Cisco live!

What You Make Possible

TOMORROW starts here.

CISCO

Firewall Deployment

BRKSEC-2020

Session Objectives & Housekeeping

At the end of the session, you will:

- Know what ASA hardware and software exists and how it all fits together
- Know of common firewall deployment scenarios including Multi-context firewalling
- Understand the basics of how the firewall processes packets
- Know of the main features that augment firewall services
- Get “Best Practice” suggestions for optimising your firewall deployment
- There will be time left at the end for Q&A
- Note: Session will NOT cover IPS, VPN, IOS Firewall, FWSM
- Note: Pricing will NOT be discussed

Agenda

- Firewall Specifications & Versions
- Firewall Deployment Modes
- Firewall Policy
- Advanced Firewall Features
- ASA 9.0
- Q & A

The ASA Product Family

Cisco Firewall – What is it?

- **Adaptive Security Appliance (ASA):** A family of hardened firewall appliances, proprietary OS, may have expansion slots for service modules. Has a CLI that is similar to IOS but isn't IOS.
- **FireWall Services Module (FWSM):** A module in Catalyst 6500 that provides firewall services (EoS/EoL Announced Feb 2012)
- **ASA SM:** Next Gen module for Catalyst 6500 or 7600 router, runs ASA code
- **ASA1000V Virtual/Cloud Firewall:** Virtualised edge ASA that runs with Nexus1000v and a standard ASA code
- **VSG:** Virtual Security Gateway, enforces policies between VMs
- **IOS firewall feature set:** Zone-based firewall, CBAC (not covered)

Cisco ASA Firewalls

ASA 5585-X SSP60
(20-40 Gbps, 350K conn/s
10Gb IPS, 10K VPN)

ASA 5585-X SSP40
(10-20 Gbps, 240K conn/s
5Gb IPS, 10K VPN)

ASA 5585-X SSP20
(5-10 Gbps, 125K conn/s
3Gb IPS, 5K VPN)

Multiservice 64-bit
(FW + VPN + IPS + Context)

ASA 5585-X SSP10
(2-4 Gbps, 50K conn/s
1.5Gb IPS, 5K VPN)

ASA 5555-X
(2-4Gbps,50K conn/s)
(1.5Gb IPS, 5K VPN)

ASA 5545-X
(1-3Gbps, 30K conn/s)
(900 Mb IPS, 2.5K VPN)

ASA 5525-X
(1-2Gbps, 20K conn/s)
(600 Mb IPS, 750 VPN)

ASA 5512/15-X
(1-1.2Gbps, 15K conn/s)
(400 Mb IPS, 250 VPN)

ASA CX-10
(2 Gbps, 40K conn/s)

ASA CX-20
(5 Gbps, 120K conn/s)

ASA SM
(16-20 Gbps,
300K conn/s)

Service Modules

ASA 5540
(650 Mbps, 25K conn/s)
(650 Mb IPS, 2.5K VPN)

ASA 5520
(450 Mbps, 12K conn/s)
(450Mb IPS, 750VPN)

ASA 5510
(300 Mbps, 9K conn/s)
(250Mb IPS, 250 VPN)

ASA 5505
(150 Mbps, 4K conn/s)

ASA 5550
(1.2 Gbps, 36K conn/s)
(no IPS, 5K VPN

FWSM (EOL)
(5.5 Gbps,
100K conn/s)

VSG

ASA 1000v
(650 Mbps,25K conn/s,
2.5K VPN)

Legacy Multi-Service: FW+VPN+IPS

FW + VPN Only

Virtualisation

SOHO/Teleworker | **Branch Office** | **Internet Edge** | **Campus** | **Data Centre**

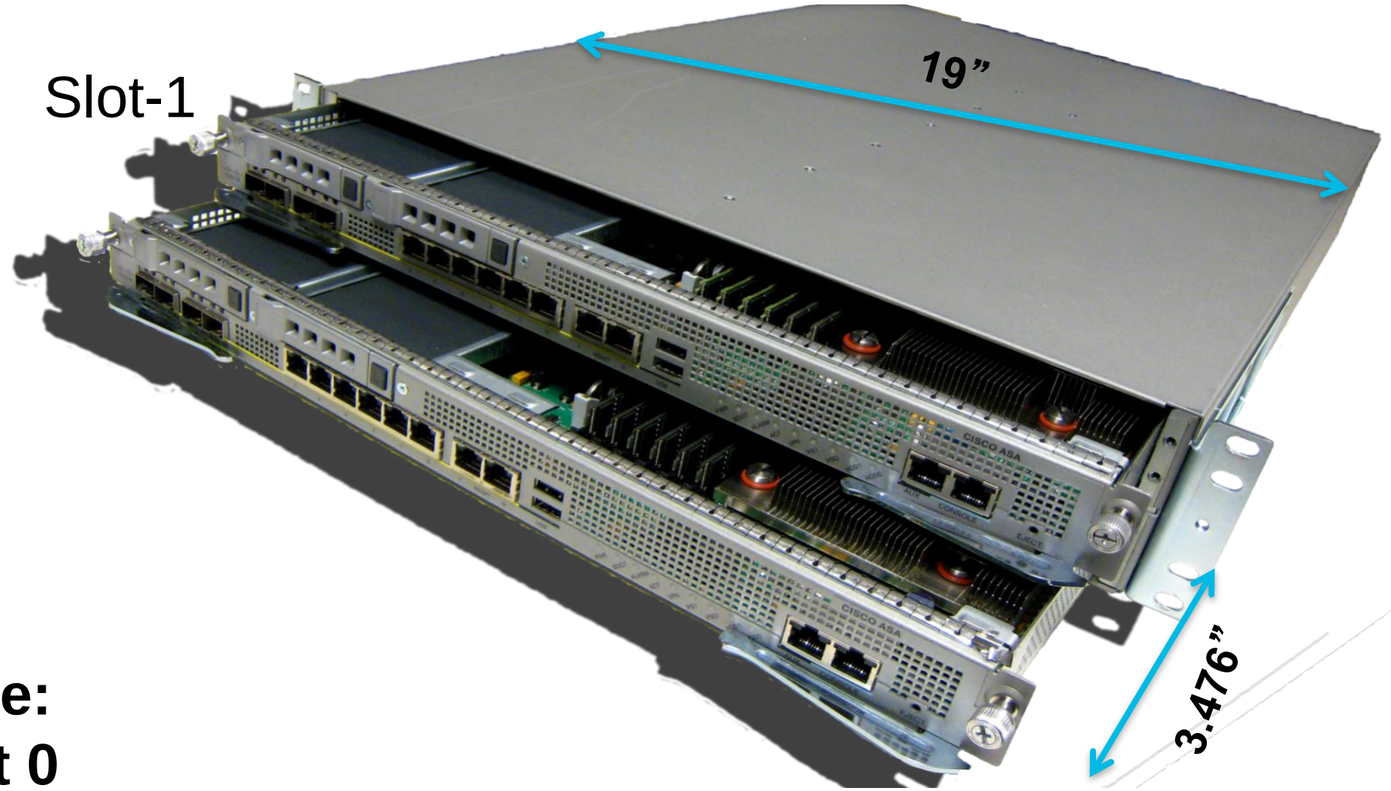
ASA Hardware Overview

Cisco ASA 5585 Chassis

2RU 19in Rack-Mountable Chassis that supports

- **2 Full-Slot Modules**
- **1 Full and 2 Half-Slot Modules**

- **Same chassis for all ASA 5585 products**
- **Weighs 30kg with 2 modules and 2 power supplies**

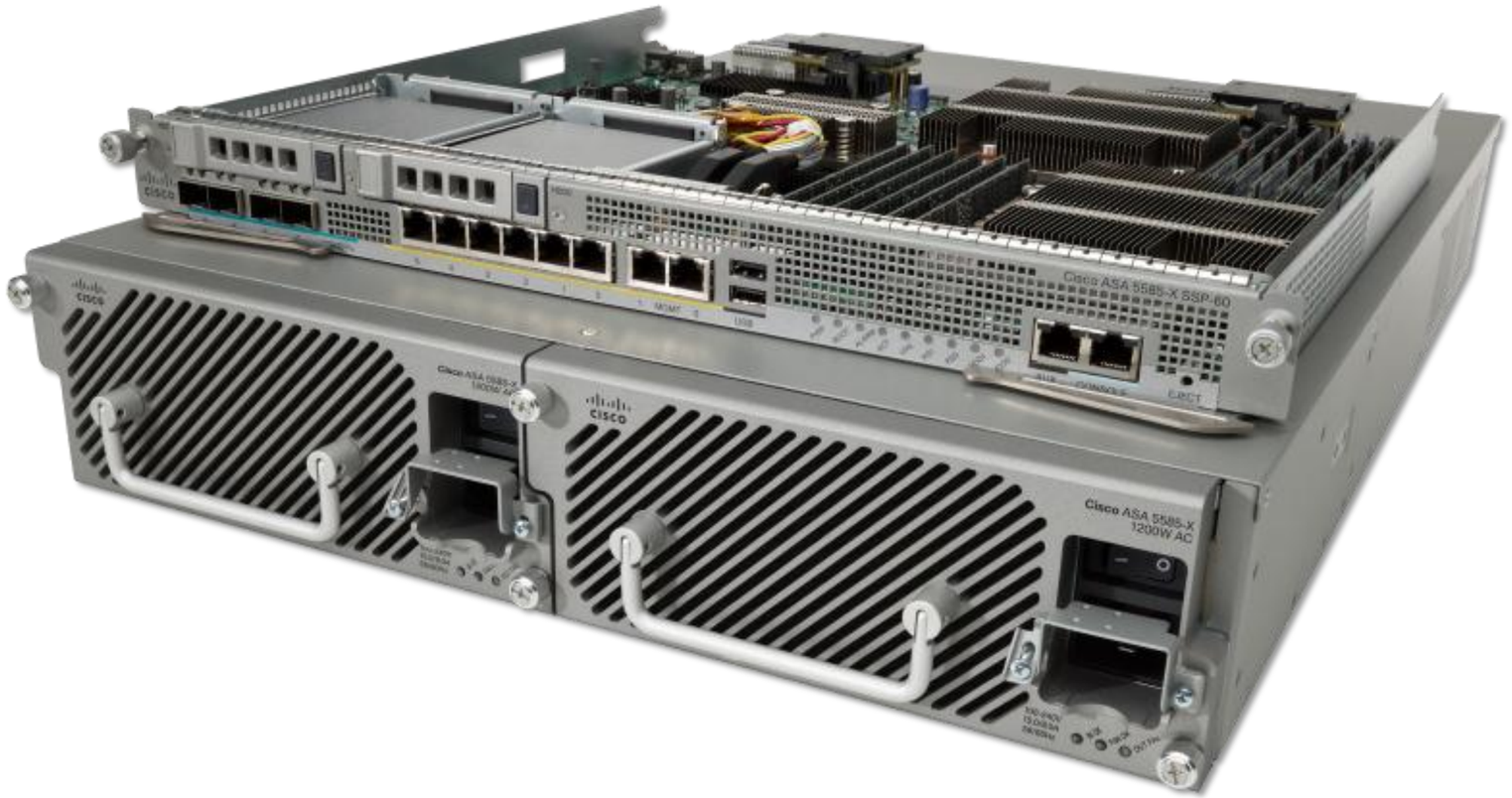


2 Full Sized Modules available:

- **ASA SSP required in Slot 0**
- **IPS/ASA/CX SSP optional in Slot 1**

ASA 5585-X with ASA CX (Context-Aware)

- Context-Aware Firewall*
- Active/Passive Authentication
- Application Visibility and Control
- Reputation Filtering
- URL Filtering
- SSL Decryption
- Secure Mobility
- SSP-10 and SSP-20 at FCS



* More detail in Context-Aware Firewall Section

ASA 5500-X Midrange Platform - Overview

Customer Benefits

Performance

Density

Flexibility

Integrated Services

Management Consolidation

ASA 5500-X H/W Features

64Bit Multi-Core Processor

Up to 16GB of Memory

Built-In Multi-Core Crypto Accelerator Hardware

Dedicated IPS Hardware Acceleration Card

Up to 14 1GE Ports

Copper & Fiber I/O options

Firewall, VPN & IPS Services

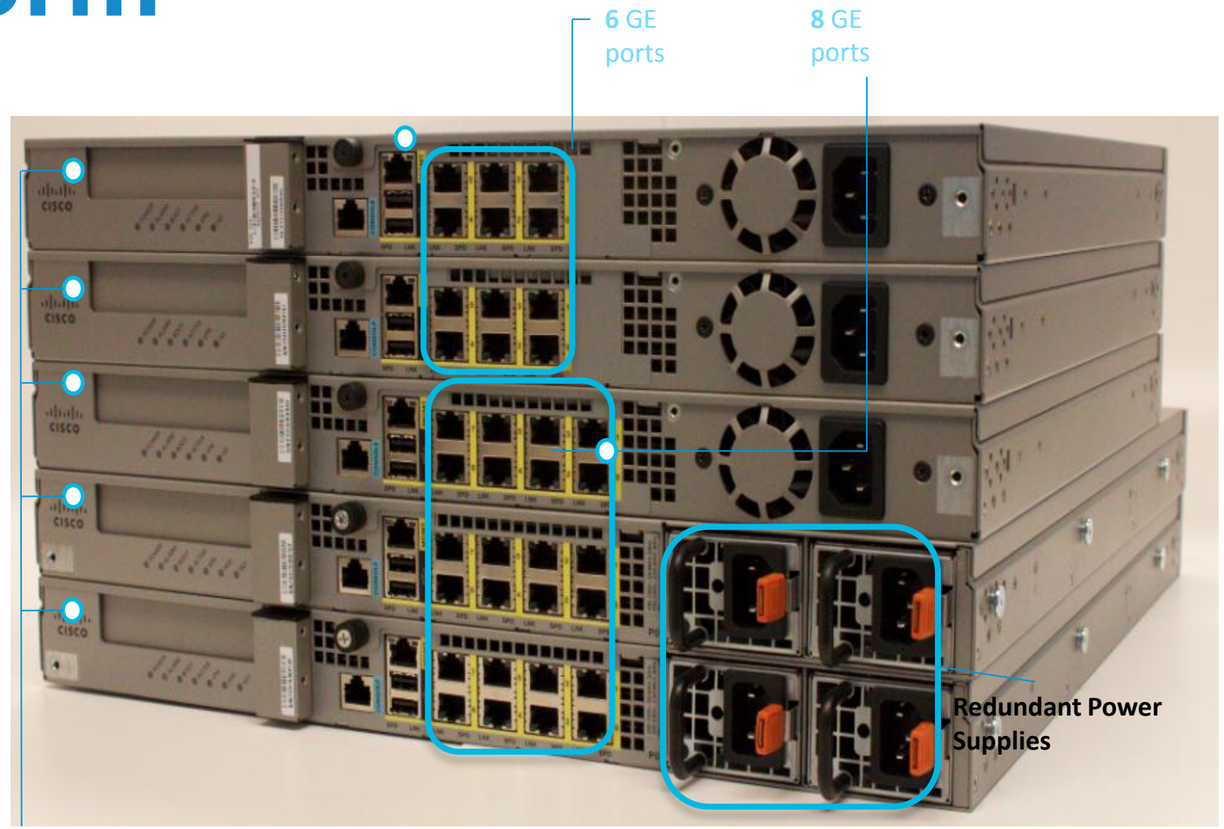
Dedicated OOB Management Port

ASA 5500-X Midrange Platform Details

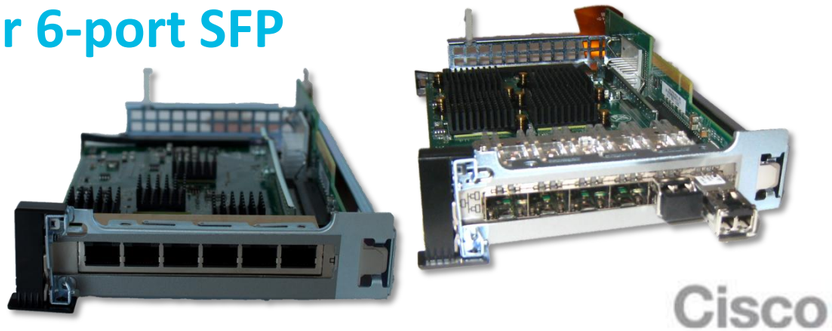
- Enterprise-class hardware architecture designed to support multiple services
  - Multi-Core multi-threaded CPUs
  - 4x Memory
  - Dedicated IPS Hardware Accelerator
  - Dedicated VPN Hardware Accelerator
- Services Supported
  - IPS (Dedicated Hardware on Mainboard) - SW License Enabled
  - Botnet Traffic Filter – SW License Enabled
    - Combined with real-time threat information from 500 feeds through Cisco SIO (Security Intelligence Operations), IPS and Botnet Protection provide protection against complex APTs.
  - VPN & AnyConnect
    - Enables BYOD with security besides providing always-on remote access
  - Support for CX enabled in 9.1.1

ASA 5500-X Platform

1 RU – 64-bit Appliances



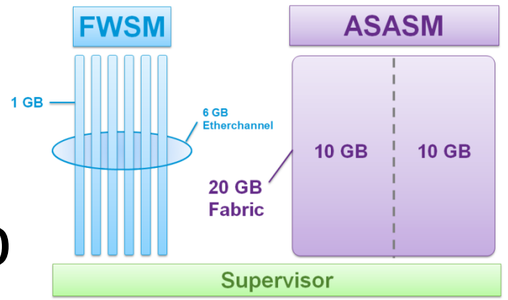
1 Expansion Slot
6-port GE or 6-port SFP



ASA Services Module (ASA SM)

Next Generation FWSM

- Integrated ASA Firewall into the Cat 6k
- Leverages architecture of the 5585-X
- Integrates two advanced Nitrox Crypto accelerato
- No physical interfaces – Uses existing VLANs
  - VLANs are redirected to inspection engine
- Standard ASA code base to maintain feature parity*
- Allows firewall scaling to meet increased traffic demands in larger Data Centre/Campus networks



* More info in Software Versions Section

ASA SM and FWSM Comparison

Feature	ASA SM	FWSM
Real-IP ACLs/ Global ACLs	Yes (2M max)	No (~80k max)
Bridge-groups	8 Bridge-groups 4 Interfaces each	8 Bridge-groups 2 Interfaces each
Virtual Contexts	250 Max	250 Max
Mixed-Mode	Yes	Yes
AutoState	Yes	Yes
VPN	Yes as of 9.x	For management only
Throughput/CPS/MaxConn	16-20G/300K/8M	4-5.5G/100K/2M

