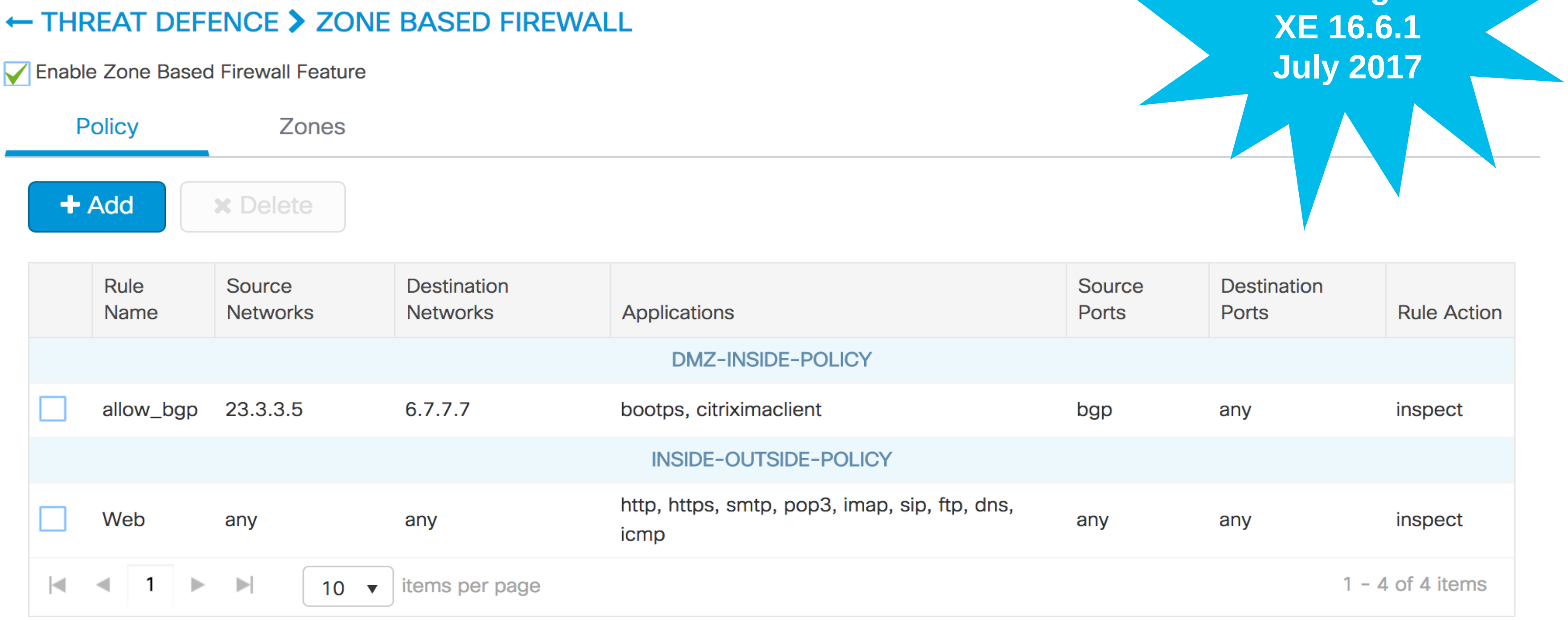
ZBFW

- 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

Coming in
XE 16.6.1
July 2017



← THREAT DEFENCE > ZONE BASED FIREWALL

☑ Enable Zone Based Firewall Feature

	Rule Name	Source Networks	Destination Networks	Applications	Source Ports	Destination Ports	Rule Action
DMZ-INSIDE-POLICY							
□	allow_bgp	23.3.3.5	6.7.7.7	bootps, citriximaclient	bgp	any	inspect
INSIDE-OUTSIDE-POLICY							
□	Web	any	any	http, https, smtp, pop3, imap, sip, ftp, dns, icmp	any	any	inspect

|◀ ◀ 1 ▶ ▶| 10 ▾ items per page 1 – 4 of 4 items

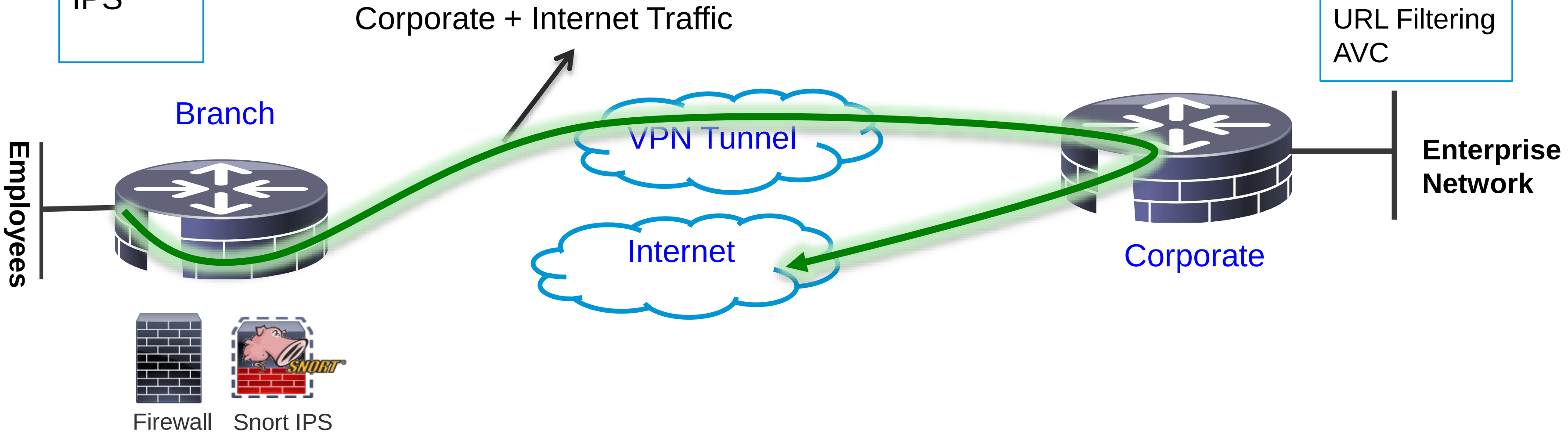
Agenda

- Zone Based Firewall
- **Snort IPS**
- Cisco Umbrella (OpenDNS)
- Firepower
- Stealthwatch Learning Network License (SLNL)
- Cloud Web Security (CWS)

Use Case: Meet PCI Compliance

MVP
FW
IPS

NGFW
NGIPS
AMP
URL Filtering
AVC



Examples:
Retail stores
Hospitals / Pharmacies

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

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
- IWAN – Intelligent WAN

Snort IPS

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

Now Orderable!

Snort

Cisco ISR 4000 Series

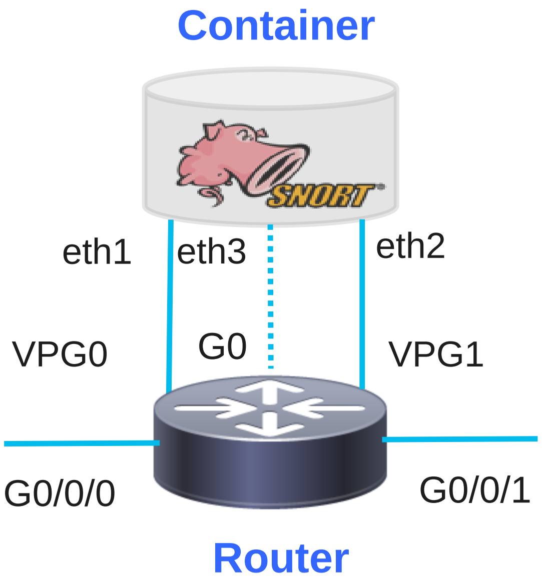
SEC-K9 on the router
4 GB Memory Upgrade
XE 3.16.1 and above

Snort - Community vs Subscriber Rule Set

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

	Community Rule Set	**Subscriber Rule Set**
Pricing	free	paid
Number of rules	3000+	30,000+
Coverage in advance of exploits	No	Yes
Signature availability	30 days later	Fastest access to Talos signature updates

Snort IPS Configuration –Virtual Service Networking



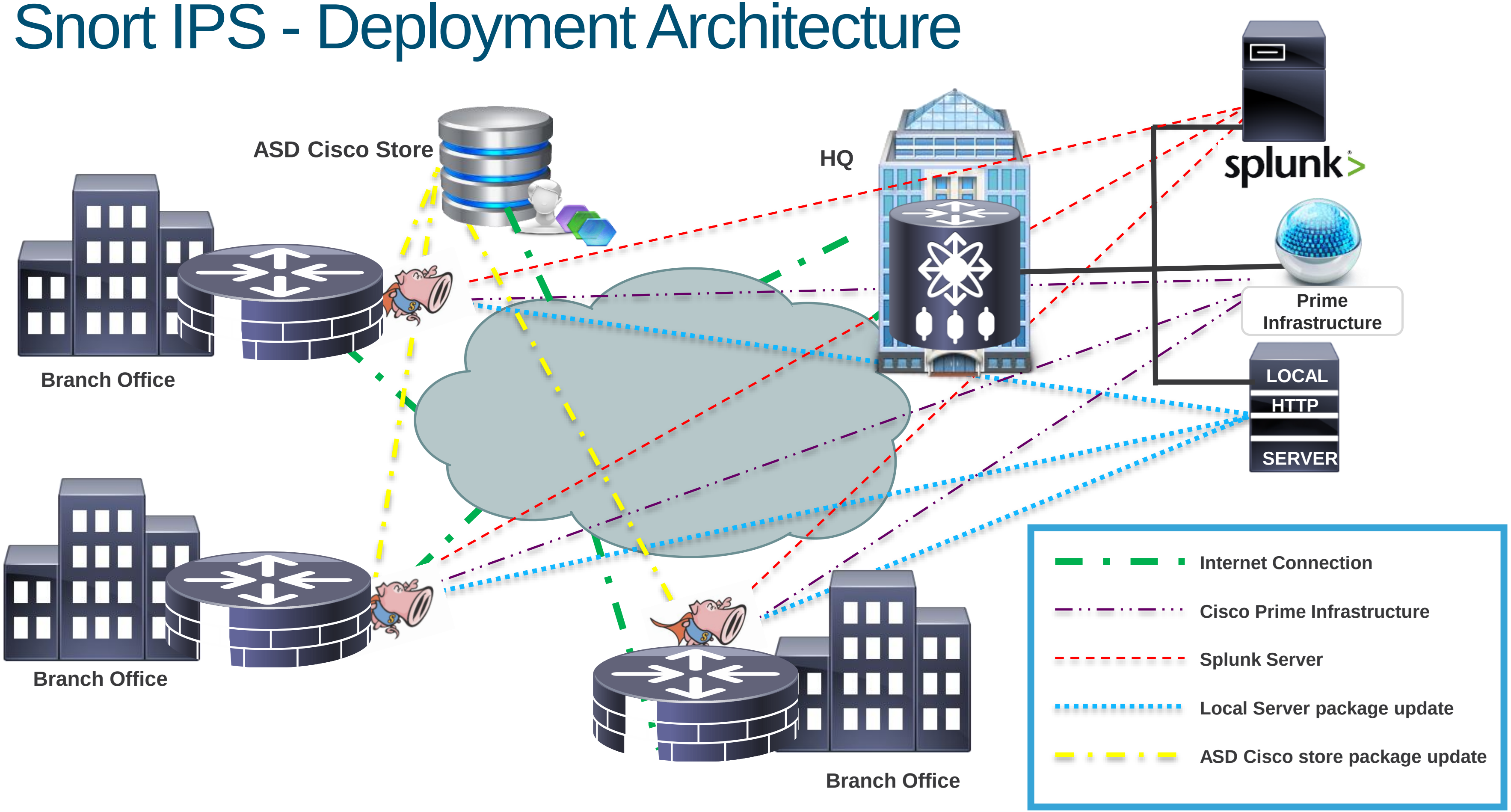
- VPGs to communicate between container and data plane
- VPG1 <==> eth2 (data plane)

- VPG0 <==> eth1 (management)

  [OR]

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

Snort IPS - Deployment Architecture



Snort IPS – Configuration

Step 6 – Whitelisting (Optional)

```
Router(config)#utd whitelist
Router(config-utd-whitelist)#signature id 15 comment test1
Router(config-utd-whitelist)#signature id 12 comment test2
```

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
```

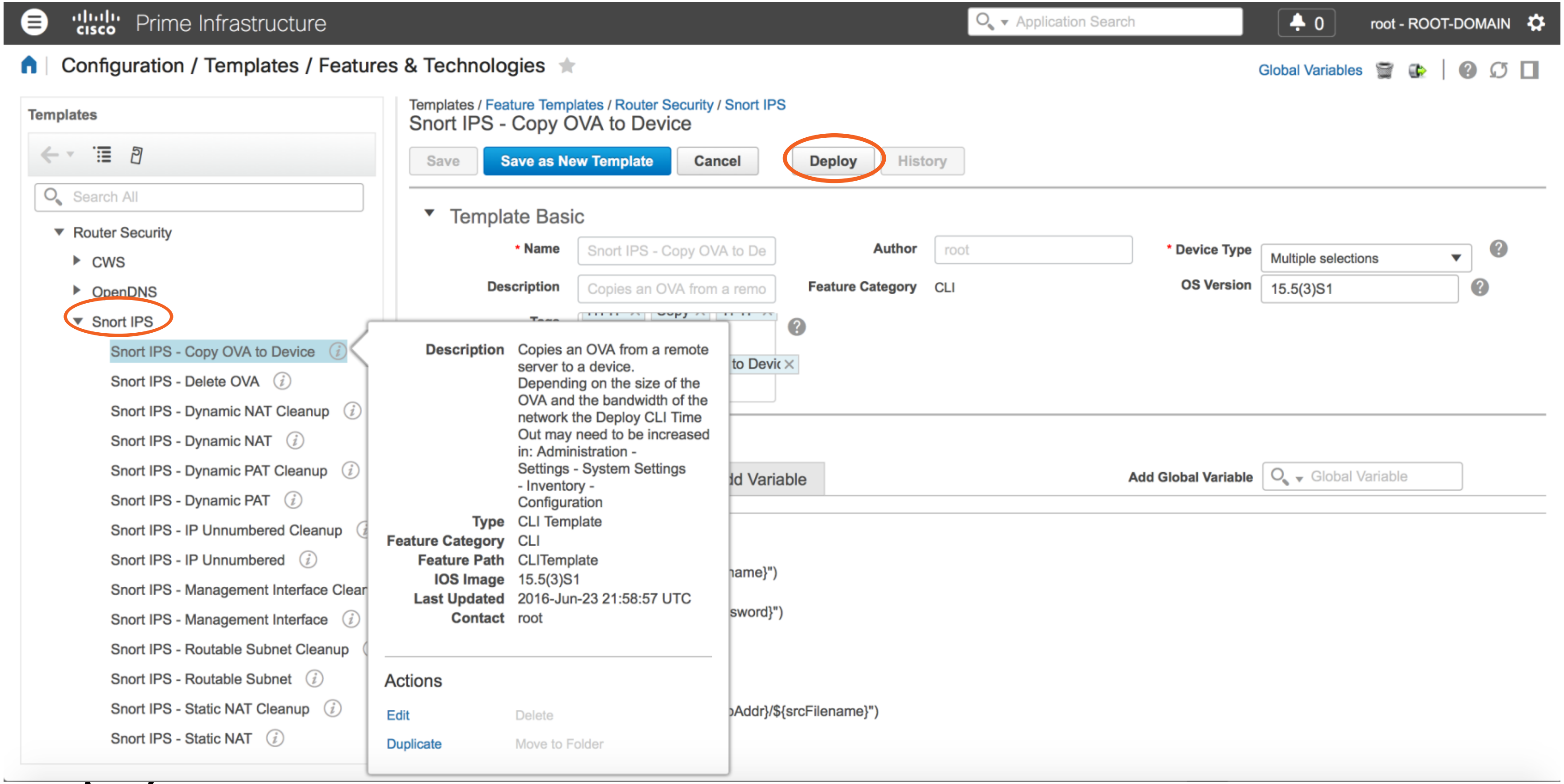
Step.5 Enabling UTD (data plane)

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

Step.6 Whitelisting (optional)

