
TOMORROW
starts here.
CISCO
Cisco live!

Firewall Architectures in the Data Centre and Internet Edge

BRKSEC-2021

Goran Saradzic

Technical Marketing Engineer

#clmel

Cisco live!


ASAv
ASA5585-X
Clustering
ACI Security Solution
Goran Saradzic

Session Objectives and Housekeeping

BRKSEC-2021 session is based upon an actual use-case of a fictional company that requires the deployment of a complete Firewall Solution project using Cisco Best Practices

The session concludes with a review of advanced ASA deployment scenarios and summary.

At the end of the session, you should have:

- Knowledge of common firewall deployment scenarios, including edge, data centre, firewall virtualisation, HA, etc., using latest code (9.x)
- "Best Practice" suggestions for optimising your firewall deployment using Cisco validated designs and vigorously tested configurations (CVD Testing / Engineering)
- Note: Session will NOT cover FirePower Services, NGFW, NGIPS, VPN, IOS Firewall, FWSM or **Pricing**
- Note: Session does not cover IPv6 deployment
- **Speed through repetitive configurations – to allow more time for Technology**

Related Sessions

- BRKSEC – 2028 – Deploying Next Generation Firewall with ASA and FirePOWER Services
- BRKSEC – 3032 – Advanced - ASA Clustering Deep Dive
- BRKSEC – 3021 – Maximising Firewall Performance
- BRKSEC – 3020 – Troubleshooting ASA Firewalls
- BRKSEC – 3033 – Advanced AnyConnect Deployment and Troubleshooting with ASA
- LABSEC – 1004 – REST Agent self paced lab (version 9.3.(2))

Agenda

- Use Case Introduction
- Initial ASA Firewall Setup
- Firewall Deployment Modes
- L3 Firewall at the Edge
- L2 Firewall in the Data Centre
- L3 Firewall in the Compute
- Advanced ASA Deployments
- Conclusion

The ASA Product Family

Cisco live!

Cisco Firewall – What is it?

- Adaptive Security Appliance (ASA) – hardened firewall appliance, proprietary OS, Ethernet and fibre ports on box. (1G/10G)
  - Does not run IOS but CLI has a similar look and feel
  - All management can also be completed with GUI (on-box or multi-manager)
- ASA SM – Next Gen line card for Catalyst 6500, no physical interfaces, runs ASA code image
- Adaptive Security Virtual Appliance Firewall (ASAv) – Virtualisation-based ASA that runs with a full ASA code base, not dependent upon Nexus1000v
- ASA with FirePOWER Services – ASA firewall appliance which integrates a full installation of FirePOWER NGFW, NGIPS, AMP and Contextual Services
- VSG – Virtual Security Gateway – Zone-based Virtual firewall dependent upon Nexus1000v Switch – mentioned but not detailed in this session
- Meraki MX- Security appliance that implements security for users of the Meraki cloud. Not covered in this session

Cisco ASA Firewalls

Multiservice 64-bit
(FW + VPN + NGFW + NGIPS + Context)

ASA Cluster 2-16x
(320-640Gbps, 2.8M CPS, 96M conns)
(>100Gbps NGIPS/NGFW)

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

ASA 5585-X SSP40
(10-20 Gbps, 240K conn/s
6Gb NGFW/NGIPS, 10K VPN)

ASA 5585-X SSP20
(5-10 Gbps, 125K conn/s
3.5Gb NGFW/NGIPS, 5K VPN)

ASA 5585-X SSP10
(2-4 Gbps, 75K conn/s
2Gb NGFW/NGIPS, 5K VPN)

ASA SM (6K)
(16-20 Gbps,300K conn/s)

ASA 5506/08-X
(1-1.2Gbps, 15K conn/s)
(300 Mb NGFW/NGIPS)

ASA 5512/15-X
(1-1.2Gbps, 15K conn/s)
(300 Mb NGFW/NGIPS)

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

ASA 5525-X
(1-2Gbps, 20K conn/s)
(650 Mb NGFW/NGIPS)

ASA 5545-X
(1-3Gbps, 30K conn/s)
(1Gb NGFW/NGIPS)

ASA 5555-X
(2-4Gbps, 50K conn/s)
(1.25Gb NGFW/NGIPS)

Service Modules

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

VSG

Virtual ASA
(1-2Gbps, 60K cps, VPN)

Virtualisation

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

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

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

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

Legacy Multi-Service: FW+VPN+IPS **FW + VPN Only**

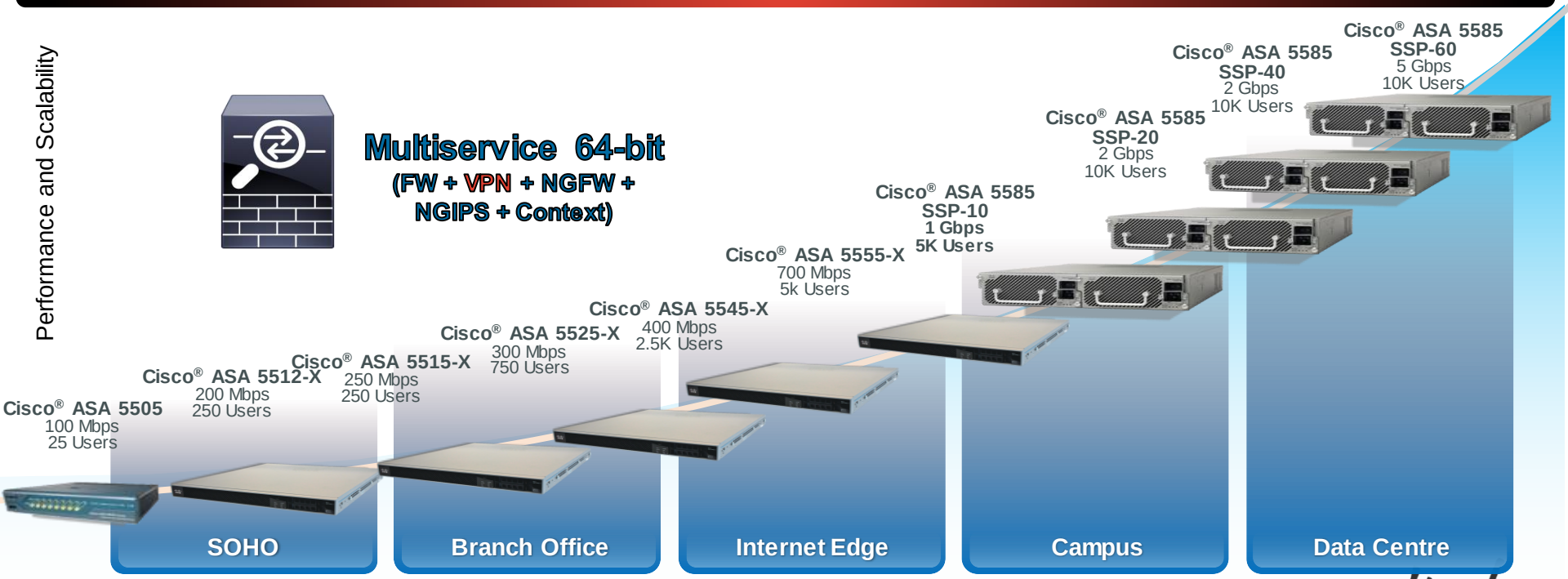
SOHO/Teleworker | **Branch Office** | **Internet Edge** | **Campus** | **Data Centre**

Red* = EoL Product**

Cisco live!

Cisco ASA Remote Access Security Gateway

Solutions Ranging from the Branch Office to the Enterprise



Use Case Network – CLINET (clinet.com)

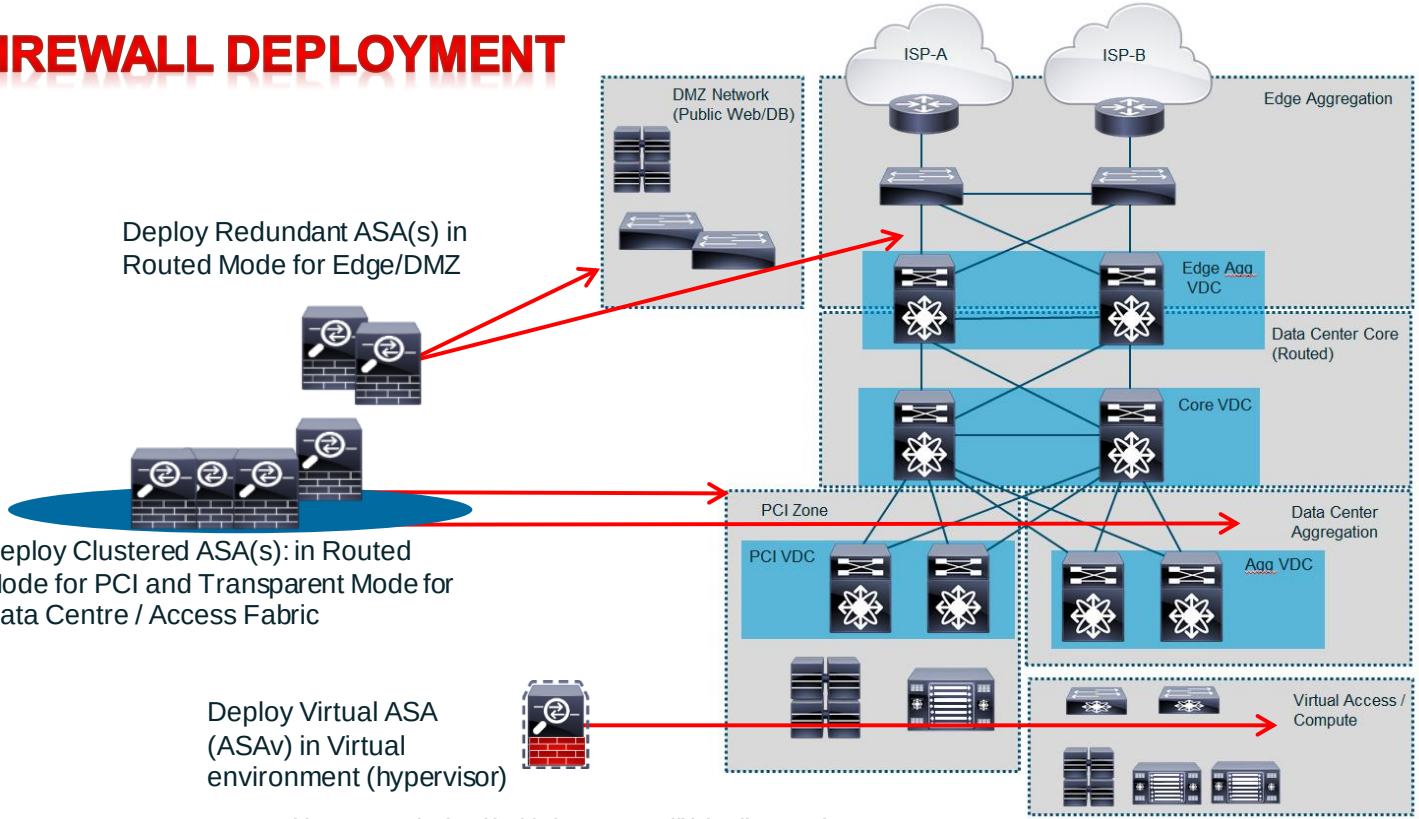
CLINET (clinet.com)

Cisco LIVE Information Networking Company

- CLINET (clinet.com) is a fictional company created for understanding use cases in ASA Firewall deployment
  - clinet.com has embarked on a network/security deployment project entitled "The Security 20/20 Project" which you will now be a part of
- Company requirements and configuration examples are based upon real-life customer conversations and deployments
  - Only designs we have fully certified in the Validated Design Lab
  - Cisco Validated Design (CVD) approved configuration(s)
    - e.g.
      DesignZone: http://www.cisco.com/go/designzone
      VMDC (Data Centre CVD): http://www.cisco.com/go/vmdc
      New Data Centre Security CVDs: http://www.cisco.com/go/designzonesecuredc