ASA SM Supported Hardware Summary

- WS-C6500-E series
- CISCO7600-S series + CISCO7604

Supervisor Cards

- VS-S720-10G-3C (SXJ4+)
- WS-SUP720-3B (SXJ4+)
- VS-S2T-10G (15.0.1(SY1) for 6K and 15.1.1(SY) for 7600)
- RSP720-3C and up (15.2(4)S2)

ASA SM Deployment

- ASA SM only works in 6500-E chassis, will not boot up in non-E chassis due to airflow requirement
- Design based on whether ASA SM sits in front of or behind a Switched Virtual Interface (SVI)
  - This is achieved via assigning specific VLANs to be firewalled (similar to FWSM)
- Autostate on the Catalyst alerts the ASA SM when a physical port in a specific VLAN goes down
  - Speeds up failover time significantly, as ASA SM will bypass interface monitoring
- Migration Tool on Cisco.com for FWSM → ASA replacement

ASA Software Versions

ASA Software Versioning

- Older ASA Software versions (7.2.x, 8.0x – 8.2x) still supported on legacy hardware
- Specific ASA code versions required for specific hardware/platform (and some software have hw requirements too: memory for 8.3+, SSD for CX)
- Current ASA Features based upon ASA 8.4x code base
  - 64-bit (on supported hardware)
  - New NAT model, Real-IP
  - Identity Firewall (AD Agent)
  - CX for 5585-X
- ASA code convergence into a single version (9.x) which also introduces:
  - Multi-context enhancements (s2s VPN, dynamic routing, …)
  - Enhanced IPv6 (ipv6 NAT: 64, 46, 66, mixed ACL, OSPFv3, …)
  - CX as a software module for mid range 55x5-X hardware (9.1)
  - Scansafe, Trustsec
  - Clustering

ASA compatibility

Mapping ASA Software Versions to ASA Hardware

ASA 9.x*


ASA 5585-X SSP60


ASA 5585-X SSP40

SMP8.2 or 8.4.4


ASA 5585-X SSP20


ASA 5585-X SSP10


ASA 5555-X

SMP8.6


ASA 5545-X


ASA 5525-X


ASA 5512/15-X


ASA CX-20


ASA CX-10

8.4.5

8.5

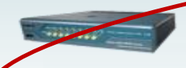

ASA SM

8.0 – 8.4.4


ASA 5540


ASA 5520


ASA 5510


ASA 5505


ASA 5550

N/A


FWSM (EOL)

N/A


VSG

8.7


ASA 1000v

SOHO/Teleworker | Branch Office | Internet Edge | Campus | Data Centre

* Intended ASA Code Convergence for all ASA platforms

ASA 8.4.x Base Features Overview

In addition to previous ASA features:

- 8.4x is now 64-bit on supported platforms
  - Increases ASA platform limits for connections and VLANs
  - 5500-X / 5585-X platform(s) require SMP image
- Port Channel and Bridge-Group enhancements for easier deployments
- Stateful failover of EIGRP and OSPF
- **All licenses are shared between HA pairs** (from 8.3)
- Native Identity Firewall Support to AD Agent
- Resource Mapping to FQDN for access rules
- IPv6 Inspection with service policy
- Increased NAT/PAT capabilities
  - Identity NAT configurable proxy ARP and route lookup
  - PAT pool and round robin address assignment
- Additional SNMP traps, Log Viewer enhancements on ASDM, TCP Ping, WhoIs lookups and more for manageability and troubleshooting
- See release notes for a complete list

8.4.x Release Notes

Current ASA Version Deltas

New Features By Release

- 8.4.3 enables extended PAT pool options
  - Round Robin pool allocation using same IP address
  - Configurable PAT xlate timeout
  - Flat range of PAT ports, PAT pools and extended PAT for a PAT pool
- 8.4.5 enables policy redirection to CX Module for Context-Aware Firewall
- 8.5.x allows mixed-mode deployment for ASA SM installations
  - More detail later in this session
- 8.6.x is SMP version of 8.4.x for 5500-X mid-range appliances
- 8.7.x provides base ASA feature-set for ASA1000V Virtual/Cloud Firewall
  - Demo Link: http://www.youtube.com/watch?v=5Vwo6n5tXao

ASA 9.x New Features Overview

- IPv6 enhancements: Mixed IPv4/IPv6 ACL, NAT, …
- Multiple-Context Mode enhancements: Dynamic routing, S2S VPN, …
- Trustsec: SGT, SXP
- Cloud Web Security (ScanSafe)
- Clustering
- VPN infrastructure enhancements
- Clientless SSLVPN enhancements
- CX for 5585-X + SSP and mid-range with 9.1.1
- Core infrastructure enhancements:

  Feature parity between ASASM and appliances, ICMP code support in ACLs and Objects

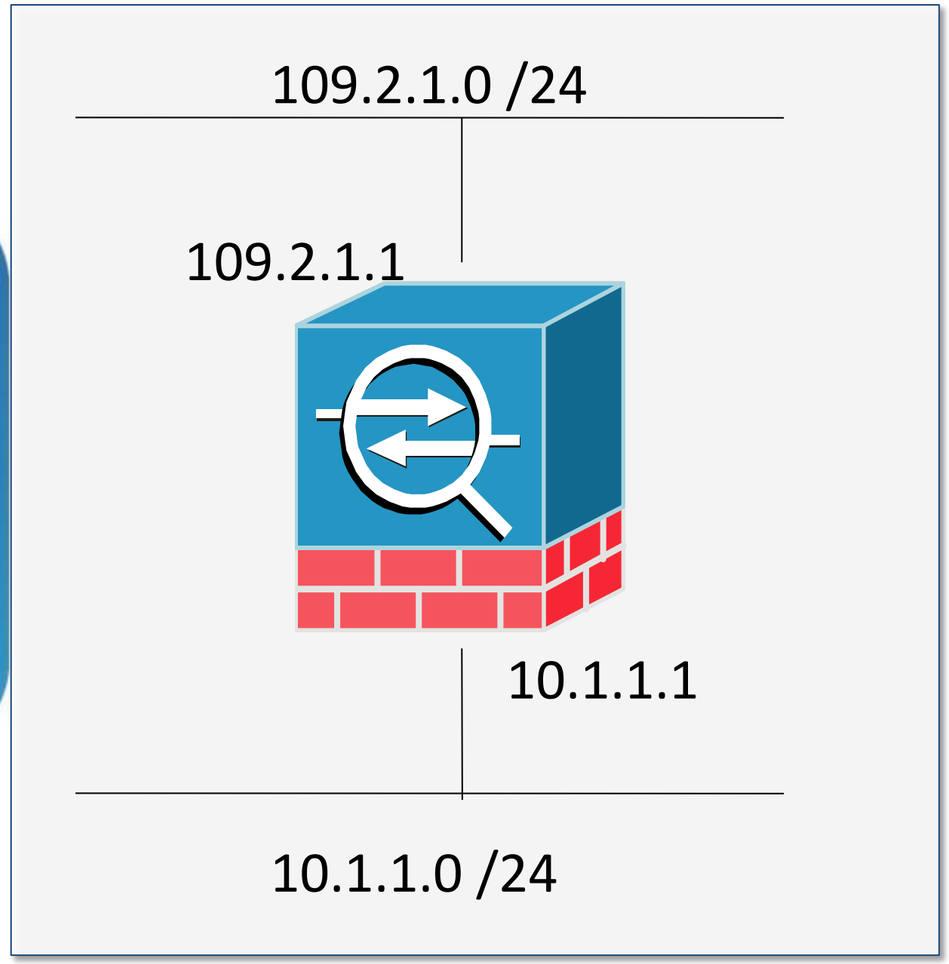
9.0.x Release Notes

Firewall Deployment Modes

Firewall Design – Modes of Operation

- **Routed Mode** is the traditional mode of the firewall. Two or more interfaces that separate L3 domains
- **Transparent Mode** is where the firewall acts as a bridge functioning mostly at L2
- **Multi-context** mode involves the use of virtual firewalls, which can be either routed or transparent mode
- **Mixed mode** is the concept of using virtualisation to combine routed and transparent mode virtual firewalls

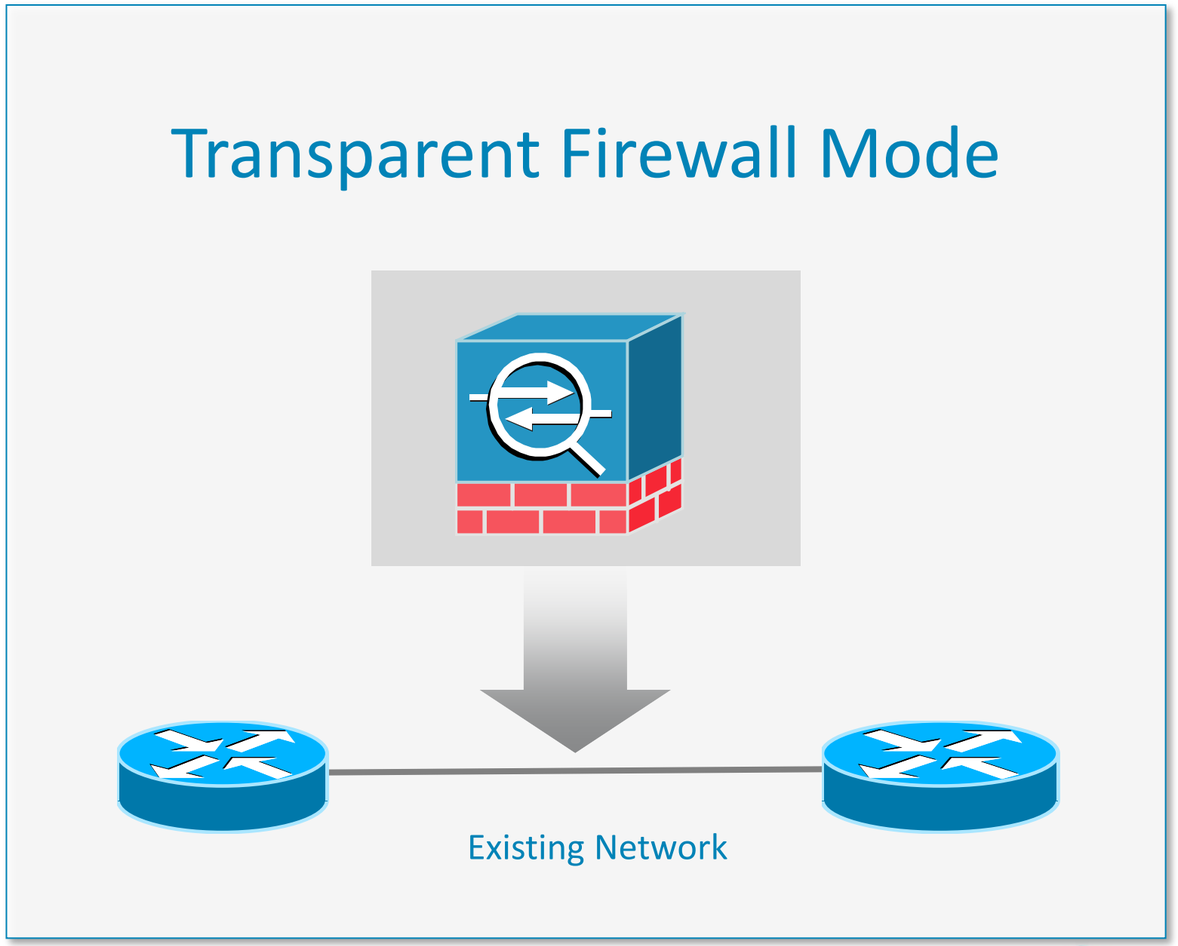
Firewall - Routed Mode



- Traditional mode of the firewall (layer 3 hop)
- Separates two L3 domains
- Often a NAT boundary
- Policy is applied to flows as they transit the firewall

Firewall – Transparent Mode

- Operates at layer 2, transparent to the network
- Drops into existing networks without re-addressing or re-design
- Simplifies internal firewalling & network segmentation



Why Deploy Transparent Mode?

- Routing protocols can establish adjacencies through the firewall
- Protocols such as HSRP, VRRP, GLBP can cross the firewall
- Multicast streams can traverse the firewall
- Non-IP traffic can be allowed (IPX, MPLS, BPDUs)
- Deploy where IP address schemes can not be modified
- NO dynamic routing protocol support (on the FW itself) or VPN support
- NO QoS or DHCP Relay support
- More caveats and gotchas, refer to the Cisco.com docs for details

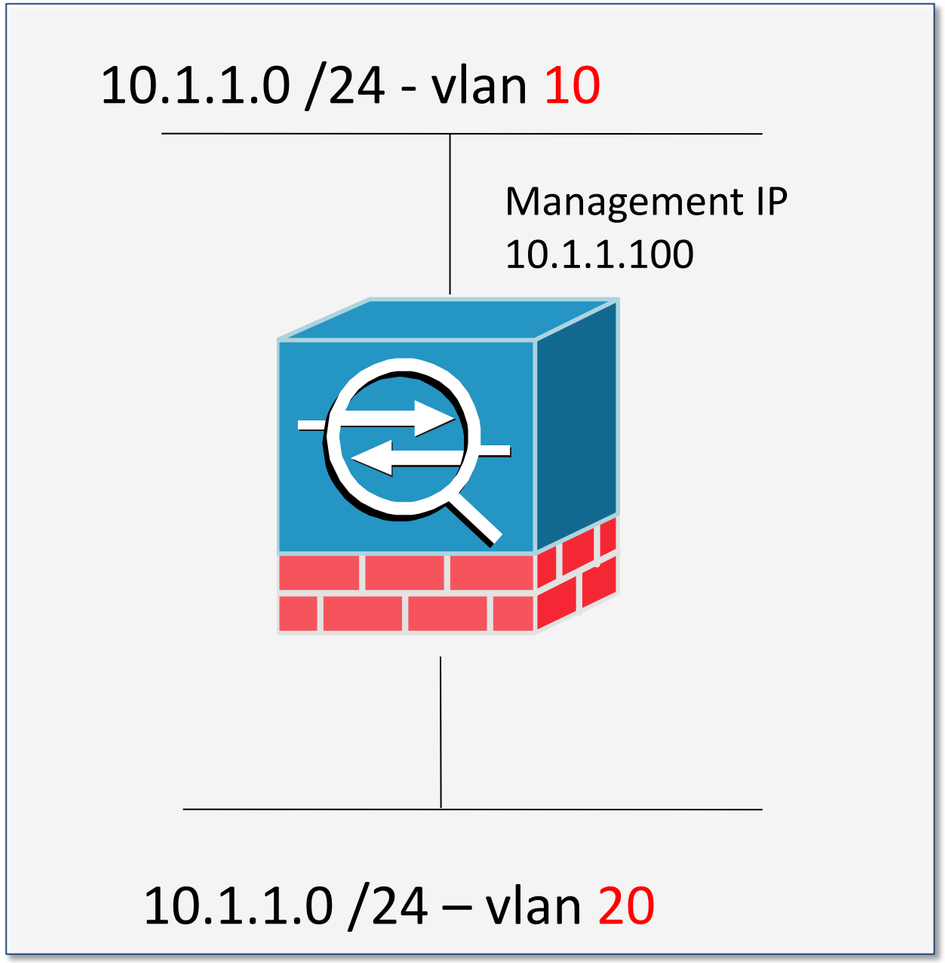
How Does Transparent Mode Work?

- Often used in Data Centre/Campus deployment in Core/Aggregation layer
- Firewall functions like a bridge (“bump in the wire”) at L2, only ARP packets pass without an explicit ACL (does not pass Cisco Discovery Protocol)
- **Same** subnet exists on inside and outside of ASA
  - **Different** VLANs on inside and outside
- No need to change the network design to introduce Firewall Access Control (ACL)
- NAT is supported in Transparent Firewall, requires 8.0.2+ on the ASA

Transparent Mode Requirements

- A management IP is **required** for both management and for traffic to pass through the transparent firewall
  - IP address MUST be on same subnet
  - If management by IP is required with L3 routing, assign 2nd IP address to Management Interface + add route to default gateway – overlapping IP is okay
- Set default gateways of hosts to L3 on far side of firewall, NOT the management IP of firewall
- Up to 32 interfaces are supported per virtual context (4 per BVI x8)
- For specifics reference the ASA Configuration Guide here:
  http://www.cisco.com/en/US/docs/security/asa/asa84/configuration/guide/mode_fw.html

Transparent Mode Configuration




```
firewall transparent
hostname ciscoasa
!
interface GigabitEthernet0/0
 nameif outside
 security-level 0
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
!
ip address 10.1.1.100 255.255.255.0
```

Configuration Example: ASA 8.3 vs. ASA

Transparent Firewall ASA 8.3 and Earlier

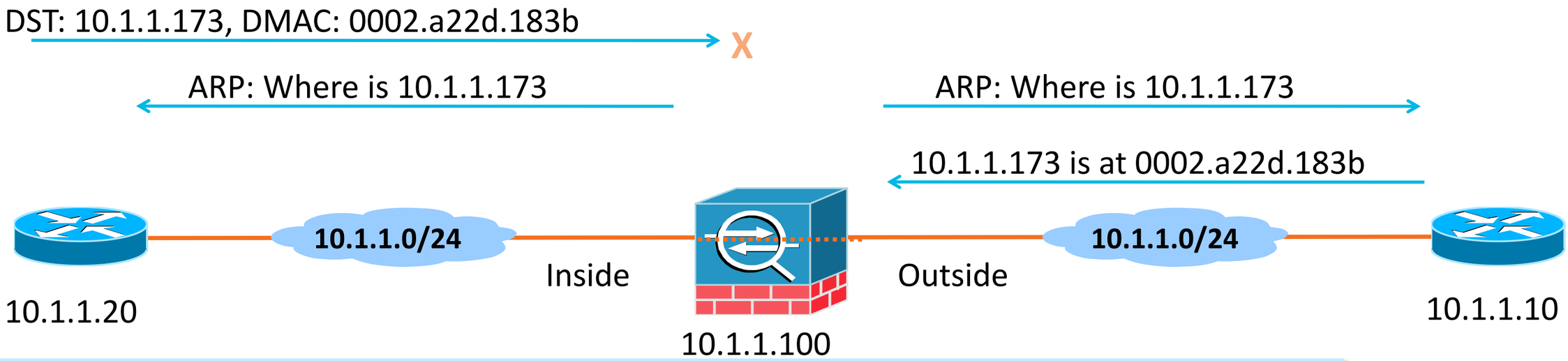
```
firewall transparent

interface GigabitEthernet 0/0
    nameif inside
    security-level 100

interface GigabitEthernet 0/1
    nameif outside
    security-level 0

    ip address 10.1.1.100 255.255.255.0
```