```
utd whitelist
  signature id 12 comment test1
  signature id 15 comment test2
```

Snort IPS – Provisioning (Prime Infrastructure 3.1 and above)



Templates / Feature Templates / Router Security / Snort IPS

Snort IPS - Copy OVA to Device

- 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

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}")

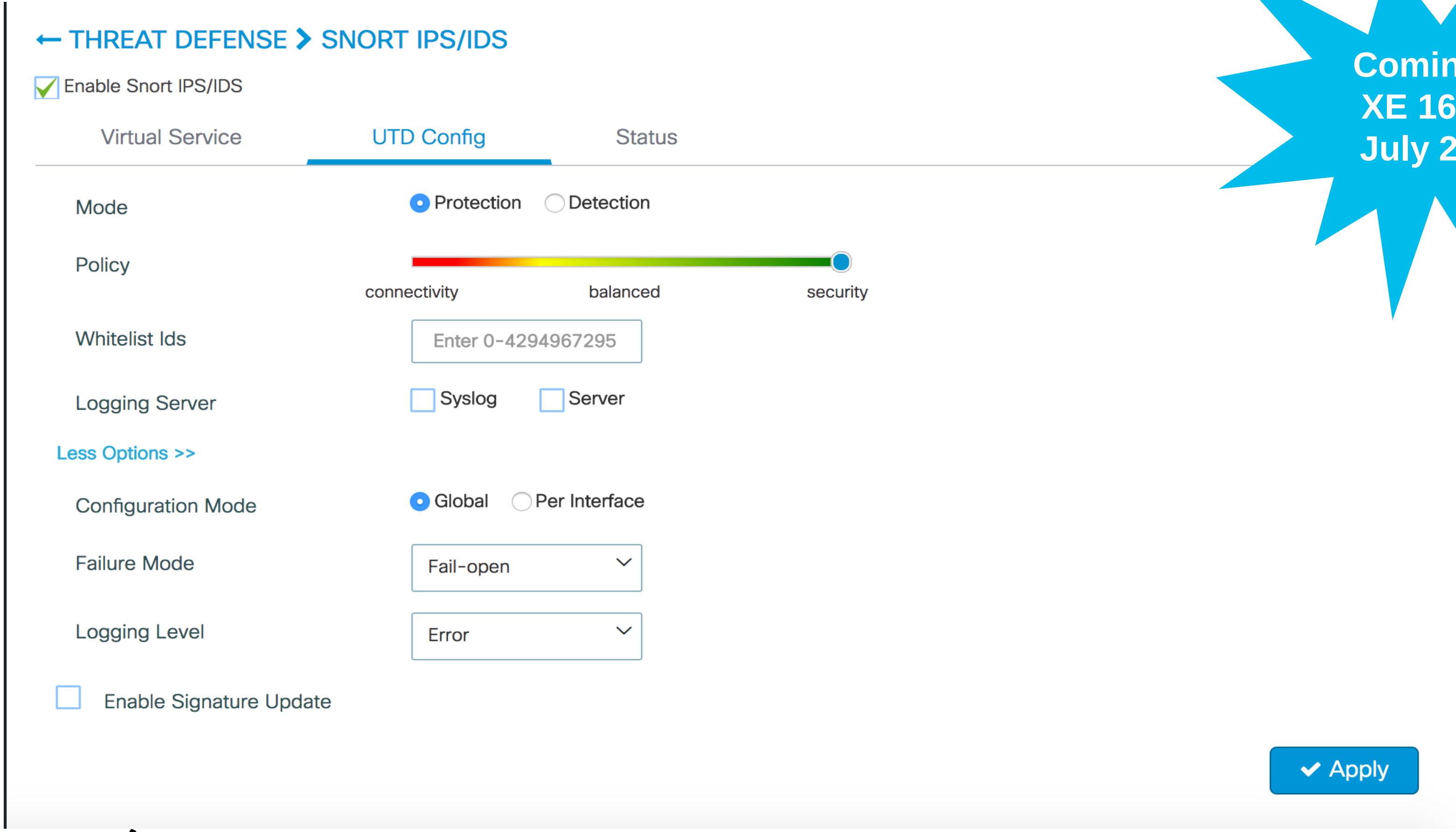
Addr}/${srcFilename}")

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



← THREAT DEFENSE › SNORT IPS/IDS

☑ Enable Snort IPS/IDS

Virtual Service | UTD Config | Status

Mode: ● Protection ○ Detection

Policy: connectivity — balanced — security (set to security)

Whitelist Ids: Enter 0-4294967295

Logging Server: □ Syslog □ Server

Less Options >>

Configuration Mode: ● Global ○ Per Interface

Failure Mode: Fail-open

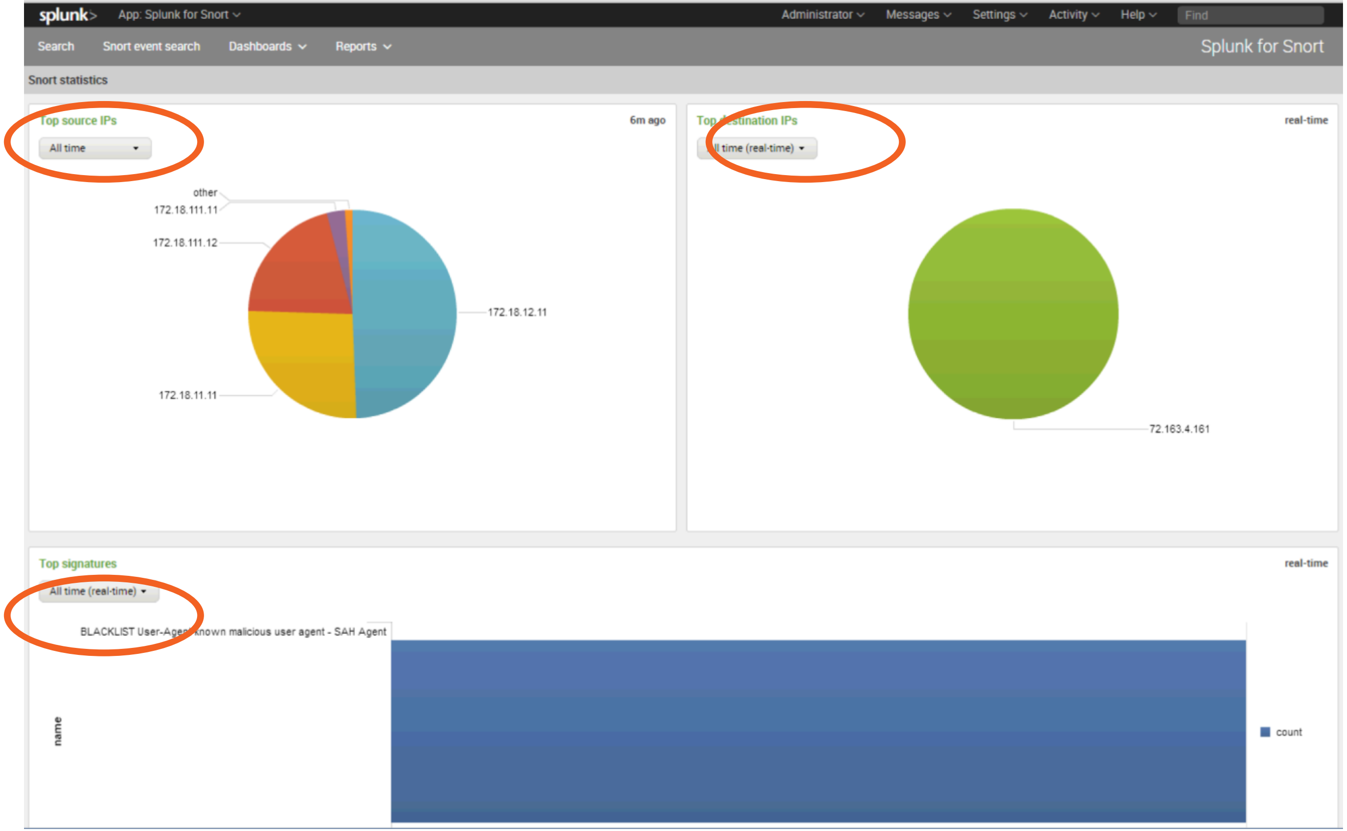
Logging Level: Error

□ Enable Signature Update

✓ Apply

Coming in XE 16.6.1 July 2017

Snort IPS – Monitoring (Splunk for Snort)



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

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

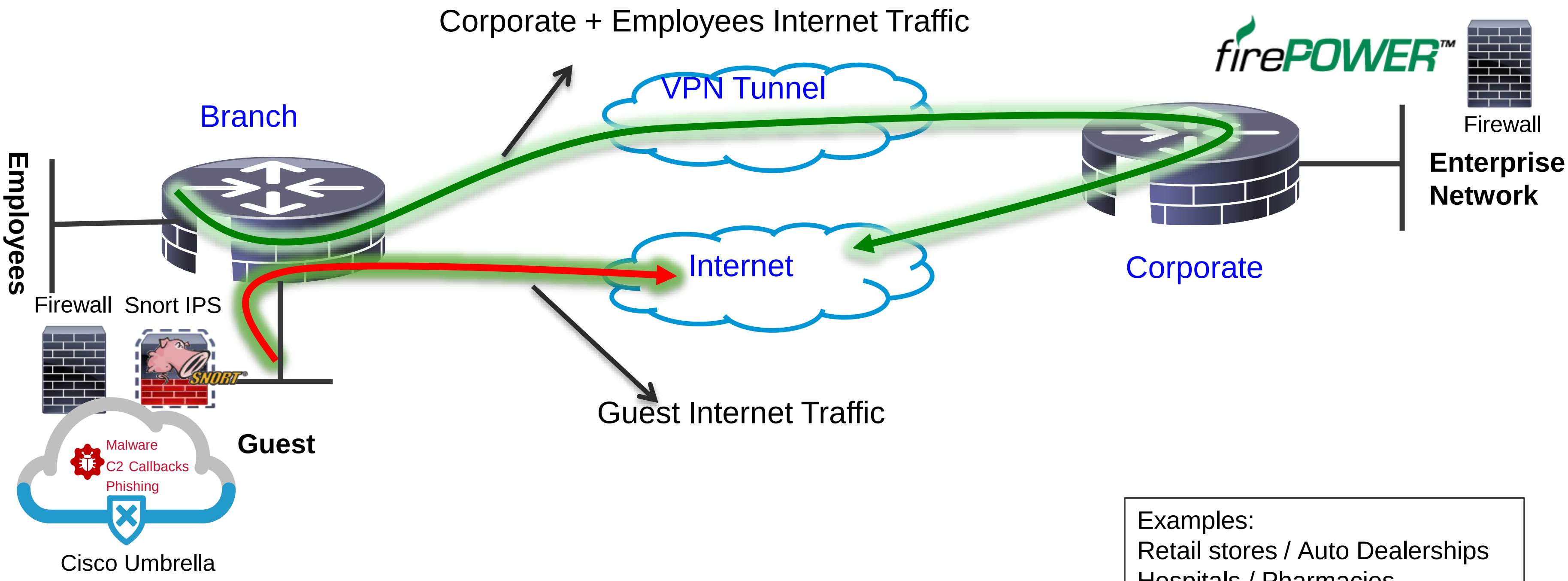
Data Sheet
http://www.cisco.com/c/en/us/products/collateral/security/router-security/datasheet-c78-736114.html

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

Agenda

- Zone Based Firewall
- Snort IPS
- **Cisco Umbrella (OpenDNS)**
- Firepower
- Stealthwatch Learning Network License (SLNL)
- Cloud Web Security (CWS)

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

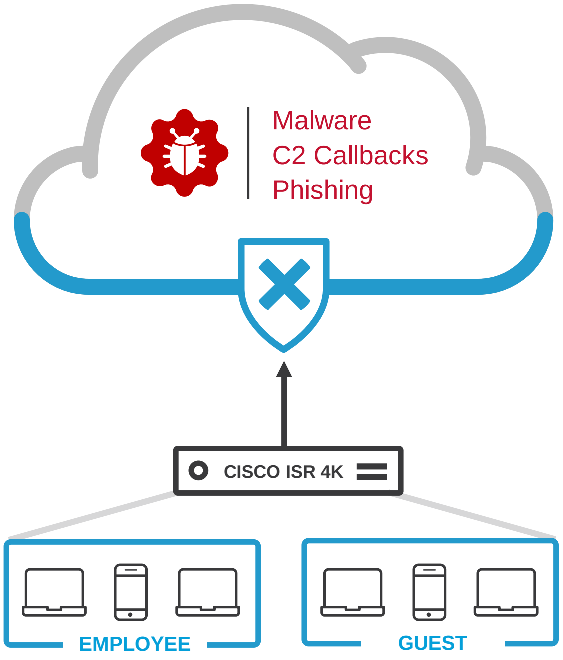
Examples:
Retail stores / Auto Dealerships
Hospitals / Pharmacies
Financials
Schools / Universities

Cisco Umbrella

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)
- DIA – Direct Internet Access

Cisco Umbrella



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

Protect against malware, phishing and C2 callbacks

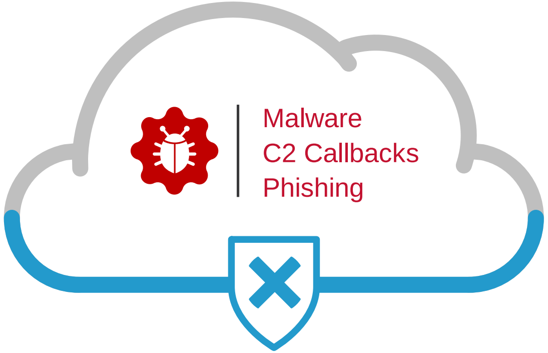
Enable domain filtering

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

Review deployment and research incidents using reports

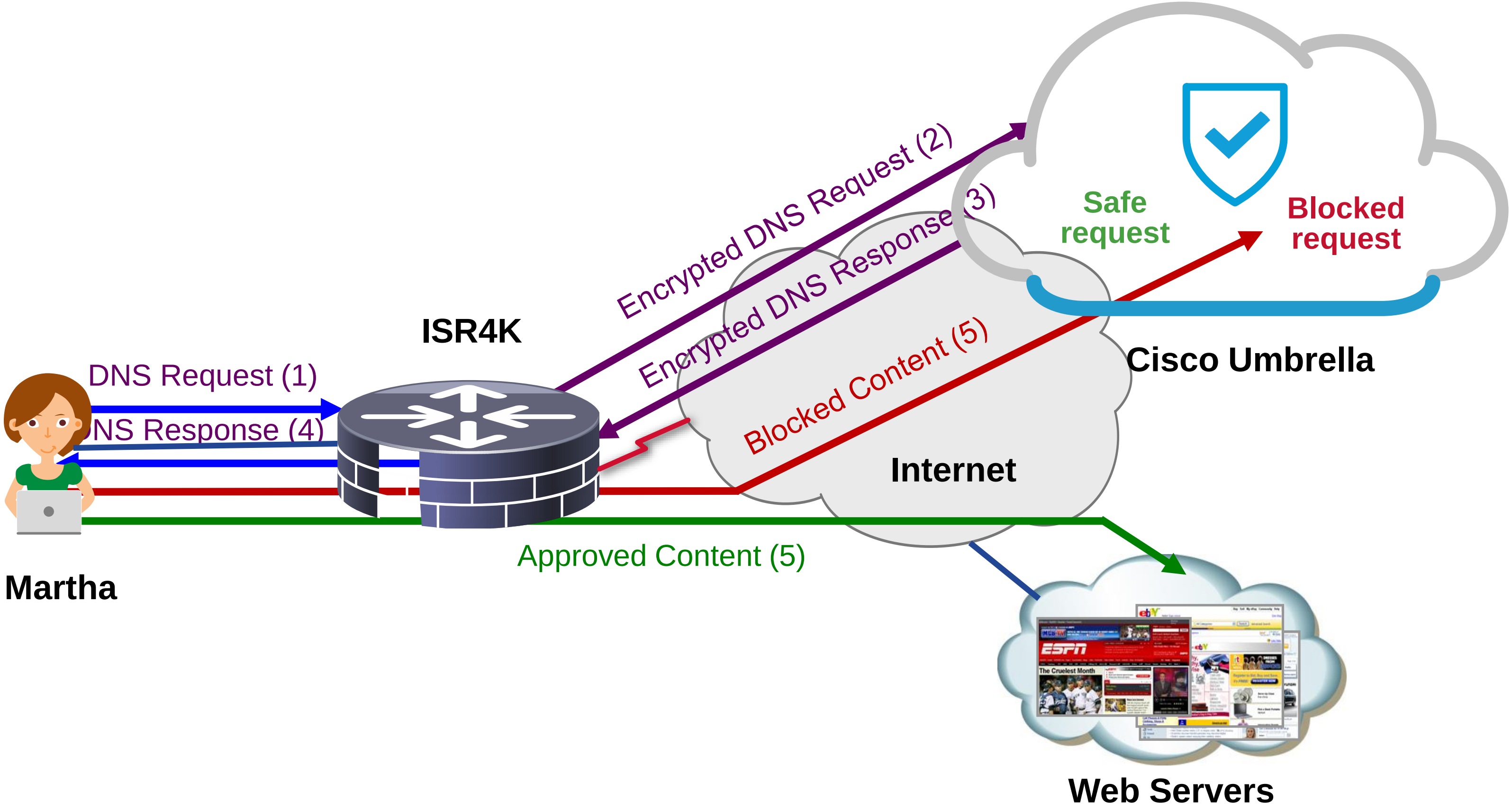
Cisco Umbrella – Fast & Easy Deployment

1. Cisco Umbrella provisioning
   - Get token ID
   - Cloud Portal Login
2. Subscription is per site per device
3. Configure ISR Connector (can be provisioned via Cisco Prime or CLI)
4. ISR registers and obtains device IDs
   - ISR encrypts and redirects DNS packets to Cisco Umbrella cloud
   - Security policies are applied

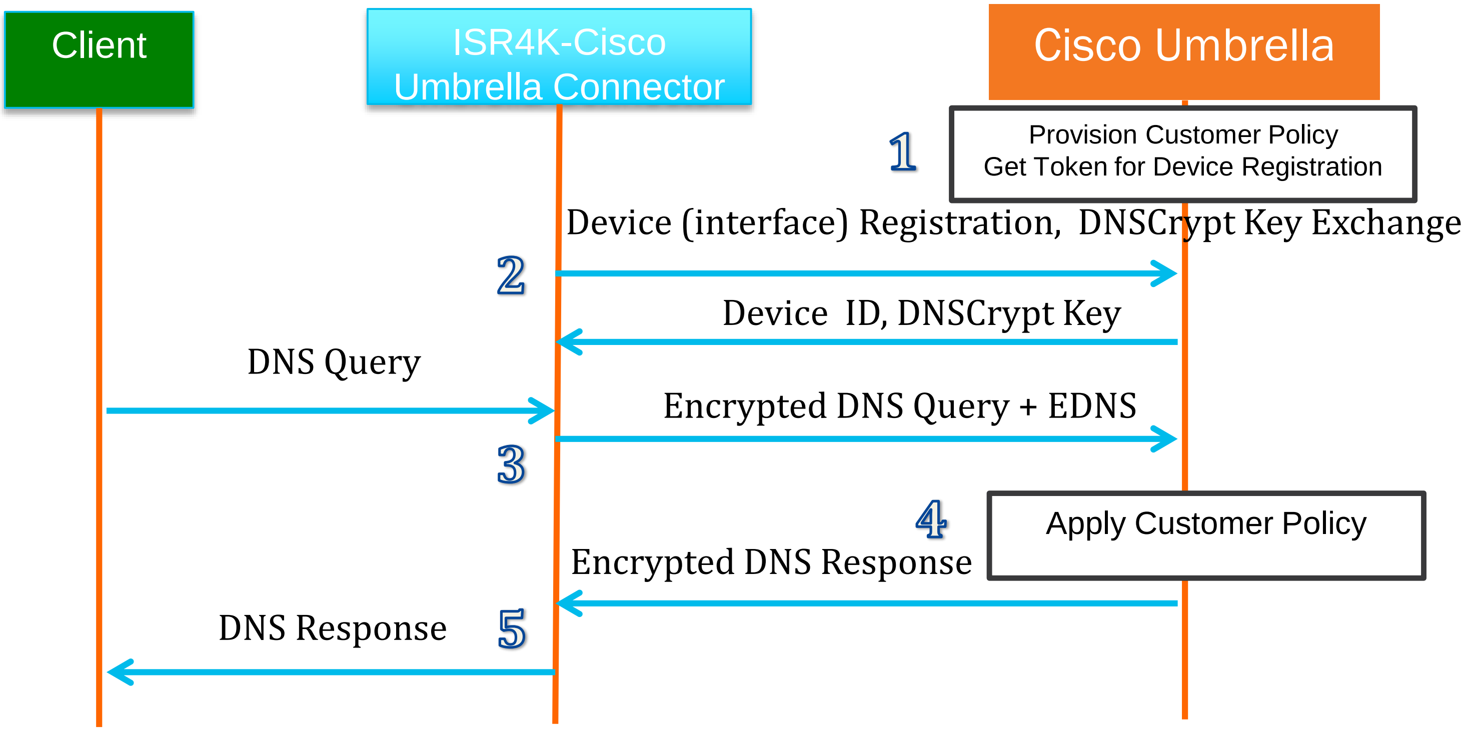


SEC-K9 License is required
XE 16.3 and above

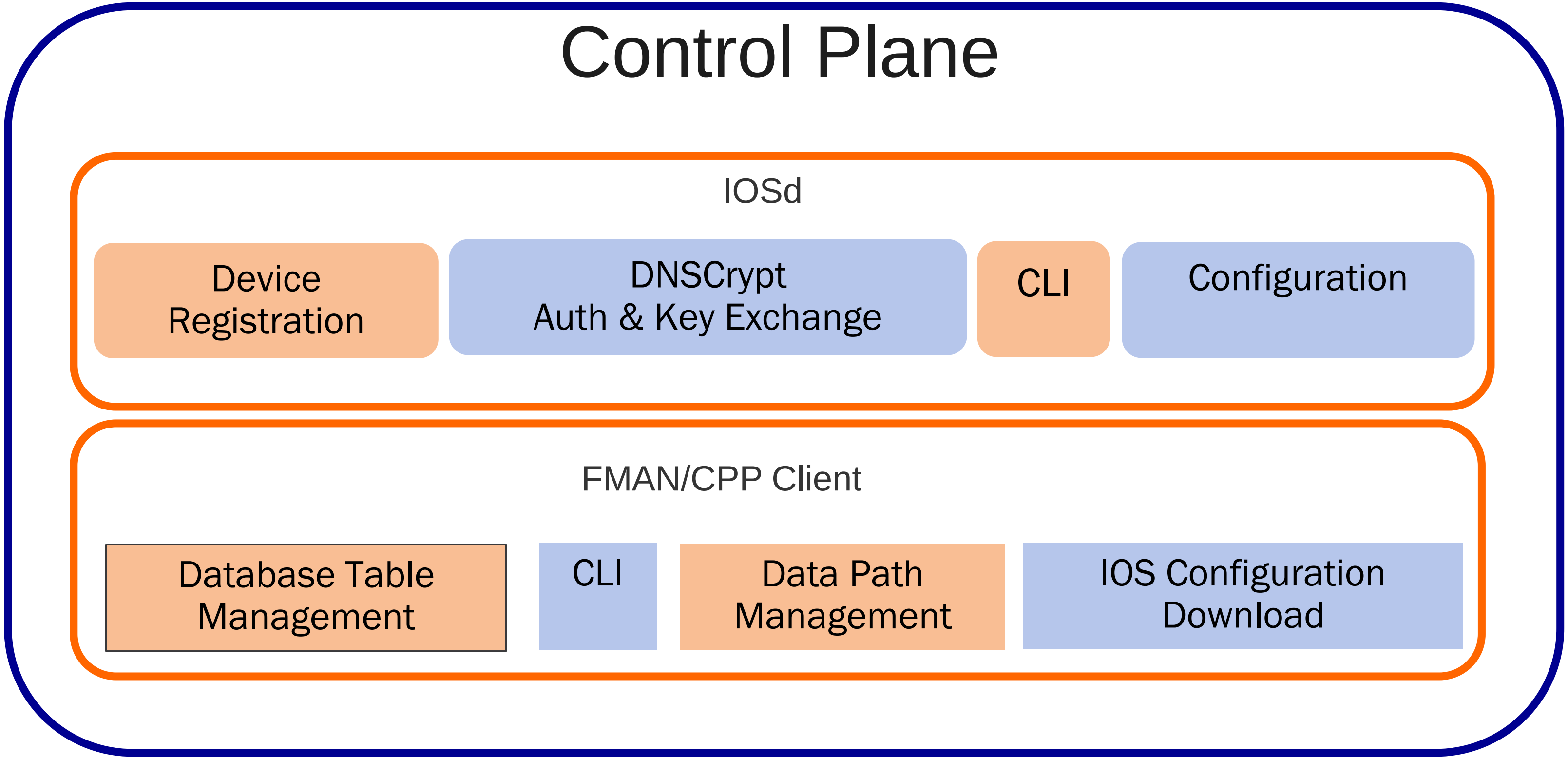
Cisco Umbrella - Solution Overview



Cisco Umbrella - Packet Flow with DNSCrypt


Client
ISR4K-Cisco Umbrella Connector
Cisco Umbrella
1
Provision Customer Policy
Get Token for Device Registration
Device (interface) Registration, DNSCrypt Key Exchange
2
Device ID, DNSCrypt Key
DNS Query
Encrypted DNS Query + EDNS
3
4
Apply Customer Policy
Encrypted DNS Response
DNS Response
5

Cisco Umbrella – Software Architecture



Control Plane

IOSd

Device Registration

DNSCrypt
Auth & Key Exchange

CLI

Configuration

FMAN/CPP Client

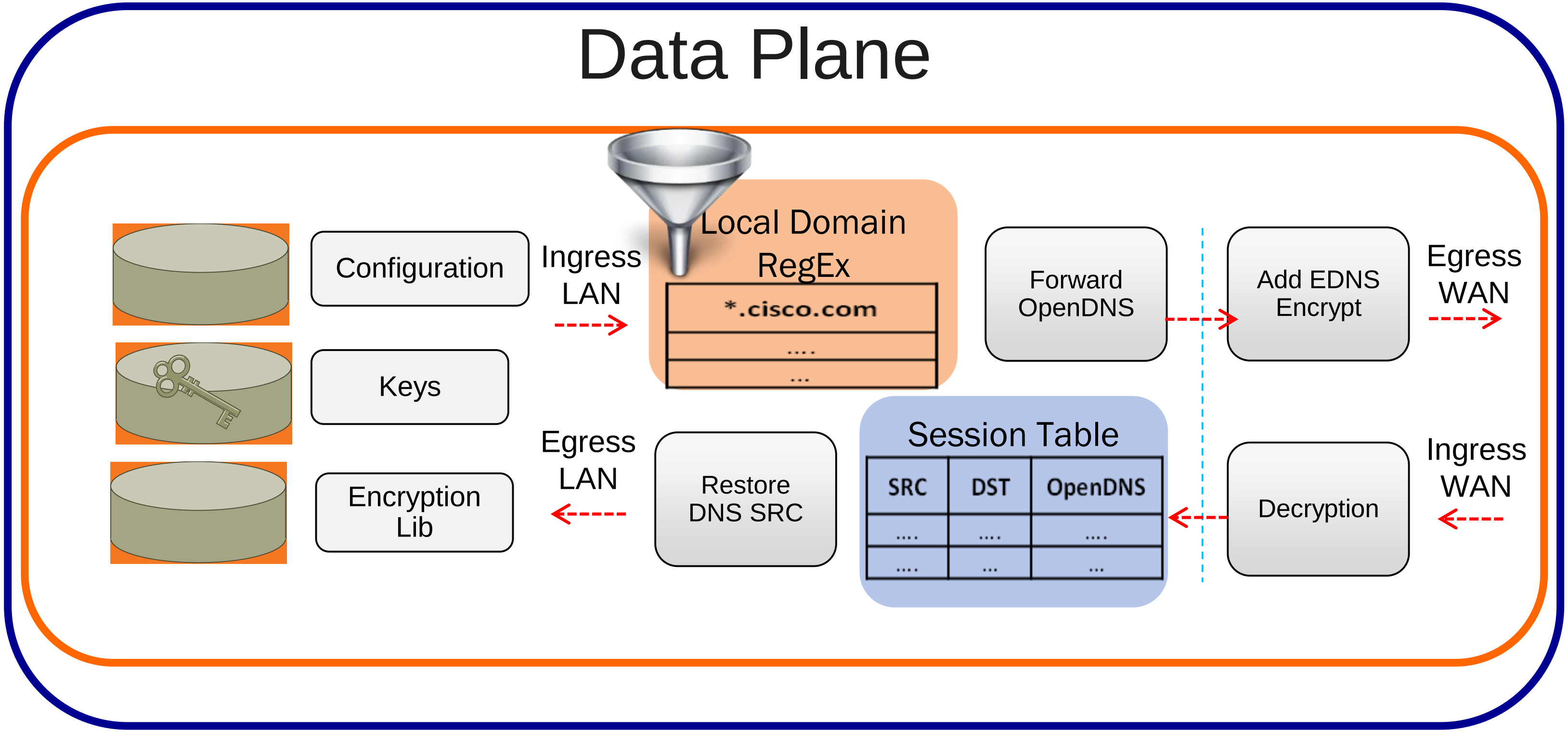
Database Table Management

CLI

Data Path Management

IOS Configuration Download

Cisco Umbrella – Software Architecture



Data Plane

Configuration

Keys

Encryption Lib

Ingress LAN

Local Domain RegEx

*.cisco.com
….
…

Forward OpenDNS

Add EDNS Encrypt

Egress WAN

Egress LAN

Restore DNS SRC

Session Table

SRC	DST	OpenDNS
….	….	….
….	…	…

Decryption

Ingress WAN

Cisco Umbrella – Configuration

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

```
Router(config-if)#interface g0/0/0
Router(config-if)#opendns out


Router(config-if)#interface g0/0/1
Router(config-if)#opendns in Guest
```

https://www.digicert.com/CACerts/DigiCertSecureServerCA.crt - Certificate URL

“opendns” command will be 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
….
8FAB492E 9D3B9334 281F78CE 94EAC7BD
D3C96D1C DE5C32F3
quit
```

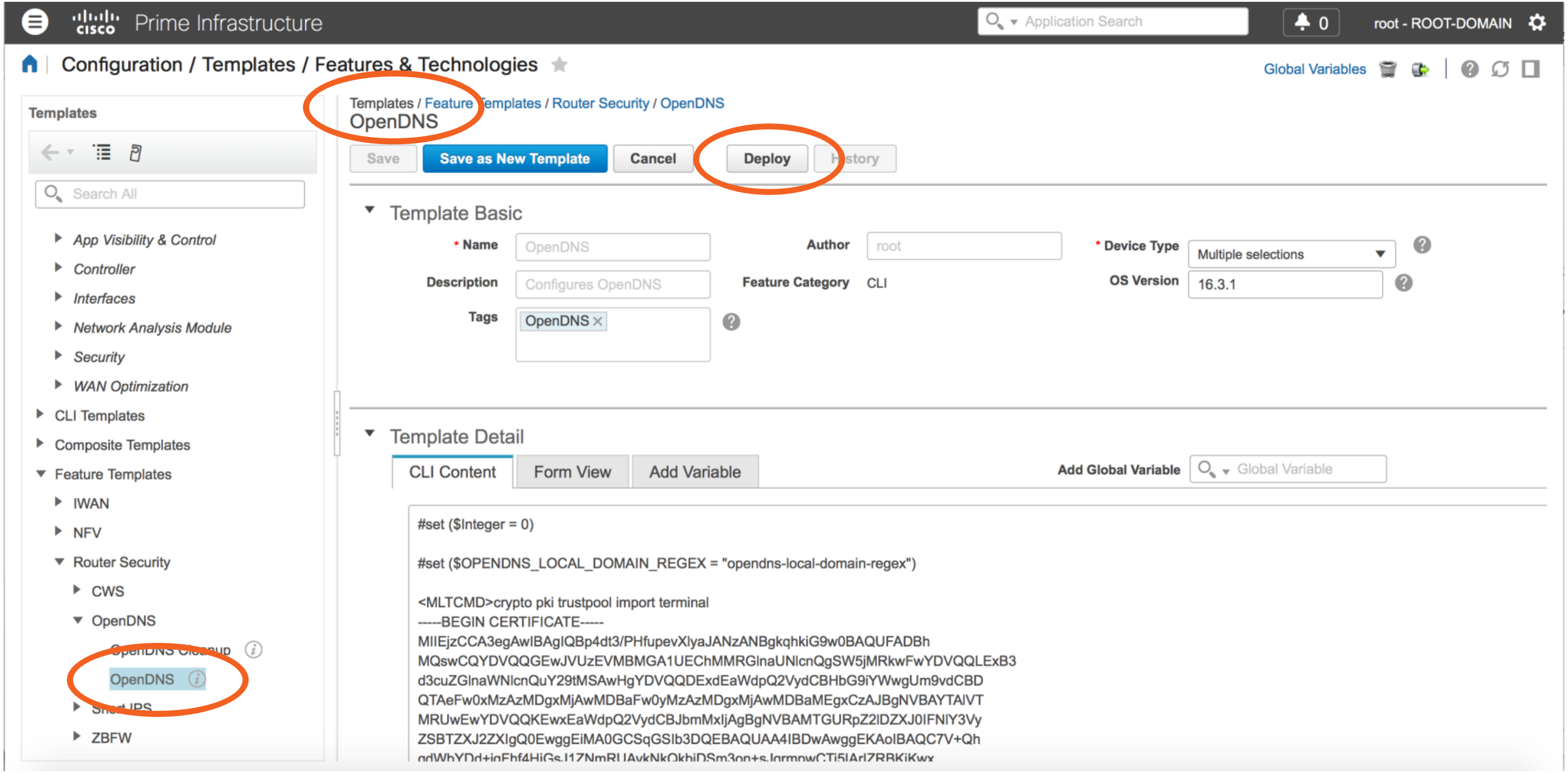
Step. 2 Configure local domain (optional) and token

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

Router(config)#parameter-map type opendns global
Router(config-profile)#token
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)#opendns out →”umbrella out” starting 16.6.1

Router(config-if)#interface g0/0/1
Router(config-if)#opendns in Guest →”umbrella in Guest” starting 16.6.1
```

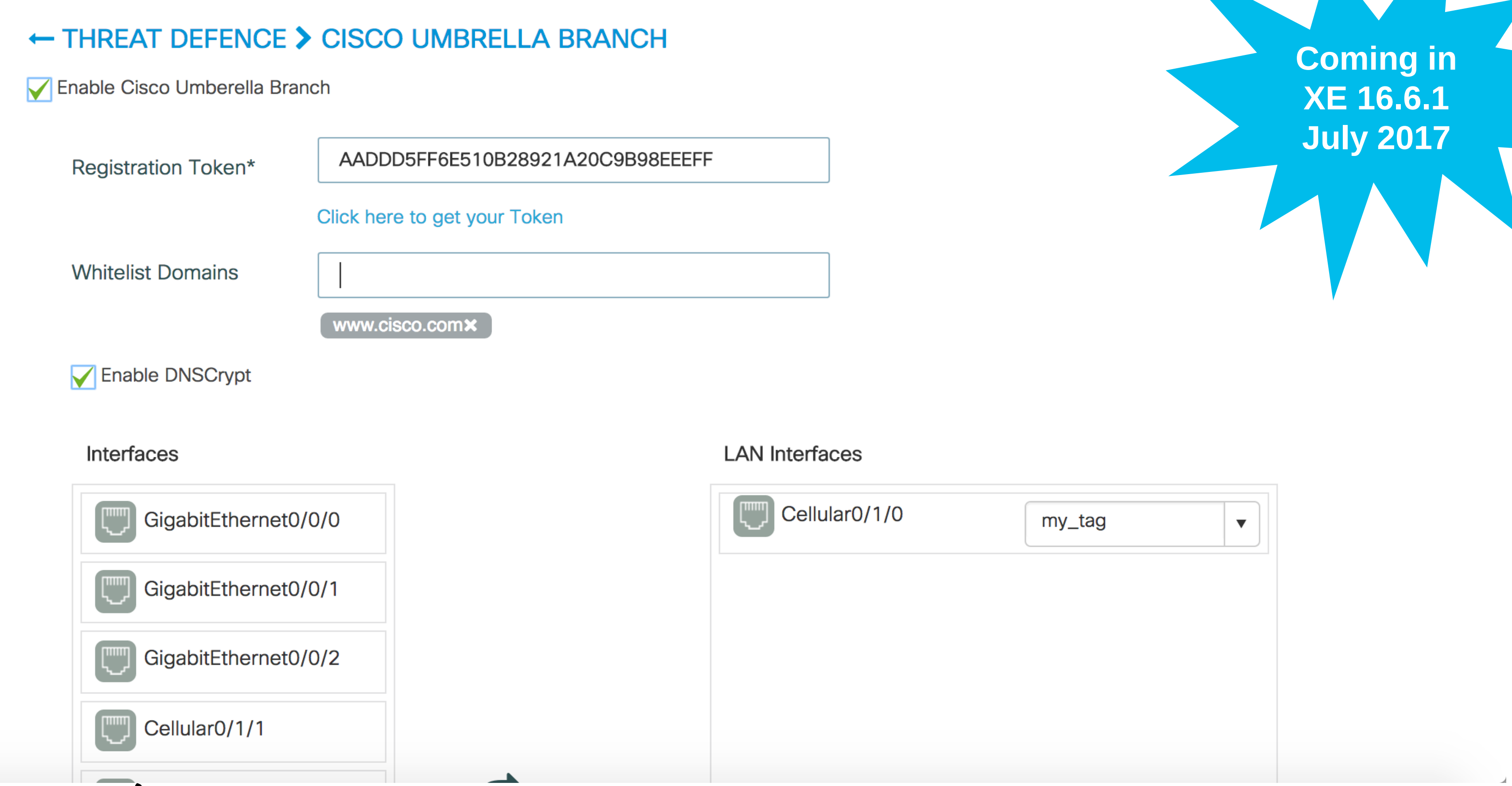
Cisco Umbrella – Provisioning (Prime Infrastructure 3.1 and above)



* 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
MRUwEwYDVQQKEwxEaWdpQ2VydCBJbmMxIjAgBgNVBAMTGURpZ2lDZXJ0IFNlY3Vy
ZSBTZXJ2ZXIgQ0EwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC7V+Qh
gdWhYDd+iqFhf4HiGsJ1ZNmRUAvkNkQkhjDSm3qp+sJqrmpwCTi5lArlZRBKjKwx
```

