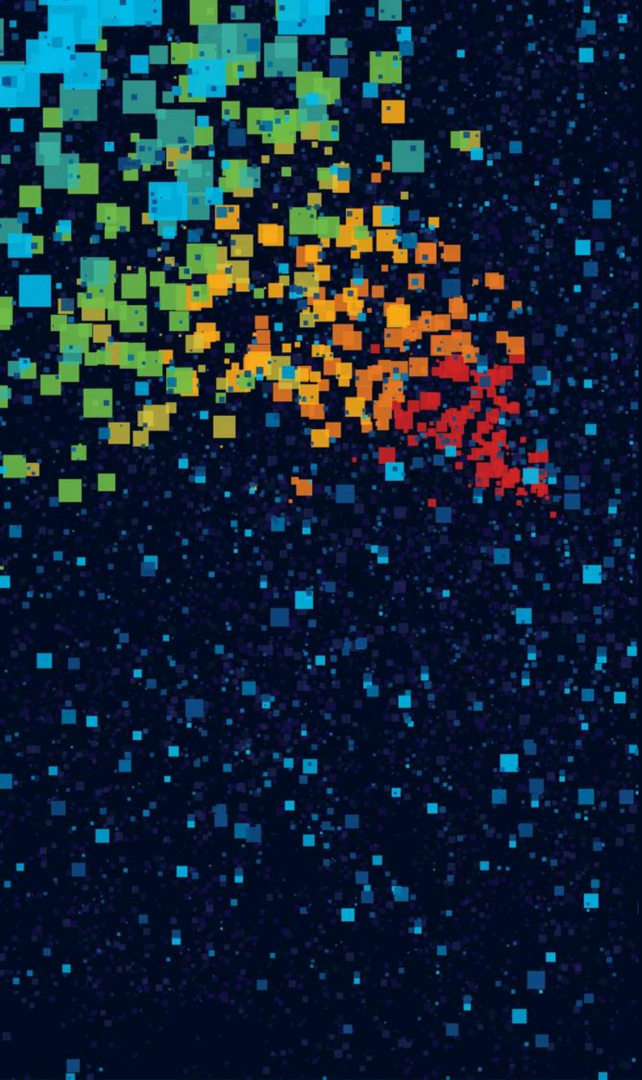
Интегрированные функции безопасности и унифицированных коммуникаций. Лучшие практики и рекомендации по настройке. Часть 1

Дмитрий Демин
Системный архитектор, CISSP

22.04.2021



Agenda

- Device Identity
- Security Baseline
- Data Plane Security
  - Zone Based Firewall
  - Snort IPS
  - URL Filtering
  - Cisco Umbrella Integration
  - Firepower Threat Defense for ISR
  - Encrypted Traffic Analytics (ETA)
- Control Plane Security
- Management Plane Security
- IOS-XE VS XE SD-WAN
- Management
- Appendex: NAT

Cisco Enterprise Routing Portfolio

Branch

ISR 900

- Fixed and fan less
- IOS Classic based

ISR 1000

- Integrated wired and wireless access
- PoE/PoE+

ISR 4000

- WAN and voice module flexibility
- Compute with UCS E
- Integrated Security stack
- WAN Optimization

vEdge 100

- 4G LTE & Wireless

vEdge 1000 & 2000

- Fixed/Pluggable Module

Aggregation

ASR 1000

- Hardware and software redundancy
- High-performance service with hardware assist

vEdge 5000

- Modular
- RPS

SD-WAN

Virtual and Cloud

Cisco ENCS

- Service chaining virtual functions
- Options for WAN connectivity
- Open for 3rd party services & apps

CSR 1000V

- Cisco DNA virtualization
- Extend enterprise routing, security & management to cloud

Device Identity

Device Identity - Appendix

FYI

- RNG – Random Number Generator
- ASLR – Address Space Layout Randomization
- BOSC - Built-in Object Size Checking
- X-Space – Execution Space
- TAm – Trust Anchor Module
- RTD – Run Time Defense
- PKI – Public Key Infrastructure

Foundations of Trustworthy Technologies

Secure Boot of Signed Images

- Helps prevent malicious code from booting on a Cisco platform
- Automated integrity checks
- Monitors startup process and shuts down if compromised
- Faster identification of threats

Trust Anchor module (TAm)

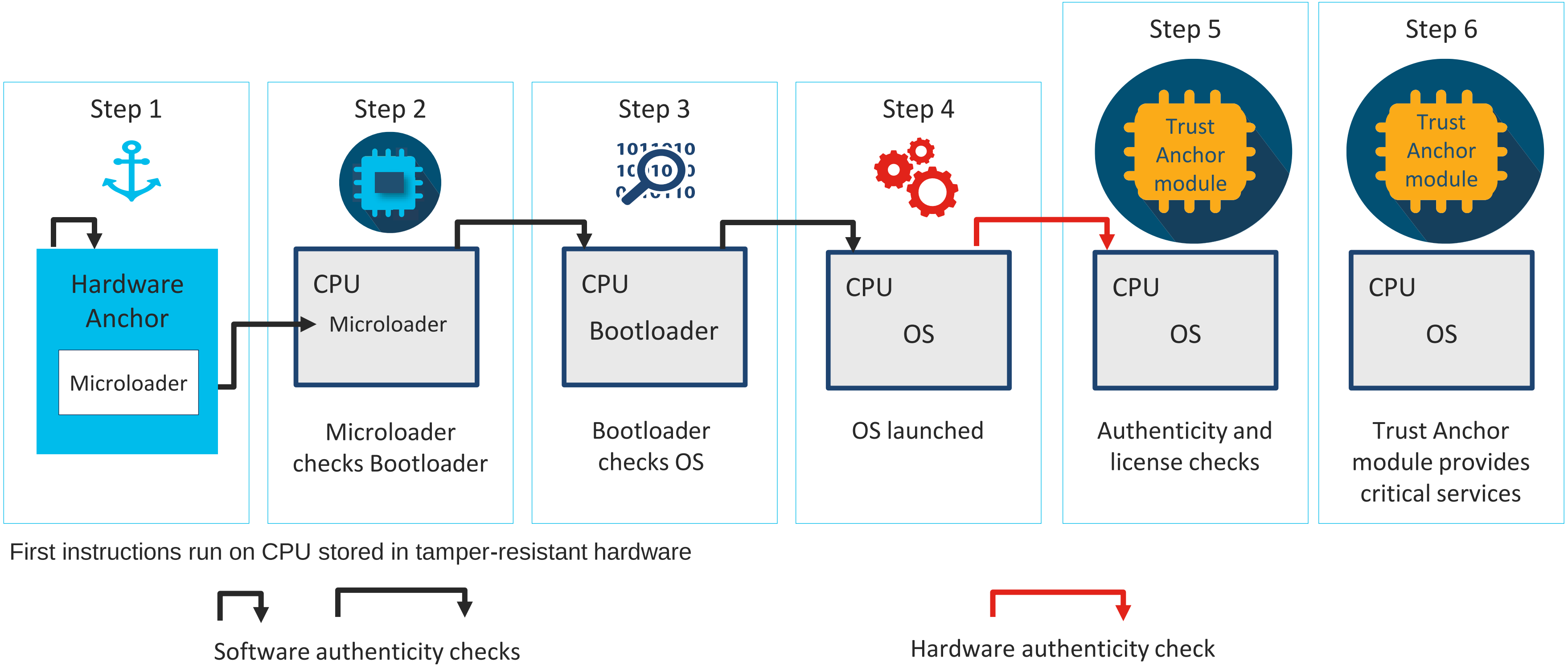
- Tamper-resistant chip with X.509 cert installed at manufacturing
- Provides unique device identity and anti-counterfeit protections
- Secure, non-volatile on-board storage and RNG/crypto services
- Enables zero-touch provisioning; minimizes deployment costs

Runtime Defenses (RTD)

- Protects against injection of malicious code into running code
- Makes it harder for attackers to exploit vulnerabilities in running software
- Runtime technologies include ASLR, BOSC, and X-Space

Trustworthy technologies enhance the security and resilience of Cisco solutions

Hardware-Anchored Secure Boot



Step 1

Hardware Anchor

Microloader

Step 2

CPU

Microloader

Microloader checks Bootloader

Step 3

CPU

Bootloader

Bootloader checks OS

Step 4

CPU

OS

OS launched

Step 5

Trust Anchor module

CPU

OS

Authenticity and license checks

Step 6

Trust Anchor module

CPU

OS

Trust Anchor module provides critical services

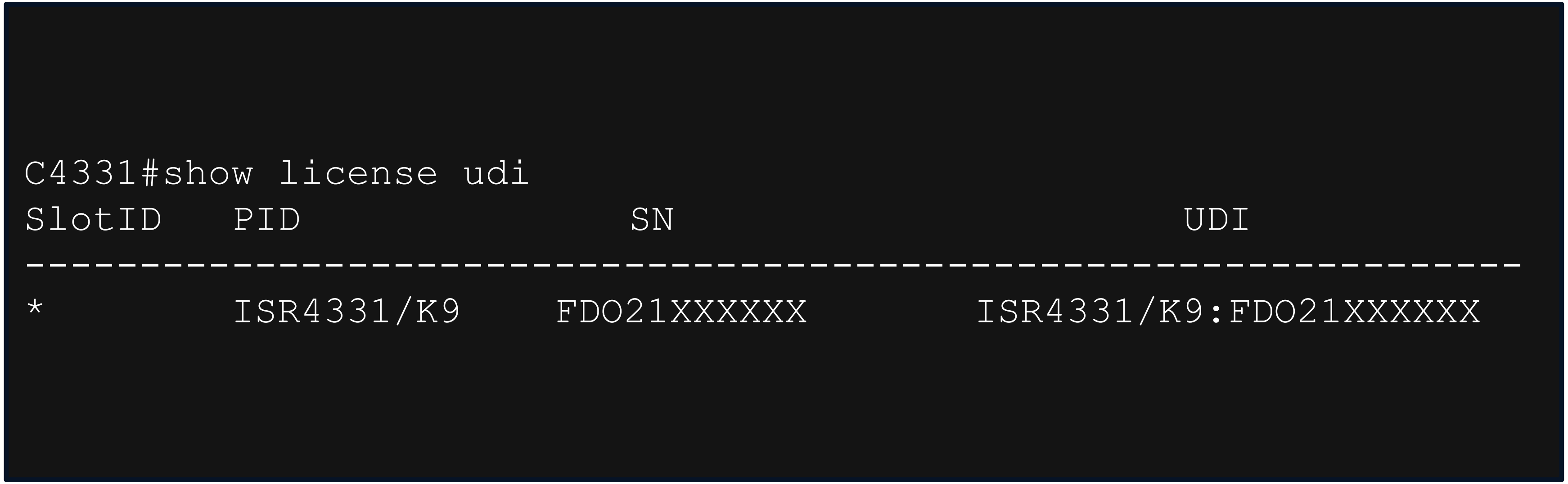
First instructions run on CPU stored in tamper-resistant hardware

Software authenticity checks

Hardware authenticity check

Cisco hardware-anchored secure boot verifies platform authenticity and integrity. Provides a secure device identity for authentication. Helps prevent inauthentic or compromised code from booting on a Cisco platform.

Secure (UDI) = SUDI



```
C4331#show license udi
SlotID   PID              SN                      UDI
-----------------------------------------------------------------
*        ISR4331/K9    FDO21XXXXXX       ISR4331/K9:FDO21XXXXXX
```

Trust Anchor module (TAm)

TAm Features:

- Tamper-resistant chip
- Hardware-anchored device identity
- Secure onboard storage
- Built-in crypto functions including random number generator (RNG)

Secure Unique Device ID (SUDI) X.509 Certificate = Device’s Identity

- Manufacturer-installed certificate
- Hardware serial numbers
- Device-unique public key

Key Use Cases

- Verifying the integrity of a device’s identity
- Onboarding a new device – Secure Zero Touch Provisioning
- Secure enrollment within an organization's PKI

Security Baseline

FYI

Hardening Guides

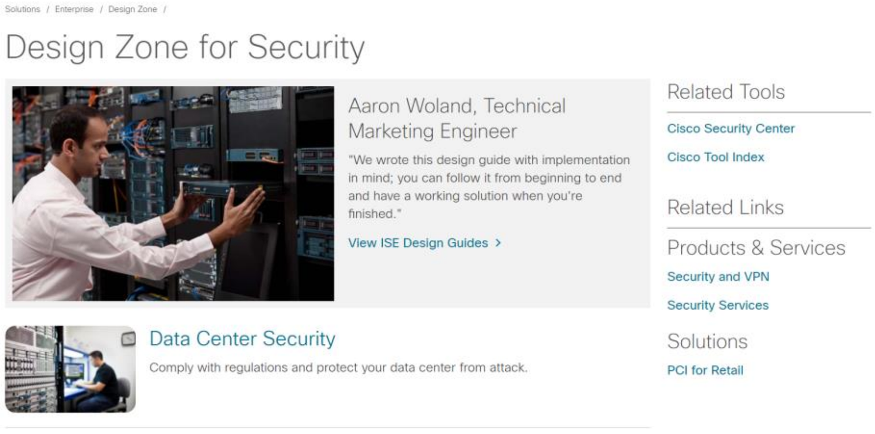
- Cisco Guide to Harden Cisco IOS Devices (also covers IOS XE)

https://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html

- Cisco Guide to Harden Cisco IOS XR Devices
- Cisco Guide to Securing NX-OS Software Devices
- Cisco UCS Hardening Guide
- Cisco Guide to Harden Cisco ASA Firewall
- Cisco Firepower Threat Defense Hardening Guide
- Cisco Firepower Management Center Hardening Guide
- …

FYI

Cisco.com: CVDs, SAFE and more…



Solutions / Enterprise / Design Zone /

Design Zone for Security

Aaron Woland, Technical Marketing Engineer

"We wrote this design guide with implementation in mind; you can follow it from beginning to end and have a working solution when you're finished."

View ISE Design Guides ›

Data Center Security

Comply with regulations and protect your data center from attack.

Related Tools

Cisco Security Center

Cisco Tool Index

Related Links

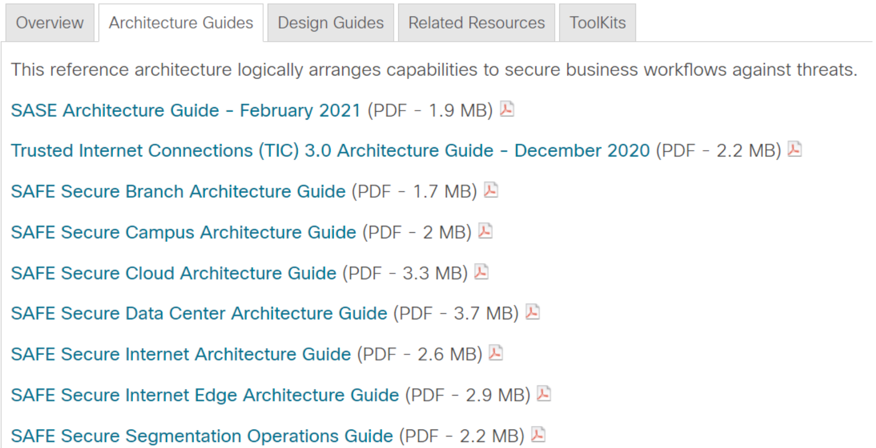
Products & Services

Security and VPN

Security Services

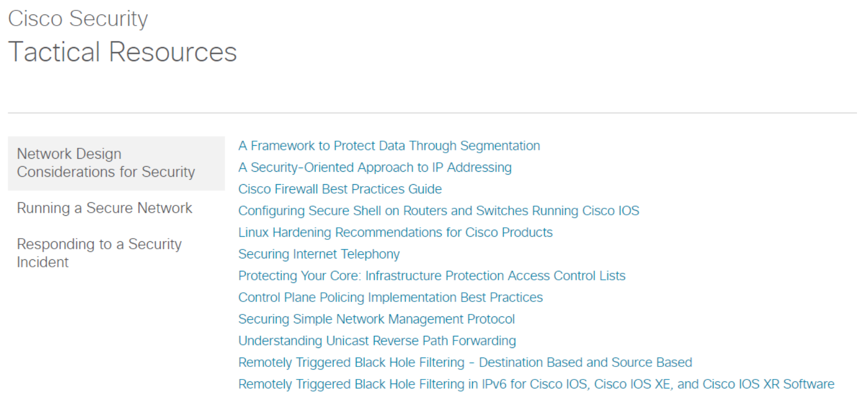
Solutions

PCI for Retail



This reference architecture logically arranges capabilities to secure business workflows against threats.

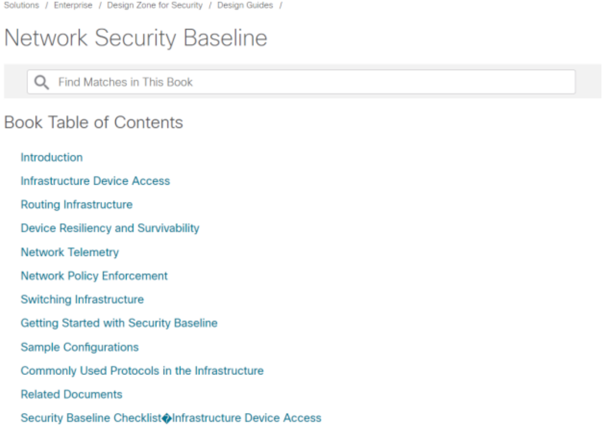
- SASE Architecture Guide - February 2021 (PDF - 1.9 MB)
- Trusted Internet Connections (TIC) 3.0 Architecture Guide - December 2020 (PDF - 2.2 MB)
- SAFE Secure Branch Architecture Guide (PDF - 1.7 MB)
- SAFE Secure Campus Architecture Guide (PDF - 2 MB)
- SAFE Secure Cloud Architecture Guide (PDF - 3.3 MB)
- SAFE Secure Data Center Architecture Guide (PDF - 3.7 MB)
- SAFE Secure Internet Architecture Guide (PDF - 2.6 MB)
- SAFE Secure Internet Edge Architecture Guide (PDF - 2.9 MB)
- SAFE Secure Segmentation Operations Guide (PDF - 2.2 MB)



Cisco Security

Tactical Resources

Network Design Considerations for Security	A Framework to Protect Data Through Segmentation A Security-Oriented Approach to IP Addressing Cisco Firewall Best Practices Guide Configuring Secure Shell on Routers and Switches Running Cisco IOS Linux Hardening Recommendations for Cisco Products Securing Internet Telephony Protecting Your Core: Infrastructure Protection Access Control Lists Control Plane Policing Implementation Best Practices Securing Simple Network Management Protocol Understanding Unicast Reverse Path Forwarding Remotely Triggered Black Hole Filtering - Destination Based and Source Based Remotely Triggered Black Hole Filtering in IPv6 for Cisco IOS, Cisco IOS XE, and Cisco IOS XR Software
Running a Secure Network	
Responding to a Security Incident	



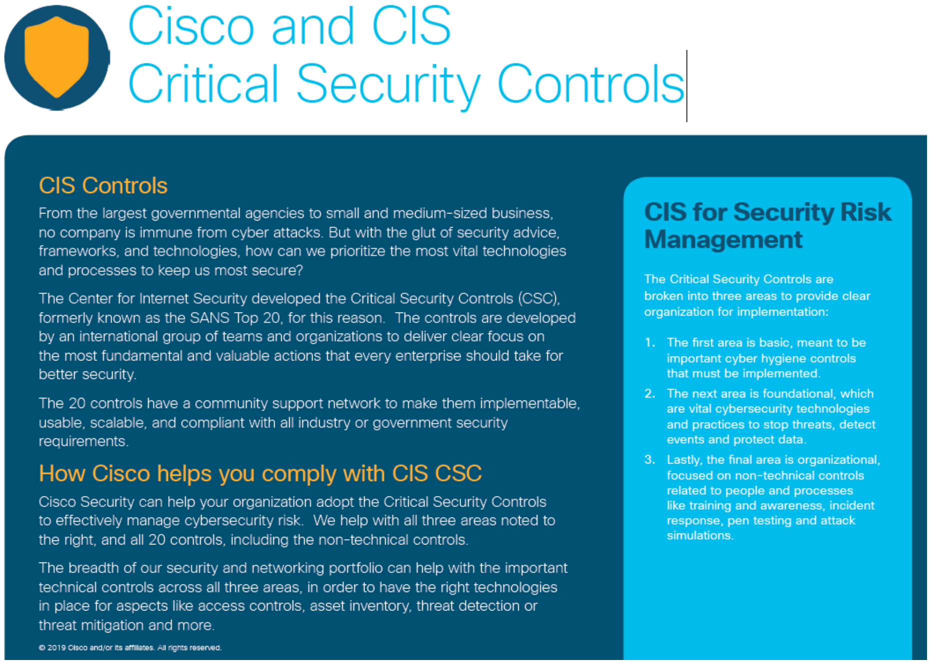
Solutions / Enterprise / Design Zone for Security / Design Guides /

Network Security Baseline

Book Table of Contents

FYI

CIS Critical Security Controls



Cisco and CIS Critical Security Controls

CIS Controls

From the largest governmental agencies to small and medium-sized business, no company is immune from cyber attacks. But with the glut of security advice, frameworks, and technologies, how can we prioritize the most vital technologies and processes to keep us most secure?

The Center for Internet Security developed the Critical Security Controls (CSC), formerly known as the SANS Top 20, for this reason. The controls are developed by an international group of teams and organizations to deliver clear focus on the most fundamental and valuable actions that every enterprise should take for better security.

The 20 controls have a community support network to make them implementable, usable, scalable, and compliant with all industry or government security requirements.

How Cisco helps you comply with CIS CSC

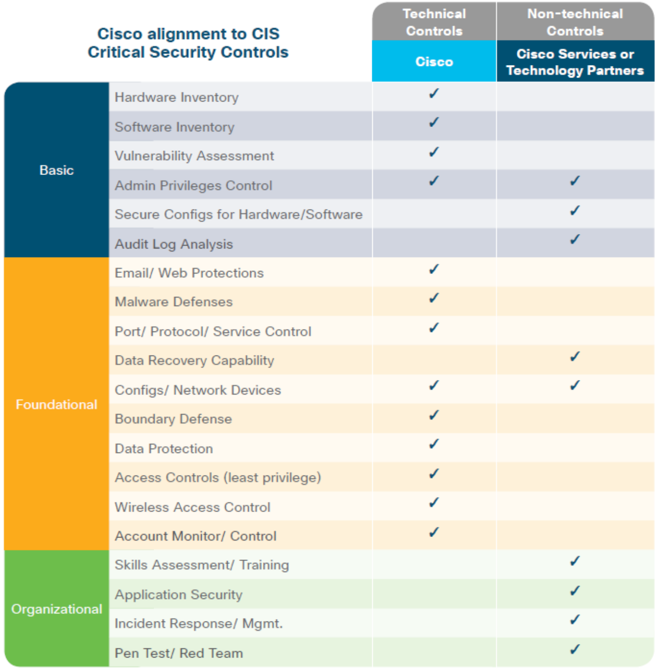
Cisco Security can help your organization adopt the Critical Security Controls to effectively manage cybersecurity risk. We help with all three areas noted to the right, and all 20 controls, including the non-technical controls.

The breadth of our security and networking portfolio can help with the important technical controls across all three areas, in order to have the right technologies in place for aspects like access controls, asset inventory, threat detection or threat mitigation and more.

CIS for Security Risk Management

The Critical Security Controls are broken into three areas to provide clear organization for implementation:

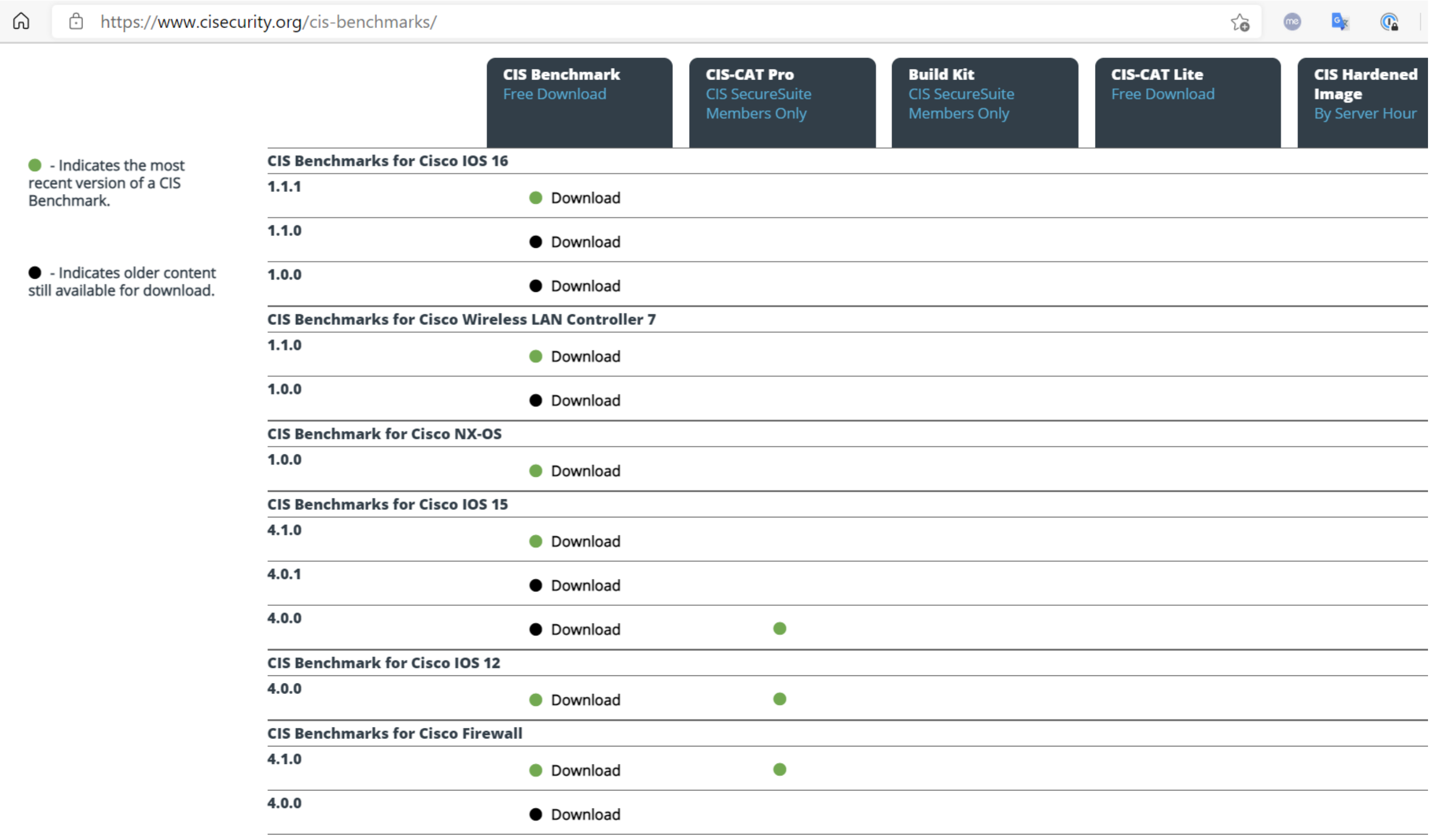
1. The first area is basic, meant to be important cyber hygiene controls that must be implemented.
2. The next area is foundational, which are vital cybersecurity technologies and practices to stop threats, detect events and protect data.
3. Lastly, the final area is organizational, focused on non-technical controls related to people and processes like training and awareness, incident response, pen testing and attack simulations.



	Cisco alignment to CIS Critical Security Controls	Technical Controls	Non-technical Controls
		Cisco	Cisco Services or Technology Partners
Basic	Hardware Inventory	✓	
	Software Inventory	✓	
	Vulnerability Assessment	✓	
	Admin Privileges Control	✓	✓
	Secure Configs for Hardware/Software		✓
	Audit Log Analysis		✓
Foundational	Email/ Web Protections	✓	
	Malware Defenses	✓	
	Port/ Protocol/ Service Control	✓	
	Data Recovery Capability		✓
	Configs/ Network Devices	✓	✓
	Boundary Defense	✓	
	Data Protection	✓	
	Access Controls (least privilege)	✓	
	Wireless Access Control	✓	
	Account Monitor/ Control	✓	
Organizational	Skills Assessment/ Training		✓
	Application Security		✓
	Incident Response/ Mgmt.		✓
	Pen Test/ Red Team		✓

CIS Benchmarks for Cisco

FYI



https://www.cisecurity.org/cis-benchmarks/

🟢 - Indicates the most recent version of a CIS Benchmark.

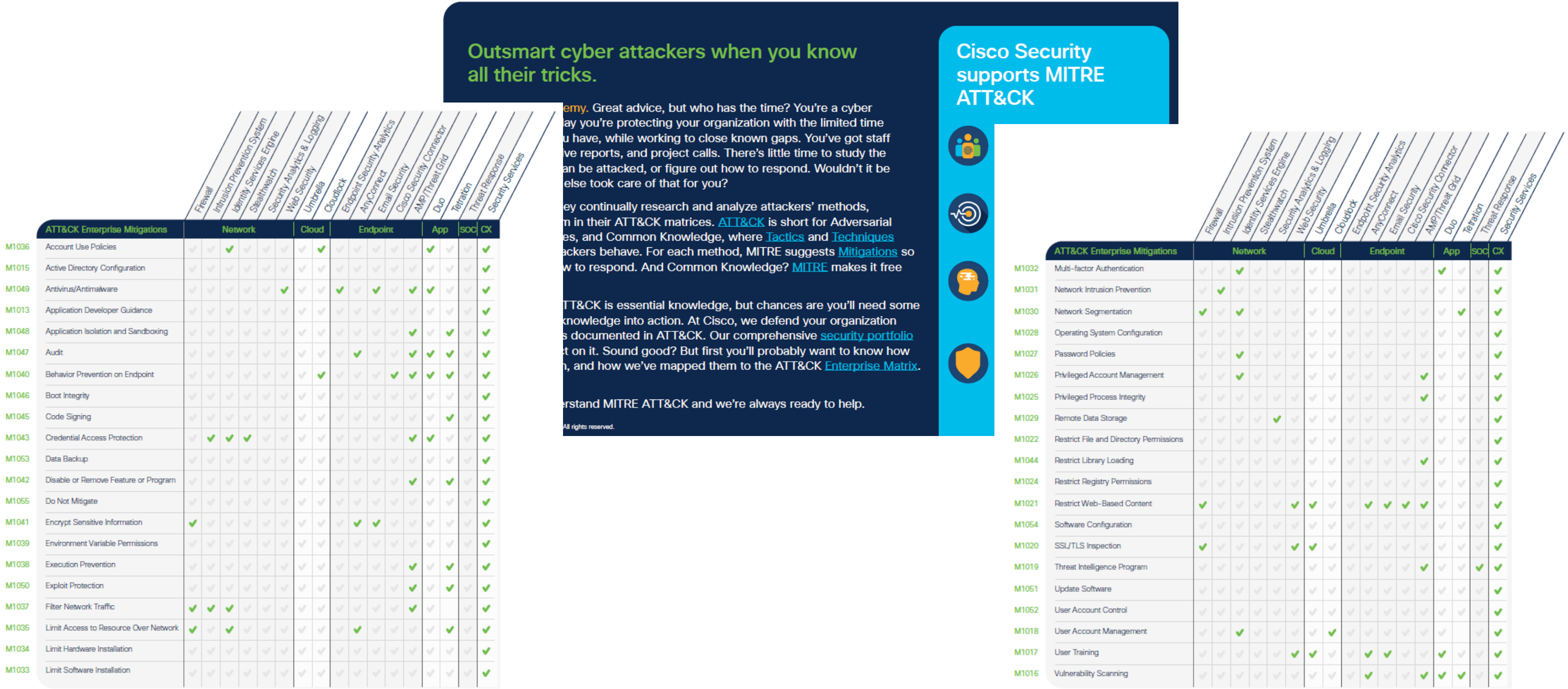
● - Indicates older content still available for download.

	CIS Benchmark Free Download	CIS-CAT Pro CIS SecureSuite Members Only	Build Kit CIS SecureSuite Members Only	CIS-CAT Lite Free Download	CIS Hardened Image By Server Hour
CIS Benchmarks for Cisco IOS 16					
1.1.1	🟢 Download				
1.1.0	● Download				
1.0.0	● Download				
CIS Benchmarks for Cisco Wireless LAN Controller 7					
1.1.0	🟢 Download				
1.0.0	● Download				
CIS Benchmark for Cisco NX-OS					
1.0.0	🟢 Download				
CIS Benchmarks for Cisco IOS 15					
4.1.0	🟢 Download				
4.0.1	● Download				
4.0.0	● Download	🟢			
CIS Benchmark for Cisco IOS 12					
4.0.0	🟢 Download	🟢			
CIS Benchmarks for Cisco Firewall					
4.1.0	🟢 Download	🟢			
4.0.0	● Download				

MITRE ATT&CK

FYI

Cisco Security for MITRE ATT&CK



	ATT&CK Enterprise Mitigations	Network						Cloud		Endpoint					App		SOC	CX
		Firewall	Intrusion Prevention System	Identity Services Engine	Stealthwatch	Security Analytics & Logging	Web Security	Umbrella	Cloudlock	Endpoint Security Analytics	AnyConnect	Email Security	Cisco Security Connector	AMP/Threat Grid	Duo	Tetration	Threat Response	Security Services
M1036	Account Use Policies			✓					✓						✓			✓
M1015	Active Directory Configuration																	✓
M1049	Antivirus/Antimalware						✓			✓		✓		✓	✓			✓
M1013	Application Developer Guidance																	✓
M1048	Application Isolation and Sandboxing													✓		✓		✓
M1047	Audit										✓			✓	✓	✓		✓
M1040	Behavior Prevention on Endpoint								✓				✓	✓	✓	✓		✓
M1046	Boot Integrity																	✓
M1045	Code Signing															✓		✓
M1043	Credential Access Protection		✓	✓	✓									✓	✓			✓
M1053	Data Backup																	✓
M1042	Disable or Remove Feature or Program													✓		✓		✓
M1055	Do Not Mitigate																	✓
M1041	Encrypt Sensitive Information	✓									✓	✓						✓
M1039	Environment Variable Permissions																	✓
M1038	Execution Prevention													✓		✓		✓
M1050	Exploit Protection													✓		✓		✓
M1037	Filter Network Traffic	✓	✓	✓										✓				✓
M1035	Limit Access to Resource Over Network	✓		✓							✓					✓		✓
M1034	Limit Hardware Installation																	✓
M1033	Limit Software Installation																	✓

Outsmart cyber attackers when you know all their tricks.

emy. Great advice, but who has the time? You're a cyber
ay you're protecting your organization with the limited time
u have, while working to close known gaps. You've got staff
ive reports, and project calls. There's little time to study the
an be attacked, or figure out how to respond. Wouldn't it be
else took care of that for you?

ey continually research and analyze attackers' methods,
n in their ATT&CK matrices. ATT&CK is short for Adversarial
es, and Common Knowledge, where Tactics and Techniques
ackers behave. For each method, MITRE suggests Mitigations so
w to respond. And Common Knowledge? MITRE makes it free

TT&CK is essential knowledge, but chances are you'll need some
knowledge into action. At Cisco, we defend your organization
s documented in ATT&CK. Our comprehensive security portfolio
t on it. Sound good? But first you'll probably want to know how
n, and how we've mapped them to the ATT&CK Enterprise Matrix.

erstand MITRE ATT&CK and we're always ready to help.