Transparent Firewall ASA 8.4

```
firewall transparent
interface GigabitEthernet 0/0
    nameif inside
    security 100
    bridge-group 1

interface GigabitEthernet 0/1
    nameif outside
    security 0
    bridge-group 1

interface GigabitEthernet 0/2
    nameif dmz
    security 50
    bridge-group 1

interface GigabitEthernet 0/3
    nameif inside
    security 51
    bridge-group 1

interface BVI 1
    Ip address 10.1.1.100 255.255.255.0
```

ASA TFW Behaviour with Local Destination

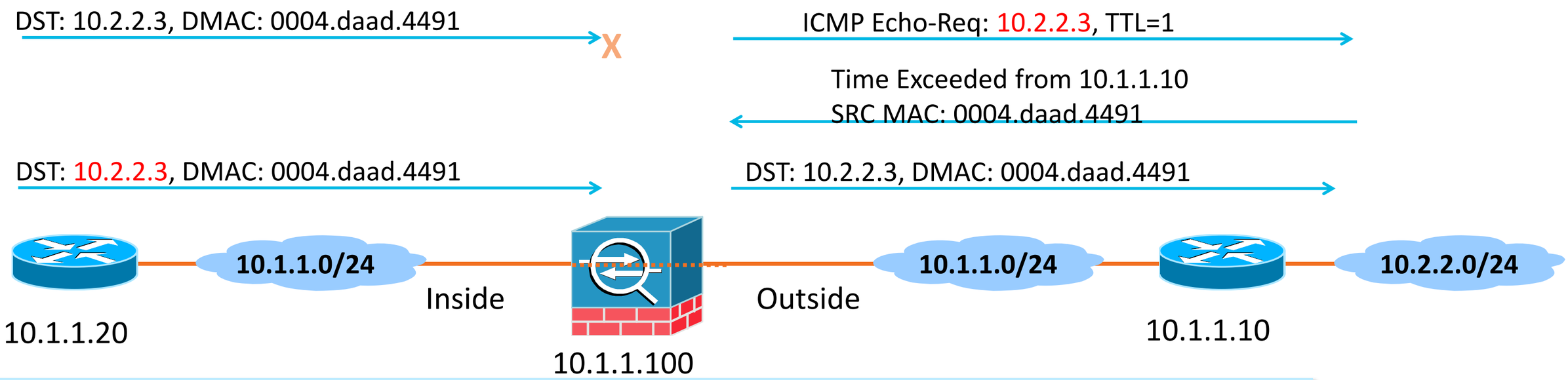
```
ciscoasa# show mac-address-table
interface                       mac   address           type       Age(min)
--------------------------------------------------------------------------
Outside                        0024.c4b3.c6e1            dynamic     3
Inside                         0050.56b2.1351            dynamic     2
```




```
ciscoasa# show mac-address-table
interface                       mac   address           type       Age(min)
--------------------------------------------------------------------------
Outside                        0024.c4b3.c6e1            dynamic     3
Outside                        0002.a22d.183b            dynamic     5
Inside                         0050.56b2.1351            dynamic     2
```

ASA TFW Behaviour with Remote Destination

```
ciscoasa# show mac-address-table
interface                       mac   address           type       Age(min)
--------------------------------------------------------------------------
Inside                        0050.56b2.1351            dynamic     2
```



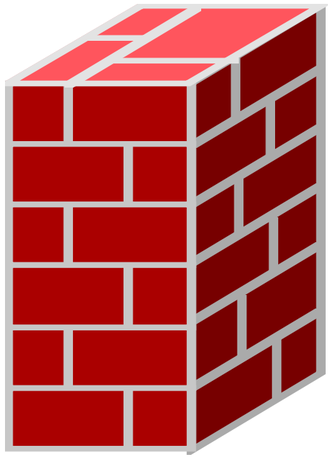

```
ciscoasa# show mac-address-table
interface                       mac   address           type       Age(min)
--------------------------------------------------------------------------
Outside                       0004.daad.4491            dynamic     5
Inside                        0050.56b2.1351            dynamic     2
```

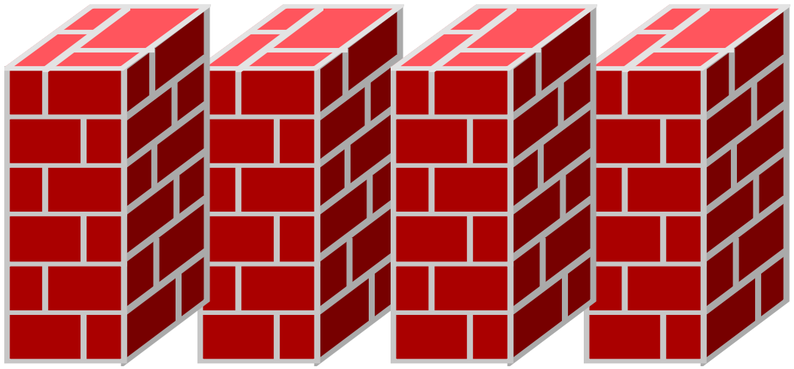
Firewall Deployment Modes

Virtualisation (Multi-Context Mode)

Firewall Design - Virtualisation

- Virtualisation provides a way to create multiple firewalls in the same physical chassis
- Maximum number of virtual firewalls is 250 on both ASA/ASA SM* - Platform Dependent





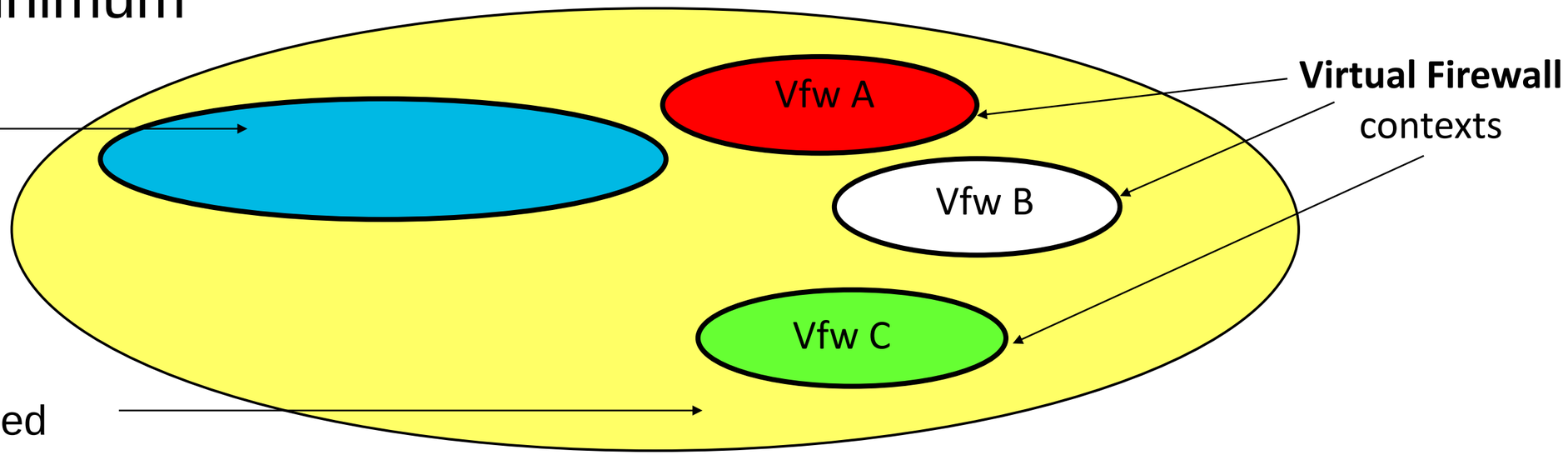
- Virtualisation is a licensed feature
- Commonly used to apply unique security policies in one physical chassis

* ASA requires 8.4.1> to get 250 contexts

Multi-Context Firewall on ASA and ASA SM

- Context = a virtual firewall
- All virtualised firewalls must define a System context and an Admin context at a minimum

Admin Context:
Remote root access and access to **all** contexts

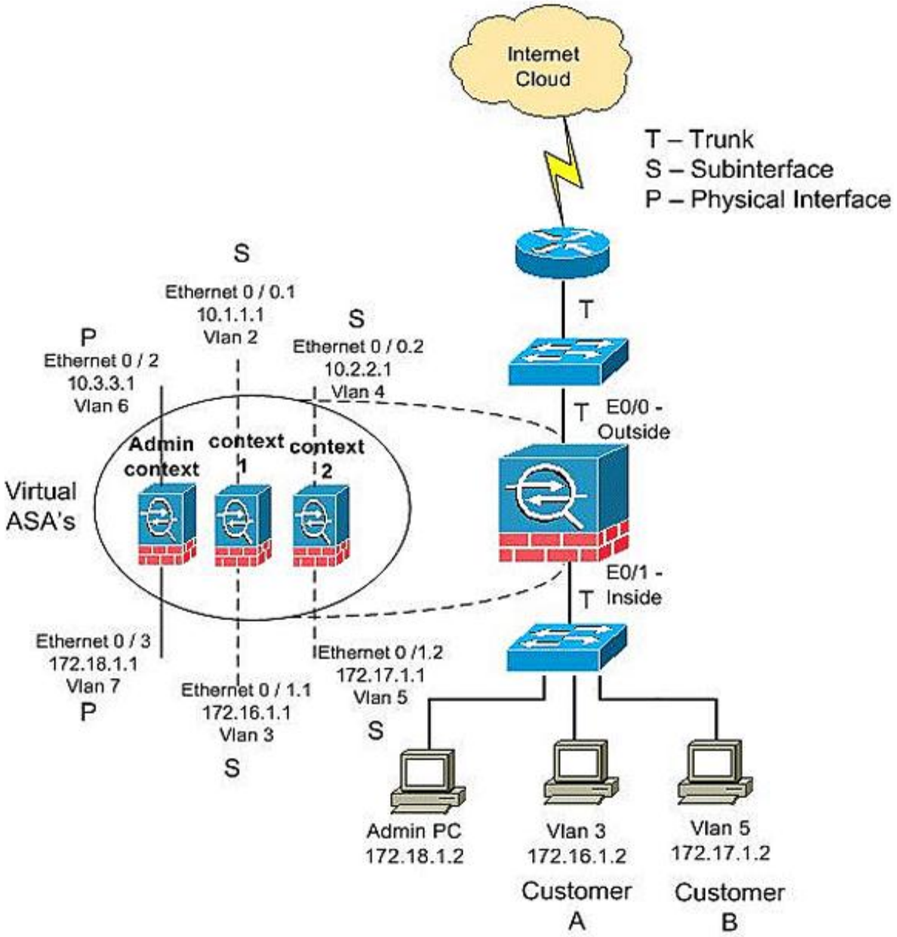


System Context:
Physical ports assigned

- There is no policy inheritance between contexts
- The system space uses the admin context for network connectivity; system space creates other contexts

Multi-context Deployment

```
mode multiple

admin-context admin

context admin
  allocate-interface Ethernet0/2 outside
  allocate-interface Ethernet0/3 inside
  config-url disk0:/admin.cfg

context context1
  allocate-interface Ethernet0/0.1 outside-context1
  allocate-interface Ethernet0/1.1 inside-context1
  config-url disk0:/context1.cfg

context context2
  allocate-interface Ethernet0/0.2 outside-context2
  allocate-interface Ethernet0/1.2 inside-context2
  config-url disk0:/context2.cfg
```



Unsupported Features in ASA Multi-Context Mode (prior to ASA 9.0)

- Dynamic routing protocols:
  - EIGRP
  - OSPFv2
  - OSPFv3
  - RIP
- Mix of transparent and routed contexts (below 8.5.1)
- Multicast routing (multicast bridging is supported)
- VPN services:
  - Site to Site
  - Remote access

Unsupported Features in ASA Multi-Context Mode (ASA 9.0)

- Dynamic routing protocols (inter-context routing still not supported):
  - OSPFv3
  - RIP
- Multicast routing (multicast bridging is supported)
- VPN services:
  - Remote access

Multi-Context and Resource Management

- By default, all virtual firewalls (contexts) have access to unlimited physical resources in the ASA
- To avoid exhausting system resources, the ASA can be configured to manage resources as a percentage or an absolute number

```
class gold
limit-resource mac-addresses 10000
limit-resource conns 15%
limit-resource rate conns 1000
limit-resource rate inspects 500
limit-resource hosts 9000
limit-resource asdm 5
limit-resource ssh 5
limit-resource rate syslogs 5000
limit-resource telnet 5
limit-resource xlates 36000
```

- This is common in multi-tenant environments where one physical firewall is virtualised to serve multiple customers

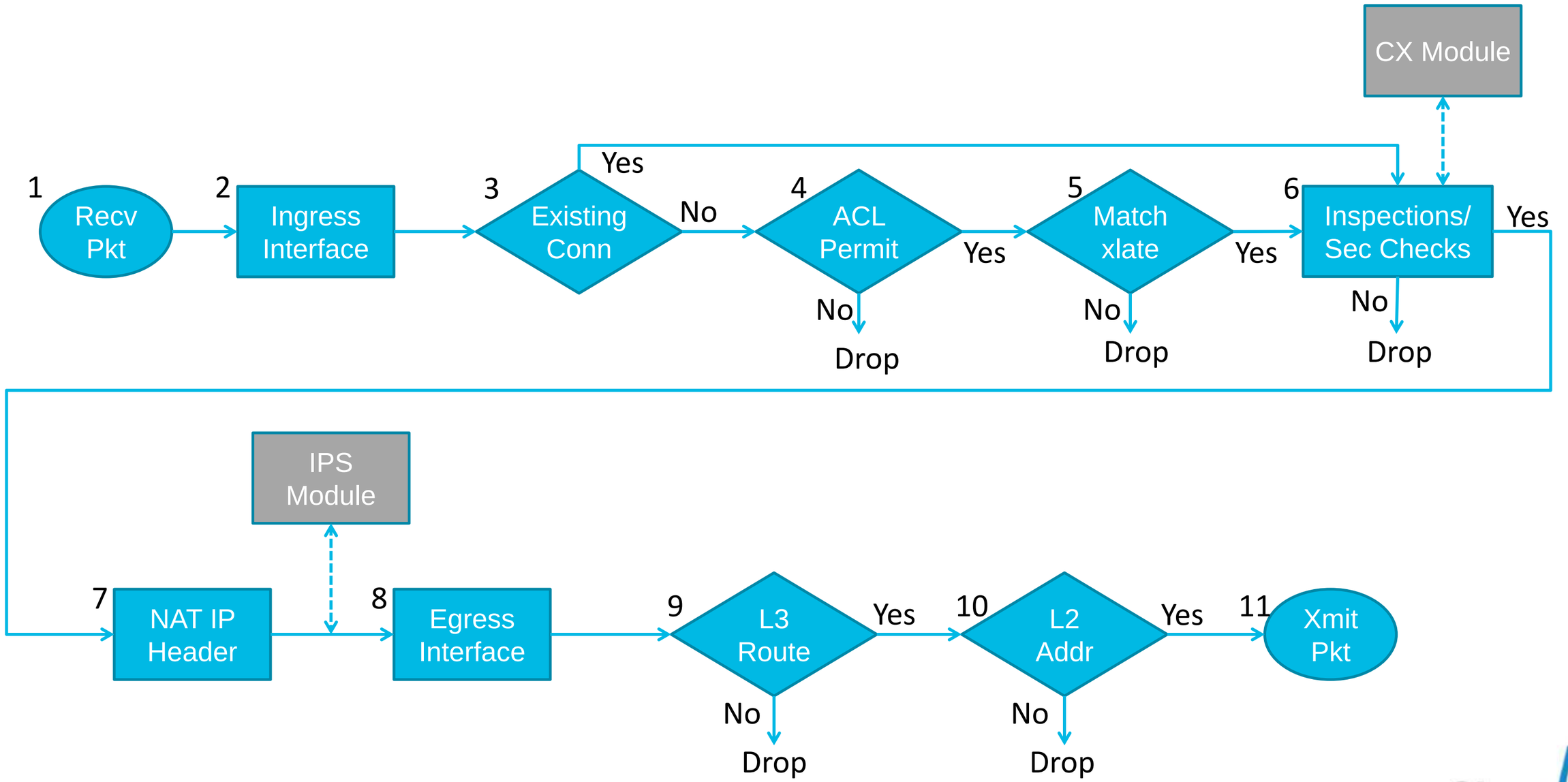
Firewall Design - Mixed Mode

- Mixed Mode is the concept of using virtual firewalls, some in routed mode and some in transparent (L2) mode
- This is only supported on the ASA-SM today with 8.5 code or ASA 9.x
- Up to 8 pairs of interfaces are supported per context
- Some caveats and dependencies, check the Release Notes

```
mode multiple

context context1
  firewall transparent
  allocate-interface vlan99 outside
  allocate-interface vlan100 inside
  config-url disk0:/ctx1.cfg
  member gold
context context2
  allocate-interface vlan200 outside
  allocate-interface vlan210 inside
  config-url disk0:/ctx2.cfg
```

ASA Firewall Policy

ASA Packet Processing Flow



NAT on the ASA

Network Address Translation

NAT Control

- **NAT control** is the concept that a packet from a high security interface (e.g. “inside”) must match a NAT policy when traversing a lower level security interface (e.g. “outside”)
- If the packet does not match a NAT policy, then it is dropped
- NAT control is **disabled** by default**

** In certain cases it may be enabled after an upgrade

Configuring NAT (pre 8.3)

- NAT configuration requires at least two parts: a **nat** statement and a matching **global** statement

```
asa(config)# nat (inside) 1 10.1.2.0 255.255.255.0
asa(config)# global (outside) 1 172.16.1.3-172.16.1.10
```

- Multiple **nat** statements can reference the same **global**

```
asa(config)# nat (inside) 1 10.1.2.0 255.255.255.0
asa(config)# nat (inside) 1 192.168.1.0 255.255.255.0
asa(config)# nat (dmz) 1 10.1.1.0 255.255.255.0
asa(config)# global (outside) 1 209.165.201.3-209.165.201.10
```

- Multiple NAT ids can be used for NAT policy granular matching

NAT Redesign in ASA 8.3

NAT configuration in 8.3 and above is the same

VoD on 8.3+ NAT

- Starting with the 8.3 release, NAT has been completely redesigned to simplify configuration and troubleshooting
- Follows original packet vs. translated packet model
- New features:
  1. Unified NAT Table to view all NAT policies
  2. Object-based NAT: object can be created for hosts, networks or address ranges and NAT can be configured within the object
  3. Two NAT Options: Object-based (Auto) and Manual NAT
  4. Interface independent NAT