On-box WebUI - Cisco Umbrella



← THREAT DEFENCE › CISCO UMBRELLA BRANCH

☑ Enable Cisco Umberella Branch

Registration Token*: AADDD5FF6E510B28921A20C9B98EEEFF

Click here to get your Token

Whitelist Domains:

www.cisco.com✖

☑ Enable DNSCrypt

Interfaces

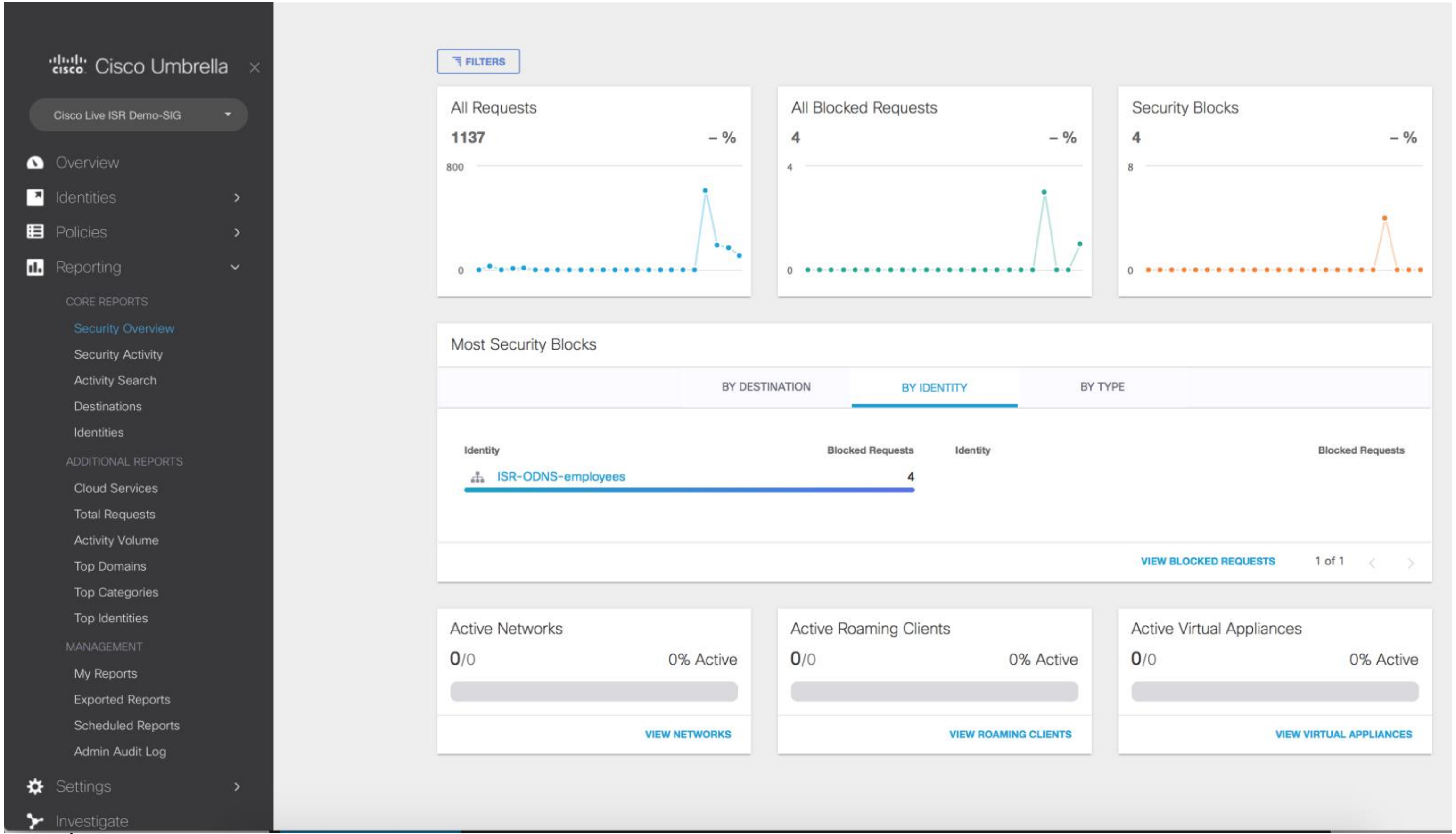
- GigabitEthernet0/0/0
- GigabitEthernet0/0/1
- GigabitEthernet0/0/2
- Cellular0/1/1

LAN Interfaces

- Cellular0/1/0 — my_tag ▾

Coming in XE 16.6.1 July 2017

Cisco Umbrella – Monitoring Using Umbrella Portal



All Requests
1137 – %

All Blocked Requests
4 – %

Security Blocks
4 – %

Most Security Blocks

BY DESTINATION | BY IDENTITY | BY TYPE

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

VIEW BLOCKED REQUESTS 1 of 1

Active Networks
0/0 0% Active
VIEW NETWORKS

Active Roaming Clients
0/0 0% Active
VIEW ROAMING CLIENTS

Active Virtual Appliances
0/0 0% Active
VIEW VIRTUAL APPLIANCES

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

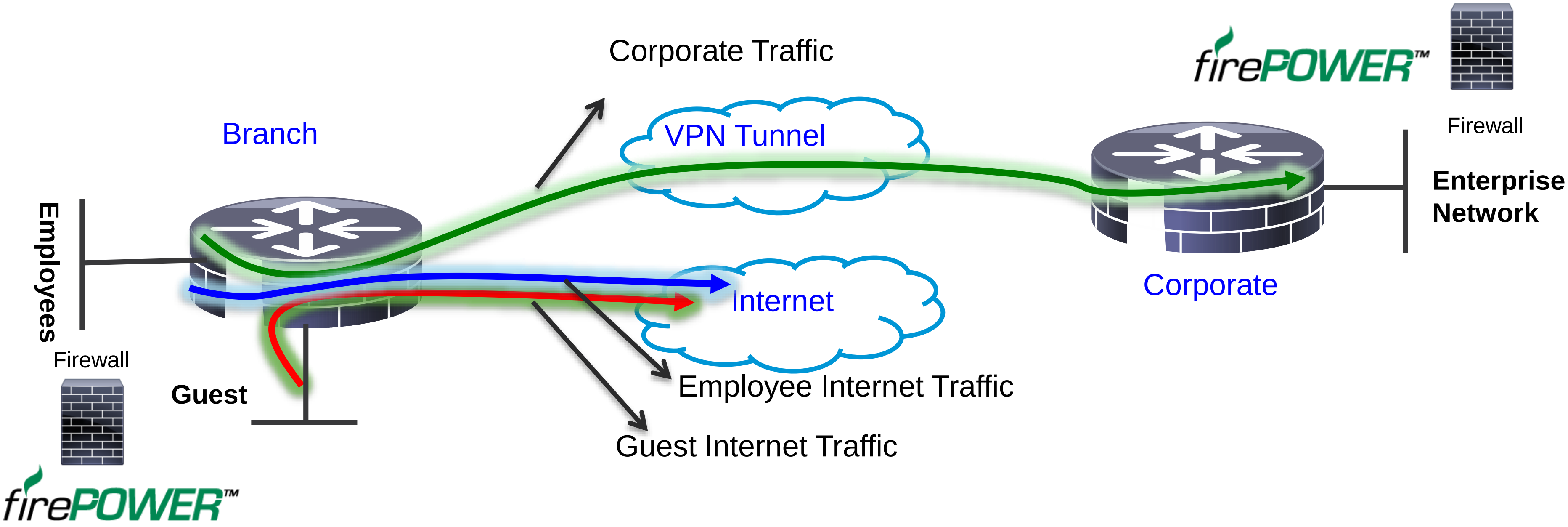
Cisco Umbrella Configuration Guide:
http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_utd/configuration/xe-16/sec-data-umbrella-branch-xe-16-book/sec-data-umbrella-bran.html

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

Agenda

- Zone Based Firewall
- Snort IPS
- Cisco Umbrella (OpenDNS)
- **Firepower**
- Stealthwatch Learning Network License (SLNL)
- Cloud Web Security (CWS)

Use Case: Full DIA



- ➢ VLAN separation, guest and employees network are separated
- ➢ ZBFW blocks guest to employees traffic and vice versa
- ➢ Firepower URL Filtering provides web reputation and category based filtering
- ➢ Corporate and Guest devices reach Internet directly from the Branch
- ➢ Firepower provides IPS, AVC and AMP

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

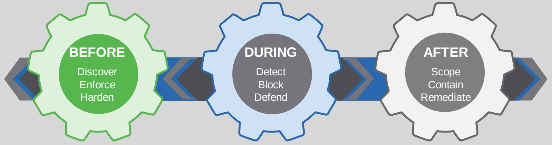
Firepower Threat Defense for ISR - Appendix

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®

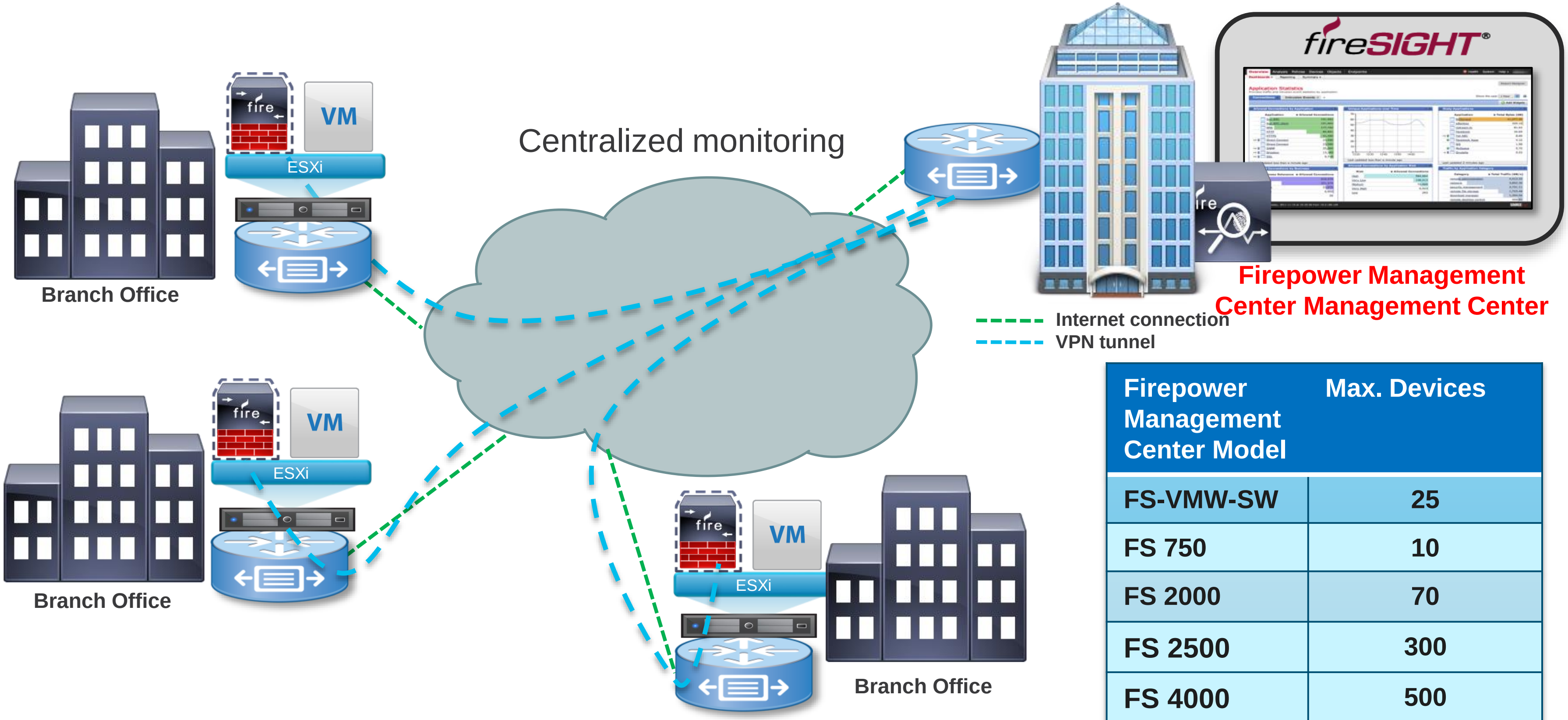
Cisco® 4000 Series ISR

OR

Cisco ISR G2 Series

Free Up Valuable Square Footage Generate More Revenue $$$

Firepower Threat Defense - Deployment Architecture

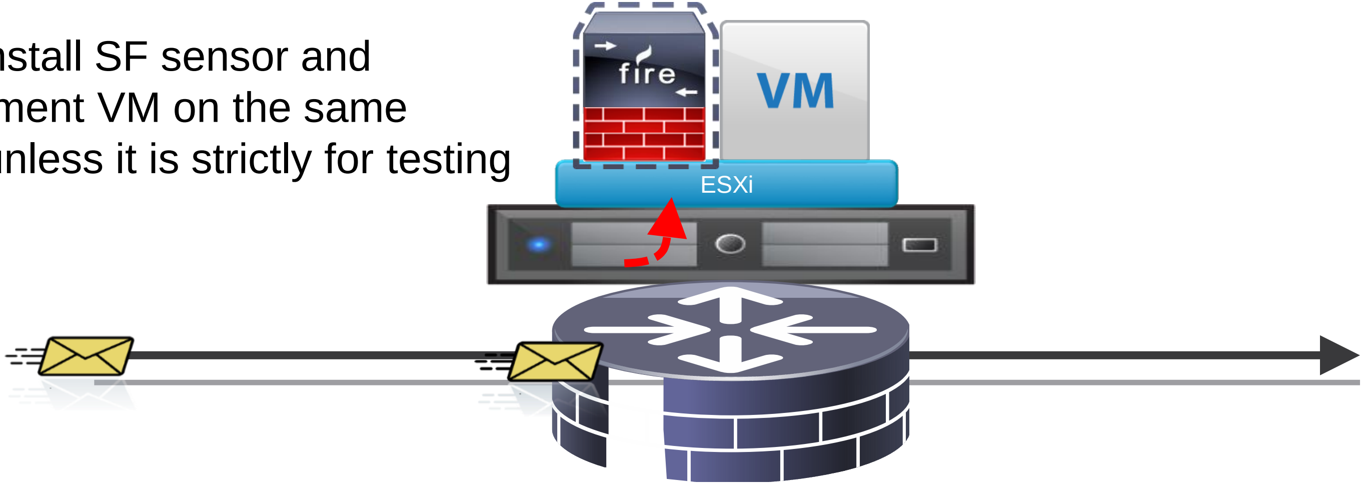


Firepower Management Center Model	Max. Devices
FS-VMW-SW	25
FS 750	10
FS 2000	70
FS 2500	300
FS 4000	500
FS 4500	750

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 – Configuration Steps

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

```
utd
 ids redirect interface Vlan10
 ids 000c.2923.abdc (mac address of the sensor interface)
 mode ids-global
!
interface ucse1/1
 description Internal switch interface connected to Service Module
 switchport mode trunk
 no ip address
!
Interface vlan10
 ip address 10.10.10.1 255.255.255.0
```

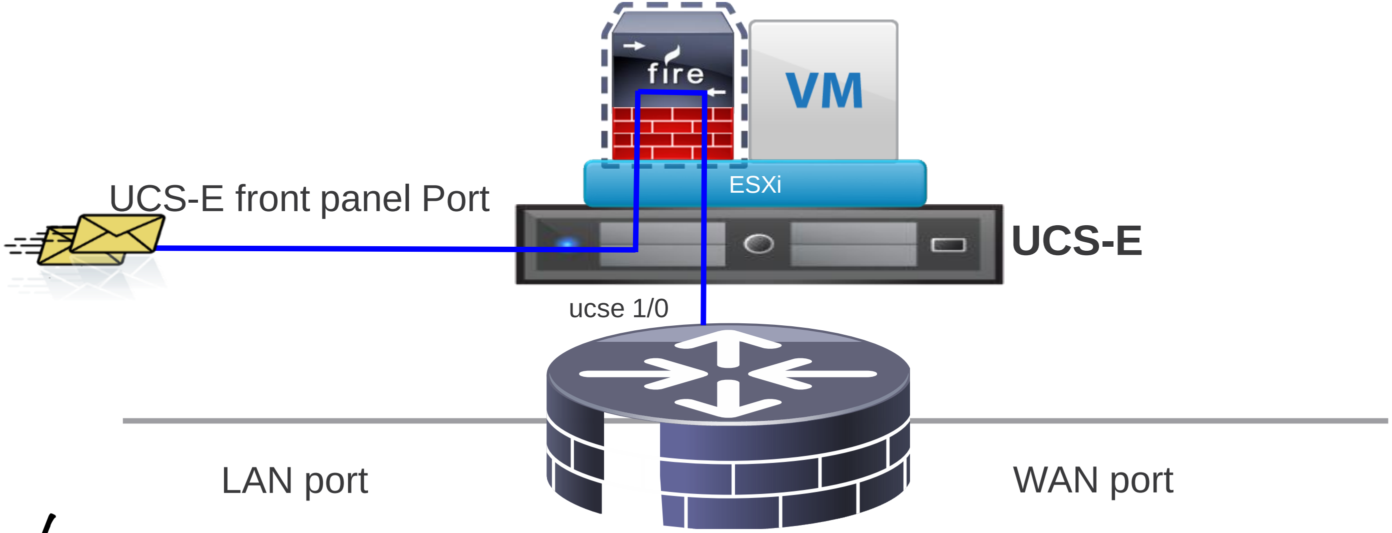
Cisco Firepower Threat Defense for ISR–
Configuration Steps

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

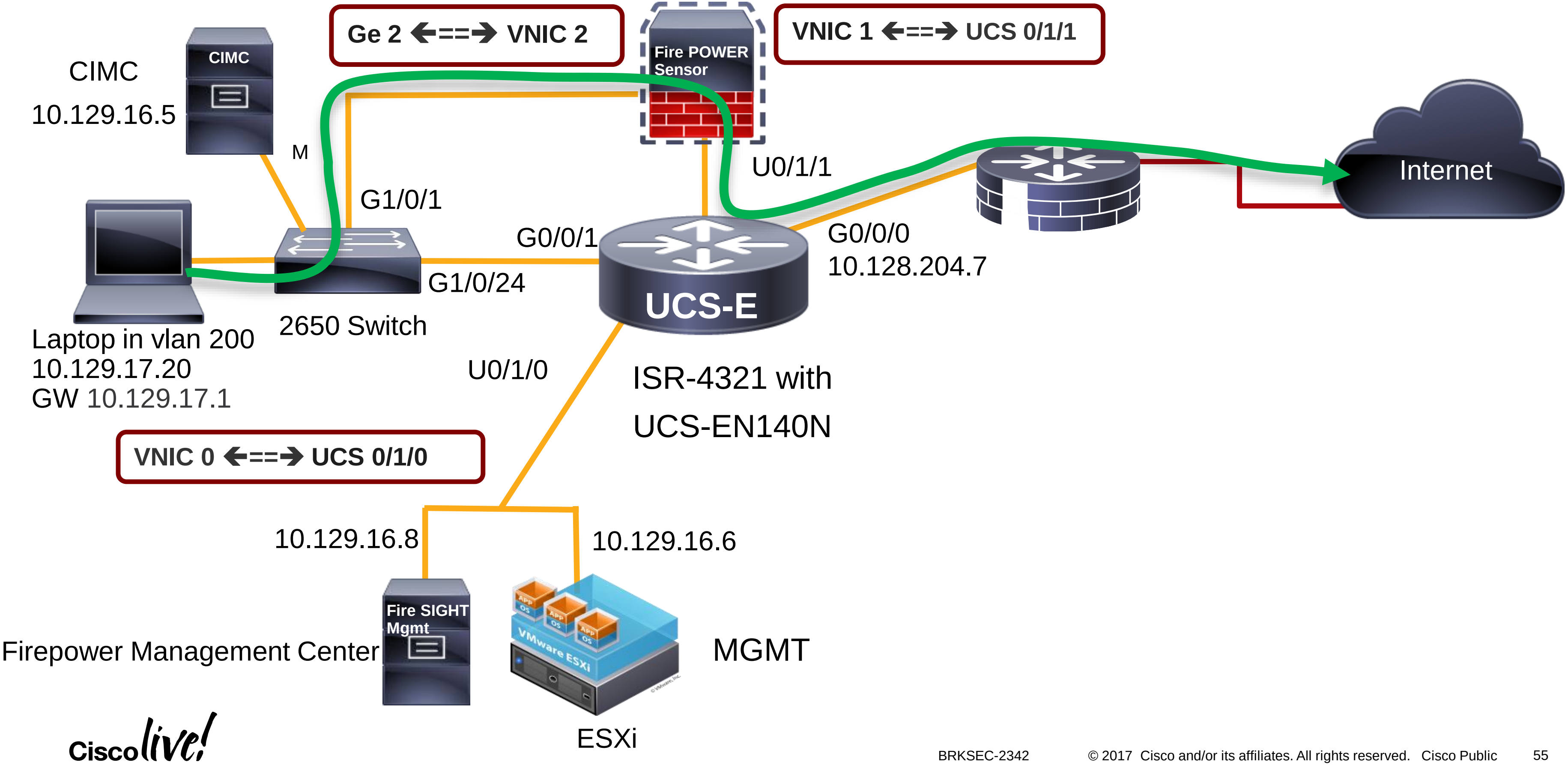
```
interface ucse2/0/0
 no ip address
 no negotiation auto
 switchport mode trunk
service instance 1
  ethernet encapsulation untagged bridge-domain 1
!
interface BDI1
 ip unnumbered GigabitEthernet0/0/1
!
utd  (data plane)
 all-interfaces
 redirect interface BDI1
 engine advanced
```

Firepower Threat Defense for ISR- IPS (front panel port)

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



Cisco Firepower Threat Defense for ISR - IPS



Firepower IPS using Front Panel Port - Switch Config

Enable Rapid Spanning Tree on the Switch

```
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 100,200 hello-time 1
spanning-tree vlan 100,200 forward-time 4
!
```

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

```
interface GigabitEthernet1/0/1
  description Connected to the UCS-E Front Panel Ge 2 Port
  switchport mode trunk
!
```

Port connected to the routers G0/0/1 Port

```
interface GigabitEthernet1/0/24
   description connected to the routers G0/0/1 Port
   switchport mode trunk
!
```

Firepower IPS using Front Panel Port – Router Config

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

```
interface GigabitEthernet0/0/1
 no ip address
 spanning-tree cost 100
 service instance 100 ethernet
  encapsulation dot1q 100
  rewrite ingress tag pop 1 symmetric
  bridge-domain 100

 service instance 200 ethernet
  encapsulation dot1q 200
  rewrite ingress tag pop 1 symmetric
  bridge-domain 200
```

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

```
interface ucse0/1/0
 ip unnumbered BDI100
 no negotiation auto
 switchport mode trunk
 no mop enabled
 no mop sysid
```

```
interface ucse0/1/1
 no ip address
 switchport mode trunk
 no mop enabled
 no mop sysid
 spanning-tree cost 10
 service instance 200 ethernet
  encapsulation dot1q 200
  rewrite ingress tag pop 1 symmetric
  bridge-domain 200
```

BDI Interface for vlan 100 (management to ESXi)

```
interface BDI100
 ip address 10.129.16.1 255.255.255.0
```

BDI Interface to terminate vlan 200 on the outside of the FP sensor

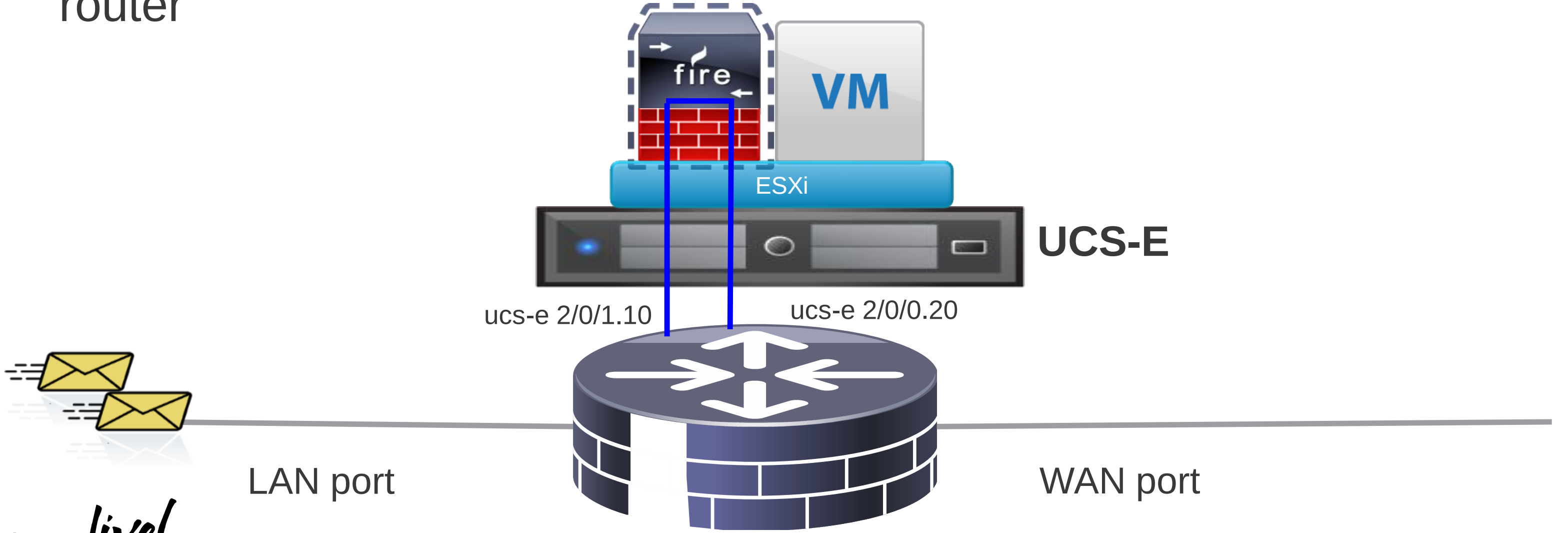
```
interface BDI200
 ip address 10.129.17.1 255.255.255.0
```