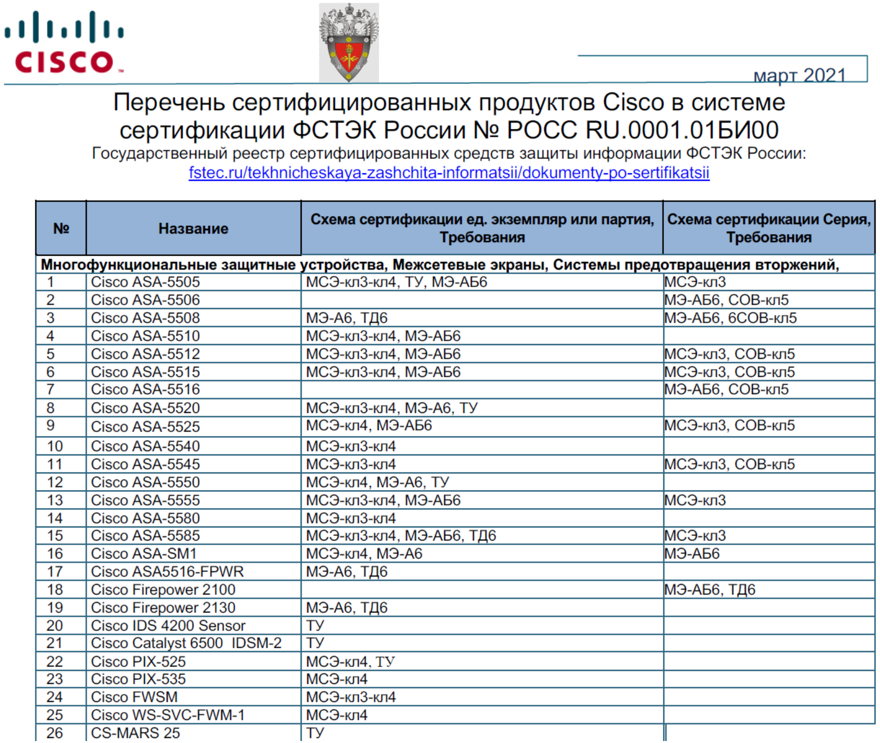
All rights reserved.

Cisco Security supports MITRE ATT&CK

	ATT&CK Enterprise Mitigations	Network						Cloud		Endpoint					App		SOC	CX
		Firewall	Intrusion Prevention System	Identity Services Engine	Stealthwatch	Security Analytics & Logging	Web Security	Umbrella	Cloudlock	Endpoint Security Analytics	AnyConnect	Email Security	Cisco Security Connector	AMP/Threat Grid	Duo	Tetration	Threat Response	Security Services
M1032	Multi-factor Authentication			✓											✓			✓
M1031	Network Intrusion Prevention		✓															✓
M1030	Network Segmentation	✓		✓												✓		✓
M1028	Operating System Configuration																	✓
M1027	Password Policies			✓														✓
M1026	Privileged Account Management			✓										✓				✓
M1025	Privileged Process Integrity													✓				✓
M1029	Remote Data Storage					✓												✓
M1022	Restrict File and Directory Permissions																	✓
M1044	Restrict Library Loading													✓				✓
M1024	Restrict Registry Permissions																	✓
M1021	Restrict Web-Based Content	✓					✓	✓			✓	✓	✓	✓				✓
M1054	Software Configuration																	✓
M1020	SSL/TLS Inspection	✓					✓	✓										✓
M1019	Threat Intelligence Program													✓			✓	✓
M1051	Update Software																	✓
M1052	User Account Control																	✓
M1018	User Account Management			✓					✓									✓
M1017	User Training						✓	✓			✓	✓			✓			✓
M1016	Vulnerability Scanning										✓			✓	✓	✓		✓

ФСТЭК России

FYI

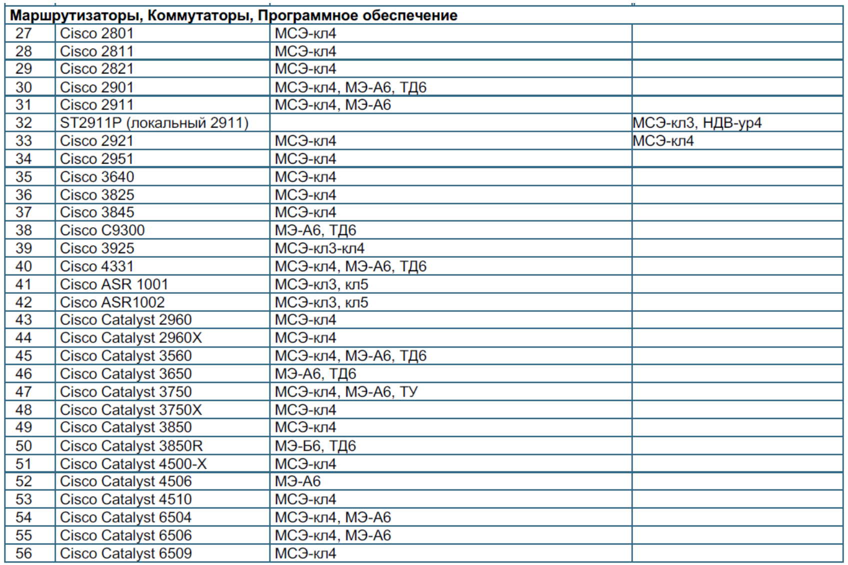


март 2021

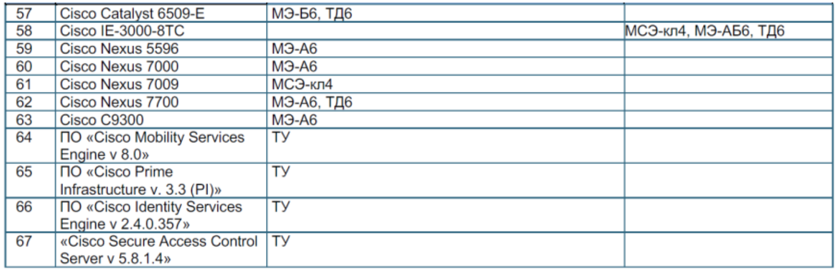
Перечень сертифицированных продуктов Cisco в системе сертификации ФСТЭК России № РОСС RU.0001.01БИ00

Государственный реестр сертифицированных средств защиты информации ФСТЭК России:
fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii

№	Название	Схема сертификации ед. экземпляр или партия, Требования	Схема сертификации Серия, Требования
Многофункциональные защитные устройства, Межсетевые экраны, Системы предотвращения вторжений,			
1	Cisco ASA-5505	МСЭ-кл3-кл4, ТУ, МЭ-АБ6	МСЭ-кл3
2	Cisco ASA-5506		МЭ-АБ6, СОВ-кл5
3	Cisco ASA-5508	МЭ-А6, ТД6	МЭ-АБ6, 6СОВ-кл5
4	Cisco ASA-5510	МСЭ-кл3-кл4, МЭ-АБ6	
5	Cisco ASA-5512	МСЭ-кл3-кл4, МЭ-АБ6	МСЭ-кл3, СОВ-кл5
6	Cisco ASA-5515	МСЭ-кл3-кл4, МЭ-АБ6	МСЭ-кл3, СОВ-кл5
7	Cisco ASA-5516		МЭ-АБ6, СОВ-кл5
8	Cisco ASA-5520	МСЭ-кл3-кл4, МЭ-А6, ТУ	
9	Cisco ASA-5525	МСЭ-кл4, МЭ-АБ6	МСЭ-кл3, СОВ-кл5
10	Cisco ASA-5540	МСЭ-кл3-кл4	
11	Cisco ASA-5545	МСЭ-кл3-кл4	МСЭ-кл3, СОВ-кл5
12	Cisco ASA-5550	МСЭ-кл4, МЭ-А6, ТУ	
13	Cisco ASA-5555	МСЭ-кл3-кл4, МЭ-АБ6	МСЭ-кл3
14	Cisco ASA-5580	МСЭ-кл3-кл4	
15	Cisco ASA-5585	МСЭ-кл3-кл4, МЭ-АБ6, ТД6	МСЭ-кл3
16	Cisco ASA-SM1	МСЭ-кл4, МЭ-А6	МЭ-АБ6
17	Cisco ASA5516-FPWR	МЭ-А6, ТД6	
18	Cisco Firepower 2100		МЭ-АБ6, ТД6
19	Cisco Firepower 2130	МЭ-А6, ТД6	
20	Cisco IDS 4200 Sensor	ТУ	
21	Cisco Catalyst 6500 IDSM-2	ТУ	
22	Cisco PIX-525	МСЭ-кл4, ТУ	
23	Cisco PIX-535	МСЭ-кл4	
24	Cisco FWSM	МСЭ-кл3-кл4	
25	Cisco WS-SVC-FWM-1	МСЭ-кл4	
26	CS-MARS 25	ТУ	



Маршрутизаторы, Коммутаторы, Программное обеспечение			
27	Cisco 2801	МСЭ-кл4	
28	Cisco 2811	МСЭ-кл4	
29	Cisco 2821	МСЭ-кл4	
30	Cisco 2901	МСЭ-кл4, МЭ-А6, ТД6	
31	Cisco 2911	МСЭ-кл4, МЭ-А6	
32	ST2911P (локальный 2911)		МСЭ-кл3, НДВ-ур4
33	Cisco 2921	МСЭ-кл4	МСЭ-кл4
34	Cisco 2951	МСЭ-кл4	
35	Cisco 3640	МСЭ-кл4	
36	Cisco 3825	МСЭ-кл4	
37	Cisco 3845	МСЭ-кл4	
38	Cisco C9300	МЭ-А6, ТД6	
39	Cisco 3925	МСЭ-кл3-кл4	
40	Cisco 4331	МСЭ-кл4, МЭ-А6, ТД6	
41	Cisco ASR 1001	МСЭ-кл3, кл5	
42	Cisco ASR1002	МСЭ-кл3, кл5	
43	Cisco Catalyst 2960	МСЭ-кл4	
44	Cisco Catalyst 2960X	МСЭ-кл4	
45	Cisco Catalyst 3560	МСЭ-кл4, МЭ-А6, ТД6	
46	Cisco Catalyst 3650	МЭ-А6, ТД6	
47	Cisco Catalyst 3750	МСЭ-кл4, МЭ-А6, ТУ	
48	Cisco Catalyst 3750X	МСЭ-кл4	
49	Cisco Catalyst 3850	МСЭ-кл4	
50	Cisco Catalyst 3850R	МЭ-Б6, ТД6	
51	Cisco Catalyst 4500-X	МСЭ-кл4	
52	Cisco Catalyst 4506	МЭ-А6	
53	Cisco Catalyst 4510	МСЭ-кл4	
54	Cisco Catalyst 6504	МСЭ-кл4, МЭ-А6	
55	Cisco Catalyst 6506	МСЭ-кл4, МЭ-А6	
56	Cisco Catalyst 6509	МСЭ-кл4	



57	Cisco Catalyst 6509-E	МЭ-Б6, ТД6	
58	Cisco IE-3000-8TC		МСЭ-кл4, МЭ-АБ6, ТД6
59	Cisco Nexus 5596	МЭ-А6	
60	Cisco Nexus 7000	МЭ-А6	
61	Cisco Nexus 7009	МСЭ-кл4	
62	Cisco Nexus 7700	МЭ-А6, ТД6	
63	Cisco C9300	МЭ-А6	
64	ПО «Cisco Mobility Services Engine v 8.0»	ТУ	
65	ПО «Cisco Prime Infrastructure v. 3.3 (PI)»	ТУ	
66	ПО «Cisco Identity Services Engine v 2.4.0.357»	ТУ	
67	«Cisco Secure Access Control Server v 5.8.1.4»	ТУ	

Zone Based Firewall

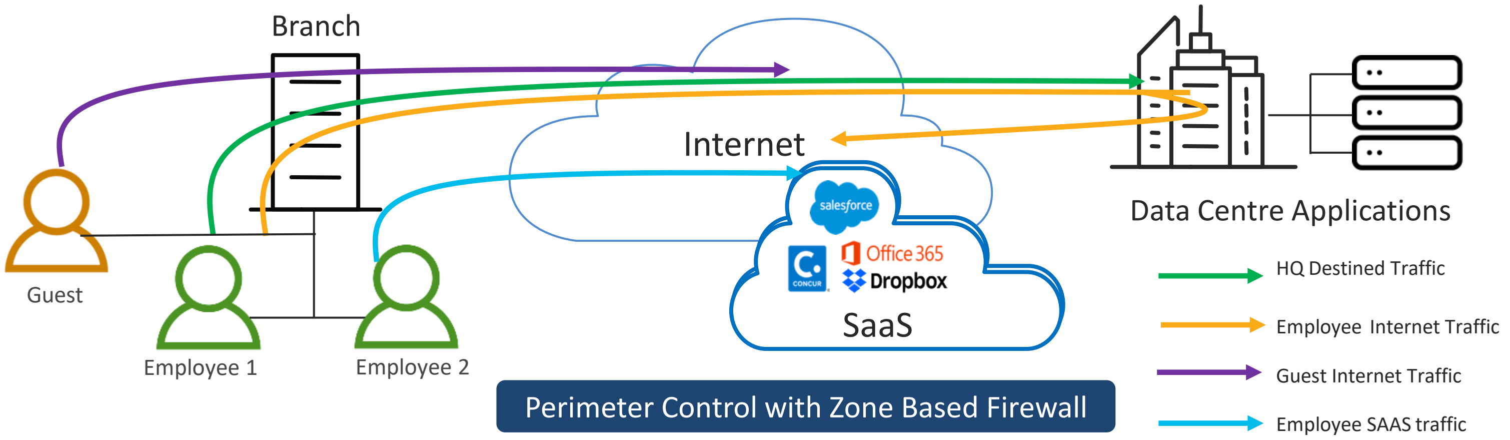
Zone Based Firewall Features

Configuration

Comprehensive security solution that covers:

- Stateful inspection
- Application Inspection
- DDOS Protection
- Zone Mismatch handling
- Application Visibility and Granular Control
- Layer 2 Transparent Firewall
- VRF-Aware Firewall
- Resource Management
- Firewall High-Speed Logging
- 1400+ layer 7 applications classified

Zone Based Firewall Use Cases



Perimeter Control with Zone Based Firewall

PCI Compliance	Protect sensitive information against data breaches (such as card holder or patient information)
Guest Access	Offload guest internet traffic from corporate WAN with enhanced security
Direct Cloud Access	Offload SaaS traffic from premium WAN connections & improve application experience
Direct Internet Access	Secure direct internet access for improved branch office user experience

Zone Based Firewall – Benefits and Requirements

Benefits

- PCI * compliance
- Stateful firewall built into branch routers
- VLAN Segmentation
- Supports VRF
- Supports IPv6

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
- XE 3.7S and above on ASR1K
- XE 3.10S and above on CSR 1000V

* PCI – Payment Card Industry

Supported Platforms

Platform	Minimum IOS XE Release
ISR 1000	IOS XE 16.6.1
ISR 4000	IOS XE 3.9
ASR 1000	IOS XE 3.7S
CSR 1000v	IOS XE 3.10S
Catalyst 8200	IOS XE 17.4.1
Catalyst 8300	IOS XE 17.3.2
Catalyst 8500	IOS XE 17.3.2
Catalyst 8000v	IOS XE 17.4.1

With SEC-K9 / DNA Essentials Licensing SKU

Firewall Zones

Default Zone

- Interfaces that do not belong to a custom zone automatically assigned to default zone
- Not enabled by default
- Configuration CLI : zone security default

Custom Zone

- Zoned created by the administrator to manually assign network interfaces
- Same custom zones can be assigned to multiple interfaces
- Configuration CLI : zone security <custom zone name>

Self Zone

- System defined zone with no interfaces as members
- Protects traffic sourced or destined TO and FROM the router
- Protects management and control plane traffic.(Default explicit allow action)
- Inspect policing not configuration

⚠ No Policy inspection from Default-to-Default Zone

Zone Pair Policy Considerations

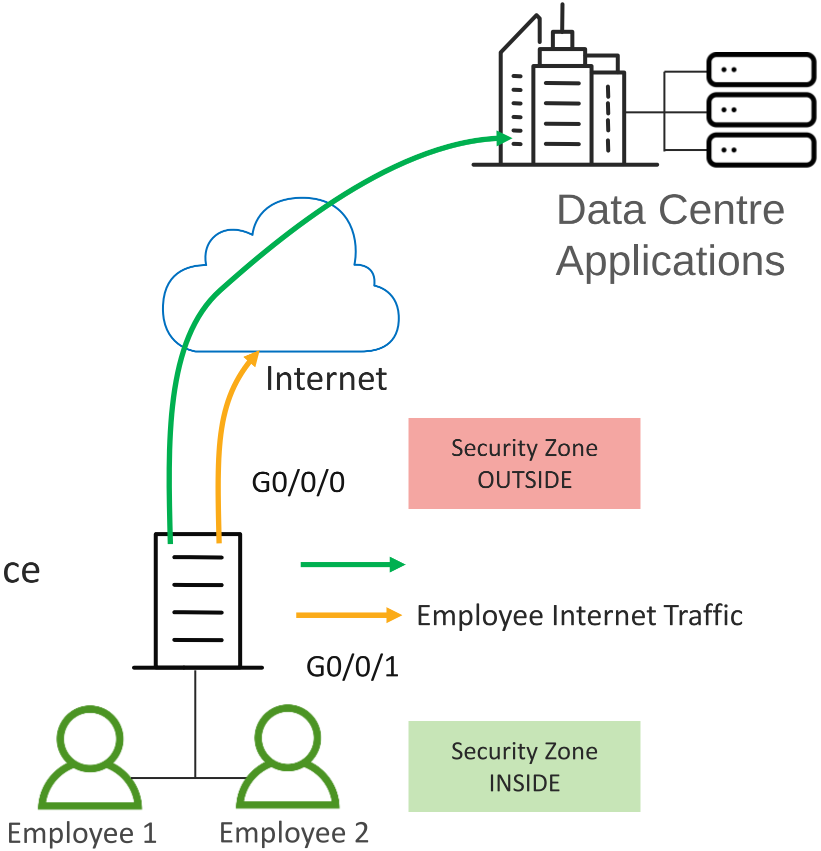
- An interface can be assigned to only one security zone.

- All inter zone traffic is implicitly blocked when an interface is assigned to a zone.

- Intra zone traffic is implicitly allowed to flow by default

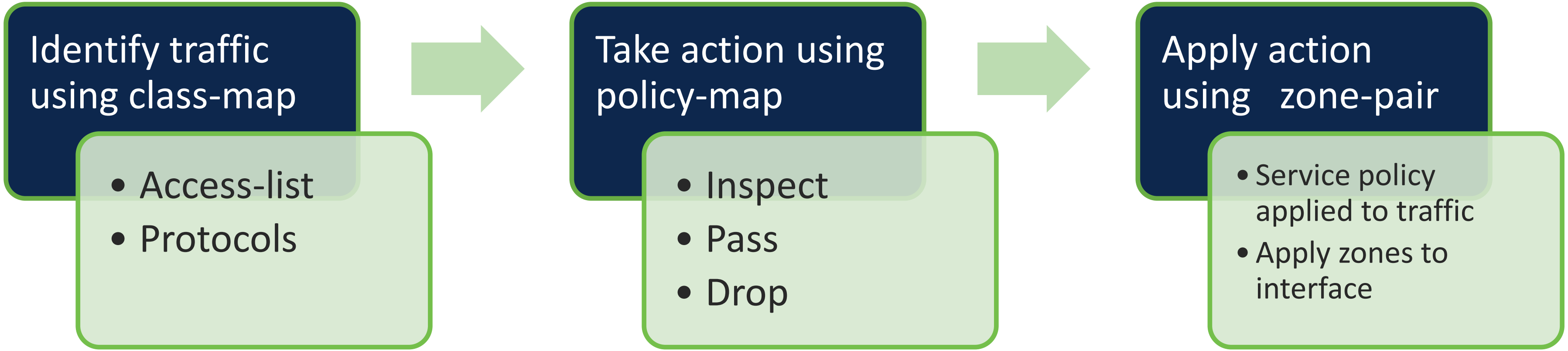
- Traffic cannot flow between a zone-member interface and any interface which is not a zone-member. *(If default zone is not enabled & configured)*

- Zone-pair policy is required to permit or inspect traffic between two zones



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
- Pass
- Drop

Apply action using zone-pair

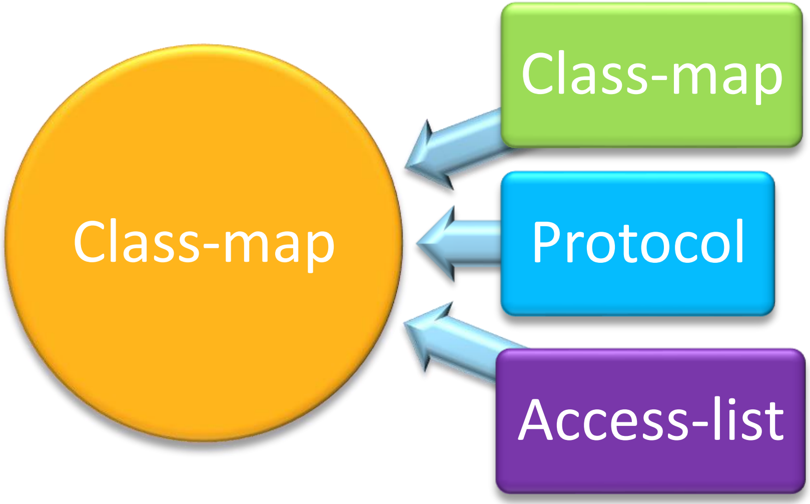
- Service policy applied to traffic
- Apply zones to interface

Identifying Traffic using Class-Maps

- Class-maps identify traffic
  - Access-lists for IP addresses and ports
  - Protocols for Layer 7 matching

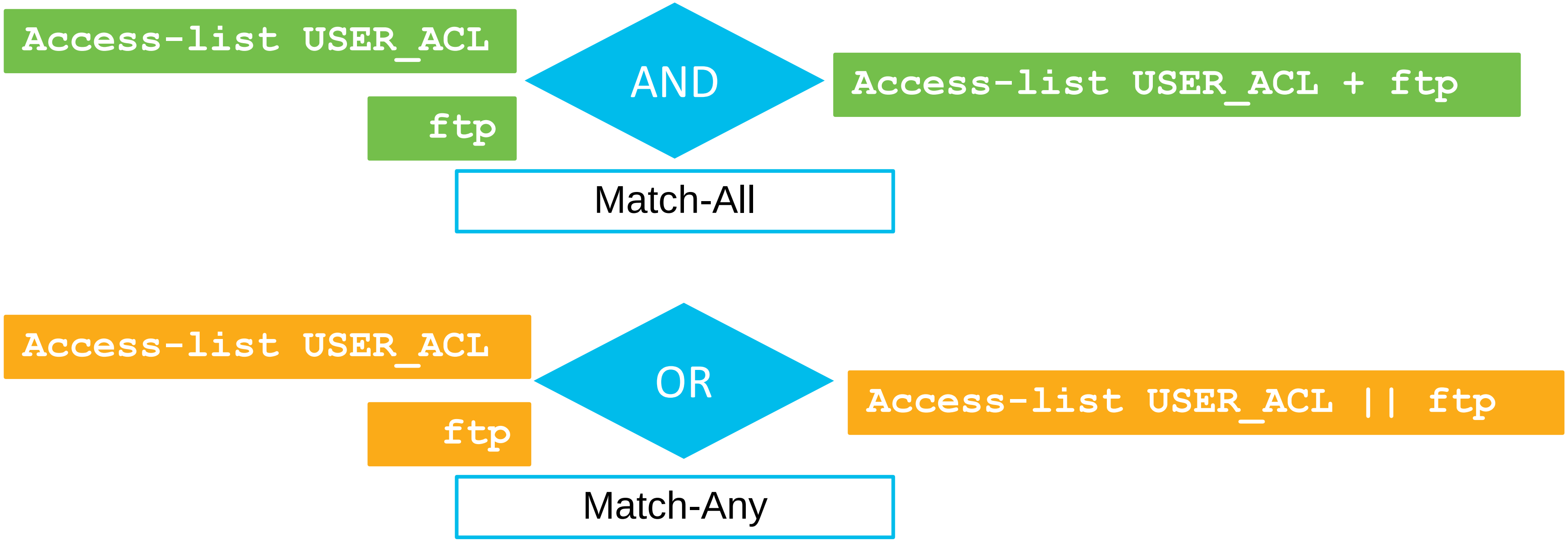
- Class-maps can be nested
  - Scalability through reuse
  - Directed match criteria

```
class-map type inspect match-all USERS_PROTOCOLS
  match access-group name USER_ACL
  match protocol ftp
```



Identifying Traffic using Class-Maps

- Match-Any vs Match-All



Access-list USER_ACL

ftp

AND

Access-list USER_ACL + ftp

Match-All

Access-list USER_ACL

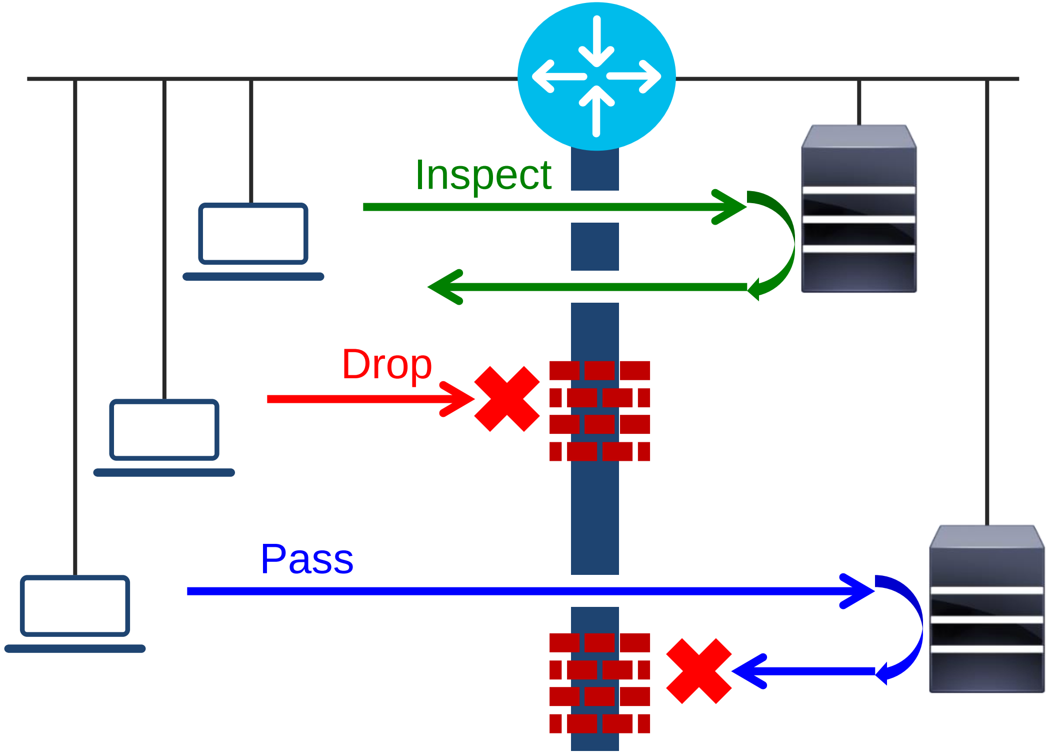
ftp

OR

Access-list USER_ACL || ftp

Match-Any

Take Action using Policy-Map



Inspect

- Builds connections for traffic
- Statefully examines the flow
- Allows return packets that match connection
- Preferred action for traffic

Drop

- Drops packets silently

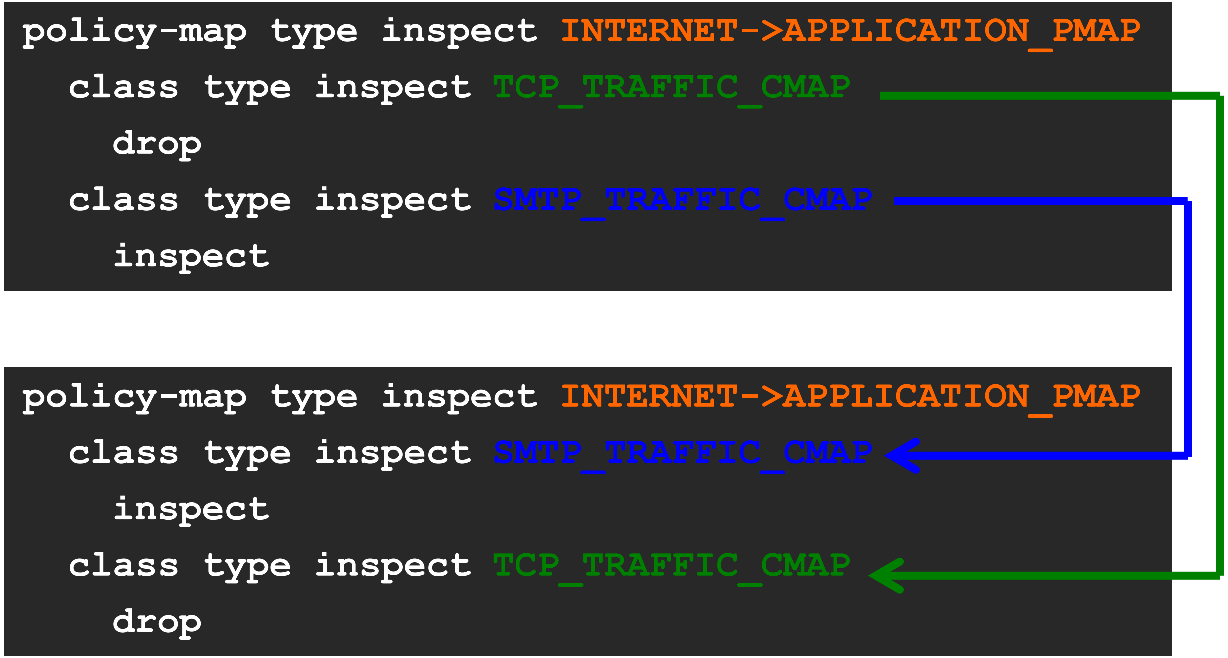
Pass

- Bypasses firewall checks
- Return traffic must be explicitly allowed (*with mirrored policy)*
- Only for customized traffic

Take Action using Policy-Map

Class-maps Order of Operation :

- Class-maps are processed in order
- Always put more specific match conditions first
- Order matters when applying action/application inspection



```
policy-map type inspect INTERNET->APPLICATION_PMAP
  class type inspect TCP_TRAFFIC_CMAP
    drop
  class type inspect SMTP_TRAFFIC_CMAP
    inspect
```

```
policy-map type inspect INTERNET->APPLICATION_PMAP
  class type inspect SMTP_TRAFFIC_CMAP
    inspect
  class type inspect TCP_TRAFFIC_CMAP
    drop
```

Zone Based Firewall - Custom Zone

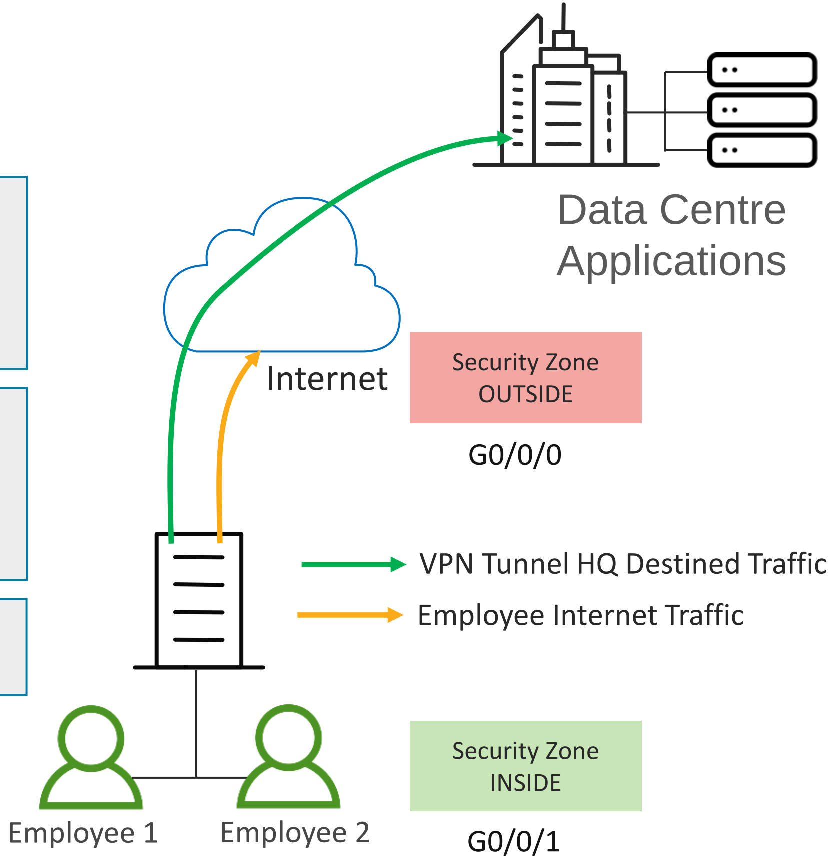
```
zone security INSIDE
zone security OUTSIDE
```

```
class-map type inspect match-any INSIDE-TO-OUTSIDE-CLASS
 match protocol ftp
 match protocol tcp                    | or match access-list
 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
```