Overview – clinet.com Logical Network Diagram

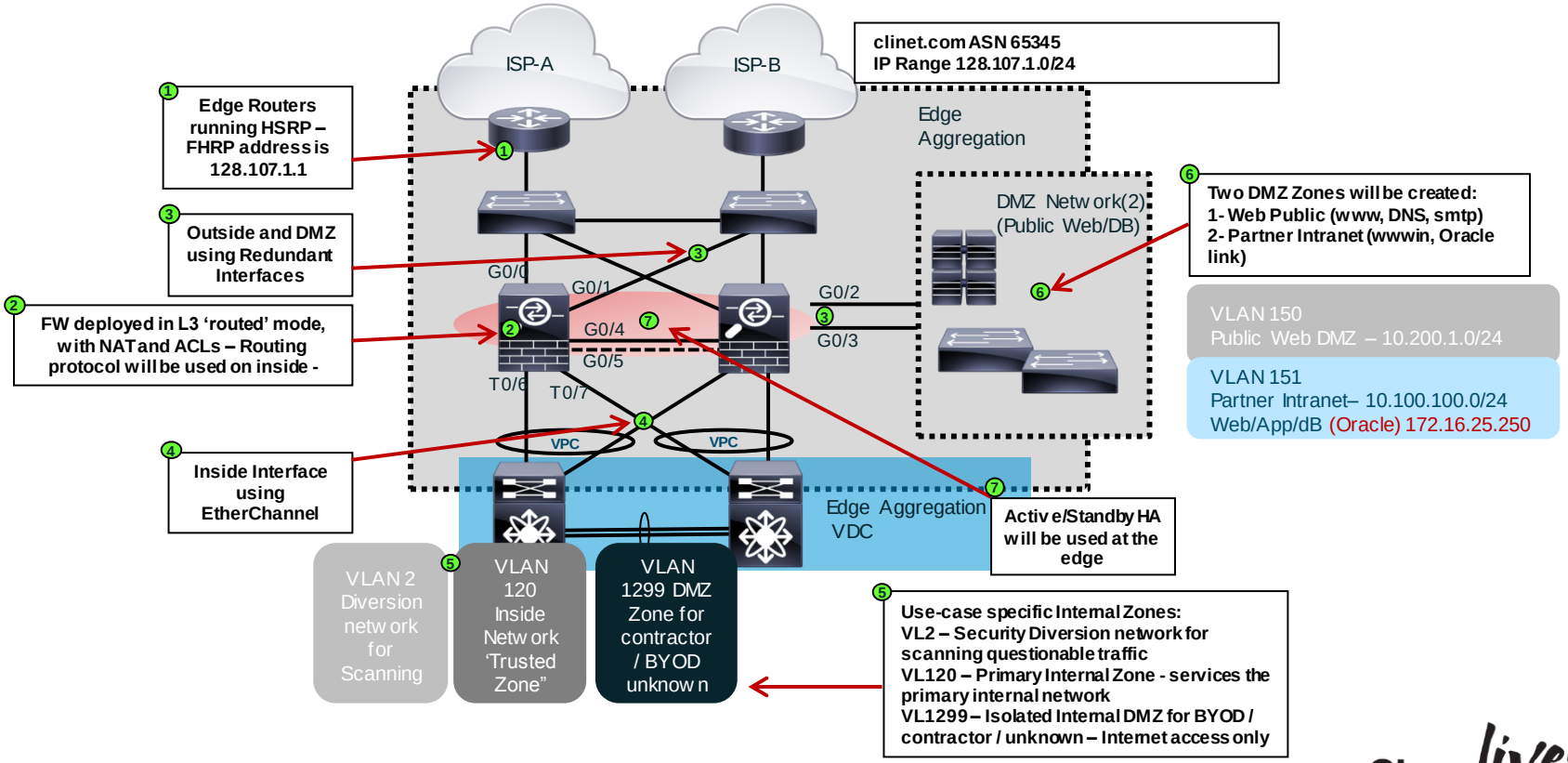
FIREWALL DEPLOYMENT



Note: Storage architecture not depicted in this layout, nor will it be discussed

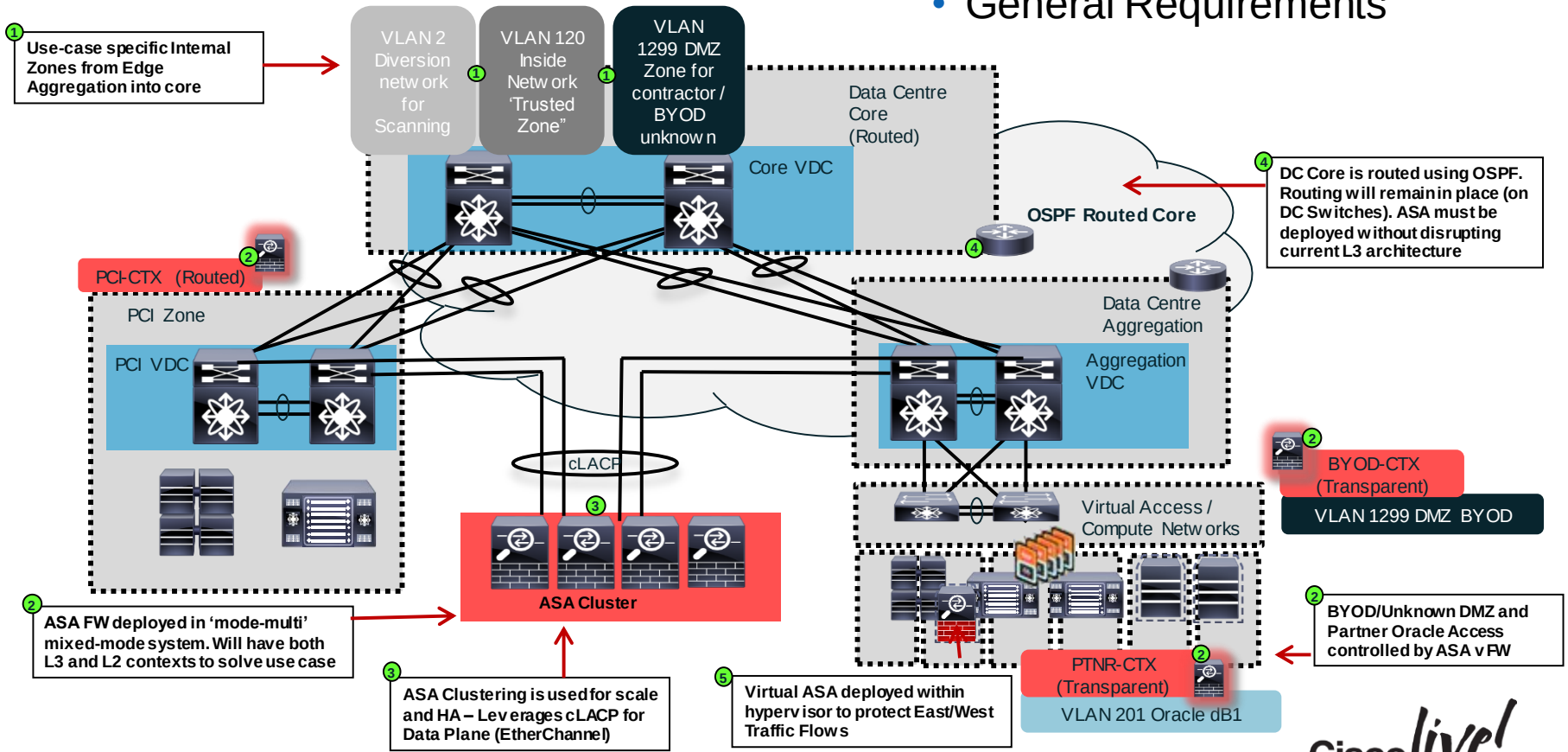
clinet.com Edge ASA Deployment Details

- General Requirements



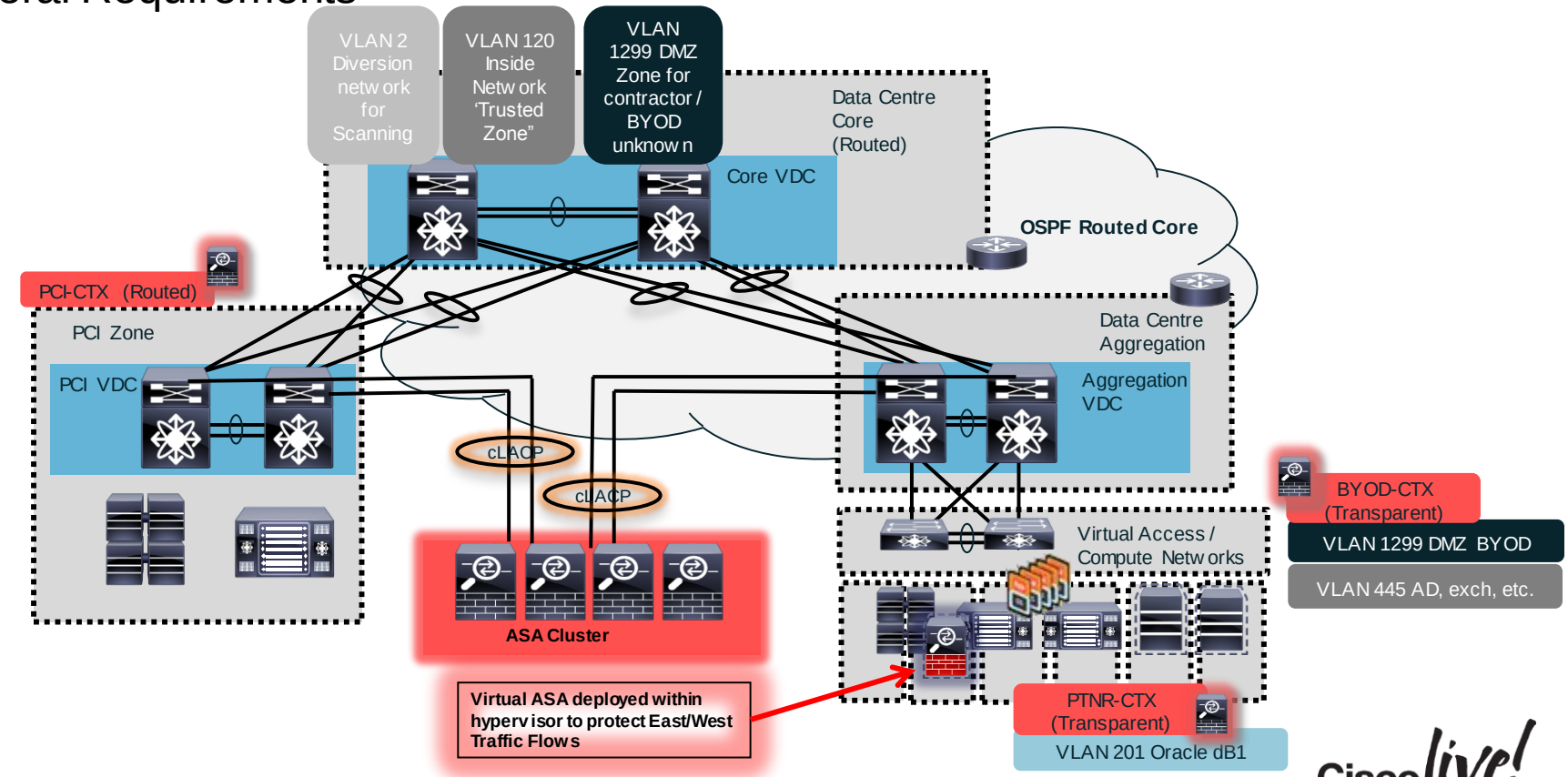
clinet.com DC AGG ASA Deployment Details

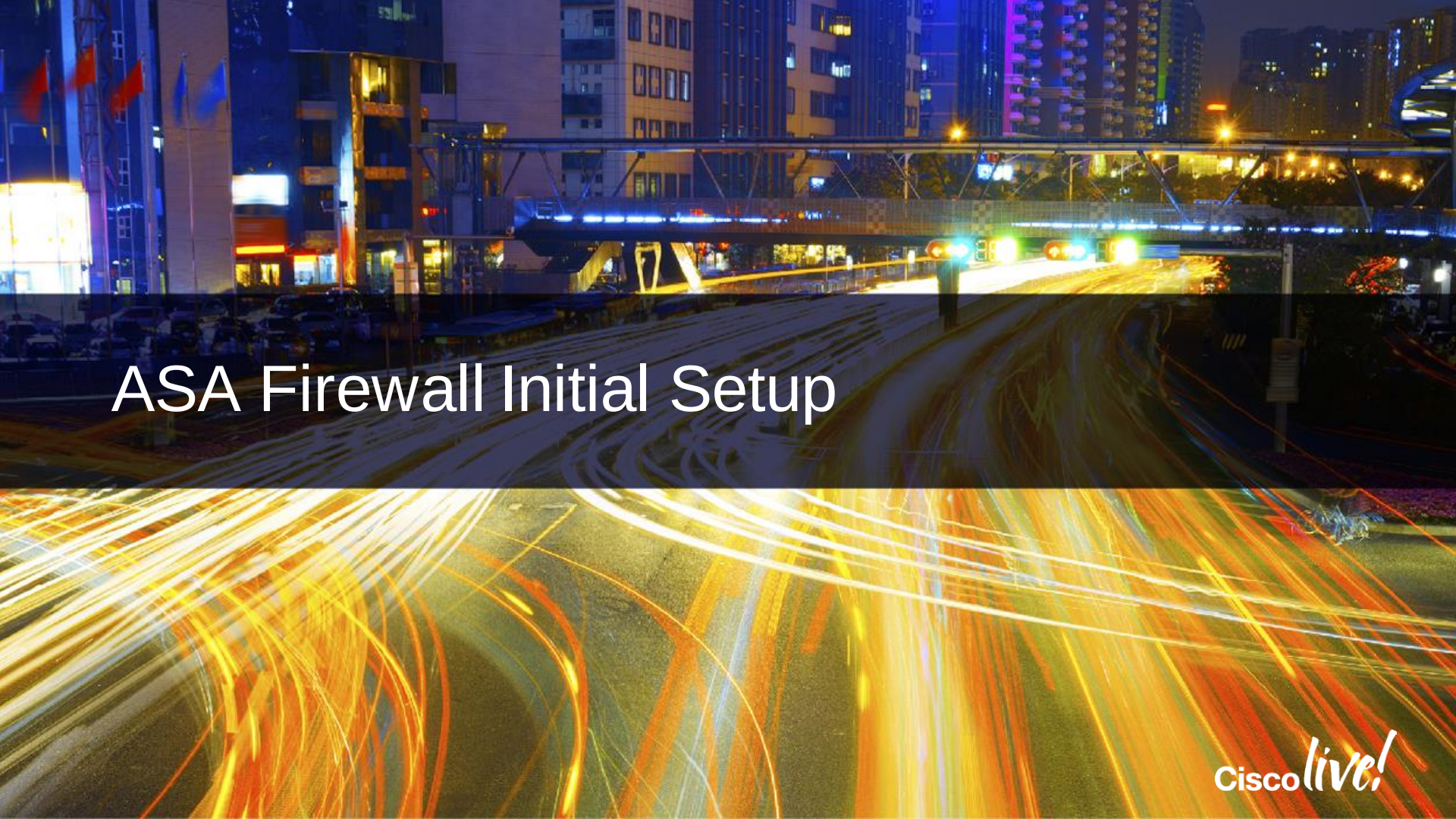
- General Requirements



clinet.com Data Centre Compute ASAv Deployment

- General Requirements





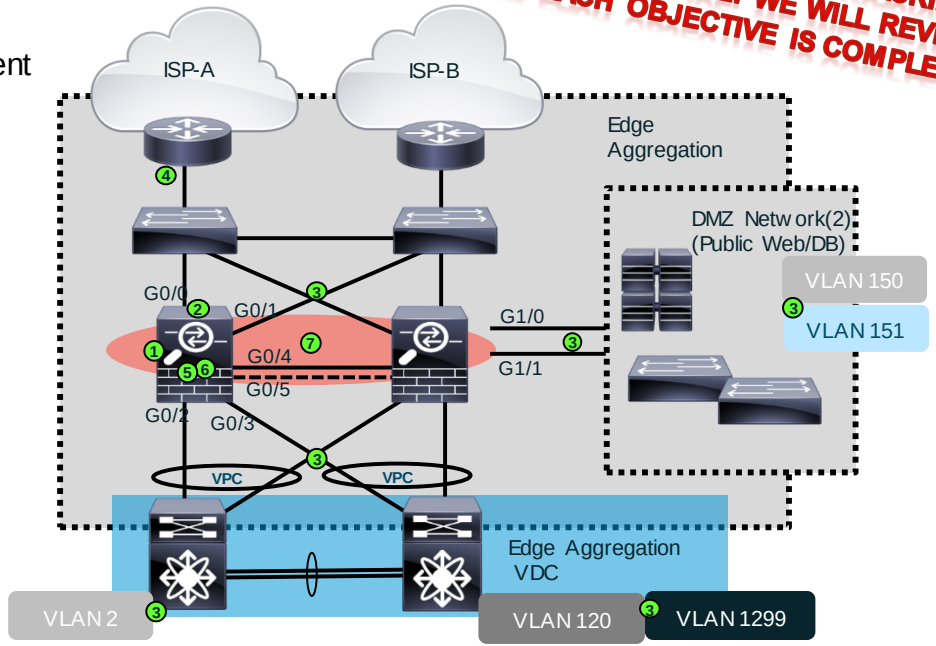
ASA Firewall Initial Setup

Cisco live!

ASA Deployment Checklist (Edge)

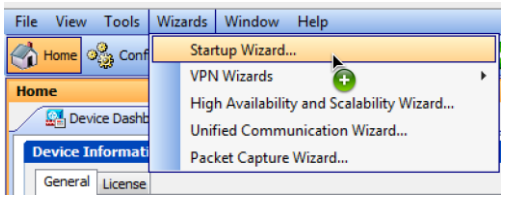
THIS WILL BE OUR PROJECT TRACKING AND SUMMARY SLIDE: WE WILL REVISIT AFTER EACH OBJECTIVE IS COMPLETE

- **On Primary ASA: (after initial setup)**
  - ① – Determine deployment mode –routed or transparent or both (mode multi)
  - ② – Examine Interface Security logic
  - ③ – Interface Configuration(s)
    - EtherChannel / LACP / Redundant
    - Nameif / Security-level / IP addressing
    - VLAN tagging / sub-interfaces / trunk
  - ④ – Routing
    - Default route / static / routing protocols
  - ⑤ – NAT
    - Static and Dynamic Translations
    - Auto NAT & Twice NAT
  - ⑥ – ACLs
    - Interface ACLs
    - Global ACLs
    - ACL Simplification methods
- **Implement HA**
  - ⑦ – A/S, A/A or Clustering



Initial FW Setup

- Valid for Appliance or Module
- ASA Bootstrapping – 2 options
  - Option 1: (If new) May connect directly to Management interface using a PC (DHCP) and execute: https://192.168.1.1/admin
    - No username / password needed
    - ASDM GUI will be used to run Startup Wizard



    - Once complete the ASA configuration guide can be used for further configuration:
    - http://www.cisco.com/c/en/us/td/docs/security/asa/asa91/configuration/firewall/asa_91_firewall_config.html
  - Load desired version of ASA 9x code – may be done via USB (64-bit appliances)
  - To use GUI – Make the latest ASDM image available in flash (disk0:/disk1:/,etc)

Initial FW Setup

- Valid for Appliance or Module
- ASA Bootstrapping – 2 options
  - Option 2: Connect PC to the management interface on ASA, then connect with console cable and execute in terminal

```
ciscoasa# config t
(config)#hostname EDGE-FW
EGDE-FW(config)# int m0/0
(config-if)#nameif management
(config-if)#sec 100
(config-if)#ip address 192.168.1.1 255.255.255.0
(config-if)#no shut
(config-if)#http server enable
(config)#http 0 0 management
(config)#aaa authentication http console LOCAL
(config)#domain-name CLINet.com
(config)#asdm image disk0:/nameofASDMimage.bin
(config)#username admin password cisco priv 15
(config)#crypto key gen rsa gen mod 1024 (use if SSL shows certificate error)
```

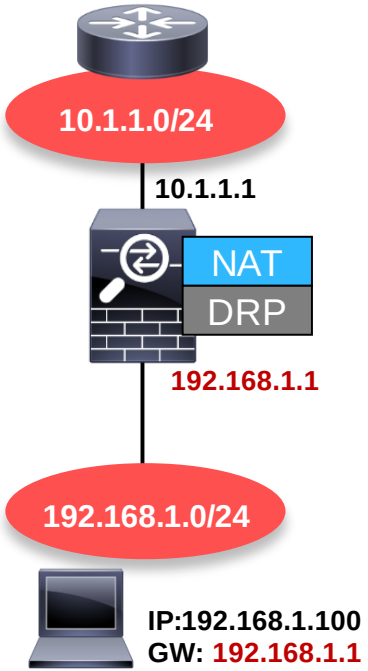
  - From a PC configured on the 192.168.1.0/24 subnet, you can launch ASDM and run startup wizard

Firewall Deployment Modes

Cisco live!