Route statements for FP-Sensor and ESXI management

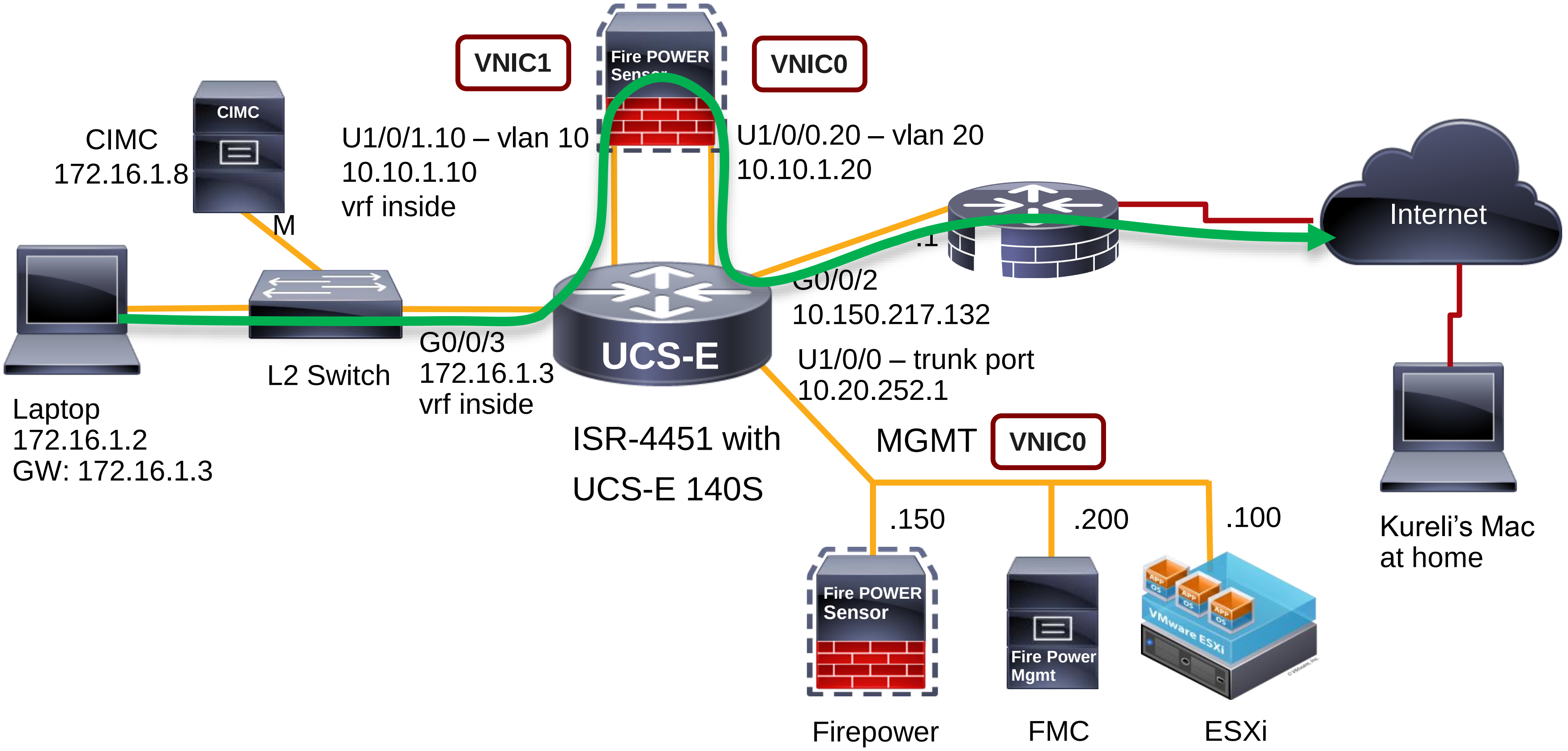
```
ip route 10.129.16.6 255.255.255.255 ucse0/1/0
ip route 10.129.16.8 255.255.255.255 ucse0/1/0
```

Firepower Threat Defense for ISR – IPS (vrf method)

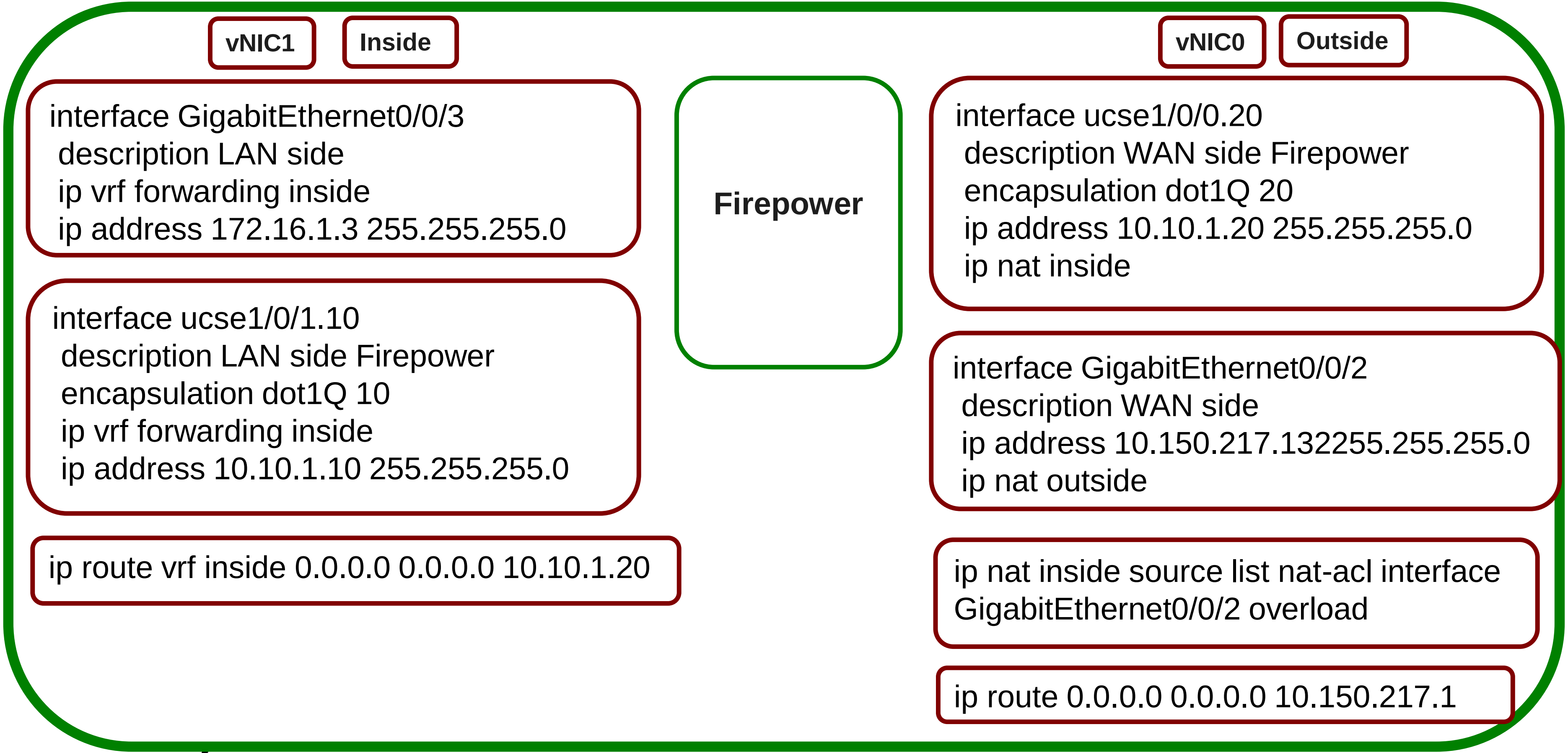
- Host the Sensor on the UCS-E
- IPS is in inline mode
- Packets ingress via the LAN interface of the router
- SF sensor examines traffic; allowed packets egress the WAN interface of the router



Cisco Firepower Threat Defense for ISR - IPS



Cisco Firepower Threat Defense for ISR - IPS



```
interface GigabitEthernet0/0/3
 description LAN side
 ip vrf forwarding inside
 ip address 172.16.1.3 255.255.255.0
```

```
interface ucse1/0/1.10
 description LAN side Firepower
 encapsulation dot1Q 10
 ip vrf forwarding inside
 ip address 10.10.1.10 255.255.255.0
```

```
ip route vrf inside 0.0.0.0 0.0.0.0 10.10.1.20
```

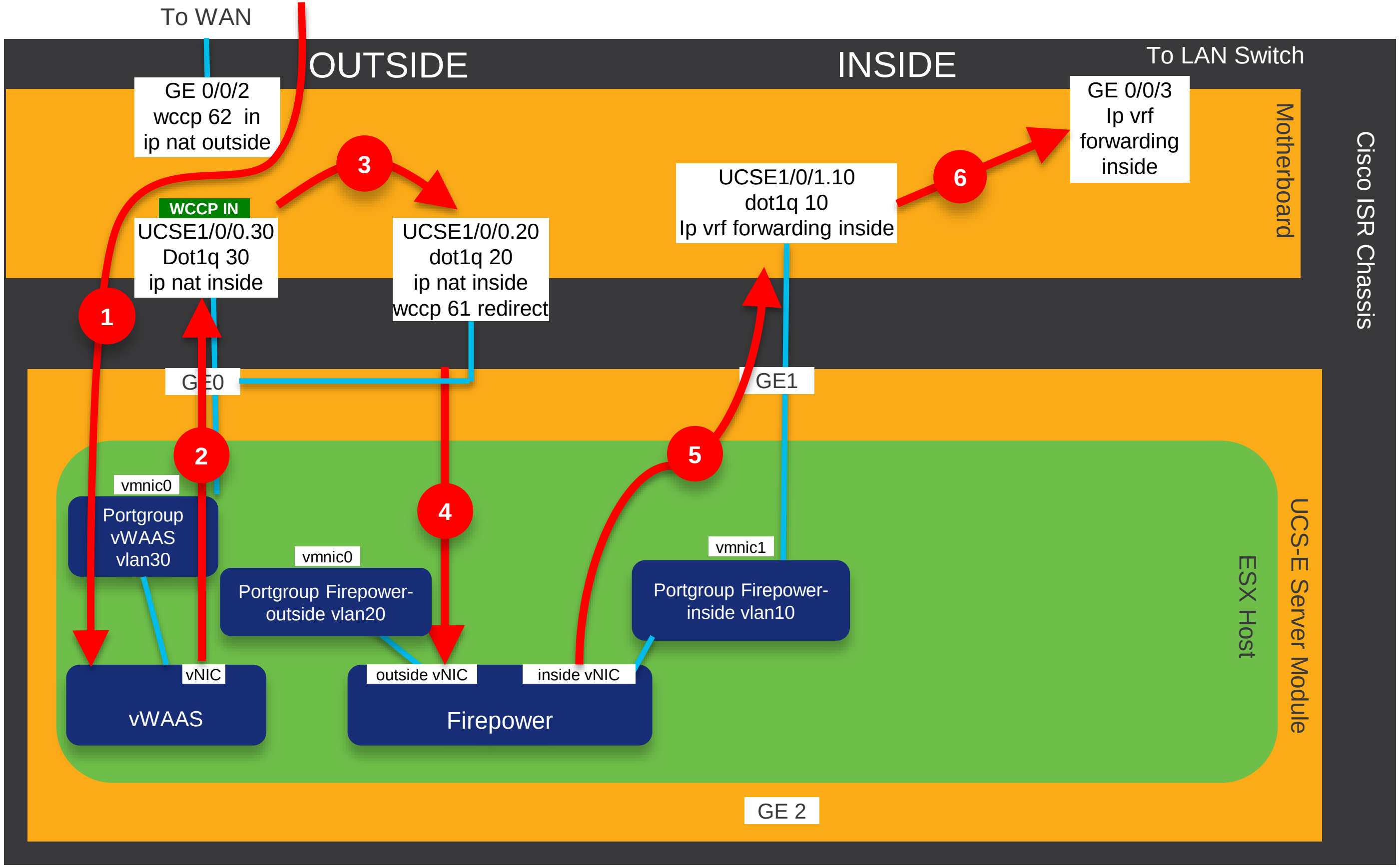
```
interface ucse1/0/0.20
 description WAN side Firepower
 encapsulation dot1Q 20
 ip address 10.10.1.20 255.255.255.0
 ip nat inside
```

```
interface GigabitEthernet0/0/2
 description WAN side
 ip address 10.150.217.132255.255.255.0
 ip nat outside
```

```
ip nat inside source list nat-acl interface
GigabitEthernet0/0/2 overload
```

```
ip route 0.0.0.0 0.0.0.0 10.150.217.1
```

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
- 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

Agenda

- Zone Based Firewall
- Snort IPS
- Cisco Umbrella (OpenDNS)
- Firepower
- **Stealthwatch Learning Network License (SLNL)**
- Cloud Web Security (CWS)

Stealthwatch Learning Network License - Appendix

For Your Reference

- DLA – Distributed Learning Agent (Network Element)
- TALOS – Talos is the industry-leading threat intelligence organization
- VPG – Virtual Port Group
- NSC – Network Sensing Component
- NCC – Network Control Component
- NIM-SSD – Network Interface Module Solid State Drive
- ISE – Identity Services Engine
- DPI – Deep Packet Inspection
- NBAR - Network Based Application Recognition

Cisco Stealthwatch Learning Network License

Brings self-learning attributes to the Cisco 4000 ISR

Needs no programming of firewall rules, malware signatures, or access control lists (ACLs)

Uses machine learning, network context, and packet capture to determine what's normal and what's not

Uses advanced analytics and models to identify and block true anomalies

Adapts as conditions change

Learning Network Components

Learning Network Agent

Machine-learning security agent software for the Cisco 4000 Integrated Services Router that collects and analyzes information, which it communicates to the Controller.

Learning Network Controller

Virtual machine application software that provides web-based advanced visualization of the anomalies that the Distributed Learning Agents discover.

Basic Operation of the Learning Network License

1 Discovers traffic paths

2 Builds map of IP addresses to learn about its environment

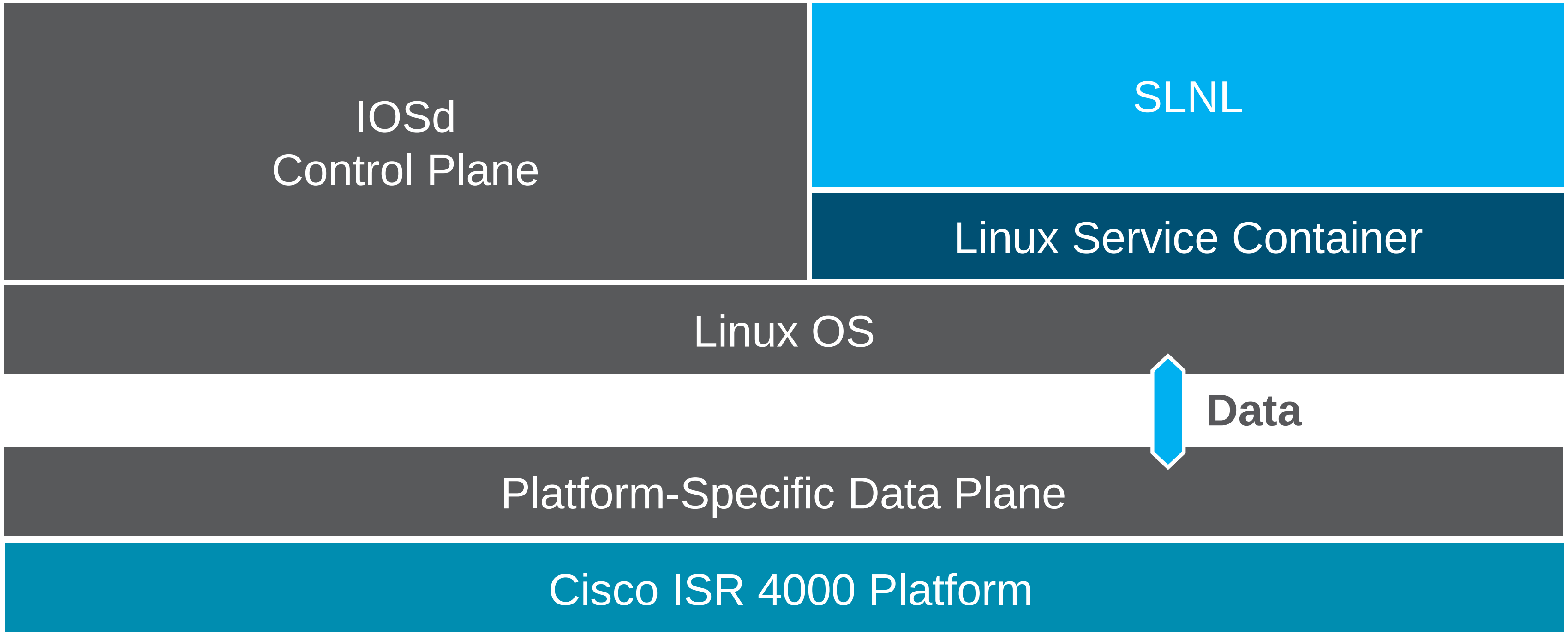
3 Identifies applications on NBAR and DPI

4 Studies traffic movement, volumes, patterns, times of day

5 Learns to distinguish normal from anomalous

6 Precisely identifies anomaly; allows operator to take action to remediate

SLNL - ISR 4000 with Learning Agent



IOSd
Control Plane

SLNL

Linux Service Container

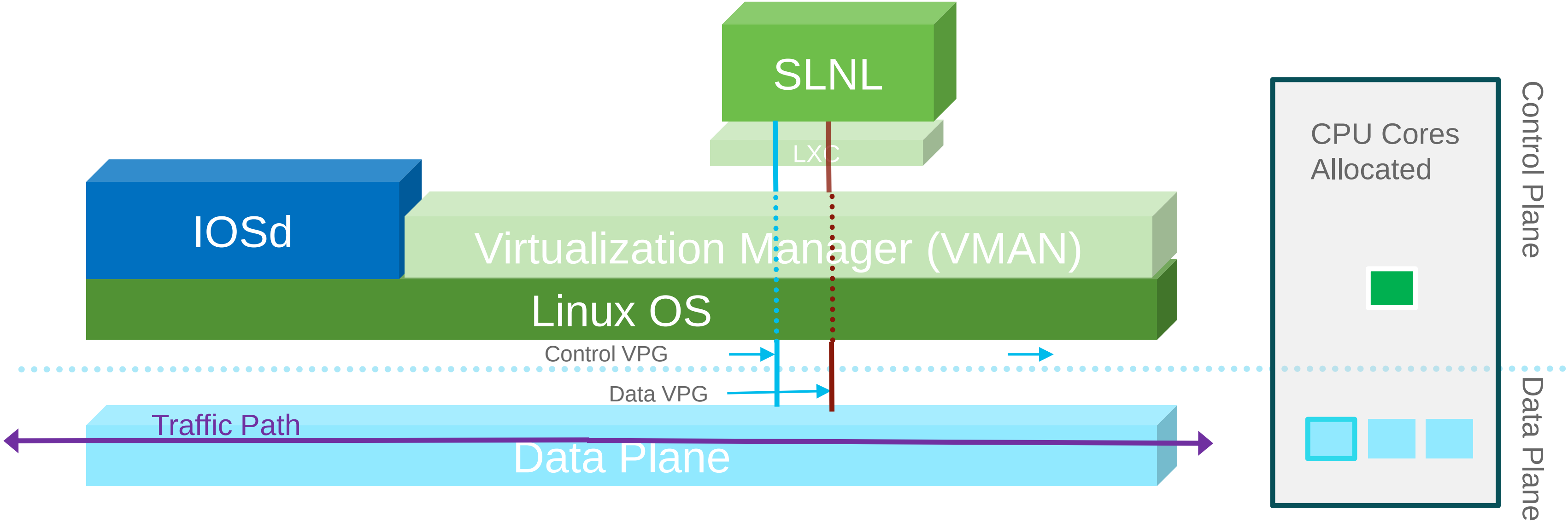
Linux OS

Data

Platform-Specific Data Plane

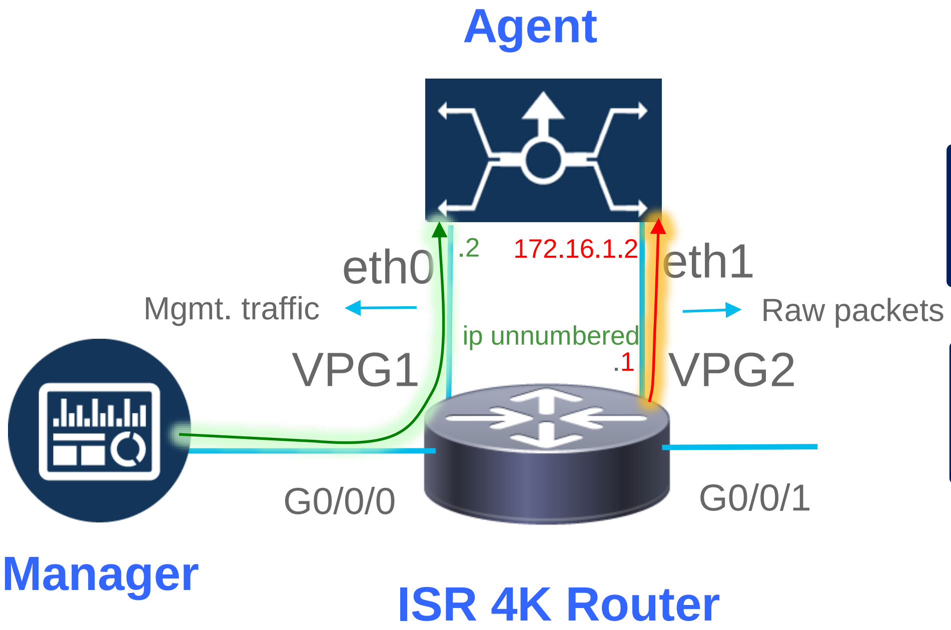
Cisco ISR 4000 Platform

SLNL - Container Architecture



- SLNL Agent runs on a Linux Container using control plane resources
- NetFlow records are sent to the container using Virtual Port Group interface
- Reserved CPU and memory for SNLN agent

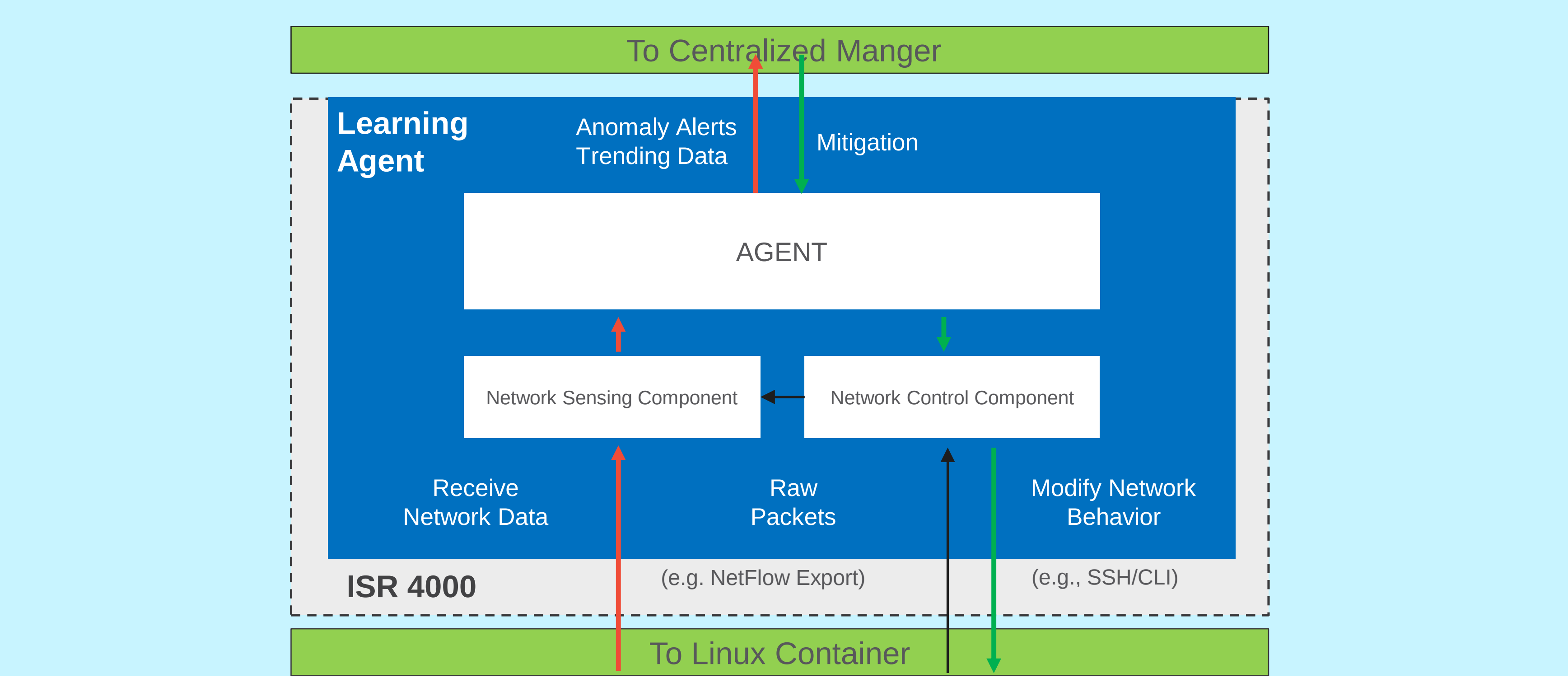
SLNL - Virtual Service Networking



VPGs to communicate between container and router

VPG1 <==> eth0 (mgmt traffic)
VPG2 <==> eth1 (data traffic)

SLNL Learning Agent - A Closer Look



The Power of the Learning Network: What's New?