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

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



Zone Based Firewall – Default Zone

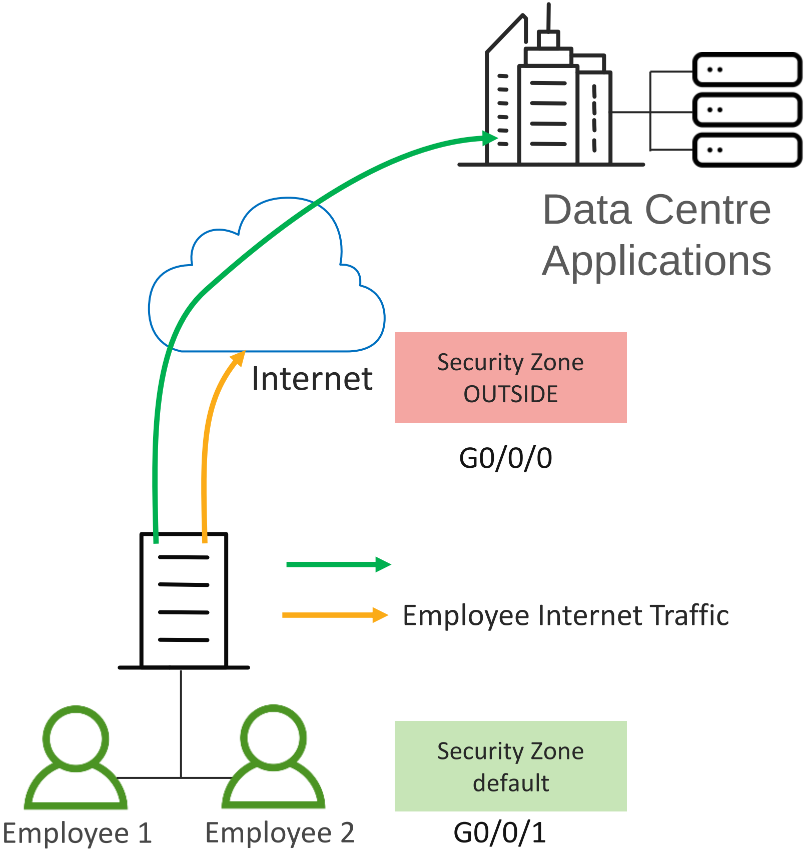
```
zone security default
zone security OUTSIDE
```

```
class-map type inspect match-any INSIDE-TO-OUTSIDE-CLASS
 match protocol ftp
 match protocol tcp          | or match access-list
 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
```

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

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

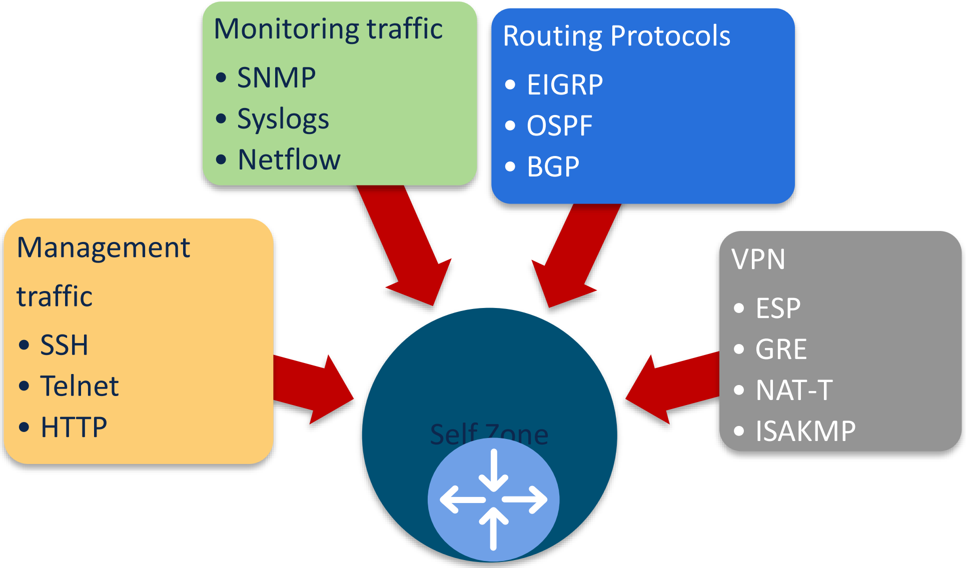


Zone Based Firewall – Self Zone

- 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

Zone Based Firewall

Self Zone inbound - Inbound traffic 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 host x.x.x.x 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 – Outbound 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
```

App-aware Firewall – Benefits and Requirements

Benefits

- Application Visibility and Granular control
- 1400+ layer 7 applications classified
- Allow or block traffic by application, category, application-family or application-group
- Segmentation
- PCI compliance
- Supports VRF
- Supports IPv6

Requirements

- AppX license (includes Sec-K9)
- XE 16.9.1 and above

  on ISR4K, ISR1K, CSR and ASR1K

Ent. Firewall App Aware - Configuration

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

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

```
class-map match-any AVC-CLASS
 match protocol yahoo
 match protocol amazon
 match protocol attribute category consumer-streaming
 match protocol attribute category gaming
 match protocol attribute category social-networking
```

```
policy-map type inspect avc AVC-POLICY
 class AVC-CLASS
  deny
 class class-default
  allow
```

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

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

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

TCP SYN Cookie Protection

- Protects the firewall from TCP SYN-flooding DoS attacks
- TCP SYN flooding can be resource intensive for the firewall and end host
- Two types of Protection
  - **Host Based**

    Limit the rate of SYN packets to each host
  - **Session Table Protection**

    Limit the rate of half-open session counts for each VRF domain

Limitations:

- Firewall TCP SYN Cookie feature cannot be configured for a default zone.
- TCP SYN Cookie feature does not support per-subscriber firewall

SYN Cookie Protection Packet Flow

1.Client initiates a SYN

2. The firewall intercepts TCP SYN packets that are sent from clients to servers.

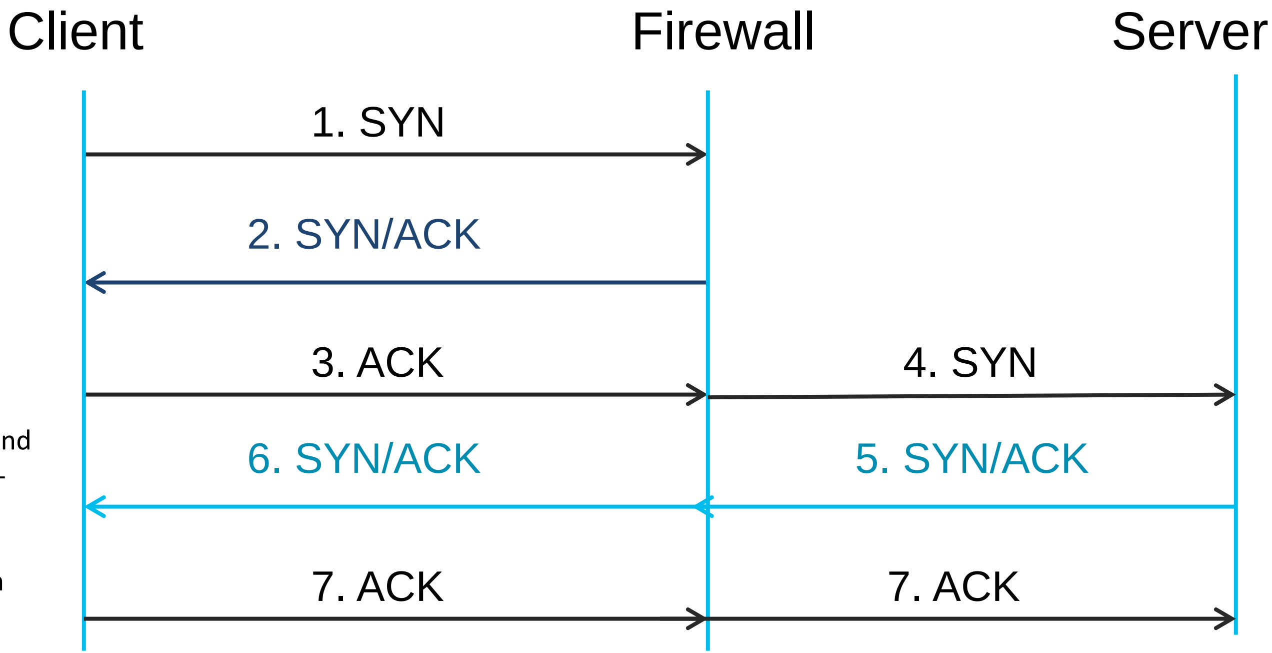
3. Client send the ACK

4. Firewall verifies cookie and sends SYN to the server

5. Firewall receives the SYN/ACK, computes the SYN cookie fixup

6. Firewall establishes connections client and the destination server as transparent man-in-middle device

7. This prevents connection attempts from unreachable host to reach the service



TCP SYN Cookie Host Protection

```
Router(config)# parameter-map type inspect-zone zone-pmap
Router(config-profile)# tcp syn-flood rate per-destination 400
Router(config-profile)# max-destination 10000
Router(config-profile)# exit

Router(config)# zone security EMPLOYEE
Router(config-sec-zone)# protection zone-pmap
```

TCP SYN Cookie Session Table Protection

Firewall session table protection for global routing domains:

```
Router(config)# parameter-map type inspect-global
Router(config-profile)# tcp syn-flood limit 500
Router(config-profile)# end
```

Firewall session table protection for VRF routing domains:

Number of half-open connections that triggers SYN cookie

```
Router(config)# parameter-map type inspect-vrf vrf-pmap
Router(config-profile)# tcp syn-flood limit 200
Router(config-profile)# exit

Router(config)# parameter-map type inspect-global
Router(config-profile)# inspect vrf vrf1 inspect vrf-pmap
Router(config-profile)# end
```

Zone Mismatch Handling

- By Default, ZBFW allows return traffic to pass through based on session match (*5-tuple info*) with zone-Pair check.

- If the return traffic arrives on a different interface than the original traffic was egressed, it leads to **zone mismatch scenario**.

Zone Mismatch Handling:

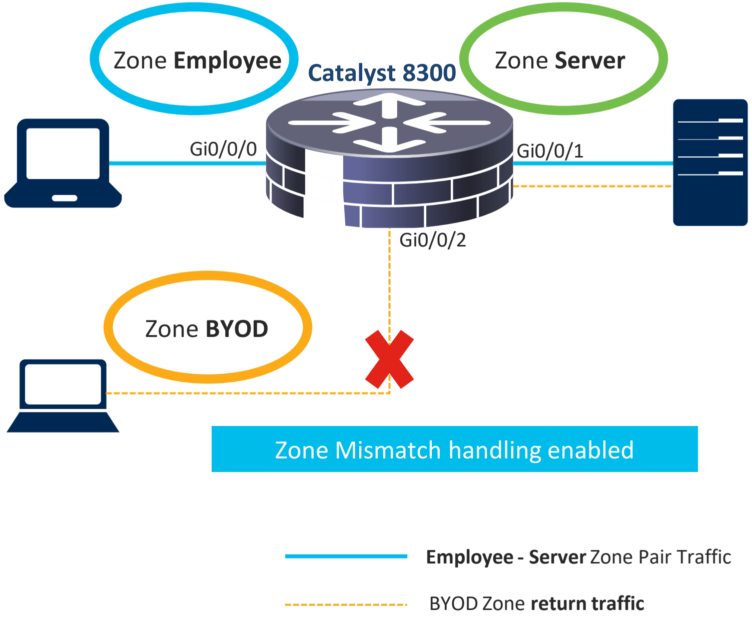
- Validates Zone-Pair associated with an existing session.

- Drops traffic in the even of a zone mismatch for the return traffic & protects against security vulnerabilities.

- Feature **not enabled** as default.

- CLI *zone-mismatch drop* enables mismatch handling.

- Configuration can be applied at **global level** or on **per-policy basis**



Zone Mismatch Handling Configuration

- **Per Policy Configuration**

```
parameter-map type inspect Network-Policy
Zone mismatch drop
exit
```

- **Global firewall Configuration**

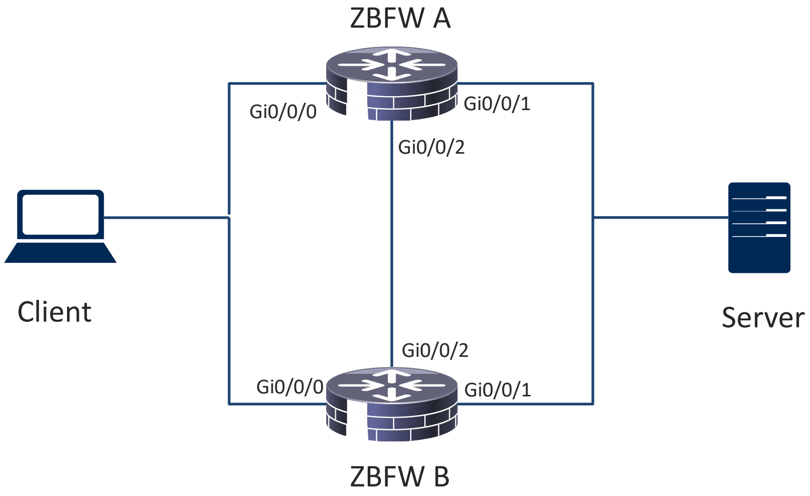
```
parameter-map type inspect-global
Zone mismatch drop
exit
```

⚠ Command not configurable under *parameter-map type inspect-vrf* or *parameter-map type inspect-zone*

Zone Based Firewall High Availability

High availability support based on redundancy groups (RGs) enables you to configure pairs of devices to act as backup for each other.

- ZBFW)supports HA in an active/standby or **active/active** setup.
- Active and standby devices must have the same zone-based policy firewall configuration.
- Active and standby devices must run on identical versions of Cisco software.
- Interfaces attached to a firewall must have the same redundant interface identifier (RII)



High Availability Overview

In HA, the redundant devices are joined by a configurable control link and a data synchronization link.

Control Link

- Provides peer reachability detection
- Used for RG transport query & failover protocol negotiation

Data Link

- Transfers stateful information from the firewall
- Used for data synchronize the stateful database e.g., NAT & FW session sync etc.

Redundant interface identifier (RII)

- Unique ID number configured on the pair of redundant interfaces

- Monitory RG members relies on hello messages

- Two configurable timers:
  - Hello(default 3 sec) - The interval at which hello messages are sent.
  - Hold time (default 10 sec) - The amount of time before which the active or standby device is declared to be down.

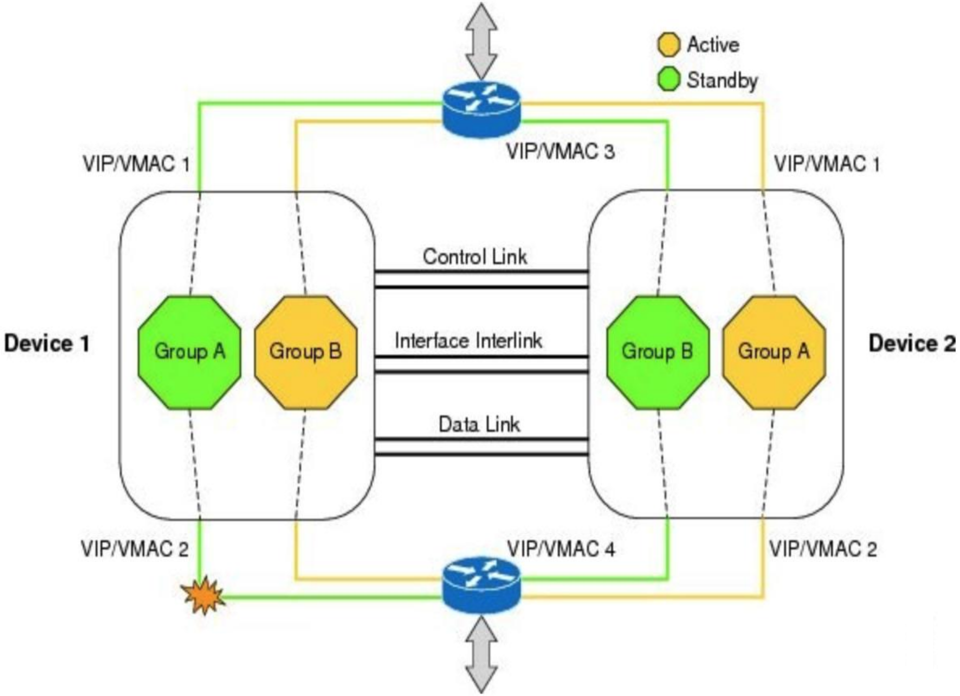
Active/Active High Availability

- The active/active failover allows both devices can process network traffic simultaneously.

- Redundancy groups(RG) configured for device pair with two outgoing interfaces.

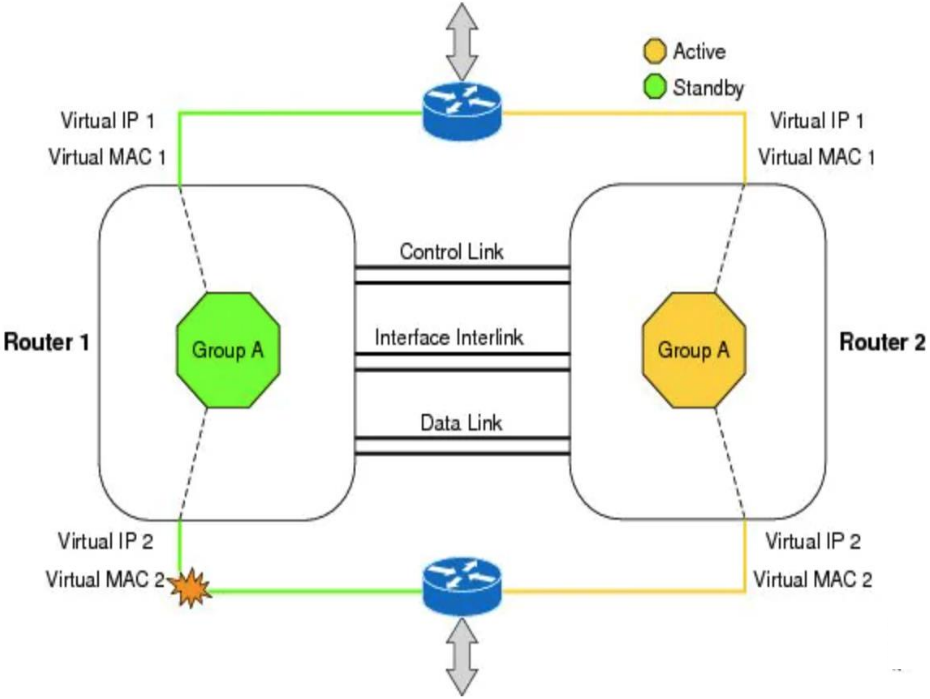
- Virtual MAC assigned for interface in each RG.

- Each RG has one active(primary) & one standby(secondary) device.



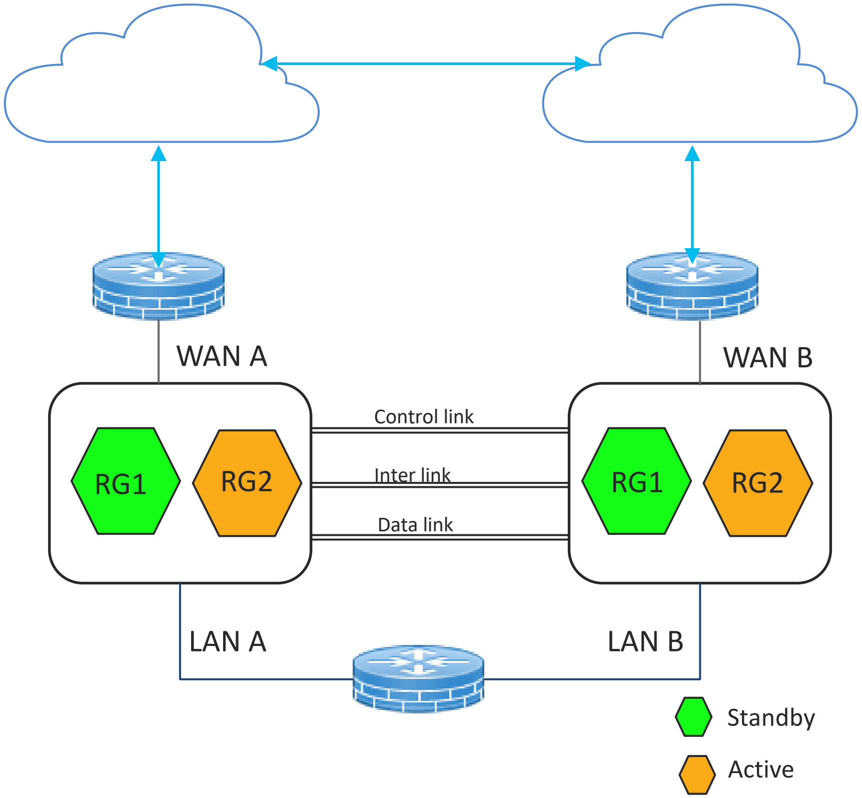
Active/Standby High Availability

- In active/standby failover only one of the devices involved in the failover handles the traffic at a time.
- During failover:
  - Active device takes over IP addresses and MAC addresses of the failed device.
  - Standby device takes over standby IP addresses and MAC addresses
- MAC addresses of the active device are always paired with active IP addresses.



Asymmetric Routing

- Zone-Based Firewall HA supports asymmetric routing in a LAN-WAN scenario.
- Supports forwarding of packets from standby RG to active RG with a dedicated interface (interlink interface) for asymmetric traffic.
- If not enabled, the return packets received on the standby RG are dropped
- For firewall with NAT config, default asymmetric routing rule is to always divert the packets to the active RG



What Triggers a Failover ?

- Power loss/reload on the active device.
- Control interface for RG in link down status .
- Data interface for RG in link down status.
- Run-time priority of the active device going below threshold value.
- Run-time priority of the active device goes down below that of the standby device.
- The redundancy group on the active device is reloaded manually by using the *redundancy application reload group* rg-number command.

ZBFW High Availability Configuration

ZBFW A

```
# RG Protocol
redundancy
application redundancy
Protocol 1
name ZBFWHA
timers hellotime 6 holdtime 4
end

# Redundancy Application Group
redundancy
application redundancy
group 1
name group1
priority 100 failover threshold 50
Preempt
track 200 decrement 200
data GigabitEthernet 0/0/0
control GigabitEthernet 0/0/2 protocol 1
asymmetric-routing interface GigabitEthernet 0/1/1
asymmetric-routing always-divert enable
timers delay 100 reload 400
end
```

```
# LAN traffic Configuration
interface gigabitethernet 2/0/2
ip address 10.1.1.1 255.255.255.0
description lan interface
encapsulation dot1q 18
ip vrf forwarding trust
zone member security z1
redundancy rii 100
redundancy group 1 ipv4 10.1.1.3 exclusive
end

# WAN traffic Configuration
interface gigabitethernet 2/1/0
ip address 10.2.1.1 255.255.255.0
description wan interface
ip tcp adjust-mss 1360
zone member security z2
redundancy rii 360
redundancy asymmetric-routing enable
end
```

ZBFW High Availability Configuration

ZBFW B

```
# RG Protocol
redundancy
application redundancy
Protocol 1
name ZBFWHA
timers hellotime 6 holdtime 4
end

# Redundancy Application Group
redundancy
application redundancy
group 1
name group1
priority 100 failover threshold 50
Preempt
track 200 decrement 200
data GigabitEthernet 0/0/0
control GigabitEthernet 0/0/2 protocol 1
asymmetric-routing interface GigabitEthernet 0/1/1
asymmetric-routing always-divert enable
timers delay 100 reload 400
end
```

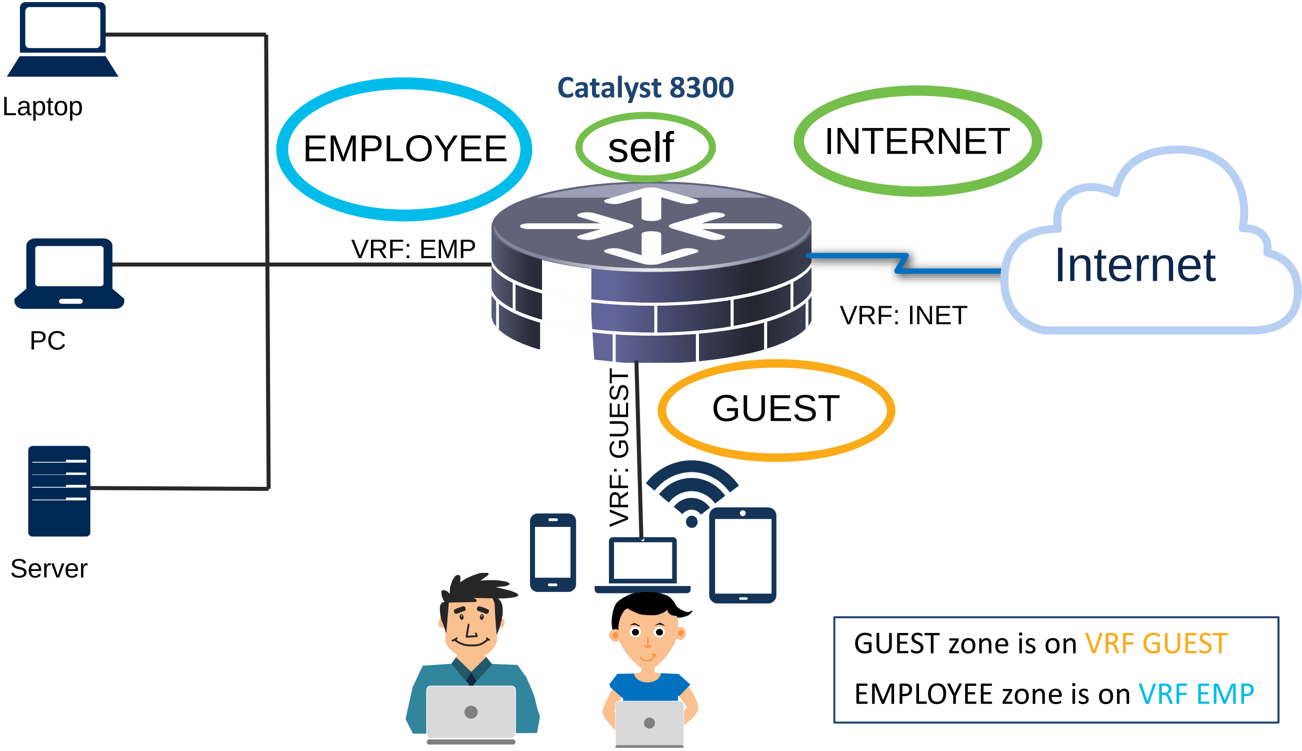
```
# LAN traffic Configuration
interface gigabitethernet 2/0/2
ip address 10.1.1.2 255.255.255.0
description lan interface
encapsulation dot1q 18
ip vrf forwarding trust
zone member security z1
redundancy rii 100
redundancy group 1 ipv4 10.1.1.3 exclusive
end

# WAN traffic Configuration
interface gigabitethernet 2/1/0
ip address 10.2.1.2 255.255.255.0
description wan interface
ip tcp adjust-mss 1360
zone member security z2
redundancy rii 360
redundancy asymmetric-routing enable
end
```

Firewall Resource Management

- Limits the number of VPN VRF and global firewall sessions configured on a router

- limits the level of usage of shared resources on a device which includes:
  - Connection states
  - Memory usage (per table)
  - Number of sessions or calls
  - Packets per second
  - Ternary content addressable memory (TCAM) entries



GUEST zone is on VRF GUEST

EMPLOYEE zone is on VRF EMP

Resource Management Configuration

- Limit the number & rate of opened or half-opened sessions

- Parameter map config applicable at global routing domain or at routing level

```
parameter-map type inspect-vrf vrf1-pmap
      session total 1000
      tcp syn-flood limit 2000
exit
parameter-map type inspect-global
      vrf vrf1 inspect pmap1
exit
parameter-map type inspect-vrf vrf-default
      session total 6000
      tcp syn-flood limit 7000
end
```

Resource Management Configuration

```
zone security GUEST
zone security INTERNET
```

```
class-map type inspect match-any GUEST-INTERNET-CLASS
 match protocol dns
 match protocol http
 match protocol https
```

```
Parameter-map type inspect GUEST-PRAM-MAP
 session maximum 1000
```

```
policy-map type inspect GUEST-INTERNET-POLICY
 class type inspect GUEST-INTERNET-CLASS
  inspect GUEST-PRAM-MAP
 class class-default
  drop
```

```
Parameter-map type inspect-vrf GUEST-PRAM-MAP-VRF-GUEST
 session total 1000
```

```
parameter-map type inspect-global
 vrf GUEST inspect GUEST-PRAM-MAP-VRF-GUEST
```

```
Interface G0/0/3
 zone security INTERNET
Interface g0/0/2.30
 Zone security GUEST
 vrf forward GUEST
```

```
zone-pair security GUEST-INTERNET source GUEST destination INTERNET
 service-policy type inspect GUEST-INTERNET-POLICY
```

High-Speed Logging

- Logging new connections is not on by default.
- Processor intensive
  - Interrupt driven messages can cause high CPU
  - Similar to log keyword on ACLs
- Used for troubleshooting
  - Not recommended for monitoring

```
enable
configure terminal
parameter-map type inspect global
 audit trail-on
 log dropped-packets
 log flow-export v9 udp destination 10.0.2.0 5000
 log flow-export template timeout-rate 5000
end
```

High-Speed Logging

```
zone security GUEST
zone security INTERNET
```

```
class-map type inspect match-any GUEST-INTERNET-CLASS
 match protocol dns
 match protocol http
 match protocol https
```

```
policy-map type inspect GUEST-INTERNET-POLICY
 class type inspect GUEST-INTERNET-CLASS
  inspect LOG_CONNECTION_PARAM
class class-default
  drop log
```

```
Interface G0/0/3
 zone security INTERNET
Interface g0/0/2.30
 Zone security GUEST
```

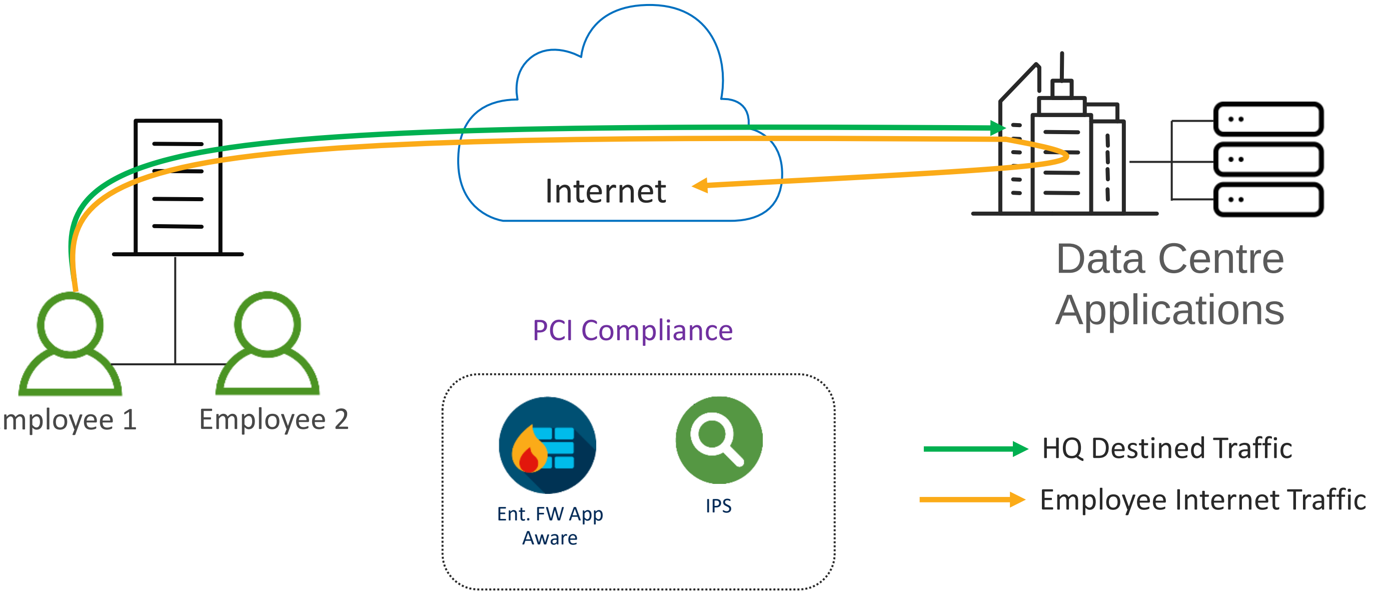
```
zone-pair security GUEST-INTERNET source GUEST destination INTERNET
 service-policy type inspect GUEST-INTERNET-POLICY
```

```
Parameter-map type inspect inspect-global
 log dropped-packets
 log flow-export v9 udp destination 10.0.2.0 5000
 log flow-export template timeout-rate 5000
```

```
Parameter-map type inspect LOG_CONNECTION_PARAM
  audit-trail on
  alert on
  one-minute high 10000
  tcp max-incomplete host 100
```

Snort IPS

Snort IPS Use Case: PCI Compliance



Internet

Data Centre Applications

Employee 1

Employee 2

PCI Compliance

Ent. FW App Aware

IPS

HQ Destined Traffic

Employee Internet Traffic

Snort IPS - Appendix

FYI

- VPG – Virtual Port Group
- DIA – Direct Internet Access
- CSR - Cloud Services Router
- WL – White Listing
- OVA – Open Virtual Appliance
- UTD – Unified Threat Defense
- PCI – Payment Card Industry
- TCO – Total Cost of Ownership
- VMAN – Virtualization Manager

Snort IPS – Benefits and Requirements

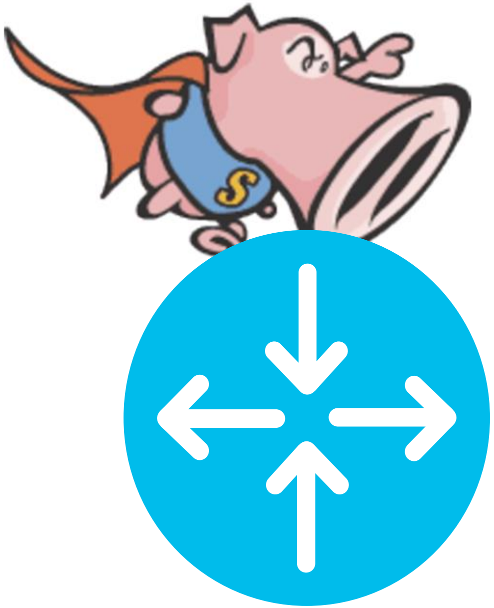
Benefits

- 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)
- Supports IPv6

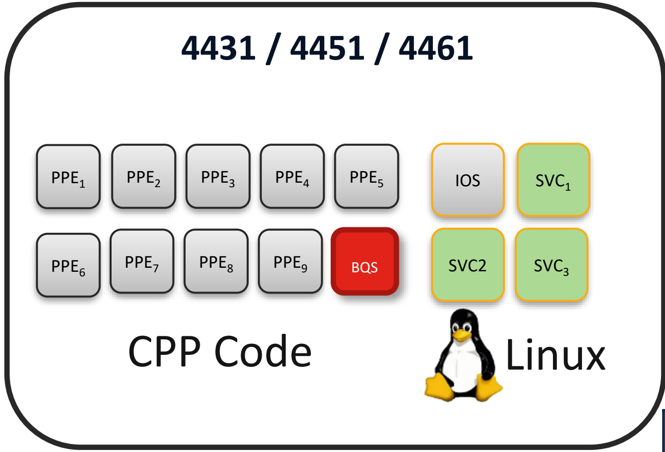
Requirements

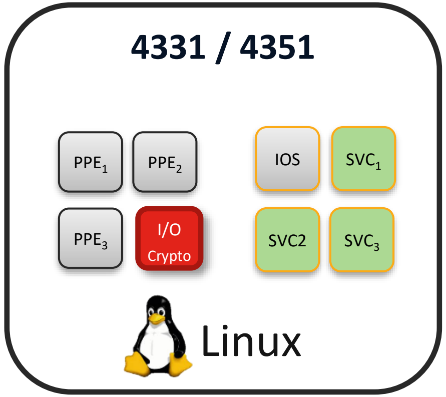
- SEC-K9 license
- 4 GB additional memory
- XE 3.16.1 and above on ISR4K
- XE 16.8.1 and above on ISRv
- XE 16.3.1 and above on CSR
- Subscription (1Yr, 3Yr or 5Yr)
- Monitoring via 3-rd party

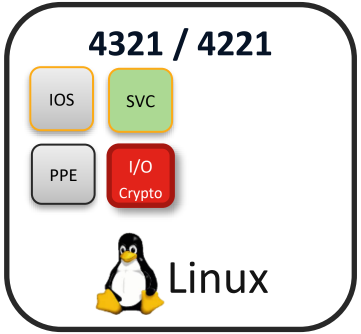
splunk>



Security App Hosting Profile & Resources

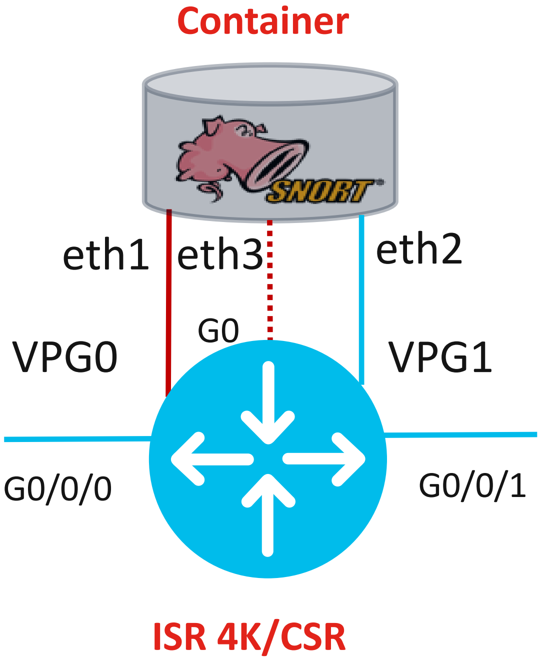






	Total No of CP Cores	Low Profile % of CPU	Medium Profile % of CPU	High Profile % of CPU
4221	2	50%	_	_
4321	2	50%	_	_
4331	4	25%	50%	75%
4351	4	25%	50%	75%
4431	4 (8)	25%	50%	75%
4451	4 (8)	25%	50%	75%
4461	4 (8)	25%	50%	75%

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 – Configuration using VMAN

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 192.0.2.1 255.255.255.252
```