Network Objects in 8.3+ NAT

- No longer use global and static elements found in pre 8.3 NAT configuration
- ACLs now reference the original (pre-translated) IP address
- New building block for NAT configuration is the **network object**
- Network objects can be a single host, a subnet or a range of networks
- Two new NAT types:
  1. Auto-NAT – will cover most source NAT use cases
  2. Twice NAT – when NAT is required based on destination

Understanding Auto NAT in 8.4

Pre 8.3 NAT

```
asa(config)# nat (inside) 1 192.168.1.0 255.255.255.0
asa(config)# global (outside) 1 interface
```

- Auto NAT requires the object configuration and the NAT configuration is contained within

```
asa(config)# object network inside-net
asa(config)# subnet 192.168.1.0 255.255.255.0
asa(config)# nat (inside,outside) dynamic interface
```

  - Now add a static NAT translation to translate a server at 192.168.1.201 to 172.16.1.201:

```
asa(config)# object network big-server
asa(config)# host 192.168.1.201 255.255.255.0
asa(config)# nat (inside,outside) static 172.16.1.201
```

Caveats with Auto NAT

- Because the rules are never paired, you cannot specify that sourceA/destinationA should have a different translation than sourceA/destinationB
- Access Lists reference the internal (real) IP address and not the global
- Auto NAT either applies to the source OR the destination of a packet—NOT both
- Doing both requires a new construct: Twice NAT (also known as Manual NAT)

Understanding Twice NAT

- Unlike Auto NAT, Twice NAT policy configuration is not done within the network object
- Configuration for both source and destination policy are done in a single rule (bidirectional)
- Twice NAT can reference network objects and object-groups but NAT policy is assigned outside of network object element

```
asa(config)# object service FTP_PASV_PORT_RANGE
asa(config)# service tcp port range 65000 65004
asa(config)# object network FTP_SERVER
asa(config)# service host 192.168.1.201
nat (inside,outside) source static host FTP_SERVER interface service
FTP_PASV_PORT_RANGE
```

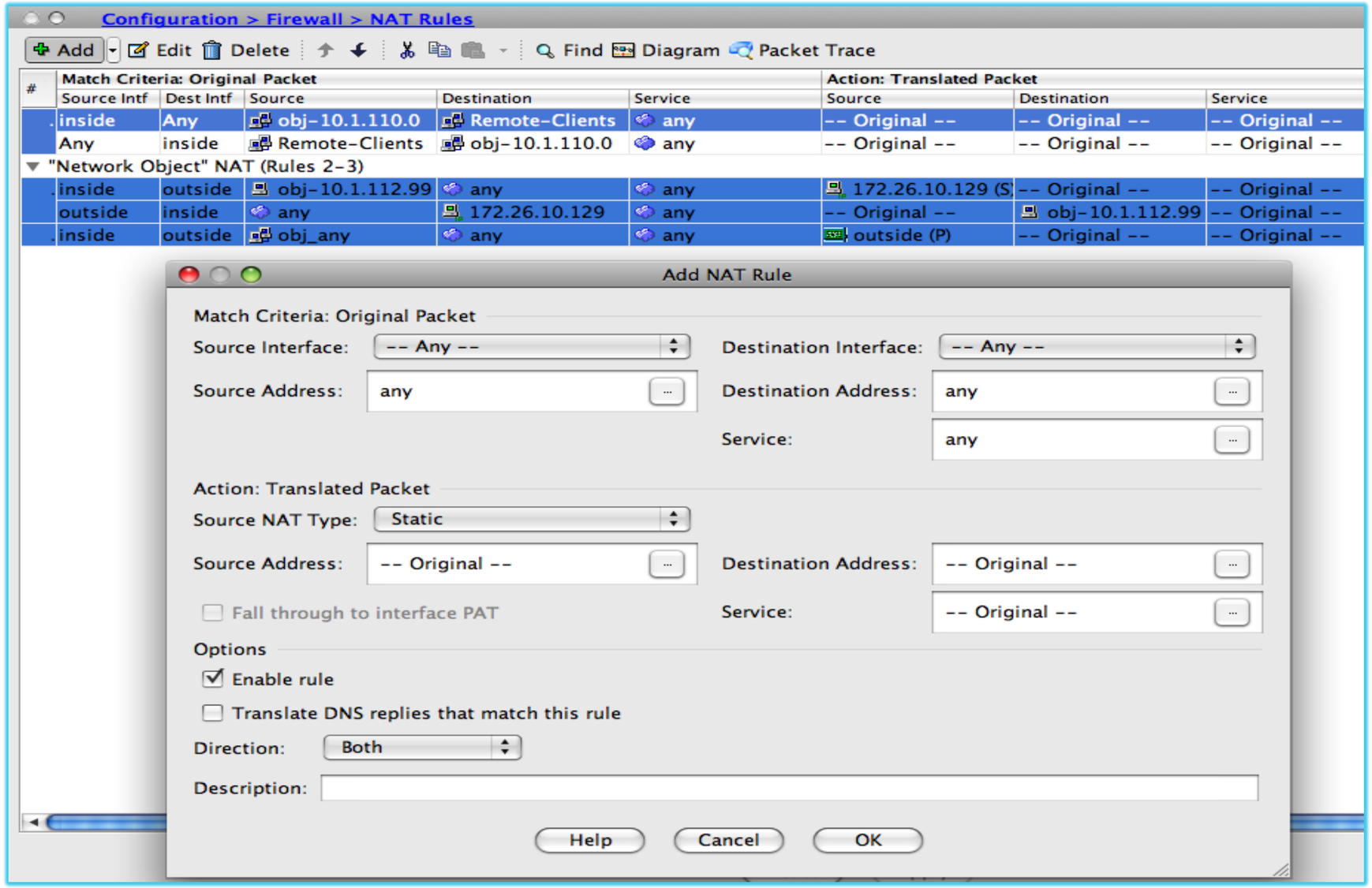
Much more detail in 8.4 Configuration Guide:
http://www.cisco.com/en/US/docs/security/asa/asa84/configuration/guide/nat_overview.html

NAT Order of Operation

- NAT rules are applied via top down order with first match
- Rules are processed in the following order:
  1. Twice NAT (Manual NAT) rules
  2. Object-based NAT rules
  3. Twice NAT (Manual NAT) rules (When translating both source and dest IP/Ports)
- Use packet tracer in ASDM for validating NAT policy
- Helpful show commands for NAT configuration:

  show run nat, show nat, show run object

ASA 8.3+ Unified NAT Table



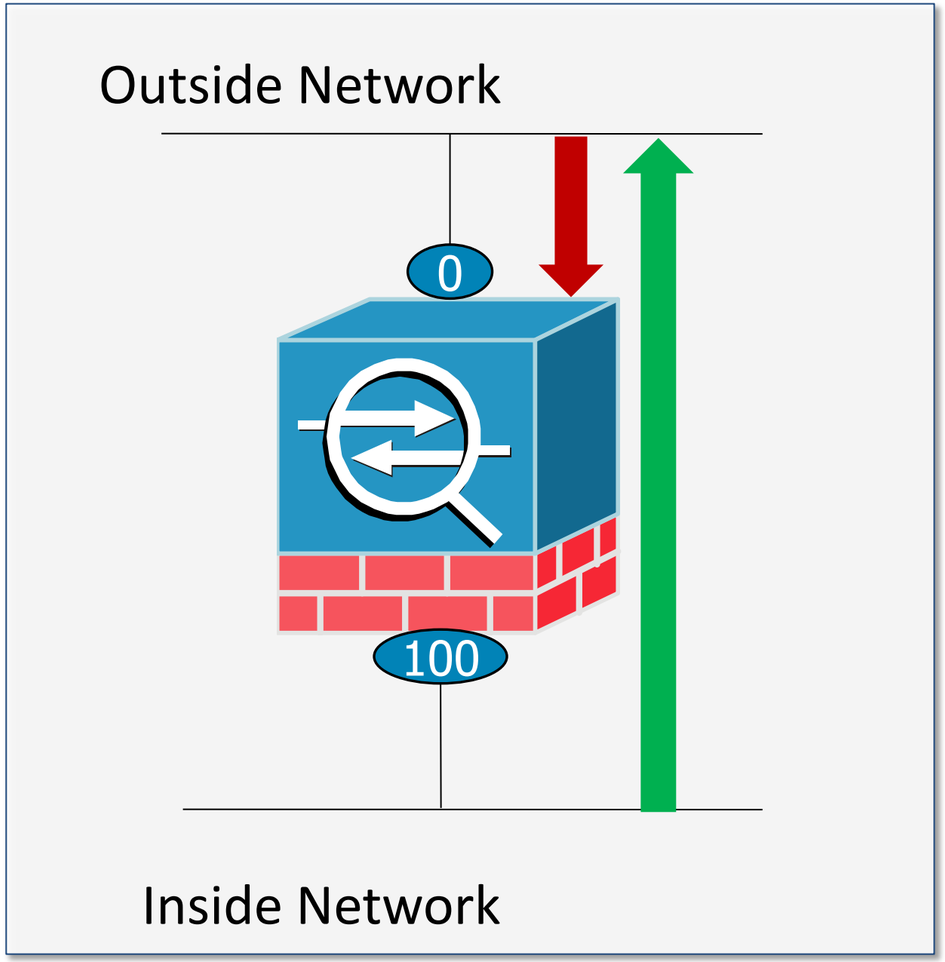
Firewall Access Control

Firewall Security Levels and Access Control Lists

Firewall Security Levels

- A security level is a number between 0 and 100 that determines how firewall rules are processed for the data plane
- Security levels are tied to an interface: the inside or private side interface is always 100 (most trusted) and the outside or public interface is always 0 (least trusted)
  - DMZ interfaces, if used, may be assigned numbers between 1 and 99
- All conversations are based only on two interfaces at a time – one will be considered inside, one outside, based on Sec-level that is set
- Traffic on the ASA is allowed by default from a higher security level interface to a lower security level interface
- An ACL must explicitly permit traffic from a lower security level interface to a higher (e.g. outside to in)

Security Levels Configuration Example




```
hostname ciscoasa
!
interface GigabitEthernet0/0
 nameif outside
 security-level 0
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
!
```

Access Control Lists

Type	Description
Standard	Used for routing protocols, not firewall rules
Extended	Source/destination port and protocol
Ethertype	Used with transparent mode
Webtype	Used for clientless SSL VPN

- Like Cisco IOS, ACLs are processed from top down, sequentially with an implicit deny all at the bottom
- A criteria match will cause the ACL to be exited
- ACLs are made up of Access Control Entries (ACE)
- Remarks can be added per ACE or ACL
- ACLs can be enabled/disabled based on time ranges

Object Groups Simplify Configurations

```
(config)# object-group network ADMINS
(config-protocol)# description LAN Addresses
(config-protocol)# network-object host 10.1.1.4
(config-protocol)# network-object host 10.1.1.78
(config-protocol)# network-object host 10.1.1.34

(config)# object-group service RADIUS-GROUP udp
(config-service)# description RADIUS Group
(config-service)# port-object eq radius
(config-service)# port-object eq radius-acct

(config)#access-list RADIUS permit udp object ADMINS
host 10.100.1.200 eq object RADIUS-GROUP
```

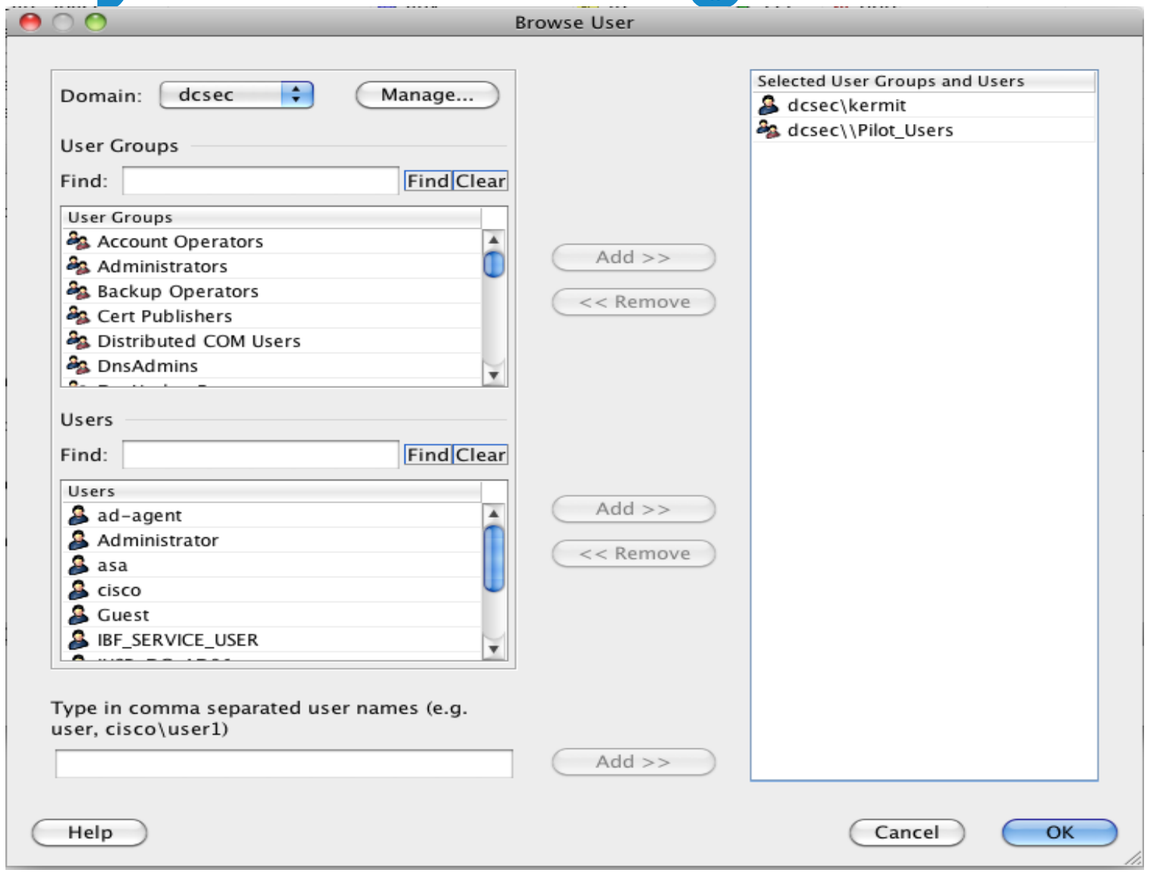
- Object groups allow grouping of similar items for easing configuration and operational maintenance of the ASA firewall
- Can be grouped by protocol, network or service
- Can be nested for more granular configuration options

ASA Global Policies

- Until recently, ACLs were applied to firewall interfaces for inbound and outbound traffic
- Release 8.3 and newer adds the ability to configure Global Access Policies which are not tied to a specific interface
- GA policies only affect traffic going through the firewall, not used with control-plane traffic
- Interface ACLs take priority over Global Access Policies
- All Access control policies now reference the real (pre-NAT) IP address

ASA 8.4.2+ Identity Firewalling

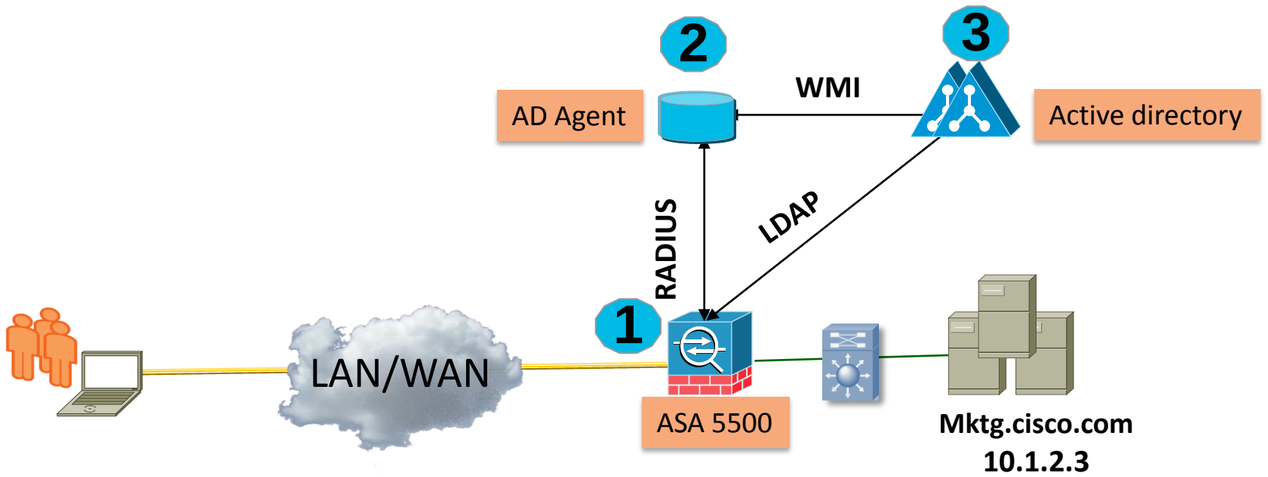
- 8.4.2> allows two new features: AD user and group import and FQDN in ACLs
- Requires use of an agent on a Windows server (Server 2003 or Server 2008)
- Can be built out for redundancy and scalability
- Not required to be installed on domain controller or on M0/0
- User and group info show in ACL logs (if enabled)



Global (8 rules)

1	☑	any		Cisco	HTTP-services	Permit			
2	☑	any	Cisco\\Marketing Cisco\sales-user	Youtube	HTTP-services	Permit	Info...		Marketing, and one of the sales people need access to Youtu.
3	☑	any		Youtube	HTTP-services	Deny			
4	☑	any	Cisco\\Administrators Cisco\\Employees	Facebook	HTTP-services	Permit	Info...		Allow only employees to visit Facebook
5	☑	any	Cisco\\Users	Facebook	HTTP-services	Deny			
6	☑	any		Twitter	HTTP-services	Deny			
7	☑	any		Web_server_group	HTTP-services	Permit			Allow everyone to get to the Web Servers from anywhere
8		any		any	ip	Deny			Implicit rule

How ID Firewall Works



① Cisco ASA 5500 Appliance
② Off-box AD Agent
③ AD Domain Controllers

Key Components

Roles of IDFW components:

ASA Firewall:
- Download AD group(s) from AD domain controller via LDAP protocol.
- Receive IP-user mappings from AD-Agent via Radius protocol.
- Report IP-user mappings from VPN/Cut-through-proxy to AD agent.
- Apply policies (ACL, MPF) based on user identity.