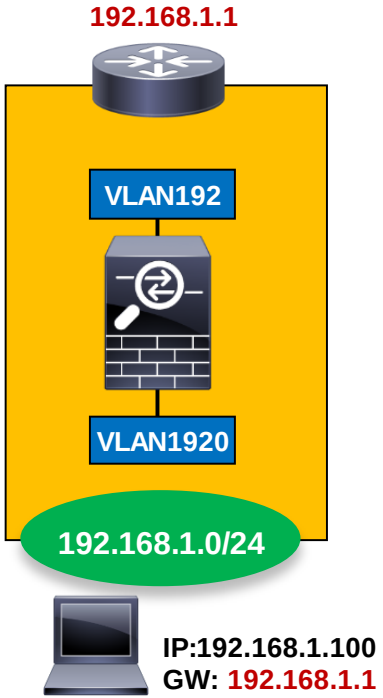
Firewall Design: Modes of Operation

- **Routed Mode** is the traditional mode of the firewall. Two or more interfaces that separate L3 domains – Firewall is the Router and Gateway for local hosts



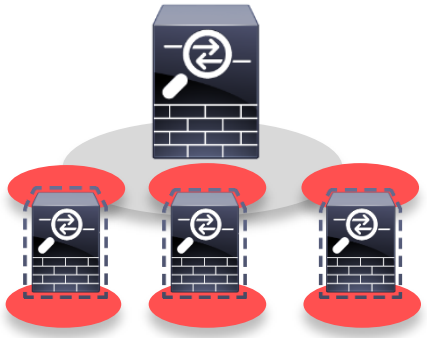
Firewall Design: Modes of Operation

- **Routed Mode** is the traditional mode of the firewall. Two or more interfaces that separate L3 domains – Firewall is the Router and Gateway for local hosts
- **Transparent Mode** is where the firewall acts as a bridge functioning at L2
  - Transparent mode firewall offers some unique benefits in the DC
  - Transparent deployment is tightly integrated with our 'best practice' data centre designs



Firewall Design: Modes of Operation

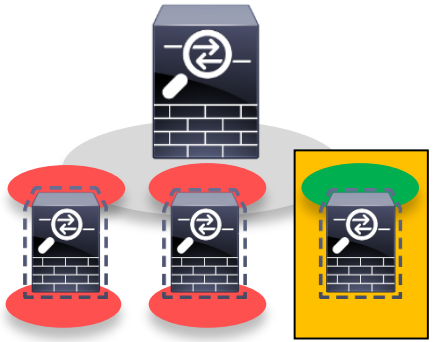
- **Routed Mode** is the traditional mode of the firewall. Two or more interfaces that separate L3 domains – Firewall is the Router and Gateway for local hosts
- **Transparent Mode** is where the firewall acts as a bridge functioning at L2
  - Transparent mode firewall offers some unique benefits in the DC
  - Transparent deployment is tightly integrated with our 'best practice' data centre designs
- **Multi-context Mode** involves the use of virtualised firewalls (vFW), which can be either routed or transparent mode



Separate Policies
Separate Control Plane
Separate Data Plane
Dedicated Interfaces

Firewall Design: Modes of Operation

- **Routed Mode** is the traditional mode of the firewall. Two or more interfaces that separate L3 domains – Firewall is the Router and Gateway for local hosts
- **Transparent Mode** is where the firewall acts as a bridge functioning at L2
  - Transparent mode firewall offers some unique benefits in the DC
  - Transparent deployment is tightly integrated with our 'best practice' data centre designs
- **Multi-context Mode** involves the use of virtualised firewalls (vFW), which can be either routed or transparent mode
- **Mixed (Multi-context) Mode** is the concept of using multi-context mode to combine routed and transparent mode virtualised firewalls on the same chassis or cluster of chassis'– Any ASA 9.x or Service Modules



Separate Policies
Separate Control Plane
Separate Data Plane
Dedicated Interfaces

Deploying ASA Routed (L3) Firewall at the Internet Edge

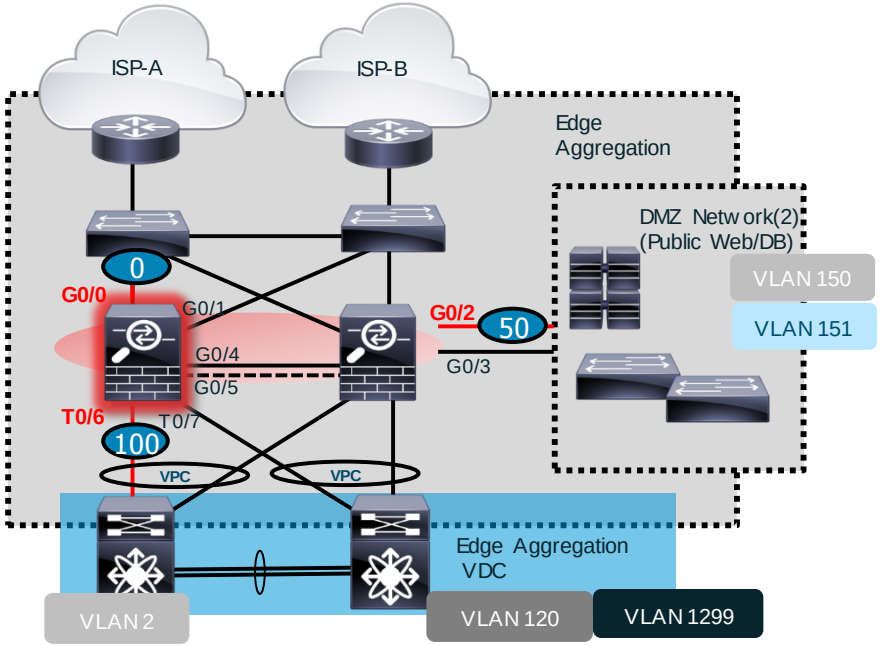
Cisco live!

Outside Interface Configuration

Redundant Interface

- **Ensure security levels are setup appropriately to allow desired communication with out ACLs**

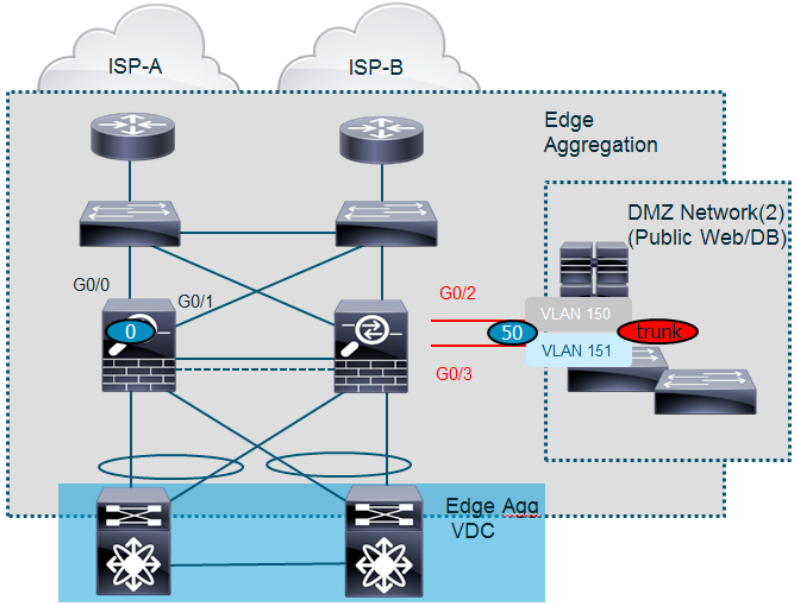
```
Edge-FW(config)#
 interface redundant1
   member-interface GigabitEthernet0/0
   member-interface GigabitEthernet0/1
   no shutdown
   description Outside Redundant Interface
   nameif outside
   security-level 0
   ip address 128.107.1.128 255.255.255.0
 interface GigabitEthernet0/0
   no shutdown
 interface GigabitEthernet0/1
  no shutdown
```



DMZ Interface Configuration

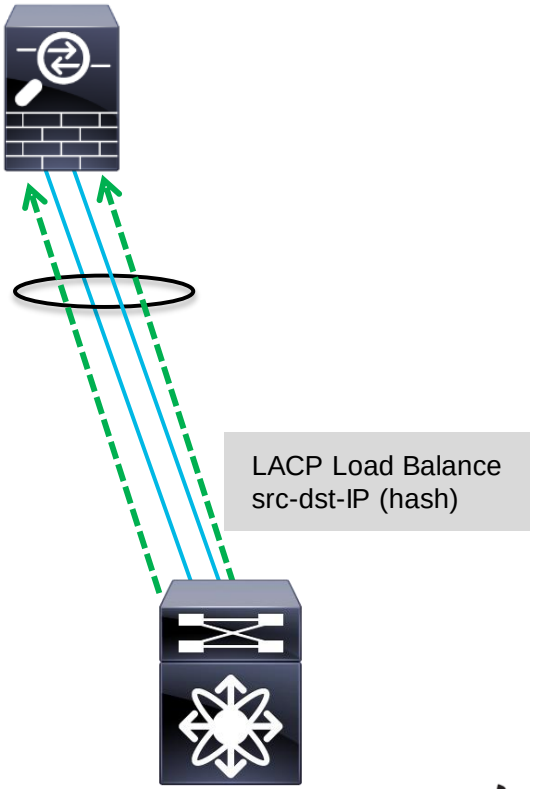
Redundant interface has VLAN sub-interfaces to accommodate multiple segments

```
Edge-FW(config)#
 interface redundant2
   member-interface GigabitEthernet0/2
   member-interface GigabitEthernet0/3
   no shutdown
interface redundant2.150
   vlan 150
   no shutdown
   nameif pubdmz
   security-level 50
   ip address  10.150.1.254 255.255.255.0
 interface redundant2.151
   vlan 151
   no shutdown
   nameif prtdmz
   security-level 50
   ip address  10.151.100.254 255.255.255.0
same-security-traffic permit inter-interface
(optional)
```



What is an EtherChannel?

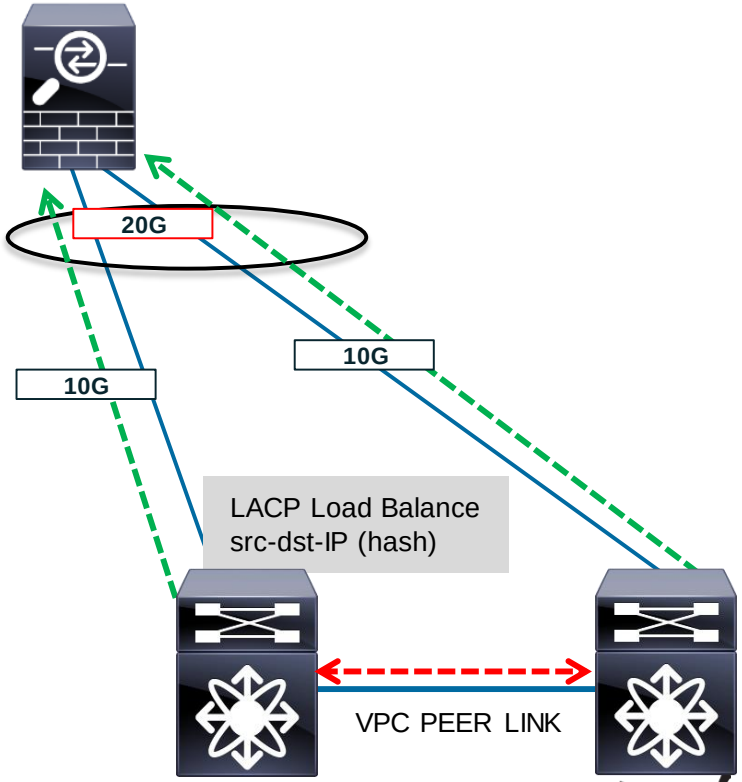
- EtherChannel LAG (IEEE standard is 802.3ad) allows up to 16 physical Ethernet links to be combined into one logical link. 8 links can be active and forwarding data*
  - Ports must be of same capabilities: duplex, speed, type, etc.
- Benefits of EtherChannel are increasing scale, load-balancing and HA
  - Load balancing is performed via a Load-Balancing Hashing Algorithm – Cisco default is src-dst IP
  - Recommended Hash is either default or src-dst ip-l4-port
- EtherChannel uses LACP (Link Aggregation Control Protocol) to allow dynamic bundling and dynamic recovery in case of failure
  - Static LAG can be used, but should be aware of potential traffic black holes this may cause



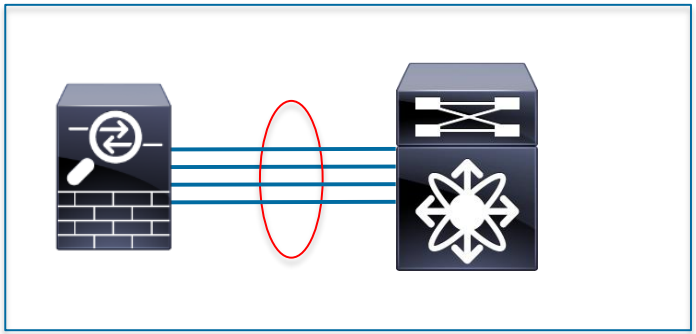
*New Versions of ASA Code have exceeded this limitation with cLACP and ASA Clustering

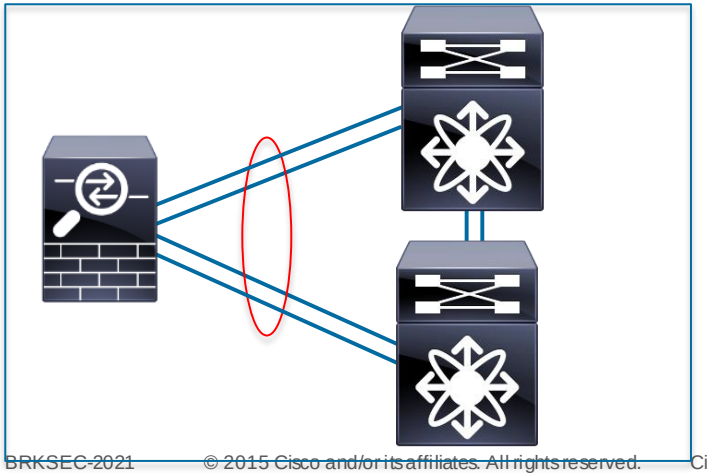
What is a vPC EtherChannel?