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 192.0.2.2
  activate
```

Step 4 Configuring UTD (service plane)

```
utd engine standard
 logging host 10.12.5.55
 logging syslog
 threat-inspection
  threat protection (protection-ips, detection-ids)
  policy security (balanced, connectivity)
  logging 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 (fail open is default)
```

Step 6 Whitelisting (optional)

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

FYI

Intrusion Prevention – Configuration using IOx

Step 1 Configure virtual service

```
app-hosting install appid utd package bootflash:utd.tar
```

Step 2 Configure Port Groups

```
interface VirtualPortGroup0
  description Management interface
  ip address 192.168.1.1 255.255.255.252
interface VirtualPortGroup1
  description Data interface
  ip address 192.0.2.1 255.255.255.252
```

Step 3 Activate virtual service and configure

```
iox
app-hosting appid utd
app-vnic gateway0 virtualportgroup 0 guest-interface 0
  guest-ipaddress 192.168.1.2 netmask 255.255.255.252
app-vnic gateway1 virtualportgroup 1 guest-interface 1
  guest-ipaddress 192.0.2.2 netmask 255.255.255.252
app-resource package-profile low (medium, high)
start
```

Step 4 Configuring UTD (service plane)

```
utd engine standard
 logging host 10.12.5.55
 logging syslog
 threat-inspection
  threat protection (protection-ips, detection-ids)
  policy security (balanced, connectivity)
  logging 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 (fail open is default)
```

Step 6 Whitelisting (optional)

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

Snort IPS - Resources

FYI

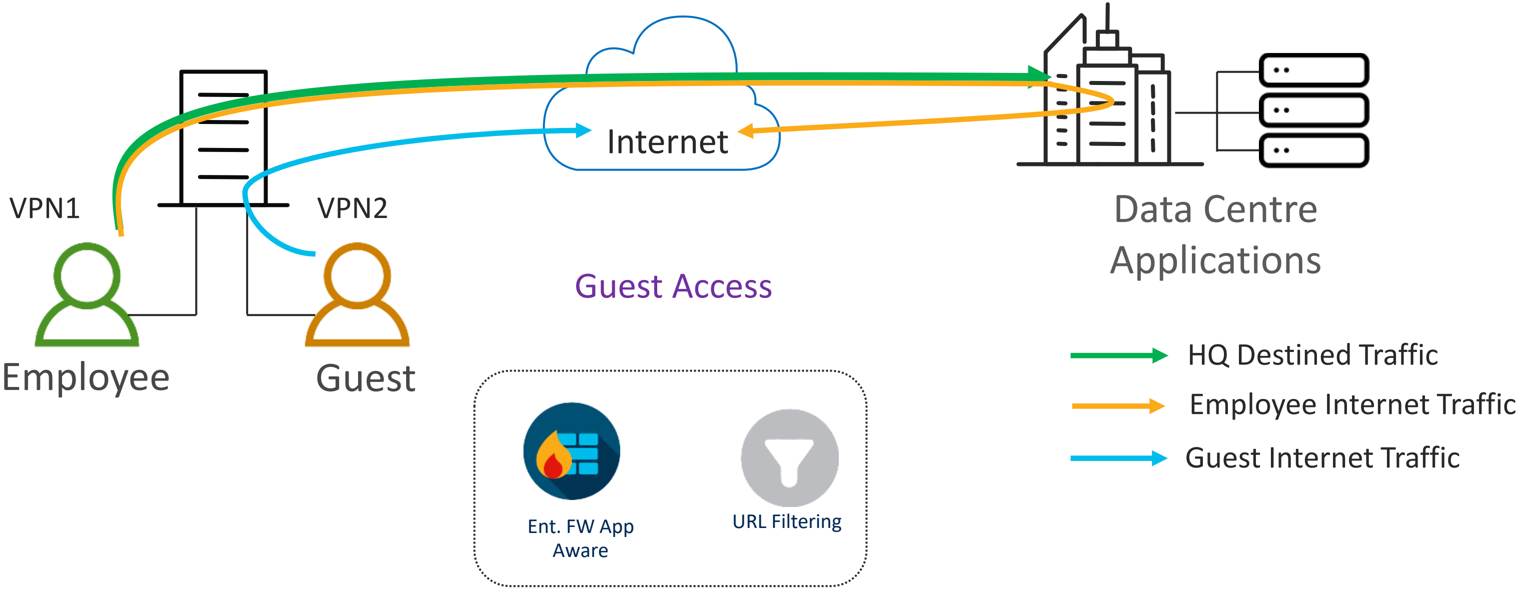
At-A-Glance
http://www.cisco.com/c/dam/en/us/products/collateral/security/router-security/at-a-glance-c45-735895.pdf

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

URL Filtering

URL Filtering Use Case: Guest Internet Access



URL – Filtering - Appendix

FYI

- VPG – Virtual Port Group
- DIA – Direct Internet Access
- CSR - Cloud Services Router
- WL – White Listing
- OVA – Open Virtual Appliance
- UTD – Unified Threat Defense
- PCI – Payment Card Industry
- TCO – Total Cost of Ownership
- VMAN – Virtualization Manager

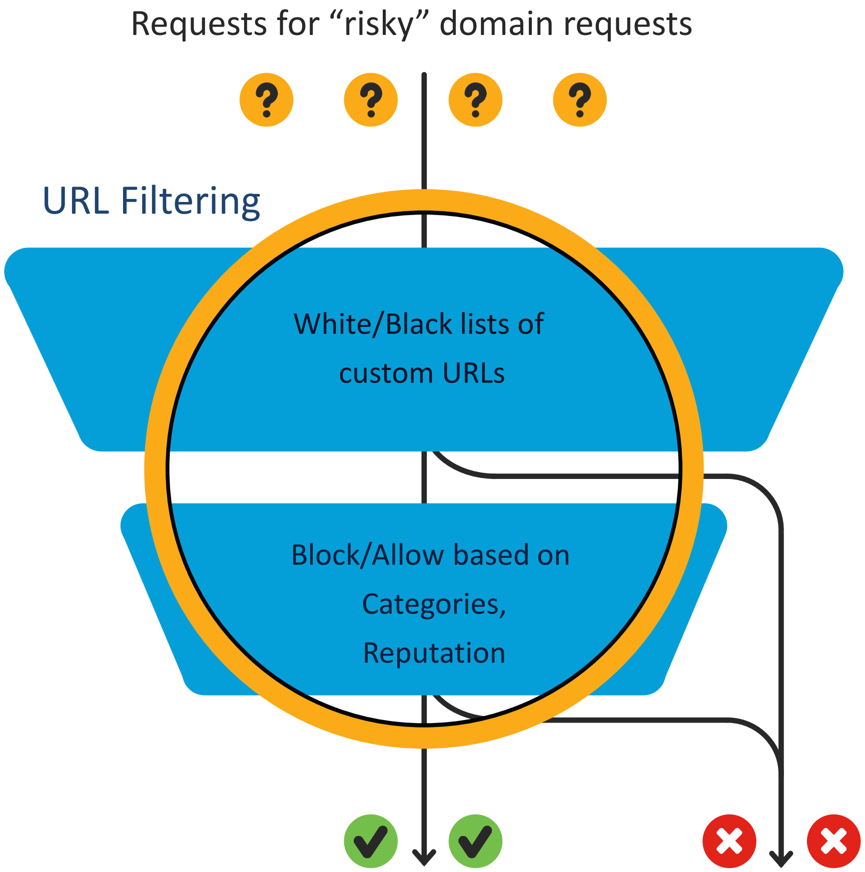
URL Filtering

Benefits

- Content Filtering for BYOD
- 82+ Web Categories with dynamic updates from Webroot/BrightCloud
- Block based on Web Reputation score
- Create custom Black and White Lists
- Customizable Block Page
- Supports VRF and IPv6

Requirements

- SEC-K9 license
- 4 GB additional memory
- XE 16.3 and above on CSR
- Multitenancy 16.6.1 on CSR


Requests for "risky" domain requests
URL Filtering
White/Black lists of custom URLs
Block/Allow based on Categories, Reputation

URL Filtering – Configuration using VMAN

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 192.0.2.1 255.255.255.252
```

Step 3 Activate virtual service and configure

```
virtual-service utd
  vnic gateway VirtualPortGroup0
    guest ip address 172.18.21.2
  vnic gateway VirtualPortGroup1
    guest ip address 192.0.2.2
  profile urlf-low
  activate
```

Step 4 Configure (optional) white and black list

```
parameter-map type regex wlist
   pattern www.google.com
   pattern www.cisco.com
parameter-map type regex blist
  pattern www.exmaplehoo.com
  pattern www.bing.com
```

Step 5 Configure web-filter profile

```
utd engine standard multi-tenancy
 web-filter url profile URL-FILTER-POLICY
  blacklist
    parameter-map regex blist
  whitelist
    parameter-map regex wlist
```

URL Filtering – Configuration using VMAN

Step 6 Attach blacklist and whitelist to the profile

```
utd engine standard multi-tenancy
 web-filter url profile URL-FILTER-POLICY
   categories block
    abortion
    abused-drugs
    adult-and-pornography
    bot-nets
  alert all
  reputation
   block-threshold moderate-risk
```

Step 7 Configure and attach block page

```
utd engine standard multi-tenancy
 web-filter block page profile block-URL-FILTER-      POLICY
   text “WHAT ARE YOU DOING??!!!”
 web-filter url profile URL-FILTER-POLICY
   block page-profile block-URL-FILTER-POLICY
```

Step 8 Configure data plane policy

```
utd global
  logging syslog
 !
utd engine standard multi-tenancy
 policy utd-policy
  vrf 1, 2
  all-interfaces
  fail close
  web-filter url profile URL-FILTER-POLICY
```

FYI

URL Filtering – Configuration using IOx

Step 1 Configure virtual service

```
app-hosting install appid utd package bootflash:utd.tar
```

Step 2 Configure Port Groups

```
interface VirtualPortGroup0
  description Management interface
  ip address 192.168.1.1 255.255.255.252
interface VirtualPortGroup1
  description Data interface
  ip address 192.0.2.1 255.255.255.252
```

Step 3 Activate virtual service and configure

```
iox
app-hosting appid utd
app-vnic gateway0 virtualportgroup 0 guest-interface 0
  guest-ipaddress 192.168.1.2 netmask 255.255.255.252
app-vnic gateway1 virtualportgroup 1 guest-interface 1
  guest-ipaddress 192.0.2.2 netmask 255.255.255.252
app-resource package-profile urlf-low
start
```

Step 4 Configure (optional) white and black list

```
parameter-map type regex wlist
   pattern www.google.com
   pattern www.cisco.com
parameter-map type regex blist
  pattern www.exmaplehoo.com
  pattern www.bing.com
```

Step 5 Configure web-filter profile

```
utd engine standard multi-tenancy
 web-filter url profile URL-FILTER-POLICY
   categories block
    abortion
    abused-drugs
    adult-and-pornography
    bot-nets
  alert all
  reputation
   block-threshold moderate-risk
```

FYI

URL Filtering – Configuration using IOx

Step 6 Attach blacklist and whitelist to the profile

```
utd engine standard multi-tenancy
 web-filter url profile URL-FILTER-POLICY
   blacklist
    parameter-map regex blist
   whitelist
    parameter-map regex wlist
```

Step 7 Configure and attach block page

```
utd engine standard multi-tenancy
 web-filter block page profile block-URL-FILTER-        POLICY
   text “WHAT ARE YOU DOING??!!!”
 web-filter url profile URL-FILTER-POLICY
   block page-profile block-URL-FILTER-POLICY
```

Step 8 Configure data plane policy

```
utd global
  logging syslog
 !
utd engine standard multi-tenancy
 policy utd-policy
  vrf 1, 2
  all-interfaces
  fail close
  web-filter url profile URL-FILTER-POLICY
```

URL Filtering - Resources

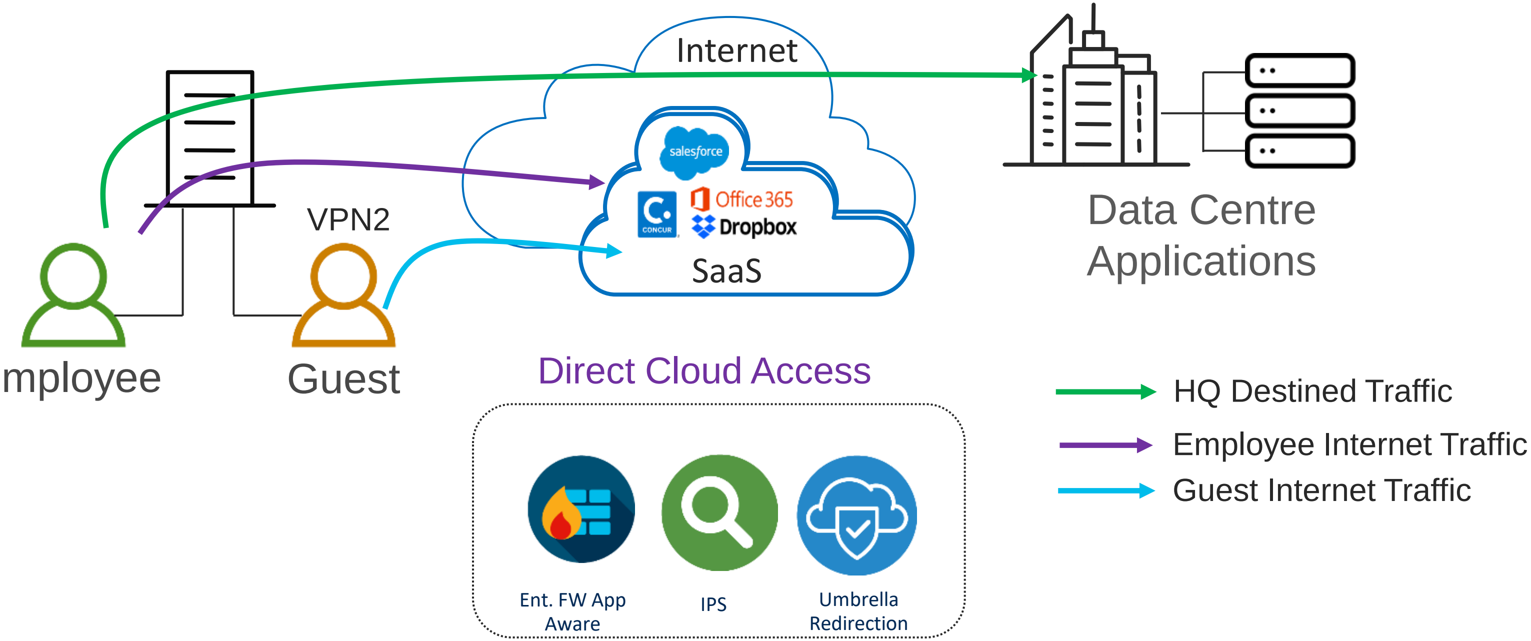
FYI

Configuring Multi-Tenancy for Unified Threat Defense

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_utd/configuration/xe-16/sec-data-utd-xe-16-book/sec-data-utd-xe-16-book_chapter_011.pdf

Cisco Umbrella Integration

Cisco Umbrella Integration



Internet

salesforce

Office 365

Dropbox

CONCUR

SaaS

VPN2

Employee

Guest

Data Centre Applications

Direct Cloud Access

Ent. FW App Aware

IPS

Umbrella Redirection

HQ Destined Traffic

Employee Internet Traffic

Guest Internet Traffic

Cisco Umbrella Integration

FYI

- 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.

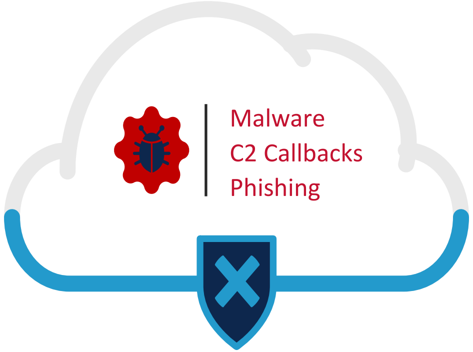
Umbrella Integration – Benefits and Requirements

Benefits

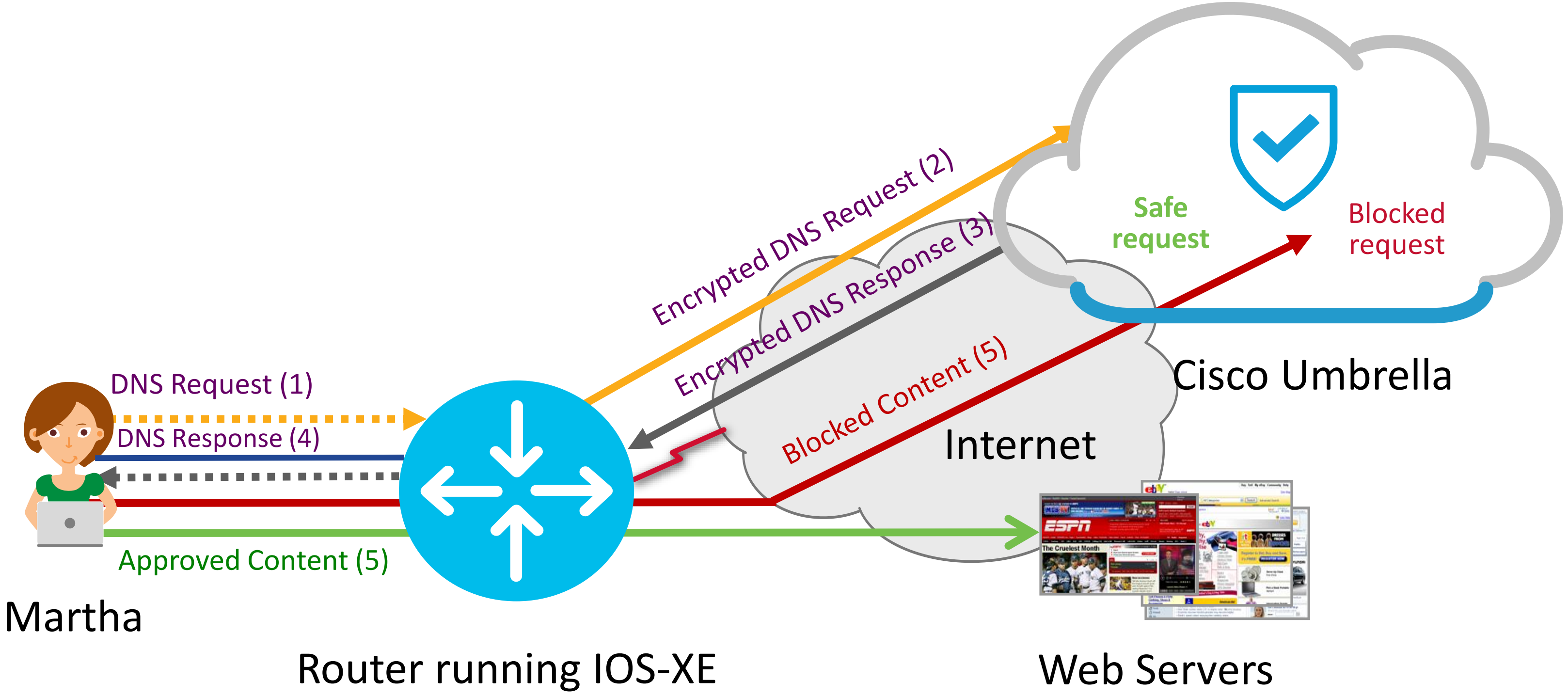
- DNS layer protection
- No need to look within HTTP or HTTPS packets
- Complements ISR Integrated Security
- Configure policies based on ’tags’ per interface
- Supports VRF

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
- XE 16.10.1 and above on ASR1K
- XE 16.3 and above on CSR
- Per device subscription
- Monitoring and Reporting via Umbrella Portal

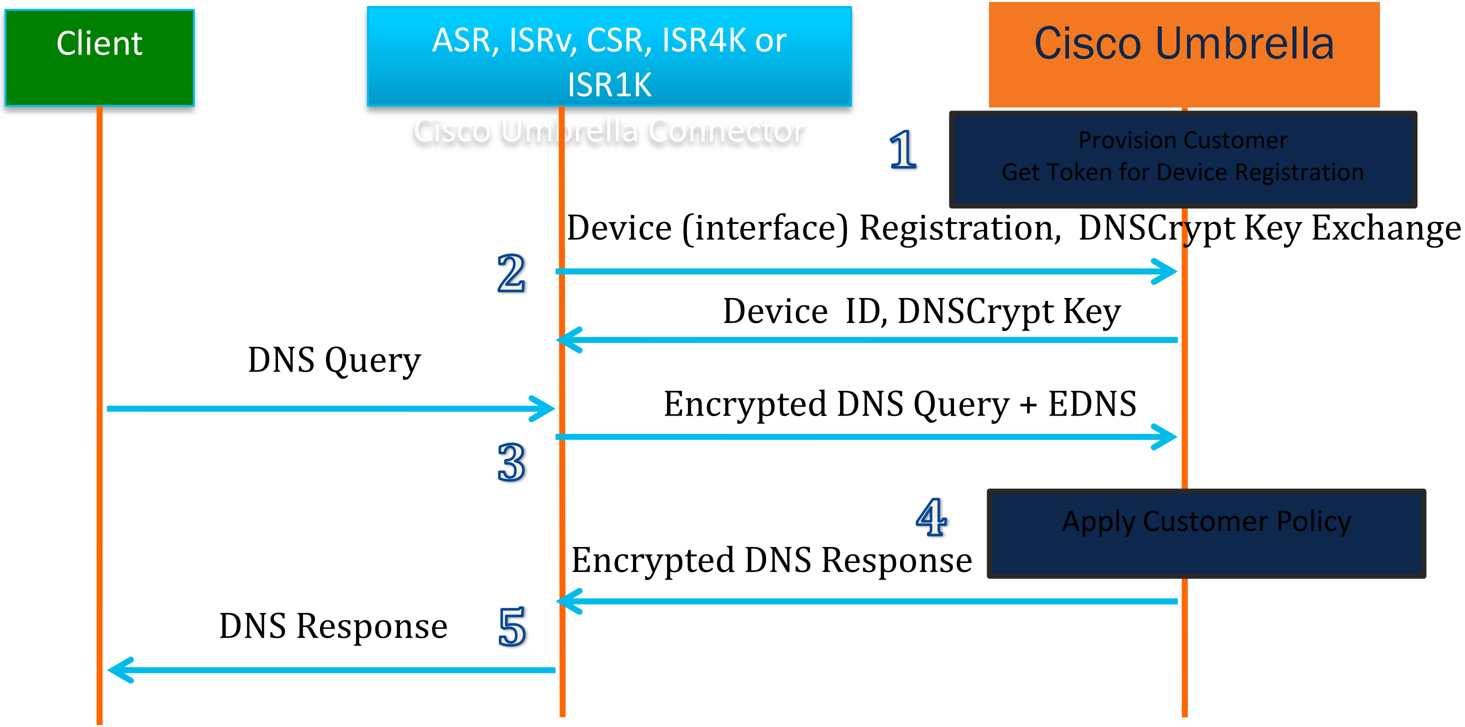


Cisco Umbrella Integration - Solution Overview



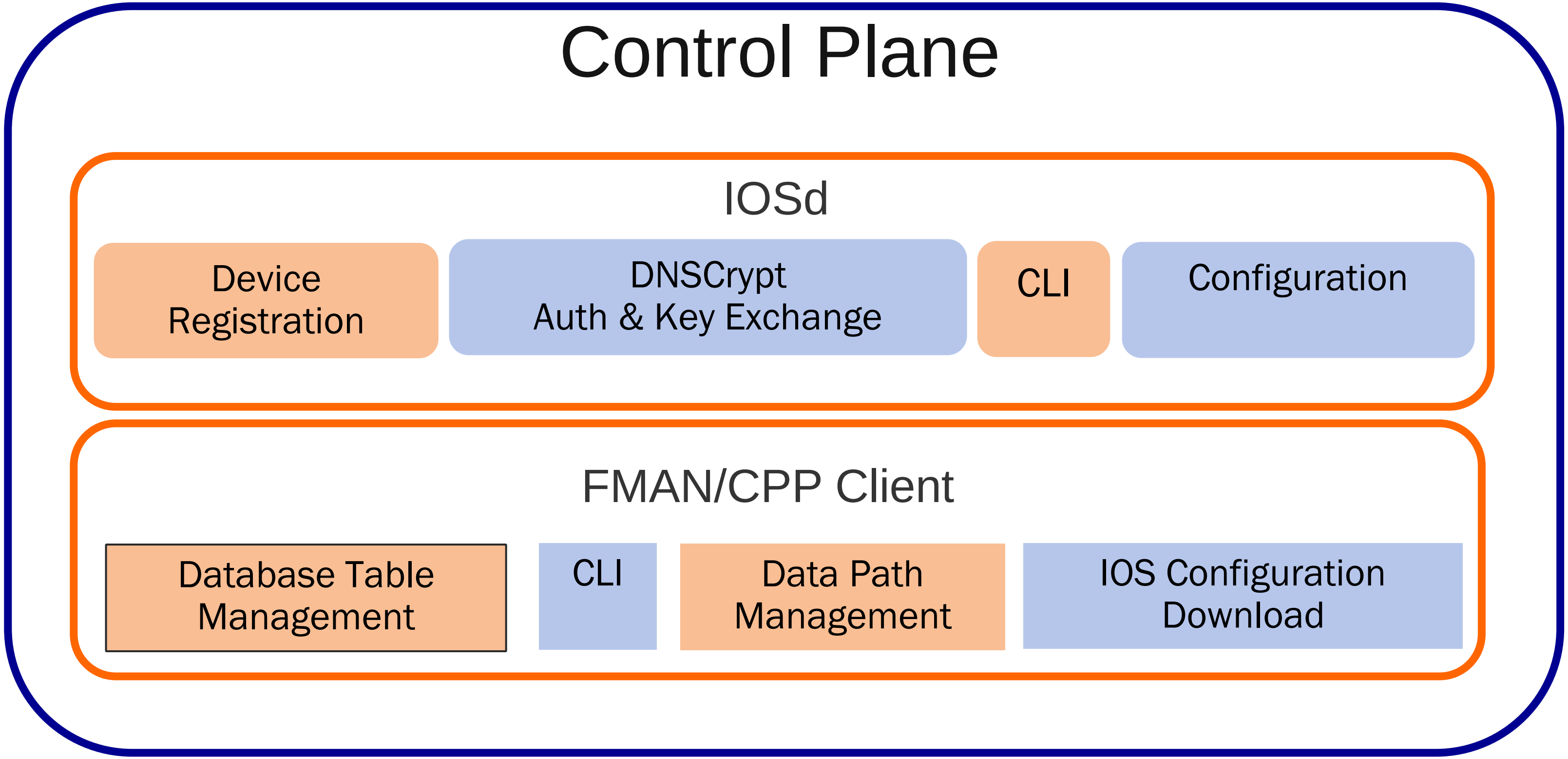
Cisco Umbrella Integration - Packet Flow with DNSCrypt

FYI



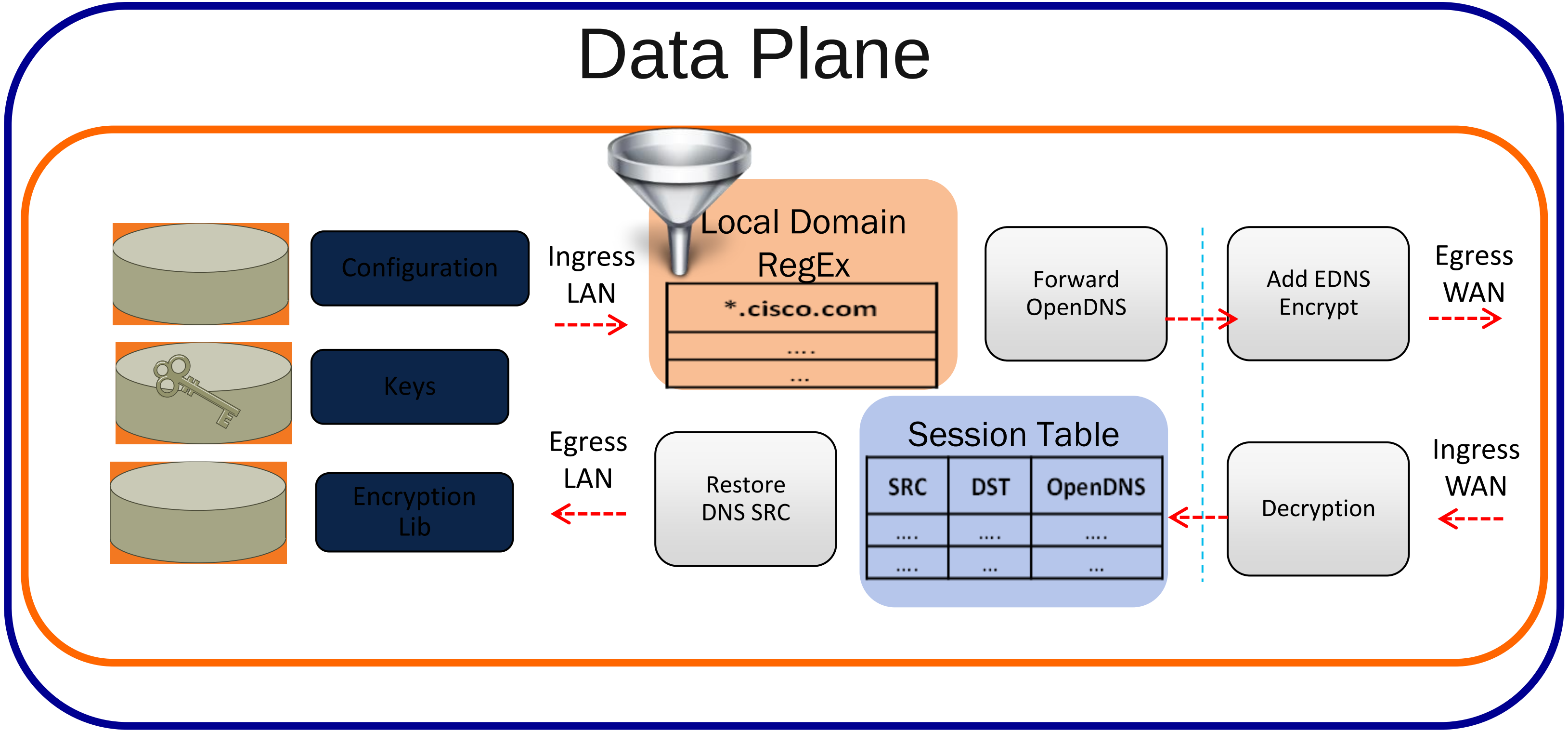
Cisco Umbrella – Software Architecture

FYI



Cisco Umbrella – Software Architecture

FYI



*.cisco.com
....
...

SRC	DST	OpenDNS
....	....	....
....	...	...