Current Security Solutions	Stealthwatch Learning Network License
▪ Consist of specialized security appliances connected to the network, such as firewalls and intrusion prevention systems ▪ Rely heavily on known signatures to detect known malware ▪ Have limited adaptability so newer threats are more likely to get through	▪ Pervasive and adaptive ▪ Uses machine learning (artificial intelligence) to detect advanced, evasive malware network-wide ▪ High focus on 0-day attacks ▪ Uses ISR 4000 as distributed analytic engines (sensor) and security system (enforcer)

The Power of the Learning Network: Precision Detection

Traditional Anomaly Detection System

- Focuses on detecting as many events as it can
- Creates unwieldy number of false positives and irrelevant alarms
- Alone, the volume of detections isn’t the best measure of a system’s effectiveness
- Telemetry-driven, centralized solutions

Stealthwatch Learning Network License

- Fast, efficient, precise detection
- The network learns from its own mistakes and minimizes chasing false positives
- Detects and accounts for multiple indicators of an anomaly
- Bandwidth and processor-light, distributed solution

Learning Network License Deployment Requirements

Learning Network Manager

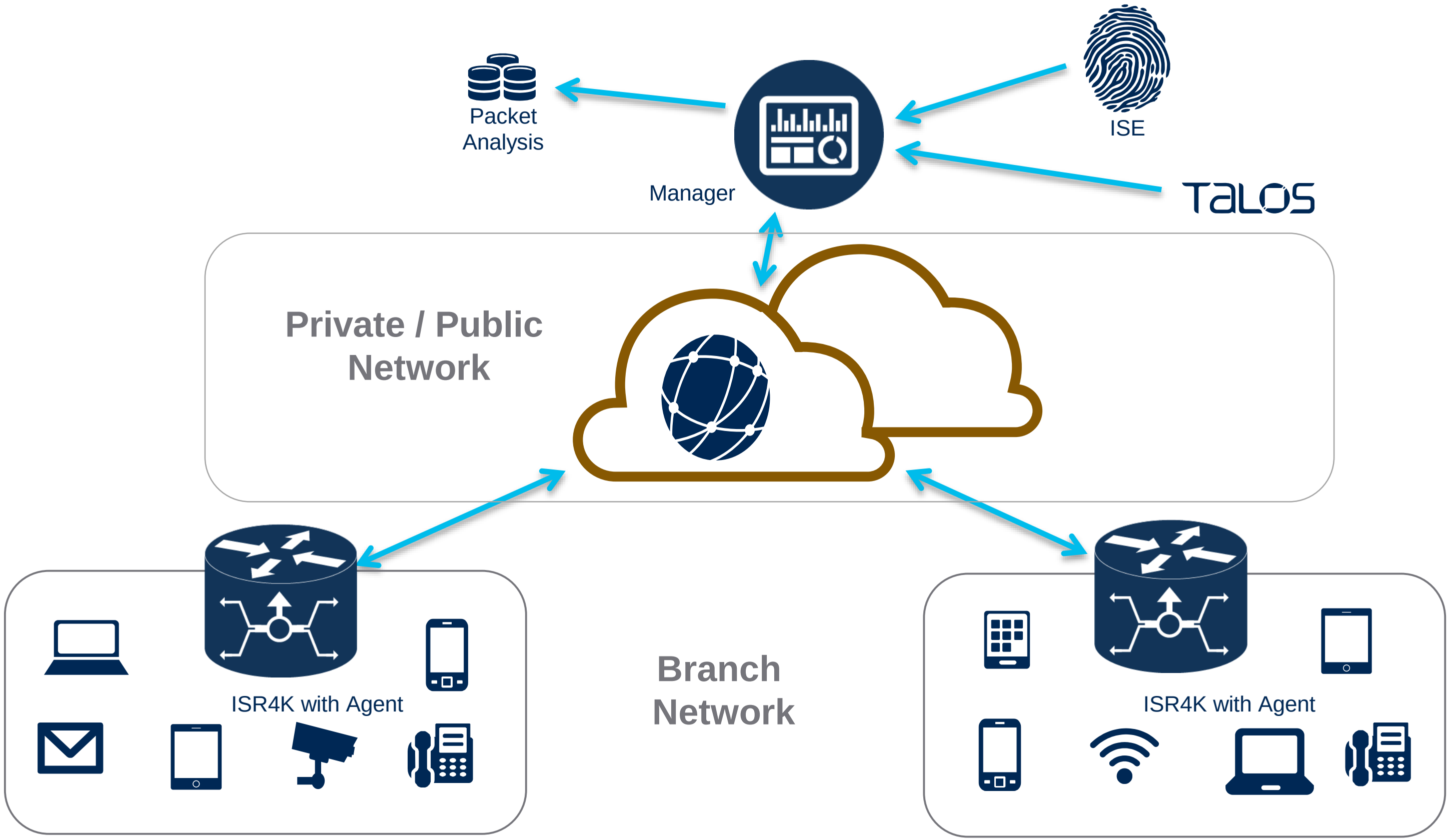
- VMWare ESXi 5.5
- Memory 16 GB
- 4 Virtual CPUs
- 1 Virtual NIC
- 200 GB of hard disk

Learning Network Agent

- ISR 4000 (4451, 4431, 4351,4331) *
- IOS-XE v3.16 with LXE Container
- IOS Application Experience (AX) Bundle
- 8 GB or 16 GB memory upgrade
- NIM-SSD 200 GB Persistent Storage (desirable option)

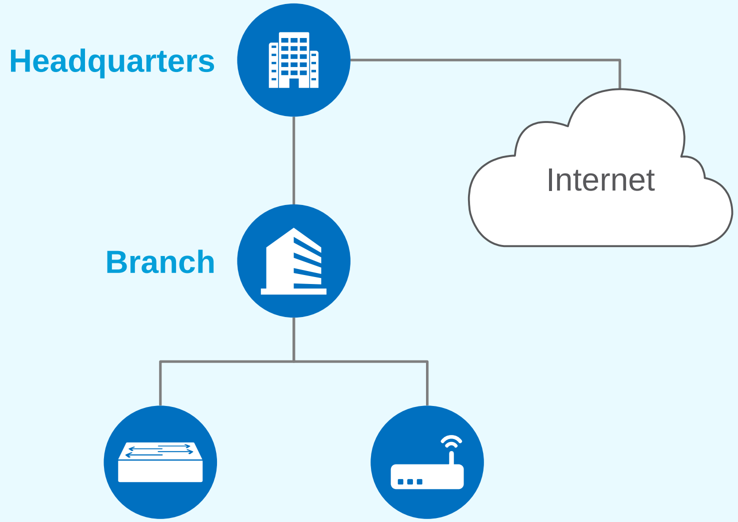
* *ISR 4321 and 4221 currently under test*

Automating Security in your Branch Offices



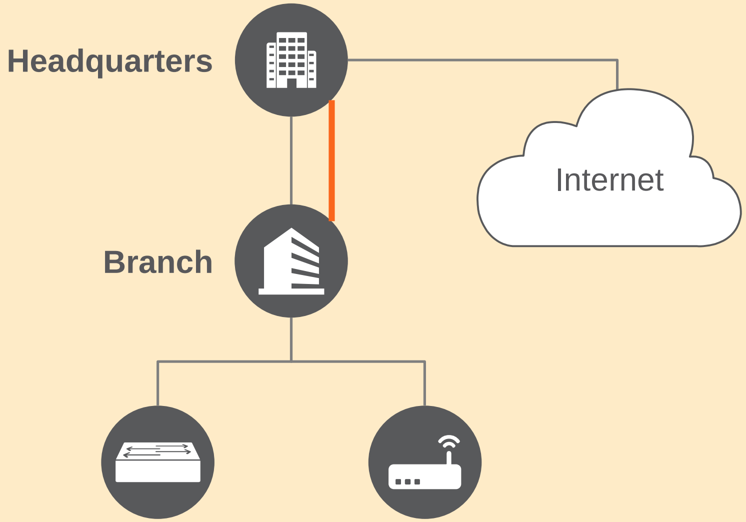
Use Case: Non Malicious Unusual Time of Day

Before



An HQ Analyst performing a manual file backup of a branch server starts the task at 12 PM rather than 12 AM.

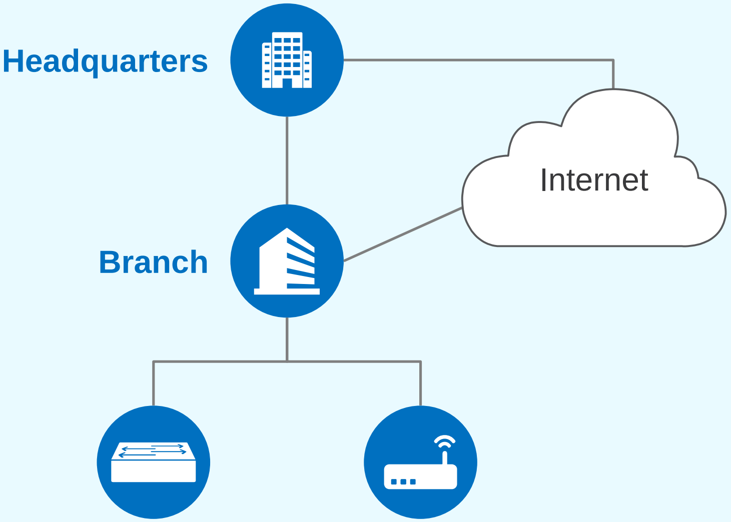
After



The Learning Agent reports the activity as unusual given the time. An analyst using the manager investigates and reports the activity as non-malicious.

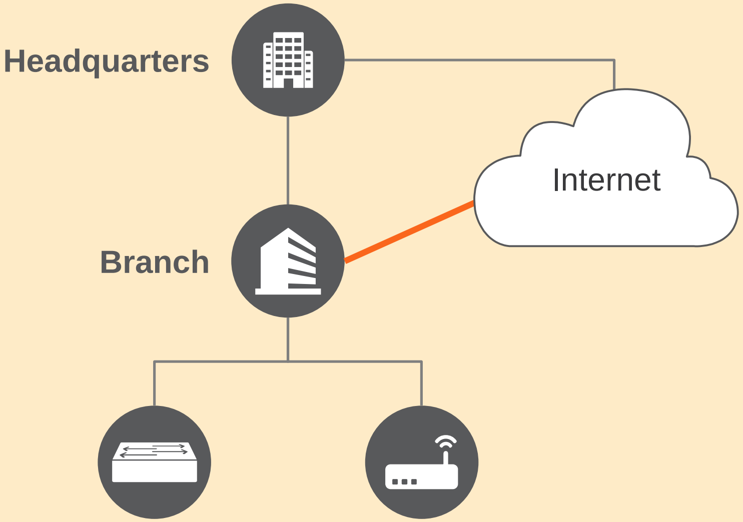
Use Case: Exfiltration via Tunneling

Before



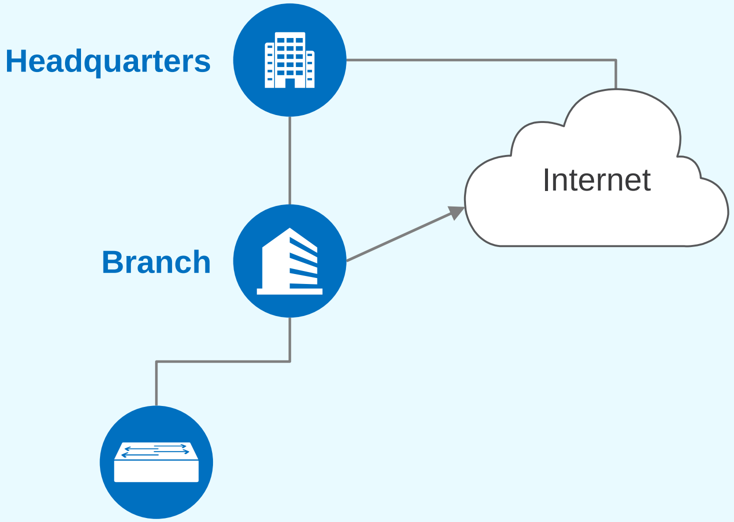
The agent notes a sudden increase in DNS traffic.

After

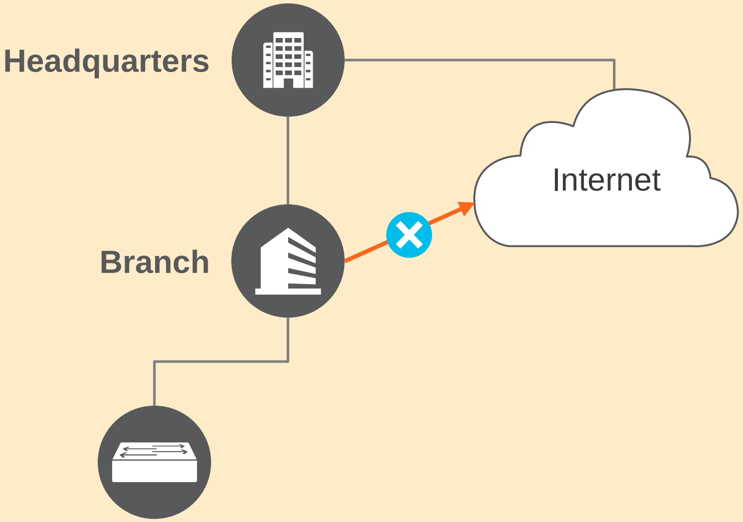


Using Stealthwatch Learning Network License, the analyst can identify attempts to pass additional data over DNS and bypass the firewall.

Use Case: New Application at the Branch



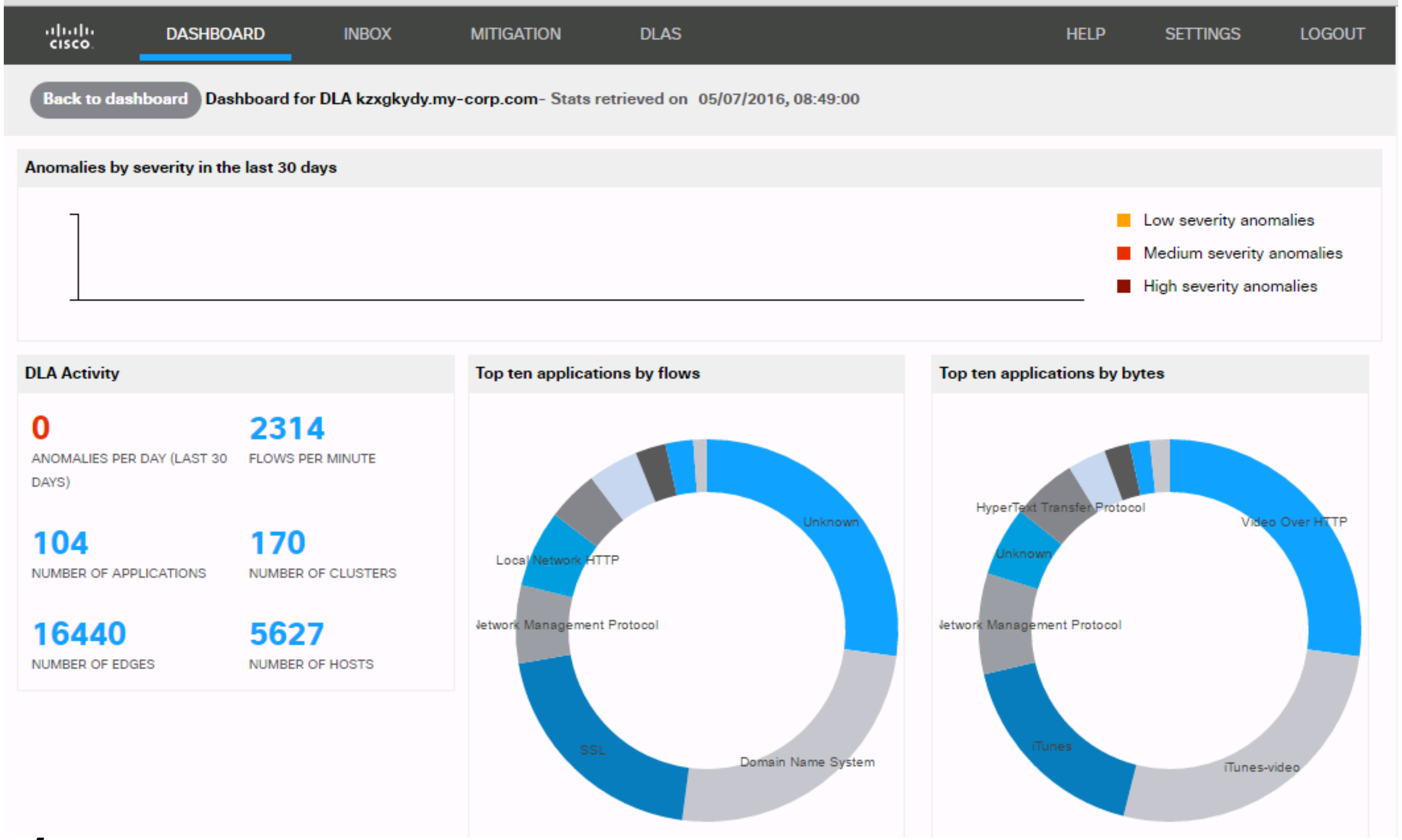
A branch user opens an application developed to send data to a suspect Internet site.



The router-based security agent identifies the attempt to connect to a suspect site and drops the connection.

SLNL Manager Dashboard

Dashboard Single Agent View



DASHBOARD INBOX MITIGATION DLAS HELP SETTINGS LOGOUT

Back to dashboard Dashboard for DLA kzxgkydy.my-corp.com- Stats retrieved on 05/07/2016, 08:49:00

Anomalies by severity in the last 30 days

- 🟧 Low severity anomalies
- 🟥 Medium severity anomalies
- 🟥 High severity anomalies

DLA Activity

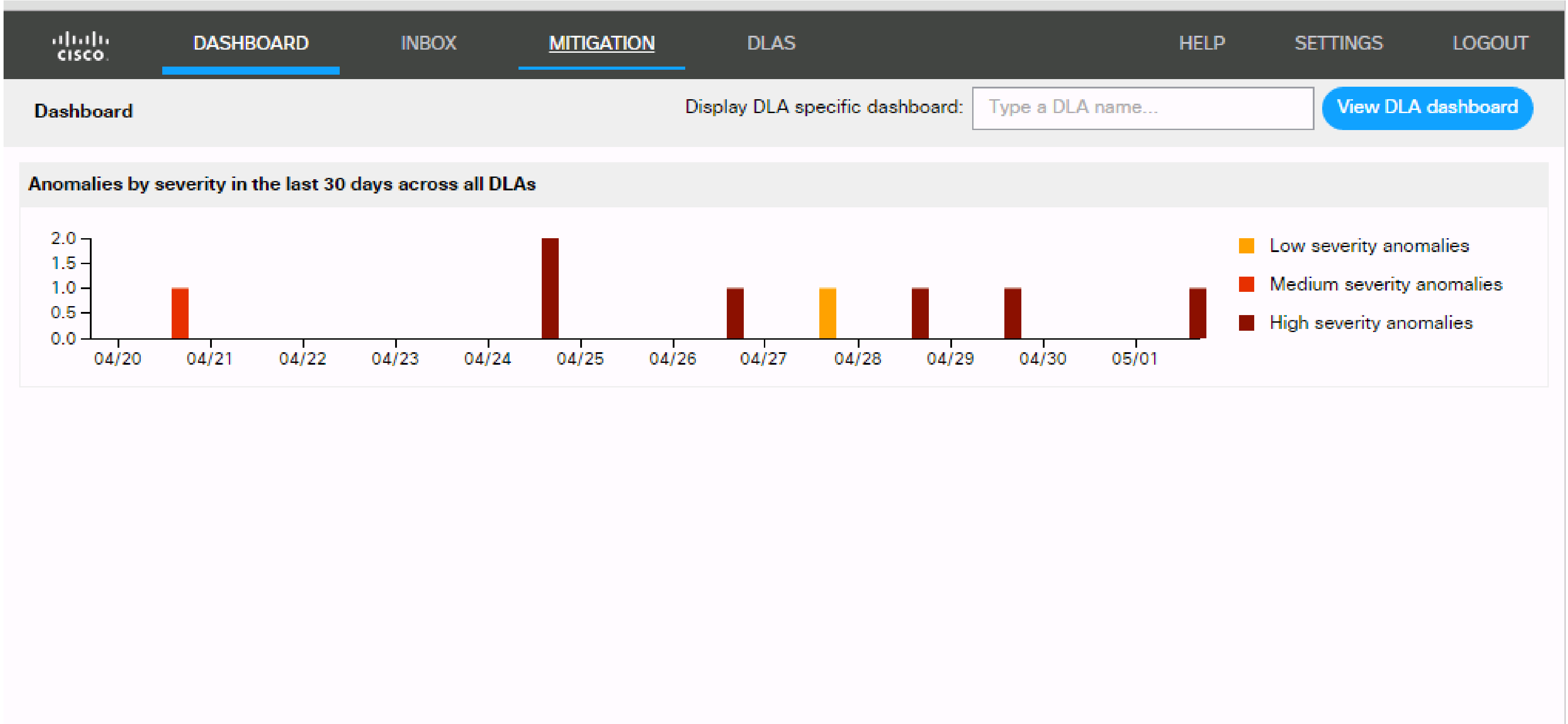
0 ANOMALIES PER DAY (LAST 30 DAYS)	2314 FLOWS PER MINUTE
104 NUMBER OF APPLICATIONS	170 NUMBER OF CLUSTERS
16440 NUMBER OF EDGES	5627 NUMBER OF HOSTS

Top ten applications by flows

Top ten applications by bytes

SLNL Manager Dashboard

Dashboard View



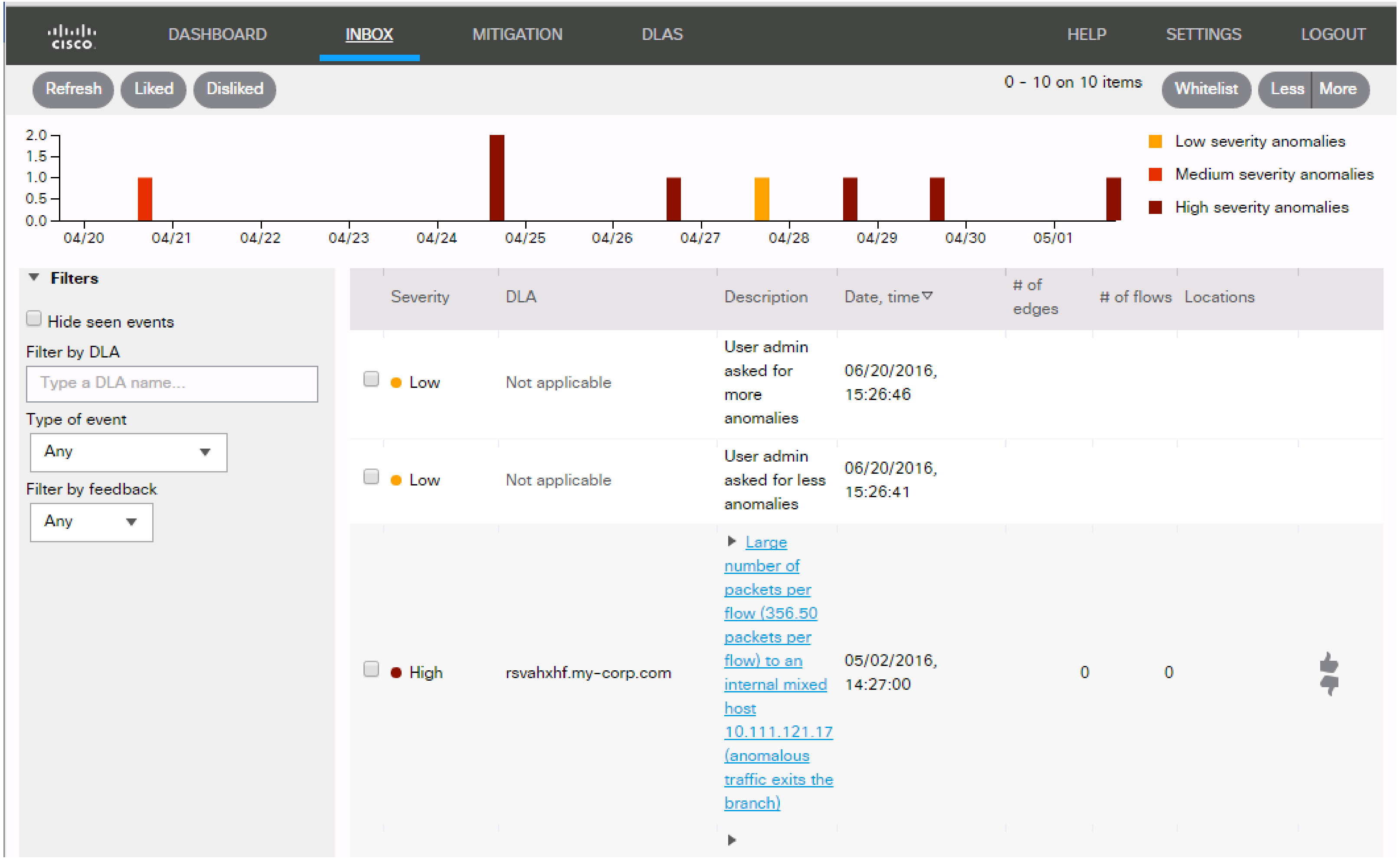
Dashboard

Display DLA specific dashboard: Type a DLA name...

Anomalies by severity in the last 30 days across all DLAs

Cisco live!

Inbox Top Level view



▼ Filters

□ Hide seen events

Filter by DLA

Type a DLA name...