AD-Agent:
- Monitor AD domain controllers' security logs via WMI.
- Push IP-user mappings to ASA via Radius protocol.
- Receive IP-user mappings from ASA via Radius protocol.

AD domain controller:
- Authenticate users.
- Generate user logon security logs.
- Reply to ASA's LDAP query(s) for user/group information.

Deploying ID Firewall

- 3 Components to configure:
  1. AD Agent on Windows Server – does not have to be a Domain Controller
     - Must be member of Domain
  2. Active Directory
     - Account for LDAP connection
     - Domain Service
  3. ASA
     - RADIUS – AD Agent Connection
     - LDAP – AD Domain Connection
     - Access Rules may now use AD groups/users

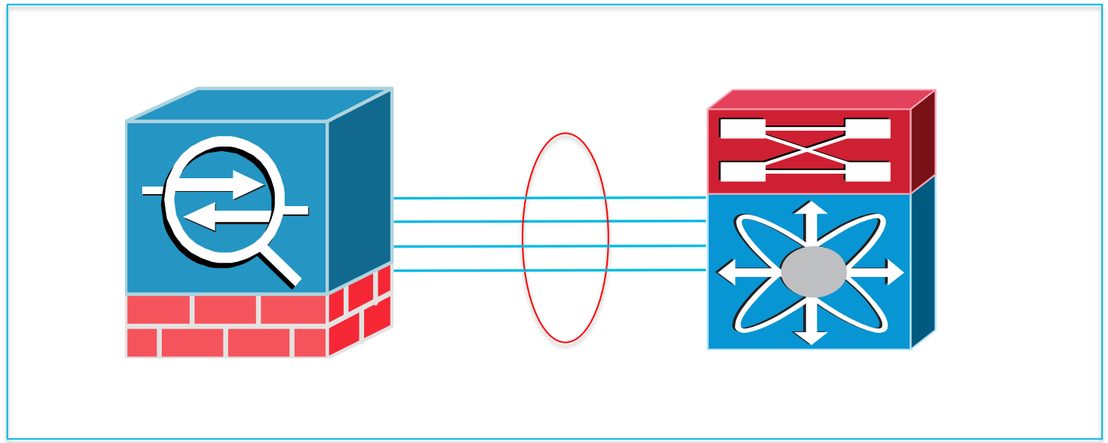
IDFW config guide

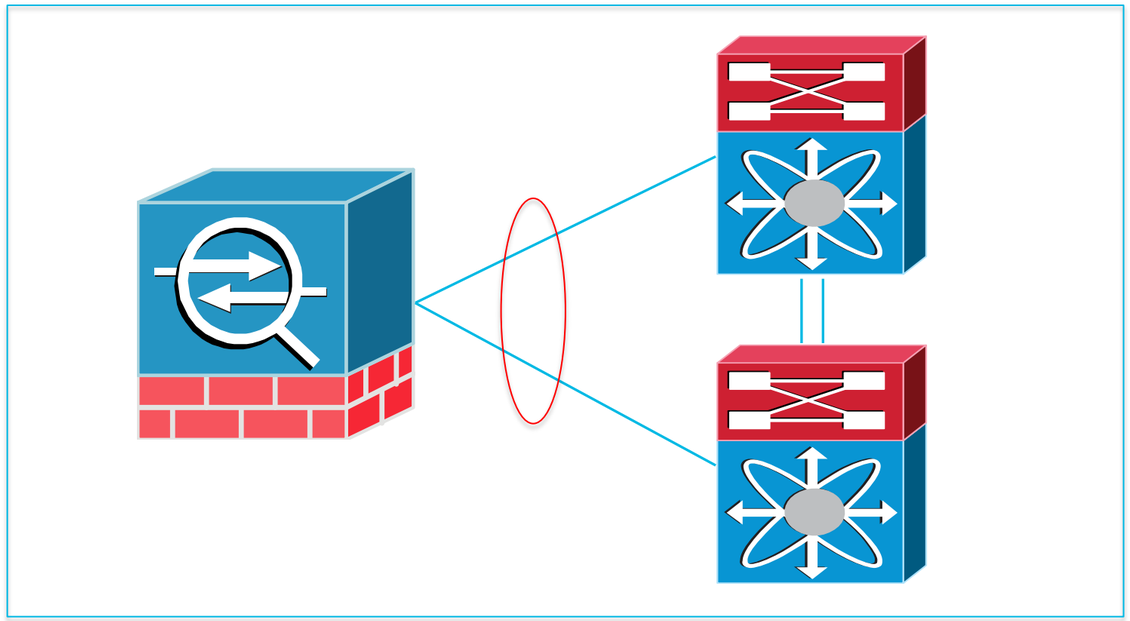
ASA 8.4 EtherChannel

What is an EtherChannel?

- Etherchannel allows up to 8 physical Ethernet links to be combined into one logical link (IEEE standard is 802.3ad)
- Ports must be of same capabilities: duplex, speed, etc.
- Benefits of EtherChannel are load-balancing and HA
- Originally these connections were between 2 switches or a server and a switch
- Virtual Port Channels (vPC) are the most recent version and allow multiple **devices** to share multiple interfaces
- vPC maximise throughput since each port channel is treated as a **single link** for spanning-tree purposes

EtherChannel on the ASA





- Supports 802.3ad and LACP standards
- Up to 8 active and 8 standby links
- Supported in all modes (transparent, routed, multi-context)
- Configurable hash algorithm (default is src/dest IP)
- Members share mac-addresses
- Not supported on 5505

ASA and Port Channel Best Practices

- ASA ECLB hashing algorithm and Nexus vPC hashing algorithm should be the same
- Redundant interface feature and ECLB on ASA are mutually exclusive
- Not supported on 4GE SSM (5540/50)
- Enable failover interface monitoring on ASA

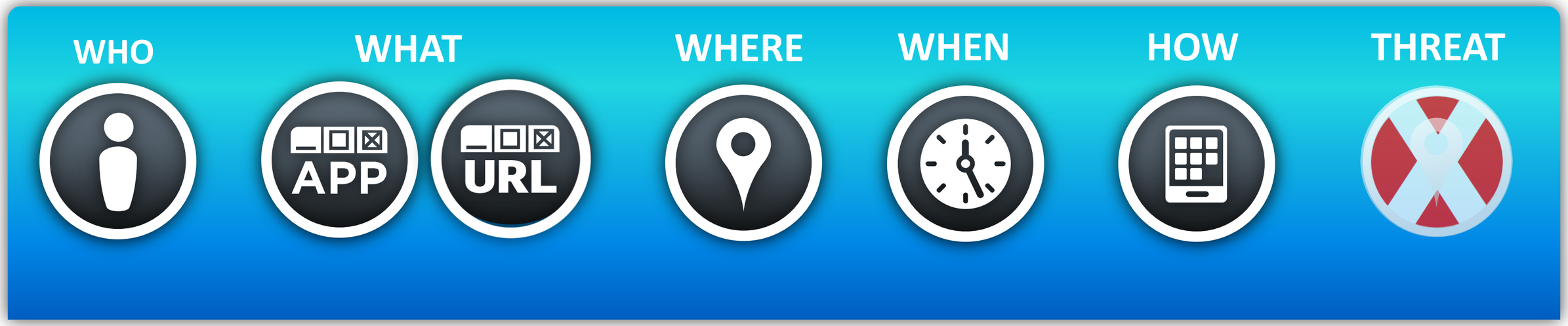
EtherChannel guide

ASA CX - Context Aware Firewall

Next Generation Firewall Capabilities

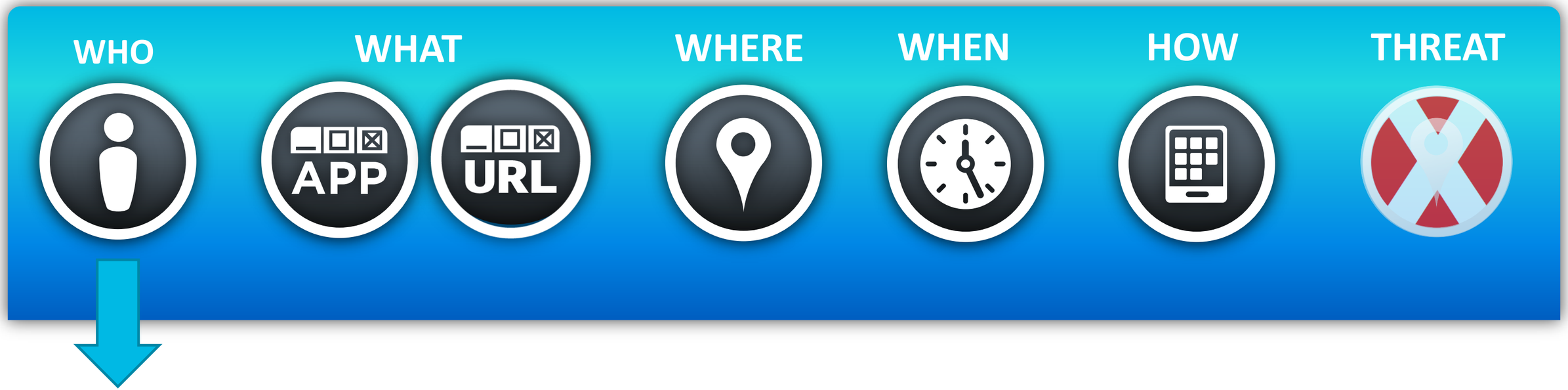
Next Generation Firewall - Cisco ASA CX

Complete Context Awareness Within Firewall Policy



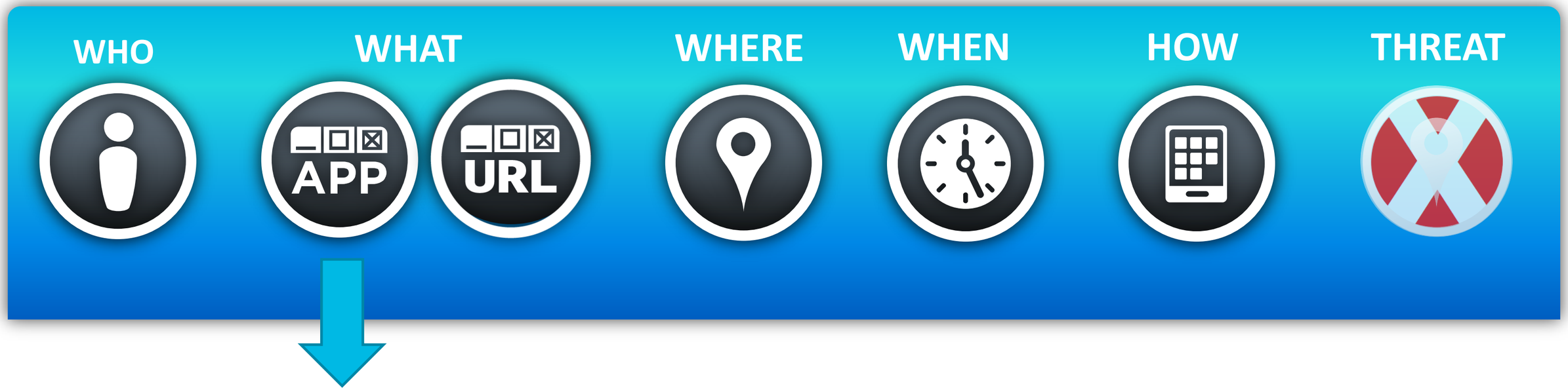
More on CX

Next Generation Firewall - Cisco ASA CX



- Rich User Identity Options
  - IP Surrogate AD Agent (also used with 8.4)
  - Agentless AD Directory integration for auth-aware applications (Kerberos/LDAP)
  - TrustSec Integration for Network Identity (Cisco ISE)

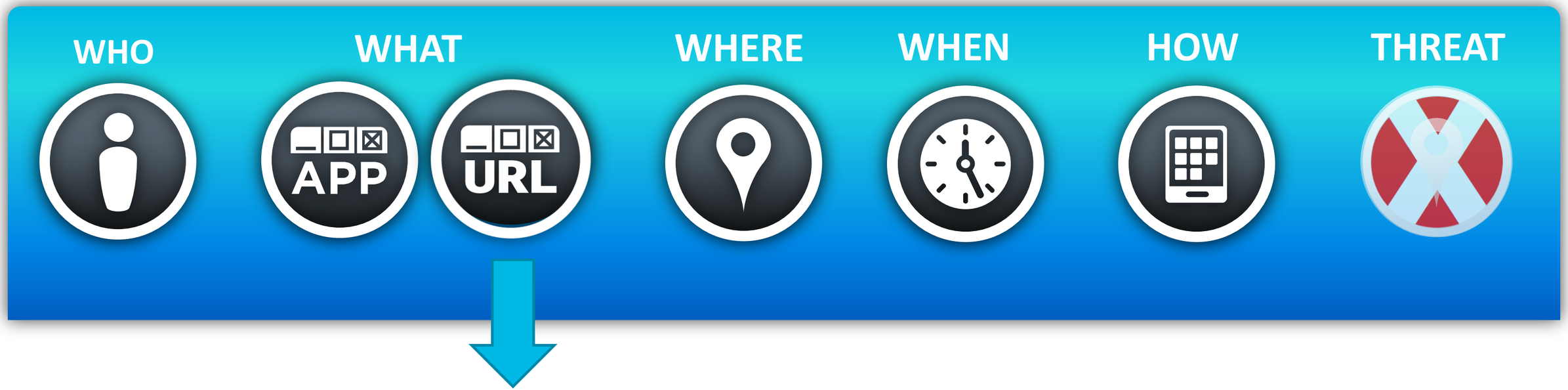
Next Generation Firewall - Cisco ASA CX



- Deep Application Visibility
  - Broad Application Classification of more than 1,100 apps (beyond port)
  - MicroApp Engine for deep classification of more than 75,000 application components
  - Behavioural application controls within MicroApp Engine manages individual behaviours

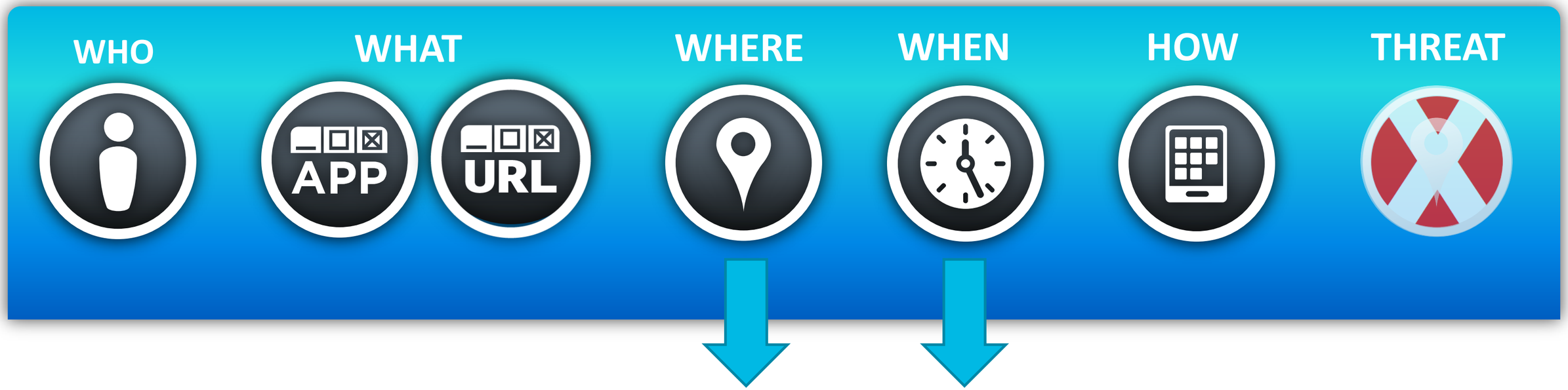
    i.e. Allow FaceBook for corporate users but do not allow Farm Ville or download

Next Generation Firewall - Cisco ASA CX



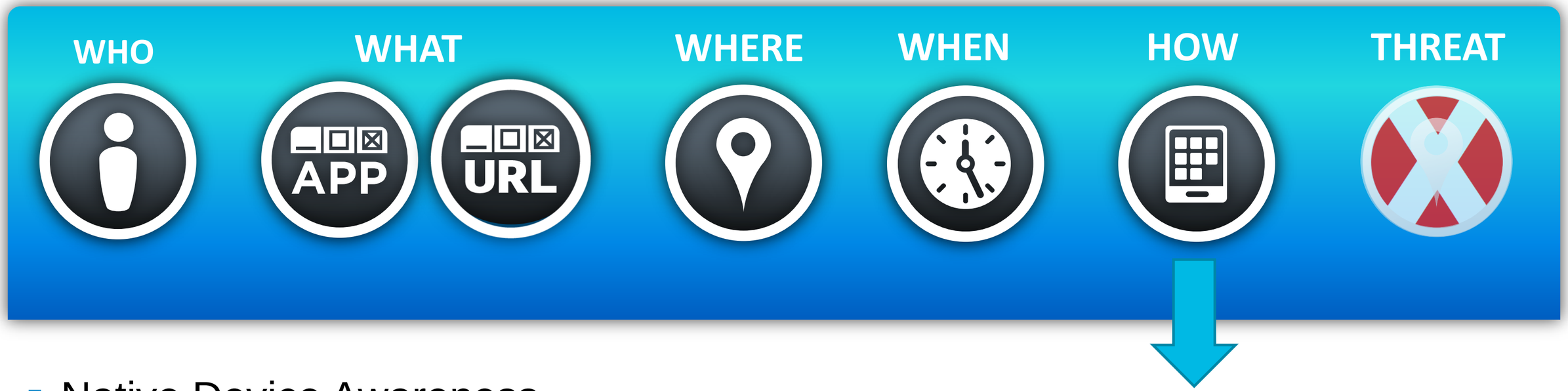
- Cisco-owned URL Database
  - Same URL database used by our Web Security products
  - 98% coverage of Web URLs in 200 countries across 60 languages in real-time (30B URLs/day)
  - 75 URL Categories with more than 200M URLs managed

Next Generation Firewall - Cisco ASA CX



- Per Transaction Location Awareness and Time-based policies
  - Blends contextual elements with traffic (GEO) source/destination for more accurate policy decisions
  - Integrates with Cisco Secure Mobility / BYOD components (AnyConnect) as well as differentiating local traffic
  - Allows policies to be adjusted dynamically at different times