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
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 - Resources

FYI

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

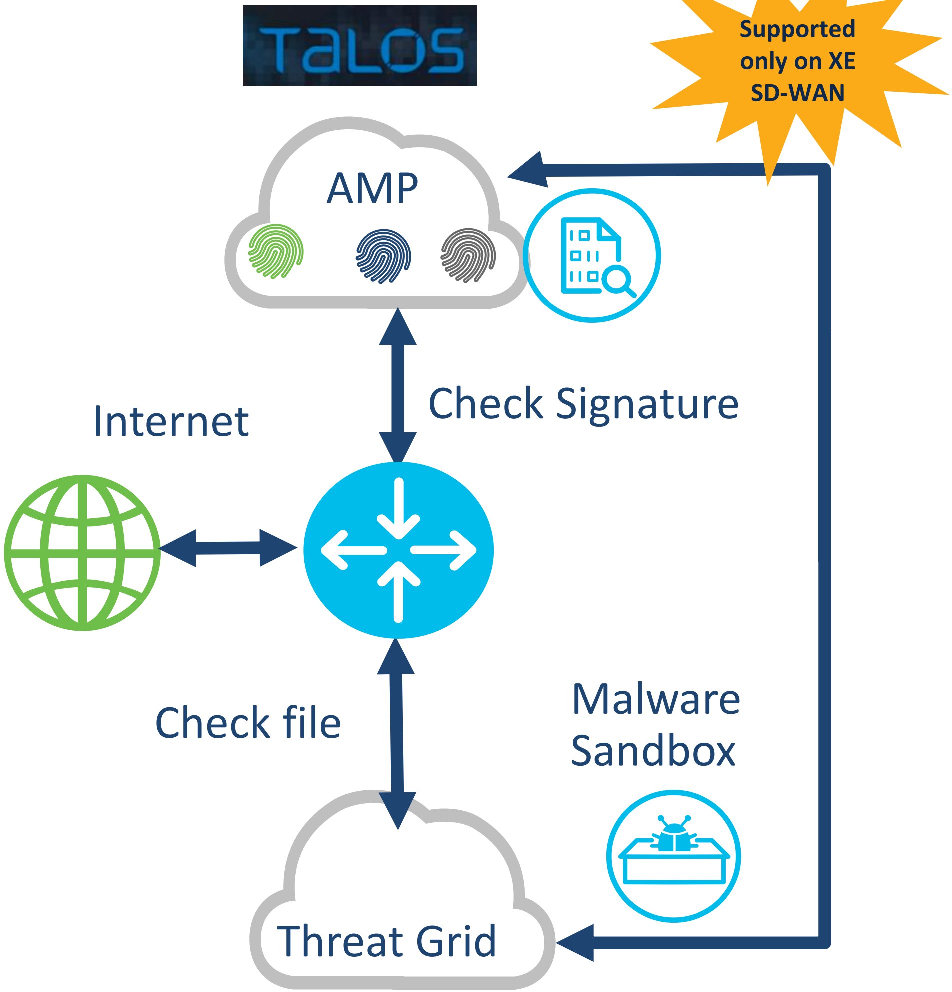
CWS EOL announcement:
http://www.cisco.com/c/en/us/products/collateral/security/cloud-web-security/eos-eol-notice-c51-738257.html

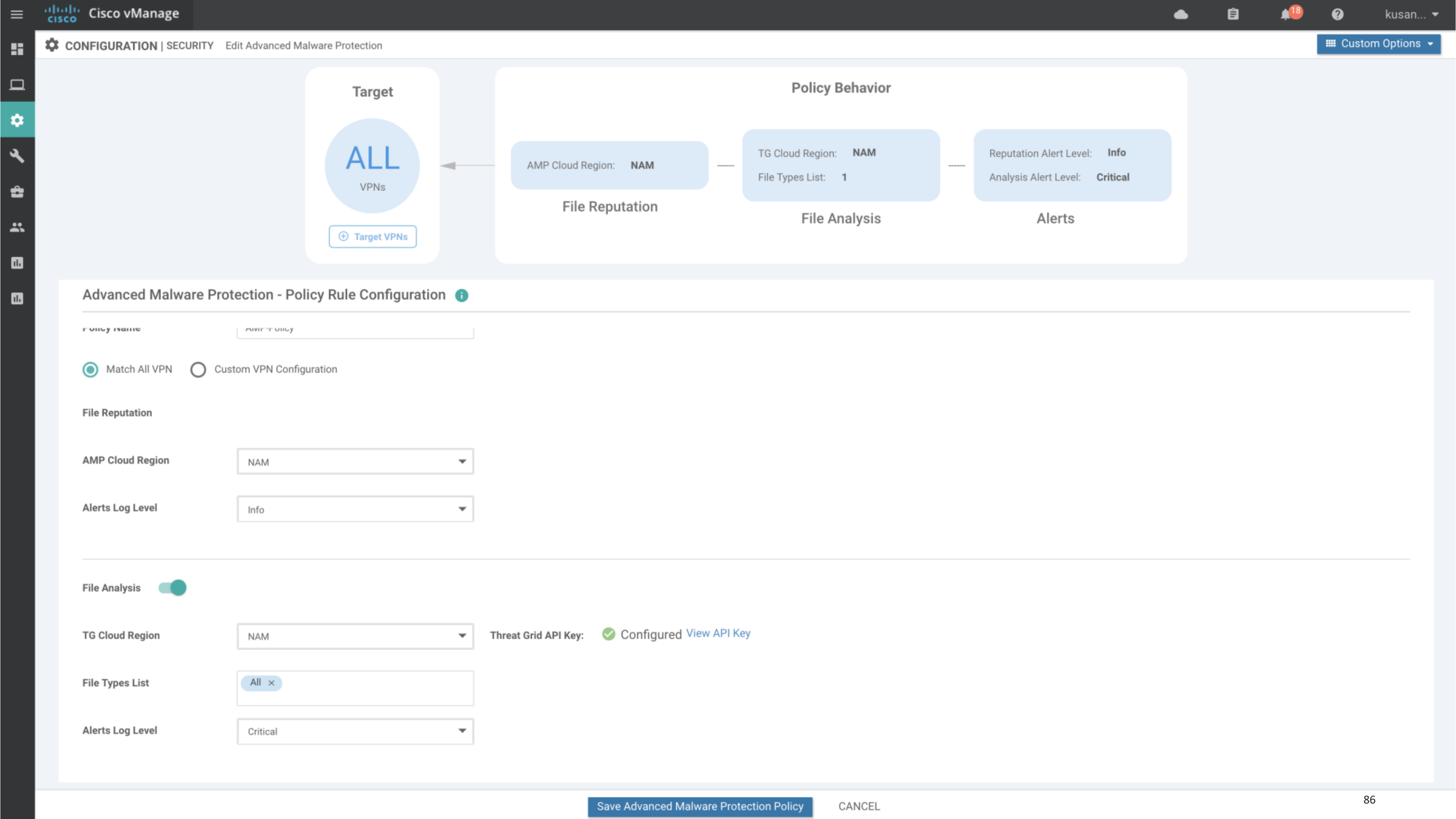
Cisco Umbrella Video:
https://youtu.be/CGeLQTWKaPQ

Advanced Malware Protection and Threat Grid

Advanced Malware Protection and ThreatGrid

- Integration with AMP
  - File reputation
  - File retrospection
- Integration with Threat Grid
  - File Analysis
- Backed with valuable Threat Intelligence
- HTTP, FTP, SMB, IMAP, POP3, SMTP





AMP Cloud Region: NAM

TG Cloud Region: NAM

File Types List: 1

Reputation Alert Level: Info

Analysis Alert Level: Critical

Advanced Malware Protection - Policy Rule Configuration

Policy Name: AMP-Policy

● Match All VPN ○ Custom VPN Configuration

File Reputation

AMP Cloud Region: NAM

Alerts Log Level: Info

File Analysis (toggle on)

TG Cloud Region: NAM

Threat Grid API Key: ✓ Configured View API Key

File Types List: All ×

Alerts Log Level: Critical

FYI

AMP and TG – CLI rendered

Step 1 Configure file-reputation and file-analysis

```
utd engine standard multi-tenancy
 utd global
  file-reputation
   cloud-server cloud-isr-asn.amp.cisco.com
   est-server   cloud-isr-est.amp.cisco.com
  file-analysis
   cloud-server isr.api.threatgrid.com
   apikey 0 vlepa30tnfg76cning92e7p
```

Step 2 Configure File inspection

```
utd engine standard multi-tenancy
 file-reputation profile AMP-Policy-fr-profile
  alert level info
 file-analysis profile AMP-Policy-fa-profile
  file-types
   pdf
   new-office ..
 alert level critical
```

Step 4 Configure File Inspection Profile

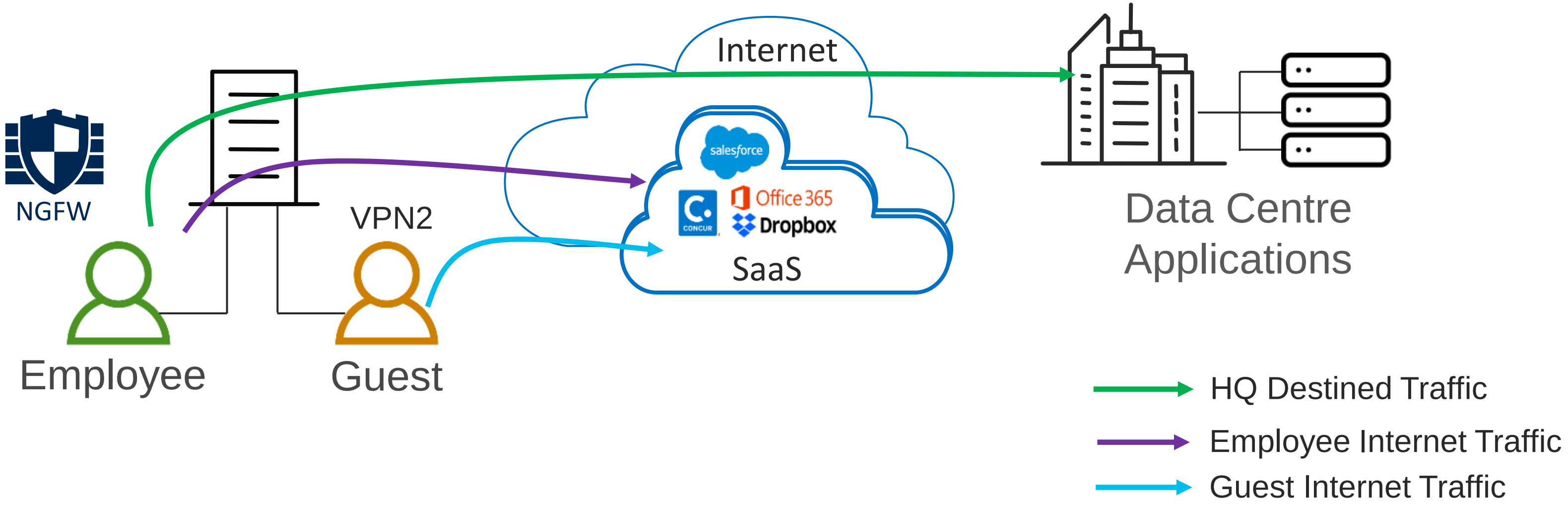
```
utd engine standard multi-tenancy
 file-inspection profile AMP-Policy-fi-profile
  analysis profile AMP-Policy-fa-profile
  reputation profile AMP-Policy-fr-profile
```

Step 5 Configure Policy

```
utd engine standard multi-tenancy
 policy utd-policy-vrf-1
  all-interfaces
  fail close
  file-inspection profile AMP-Policy-fi-profile
  vrf 1
 policy utd-policy-vrf-global
  all-interfaces
  fail close
  file-inspection profile AMP-Policy-fi-profile
  vrf global
```

Firepower Threat Defense for ISR

Firepower Threat Defense for ISR



NGFW

VPN2

Employee

Guest

Internet

SaaS

Data Centre Applications

→ HQ Destined Traffic

→ Employee Internet Traffic

→ Guest Internet Traffic

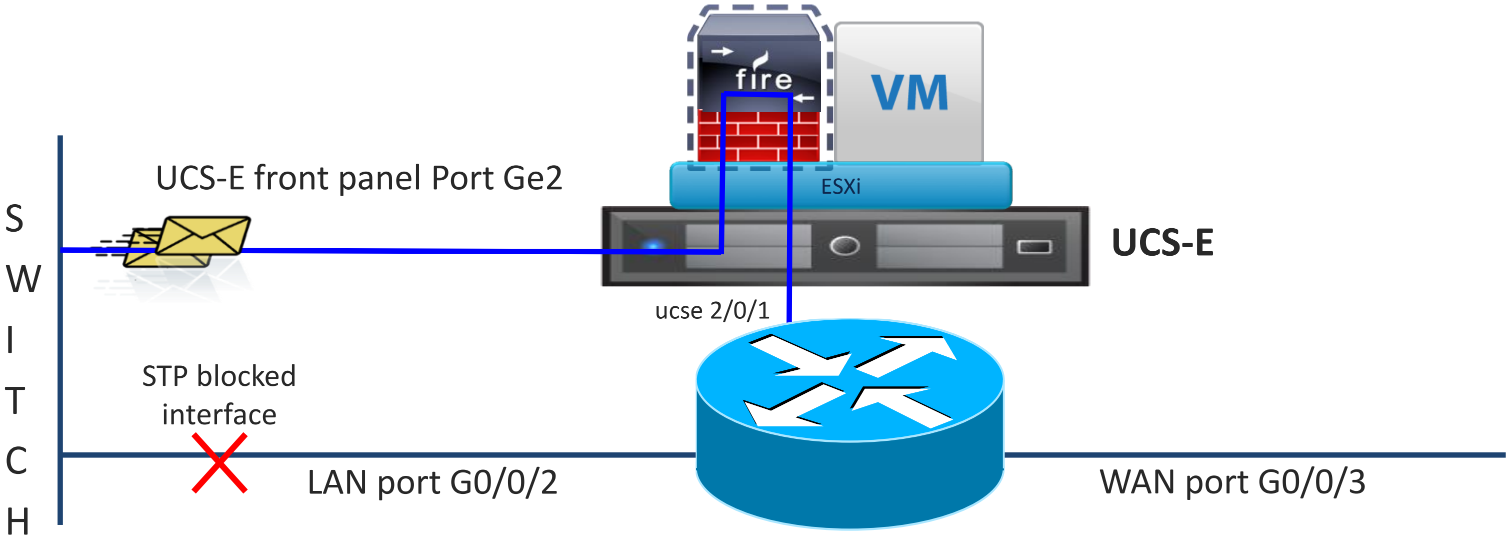
Firepower Threat Defense for ISR - Appendix

FYI

- 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-series - Unified computing system – Express (Blade servers for ISR routers)
- AMP – Advance Malware Protection
- TG – Threat Grid

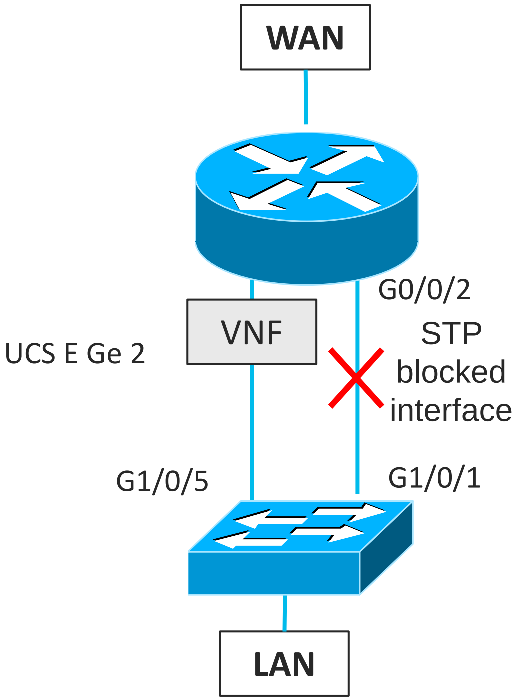
Firepower Threat Defense for ISR - using BDI method

- Host the sensor VM on the UCS-E
- FTDv 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 - FTDv 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

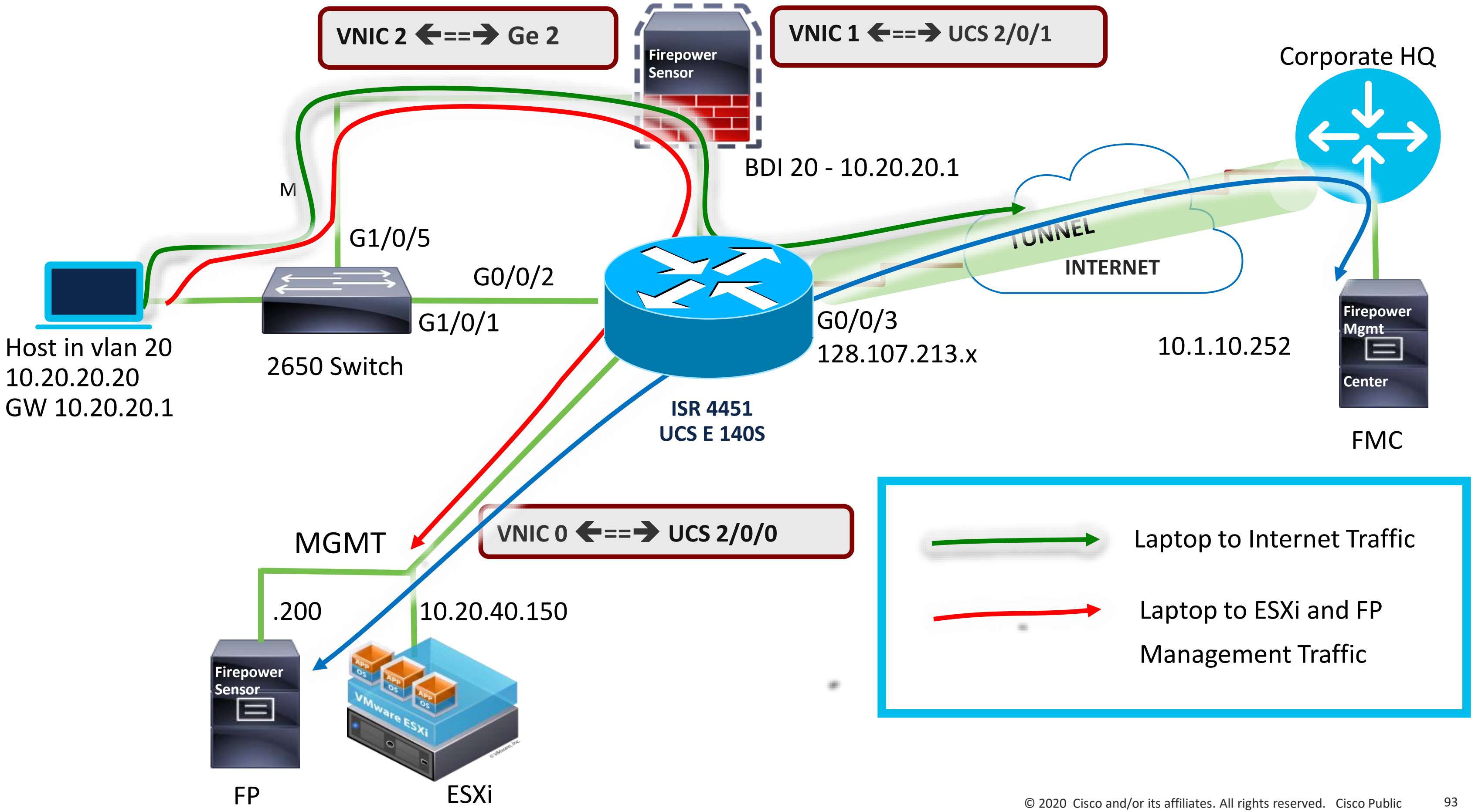
```
interface GigabitEthernet1/0/1
 description connected to ISR-4451 G0/0/2
 switchport trunk allowed vlan 20,30
 switchport mode trunk
 spanning-tree cost 100
```

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
```

FYI

Firepower Threat Defense for ISR – FTDv using BDI



Firepower Threat Defense for ISR - FTDv using BDI

FYI

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

vNIC1 **Outside**

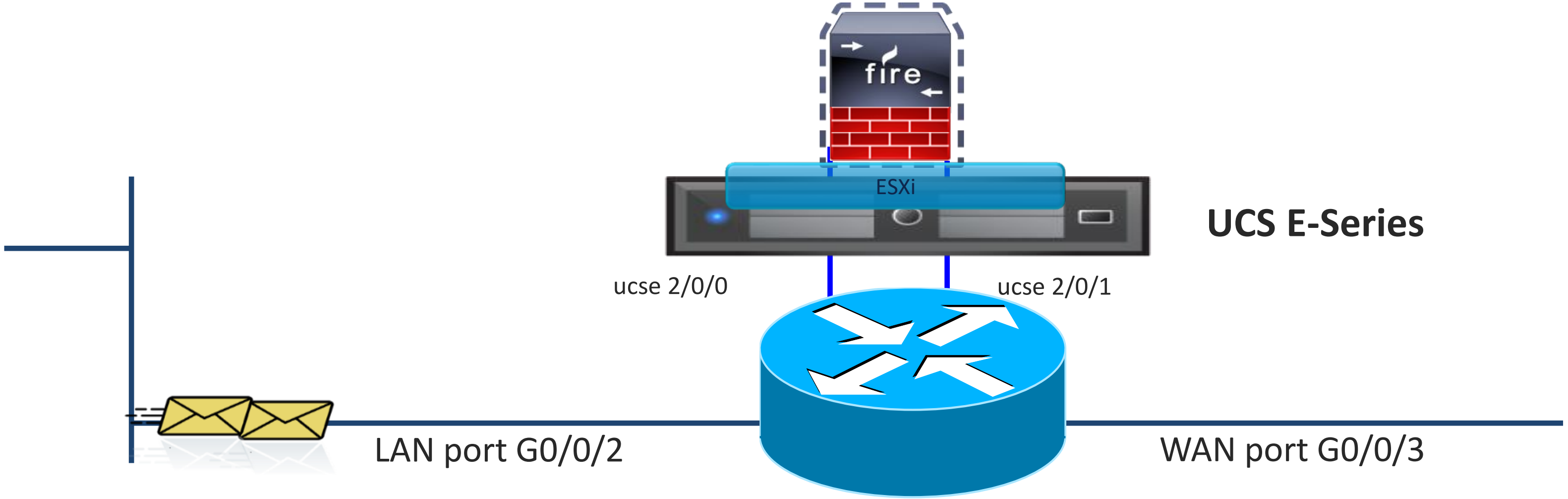
```
interface ucse2/0/1
 no ip address
 negotiation auto
 switchport mode trunk
service instance 20 ethernet
  encapsulation dot1q 20
  rewrite ingress tag pop 1 symmetric
  bridge-domain 20
interface BDI20
 ip address 10.20.20.1 255.255.255.0
 ip nat inside
```

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

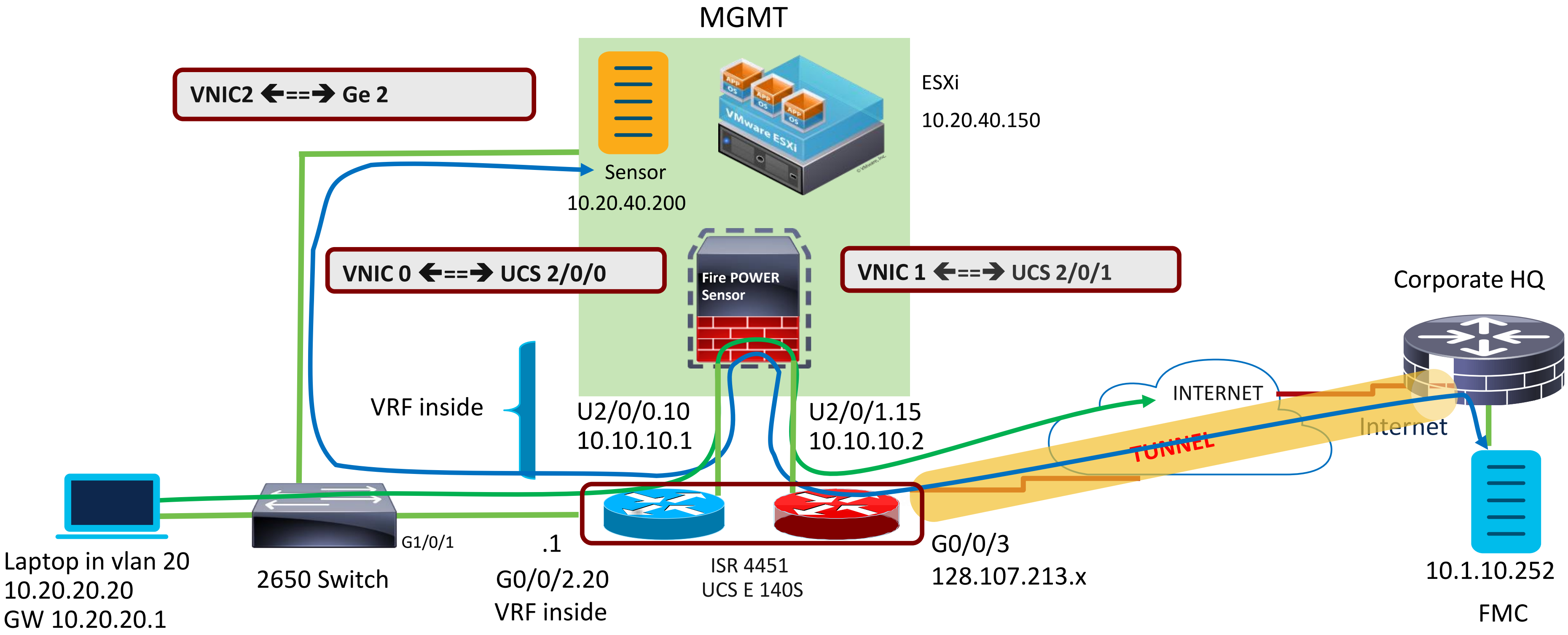
```
interface GigabitEthernet0/0/3
 ip address 128.107.213.x 255.255.255.0
 ip nat outside
```

Firepower Threat Defense for ISR – using VRF method

- Host the Sensor on the UCS-E
- FTDv is in routed mode
- Packets ingress via the router’s copper port
- Inside interface of FTDv is ucse 2/0/0
- Firepower sensor examines traffic; allowed packets are sent to router using ucse 2/0/1

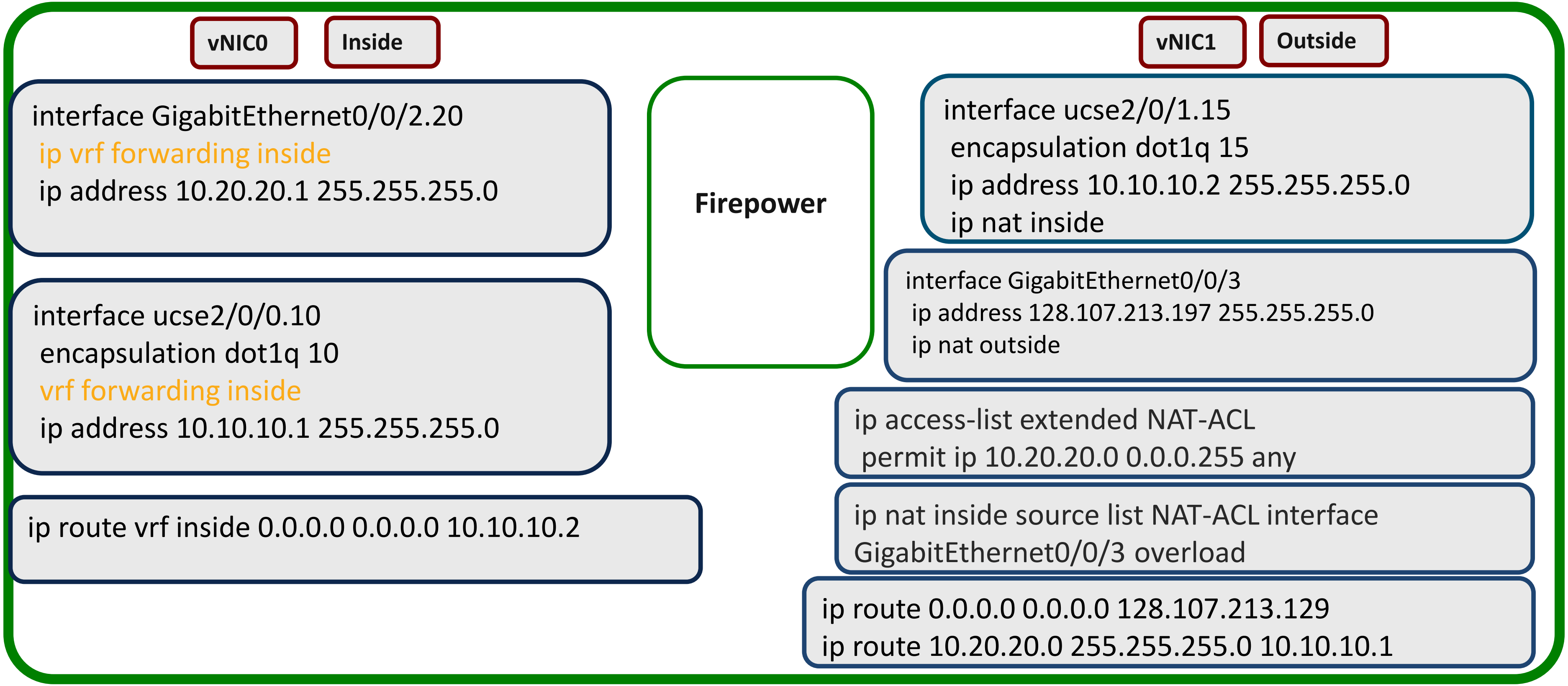


Firepower Threat Defense for ISR – FTDv using VRF



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 – FTDv 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
```

Firepower Threat Defense for ISR - Resources

FYI

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

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://community.cisco.com/t5/security-documents/firepower-threat-defense-ngipsv-for-isr-ips-using-front-panel/ta-p/3155017

Firepower Threat Defense for ISR 4K & G2 - IPS inline mode using VRF method
https://community.cisco.com/t5/security-documents/firepower-threat-defense-ngipsv-for-isr-4k-amp-g2-ips-inline/ta-p/3162267

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

Additional Resources

FYI

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-c11-739289.html#_Toc486544453

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

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

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

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

Additional Resources

FYI

Cisco NGFWv Data Sheet

https://www.cisco.com/c/en/us/products/collateral/security/firepower-ngfw/datasheet-c78-742480.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-fdm-vmware-qsg.html?referring_site=RE&pos=1&page=https://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/vmware/ftdv/ftdv-vmware-qsg.html

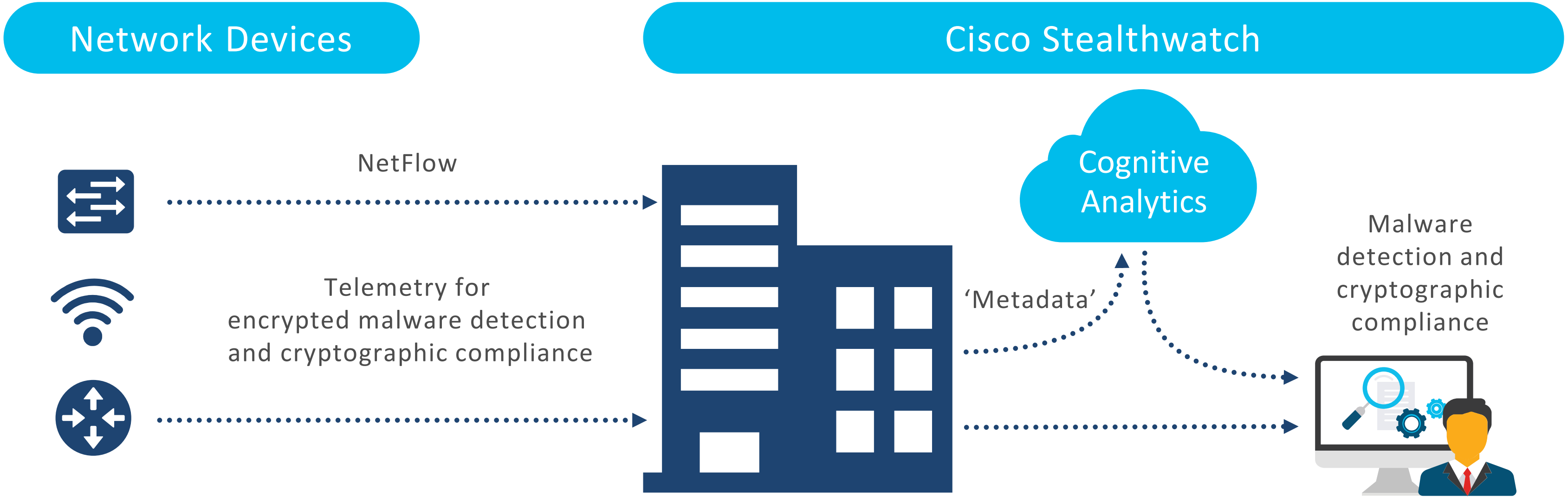
NGFWv Communities Documentation

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

https://community.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 without decrypting

Crypto audit

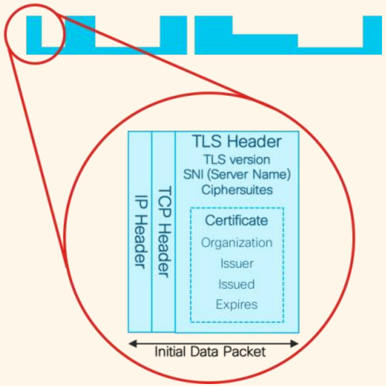
Requirements

- SEC-K9 license
- XE 16.6.2 and above on ASR, ISR 4K, 1K, ISRv and CSR
- Stealthwatch Management
- Supports VRF (16.8.1)
- Support IPv6 (coming in 16.12.1)

How do we inspect encrypted traffic?

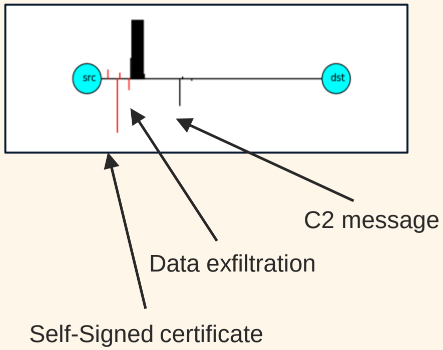
Initial Data Packet

Make the most of the unencrypted fields



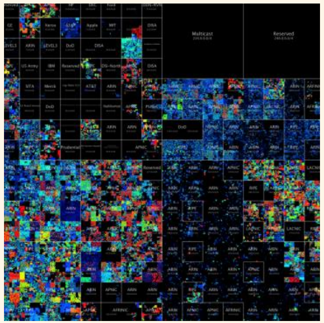
Sequence of Packet Lengths and Times

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 – 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 (ETA) - Resources

FYI

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

FYI

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

Control Plane Security

Control Plane Policing

Police inbound UDP traffic to 16 Kbps

```
ip access-list extended UDP
 permit udp any any
```

```
class-map match-all UDP
 match access-group name UDP
```

```
policy-map CoPP
 class UDP
  police 16000 conform-action transmit exceed-action drop violate-action drop
```

```
control-plane
 service-policy input CoPP
```

Punt Policing and Monitoring

Punt policing frees the RP from having to process noncritical traffic.