Type of event

Any ▼

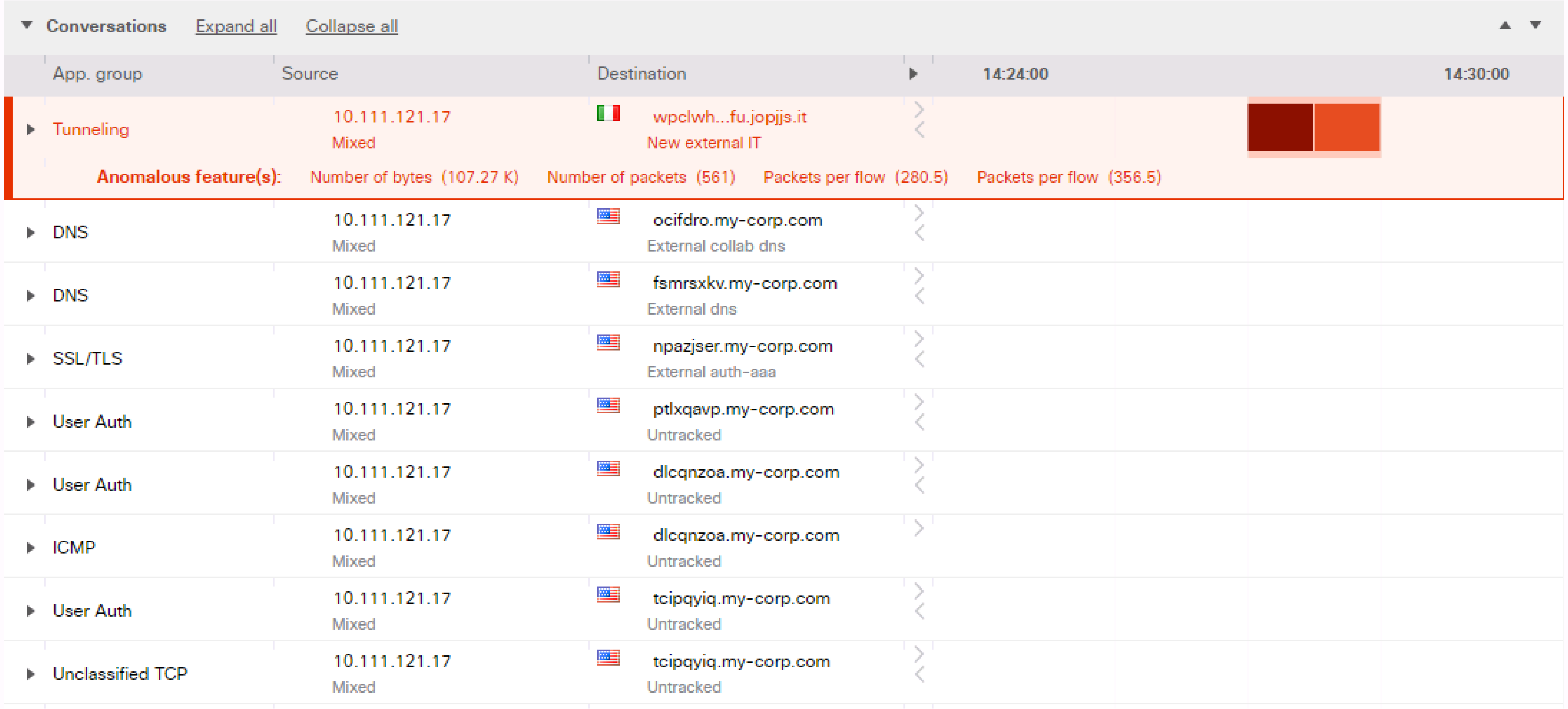
Filter by feedback

Any ▼

	Severity	DLA	Description	Date, time ▽	# of edges	# of flows	Locations	
□	● Low	Not applicable	User admin asked for more anomalies	06/20/2016, 15:26:46				
□	● Low	Not applicable	User admin asked for less anomalies	06/20/2016, 15:26:41				
□	● High	rsvahxhf.my-corp.com	▸ Large number of packets per flow (356.50 packets per flow) to an internal mixed host 10.111.121.17 (anomalous traffic exits the branch) ▸	05/02/2016, 14:27:00	0	0		👍 👎

SLNL Manager Inbox

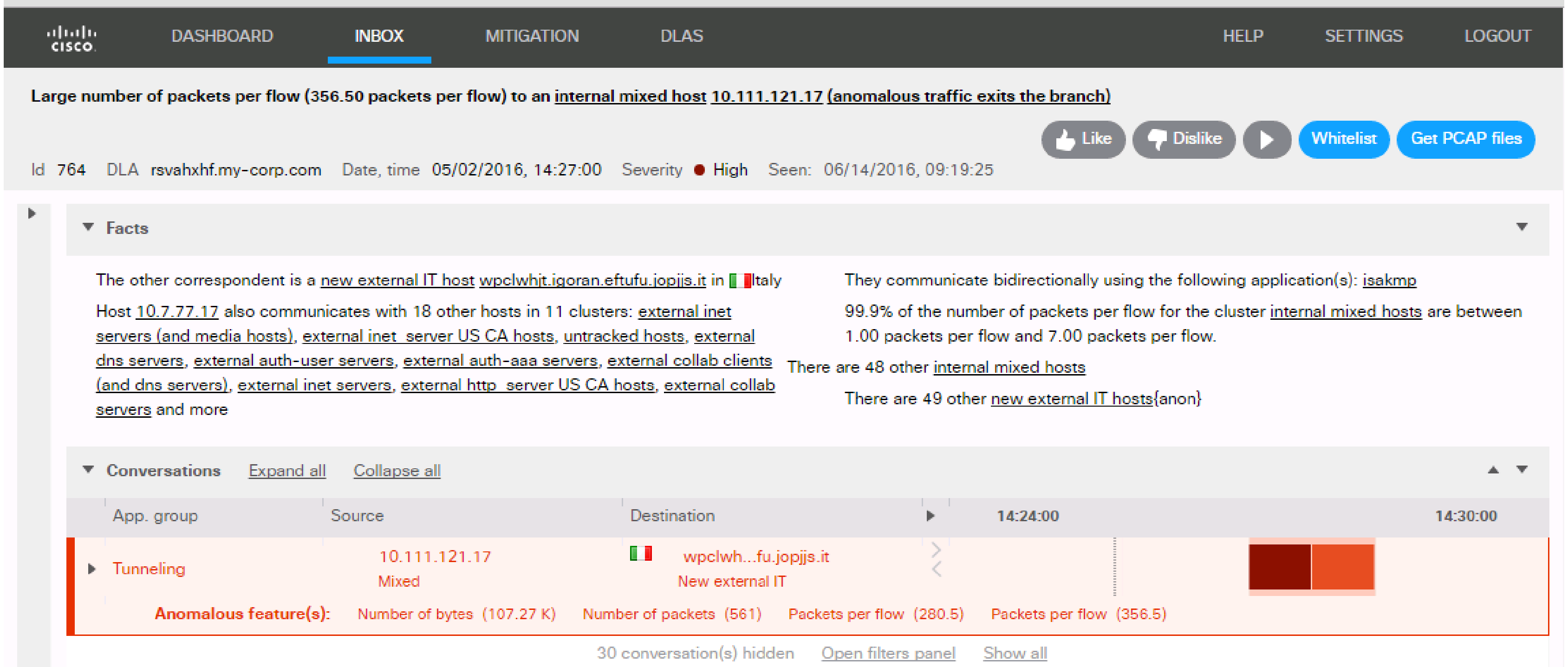
Inbox – Conversations - Expanded



▼ Conversations Expand all Collapse all ▲ ▼

App. group	Source	Destination	▶	14:24:00	14:30:00
▶ Tunneling	10.111.121.17 Mixed	wpclwh...fu.jopjjs.it New external IT			■■
Anomalous feature(s):	Number of bytes (107.27 K)	Number of packets (561)	Packets per flow (280.5)	Packets per flow (356.5)	
▶ DNS	10.111.121.17 Mixed	ocifdro.my-corp.com External collab dns			
▶ DNS	10.111.121.17 Mixed	fsmrsxkv.my-corp.com External dns			
▶ SSL/TLS	10.111.121.17 Mixed	npazjser.my-corp.com External auth-aaa			
▶ User Auth	10.111.121.17 Mixed	ptlxqavp.my-corp.com Untracked			
▶ User Auth	10.111.121.17 Mixed	dlcqnzoa.my-corp.com Untracked			
▶ ICMP	10.111.121.17 Mixed	dlcqnzoa.my-corp.com Untracked			
▶ User Auth	10.111.121.17 Mixed	tcipqyiq.my-corp.com Untracked			
▶ Unclassified TCP	10.111.121.17 Mixed	tcipqyiq.my-corp.com Untracked			

Inbox Facts View



Large number of packets per flow (356.50 packets per flow) to an internal mixed host 10.111.121.17 (anomalous traffic exits the branch)

Id 764 DLA rsvahxhf.my-corp.com Date, time 05/02/2016, 14:27:00 Severity ● High Seen: 06/14/2016, 09:19:25

Facts

The other correspondent is a new external IT host wpclwhjt.igoran.eftufu.jopjjs.it in Italy

Host 10.7.77.17 also communicates with 18 other hosts in 11 clusters: external inet servers (and media hosts), external inet server US CA hosts, untracked hosts, external dns servers, external auth-user servers, external auth-aaa servers, external collab clients (and dns servers), external inet servers, external http server US CA hosts, external collab servers and more

They communicate bidirectionally using the following application(s): isakmp

99.9% of the number of packets per flow for the cluster internal mixed hosts are between 1.00 packets per flow and 7.00 packets per flow.

There are 48 other internal mixed hosts

There are 49 other new external IT hosts{anon}

Conversations Expand all Collapse all

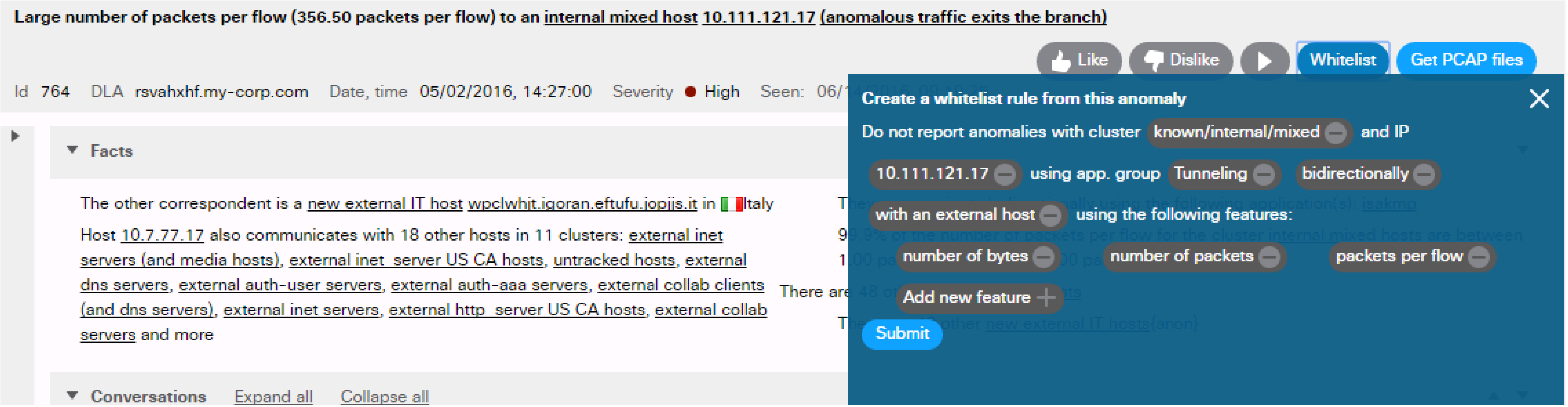
App. group	Source	Destination	14:24:00	14:30:00
Tunneling	10.111.121.17 Mixed	wpclwh...fu.jopjjs.it New external IT		

Anomalous feature(s): Number of bytes (107.27 K) Number of packets (561) Packets per flow (280.5) Packets per flow (356.5)

30 conversation(s) hidden Open filters panel Show all

SLNL Manager Whitelist

Inbox – White List



Large number of packets per flow (356.50 packets per flow) to an internal mixed host 10.111.121.17 (anomalous traffic exits the branch)

Id 764 DLA rsvahxhf.my-corp.com Date, time 05/02/2016, 14:27:00 Severity ● High Seen: 06/1

▼ Facts

The other correspondent is a new external IT host wpclwhjt.igoran.eftufu.jopjjs.it in Italy

Host 10.7.77.17 also communicates with 18 other hosts in 11 clusters: external inet servers (and media hosts), external inet server US CA hosts, untracked hosts, external dns servers, external auth-user servers, external auth-aaa servers, external collab clients (and dns servers), external inet servers, external http server US CA hosts, external collab servers and more

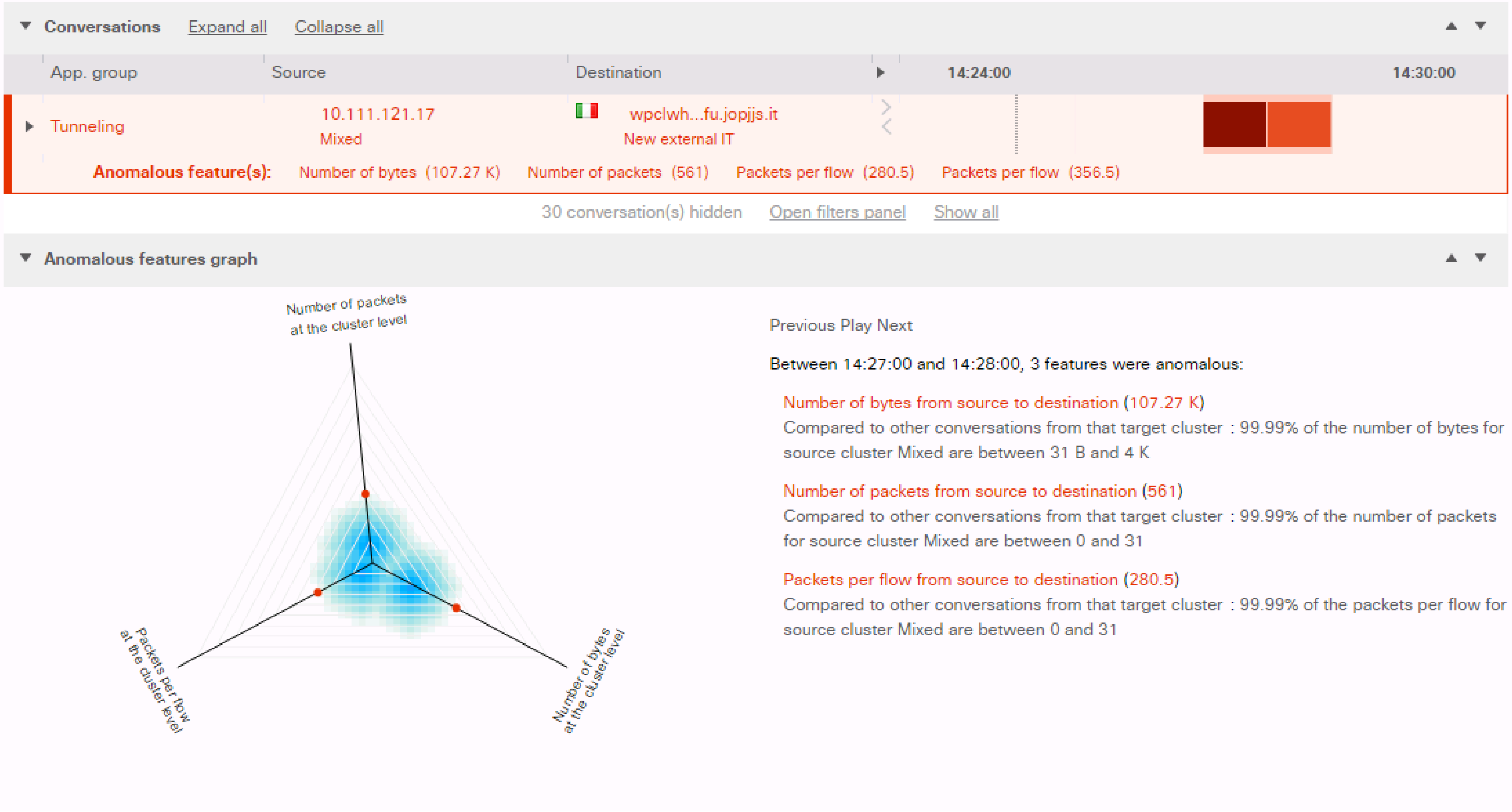
There are

▼ Conversations Expand all Collapse all

Create a whitelist rule from this anomaly

Do not report anomalies with cluster known/internal/mixed and IP 10.111.121.17 using app. group Tunneling bidirectionally with an external host using the following features:

Inbox Conversations



▼ Conversations Expand all Collapse all ▲ ▼

App. group	Source	Destination	▶	14:24:00	14:30:00
▶ Tunneling	10.111.121.17 Mixed	wpclwh...fu.jopjjs.it New external IT			

Anomalous feature(s): Number of bytes (107.27 K) Number of packets (561) Packets per flow (280.5) Packets per flow (356.5)

30 conversation(s) hidden Open filters panel Show all

▼ Anomalous features graph ▲ ▼

Number of packets at the cluster level
Packets per flow at the cluster level
Number of bytes at the cluster level

Previous Play Next

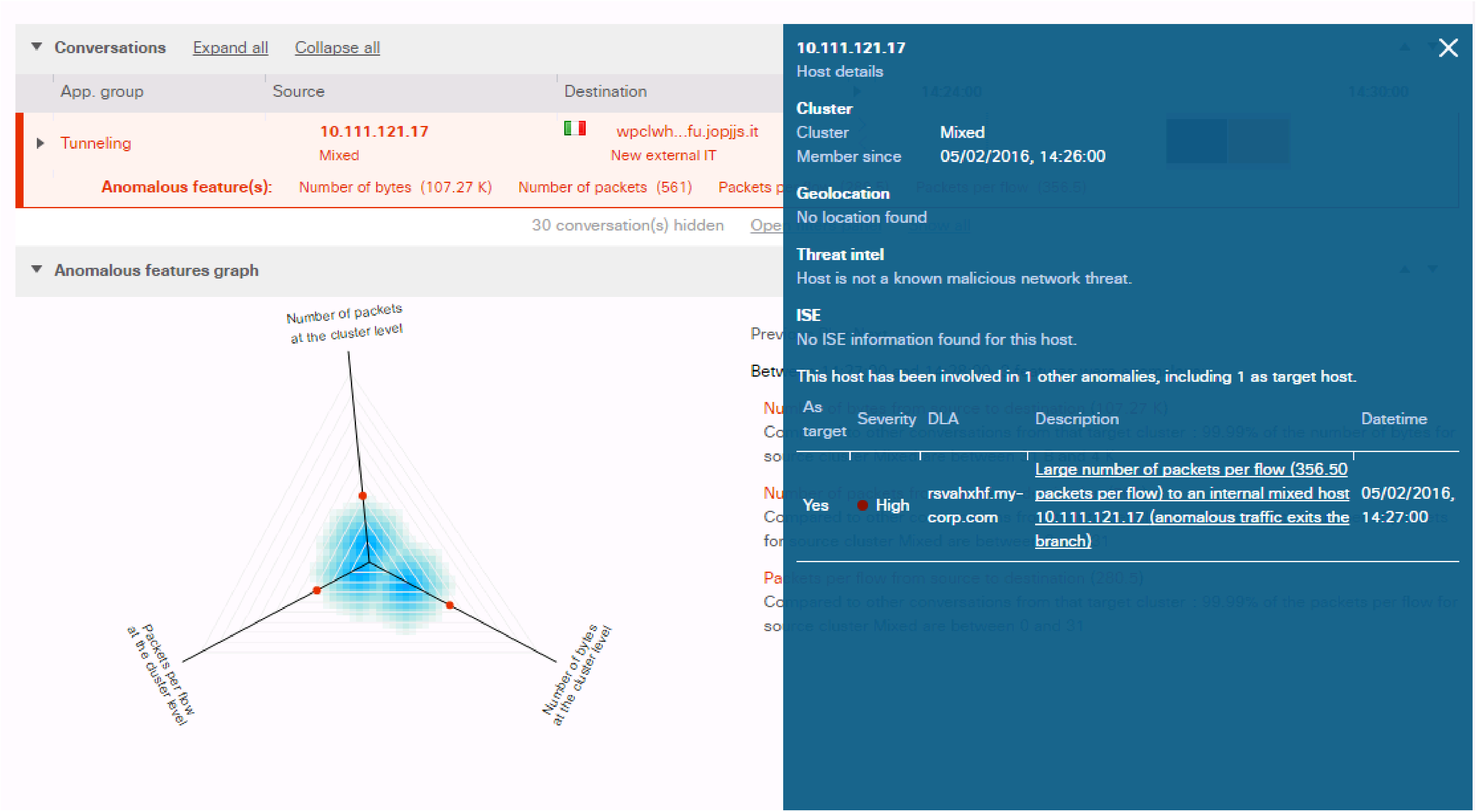
Between 14:27:00 and 14:28:00, 3 features were anomalous:

Number of bytes from source to destination (107.27 K)
Compared to other conversations from that target cluster : 99.99% of the number of bytes for source cluster Mixed are between 31 B and 4 K

Number of packets from source to destination (561)
Compared to other conversations from that target cluster : 99.99% of the number of packets for source cluster Mixed are between 0 and 31

Packets per flow from source to destination (280.5)
Compared to other conversations from that target cluster : 99.99% of the packets per flow for source cluster Mixed are between 0 and 31

Inbox – Conversations - Host Details



▼ Conversations
Expand all
Collapse all
App. group
Source
Destination
▶ Tunneling
Anomalous feature(s):
Number of bytes (107.27 K)
Number of packets (561)
Packets p
30 conversation(s) hidden
▼ Anomalous features graph
Number of packets at the cluster level
Packets per flow at the cluster level
Number of bytes at the cluster level

Tunneling	10.111.121.17 Mixed	wpclwh...fu.jopjjs.it New external IT

10.111.121.17

Host details

Cluster

Cluster	Mixed
Member since	05/02/2016, 14:26:00

Geolocation

No location found

Threat intel

Host is not a known malicious network threat.

ISE

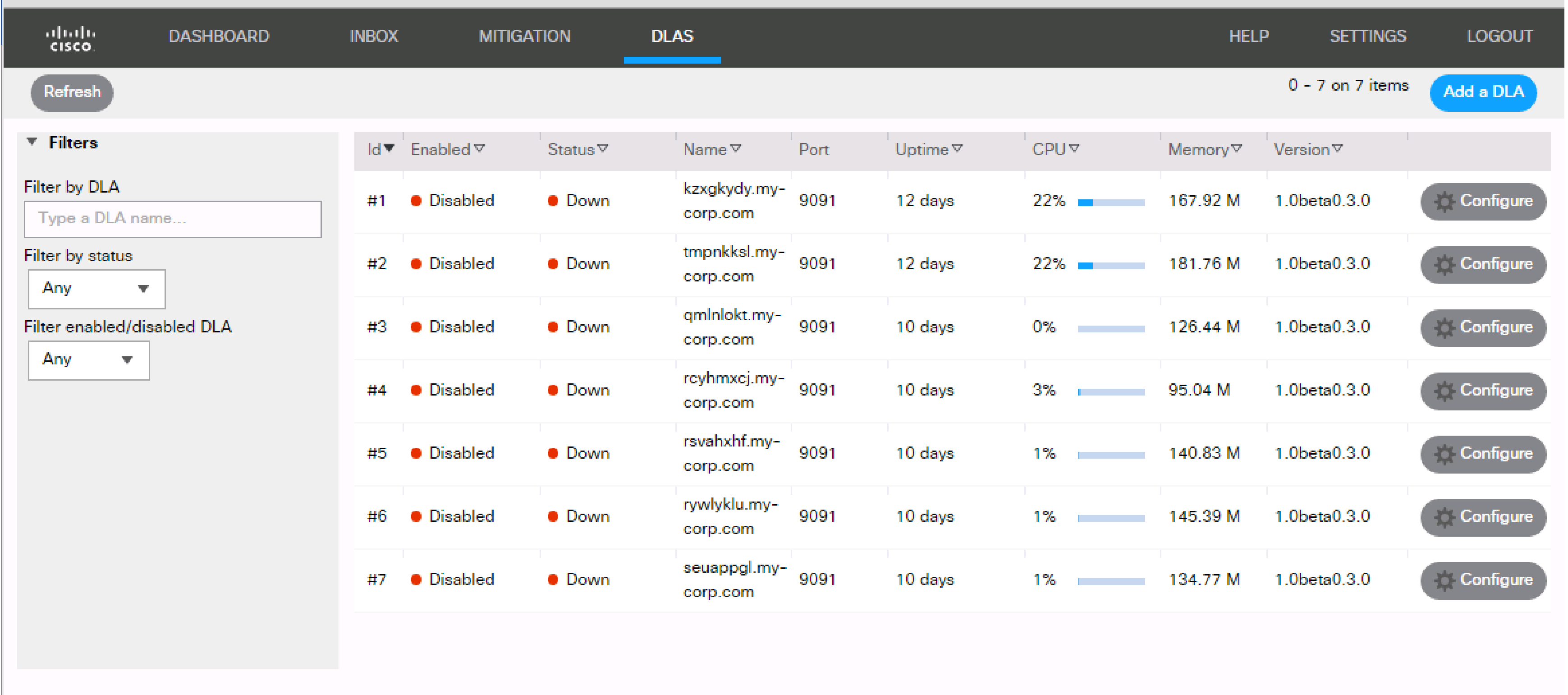
No ISE information found for this host.

This host has been involved in 1 other anomalies, including 1 as target host.

As target	Severity	DLA	Description	Datetime
Yes	● High	rsvahxhf.my-corp.com	Large number of packets per flow (356.50 packets per flow) to an internal mixed host 10.111.121.17 (anomalous traffic exits the branch)	05/02/2016, 14:27:00

SLNL Manger DLA view

Learning Agents – View All



0 - 7 on 7 items

▼ Filters

Filter by DLA: Type a DLA name...