Next Generation Firewall - Cisco ASA CX

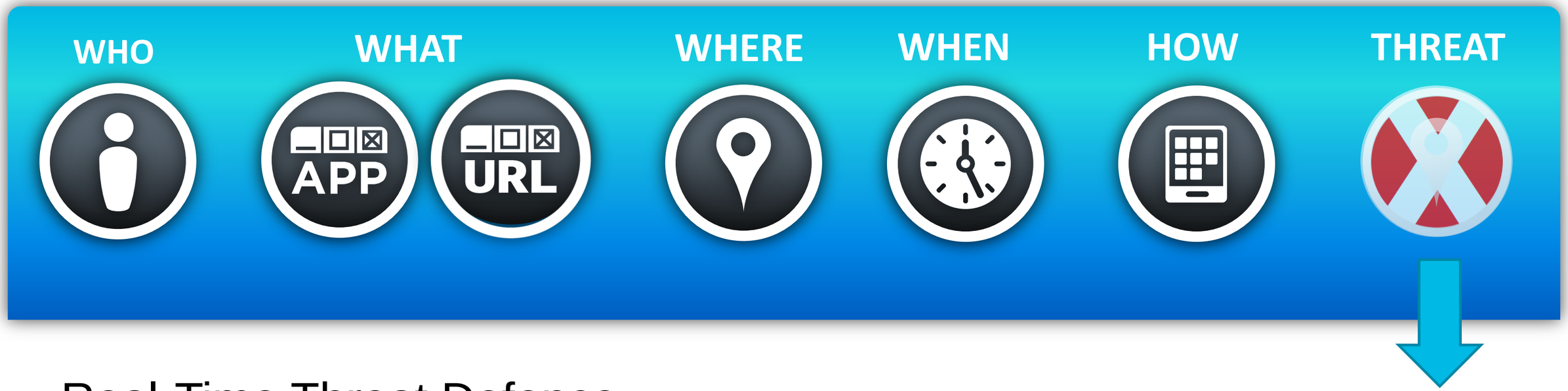


- Native Device Awareness
  - Allows Administrators to differentiate policies based upon device type

    i.e. iPad/Android versus PC-based, or access to financial app okay on PC not on iPad
  - Integrates with Cisco Secure Mobility / BYOD components (AnyConnect / ISE) as well as differentiating local traffic

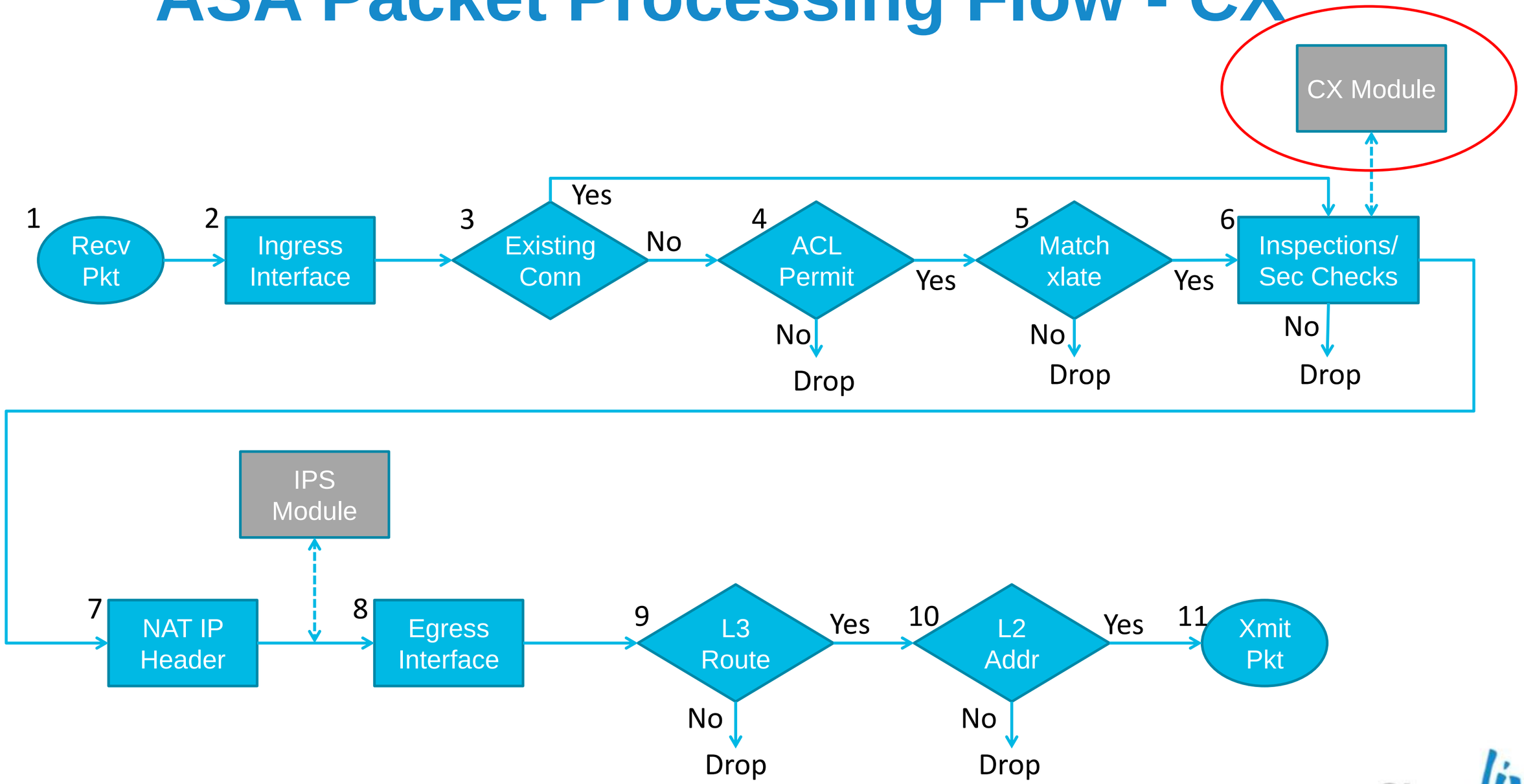
    In near future, ASA CX will leverage even richer information from ISE, like device profile, device posture, 802.1x authentication information, etc.

Next Generation Firewall - Cisco ASA CX



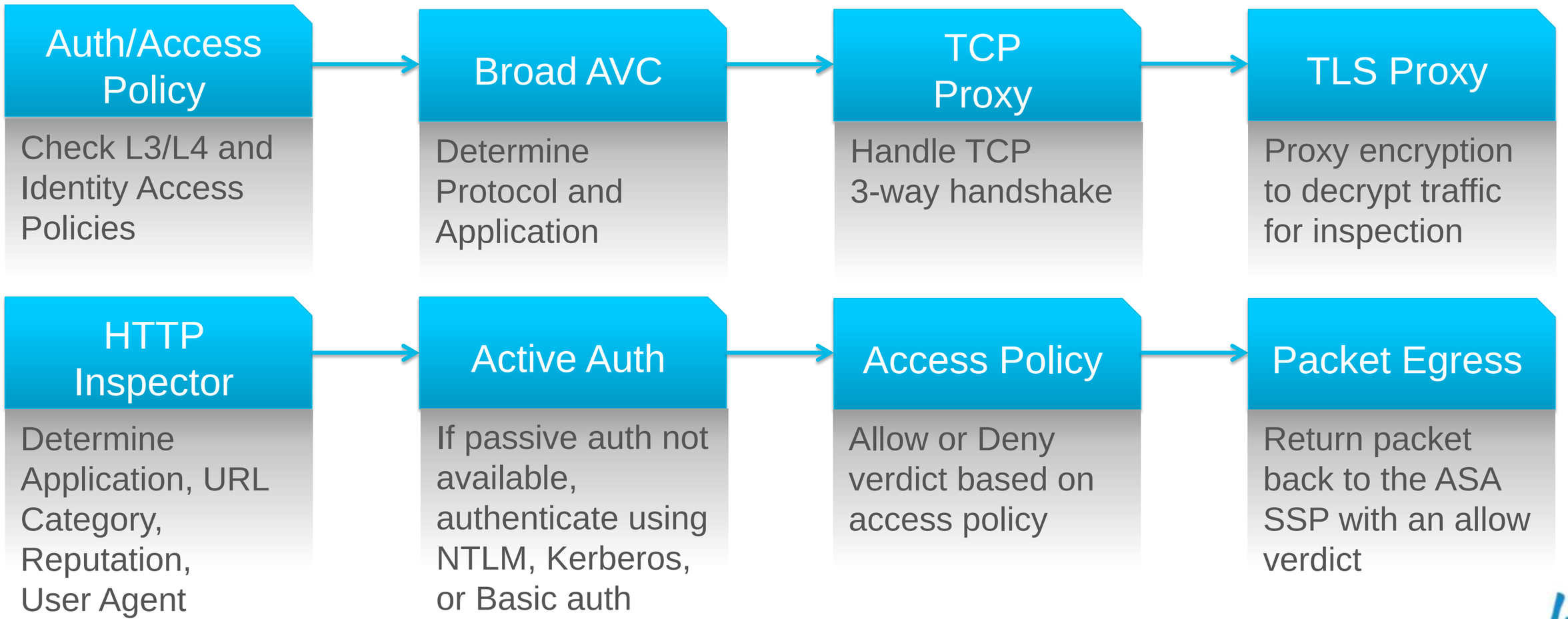
- Real-Time Threat Defence
  - Combines web reputation with context-awareness to enable safe access to applications
  - Web Reputation uses the world's largest threat analysis system, Cisco Security Intelligence Operations (CSIO), to block malicious transactions within genuine applications
  - Bi-directional Threat awareness prevents both infiltration and extrication defences

ASA Packet Processing Flow - CX



Day-in-the-life of a CX Packet

(One possible flow. May be different for other traffic.)



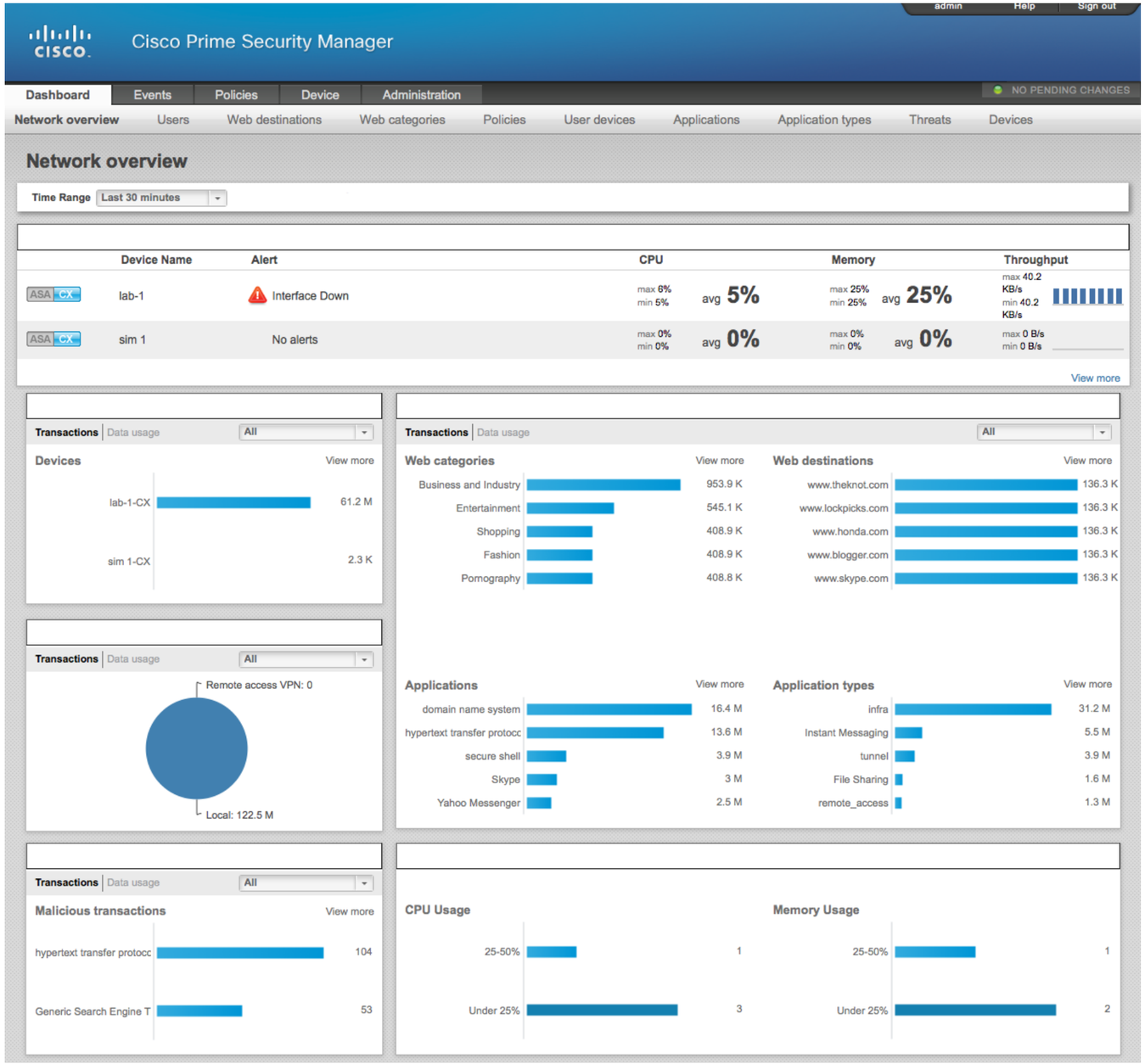
ASA CX Context Aware Firewall

- Traffic is redirected to CX module via ASA Service Policy

```
policy-map  global_policy
  class  class-default
     cxsc  fail-open  auth-proxy

service-policy  global_policy  global
```

CX Dashboard

- Provides real-time stats on all transactions, users, applications, devices, threats, etc.
- Uses a true ‘Web-Admin’ interface for management on any device
- Embedded and multi-device manager is included (Prime Security Manager)
  - Dynamically manages changes globally via REST XML

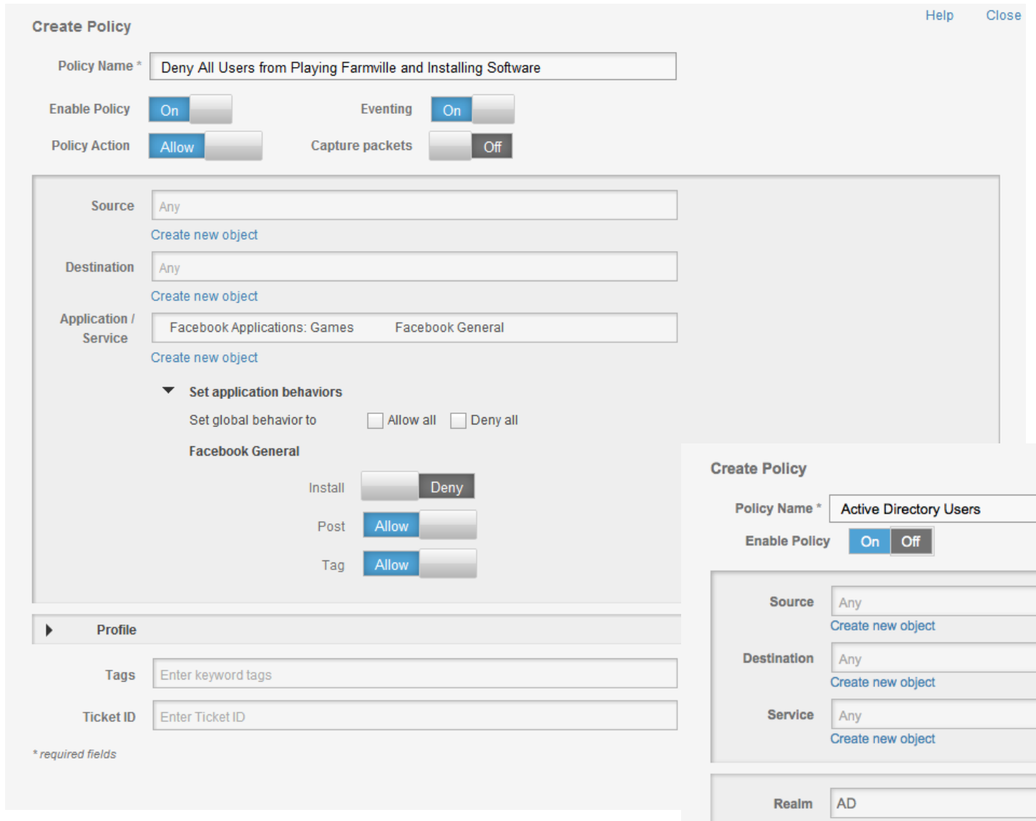


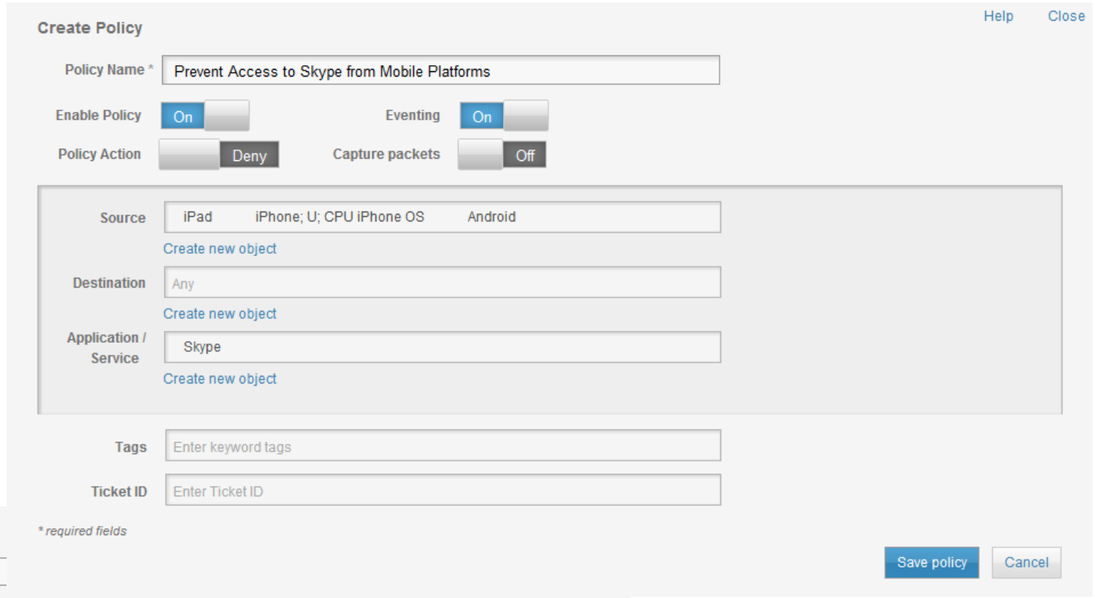
CX Policy Types

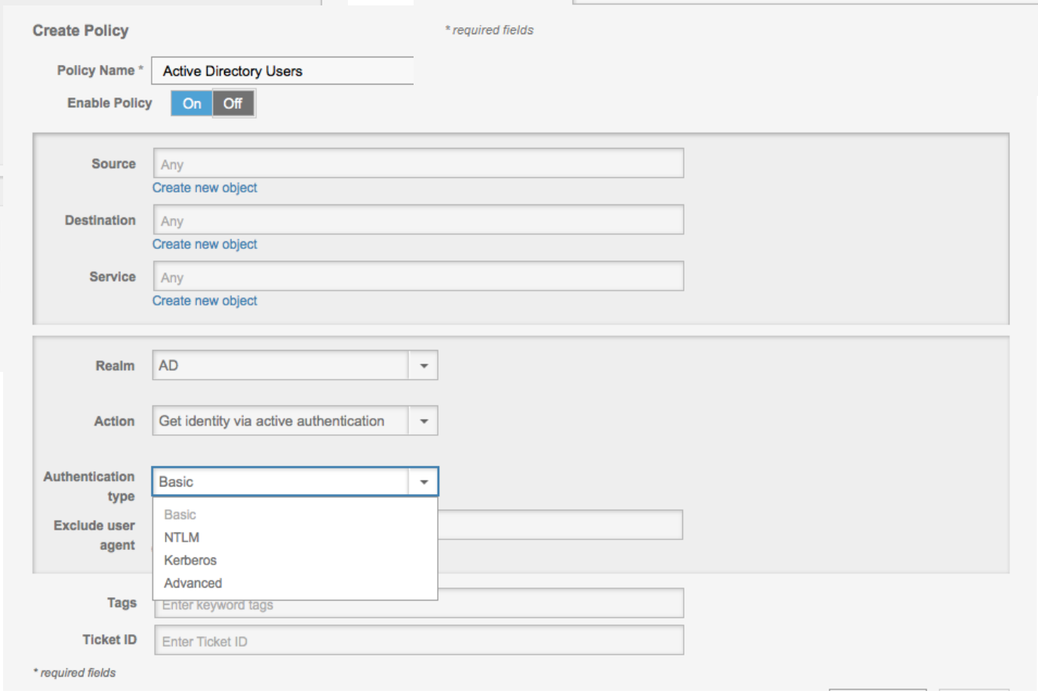
- Policies are processed in the following order:

Identity	• How to identify user?
Decryption	• What to decrypt?
Access	• Allow or Deny?