- Global Configuration

```
platform punt-police queue 20 9000 10000
```

- Per Interface Configuration (PPS)

```
platform punt-interface rate 10

interface G0/0/3
 punt-control enable 20
```

```
show platform software infrastructure punt statistics
```

Introduced in IOS-XE 16.4.1

Management Plane Security

Management Plane Protection

- Allow only ssh and snmp

```
Router(config)# control-plane host
Router(config-cp-host)# management-interface GigabitEthernet 0/0/3 allow ssh snmp
```

```
Router# show management-interface

Management interface GigabitEthernet 0/0/3
Protocol Packets processed
ssh 0
snmp 0
```

IOS-XE VS XE SD-WAN

IOS-XE

ZBF+NBAR2

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

Snort IPS

- ISR 4K Series Routers
- ISRv
- CSR

URL Filtering

- CSR

Umbrella Integration

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

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

XE SD-WAN

Ent. FW App Aware

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

IPS

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

URL-F

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

DNS/web-layer sec

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

AMP (file reputation)

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

TG (file analysis)

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

* CSR – Only on AWS & KVM

FYI

Security Features on XE SD-WAN Routers – 16.10.1

Ent FW App Aware and DNS/web-layer security will work with default 4 GB DRAM

Platforms/Featu res	Ent FW with App Awarenes s	IPS/IDS	URL Filtering	AMP **	TG **	DNS/web-layer Monitoring *
Cisco - CSR	Y	Y	Y	Y	Y	Y
Cisco – ENCS (ISRv)	Y	Y	Y	Y	Y	Y
Cisco – ISR4K (4461,4451 4431, 4351, 4331, 4321, 4221-X)	Y	Y	Y	Y	Y	Y
Cisco – ISR1K (1111X-8P)	Y	Y	Y	Y	N	Y
Cisco - ASR1K 1001-HX, 1002-HX, 1001-X, 1002-X)	Y	N/A	N/A	N/A	N/A	Y

* Need Umbrella Subscription for enforcement

** XE SD-WAN 16.11.1a and vManage 19.1

FYI

IOS-XE VS XE SD-WAN

Feature		**IOS-XE**	**XE SD-WAN**
Ent. Firewall App Aware	Custom zone	Y	Y
	Self Zone	Y	Y
	default Zone	Y	N
	Resource Management	Y	N
	SYN Cookie Protection	Y	N
	Multi Tenancy	Y	Y
	IPV6	Y	N
	L7 Inspection	Y	N
	SGT	Y	N
	High Availability	Y	N
	HSL Logging	Y	Y
IPS		Y	Y
URL Filtering		Y	Y
DNS Layer Security		Y	Y
AMP & TG		N	Y
ETA		Y	N

FYI

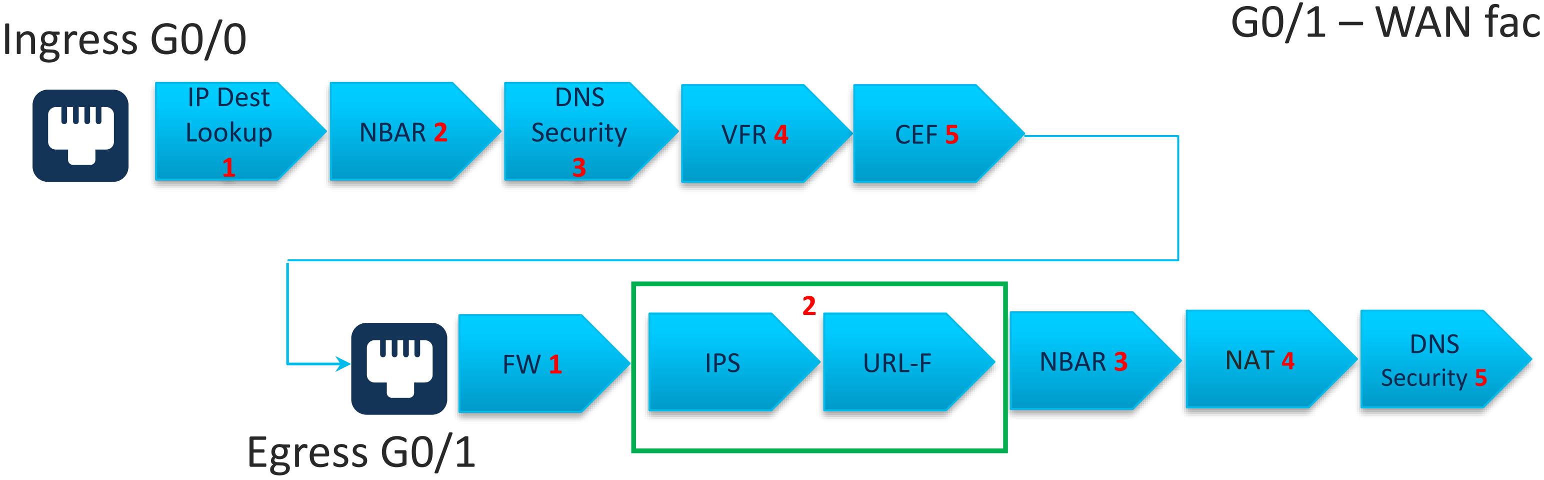
IOS-XE VS XE SD-WAN

Feature	IOS-XE	XE SD-WAN
Control Plane Protection	Y	N
Management Plane Protection	Y	road-map
Default WAN interface protection	N	Y (only allow known tunnel end points to send traffic)

IOS-XE Security Features – Order of Operation

LAN to WAN

G0/0 – LAN facing
G0/1 – WAN facing

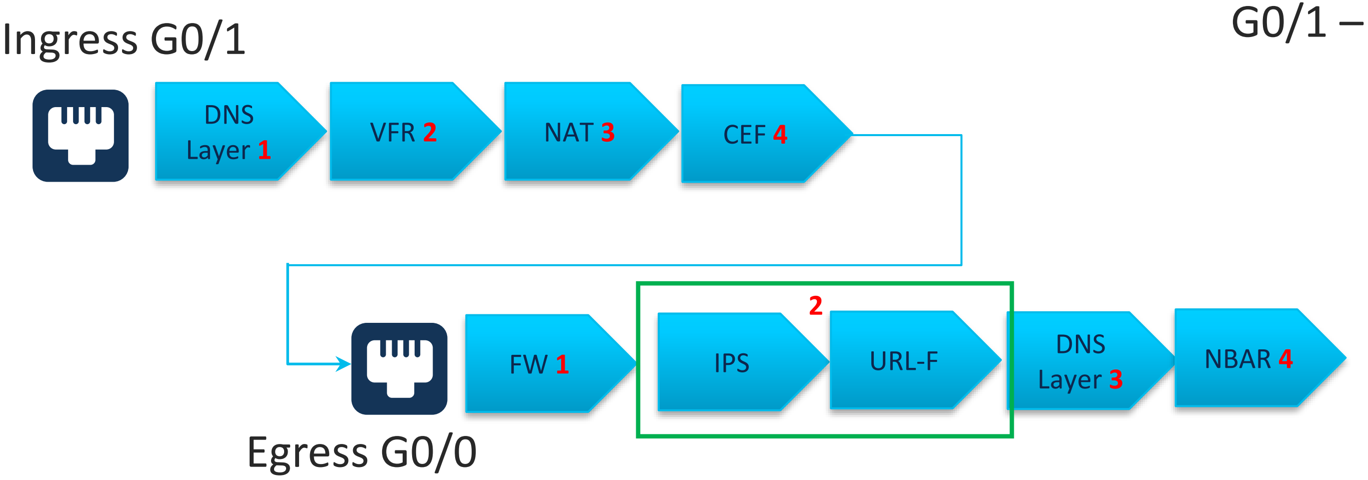


UTD – Unified Threat Defense

IOS-XE Security Features – Order of Operation

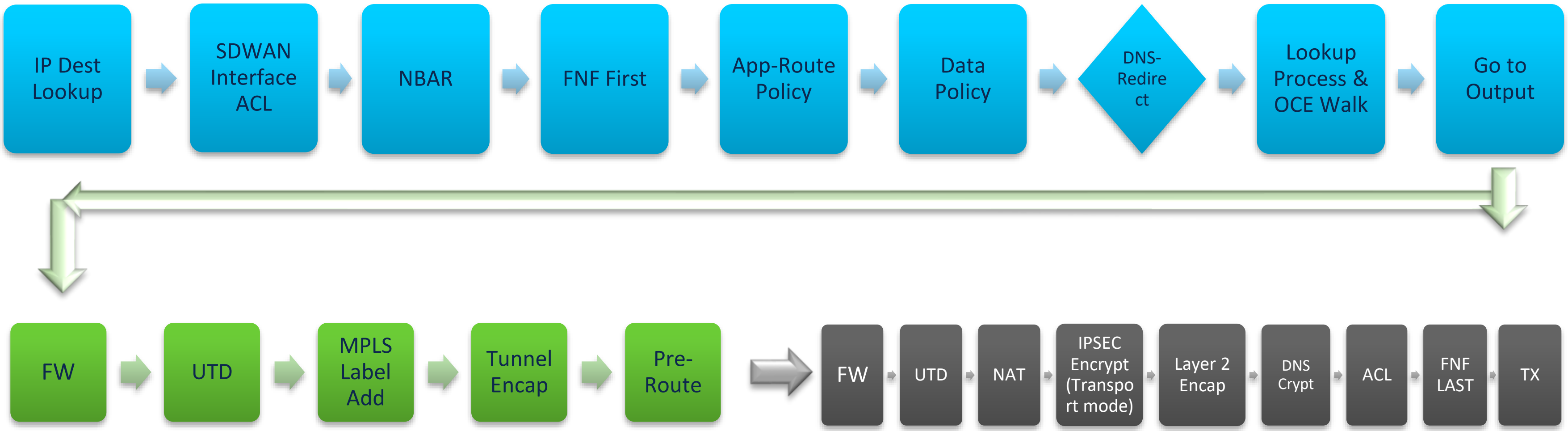
WAN to LAN

G0/0 – LAN facing
G0/1 – WAN facing



UTD (Unified Threat Defense)

XE SD-WAN: From LAN to WAN



IP Dest Lookup → SDWAN Interface ACL → NBAR → FNF First → App-Route Policy → Data Policy → DNS-Redirect → Lookup Process & OCE Walk → Go to Output

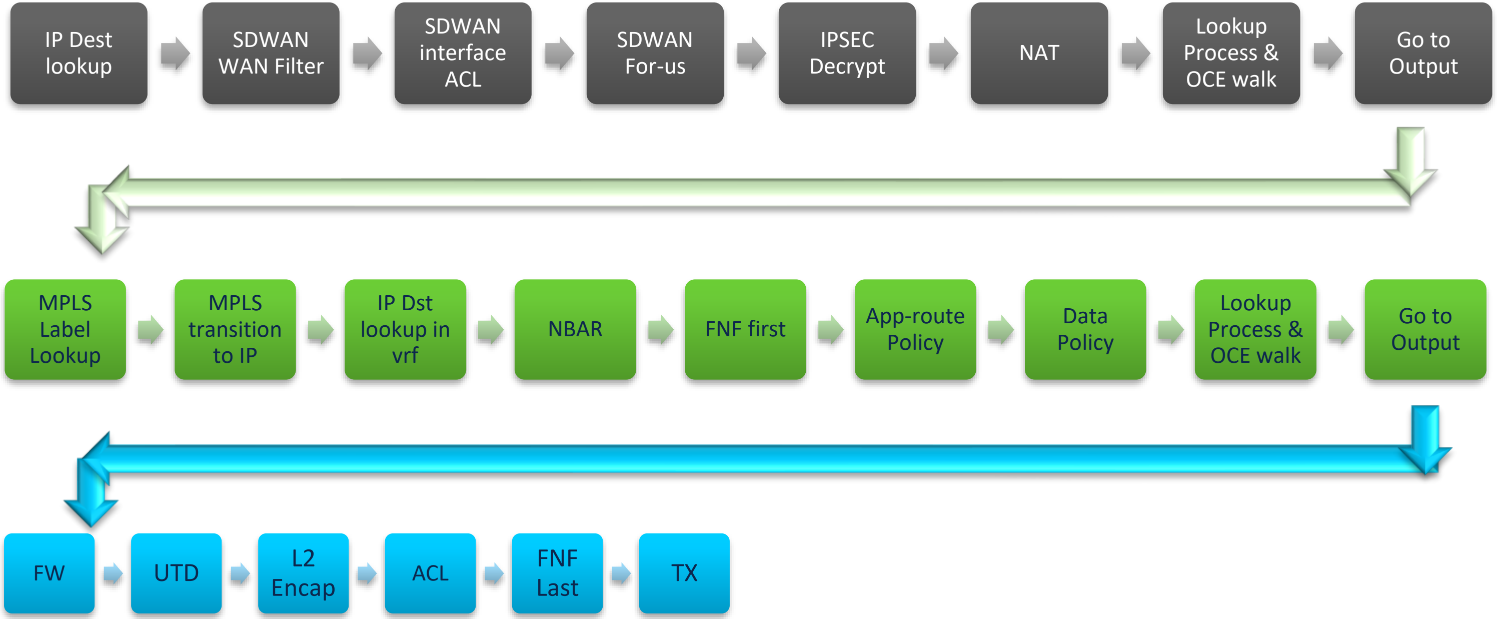
FW → UTD → MPLS Label Add → Tunnel Encap → Pre-Route → FW → UTD → NAT → IPSEC Encrypt (Transport mode) → Layer 2 Encap → DNS Crypt → ACL → FNF LAST → TX

UTD: IPS->URL-F->AMP/TG

Color Coding: LAN Interface | Tunnel Interface | WAN Interface

OCE – Output Chain Element

XE SD-WAN: From WAN to LAN



IP Dest lookup → SDWAN WAN Filter → SDWAN interface ACL → SDWAN For-us → IPSEC Decrypt → NAT → Lookup Process & OCE walk → Go to Output

MPLS Label Lookup → MPLS transition to IP → IP Dst lookup in vrf → NBAR → FNF first → App-route Policy → Data Policy → Lookup Process & OCE walk → Go to Output

FW → UTD → L2 Encap → ACL → FNF Last → TX

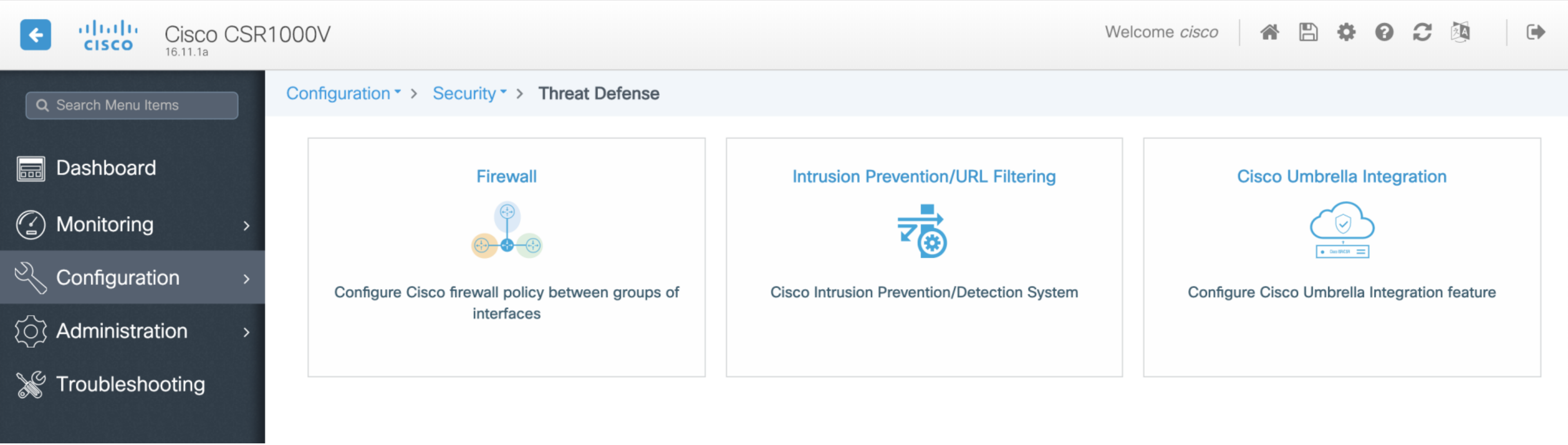
UTD: IPS->URL-F->AMP/TG

Color Coding: LAN Interface | Tunnel Interface | WAN Interface

OCE – Output Chain Element

Management

IOS-XE Routers using WebUI



Cisco CSR1000V
16.11.1a

Welcome *cisco*

Search Menu Items

- Dashboard
- Monitoring
- Configuration
- Administration
- Troubleshooting

Configuration > Security > Threat Defense

Firewall

Configure Cisco firewall policy between groups of interfaces

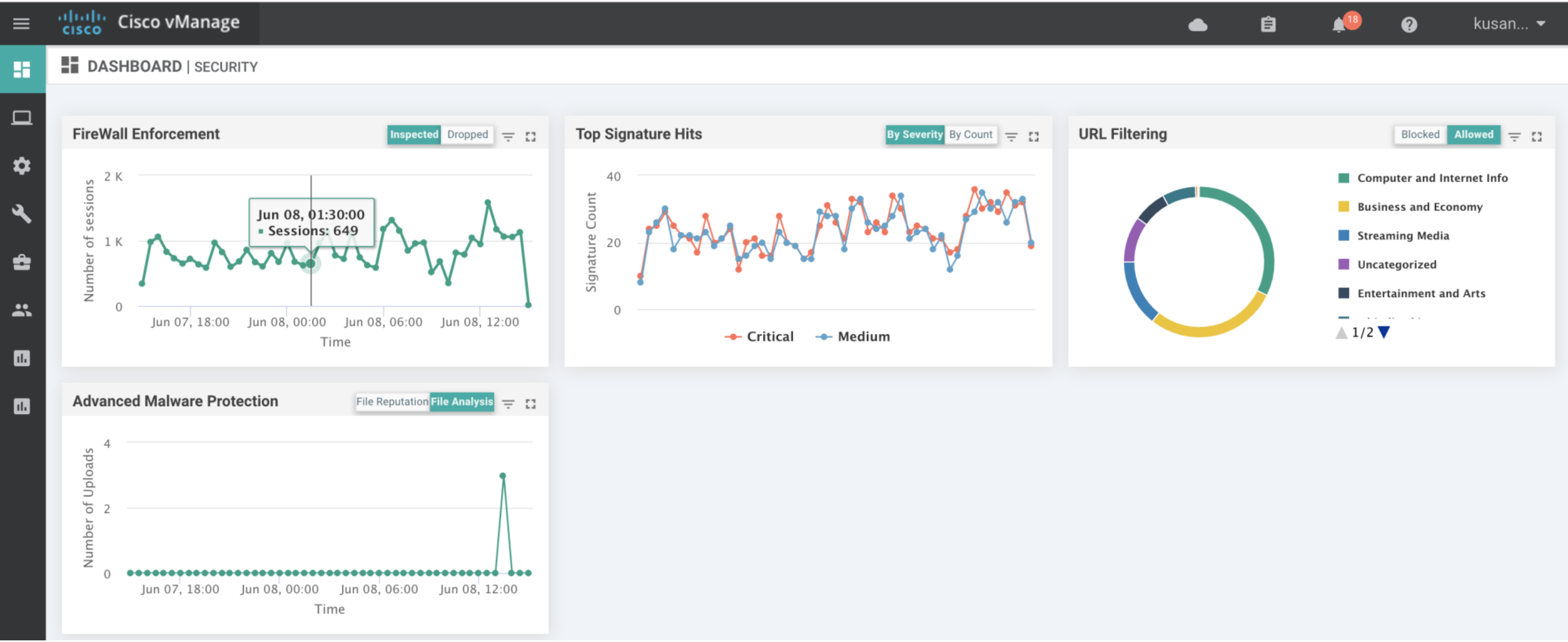
Intrusion Prevention/URL Filtering

Cisco Intrusion Prevention/Detection System

Cisco Umbrella Integration

Configure Cisco Umbrella Integration feature

XE SD-WAN Routers using vManage



WebUI VS vManage – Security Configuration

	Ent. FW App Aware	IPS	URL-F	DNS Layer Security	AMP & Threat Grid	ETA
WebUI - onbox	Y (FW only)	Y	Y	Y	N	Y
vManage - offbox	Y	Y	Y	Y	Y	N

WebUI VS vManage – Manage, Monitoring, Reporting, Troubleshoot

	Events	Alerts	Logs	Packet Captures	Network wide view	Device specific view	Real Time
WebUI - onbox	N	N	N	Y	N	N	N
vManage – offbox	Y	Y	Y	N	Y	Y	Y

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, ISRv and CSR routers. Snort monitors network traffic and analyzes against a defined rule set. Supports VRF.
URL Filtering	This on-box feature enables content filtering based on 82 different categories as well as web reputation score using Brightcloud database.
Cisco Umbrella	Cisco Umbrella Integration offers easy-to-manage DNS-layer content filtering based on categories as well as reputation. It prevents branch users and guests from accessing inappropriate content and known malicious sites that might contain malware and other security risks. Supports VRF.
AMP & TG	File Reputation – Once enabled, router computes SHA 256 for files uploaded to the internet or downloaded from the internet and reaches out to AMP cloud for file reputation. If AMP cloud has no knowledge of the computed SHA, then if ThreatGrid is enabled the entire file is sent for sandboxing. Upon using AI and machine learning algorithms TG determines if the file is malicious or not and the verdict is sent to AMP cloud for future reference. 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 and well as Crypto Audit for enterprises.

Appendix: NAT

Types of Address Translation

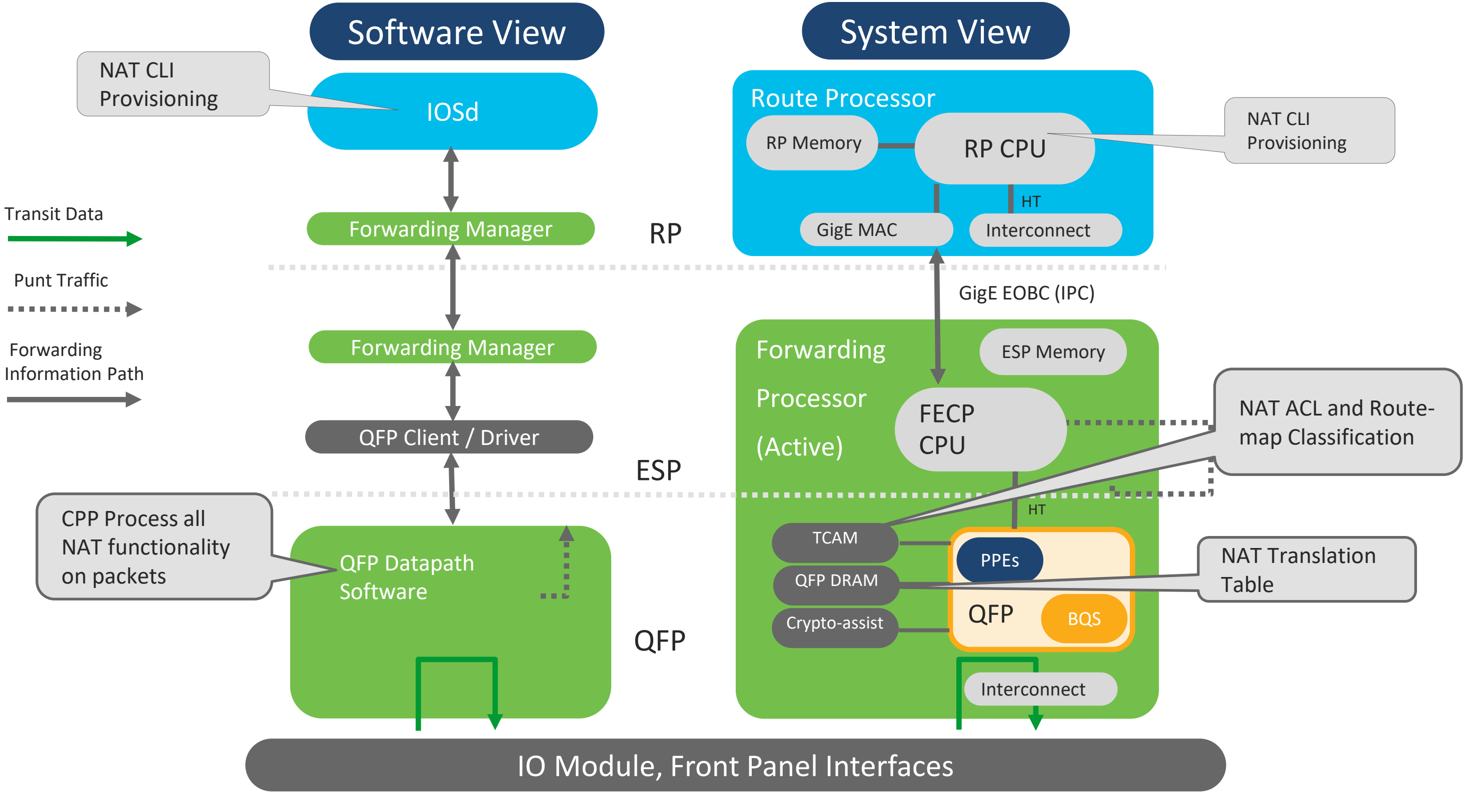
Static Translation

- Establishes a one-to-one mapping between the inside local address and an inside global address. Static translation is useful when a host on the inside must be accessible by a fixed address from the outside.

Dynamic Translation

- Establishes a mapping between an inside local address and a pool of global addresses.
- Interface overload
- Pool overload

IOS XE Network Address Translation



Traditional NAT vs Carrier Grade NAT

IOS XE NAT is implemented in Data Plane, Highly Scalable and inline to forwarding.

System default → Traditional NAT

- Full 5 tuple translation information
- Inside and outside mapping rules supported

CGN mode using "ip nat settings mode cgn" CLI

- Only source side tuple translation information
- Only inside mapping rules are supported

NAT vs CGN – Session Entry

NAT/PAT

```
 Pro. Inside global      Inside local       Outside local      Outside global
tcp  26.1.1.6:1024    27.1.1.10:29439     26.1.1.2:23            26.1.1.2:23
```

CGN

```
Pro. Inside global      Inside local       Outside local      Outside global
 tcp  26.1.1.6:1024    27.1.1.10:29439              ---                  ---
```

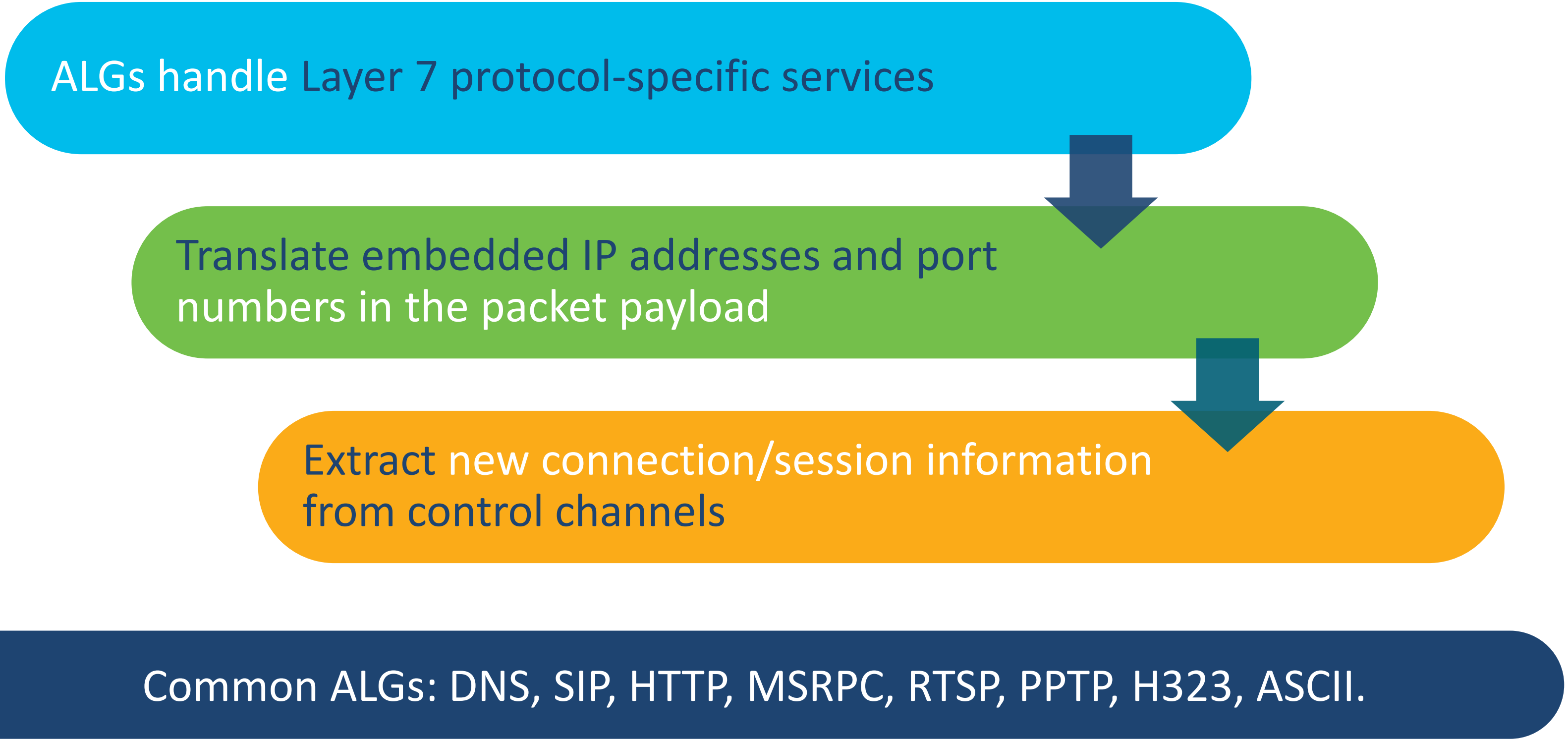
NAT vs CGN Overview

Feature	Traditional NAT	Carrier Grade NAT (CGN)
Session Entry	full 5 tuples – {protocol, source address, source port, destination address, destination port}	3 tuples - {protocol, source address, source port}
Default timeout	24 hrs for TCP	15 mins for TCP
Outside mapping rule (ip nat outside source)	Supported	Not supported
EIM/EIF	Not Supported	Supported
High Speed Logging (HSL)	Log full tuples	No destination info in the logging record
Bulk logging and Port Block Allocation	Not Supported	Supported
Scalability	-	More than double of traditional NAT

VRF NAT Support

NAT Inside Interface	NAT Outside Interface	Condition
Global VRF (also referred to as a non-VRF interface)	Global VRF (also referred to as a non-VRF interface)	Normal
VRF X	Global VRF (also referred to as a non-VRF interface)	When NAT is not configured for Match-in-VRF support. For more details, see the Match-in-VRF Support for NAT chapter.
VRF X	VRF X	When both inside and outside interfaces are in the same VRF, and NAT is configured with Match-in-VRF support.

Application-Level Gateways



ALGs handle Layer 7 protocol-specific services

Translate embedded IP addresses and port numbers in the packet payload

Extract new connection/session information from control channels

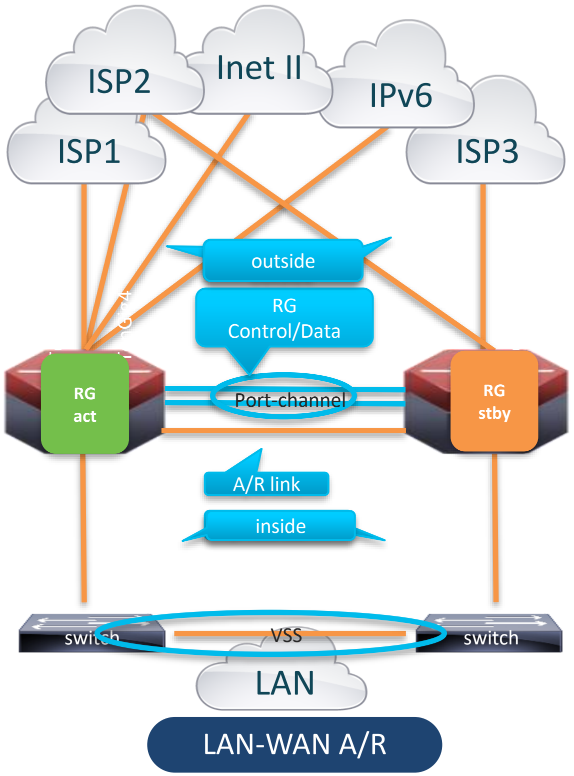
Common ALGs: DNS, SIP, HTTP, MSRPC, RTSP, PPTP, H323, ASCII.

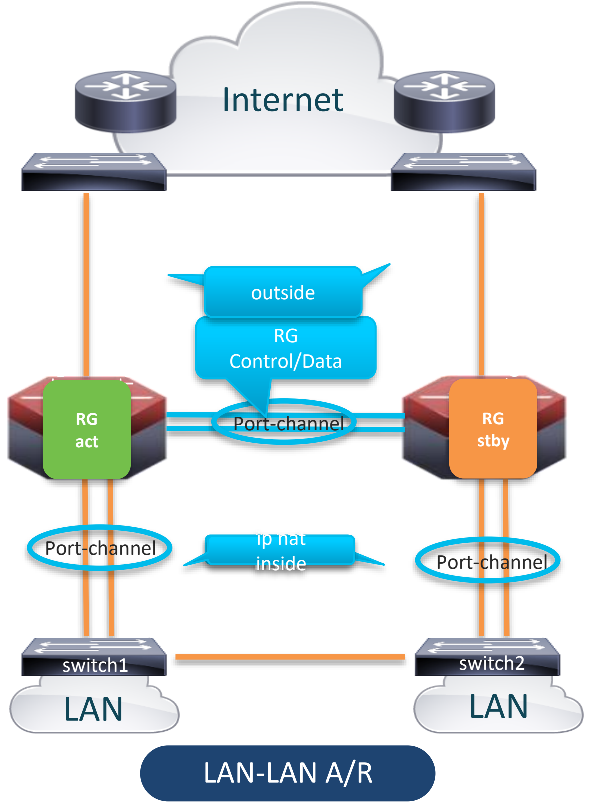
List of Supported ALGs

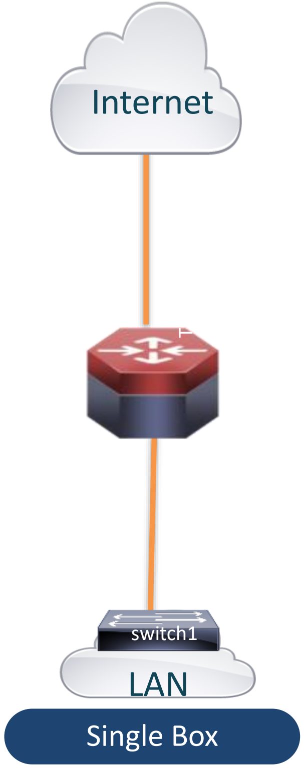
ALG	VFR	vTCP	L4	VRF	HA
FTP	Yes	No	tcp	Yes	Yes
H323	No	Yes	tcp, udp	Yes	Yes
RTSP	Yes	Yes	tcp	Yes	Yes
SCCP	No	No	tcp	Yes	Yes
SIP	Yes	Yes	tcp, udp	Yes	Yes
TFTP	No	N/A	udp	Yes	Yes
NETBIOS	No	No	tcp, udp	Yes	Yes
RCMD	No	No	tcp	Yes	Yes
LDAP	No	No	tcp	Yes	Yes
DNS	Yes	Yes	tcp, udp	Yes	Yes
SUNPRC	Yes	No	tcp	Yes	Yes
MSRPC	Yes	No	tcp	Yes	Yes
PPTP	No	No	tcp	Yes	Yes

Traditional NAT/PAT

Enterprise Internet Edge: Supported Topology





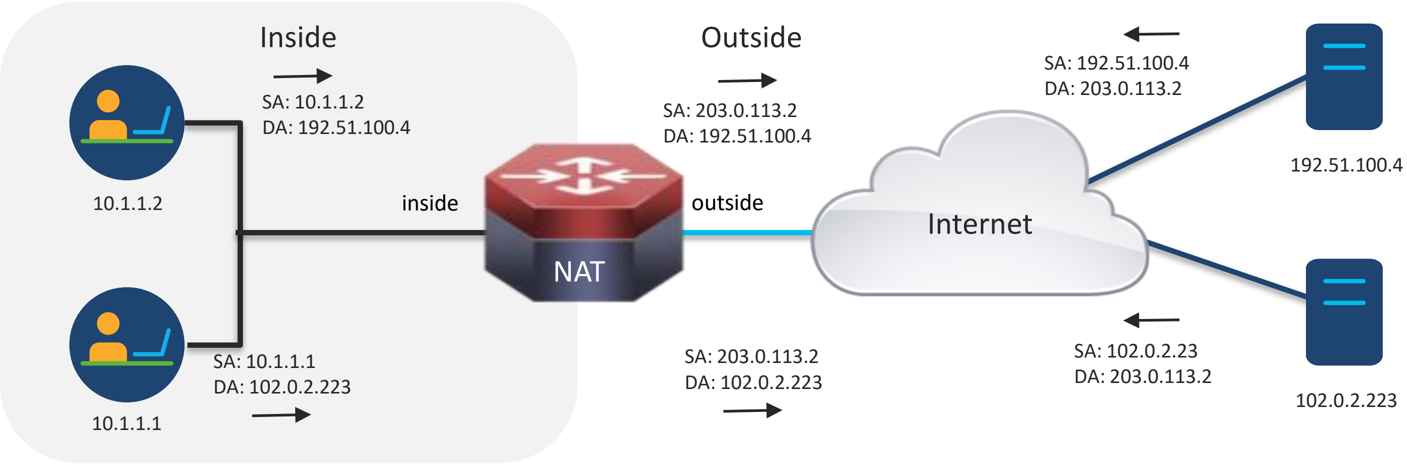


NAT Features, ALGs, Feature Combination

- Typical NAT features: Static NAT, interface overload, pool overload, VRF Aware NAT, HSL, NAT64
- There is a current restriction of NAT44 and NAT64 cannot be on the same physical interface (test gap, not code gap)
- Common ALGs: DNS, SIP, HTTP, MSRPC, RTSP, PPTP, H323, ASCII.