- vPC (like VSS) is known as Multi-Chassis EtherChannel
- Virtual Port Channels (vPC) are common EtherChannel deployments, especially in the Data Centre, and allow multiple devices to share multiple interfaces
  - All links are active – no STP blocked ports
- a vPC Peer Link is used on Nexus 5K/6K/7K devices to instantiate the vPC domain and allow sharing
  - Peer Link synchronises state between vPC peers
- vPC can maximise throughput since each port channel is treated as a single link for spanning-tree purposes
  - Spanning Tree is not disabled, but does not affect or impact the network
- vPC White paper: http://www.cisco.com/c/dam/en/us/td/docs/switches/datacenter/sw/design/vpc_design/vpc_best_practices_design_guide.pdf



EtherChannel on the ASA





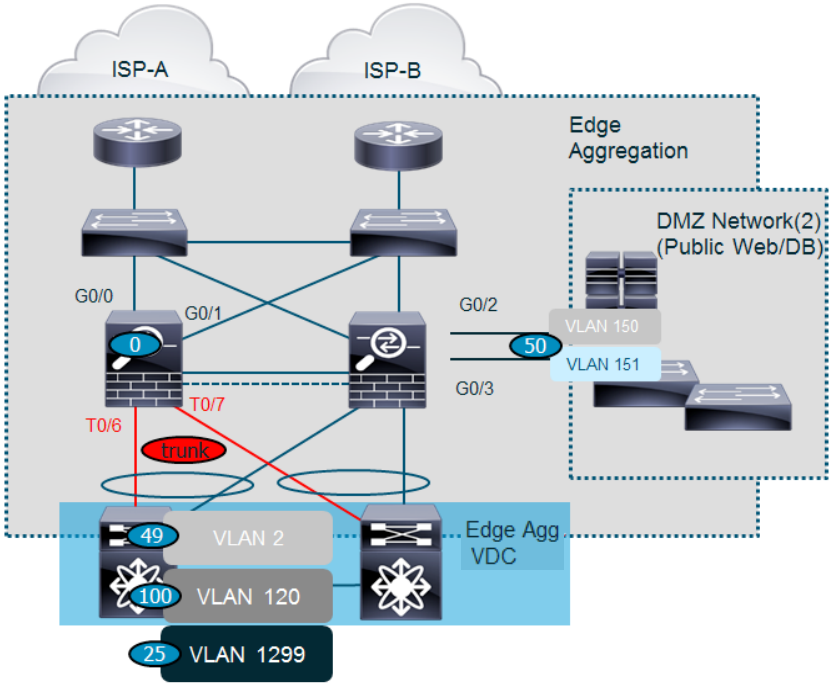
- Supports 802.3ad and LACP/cLACP standards
  - Direct support for vPC/VSS - CVD
  - No issues with traffic normalisation or asymmetry
- Up to 8 active and 8 standby links*
  - 100Mb, 1Gb, 10Gb are all supported – must match
- Supported in all modes (transparent, routed, multi-context)
- Configurable hash algorithm (default is src/dest IP)
  - SHOULD match the peer device for most deterministic flows
- Redundant interface feature and LAG on ASA are mutually exclusive
- Not supported on 4GE SSM (5540/50) or 5505
- ASA 9.2+ cluster allows 32 port active EtherChannel

*Non-clustered ASA allows 16 active and 16 standby links supported with cLACP

Inside Interface Configuration

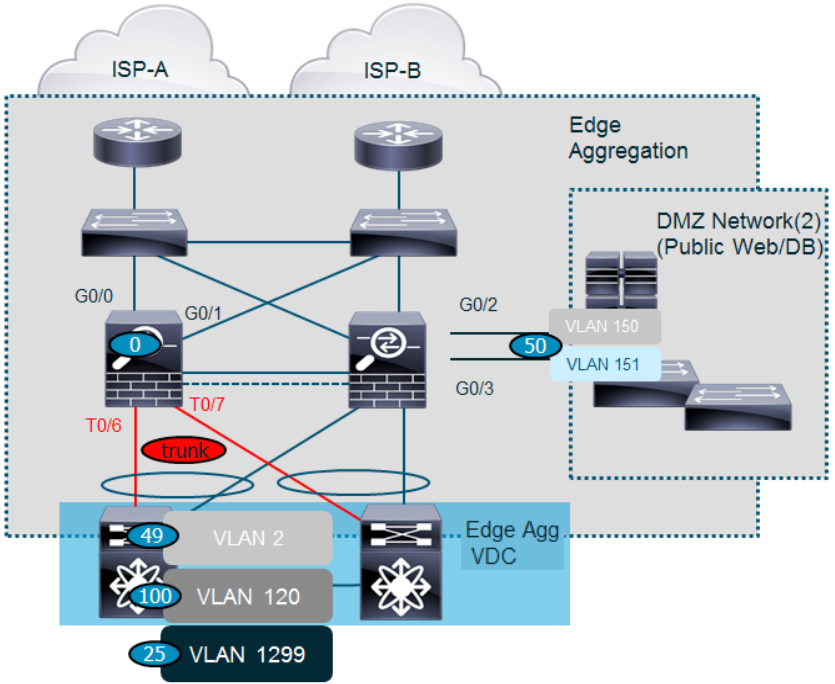
Ether-channel VLAN trunk allows multiple internal segments

```
Edge-FW(config)#
  interface TenGigabitEthernet0/6
   channel-group 10 mode active
  interface TenGigabitEthernet0/7
   channel-group 10 mode active

  interface port-channel10
   port-channel load-balance src-dst-ip (def)
   port-channel min-bundle 2
   lacp max-bundle 8
   no shutdown
   speed auto
   duplex auto
```



Inside Interface Configuration – (cont.)

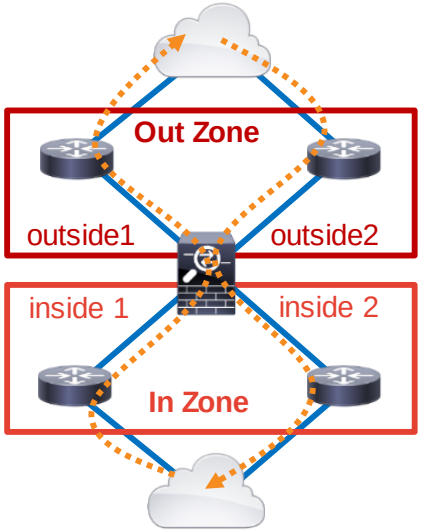
```
Edge-FW(config)# (continued)
 interface port-channel10.120
   vlan 120
   no shutdown
   nameif inside
   security-level 100
   ip address  10.120.1.254 255.255.255.0
 interface port-channel10.2
   vlan 2
   no shutdown
   nameif Diversion
   security-level 49
   ip address  10.2.1.254 255.255.255.0
 interface port-channel10.1299
   vlan 1299
   no shutdown
   nameif byod
   security-level 25
   ip address  10.255.255.254 255.255.255.0
```



New Feature – Traffic Zones

Available in ASA 9.3(2)

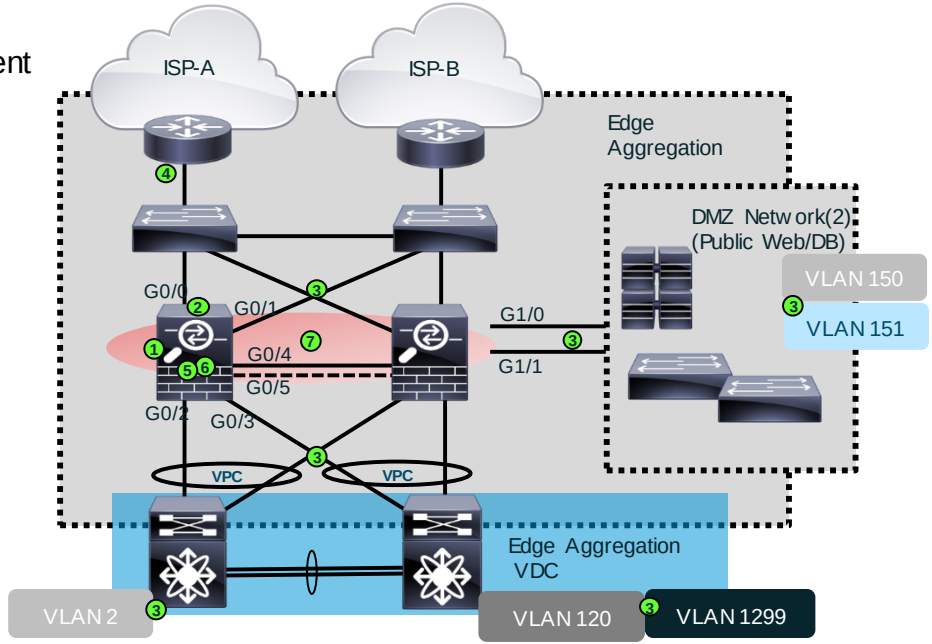
- Assign multiple logical interfaces to a Traffic Zone
  - Load-balances connections to multiple ISPs, using 6-tuple
  - Same-prefix ECMP with up to 8 next hops across all interfaces in a zone
  - Return traffic matched to the connection entry from any interface in a zone
  - All zone interfaces must be at the same security level
  - Seamless connection switchover to another egress interface in the same zone on failure
  - Fully enables Layer 3 Massively Scalable Data Centre (MSFC) spine-and-leaf model
  - Only supported in routed mode firewall



http://www.cisco.com/c/en/us/td/docs/security/asa/asa93/configuration/general/asa-general-cli/interface-zones.html

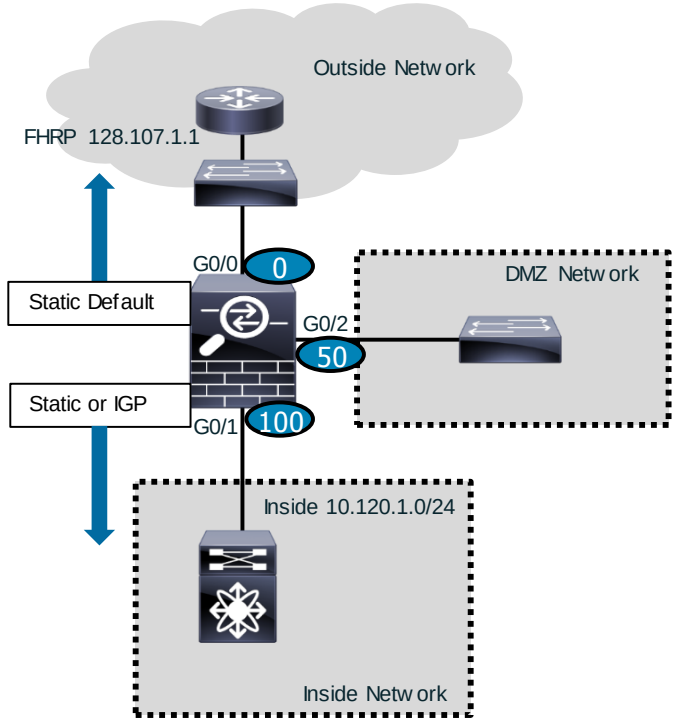
ASA Deployment Checklist – Summary

- **On Primary ASA: (after initial setup)**
  - ✓ 1 – Determine deployment mode –routed or transparent or both (mode multi)
  - ✓ 2 – Examine Interface Security logic
  - ✓ 3 – Interface Configuration(s)
    - EtherChannel / LACP / Redundant
    - Nameif / Security-level / IP addressing
    - VLAN tagging / sub-interfaces / trunk
  - 4 – Routing
    - Default route / static / routing protocols
  - 5 – NAT
    - Static and Dynamic Translations
    - Auto NAT & Twice NAT
  - 6 – ACLs
    - Interface ACLs
    - Global ACLs
    - ACL Simplification methods
- **Implement HA**
  - 7 – A/S, A/A or Clustering



Routing on the ASA

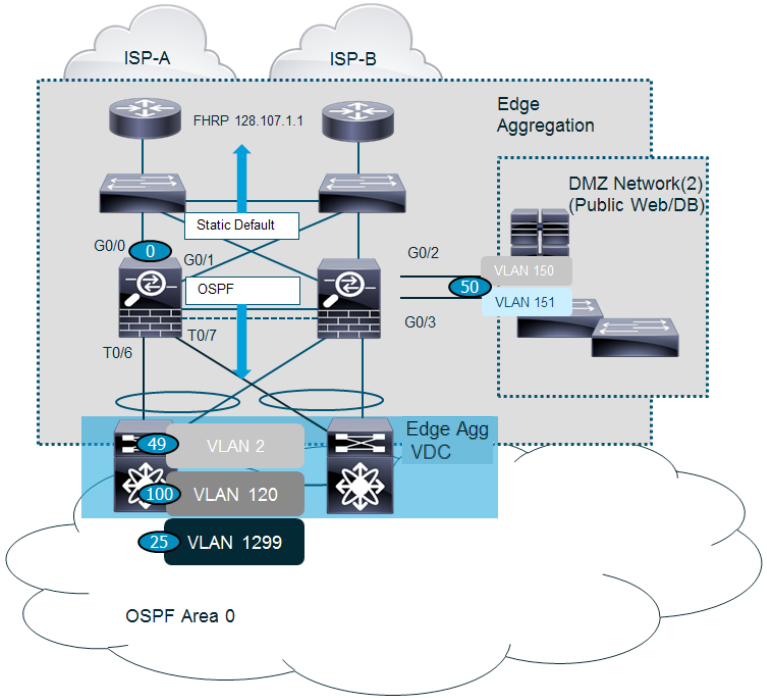
- The ASA is performs L3 route lookup as part of its normal packet processing flow
  - ASA is optimised as a ‘flow-based inspection’ device and is not optimised as a ‘packet forwarding’ router
    - As such, ASA should not be considered a viable router replacement
    - ASR1K would be a better option
  - ASA may still need to become a routing ‘source of truth’ in some network deployments
- ASA Supports both static routing and most IGP routing protocols
  - BGPv4 (9.2.1) & BGPv6 (9.3.2)
  - OSPF v2 & OSPF v3 (IPv6)
  - EIGRP
  - RIP v1/v2
  - Multicast
- Routing protocols are fully supported in Multi-Context mode
- Complete IP Routing configuration in config guides: http://www.cisco.com/c/en/us/td/docs/security/asa/asa93/configuration/firewall/asa_93_firewall_config.pdf



Deploying ASA Routing

Static outside and dynamic inside routing* example for Use Case

```
Edge-FW(config)#
route outside 0.0.0.0 0.0.0.0 128.107.1.1
or
route outside 0 0 128.107.1.1
!
router ospf 110
 network 10.0.0.0 255.0.0.0 area 0
 ospf priority 0
 redistribute connected route-map dmznets
!
route-map dmznets permit 10
 match ip address dmz
!
access-list dmz permit 10.150.1.0 255.255.255.0
access-list dmz permit 10.151.100.0 255.255.255.0
```



*Dynamic Routing across vPC is currently planned for NXOS v7.2

NAT on the ASA

- Single translation rule table
- Access Lists reference the internal (real) IP address and not the global
- **Manual NAT (Twice NAT)**
  - Allows for bi-directional translation
  - Allows to specify both Source and Destination NAT within a single line
  - More flexibility in creating NAT rules (one-to-one, one-to-many, many-to-many, many-to-one)
- **Automatic NAT (Auto NAT or Object-based)**
  - Single rule per object
  - Useful for less complex scenarios

NAT Processing Semantics

- Rules are processed in order (like ACEs inside of an ACL) – caching of those rules' IDs inside Data Plane structures assures of this
  - Rule ID is used to change it's place inside the list
- Manual NAT rules are always processed first
  - Within Manual NAT rules list, only the order matters – it doesn't take into account dynamic/static nature of the statement
- Auto NAT rules are processed next
  - Auto NAT Rule ordering is predefined based on the following order of precedence:
    - static over dynamic
    - longest prefix
    - lower numeric (start from 1st octet)
    - lexicographic ordering of object-names

Examples: Auto NAT – Object-based NAT

- Auto NAT requires the object configuration and the NAT configuration is contained within
- Dynamic NAT translation for a subnet using Interface PAT

```
object network inside-net-2out
  subnet 10.120.1.0 255.255.255.0
  nat (inside,outside) dynamic interface

object network inside-net-2dmz
  subnet 10.120.1.0 255.255.255.0
  nat (inside,dmz) dynamic interface
```

- Static NAT translation to translate a server at 172.16.25.200 to a public address 128.107.1.200:

```
object network update-server
  host 172.16.25.200
  nat (inside,outside) static 128.107.1.200
```

Examples: Auto NAT – Object-based NAT (cont.)