Example CX Policies



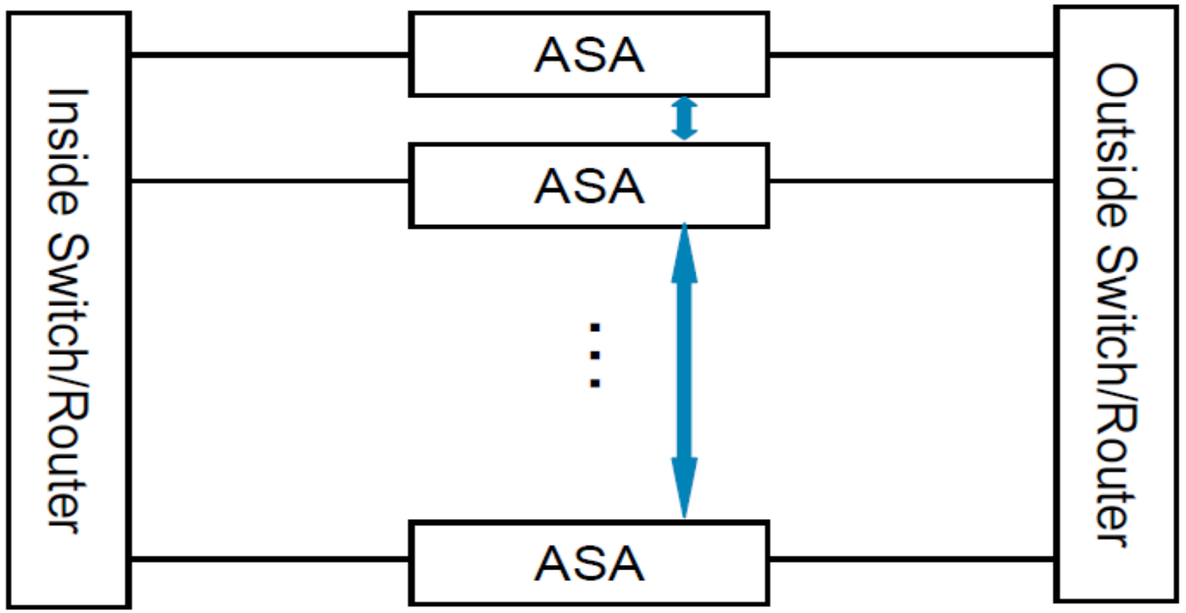




ASA 9.0

9.0 – Clustering

- Clustering = connecting multiple ASAs to form a single firewall, transparent to users and scaling in a sub-linear fashion
- Capable of handling heavy asymmetric flows without performance penalty



9.0 – Clustering (continued)

- Positioned for Data Centre environments scaling to more than 100 Gbps firewall
- The cluster can contain up to 8 ASA appliances
- One unit is designated as a Master and the rest are Slave units
  - Slave units are still processing data traffic
- A dedicated interface for Cluster Control Link (CCL)
  - Keepalive/CP/DP messages are sent over this link
- Can achieve a scaling factor of 0.7, assuming
  - N+1 redundancy
  - Using existing load balancing algorithms
  - Consistent hashing algorithm to redirect packets within cluster

9.0 – Clustering

Requirements

- Clustering is supported on all 5585-X and 5580 platforms
- All units within a cluster need to be of the same hardware type
- External switches/routers use stateless load-balancing
- Within cluster, proprietary protocol is used for connection load balancing

9.0 – Clustering

Modes of Operation

- The interfaces in a cluster of ASAs can be configured in either Layer-2 mode or Layer-3 mode
- Layer-2 mode:
  - ASA interfaces are grouped together in an Etherchannel bundle
  - Etherchannel – Aggregation of physical ethernet interfaces to form a logical ethernet link using Link Aggregation Control Protocol (LACP)
  - A switch uses Etherchannel load balancing mechanisms to send traffic between ASAs where all ASA units share a single system IP and system MAC, and appear as a single gateway in the network
- Layer-3 mode:
  - Each interface on the ASA has it's own IP address and MAC address
  - A router can use PBR (Policy Based Routing) or ECMP (Equal Cost MultiPath routing) to balance traffic between ASAs.

9.0 – Multiple-Context Mode Enhancements

Dynamic Routing

- OSPFv2 and EIGRP are supported in Multiple-Context mode
  - No support for OSPFv3, RIP, or PIM
  - Routed mode only
  - 2 instances of OSPFv2 and 1 instance of EIGRP per user context
  - No inter-context peering through a shared interface
- Per-context route limit is configurable from system context
  - Over-resource-limit routes are rejected when installing into RIB
  - Syslog appears in the admin context
    %ASA-5-321001: Resource 'routes' limit of 5000 reached for context ‘ctx2’

9.0 – Multiple-Context Mode Enhancements

VPN Support

- Full Site-to-Site VPN support in Multiple-Context mode
- No Remote Access or SSL VPN
- Some commands/features remain in the system context
  - crypto isakmp reload-wait
  - crypto engine large-mod-accel
  - Fips
  - License allocation (configured using class)
- Global “show” command for the VPN accelerator are in admin context

9.0 – IPv6 Enhancements:

- Mixed IPv4/IPv6 Object Groups
- Unified ACLs with Configuration Migration
- NAT64, NAT46, NAT66 with DNS Rewrite
- DHCPv6 Relay
- OSPFv3
- IPv6 Application Inspection
- IPv6 SSL VPN and Anyconnect Addressing

9.0 – Core Infrastructure Enhancements:

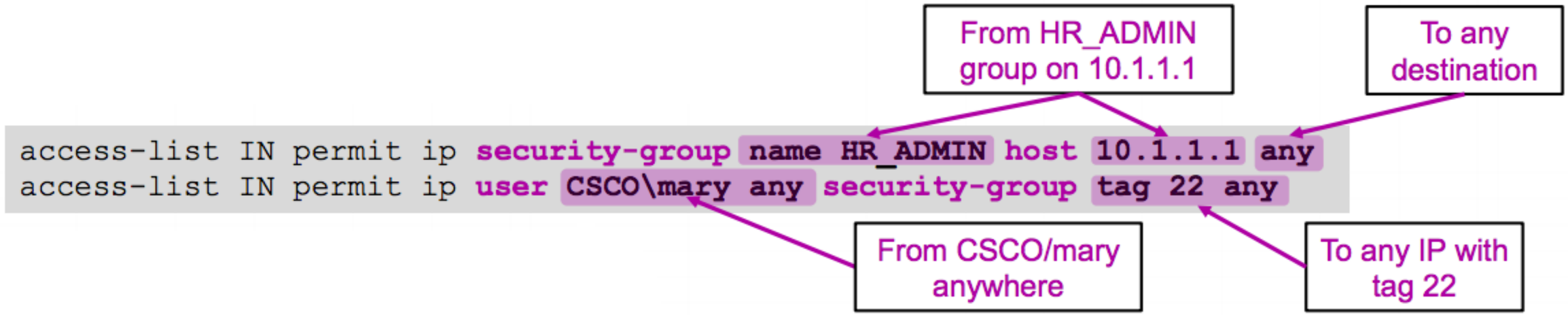
- Feature parity between ASASM and appliances
  - VPN and Unified Communications, per-context firewall mode
- ICMP code support in ACLs and Objects
- Maximum configurable MPF connection limits increased to 2M
- ASA 8.6(1) and partial 8.4(4.1) feature support
  - 5500-X IPS, CX, TCP Reset on inspection, SunRPC pinholes, SSL VPN Rewriter
  - (Common Criteria and ASA5585-X interface expansion cards are not supported)

9.0 – Cloud Web Security (Scansafe Connector)

- Cloud-based HTTP/HTTPS Content Scanning solution
  - Original request redirected to ScanSafe cloud via a destination rewrite
  - ASA supplies pre-NAT IP and other information
  - Policy management and license download is done from the ScanSafe portal
- Significant performance advantages over legacy URL Filtering and CSC
- Traffic redirection is applied in MPF with **inspect scansafe** action
- ASA can supply AD User Identity to ScanSafe cloud

9.0 – Trustsec

- ASA supports SXP to learn IP ⇔ SGT bindings (no in-line frame tagging)
- Name ⇔ SGT mappings downloaded from ISE
- Then SGT and group names can be used in ACLs
  - IP information is required (could be any)
  - Names need to resolve to tags first



9.0 – VPN Enhancements:

- VPN infrastructure enhancements
  - SSL VPN Multi-Core Performance
  - NSA Suite B
  - IPSECv3
  - Anyconnect Custom Attributes

9.0 – VPN Enhancements (continued):

- Clientless SSLVPN enhancements
  - Rewriter Enhancements (Microsoft SharePoint 2010)
  - Auto Signon enahncements
  - Server Certificate Validation
  - Citrix Mobile Receiver
  - Java File Browser
  - Java Rewriter Proxy
  - HTML5

Q & A

Complete Your Online Session Evaluation

Give us your feedback and receive a Cisco Live 2013 Polo Shirt!

Complete your Overall Event Survey and 5 Session Evaluations.

- Directly from your mobile device on the Cisco Live Mobile App
- By visiting the Cisco Live Mobile Site www.ciscoliveaustralia.com/mobile
- Visit any Cisco Live Internet Station located throughout the venue

Polo Shirts can be collected in the World of Solutions on Friday 8 March 12:00pm-2:00pm

Cisco live! 365

Don’t forget to activate your Cisco Live 365 account for access to all session material, communities, and on-demand and live activities throughout the year. Log into your Cisco Live portal and click the "Enter Cisco Live 365" button.
www.ciscoliveaustralia.com/portal/login.ww

Cisco live!

Appendix

Firewall High Availability

HA Feature – Interface Redundancy

- Up to 8 redundant interface pairs are allowed
- Compatible with all firewall modes (routed/transparent and single/multiple) and all HA deployments (A/A and A/S)
- When the active physical interface fails, traffic fails to the standby physical interface and routing adjacencies, connection, and auth state won't need to be relearned
- NOT supported on ASA 5505, FWSM or ASA-SM

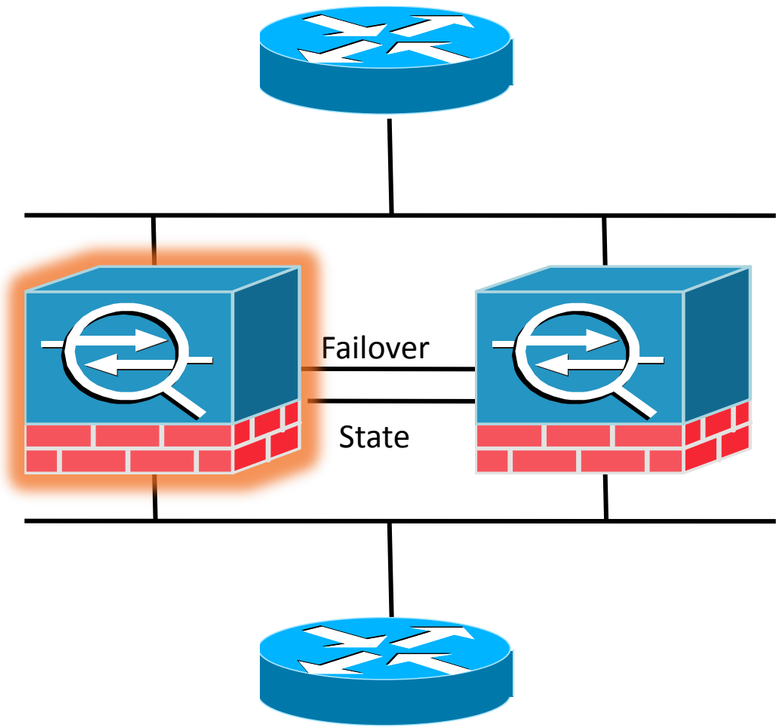
```
interface Redundant1
 member-interface GigabitEthernet0/2
 member-interface GigabitEthernet0/1
 no nameif
 no security-level
 no ip address
!
interface Redundant1.4
 vlan 4
 nameif inside
 security-level 100
 ip address 172.16.10.1 255.255.255.0
!
interface Redundant1.10
 vlan 10
 nameif outside
 security-level 0
 ip address 172.16.50.10 255.255.255.0
```

HA Feature – Route Tracking

- Method for tracking the availability of static routes with the ability to install a backup route should the primary route fail
- Commonly used for static default routes, often in a dual ISP environment
- Uses ICMP echo replies to monitor the availability of a target host, usually the next hop gateway
- Can only be used in single routed mode

```
asa(config)# sla monitor 123
asa(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1
  interface outside
asa(config-sla-monitor-echo)# frequency 3
asa(config)# sla monitor 123 life forever start-time now
asa(config)# track 1 rtr 123 reachability
asa(config)# route outside 0.0.0.0 0.0.0.0 10.1.1.1 track 1
```

Firewall HA - Active/Standby



- Supported on all models including ASA 5505**
- Requires an additional “Plus” license (5505 and 5510 only)
- ASA only supports LAN Based failover (no serial cable).
- Both platforms must be identical in software, licensing, memory and interfaces (including SSM modules)
- Same mode (i.e. routed or transparent)
- Not recommended to share the state and failover link, use a dedicated link for each if possible

**ASA 5505 does not support stateful failover, only stateless

How Failover Works

- Failover link passes Hellos between active and standby units every 15 seconds (tunable from 3-15 seconds)
- After three missed hellos, primary unit sends hellos over all interfaces to check health of its peer
- Whether a failover occurs depends on the responses received
- Interfaces can be prioritised by specifically monitoring them for responses
- If the failed interface threshold is reached then a failover occurs
- For more details refer to the Configuration Guide:
  http://www.cisco.com/en/US/docs/security/asa/asa82/configuration/guide/ha_overview.html

What Does Stateful Failover Mean?

State Info Passed to Standby	Things NOT Passed to Standby
NAT Translation Table	User authentication table
TCP connection states	Routing table information **
UDP connection states	State information for SSMs (IPS etc.)
ARP Table	DHCP Server Leases
L2 Bridge Table (Transparent Mode)	Stateful failover for phone proxy
HTTP State *	
ISAKMP and IPSEC SA Table	

* HTTP State is not passed by default for performance reasons; enable via `'http replication state'`

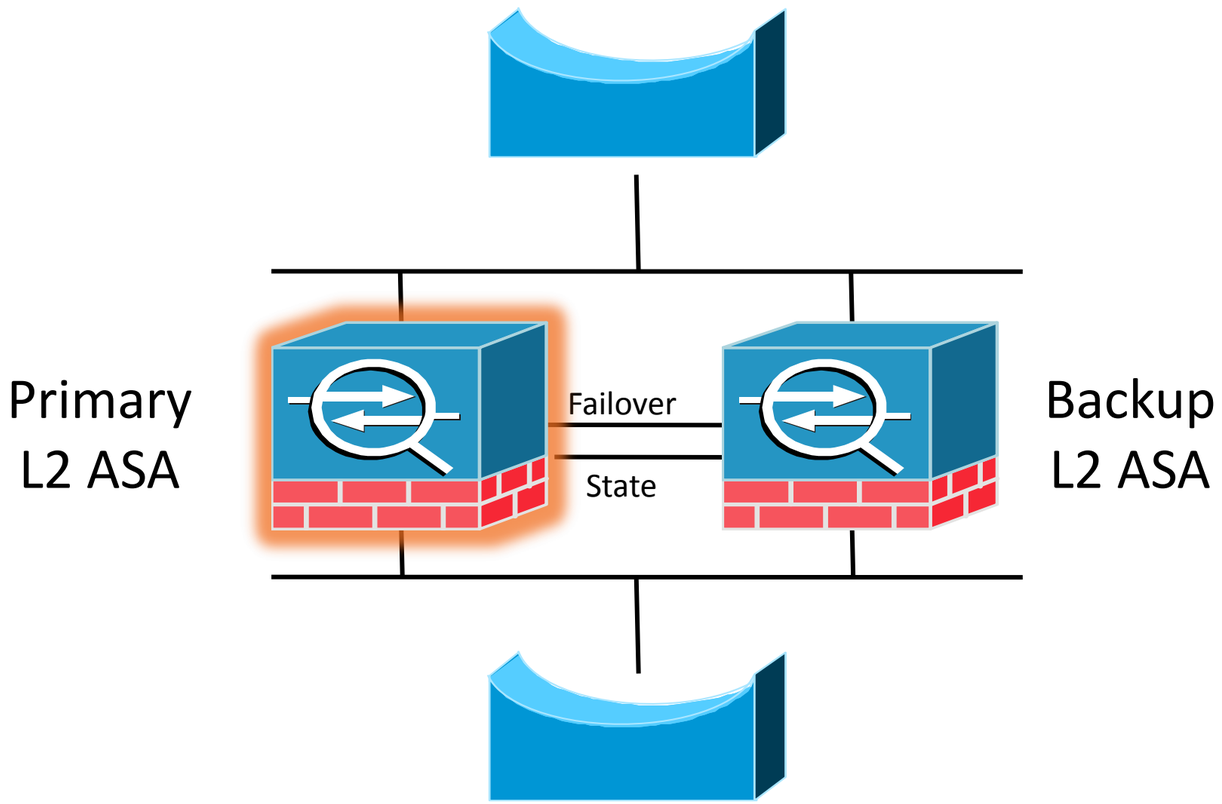
** 8.4.x> does this by default

Failover Best Practices

- In years past, the PIX firewall used a serial cable (RS-232) for failover
- The ASA uses dedicated ports for failover and failover ports will NOT pass traffic
- Recommended to use separate connections for failover and state if stateful failover is required*
- Connection can either be via X-over cable or cabled into a switch in a dedicated VLAN (ASA supports Auto MDI/MDIX)
- Long distance LAN failover is supported if latency is less than 10ms and no more than 250ms
- IPv6 HA supported since 8.2.2

* With 8.4.2 it's now possible to port-channel multiple physical links, but note that only one of the channels will be forwarding. Reference the 8.4 Configuration Guide for details.