- NBAR2, FNF, QoS, uRPF, PBR, Port-Channel, IPv6 Co-exist, Mcast co-exist, Object Group ACL, ZBFW

Dynamic PAT pool overload

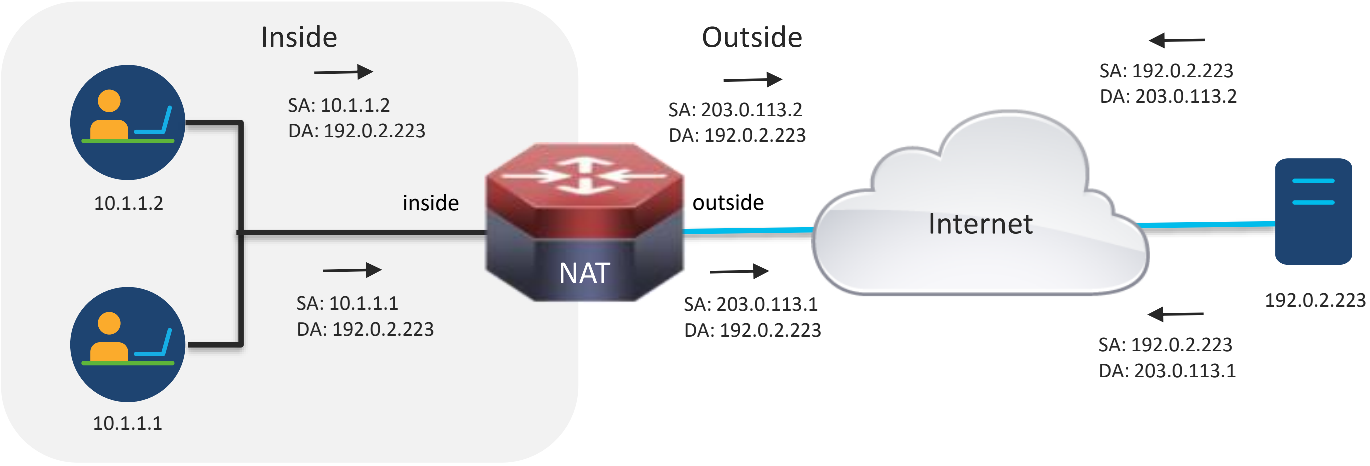


```
access-list 10 permit 10.1.1.0 0.0.0.255
ip nat pool net-inside 203.0.113.2 203.0.113.2

ip nat inside source list 10 pool net-inside overload
```

Protocol	Inside Local	Inside Global	Outside Global	Outside Local
tcp	10.1.1.2:1723	203.0.113.2:1723	192.51.100.4:23	192.51.100.4:23
tcp	10.1.1.1:10025	203.0.113.2:10025	102.0.2.223:23	102.0.2.223:23

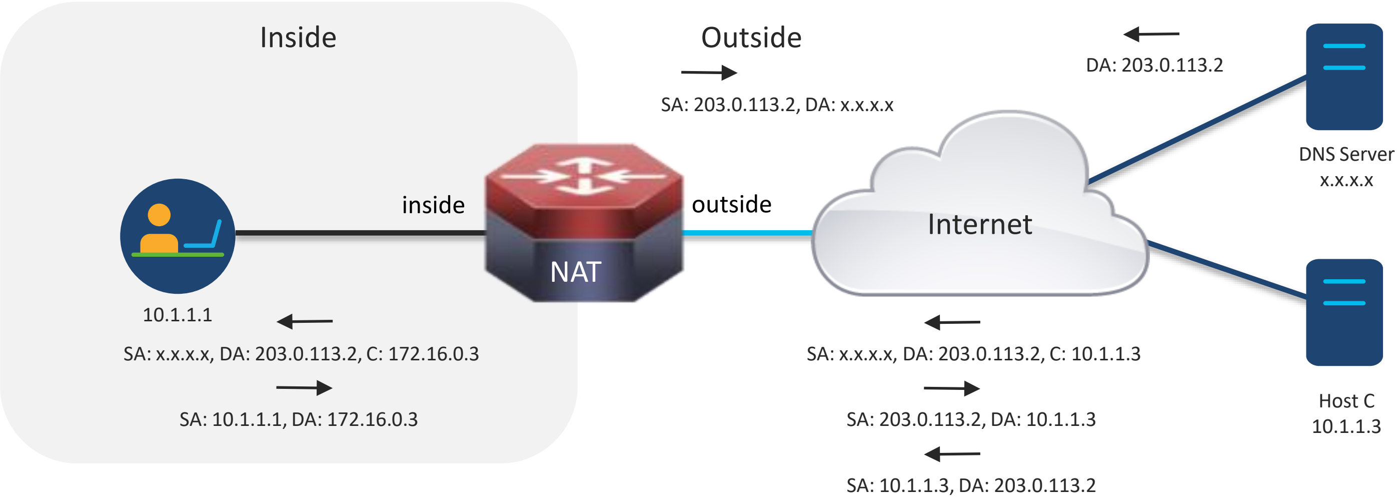
Static 1:1 NAT



```
ip nat inside source static 10.1.1.1 203.0.113.1
ip nat inside source static 10.1.1.2 203.0.113.2
```

Protocol	Inside Local	Inside Global	Outside Global	Outside Local
--	10.1.1.1	203.0.113.1	--	--
--	10.1.1.2	203.0.113.2	--	--

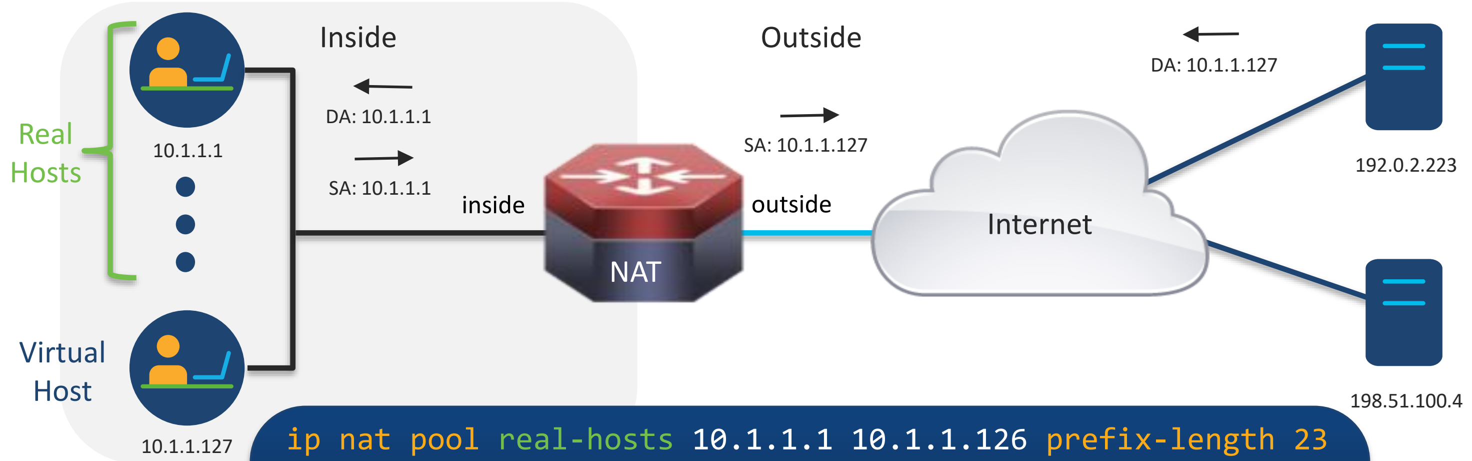
Overlapping Networks


Inside
Outside
SA: 203.0.113.2, DA: x.x.x.x
DA: 203.0.113.2
DNS Server
x.x.x.x
inside
outside
Internet
NAT
10.1.1.1
SA: x.x.x.x, DA: 203.0.113.2, C: 172.16.0.3
SA: 10.1.1.1, DA: 172.16.0.3
SA: x.x.x.x, DA: 203.0.113.2, C: 10.1.1.3
SA: 203.0.113.2, DA: 10.1.1.3
SA: 10.1.1.3, DA: 203.0.113.2
Host C
10.1.1.3

```
ip nat inside source static 10.1.1.1 203.0.113.2
ip nat outside source static 10.1.1.3 172.16.0.3
```

Protocol	Inside Local	Inside Global	Outside Global	Outside Local
--	10.1.1.1	203.0.113.2	10.1.1.3	172.16.0.3

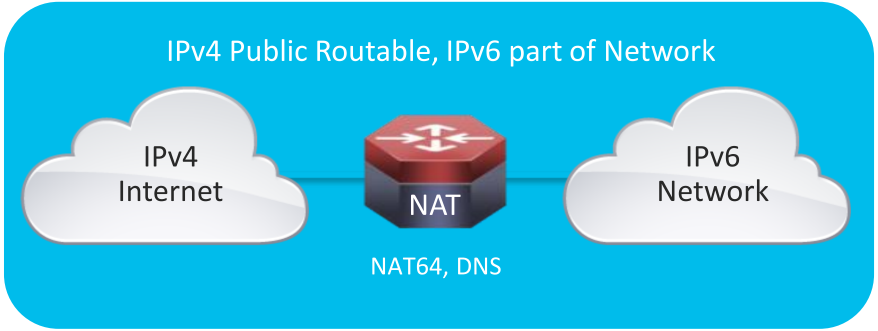
TCP Load Distribution

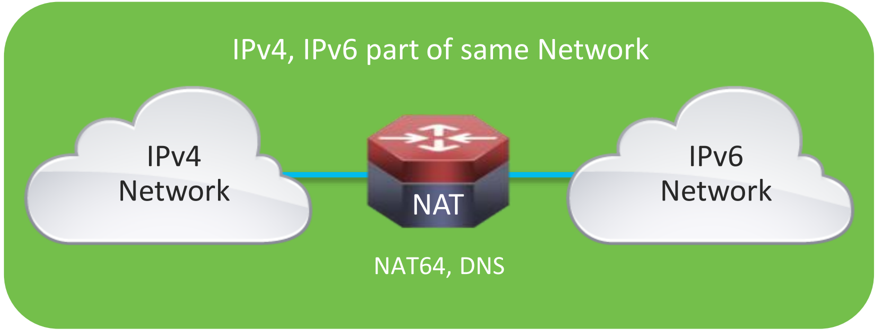


```
ip nat pool real-hosts 10.1.1.1 10.1.1.126 prefix-length 23
access-list 2 permit 10.1.1.127
ip nat inside destination list 2 pool real-hosts
```

Protocol	Inside Local	Inside Global	Outside Global	Outside Local
tcp	10.1.1.1:23	10.1.1.127:23	192.0.2.225:3058	192.0.2.225:3058
tcp	10.1.1.2:23	10.1.1.127:23	198.51.100.4	198.51.100.4:4371
tcp	10.1.1.3:23	10.1.1.127:23	192.0.2.223:3062	192.0.2.223:3062

Stateless NAT64





Scenario 1: an IPv6 network to the IPv4 Internet
Scenario 2: the IPv4 Internet to an IPv6 network

Scenario 5: an IPv6 network to an IPv4 network
Scenario 6: an IPv4 network to an IPv6 network

Standard/RFC	Document Title
RFC 6052	IPv6 Addressing of IPv4/IPv6 Translators
RFC 6144	Framework for IPv4/IPv6 Translation
RFC 6145	IP/ICMP Translation Algorithm

Parse entire IPv6 header → Extract relevant information → Translate it into an IPv4 header

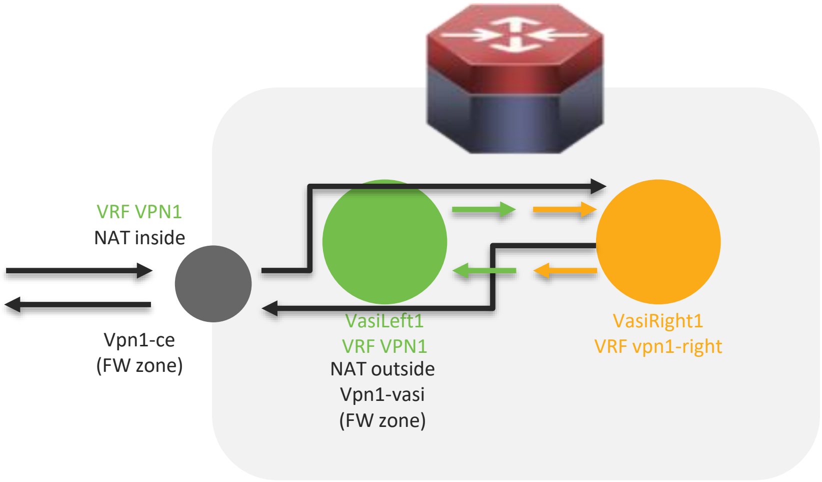
Stateful NAT64

- When an IPv6 node initiates traffic through Stateful NAT64, and the incoming packet does not have an existing state and the following events happen:
- The source IPv6 address (and the source port) is associated with an IPv4 configured pool address (and port, based on the configuration).
- The destination IPv6 address is translated mechanically based on the BEHAVE translation draft using either the configured NAT64 stateful prefix or the Well Known Prefix (WKP).
- The packet is translated from IPv6 to IPv4 and forwarded to the IPv4 network.
- The Well Known Prefix 64:FF9B::/96 is supported for Stateful NAT64.

Stateful NAT64 vs Stateless NAT64

Supported Features	Stateful NAT64	Stateless NAT64
Address savings	N:1 mapping for PAT or overload configuration that saves IPv4 addresses.	One-to-one mapping—one IPv4 address is used for each IPv6 host).
Address space	IPv6 systems may use any type of IPv6 addresses.	IPv6 systems must have IPv4-translatable addresses (based on RFC 6052).
ALGs supported	FTP64	None
Protocols supported	ICMP, TCP, UDP	All
Standards	Draft-ieft-behave-v6v4-xlate-stateful-12	Draft-ietf-behave-v6v4-xlate-05
State creation	Each traffic flow creates a state in the NAT64 translator. The maximum number of states depends on the number of supported translations.	Traffic flow does not create any state in the NAT64 translator. Algorithmic operation is performed on the packet headers.

NAT on a Stick Using VASI



- IOS XE do not support classical inter-vrf NAT configurations as those found on IOS devices
- Support for Inter-vrf NAT on IOS-XE is achieved via VASI implementation

Other Important NAT Features

- NAT default Inside Server: Out-to-In traffic for specified inside local address

```
ip nat inside source static 10.1.1.1 interface Gig0/0/0
ip nat inside source static tcp  10.1.1.1 23 interface 23
```

- NAT of External IP Address only

```
ip nat inside source static tcp 10.1.1.1 2000 192.168.1.1 2000 no-payload
ip nat outside source static tcp 10.1.1.1 20000 192.168.1.1 20000 no-payload
```

- Rate Limiting NAT Translation

```
ip nat translation max-entries <xxxx>
```

- NAT Route Maps Outside-to-Inside

```
ip nat inside source route-map MAP-A pool POOL-A reversible
ip nat inside source route-map MAP-B pool POOL-B reversible
```

Carrier Grade NAT (CGN)

CGN Supported Features

- All traditional NAT ALGs supported with CGN
- Endpoint-Independent Mapping/Filtering (EIM/EIF)
- Hairpinning using VASI and PBR
- Lawful Intercept
- High Speed Logging
- Multihoming- multiple outside interfaces
- VRF aware NAT
- Higher CGN scale using ‘ip nat settings scale bind’ CLI

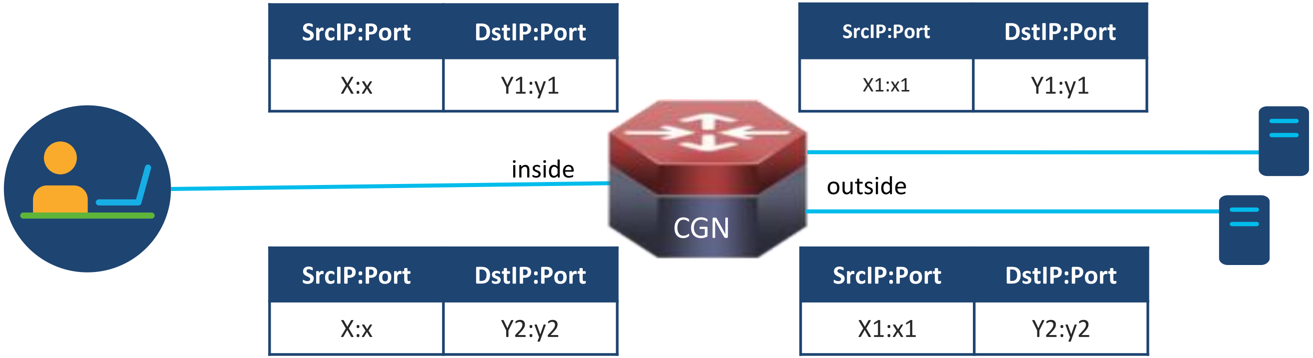
Supported RFCs:

- RFC4787
- RFC5382
- RFC5508

NAT64 CGN is not supported

Endpoint-Independent Mapping/Filtering (EIM/EIF)

```
Pro. Inside global         Inside local         Outside local        Outside global
 tcp  26.1.1.6:1024      27.1.1.10:11806             ---                  ---
```



SrcIP:Port	DstIP:Port
X:x	Y1:y1

SrcIP:Port	DstIP:Port
X1:x1	Y1:y1

SrcIP:Port	DstIP:Port
X:x	Y2:y2

SrcIP:Port	DstIP:Port
X1:x1	Y2:y2

EIM implies X1:x1 = X2:x2 for all Y:y (Y1:y1 and Y2:y2)

CGN Config Variations

Static Carrier Grade NAT

```
ip nat inside source static 192.168.2.1 192.168.34.2
```

Dynamic Carrier Grade NAT

```
ip nat pool nat-pool 10.1.1.1 10.1.254.254 prefix-length 16
ip nat inside source route-map nat-route-map pool nat-pool
```

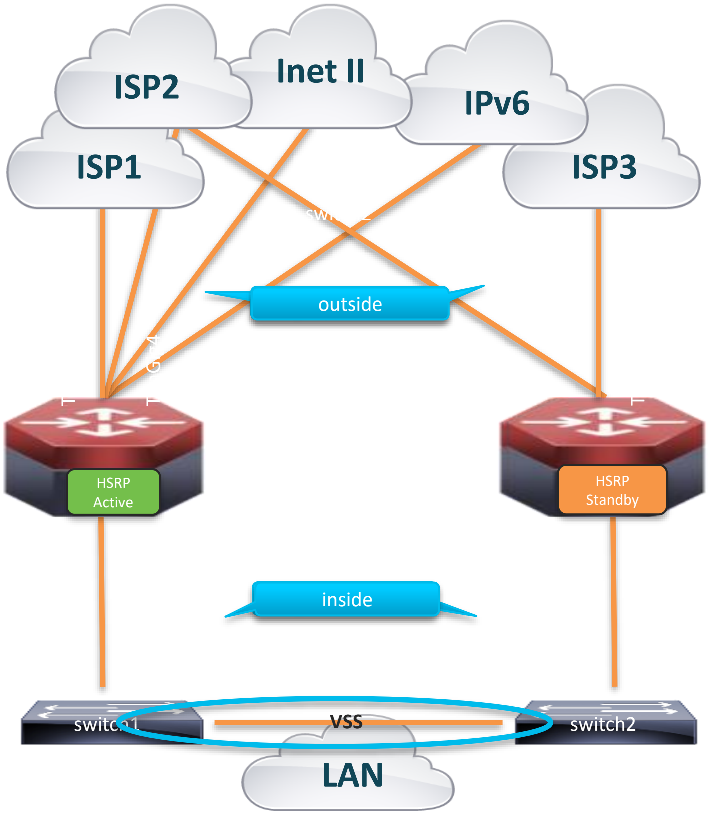
Dynamic Port Address Carrier Grade NAT

```
ip nat pool nat-pool 10.1.1.1 10.1.254.254 netmask 255.255.0.0
access-list 1 permit 172.16.0.0 255.255.0.0
ip nat inside source list 1 pool nat-pool overload
```

NAT High Availability

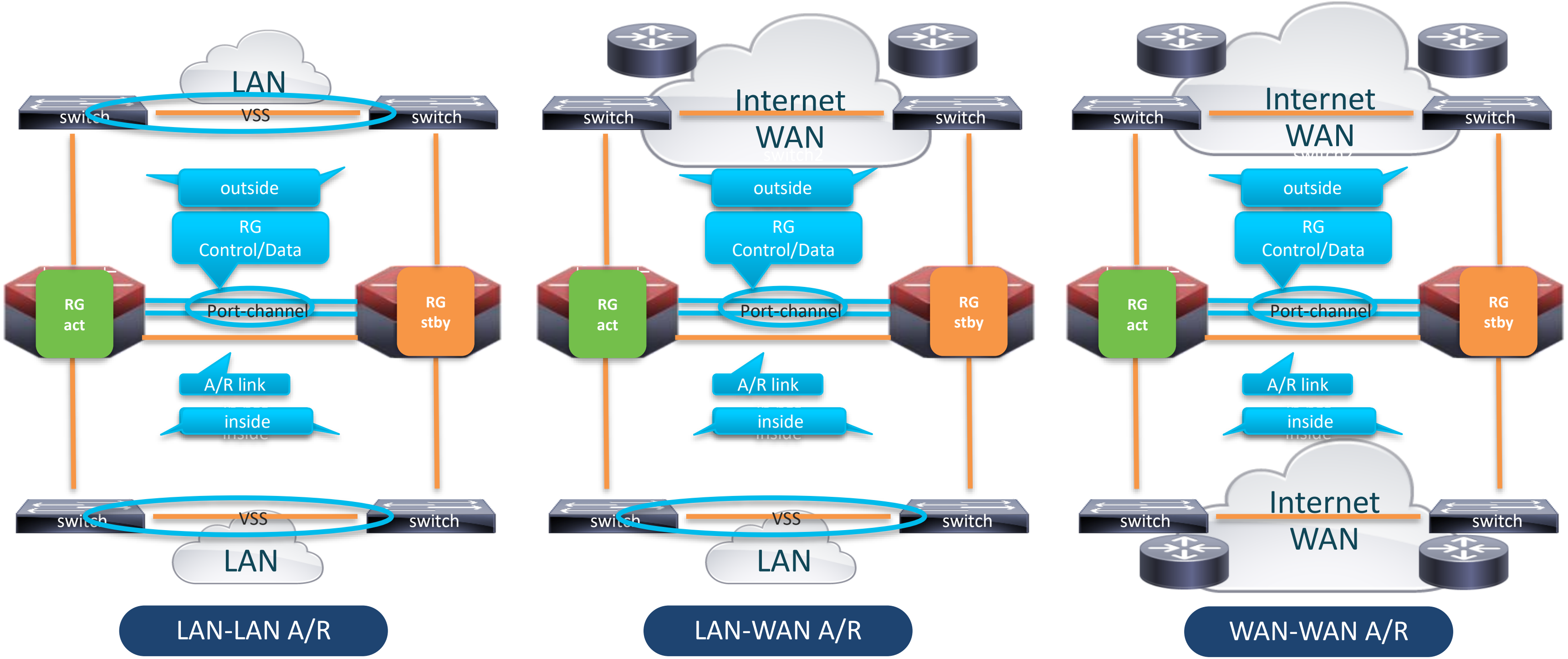
NAT with HSRP – Stateless Redundancy

- Dynamic NAT, PAT, Interface Overload config supported with and without VRF instances
- NAT Static Mapping with HSRP supported
- Dynamic NAT and PAT are stateless – session states are NOT synced, after switchover all NAT sessions will be recreated on the newly active HSRP router
- HSRP VIP can not be used by NAT pools
- Only Active/Standby configuration supported
- HSRP and B2B HA can not co-exist



Box-to-box NAT Stateful Redundancy

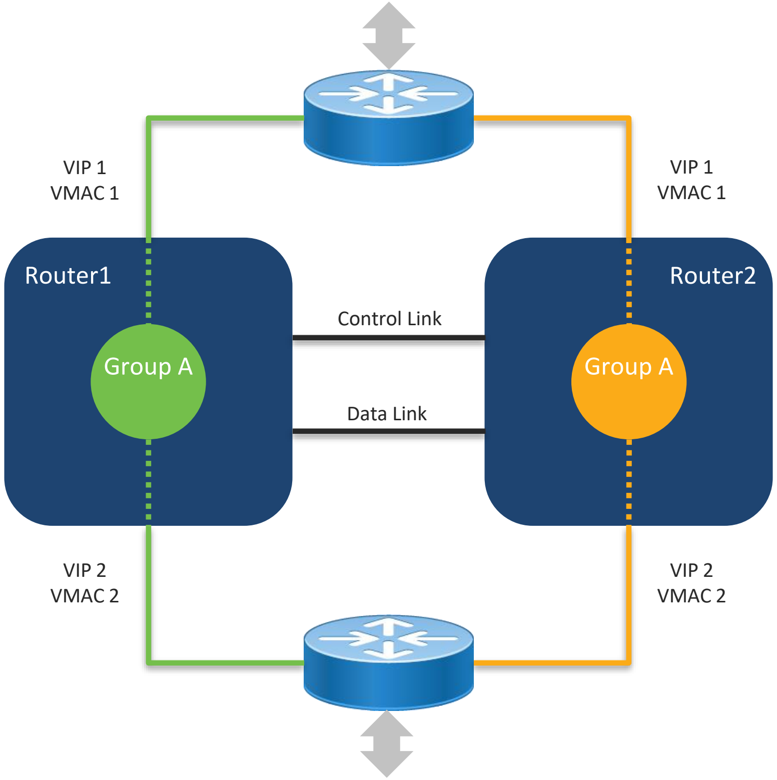
B2BHA – Application-Level Redundancy



Box-to-box Redundancy

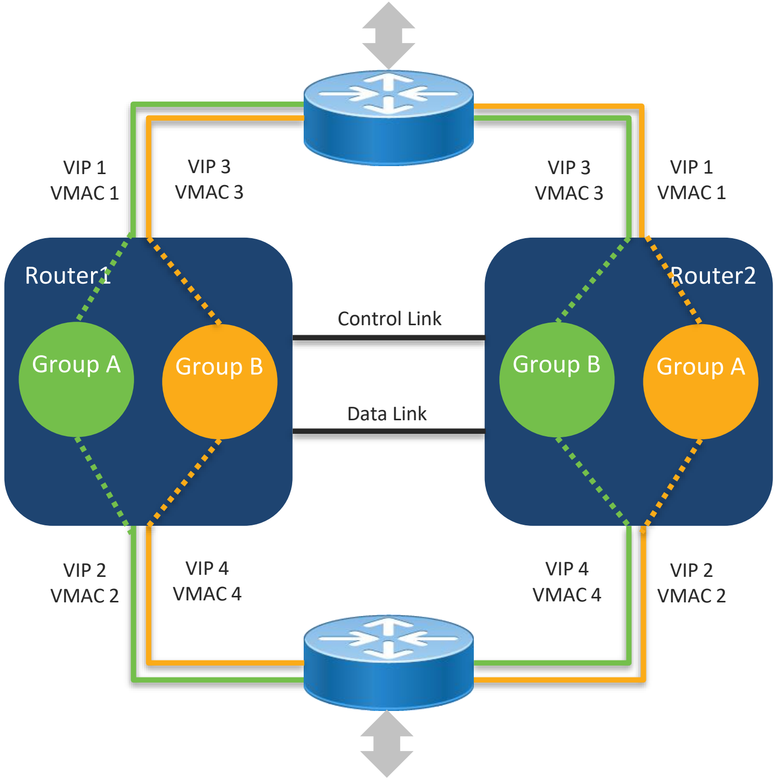
- Can not co-exists with Intra-chassis (HW/SW) redundancy
- What’s Synced v/s not Synced?
  - HTTP NAT Sessions are not synced be default
  - Configure ‘ip nat switchover replication http’ if sync is required o Half- Open FW sessions are not synced
  - For TCP based sessions, state is synced as soon as 3-way handshake is complete
  - For UDP based sessions, state is synced when the router receive 2nd packet for the same UDP flow
  - Configuration is not synced across boxes

Box-to-box Redundancy: Active/Standby



- Active and Standby behavior from the perspective of NAT Application
- Active router would have active translations and Sessions and standby would only maintain the sessions synced information for these sessions from Active.

Box-to-box Redundancy: Active/Standby



- Active and Active behavior from the perspective of NAT Application
- Two RG Groups, one active on each of routers
- Both would have active sessions/translations and peer would be in standby mode for those set of sessions. .

HSL and NAT Features

High Speed Logging (HSL)

- Logging can be export to external device in Netflow v9 format
- Syslog is NOT supported for NAT or CGN
- HSL is implemented in NAT data path directly export the transaction records (NetFlow v9-like) to an external collector
- Destination Info not available in CGN Mode

Field	Format
Source IP address	IPv4 address
Translated source IP address	IPv4 address
Destination IP address	IPv4 address
Translated destination IP address	IPv4 address
Original source port	16-bit port
Translated source port	16-bit port
Original destination port	16-bit port
Translated destination port	16-bit port
VRF ID	32-bit ID
Protocol	8-bit value
Event	0-Invalid 1-Adds event 2-Deletes event 3-Pool exh.
Unix timestamp in milliseconds	64-bit value

High Speed Logging

- Per VRF NAT HSL is supported, Udp flow export supported
- Bind-only logging option logs ip to ip translations, does not send ip + port translations logs
- Configuration of HSL differs for NAT44 vs NAT64:

```
ip nat log translations flow-export v9 udp destination <ip> <port> source interface
type <interface>
ip nat log translations flow-export v9 {vrf-name | global-on }

nat64 logging translations flow-export v9 udp destination addr|ipv6-destination IPv6
address vrf vrf name source interface type interface-number
nat64 logging translations flow-export v9 {vrf-name | global-on }
```

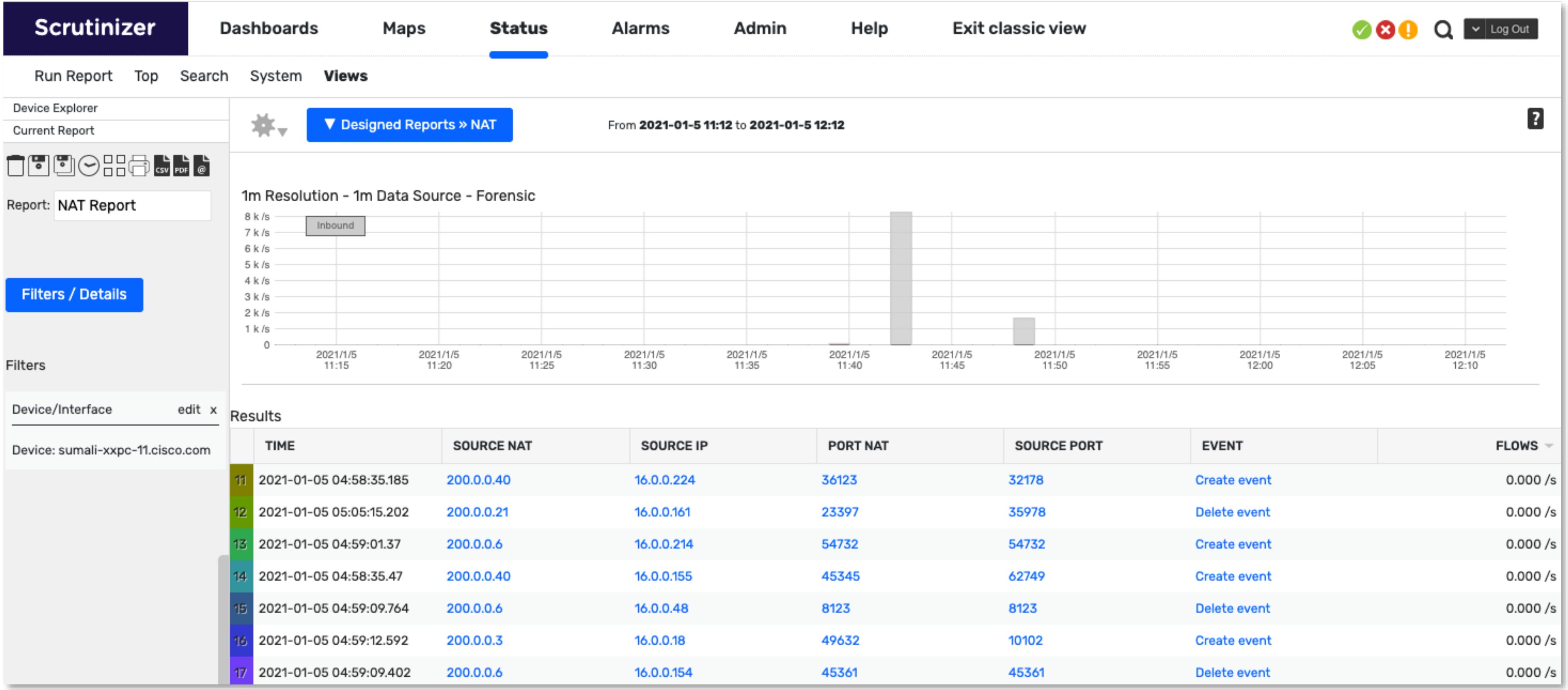
CGN – Bulk Logging and Port Block Allocation (BPA)

- The Bulk Logging and Port Block Allocation feature allocates a block of ports for translation instead of allocating individual ports.
- Supported only in (CGN) mode.