- Dynamic NAT translation for a subnet using IP Address Range

```
object network pub-nat-range
    range 128.107.1.10 128.107.1.20

object network inside-net-2out
   subnet 10.120.1.0 255.255.255.0
   nat (inside,outside) dynamic pub-nat-range
```

- Dynamic NAT translation for a subnet using PAT

```
object network obj-128.107.1.8
   host 128.107.1.8
object network obj-128.107.1.9
   host 128.107.1.9
object-group network pat-IP-group
   network-object object obj-128.107.1.8
   network-object object obj-128.107.1.9
object network inside-net-PAT-outside
   subnet 10.120.1.0 255.255.255.0
   nat (inside,outside) dynamic pat-pool pat-IP-group
```

Understanding Manual NAT (Twice NAT)

- Unlike Auto NAT, Twice NAT policy config must use network objects
- A single rule contains both source and destination policy (bidirectional)
- Twice NAT can reference network objects and object-groups but NAT policy is assigned outside of network object element

```
object network in-host
   host 192.168.1.10
object network in-host-nat
   host 128.107.1.242
object network out-host-nat
   host 192.168.1.155
object network out-host
   host 128.107.1.155
nat (inside,outside) source static in-host in-host-nat dest static out-host-nat out-host
```

Packet enters on inside: (srcIP:in-host –> destIP:out-host-nat)

Packet exits on outside: (in-host-nat –> out-host)

Much more detail in 9.3 Configuration Guide: http://www.cisco.com/c/en/us/td/docs/security/asa/asa93/configuration/firewall/asa-firewall-cli/nat-basics.html

Understanding Manual NAT (Twice NAT)

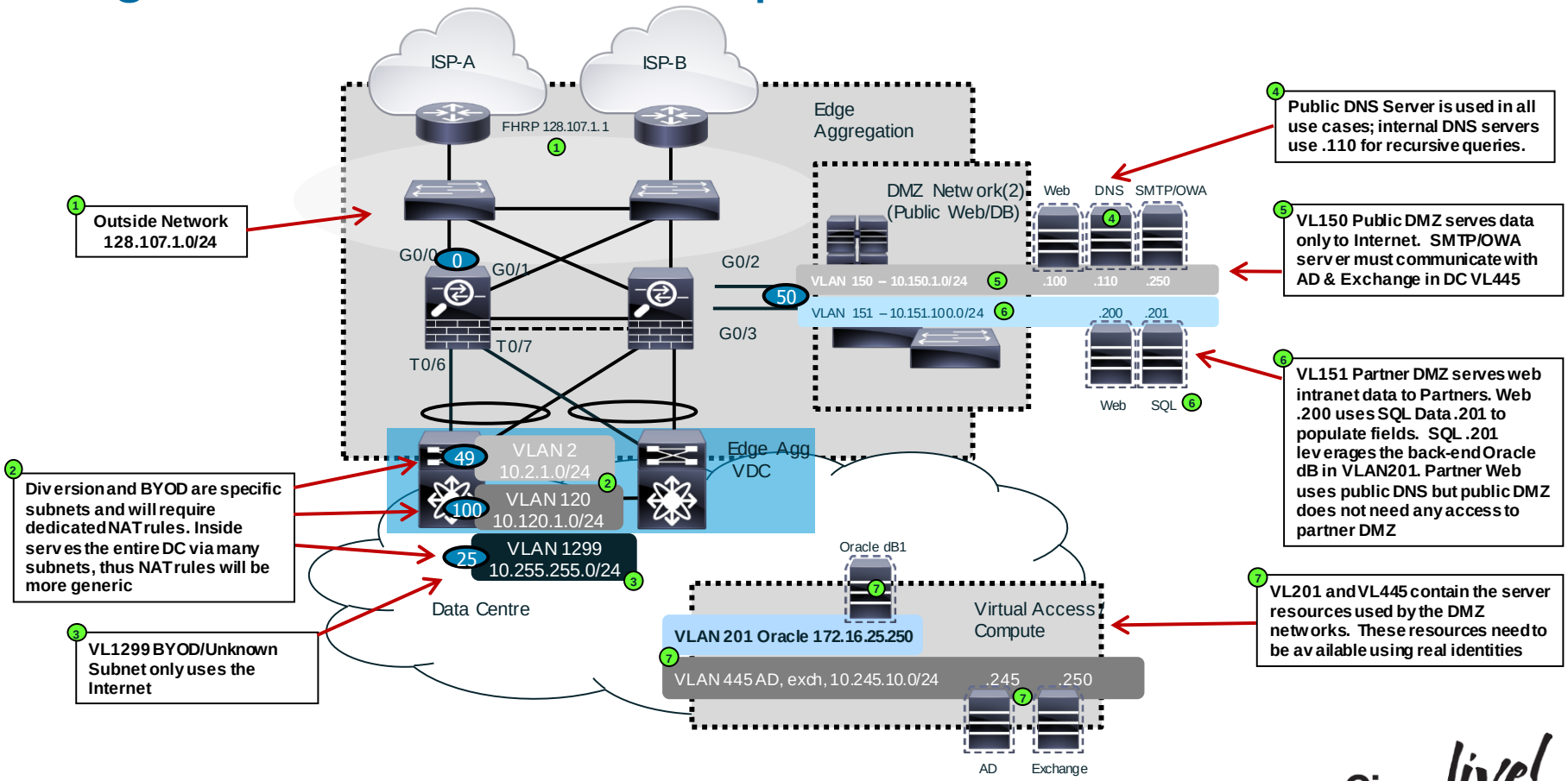
- Identity NAT Example for a subnet

```
object network obj-10.1.2.0
   subnet 10.1.2.0 255.255.255.0
nat (inside,dmz) source static obj-10.1.2.0 obj-10.1.2.0
```

- Identity NAT example for a host

```
object network obj-10.120.2.100
   host 10.120.2.100
nat (inside,dmz) source static obj-10.120.2.100 obj-10.120.2.100
```

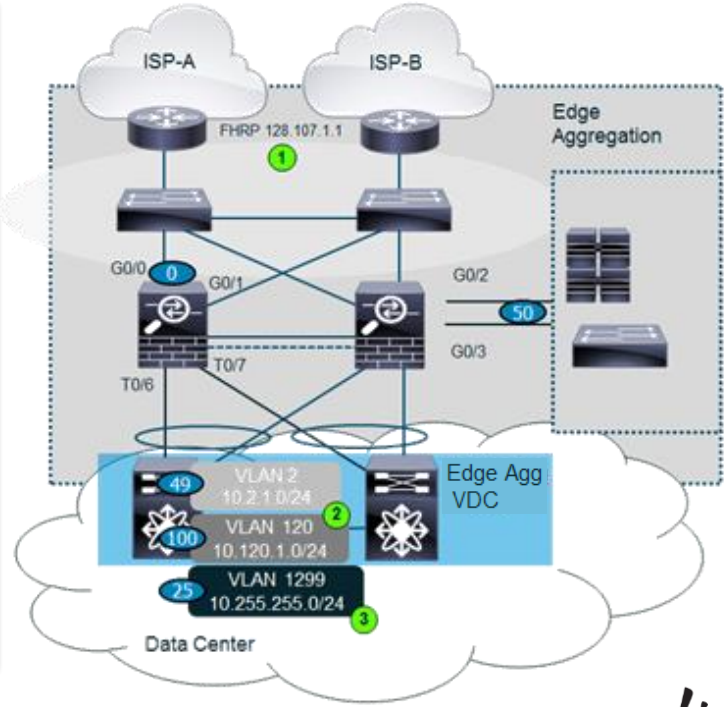
Edge NAT Use Case Requirements



Deploying NAT on the ASA

Inside, Diversion, and BYOD Network Use-cases

```
Edge-FW(config)#

object network obj-pub-nat-range
  range 128.107.1.150 128.107.1.155
object network obj-net-in-2out
  subnet 10.0.0.0 255.0.0.0
  nat (inside,outside) dynamic obj-pub-nat-range interface

object network cyber-IP
  host 128.107.1.99
object network obj-net-Diversion
  subnet 10.2.1.0 255.255.255.0
  nat (inside,outside) dynamic cyber-IP

object network BYOD-IP
  host 128.107.1.200
object network obj-net-BYOD
  subnet 10.255.255.0 255.255.255.0
  nat (inside,outside) dynamic BYOD-IP
```

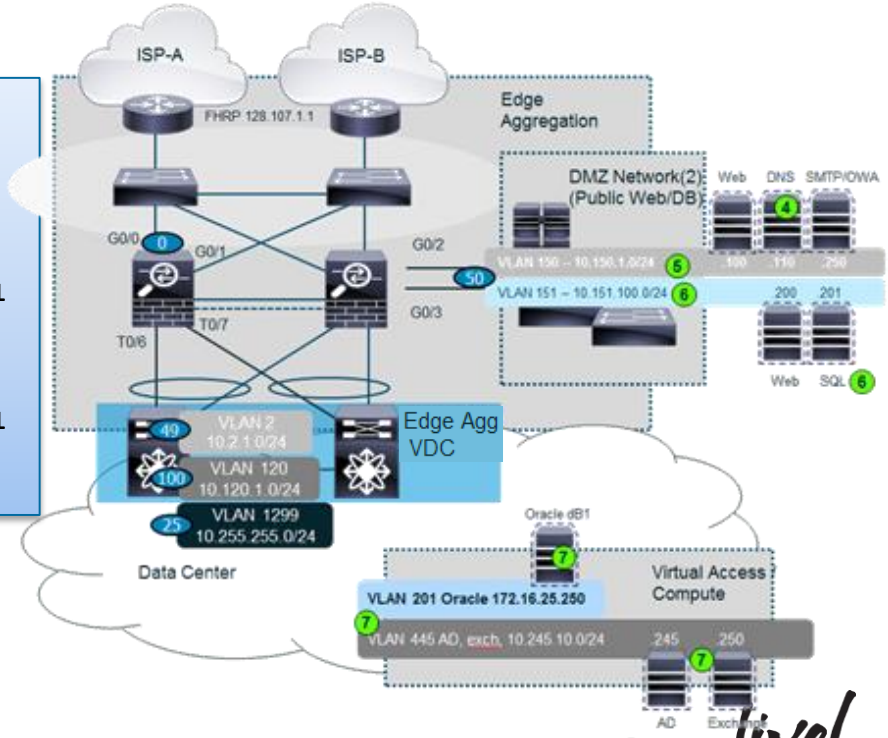


Cisco live!

QUICK- Deploying NAT on the ASA

Pub-DMZ Use-Cases - WebServer

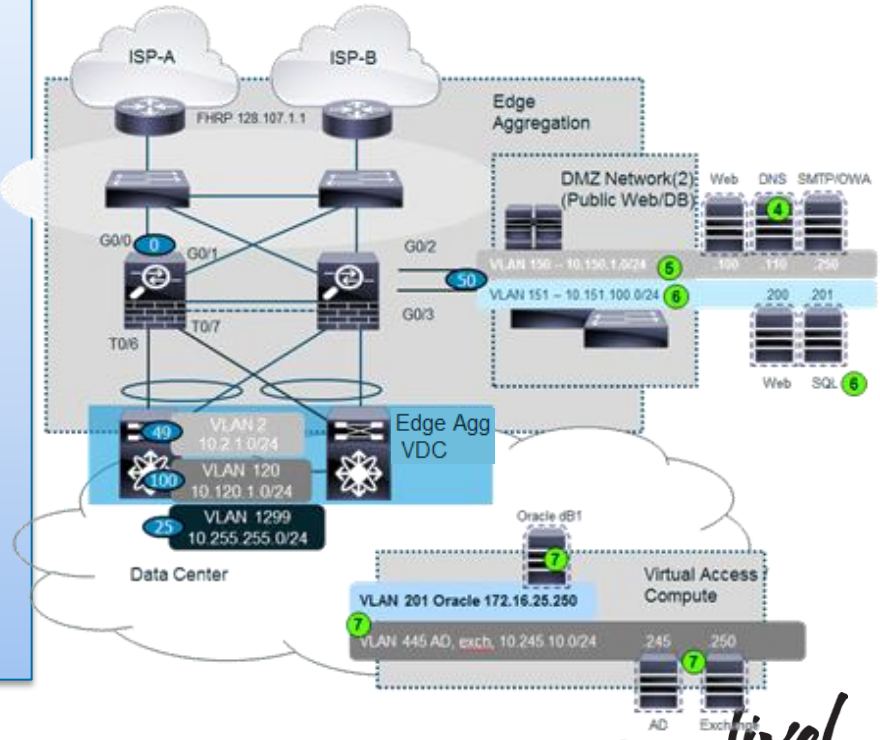
```
Edge-FW(config)#
object network real-pubWEB1
   host 10.150.1.100
object network nat-pubWEB1
   host 128.107.1.100

nat (pubdmz,outside) source static real-pubWEB1 nat-pubWEB1

object network obj-DC-nets
   subnet 10.0.0.0 255.0.0.0
nat (pubdmz,inside) source static real-pubWEB1 real-pubWEB1
destination static obj-DC-nets obj-DC-nets
```



QUICK-Deploying NAT on the ASA

Pub-DMZ Use-Cases – DNS Server

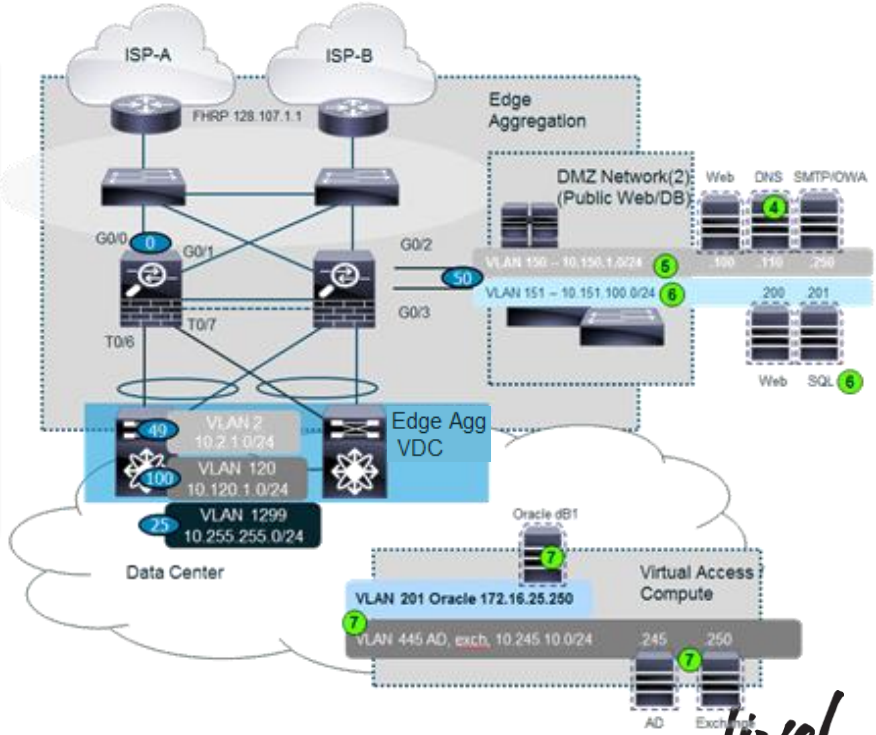
```
Edge-FW(config)#
object network real-pubDNS
   host 10.150.1.110
object network nat-pubDNS
   host 128.107.1.110

nat (pubdmz,outside) source static real-pubDNS nat-pubDNS

object network prtDMZ-net
   subnet 10.151.0.0 255.255.0.0
object-group network inside-nets
   subnet 10.2.0.0 255.255.0.0
   subnet 10.120.0.0 255.255.0.0
   subnet 10.255.0.0 255.255.0.0

nat (pubdmz,prtdmz) source static real-pubDNS real-pubDNS
destination static prtDMZ-net prtDMZ-net route-lookup

nat (pubdmz,inside) source static real-pubDNS real-pubDNS
destination static inside-nets inside-nets route-lookup
```