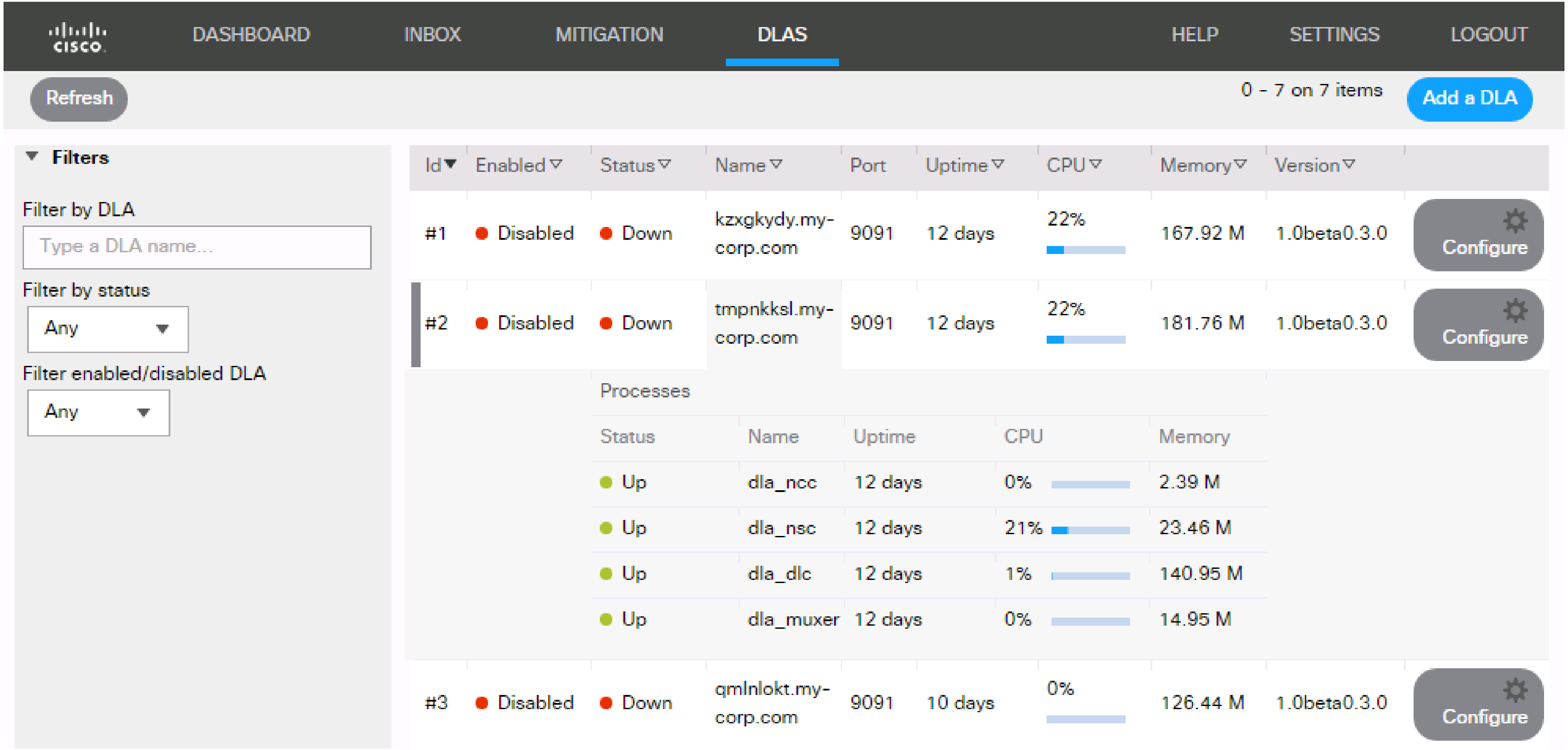
Filter by status: Any ▼

Filter enabled/disabled DLA: Any ▼

Id▼	Enabled ▽	Status ▽	Name ▽	Port	Uptime ▽	CPU ▽	Memory ▽	Version ▽	
#1	● Disabled	● Down	kzxgkydy.my-corp.com	9091	12 days	22%	167.92 M	1.0beta0.3.0	Configure
#2	● Disabled	● Down	tmpnkksl.my-corp.com	9091	12 days	22%	181.76 M	1.0beta0.3.0	Configure
#3	● Disabled	● Down	qmlnlokt.my-corp.com	9091	10 days	0%	126.44 M	1.0beta0.3.0	Configure
#4	● Disabled	● Down	rcyhmxcj.my-corp.com	9091	10 days	3%	95.04 M	1.0beta0.3.0	Configure
#5	● Disabled	● Down	rsvahxhf.my-corp.com	9091	10 days	1%	140.83 M	1.0beta0.3.0	Configure
#6	● Disabled	● Down	rywlyklu.my-corp.com	9091	10 days	1%	145.39 M	1.0beta0.3.0	Configure
#7	● Disabled	● Down	seuappgl.my-corp.com	9091	10 days	1%	134.77 M	1.0beta0.3.0	Configure

SLNL Manager Agent Expanded

Agent Expanded View



0 - 7 on 7 items

Filters

Filter by DLA: Type a DLA name...

Filter by status: Any

Filter enabled/disabled DLA: Any

Id	Enabled	Status	Name	Port	Uptime	CPU	Memory	Version
#1	● Disabled	● Down	kzxgkydy.my-corp.com	9091	12 days	22%	167.92 M	1.0beta0.3.0
#2	● Disabled	● Down	tmpnkksl.my-corp.com	9091	12 days	22%	181.76 M	1.0beta0.3.0
#3	● Disabled	● Down	qmlnlokt.my-corp.com	9091	10 days	0%	126.44 M	1.0beta0.3.0

Processes

Status	Name	Uptime	CPU	Memory
● Up	dla_ncc	12 days	0%	2.39 M
● Up	dla_nsc	12 days	21%	23.46 M
● Up	dla_dlc	12 days	1%	140.95 M
● Up	dla_muxer	12 days	0%	14.95 M

StealthWatch (Lancope) VS SLNL

	StealthWatch	**Stealthwatch Learning Network License**
Target Network	Enterprise network	Branch network
Data Source	Aggregates data from many devices	Processes data from each router separately
Contexts	NetFlow, Syslog	NetFlow, NBAR, DPI
Database	IP Connectivity Database	Detected Anomaly Database
Detection	Analytics & Rules	Distributed Machine Learning
Packet Capture	Triggered On Demand	Automatic
Integration	ISE (identity & mitigation), AD integration	ISE (identity only) Integration
Threat Intel Feed	SLIC Feed	TBD Talos Threat Feed
Physical/Virtual	Delivered as Appliance or VM	ISR 44xx & OVA for LXC or UCS-E

SLNL - Resources

For Your Reference

- Cisco Stealthwatch Learning Network License Configuration Guide
  http://www.cisco.com/c/en/us/td/docs/security/sln/configuration/guide/Learning_Network_License_Configuration_Guide.html

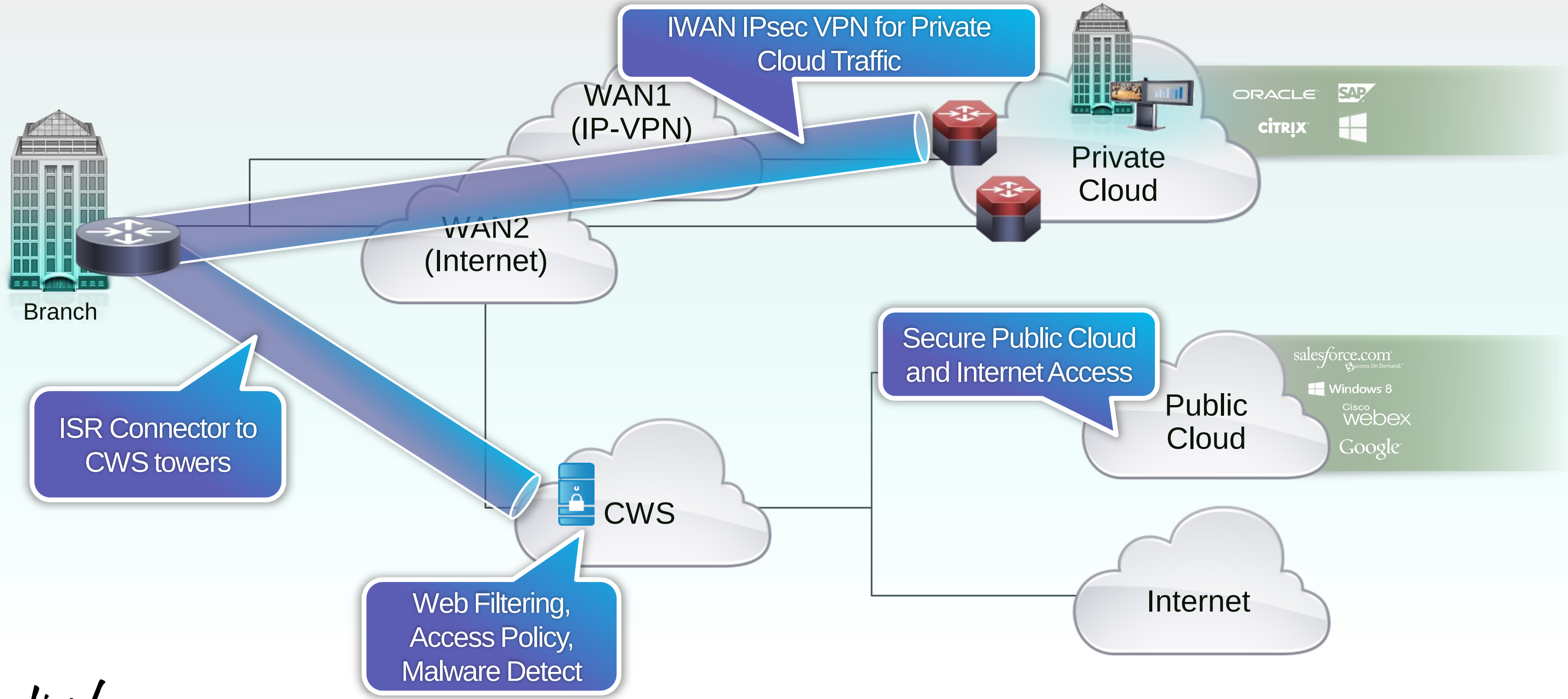
- Cisco Stealthwatch Learning Network License UCS E-Series Server Installation
  http://www.cisco.com/c/en/us/td/docs/security/sln/installation/guide/Learning_Network_License_UCS_E_Server_Installation_Guide.html

- Cisco Stealthwatch Learning Network License Virtual Service Installation Guide
  http://www.cisco.com/c/en/us/td/docs/security/sln/installation/guide/Learning_Network_License_Virtual_Service_Installation_Guide.html

Agenda

- Zone Based Firewall
- Snort IPS
- Cisco Umbrella (OpenDNS)
- Firepower
- Stealthwatch Learning Network License (SLNL)
- Cloud Web Security (CWS)

Cloud Web Security (CWS)


IWAN IPsec VPN for Private Cloud Traffic
WAN1 (IP-VPN)
Private Cloud
ORACLE
SAP
CITRIX
WAN2 (Internet)
Branch
ISR Connector to CWS towers
Secure Public Cloud and Internet Access
Public Cloud
salesforce.com
Success On Demand.
Windows 8
Cisco webex
Google
CWS
Web Filtering, Access Policy, Malware Detect
Internet

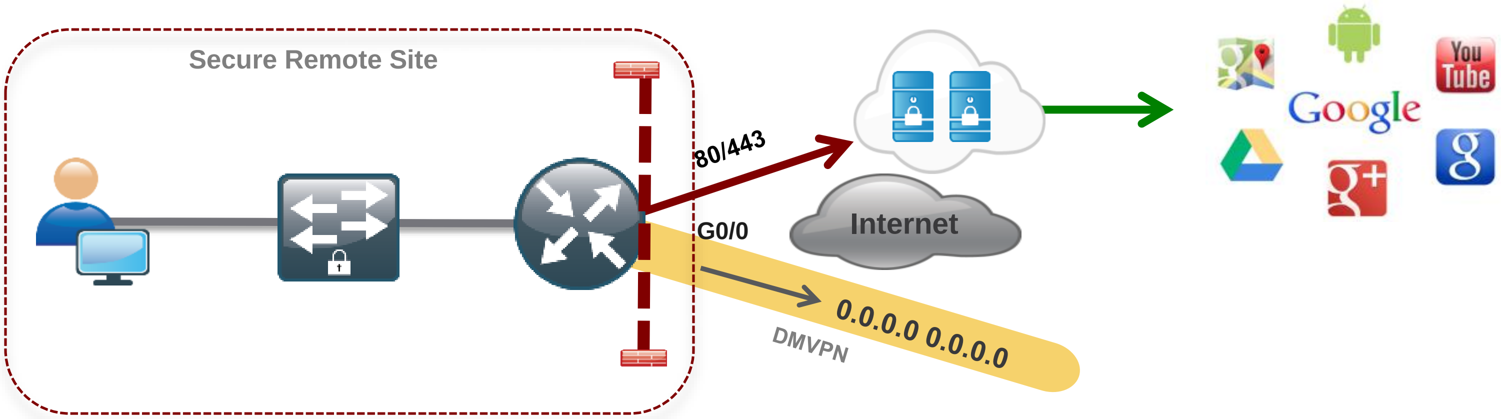
CWS - Appendix

For Your Reference

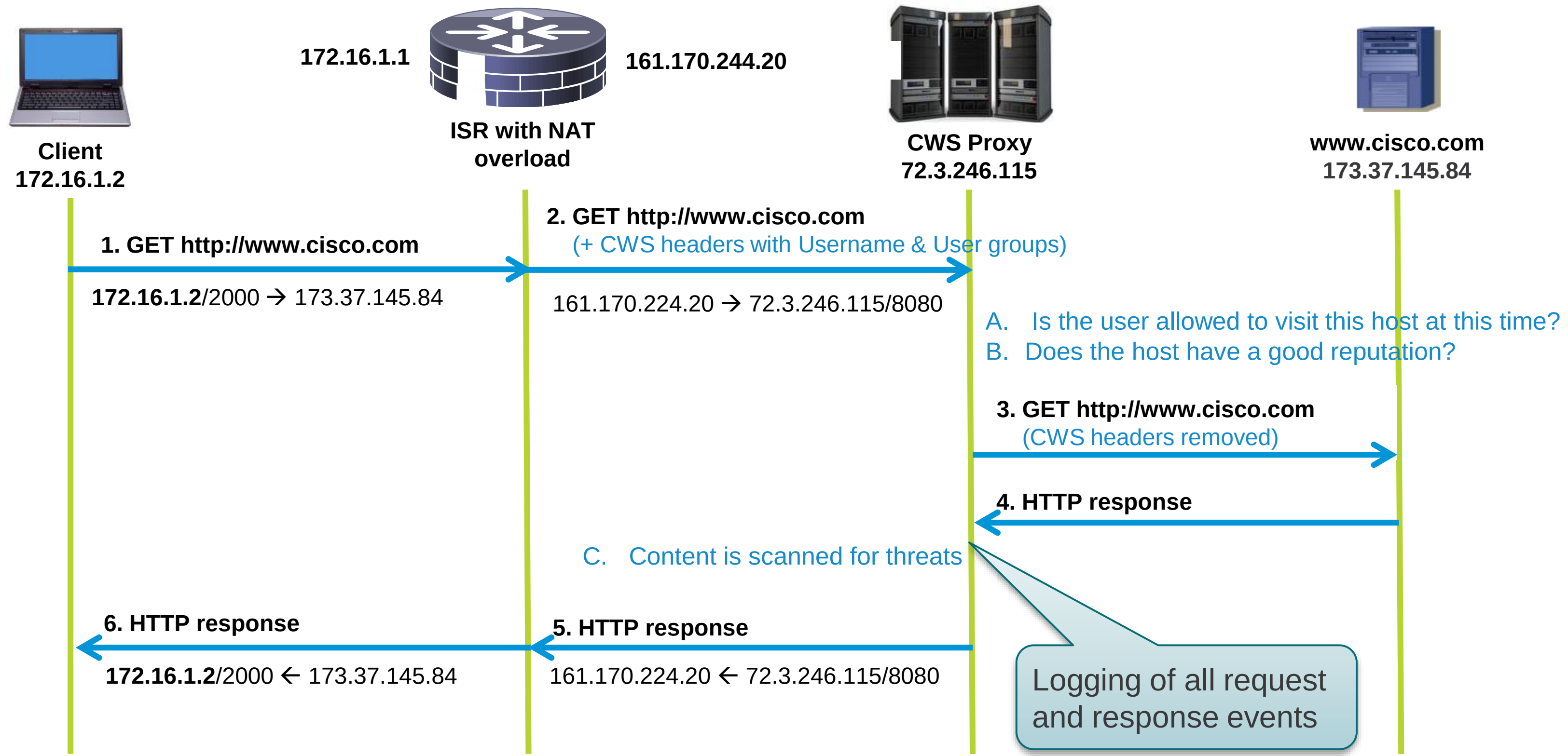
- CWS – Cloud Web Security
- IWAN – Intelligent WAN
- CSR - Cloud Services Router
- RRI – Reverse Route Injection
- L4F – Layer 4 Forwarding
- AMP – Advance Malware Protection
- WL – White Listing

CWS - Securing DIA

- Connector is integrated into Cisco **ISR G2** Router as a **Proxy**
- Connector is integrated into Cisco **ISR 4K** Router as a **Tunnel**
- Redirection of web traffic happens transparently on the remote-site router
- Tower Redundancy
- Single point of policy management and monitoring



CWS – Proxy Mode Packet Flow



Client
172.16.1.2

172.16.1.1

ISR with NAT
overload

161.170.244.20

CWS Proxy
72.3.246.115

www.cisco.com
173.37.145.84

1. GET http://www.cisco.com

172.16.1.2/2000 → 173.37.145.84

2. GET http://www.cisco.com
(+ CWS headers with Username & User groups)

161.170.224.20 → 72.3.246.115/8080

A. Is the user allowed to visit this host at this time?
B. Does the host have a good reputation?

3. GET http://www.cisco.com
(CWS headers removed)

4. HTTP response

C. Content is scanned for threats

5. HTTP response

161.170.224.20 ← 72.3.246.115/8080

6. HTTP response

172.16.1.2/2000 ← 173.37.145.84

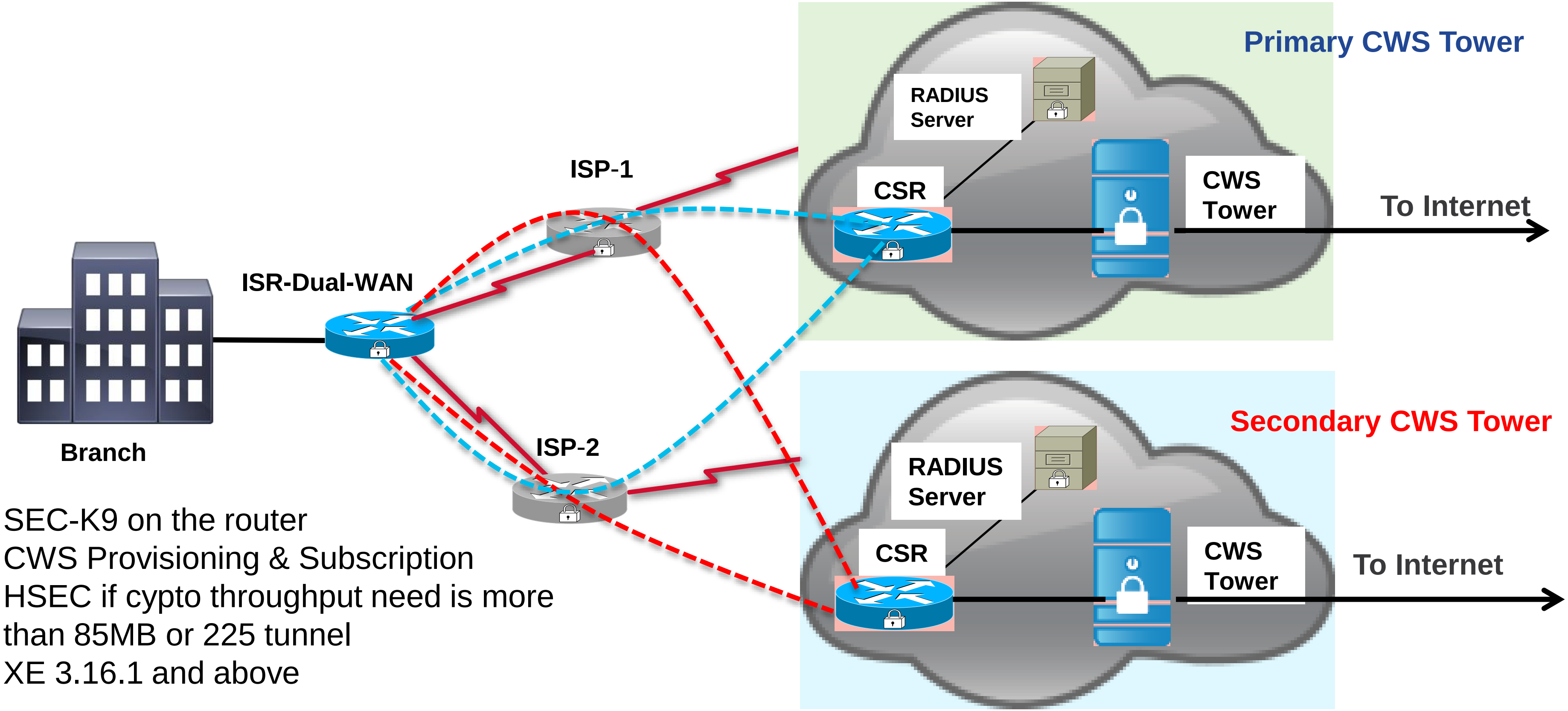
Logging of all request and response events

CWS – ISR G2 Proxy mode Configuration

Step 3 – Optional Whitelisting

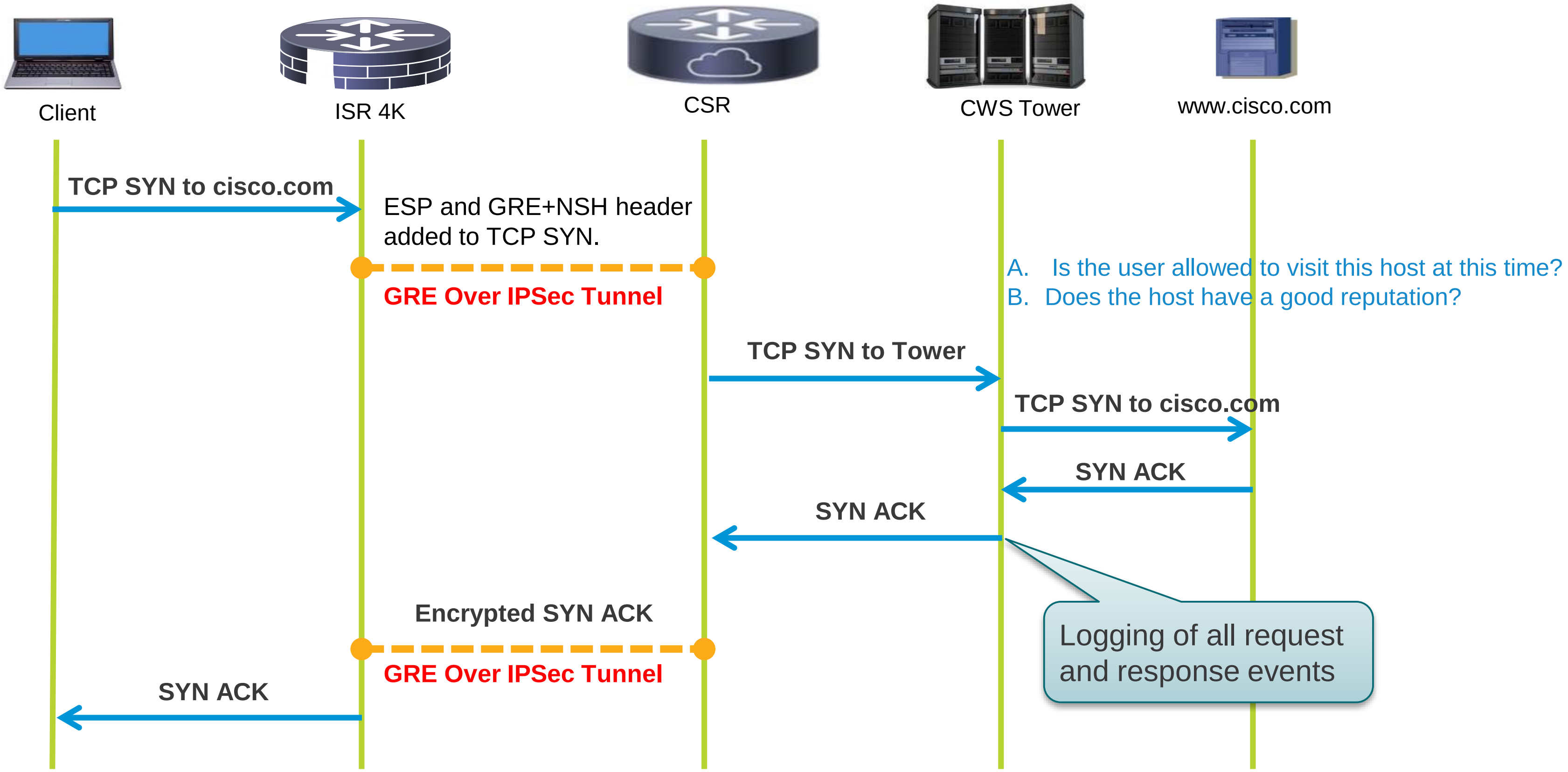
```
parameter-map type regex allowed-pattern
   pattern .*.cisco.com
   pattern .*.amazon.com
ip access-list extended inside-nw
   permit ip 172.16.1.0 0.0.0.255 any
cws whitelisting
   whitelist header host regex allowed-pattern
   whitelist acl inside-nw
```

CWS – ISR 4K Tunnel Mode



SEC-K9 on the router
CWS Provisioning & Subscription
HSEC if cypto throughput need is more than 85MB or 225 tunnel
XE 3.16.1 and above

CWS – ISR 4K Tunnel mode Packet Flow



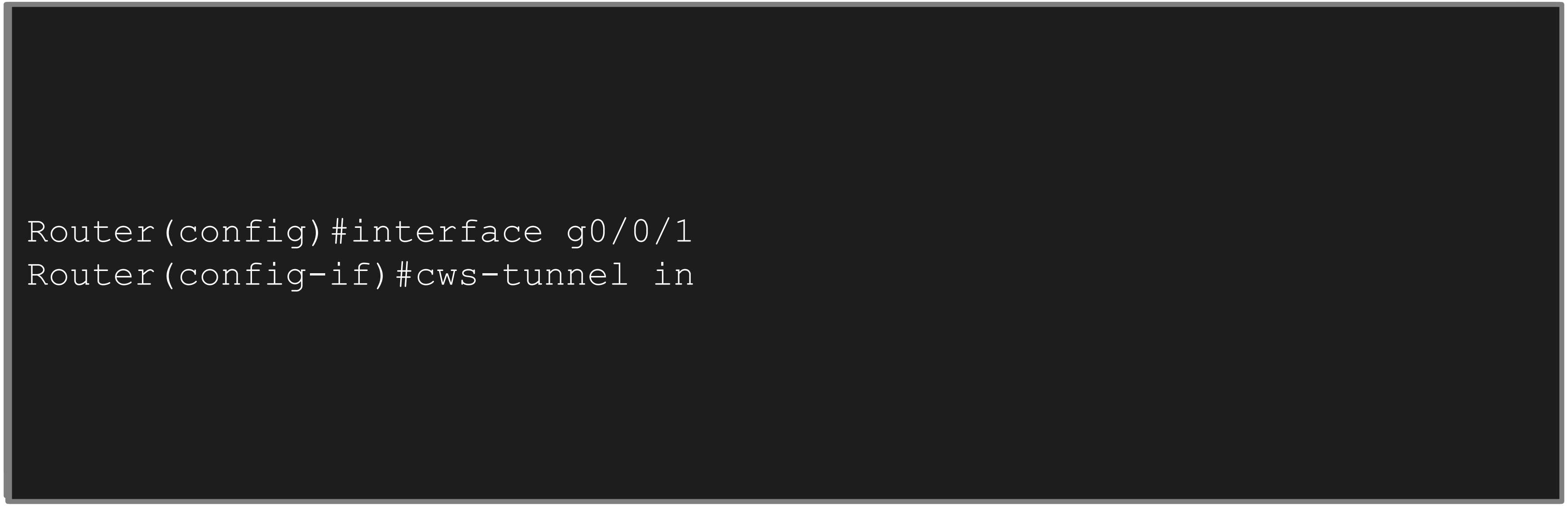
ESP and GRE+NSH header added to TCP SYN.