For example: a BPA configuration with set size 8 and step size of 4.
Set 0 = {1024, 1028, 1032, 1036, 1040, 1044, 1048, 1052}
Set 1 = {1025, 1029, 1033, 1037, 1041, 1045, 1049, 1053}
Set 2 = {1026, 1030, 1034, 1038, 1042, 1046, 1050, 1054}
Set 3 = {1027, 1031, 1035, 1039, 1043, 1045, 1051, 1055}
…

Field	Format
Source IP address	IPv4 address
Translated source IP address	IPv4 address
VRF ID	32-bit ID
Protocol	8-bit value
Event	0-Invalid 1-Adds event 2-Deletes event 3-Pool exh.
Unix timestamp in milliseconds	64-bit value
Port block start	16-bit port
Port block step size	16-bit step size
Number of ports in the block	16-bit number

CGN HSL using Plixer Collector



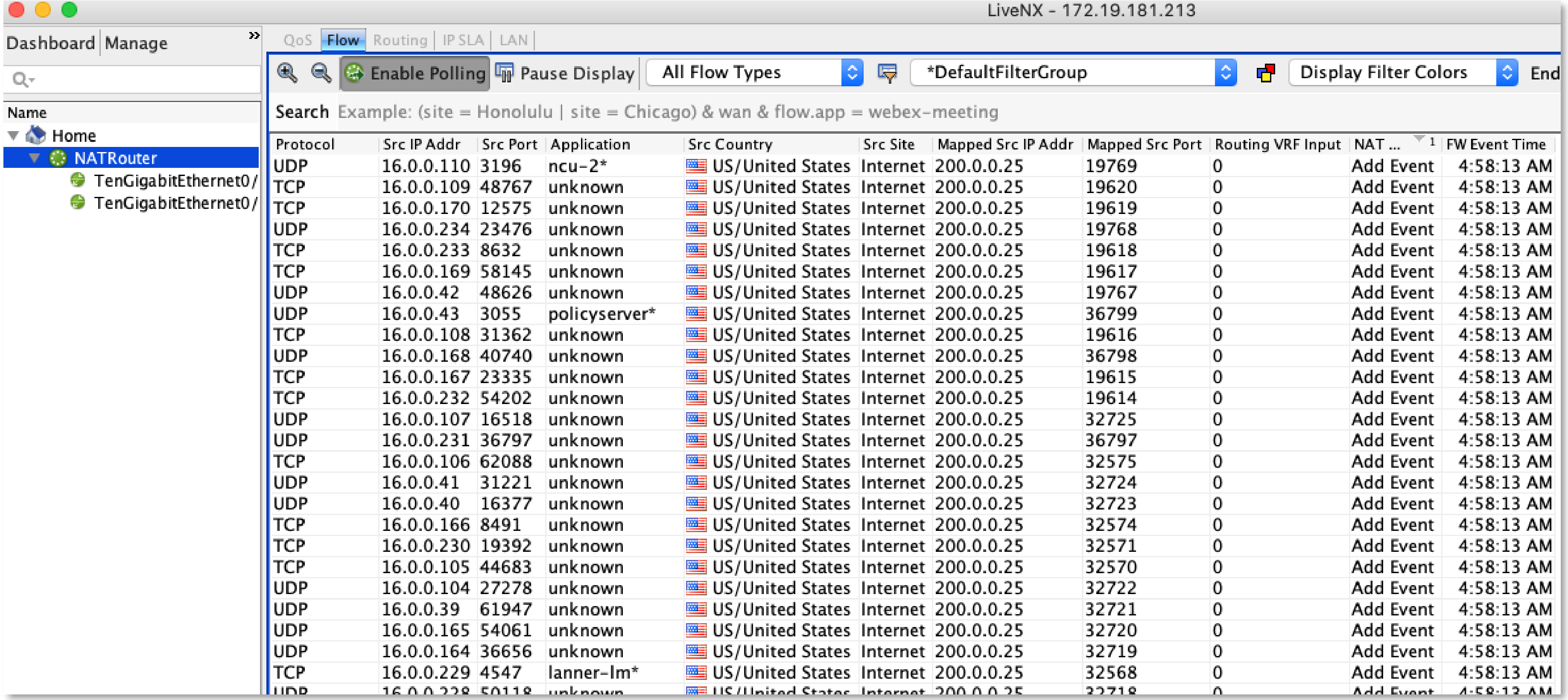
Report: NAT Report

Device: sumali-xxpc-11.cisco.com

From **2021-01-5 11:12** to **2021-01-5 12:12**

	TIME	SOURCE NAT	SOURCE IP	PORT NAT	SOURCE PORT	EVENT	FLOWS
11	2021-01-05 04:58:35.185	200.0.0.40	16.0.0.224	36123	32178	Create event	0.000 /s
12	2021-01-05 05:05:15.202	200.0.0.21	16.0.0.161	23397	35978	Delete event	0.000 /s
13	2021-01-05 04:59:01.37	200.0.0.6	16.0.0.214	54732	54732	Create event	0.000 /s
14	2021-01-05 04:58:35.47	200.0.0.40	16.0.0.155	45345	62749	Create event	0.000 /s
15	2021-01-05 04:59:09.764	200.0.0.6	16.0.0.48	8123	8123	Delete event	0.000 /s
16	2021-01-05 04:59:12.592	200.0.0.3	16.0.0.18	49632	10102	Create event	0.000 /s
17	2021-01-05 04:59:09.402	200.0.0.6	16.0.0.154	45361	45361	Delete event	0.000 /s

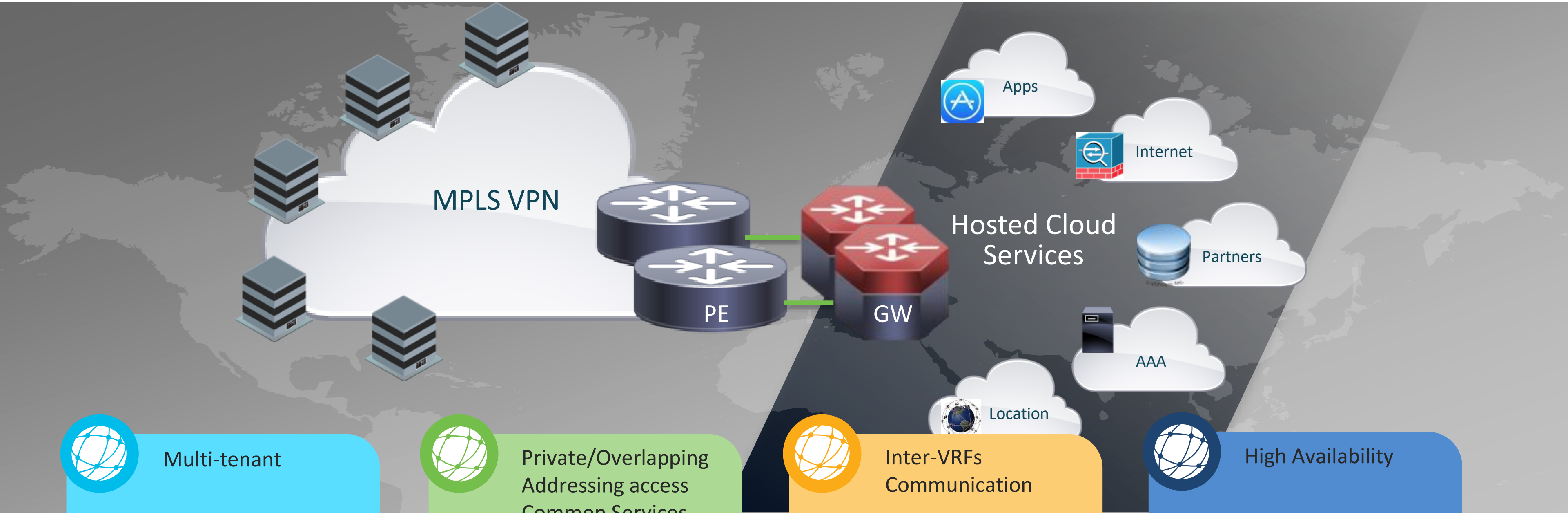
CGN HSL using LiveNX Collector



Protocol	Src IP Addr	Src Port	Application	Src Country	Src Site	Mapped Src IP Addr	Mapped Src Port	Routing VRF Input	NAT ...	FW Event Time
UDP	16.0.0.110	3196	ncu-2*	US/United States	Internet	200.0.0.25	19769	0	Add Event	4:58:13 AM
TCP	16.0.0.109	48767	unknown	US/United States	Internet	200.0.0.25	19620	0	Add Event	4:58:13 AM
TCP	16.0.0.170	12575	unknown	US/United States	Internet	200.0.0.25	19619	0	Add Event	4:58:13 AM
UDP	16.0.0.234	23476	unknown	US/United States	Internet	200.0.0.25	19768	0	Add Event	4:58:13 AM
TCP	16.0.0.233	8632	unknown	US/United States	Internet	200.0.0.25	19618	0	Add Event	4:58:13 AM
TCP	16.0.0.169	58145	unknown	US/United States	Internet	200.0.0.25	19617	0	Add Event	4:58:13 AM
UDP	16.0.0.42	48626	unknown	US/United States	Internet	200.0.0.25	19767	0	Add Event	4:58:13 AM
UDP	16.0.0.43	3055	policyserver*	US/United States	Internet	200.0.0.25	36799	0	Add Event	4:58:13 AM
TCP	16.0.0.108	31362	unknown	US/United States	Internet	200.0.0.25	19616	0	Add Event	4:58:13 AM
UDP	16.0.0.168	40740	unknown	US/United States	Internet	200.0.0.25	36798	0	Add Event	4:58:13 AM
TCP	16.0.0.167	23335	unknown	US/United States	Internet	200.0.0.25	19615	0	Add Event	4:58:13 AM
TCP	16.0.0.232	54202	unknown	US/United States	Internet	200.0.0.25	19614	0	Add Event	4:58:13 AM
UDP	16.0.0.107	16518	unknown	US/United States	Internet	200.0.0.25	32725	0	Add Event	4:58:13 AM
UDP	16.0.0.231	36797	unknown	US/United States	Internet	200.0.0.25	36797	0	Add Event	4:58:13 AM
TCP	16.0.0.106	62088	unknown	US/United States	Internet	200.0.0.25	32575	0	Add Event	4:58:13 AM
UDP	16.0.0.41	31221	unknown	US/United States	Internet	200.0.0.25	32724	0	Add Event	4:58:13 AM
UDP	16.0.0.40	16377	unknown	US/United States	Internet	200.0.0.25	32723	0	Add Event	4:58:13 AM
TCP	16.0.0.166	8491	unknown	US/United States	Internet	200.0.0.25	32574	0	Add Event	4:58:13 AM
TCP	16.0.0.230	19392	unknown	US/United States	Internet	200.0.0.25	32571	0	Add Event	4:58:13 AM
TCP	16.0.0.105	44683	unknown	US/United States	Internet	200.0.0.25	32570	0	Add Event	4:58:13 AM
UDP	16.0.0.104	27278	unknown	US/United States	Internet	200.0.0.25	32722	0	Add Event	4:58:13 AM
UDP	16.0.0.39	61947	unknown	US/United States	Internet	200.0.0.25	32721	0	Add Event	4:58:13 AM
UDP	16.0.0.165	54061	unknown	US/United States	Internet	200.0.0.25	32720	0	Add Event	4:58:13 AM
UDP	16.0.0.164	36656	unknown	US/United States	Internet	200.0.0.25	32719	0	Add Event	4:58:13 AM
TCP	16.0.0.229	4547	lanner-lm*	US/United States	Internet	200.0.0.25	32568	0	Add Event	4:58:13 AM
UDP	16.0.0.228	50118	unknown	US/United States	Internet	200.0.0.25	32718	0	Add Event	4:58:13 AM

Cloud Gateway Profile

Cloud Gateway Architecture



Multi-tenant

- VRF Aware
- VRF Scale

Private/Overlapping Addressing access Common Services

- Network Address Translation
- NAT Scale

Inter-VRFs Communication

- VRF Aware Service Infrastructure (VASI)

High Availability

- Dual Box Design
- Stateless Redundancy
- Stateful Redundancy

Cloud Gateway Requirements

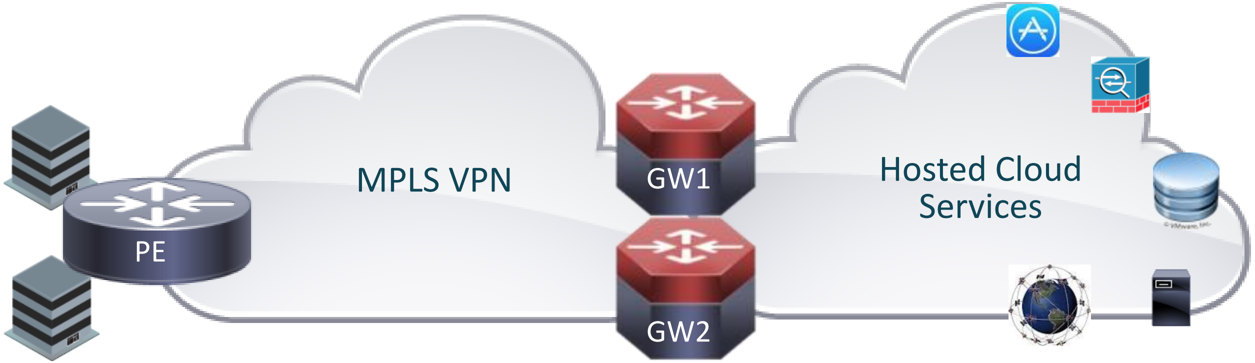
Platform delivers Cloud Services to Business Customers

Business customers would be in their respective MPLS/VPN VRFs, it is common they are in the private/overlapping IP space.

The hosted cloud provides shared services to all VPN customers, and likely in it's service VRF.

The gateway is needed to provide VRF-Aware NAT function, in addition VASI is a must requirement for Inter-VRF communication.

Cloud Gateway Profile– Supported Topology



The connectivity between PE and GW can be

- MPLS VPN (MP-iBGP)
- Inter-AS Option A (VRF back to back, eBGP in each VRF)
- Inter-AS Option B (MP-eBGP+label)
- GRE/mGRE/IPsec

Cloud Gateway Profile – High Availability

- Routing/BGP can be used to support Inter-chassis stateless redundancy:
  1) There is no connectivity between two GWs, GW1 and GW2 would be establishing their own routing connectivity with PEs and Cloud
  2) Routing is configured in a way that GW1 is the preferred path, and GW2 is the less preferred path
  3) Routing/BFD would detect the path failure and failover once routing re-convergence while NAT sessions will be built from scratch in the newly preferred gateway
- RG can be used for B2BHA in WAN-WAN symmetric routing
- HSRP can be used to failover in stateless fashion
- Support Intra-box HA (Redundant RPs/ESPs) and ISSU.

Cloud Gateway Profile – NAT Features

- Typical NAT features: VRF Aware NAT w/ VASI, match-in-vrf, pool overload, interface overload, HSL, CGN, Static NAT.
- Can run either traditional NAT44 or CGN, the choice is mostly driven by law enforcement logging requirements (i.e if need destination IP in the HSL record)

Cloud Gateway Profile – Feature Combinations

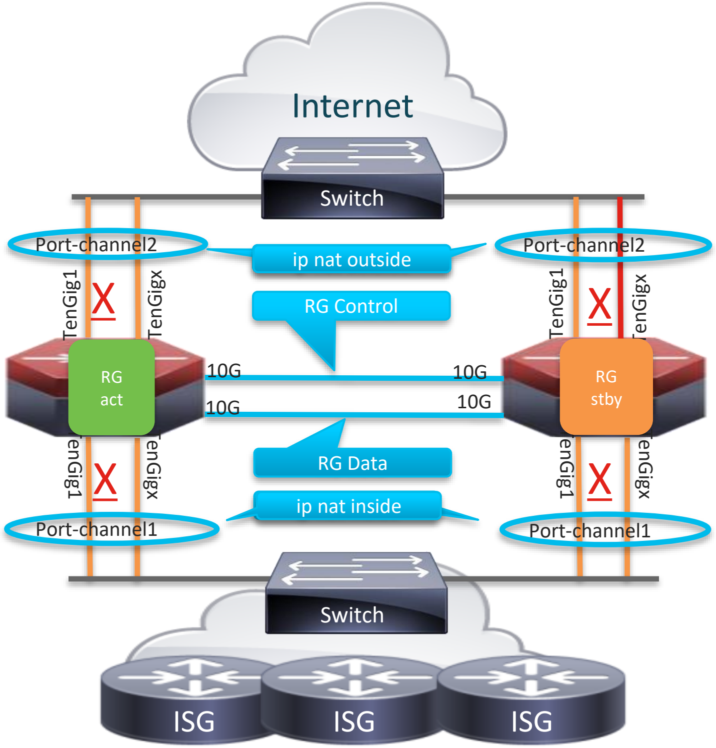
- ZBFW, FNF, QoS, PBR, BGP, BFD, Port-channel, GRE/mGRE, IPsec, WCCP
- IPsec, WCCP are risky feature combinations w/ NAT – no test coverage, recommend customer/AS/CPOC testing prior to deployment
- The super combo of NAT+WCCP+ZBFW are not supported

SP-WiFi CGN Profile

SP-WiFi CGN Profile

- NAT is an integral component of SP-WiFi architecture, after subscriber management in ISG, traffic needs to be NAT'ed while reaching out to the Internet
- Massive session count – CGN mode
- Massive short-lived session – aggressive timeout timers, higher speed session setup/tear down rate
- Limit the amount of HSL logging record and the number of ports can be used per subscriber – BPA/PAP
- Strong HA requirements: Box to box HA, link resilience (Port-Channel)
- IPv4 only

SP-WiFi Profile – Supported Topology



SP-WiFi Profile – High Availability

- B2B HA inter-chassis redundancy
- Port-Channel for throughput aggregation/load balancing & link resilience
- Stateless redundancy using HSRP

SP-WiFi Profile – NAT Features, Combination

- Typical NAT features: CGN, PAP, BPA, HSL, timeout 120, tcp-timeout 120, udp-timeout 60, VRF Aware NAT

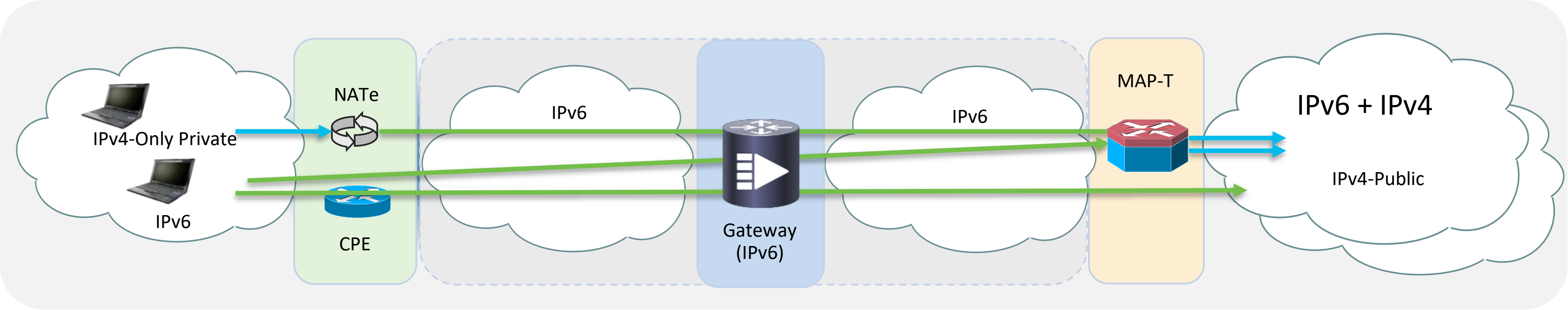
Feature Combination

- Port-channel
- RG Control & RG Data can be GE links
- FNF, BFD, HSRP
- DHCP Pool – NAT can be used as DHCP server in the SP-WiFi architecture.

MAP-T

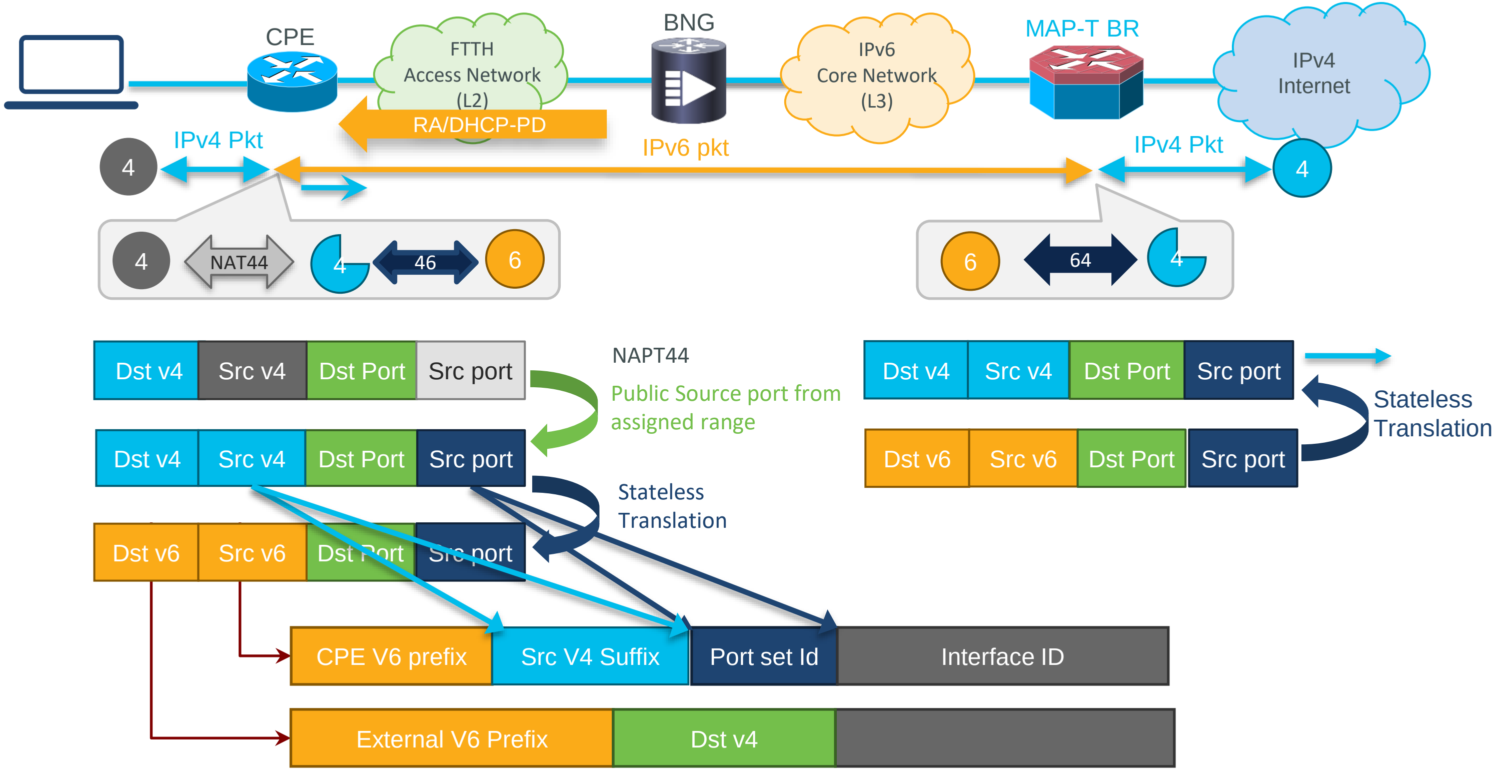
MAP-T

Truly Scalable for IPv4 over IPv6 Network



- MAP-T provides connectivity to IPv4 hosts across IPv6 domains.
- MAP-T is a mechanism that performs double translation (IPv4 to IPv6 and vice versa) on customer edge (CE) devices and border routers.
- MAP-T border router functionality is supported, customer edge (CE) functionality is not supported.

MAP-T Translation



MAP-T Advantages

- SP network can be only one domain – IPv6
- Decouples operator’s transition to IPv6 from that of the IPv4 users
- Stateless is better
    - Scales very well. reliable, robust.
    - Network architecture simplification
    - Network dimensioning
    - No new logging requirements

NAT Scale and Performance

NAT/PAT, CGN Session Scale

Feature	ASR1000 ESP200-X	ASR1000 ESP100-X	C8500-12X4QC	C8500-12X	ASR1000 ESP200	ASR1000 ESP100	ASR1002-HX	ASR1001-HX, ASR1002-X, ASR1001-X	C8500L, C8300, C8200*	CSR1K, C8000V
NAT/PAT Sessions	32M	16M	16M	12M	8M	8M	8M	2M	2M	512k
CGN/PAT Sessions	58M	32M	32M	24M	24M	12M	12M	4M	3M	512k

*C8200 scale with 16GB DRAM

High Scale NAT, CGN

- Traditional NAT and CGN both support high scale NAT with optimized data plane processing in latest code
- For 16.8.x until 16.11.x release with ASR1000-ESP200 module, following CLI needs to be configured to enable high scale processing

```
ip nat settings scale bind
```

- From 16.11.x release onward, the CLI is enabled by default for applicable platforms

NAT Scalability

- NAT translation entries are stored in QFP resource DRAM, any features also store state/session information in QFP resource DRAM will impact NAT session scalability
- The popular ones are FIB, FNF, AVC, ZBFW
- Closely monitor the utilization using:

```
show platform hardware qfp active infrastructure exmem statistics
```

- The best practice is running < 75%, otherwise should begin to plan system upgrade.

Best Practices

SET the Limit

- Set NAT max-entries per system to no more than platform scale:

  ip nat translation max-entries <number of entries>

  Be aware of that

  1. NAT sessions scaling numbers are based on a few pools
  2. PAT session scaling numbers are expected to be reduced while the number of overload pools are rising

- Set NAT max-entries per VRF to prevent single customer starving entire system translation limit:

  ip nat translation max-entries vrf <vrf_name> <number of entries>

Gatekeeper

- NAT Gatekeeper protects the NAT engine from non-NAT flows.
- Gatekeeper keeps a small cache of the non-NAT flows and has them skip the NAT engine, once NAT knows it is a non-NAT flows.
- NAT GK “extended_mode” both the source and destination are stored into the cache.
- Configurable cache size option is provided with extended mode if there is lot of non-NAT traffic on a NAT interface

```
ip nat settings gatekeeper-size <xxx>
```

Address Translation Timeout

Default NAT Translation Timeout: 24 hours, use ‘`ip nat translation timeout`’ CLI to change timeout value

Use ‘`ip nat translation max-entries`’ CLI to change default global NAT translation limit

```
show plat hard qfp active feature nat datapath time
ip nat translation <xxxx>
```

Default Timeout Values

```
timeout: 86,400 seconds (24 hours)
dns-timeout: 60 seconds (1 minute)
syn-timeout: 60 seconds (1 minute)
finrst-timeout: 60 seconds (1 minute)
icmp-timeout: 60 seconds (1 minute)
pptp-timeout: 86,400 seconds (24 hours)
tcp-timeout: 86,400 seconds (24 hours) | 900 seconds (15 mins) for CGN udp-timeout: 300
seconds (5 minutes)
```

Interface Overload

- NAT can share an IP within a router ONLY through interface overload.
- With a single IP in a pool, there should be 64k ports for UDP and TCP traffic and 65535 ports for ICMP.
- With interface overload, it could be a little lesser as the port space is shared with the RP.
- At the time of port request sent to the RP when interface overload is used, a chunk of 1024 available ports is allocated to NAT by the RP.
- Interface Overload will not pick up the secondary ip address for the interface.

Static NAT and Dynamic NAT Co-exist

- It is fine to build a configuration with both static and dynamic NAT.
- However, the same IP address cannot be used for the NAT static configuration or in the pool for NAT dynamic configuration.
- The global addresses used in static translations are not automatically excluded with dynamic pools containing those same global addresses.
- Dynamic pools must be created to exclude addresses assigned by static entries

Keep non-NAT packets out of NAT interface

- NAT code is optimized to perform NAT with assumption of all traffic should be NAT’ed.
- Non-NAT’ed traffic significantly impact the NAT performance.
- The recommendation is to break the non-NAT’ed traffic off in a different (sub)interface which does not have NAT configured.
- In the feature execution path, PBR is executed before NAT
- PBR can be used to apply on the “ip nat inside” interface, and set next-hop to another (sub)interface other than the nat outside interface, therefore bypass NAT.

Steps to add new addresses/ranges in the pool (1)

- In single box environment, perform following steps in maintenance hours

  1. Active translations have to be cleared off before adding new addresses in the pool

  ➢ shut down the NAT interface

  ➢ clear ip nat trans *

  2. Add the new addresses/ranges to the pool

  1.

```
ip nat pool fred prefix-length 24
 address 171.69.233.225 171.69.233.226
 address 171.69.233.228 171.69.233.238
```

- In a B2B HA environment, the steps can be performed in production hours

  1. Synced translations have to be cleared off in RG-standby system

  ➢ shut down the RG Control/Data link

  ➢ clear ip nat trans *

  2. Add the new addresses/ranges to the pool

  3. Unshut the RG Control/Data link

  4. Force RG-standby to become Active “redundancy application reload group” on RG-active

  5. Repeat step2 in new RG-standby system

Steps to add new addresses/ranges in the pool (2)

- There is no limit on number of “address range” lines added to the pool config.
- There is a limit on number of addresses supported in a pool, which is 524,288 (19 bits long). So the pool size should be maximum 19 bits long.

Common Issues - TCAM Deny-Jump (1)

- Problem Description:

  In Catalyst 8000 IPsec/FW/NAT deployment, user may see following message:

  “%CPP_FM-3-CPP_FM_TCAM_ERROR: F0: cpp_sp: TCAM limit exceeded…”

- Error Message Explanation:

  This is an protection mechanism prevents system from crashing with WATCH-DOG timeout error or malloc failure.

- Root Cause Analysis:

  1. Classification engine in the TCAM can only represent permit.
  2. System converts the DENY entries into PERMIT ones using cross product
  3. This recursive nature cause the required number of entries to “explode”.

Common Issues - TCAM Deny-Jump (2)

- Workaround:

1. Before deploying the platform in production, apply the configuration in lab
2. Modify the ACLs to use multiple specific permit statement, and try to reduce or eliminate the explicit use of deny statement
3. Use PBR to bypass NAT

Original NAT Config	VASI & PBR to bypass NAT		
ip nat inside source list NAT-ACL pool NAT-POOL overload ! ip access-list extended NAT-ACL deny ip any 129.25.0.0 0.0.255.255 permit ip 172.19.0.0 0.0.0.255 any	ip nat inside source list NAT-ACL pool NAT-POOL overload ! interface GigabitEthernet0/0/1 description nat inside interface ip address 6.1.1.1 255.255.255.0 ip nat inside ip policy route-map no-NAT-rmap	interface vasileft1 ip address 13.1.1.1 ! interface vasiright1 ip address 13.1.2.1 255.255.255.0 ! ip access-list extended NAT-ACL permit ip 172.19.0.0 0.0.0.255 any	ip access-list extended bypass-NAT permit ip any 129.25.0.0 0.0.255.255 ! route-map no-NAT-rmap permit 10 match ip address bypass-nat set interface vasileft1

1. Static NAT

Original NAT Config	Identity NAT
ip nat inside source list NAT-ACL pool NAT-POOL overload ! ip access-list extended NAT-ACL deny ip host 172.19.1.1 any permit ip 172.19.0.0 0.0.0.255 any	ip nat inside source static 172.19.1.1 172.19.1.1 no-alias ip nat inside source list NAT-ACL pool NAT-POOL overload ! ip access-list extended NAT-ACL permit ip 172.19.0.0 0.0.0.255 any

- Solutions:

1. IOS XE 3.10 introduced the SW classification engine to handle deny-jump like classification
2. System still use TCAM as long as it has room, in case TCAM does not fit, it will switch to SW classification engine.

Common Issues - NAT ADDR ALLOC FAILURE (1)

- Problem Description:

  In Catalyst 8000 PAT/Overload configuration, system get error message:

  "%NAT-6-ADDR_ALLOC_FAILURE: Address allocation failed; pool 1 may be exhausted”

- Debug Information that should be gathered:

  ```
  show platform hardware qfp active feature nat data pool
  show platform hardware qfp active feature nat data port
  show platform hardware qfp active feature nat data stat
  show platform hardware qfp active feature nat data base
  show ip nat translation | inc <global address of interest>
  ```

- Common Reason for Failure:

1. Customer has a small pool which is being consumed by non-PAT'able binds.
2. A non-PATtable bind will show in 'sh ip nat trans' as a single local associated with a single global IP address.

```
---   213.252.7.132   172.16.254.242         ---
```

3. It consumes an entire address in the pool.

Common Issues - NAT ADDR ALLOC FAILURE (2)

- Solution 1
  1. PAT only supports protocols that have port numbers: TCP, UDP, ICMP.
  2. The best way to prevent this is to tighten the ACL to exclude non-PAttable protocols.

```
access-list 100 permit udp 13.1.0.0 0.0.255.255 any
access-list 100 permit tcp 13.1.0.0 0.0.255.255 any
access-list 100 permit icmp 13.1.0.0 0.0.255.255 any
```

- Solution 2
  1. A non-PAttable bind could be created by ALG like DNS which does not have ports in its L7 header has requested a global NAT address.
  2. Often customers do not need the DNS ALG so the solution is to turn it off.
  3. Below shows the most common ALGs which produce non-PAttable binds being turned off.

```
no ip nat service dns udp
no ip nat service dns tcp
no ip nat service netbios-ns tcp
no ip nat service netbios-ns udp
no ip nat service netbios-ssn
no ip nat service netbios-dgm
no ip nat service ldap
```

Useful Resources

- IOS XE NAT Configuration Guide: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_nat/configuration/xe-16/nat-xe-16-book.html
- IOS XE NAT Programmability Github Reference:
  - IOS XE Parent Folder: https://github.com/YangModels/yang/tree/master/vendor/cisco/xe
  - https://github.com/YangModels/yang/blob/master/vendor/cisco/xe/1741/Cisco-IOS-XE-nat.yang
  - https://github.com/YangModels/yang/blob/master/vendor/cisco/xe/1741/Cisco-IOS-XE-nat-oper.yang

Cisco Live Reference Sessions

- BRKSEC-2342
- BRKSEC-3007
- BRKSEC-2573
- BRKSEC-3147

https://www.ciscolive.com/

Thank you

Possibilities