QUICK-Deploying NAT on the ASA

Pub-DMZ Use-Cases – AD & Exchange

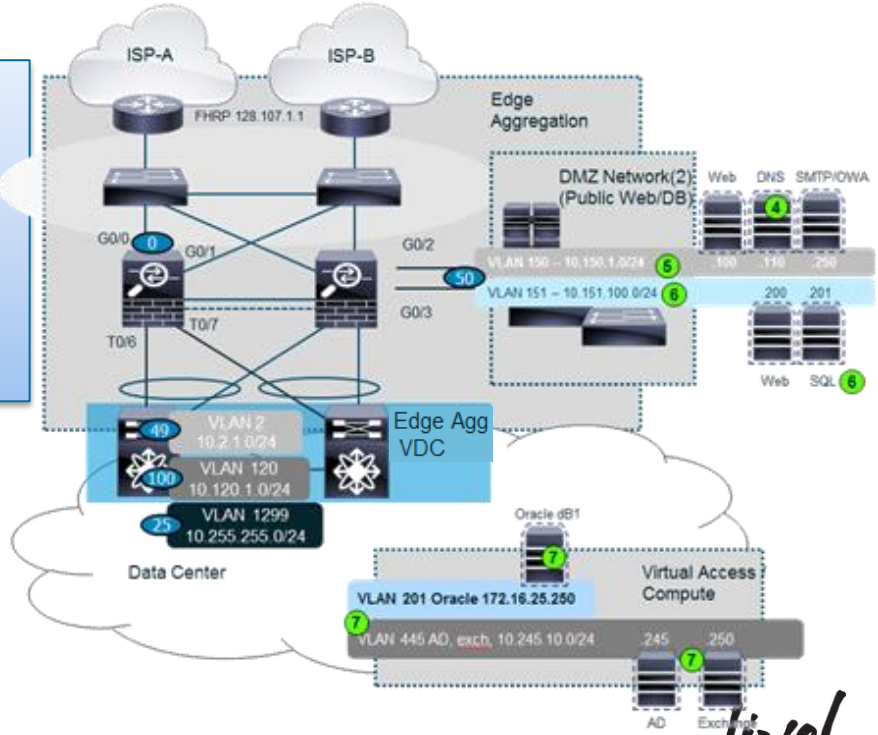
```
Edge-FW(config)#
!No need to do identity NAT as nat-control was deprecated
!So write only NAT rules for what you need to translate
!If you are not sure, it will not hurt to have it

object network real-ad
   host 10.245.10.245
   nat (inside,pubdmz) source static real-ad real-ad

object network real-exch
   host 10.245.10.250
   nat (inside,pubdmz) source static real-exch real-exch
```



QUICK-Deploying NAT on the ASA

Partner-DMZ Use-Cases – Web Server

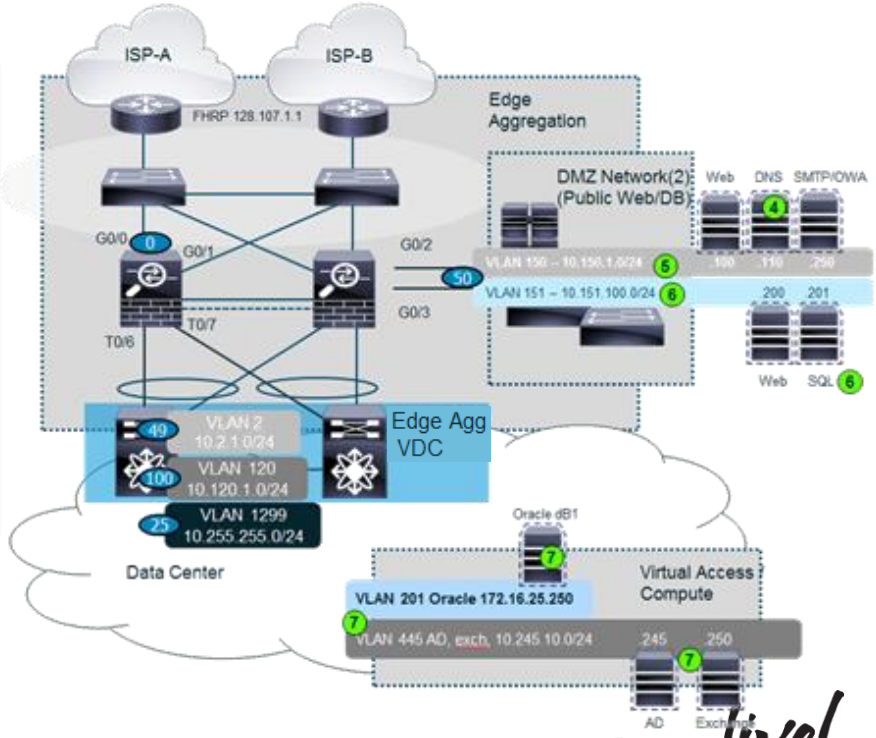
```
Edge-FW(config)#
object network real-prtWEB1
   host 10.151.100.200
object network nat-prtWEB1
   host 128.107.1.200

nat (prtdmz,outside) source static real-prtWEB1 nat-prtWEB1

nat (prtdmz,pubdmz) source dynamic real-prtWEB1 interface
```



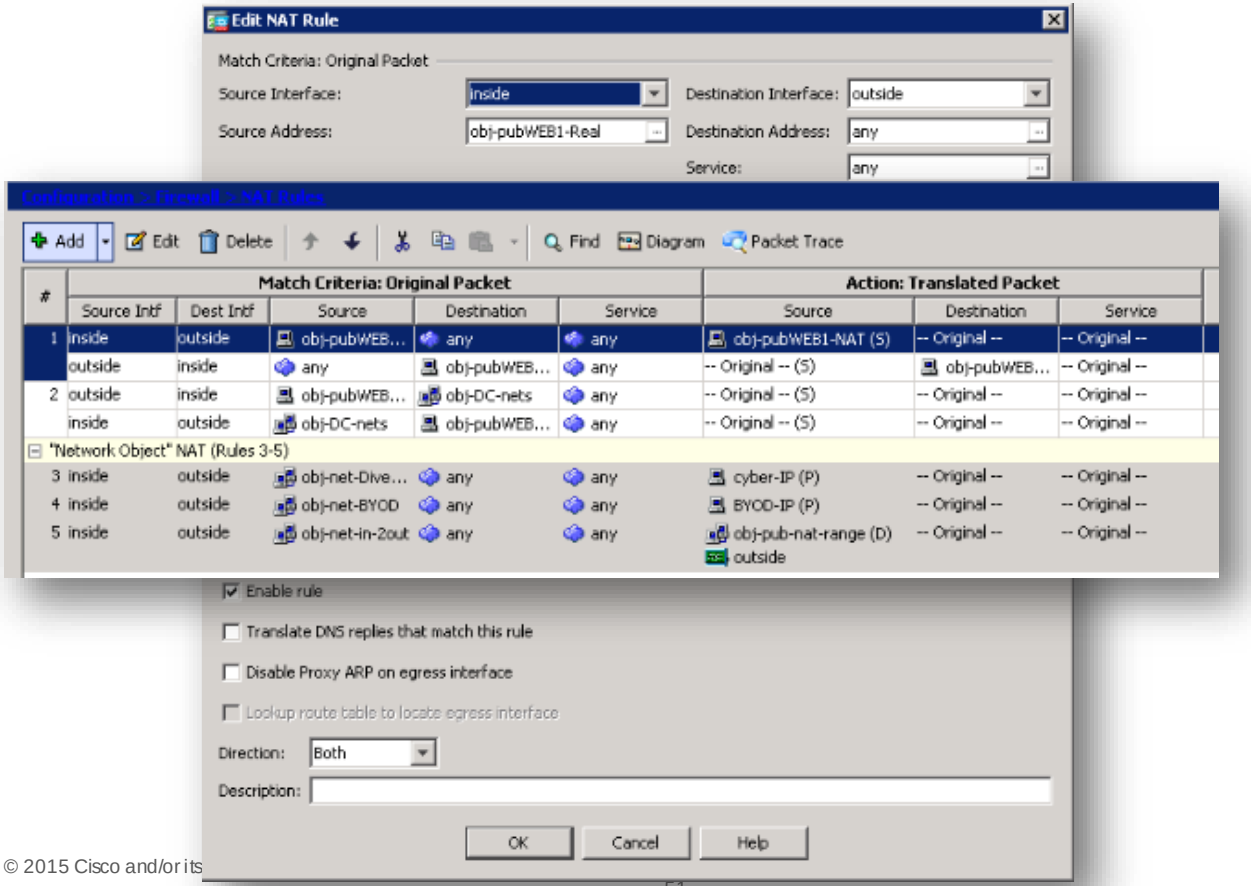
QUICK-Deploying NAT on the ASA

Partner-DMZ Use-Cases – SQL Server / Oracle

```
Edge-FW(config)#
!No need to do identity NAT as NAT-control was deprecated
!So write only NAT rules for what you need to translate
!If you are not sure, it will not hurt to have it

object network real-sql
   host 10.151.100.201
   nat (inside,pubdmz) source static real-sql real-sql

object network real-orac
   host 172.16.25.250
   nat (inside,pubdmz) source static real-orac real-orac,
```



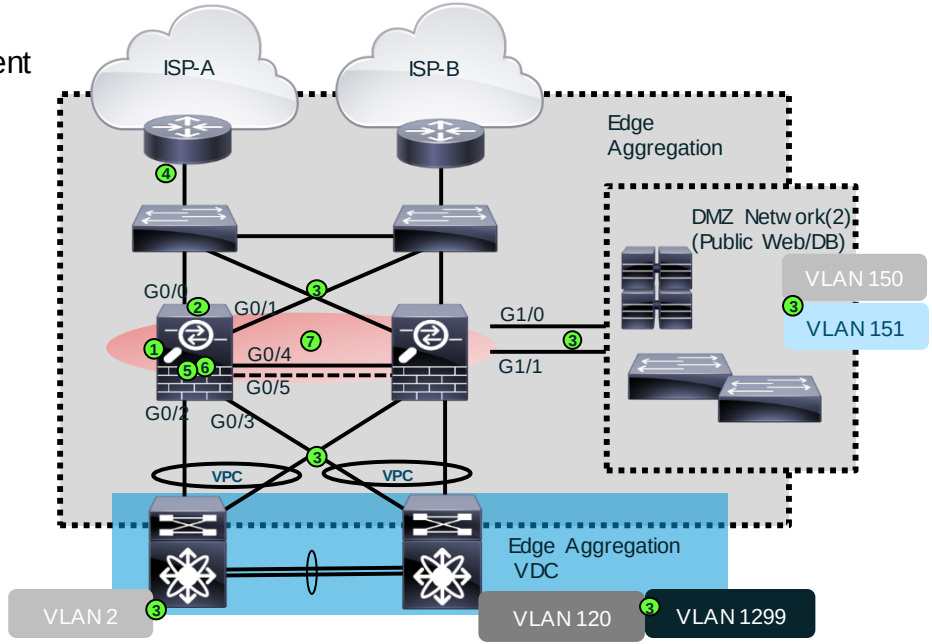
ASA 8.3+ Unified NAT Table in ASDM



ASA Deployment Checklist – Summary

- **On Primary ASA: (after initial setup)**

1. – Determine deployment mode –routed or transparent or both (mode multi)
2. – Examine Interface Security logic
3. – Interface Configuration(s)
   - EtherChannel / LACP / Redundant
   - Nameif / Security-level / IP addressing
   - VLAN tagging / sub-interfaces / trunk
4. – Routing
   - Default route / static / routing protocols
5. – NAT
   - Static and Dynamic Translations
   - Auto NAT & Twice NAT
6. – ACLs
   - Interface ACLs
   - Global ACLs
   - ACL Simplification methods

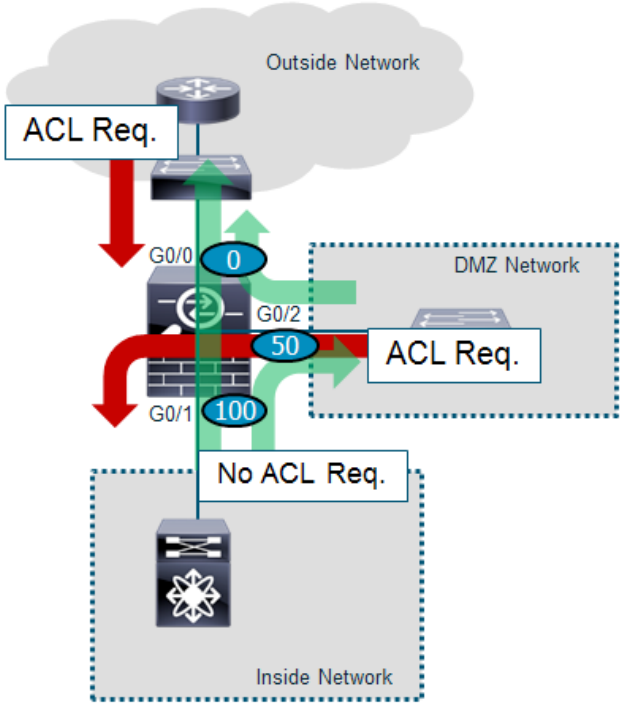


- **Implement HA**

7. – A/S, A/A or Clustering

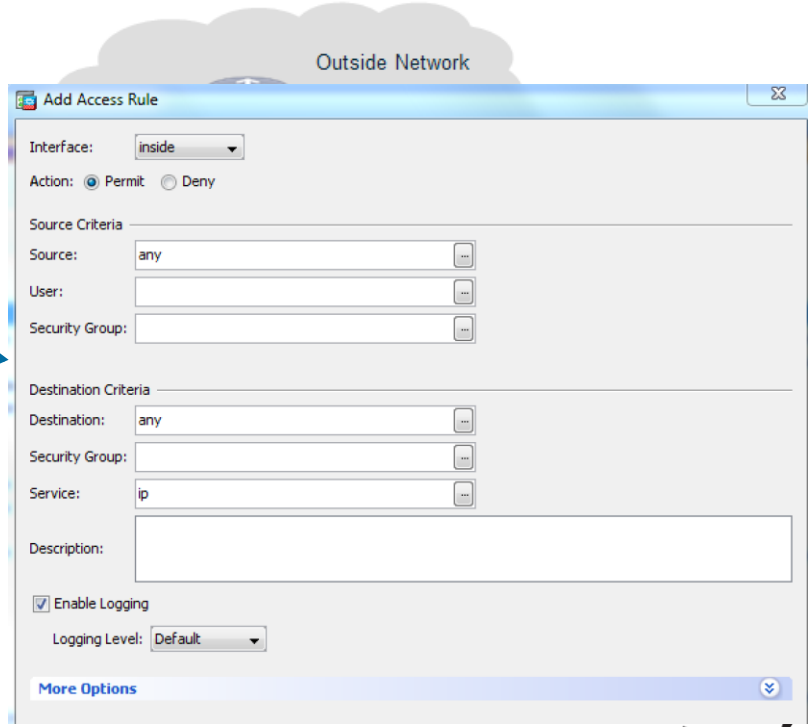
Access Control Lists

- 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 can be enabled/disabled based on time ranges



Access Control Lists

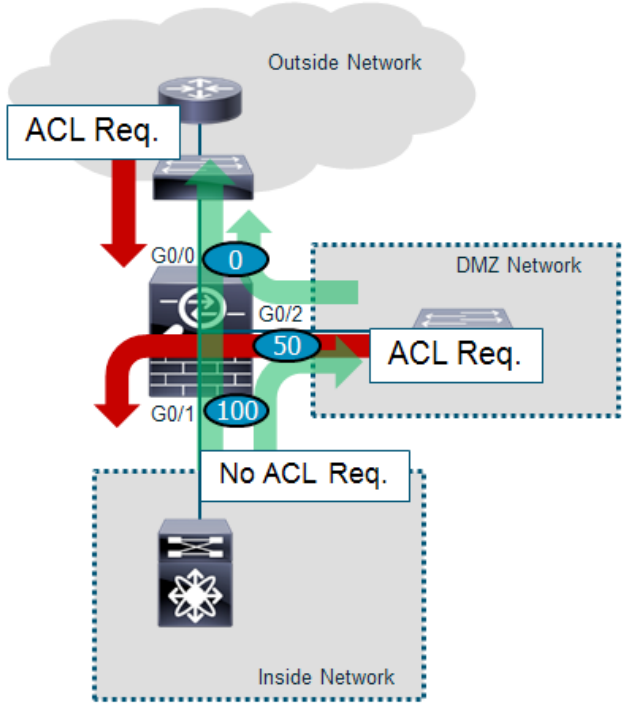
- Like Cisco IOS, ACLs are processed from top down, sequentially with an implicit deny all at the bottom
  - A criteria match will cause the ACL to be exited
- ACLs can be enabled/disabled based on time ranges
- ACLs are made up of Access Control Entries (ACE)
  - Remarks can be added per ACE or ACL
  - ACE may include objects such as user/group, SGT, etc.
- ASA references the 'Real-IP' in ACLs