A. Is the user allowed to visit this host at this time?
B. Does the host have a good reputation?

Logging of all request and response events

CWS – ISR 4K Tunnel mode Configuration

Step 6 - Apply CWS IN on the LAN facing interface



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

CWS – ISR 4K Tunnel Mode Configuration

Step. 1 Import Certificate

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

Router(config)#cry pki authenticate cws-trustpoint
```

Step.2 Define a redirect list

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

Step.3 Define a whitelist (optional)

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

Step.4 Parameter Map

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

Step.5 Apply CWS OUT

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

Step.6 Apply CWS IN

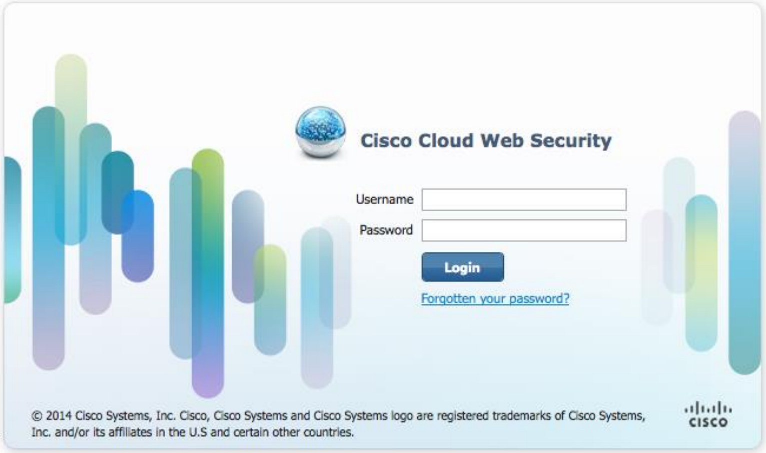
```
Router(config)#interface g0/0/1
Router(config-if)#cws-tunnel in
```

CWS - Proxy VS Tunnel Connector

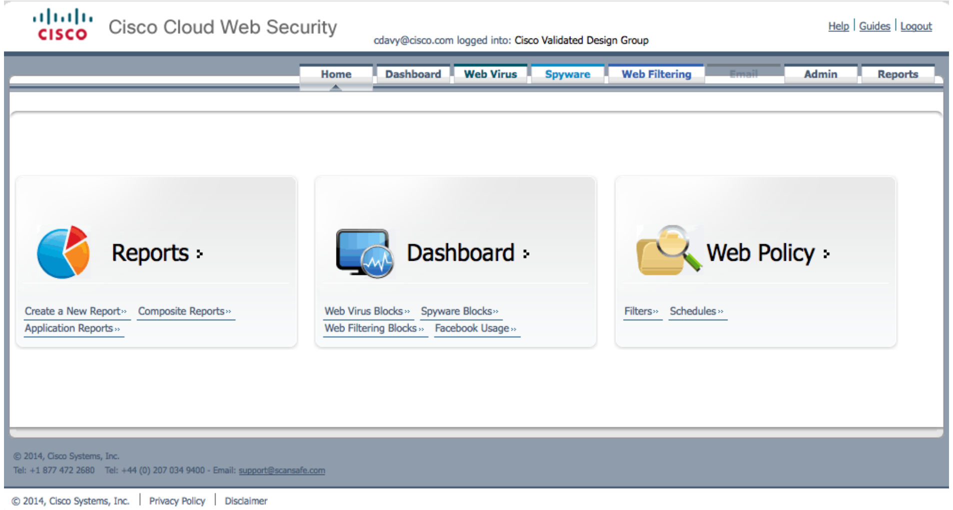
Features	Proxy ISR-G2 (IOS)	Tunnel ISR-4K (XE)
Redirection	Proxy	Tunnel
Telemetry	Yes	No
Tower Pooling	Yes	Through Tunnel Keepalives
MetaData	X-Scansafe Headers	NSH (Network Services Headers)
Whitelisitng	ACL & HTTP Headers Based	ACL & Domain Based
Authentication	Yes	Yes (Controlled Availability)*
Default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

* http://www.cisco.com/c/dam/en/us/products/collateral/security/cloud-web-security/solution_overview_c96-721282.pdf

Cloud Web Security – Portal Policy Configuration



© 2014 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S and certain other countries.

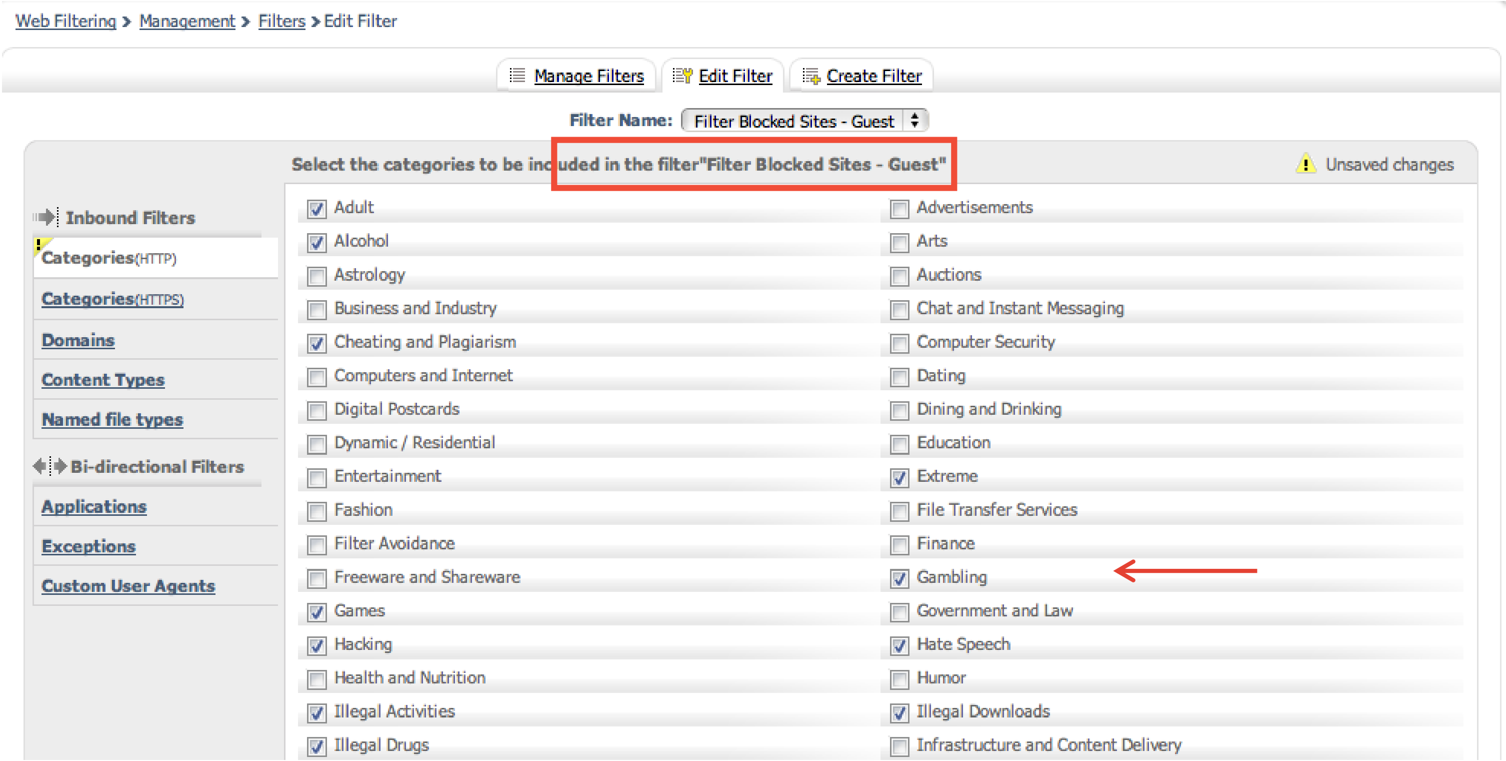


cdavy@cisco.com logged into: Cisco Validated Design Group

© 2014, Cisco Systems, Inc.
Tel: +1 877 472 2680 Tel: +44 (0) 207 034 9400 - Email: support@scansafe.com

© 2014, Cisco Systems, Inc. | Privacy Policy | Disclaimer

Cloud Web Security – Portal Policy Configuration



Web Filtering > Management > Filters > Edit Filter

Manage Filters | Edit Filter | Create Filter

Filter Name: Filter Blocked Sites - Guest

Select the categories to be included in the filter"Filter Blocked Sites - Guest"

Unsaved changes

Inbound Filters

- **Categories**(HTTP)
- **Categories**(HTTPS)
- **Domains**
- **Content Types**
- **Named file types**

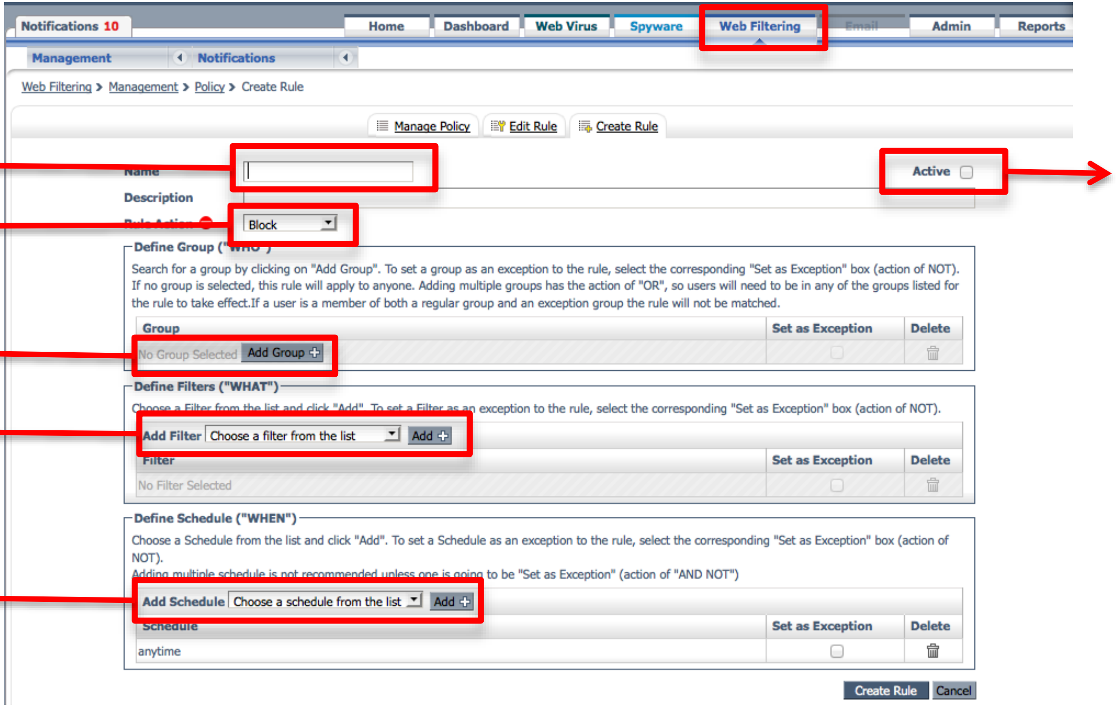
Bi-directional Filters

- **Applications**
- **Exceptions**
- **Custom User Agents**

☑ Adult
☑ Alcohol
□ Astrology
□ Business and Industry
☑ Cheating and Plagiarism
□ Computers and Internet
□ Digital Postcards
□ Dynamic / Residential
□ Entertainment
□ Fashion
□ Filter Avoidance
□ Freeware and Shareware
☑ Games
☑ Hacking
□ Health and Nutrition
☑ Illegal Activities
☑ Illegal Drugs

□ Advertisements
□ Arts
□ Auctions
□ Chat and Instant Messaging
□ Computer Security
□ Dating
□ Dining and Drinking
□ Education
☑ Extreme
□ File Transfer Services
□ Finance
☑ Gambling
□ Government and Law
☑ Hate Speech
□ Humor
☑ Illegal Downloads
□ Infrastructure and Content Delivery

Cloud Web Security – Portal Policy Configuration



Web Filtering > Management > Policy > Create Rule

Name
Active ☐
Description
Rule Action: Block

Define Group ("WHO")

Search for a group by clicking on "Add Group". To set a group as an exception to the rule, select the corresponding "Set as Exception" box (action of NOT). If no group is selected, this rule will apply to anyone. Adding multiple groups has the action of "OR", so users will need to be in any of the groups listed for the rule to take effect.If a user is a member of both a regular group and an exception group the rule will not be matched.

Group	Set as Exception	Delete
No Group Selected Add Group	☐	🗑

Define Filters ("WHAT")

Choose a Filter from the list and click "Add". To set a Filter as an exception to the rule, select the corresponding "Set as Exception" box (action of NOT).

Add Filter: Choose a filter from the list — Add

Filter	Set as Exception	Delete
No Filter Selected	☐	🗑

Define Schedule ("WHEN")

Choose a Schedule from the list and click "Add". To set a Schedule as an exception to the rule, select the corresponding "Set as Exception" box (action of NOT).
Adding multiple schedule is not recommended unless one is going to be "Set as Exception" (action of "AND NOT")

Add Schedule: Choose a schedule from the list — Add

Schedule	Set as Exception	Delete
anytime	☐	🗑

Create Rule | Cancel

Policy

Action

Who

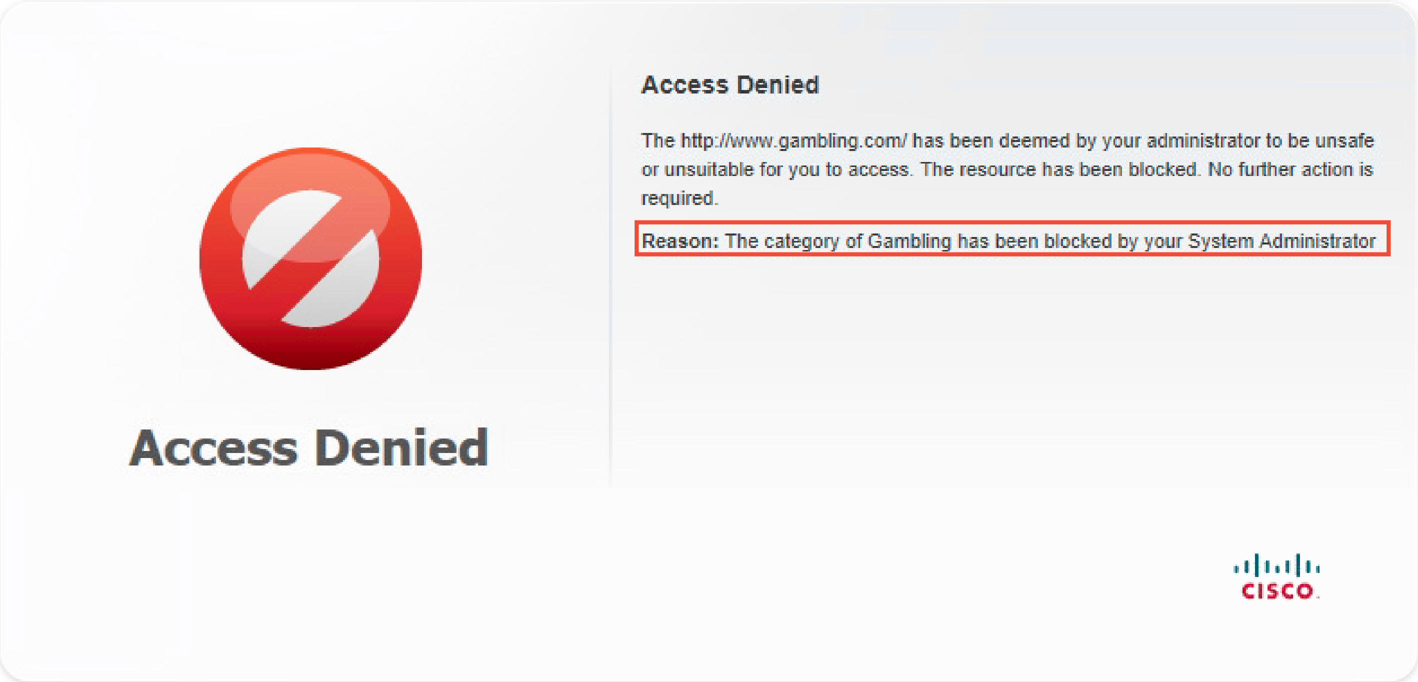
What

When

Activate the rule

Cloud Web Security – Portal Policy Configuration

CWS Guest Policy – Guest Group is not able to browse Gambling sites



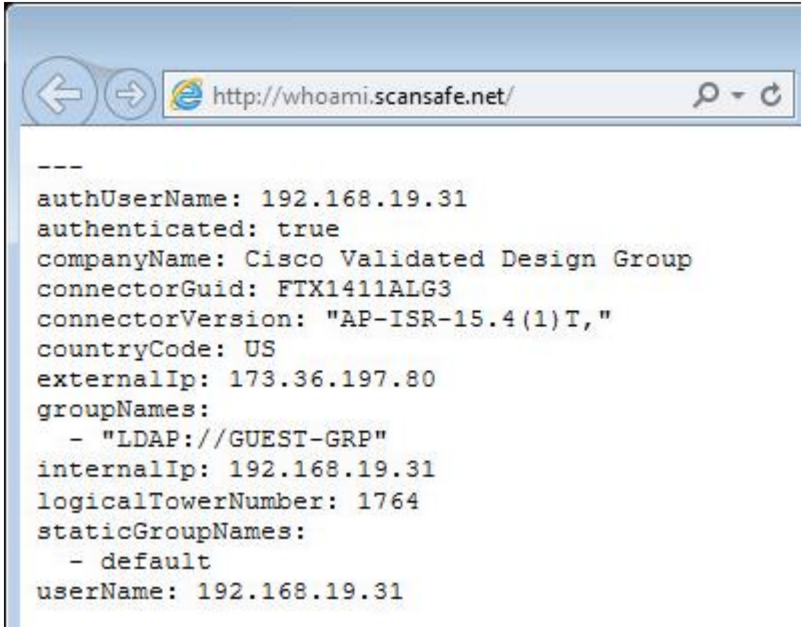
Access Denied

The http://www.gambling.com/ has been deemed by your administrator to be unsafe or unsuitable for you to access. The resource has been blocked. No further action is required.

Reason: The category of Gambling has been blocked by your System Administrator

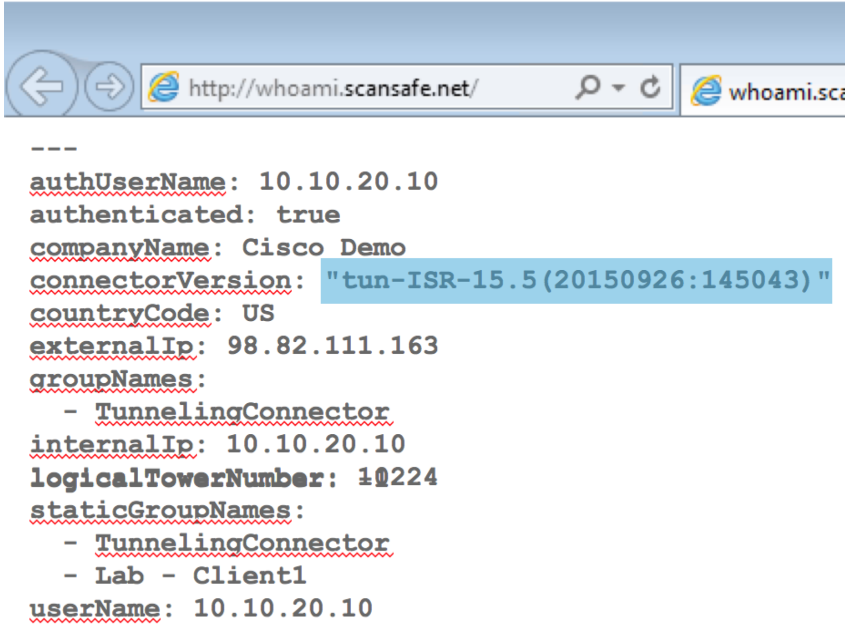
Cloud Web Security – verify with whoami output

ISR G2 Whoami output



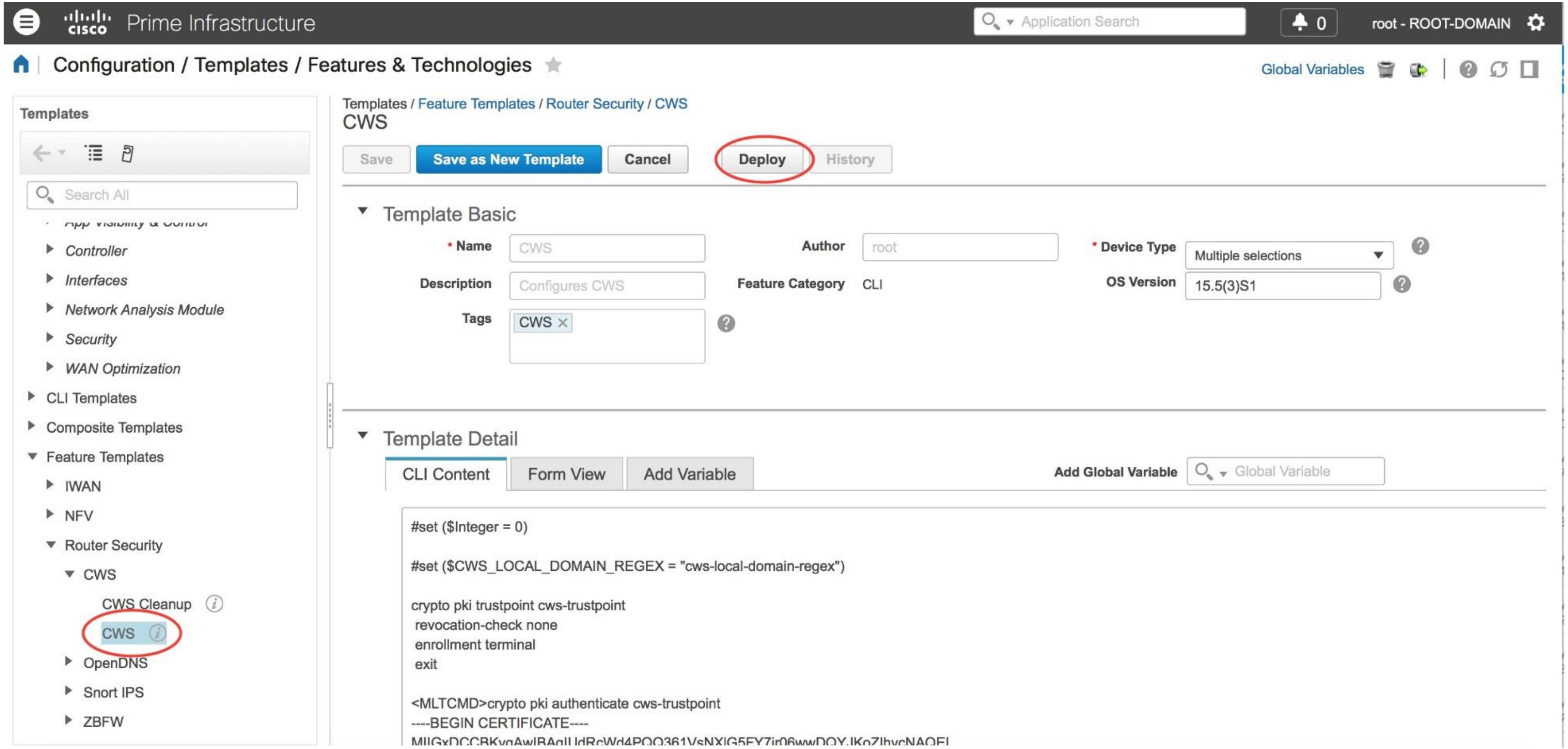
```
---
authUserName: 192.168.19.31
authenticated: true
companyName: Cisco Validated Design Group
connectorGuid: FTX1411ALG3
connectorVersion: "AP-ISR-15.4(1)T,"
countryCode: US
externalIp: 173.36.197.80
groupNames:
  - "LDAP://GUEST-GRP"
internalIp: 192.168.19.31
logicalTowerNumber: 1764
staticGroupNames:
  - default
userName: 192.168.19.31
```

ISR 4K Whoami output



```
---
authUserName: 10.10.20.10
authenticated: true
companyName: Cisco Demo
connectorVersion: "tun-ISR-15.5(20150926:145043)"
countryCode: US
externalIp: 98.82.111.163
groupNames:
  - TunnelingConnector
internalIp: 10.10.20.10
logicalTowerNumber: 10224
staticGroupNames:
  - TunnelingConnector
  - Lab - Client1
userName: 10.10.20.10
```

CWS – Provisioning (Prime Infrastructure 3.1 and above)



* Name	CWS	Author	root	* Device Type	Multiple selections
Description	Configures CWS	Feature Category	CLI	OS Version	15.5(3)S1
Tags	CWS				

```
#set ($Integer = 0)

#set ($CWS_LOCAL_DOMAIN_REGEX = "cws-local-domain-regex")

crypto pki trustpoint cws-trustpoint
 revocation-check none
 enrollment terminal
 exit

<MLTCMD>crypto pki authenticate cws-trustpoint
----BEGIN CERTIFICATE----
MIIGxDCCBKygAwIBAgIUdRcWd4PQQ361VsNXIG5FY7ir06wwDQYJKoZIhvcNAQEL
```

CWS – Resources

For Your Reference

- Configuration Guide: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_cws/configuration/xe-16/sec-data-cws-xe-16-book/cws-tunneling.html
- CWS on ISR 4K Step-by-Step Configuration Guide: https://supportforums.cisco.com/document/12713171/isr-cws-tunnel-based-redirection-step-step-configuration
- CWS on ISR 4K FAQ: https://supportforums.cisco.com/document/12949576/cisco-cloud-web-security-cws-tunnel-connector-isr-4k-faq
- **CWS EOL announcement** http://www.cisco.com/c/en/us/products/collateral/security/cloud-web-security/eos-eol-notice-c51-738257.html

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.
CWS	On the ISR 4K routers, http and https traffic is redirected to the cloud via GRE over IPSec Tunnel to provide category and reputation based granular content filtering. Supports VRF.

Router-security@cisco.com

Complete Your Online Session Evaluation

- Give us your feedback to be entered into a Daily Survey Drawing. A daily winner will receive a $750 gift card.
- 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.

Cisco live!

Continue Your Education

- Demos in the Cisco campus
- Walk-in Self-Paced Labs
- Lunch & Learn
- Meet the Engineer 1:1 meetings
- Related sessions
    - BRKSEC-2809 Deciphering Malware's Use of TLS (without Decryption)
    - BRKSEC-2010 Talos Insights: The State of Cyber Security
    - LABSEC-2006 Cisco Umbrella (OpenDNS) - Walk-In Self-Paced
    - BRKSEC-3007 Advanced IOS Security

Q & A

Thank you

cisco

You’re

iT

Cisco live!