Firewall HA – Transparent Mode

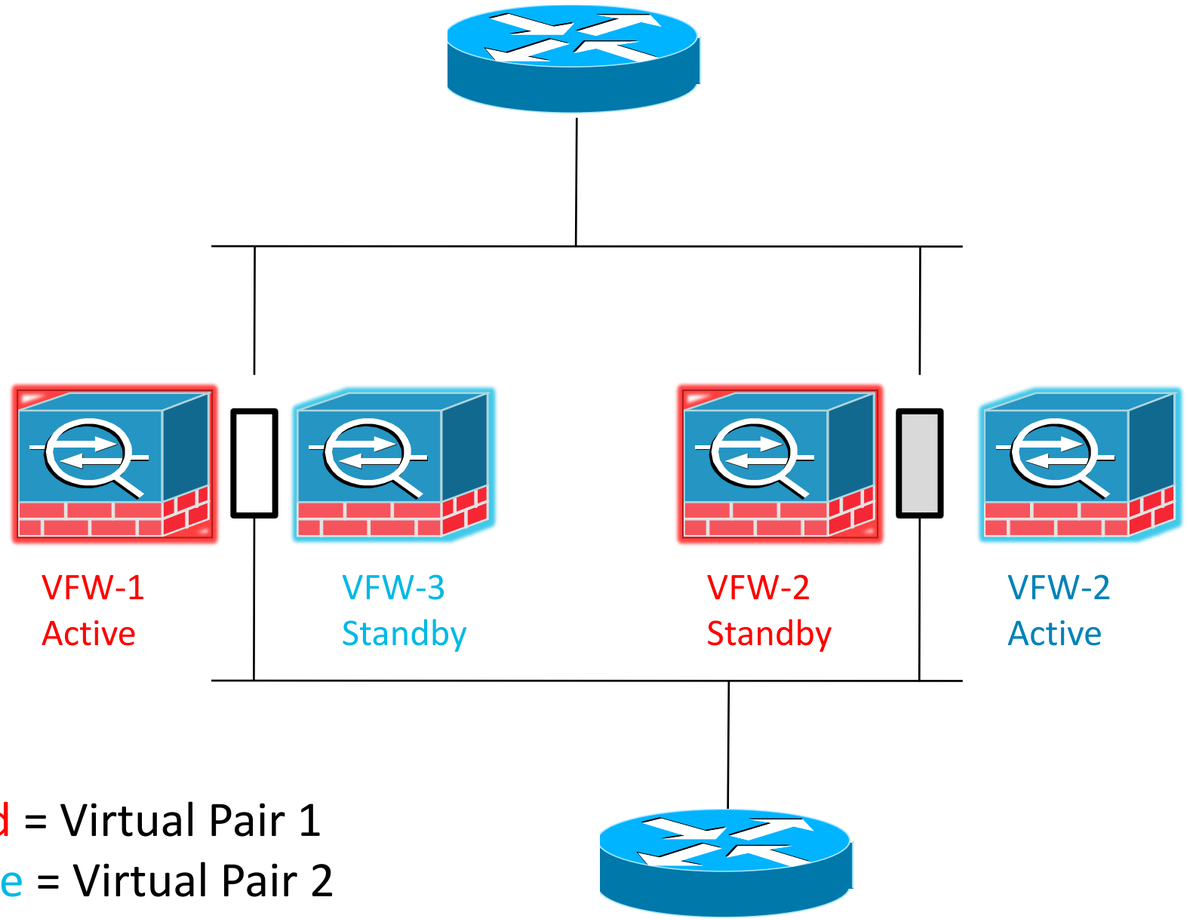


- Transparent Firewall can run in A/S or A/A mode
- Since the firewall acts like a switch, Spanning Tree is recommended to control BPDU forwarding
- Care should be taken to ensure that STP root is as intended
- Ensure that topology is free of all loops!

A/S Failover in Transparent Mode

- Mandatory that no loops in network topology!
- Switches connected to HA firewalls should be configured for STP, understand the implications
- Use RPVST (802.1w) and Port Fast feature on switches where possible
- No BPDU Guard or Loop Guard on ports connecting to firewalls
- Use caution if deploying transparent firewalls in Active/Active mode because BPDUs are forwarded by default
- TAC Podcast on Transparent Firewall: http://www.cisco.com/en/US/solutions/ns170/tac/security_tac_podcasts.html

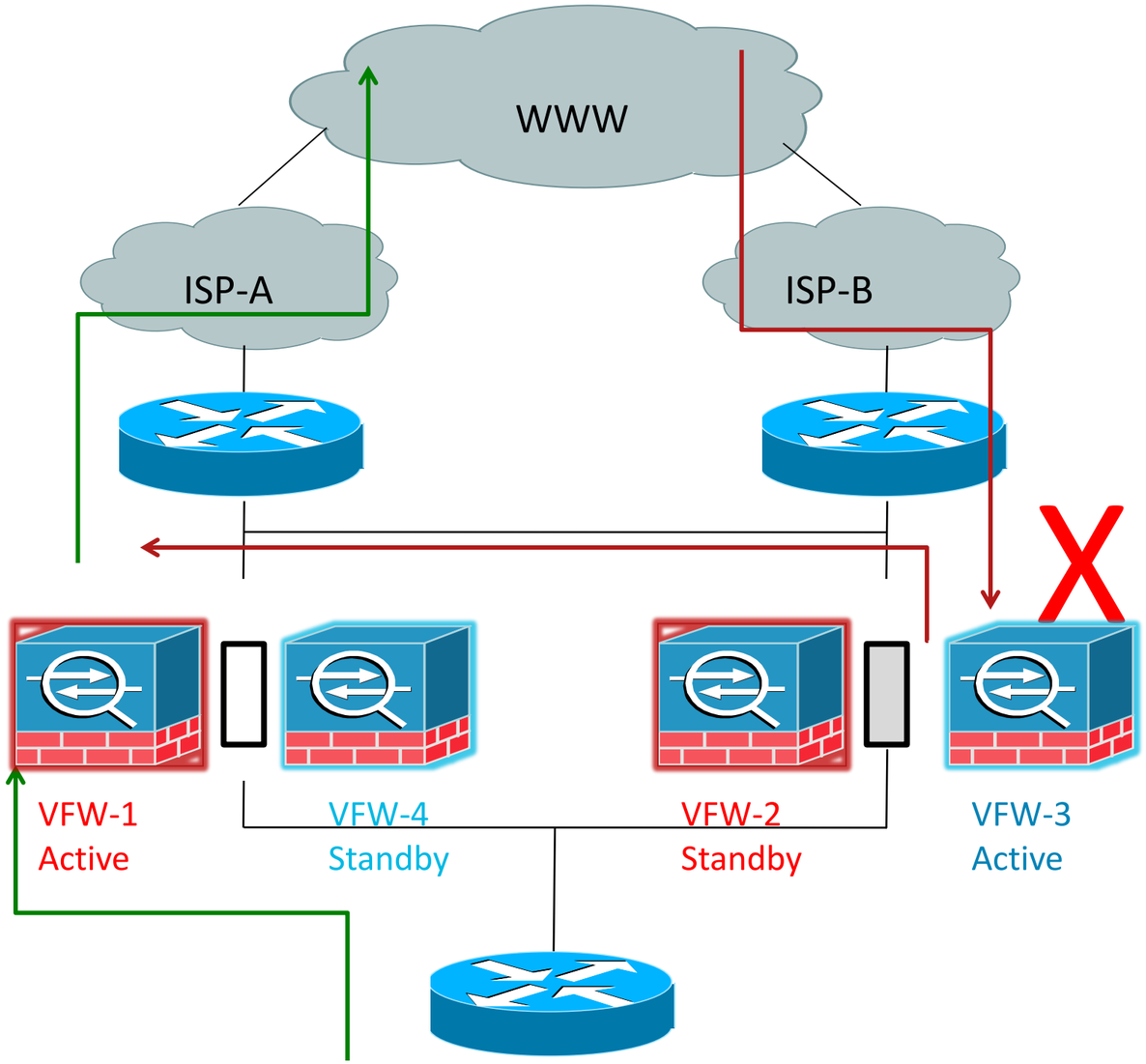
Firewall HA: Active/Active Failover



Red = Virtual Pair 1
Blue = Virtual Pair 2

- Supported on all platforms except the 5505
- Requires an additional “Plus” license (5510 only)
- Requires virtualisation which requires additional licensing
- Virtualisation does not support VPN, multicast or routing protocols
- No load-balancing or load-sharing support today

Firewall HA: A/A Failover with Asymmetric Routing Support



- ASR mode adds support for asymmetric traffic flows through an A/A system
- A/A ASR is enabled by adding multiple A/A units to the same ASR Group
- When traffic is received on VFW-3 it has no entry in state table and therefore checks state information of other interfaces in ASR Group
- If no match, packet is dropped
- If matched, then rewrite L2 header and forward to other active firewall (VFW-1)
- VFWs in same ASR group must be L2 adjacent

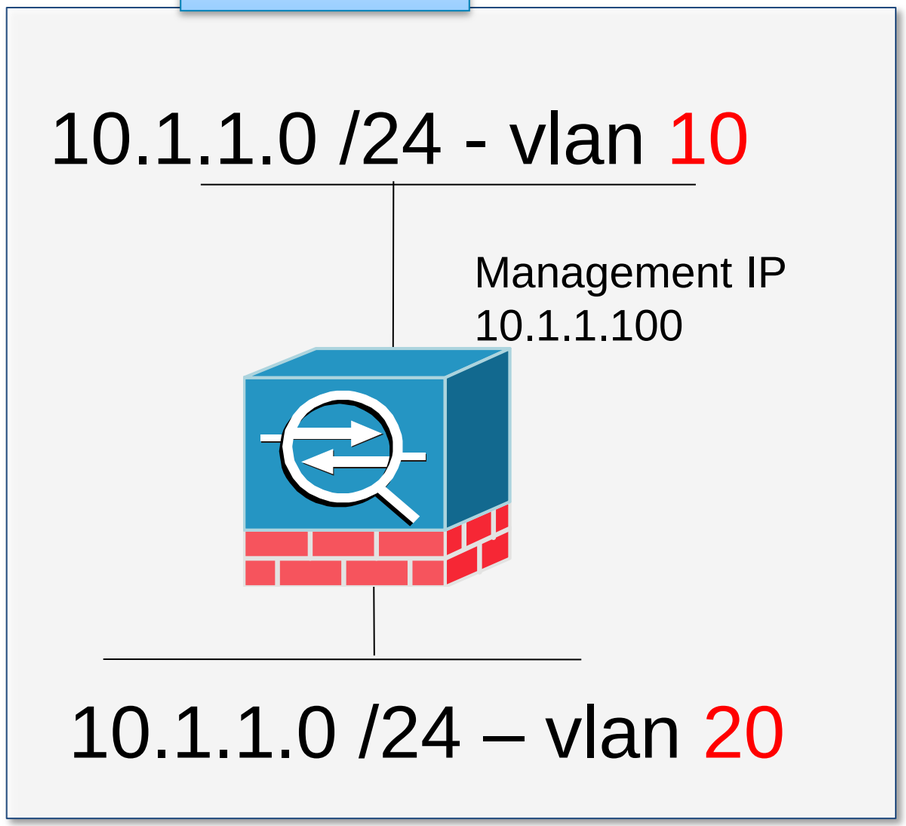
Limitations of Active/Active Failover

- Need to guarantee a low-latency state sharing between two A/A firewalls to avoid a race condition if a return connection arrives prior to state information being received
- Shared interface setup requires NAT
- HTTP state information is NOT shared by default and must be explicitly configured
- Layer 2 adjacency is required between the physical ASAs in an ASR-group
- Multi-context ASA does not support VPN, multicast routing or dynamic routing protocols

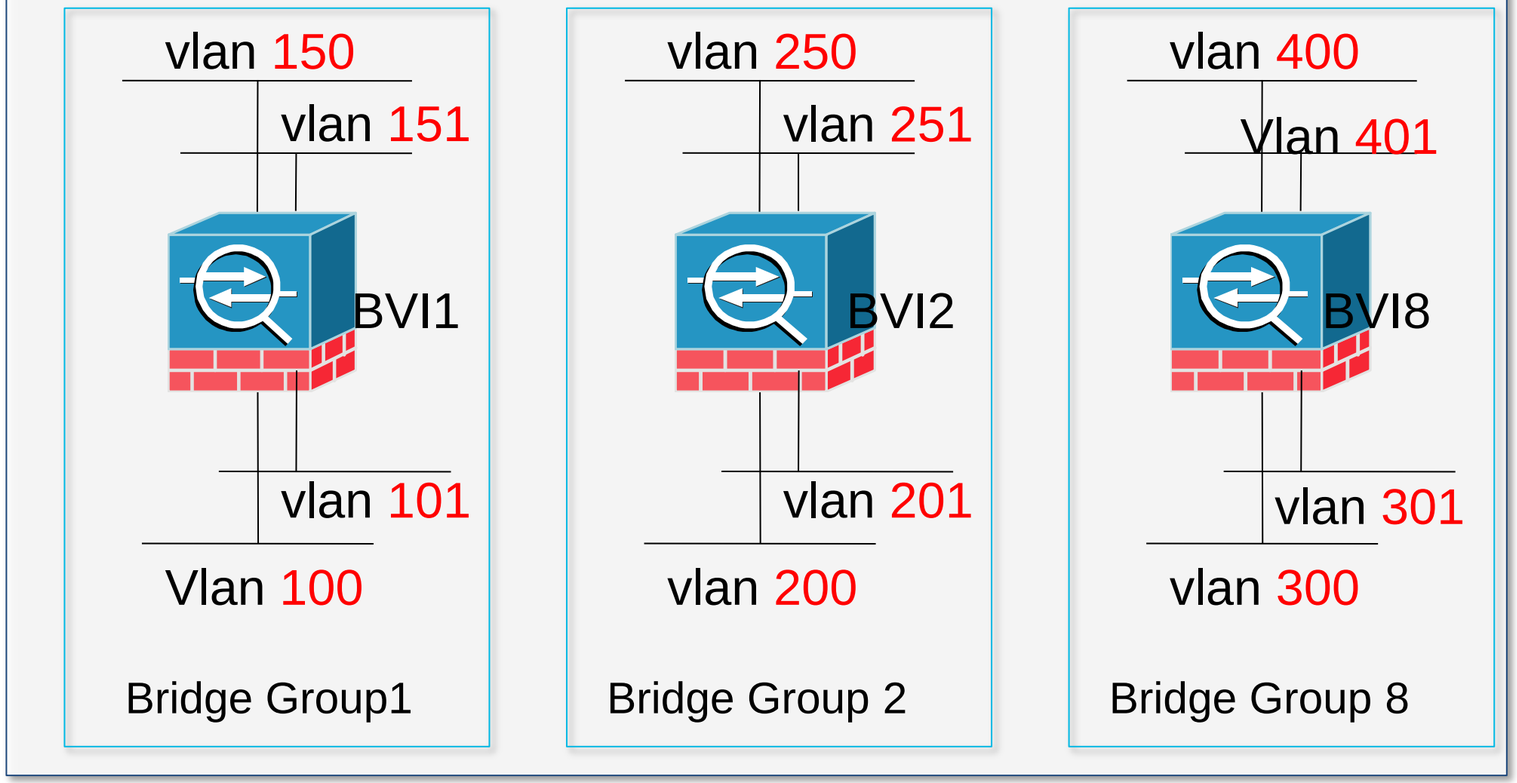
ASA 8.4 Bridge Groups

Bridge Group in ASA 8.4

Pre-8.4



8.4.



- Up to 4 VLANs per bridge-group
- 8 bridge-groups per firewall or security context (vFW)

Bridge Group Considerations

- External L3 device required to route between bridge groups
- (virtual) Interfaces can not be shared across bridge groups
- BVI must have an IP address
- Same MAC can exist on two or more **different** bridge groups (LB, HSRP, SVI environments)
- Pre 8.4 (transparent) configurations will be migrated to BVI configuration

Configuration Example: ASA 8.3 vs. ASA 8.4

Transparent Firewall ASA 8.3 and Earlier

```
firewall transparent

interface GigabitEthernet 0/0
    nameif inside
    security-level 100

interface GigabitEthernet 0/1
    nameif outside
    security-level 0

    ip address 10.10.10.100 255.255.255.0
```

Transparent Firewall ASA 8.4

```
firewall transparent
interface GigabitEthernet 0/0
    nameif inside
    security 100
    bridge-group 1

interface GigabitEthernet 0/1
    nameif outside
    security 0
    bridge-group 1

interface GigabitEthernet 0/2
    nameif dmz
    security 50
    bridge-group 1

interface GigabitEthernet 0/3
    nameif inside
    security 51
    bridge-group 1

interface BVI 1
    Ip address 10.10.10.100 255.255.255.0
```