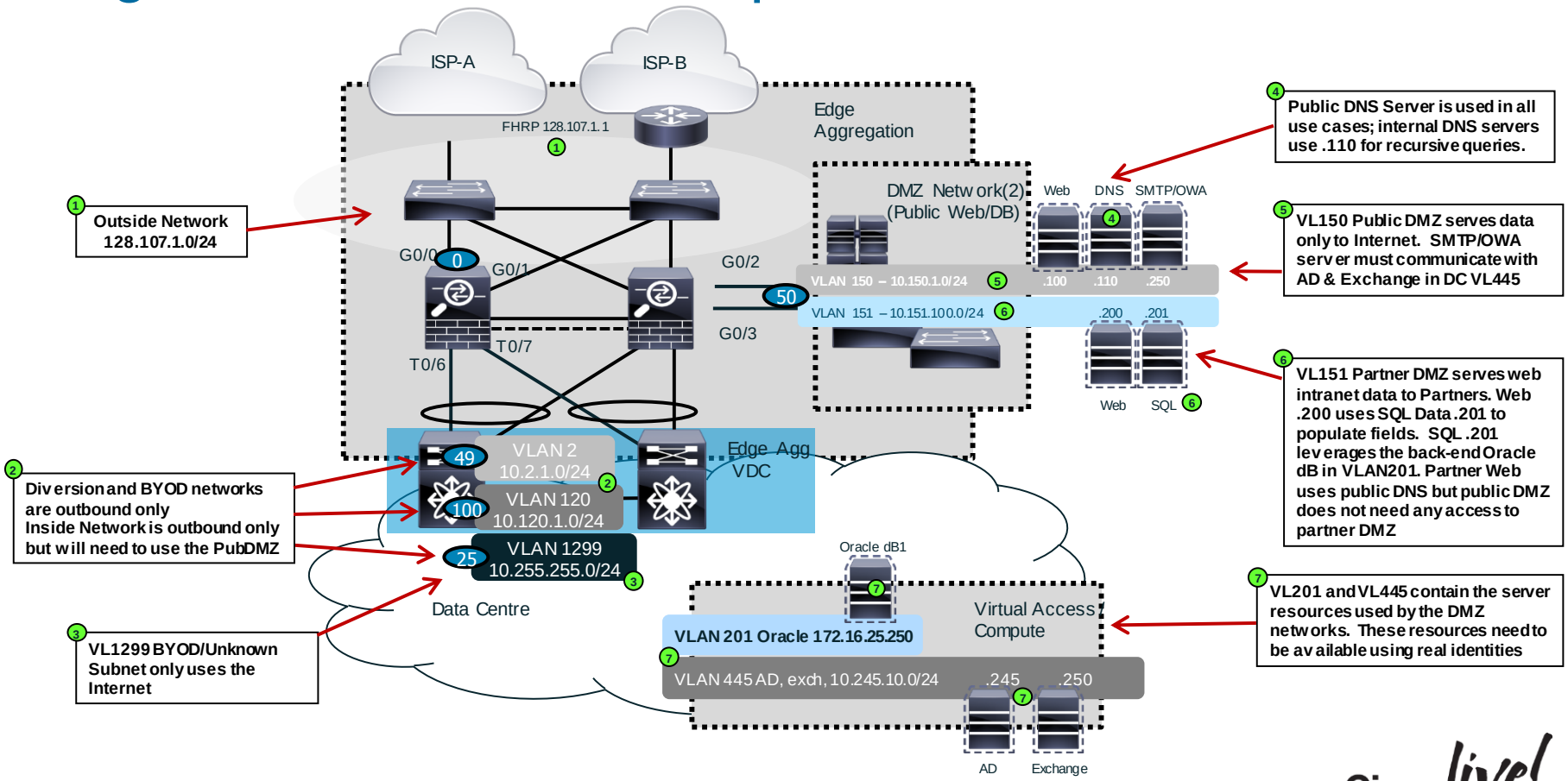
Access Control Lists

- 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 can be enabled/disabled based on time ranges
- ACLs are made up of Access Control Entries (ACE)
  - Remarks can be added per ACE or ACL
  - ACE may include objects such as user/group, SGT, etc.
- ASA references the 'Real-IP' in ACLs

Type	Description
Standard	Used for routing protocols, not firewall rules
Extended	Source/destination port and protocol + User/Group/URL-FQDN /SGT
Ethertype	Used with transparent mode
Webtype	Used for clientless SSL VPN



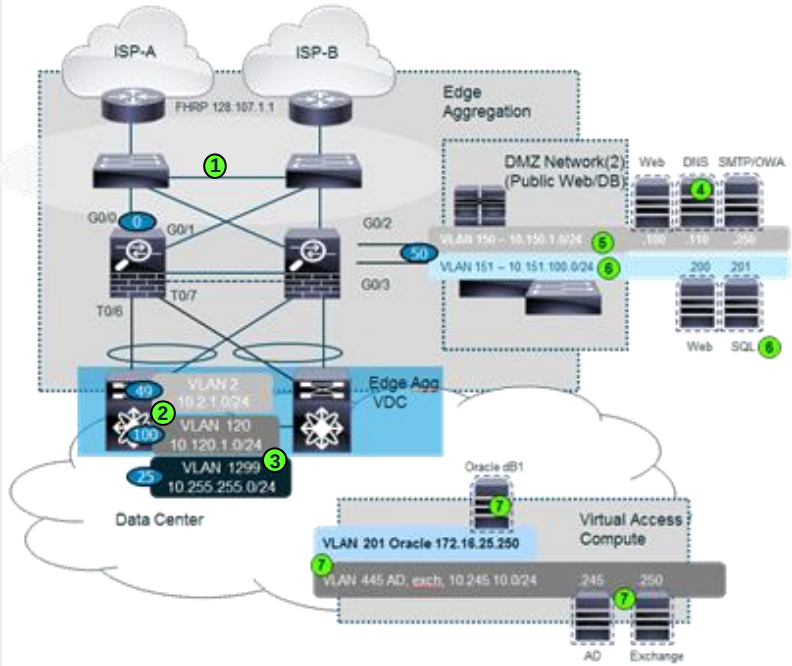
Edge ACL Use Case Requirements



Deploying the ACLs on the Edge ASA

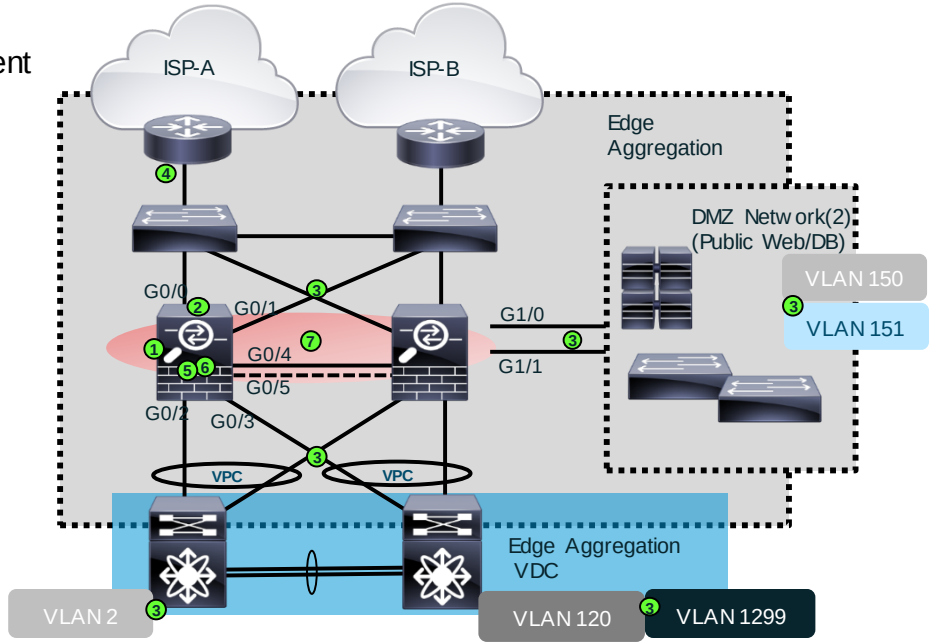
Example Pub-DMZ Use-Cases

```
access-list inet-pubdmz permit tcp any obj obj-pubWEB1-Real eq 80
access-list inet-pubdmz permit tcp any obj obj-pubWEB1-Real eq 443
access-list inet-pubdmz permit udp any obj obj-pubDNS-Real eq 53
access-list inet-pubdmz permit tcp any obj obj-pubMail1-Real eq 443
access-list inet-pubdmz permit tcp any obj obj-pubMail1-Real eq 25
access-group inet-pubdmz in interface outside

object network obj-IntDNS1-Real
  host 10.245.10.245
object network obj-IntDNS2-Real
  host 10.245.10.246
Object-group network obj-IntDNS
  network-object object obj-IntDNS1-Real
  network-object object obj-IntDNS2-Real

access-list pubdmz-inside permit udp obj obj-pubDNS-Real eq 53 obj obj-
   intDNS eq 53
access-list pubdmz-inside permit tcp obj obj-pubMail1-Real obj obj-
   EXCH1-Real eq 80
access-list pubdmz-inside permit tcp obj obj-pubMail1-Real obj obj-
   EXCH1-Real eq 443
access-list pubdmz-inside permit tcp obj obj-pubMail1-Real obj obj-
   EXCH1-Real eq 25
---input truncated---
access-group pubdmz-inside in interface pubdmz
```



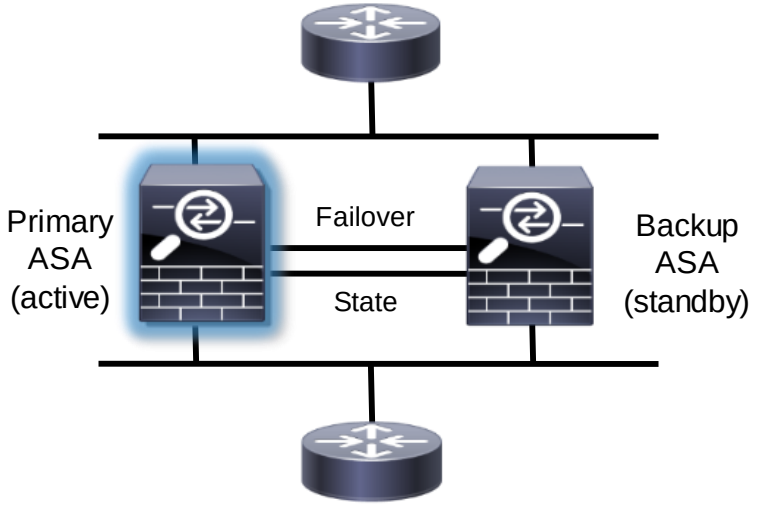
ASA Deployment Checklist – Summary

- **On Primary ASA: (after initial setup)**
  - ✓ 1 – Determine deployment mode –routed or transparent or both (mode multi)
  - ✓ 2 – Examine Interface Security logic
  - ✓ 3 – Interface Configuration(s)
    - EtherChannel / LACP / Redundant
    - Nameif / Security-level / IP addressing
    - VLAN tagging / sub-interfaces / trunk
  - ✓ 4 – Routing
    - Default route / static / routing protocols
  - ✓ 5 – NAT
    - Static and Dynamic Translations
    - Auto NAT & Twice NAT
  - ✓ 6 – ACLs
    - Interface ACLs
    - Global ACLs
    - ACL Simplification methods
- **Implement HA**
  - 7 – A/S, A/A or Clustering



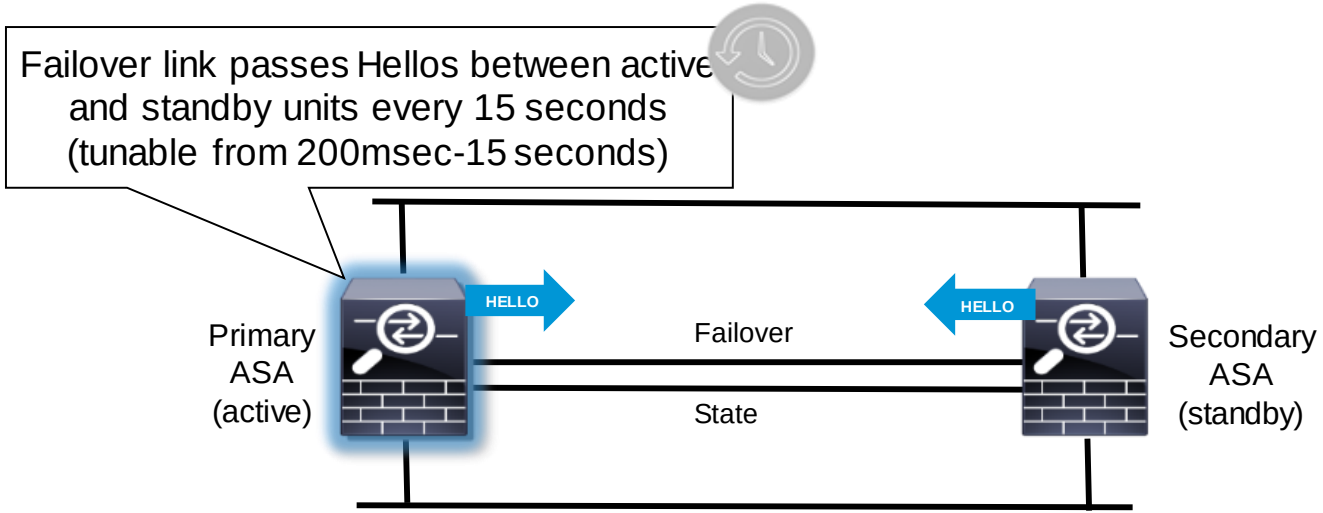
Firewall HA - Active/Standby

- Supported on all models including ASA 5505**
- All features are supported when using A/S including SSLVPN and NGFW/NGIPS
- Both ASAs in pair must be identical in software, memory and interfaces (including SSM/SSP modules) and mode
- Not recommended to share the state and failover link, use a dedicated link for each if possible –x-over or VLAN
- Long distance LAN failover is supported if latency is less than 100ms
- IPv6 HA supported since 8.2.2

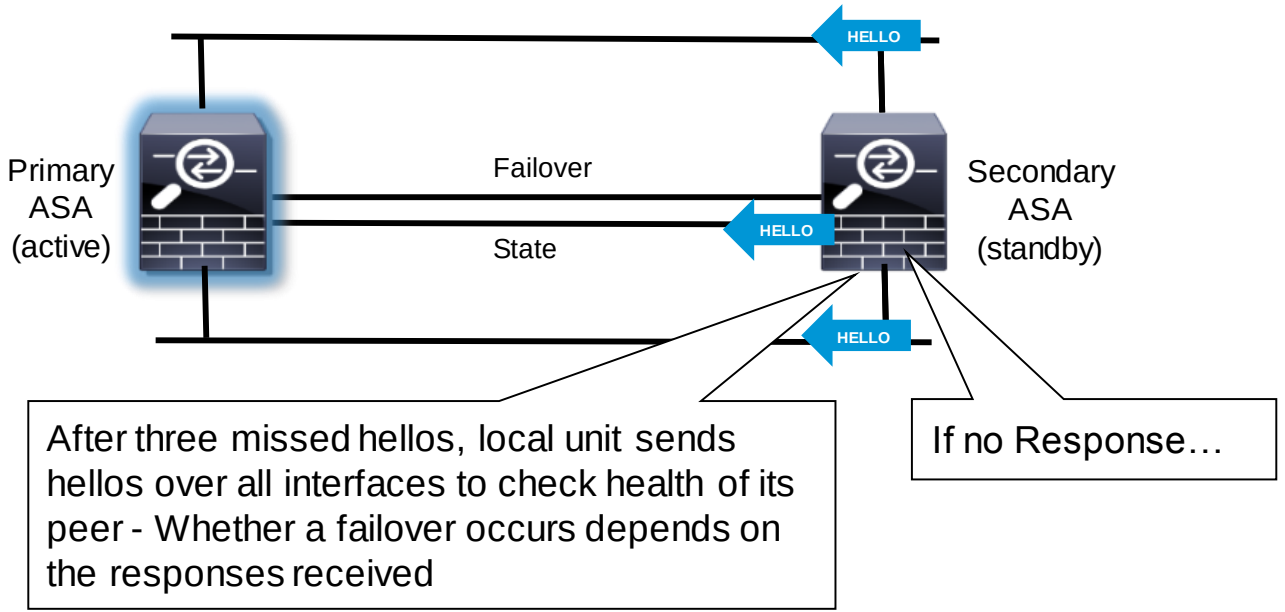


**ASA 5505 only supports stateless failover

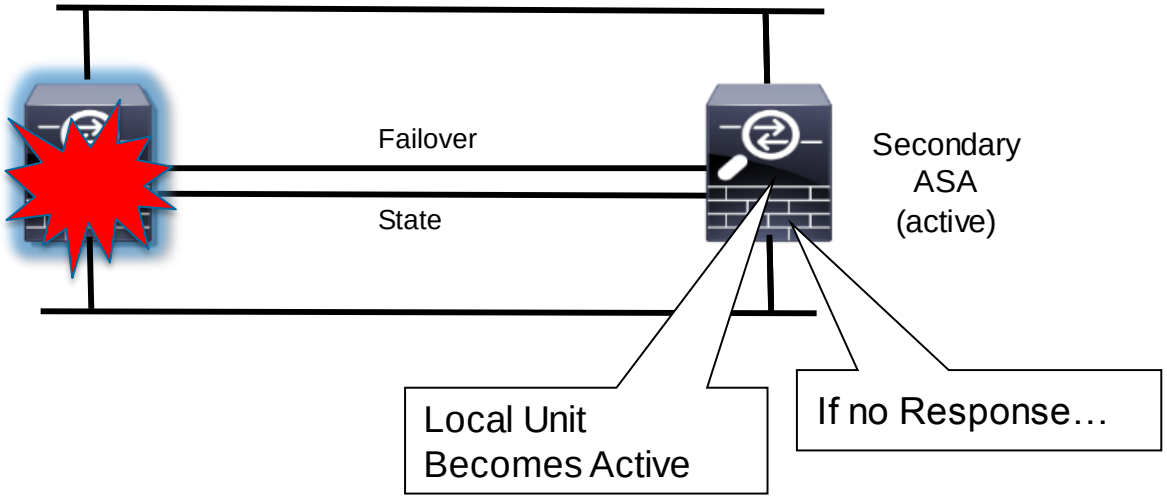
How Failover Works



How Failover Works



How Failover Works



For more details, refer to the Configuration Guide:
http://www.cisco.com/c/en/us/td/docs/security/asa/asa93/configuration/general/asa-general-cli/ha-failover.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	Stateful failover for phone proxy
UDP connection states	State information for SSMs (IPS etc.)
ARP Table	DHCP Server Leases
L2 Bridge Table (Transparent Mode)	
HTTP State *	
ISAKMP and IPSEC SA Table	

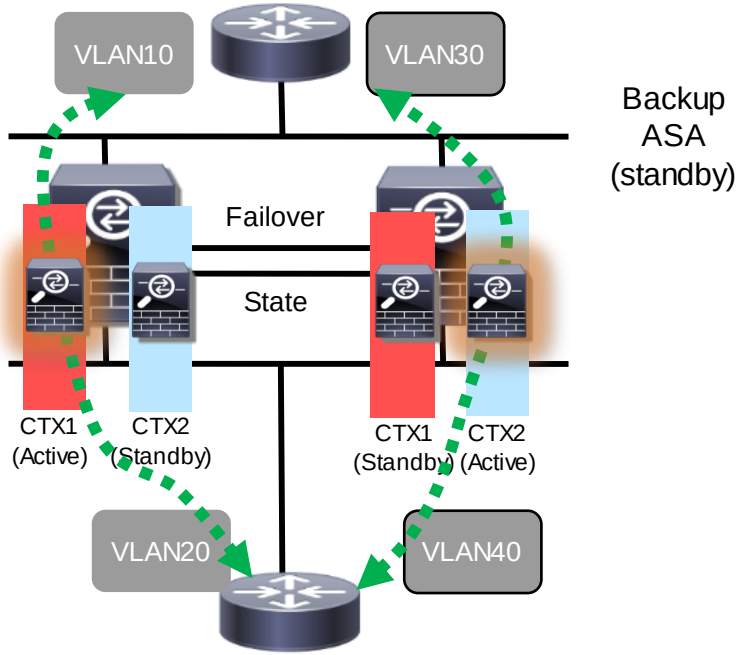
* HTTP State is not passed by default for performance reasons;
enable via `'http replication state'`

New HA Feature: Non-Stop Forwarding (NSF)

- Routing Information Base is replicated in failover and Spanned Etherchannel clustering
  - Active unit or master establish dynamic routing adjacencies and keep standby and slaves up-to-date
  - When the active unit or master fails, the failover pair or cluster continue traffic forwarding based on RIB
  - New active unit or master re-establish the dynamic routing adjacencies and update the RIB
  - Adjacent routers flush routes upon adjacency re-establishment and cause momentary traffic black holing
- Non Stop Forwarding (NSF) and Graceful Restart (GR) support in **ASA 9.3(1)**
  - Cisco or IETF compatible for OSPFv2, OSPF3; RFC 4724 for BGPv4
  - ASA notifies compatible peer routers after a switchover in failover or Spanned Etherchannel clustering
  - ASA acts as a helper to support a graceful or unexpected restart of a peer router in all modes

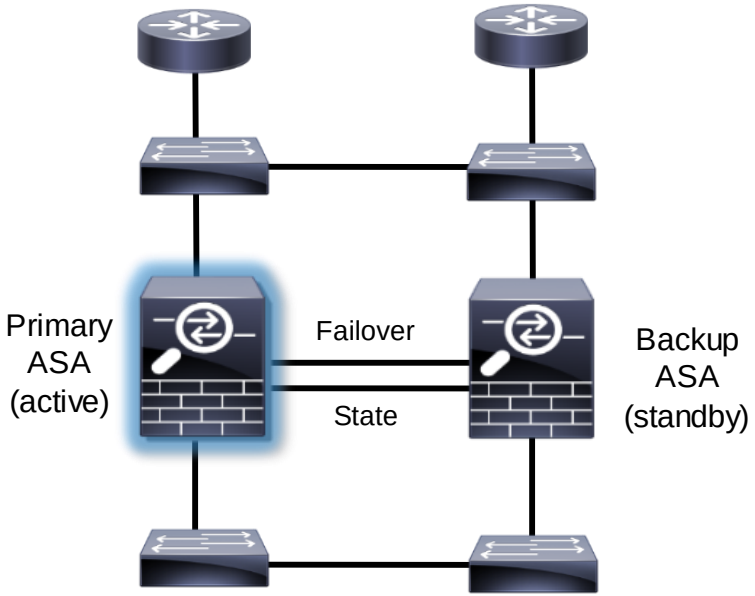
Firewall HA: Active/Active Failover

- Active-Active is 2 reciprocal pairs of Active-Standby Virtual Firewalls
- Requires virtualisation (Multi-Context) which (may) require additional licensing
- Virtualisation does not yet support SSLVPN/Remote Access VPN
- No load-balancing or load-sharing support
  - Not true Active/Active flow
    - True Active/Active flow accomplished with ASA Clustering
  - Subnet/VLAN can only be active on one node at a time
- Works well for high-density service chassis (ASA SM) deployments, where you could manually split the VLANs between chassis/line cards

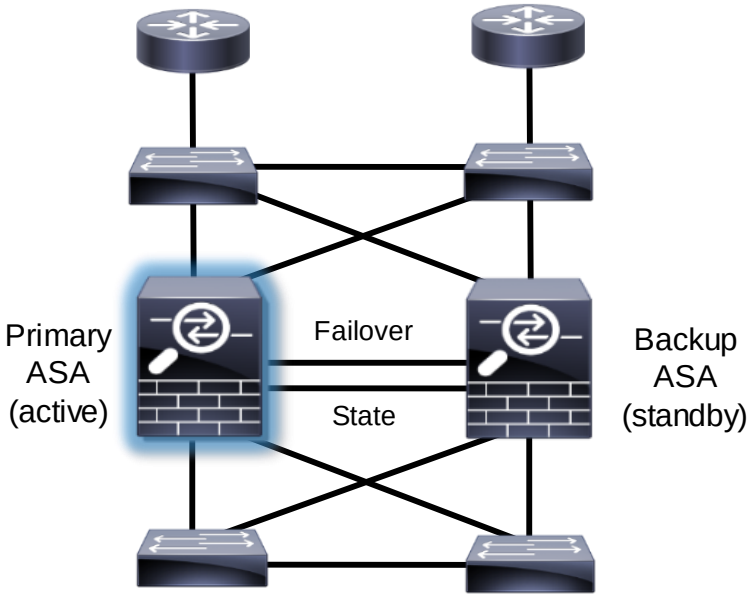


HA with Interface Redundancy

Before…

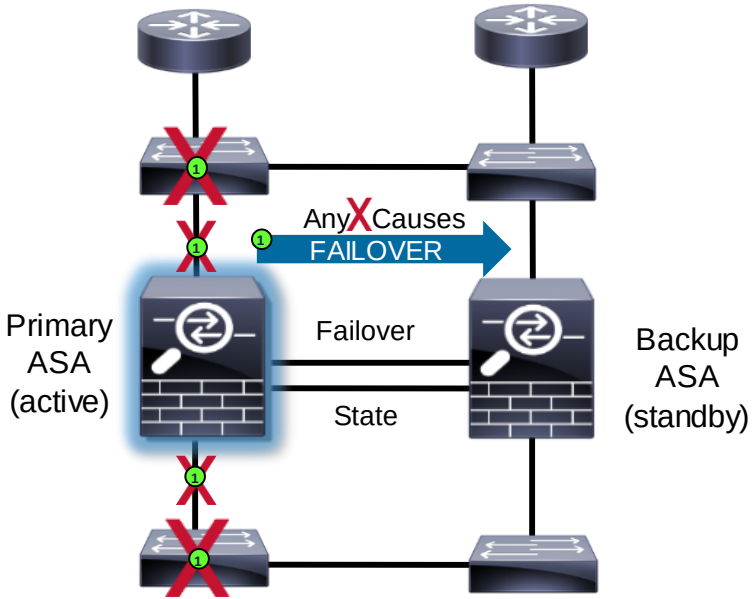


After with redundant interfaces

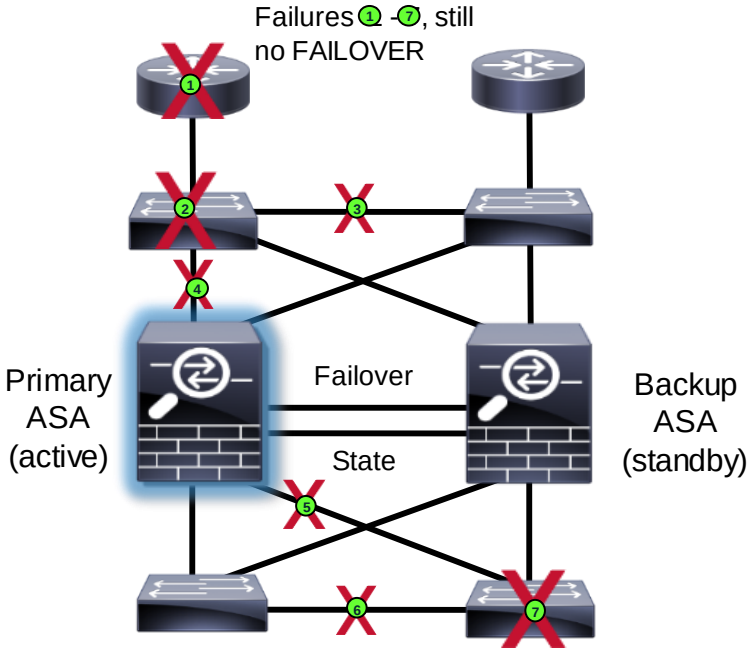


HA with Interface Redundancy

Before…



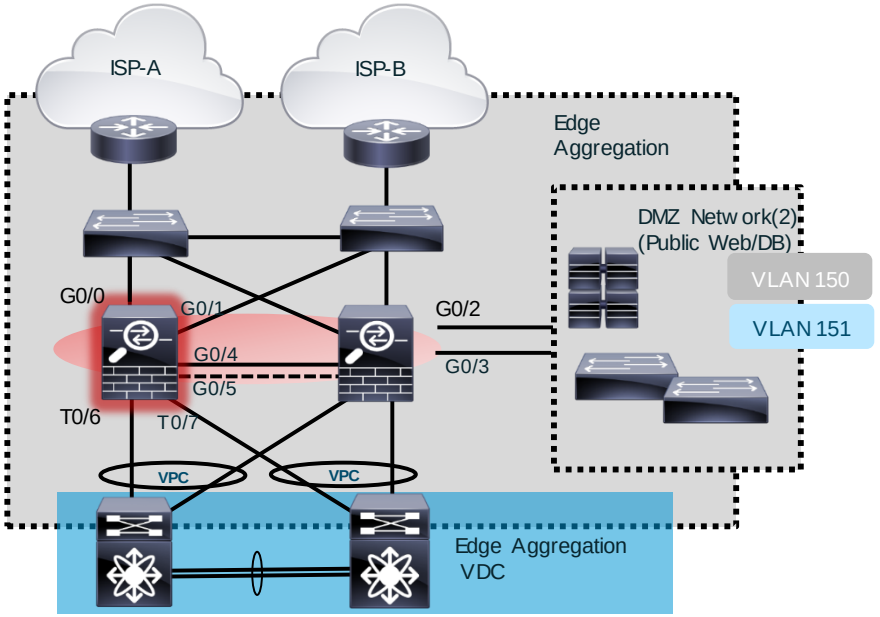
After with redundant interfaces



Port Channel feature makes this concept somewhat obsolete if switches support VSS/vPC

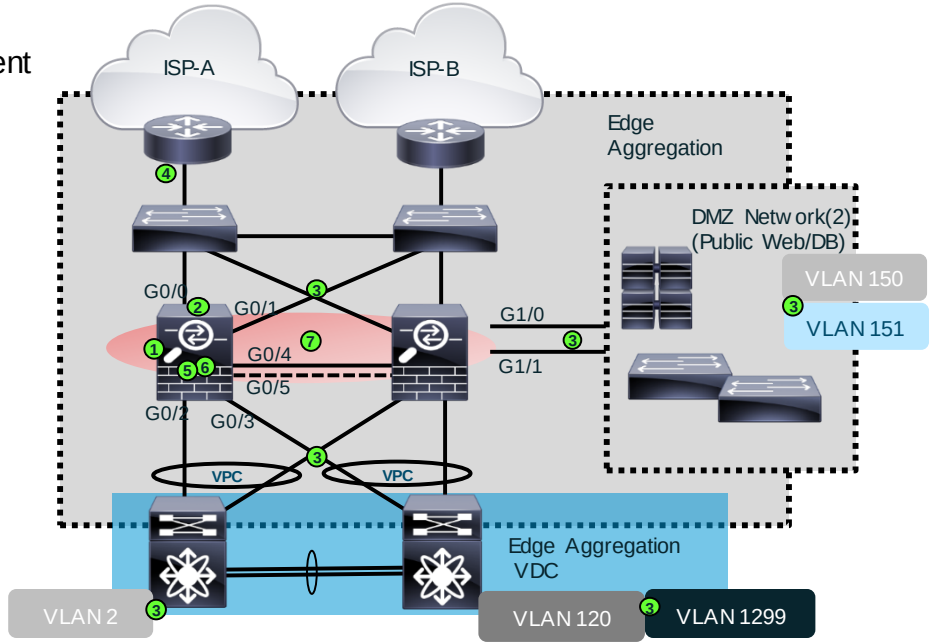
Deploying A/S Failover

```
failover
failover lan unit primary
failover lan interface failover g0/5
failover lan enable
failover key ******
failover replication http
failover polltime 3
failover link state g0/4
failover interface ip failover 99.99.99.1 standby 99.99.99.2
failover interface ip state 100.100.100.1 255.255.255.0 standby
100.100.100.2
!inside interfaces
interface port-channel10.120
 ip address  10.120.1.254 255.255.255.0 standby 10.120.1.253
interface port-channel10.2
 ip address  10.2.1.254 255.255.255.0 standby 10.2.1.253
interface port-channel10.1299
 ip address  10.255.255.254 255.255.255.0 standby 10.255.255.253
! outside interface
interface redundant1
 ip address  128.107.1.128 255.255.255.0 standby 128.107.1.129
! dmz interfaces
interface Redundant1.150
 ip address  10.150.1.254 255.255.255.0 standby 10.150.1.253
interface Redundant1.151
 ip address  10.151.100.254 255.255.255.0 standby 10.151.100.253
```



ASA Deployment Checklist – Summary

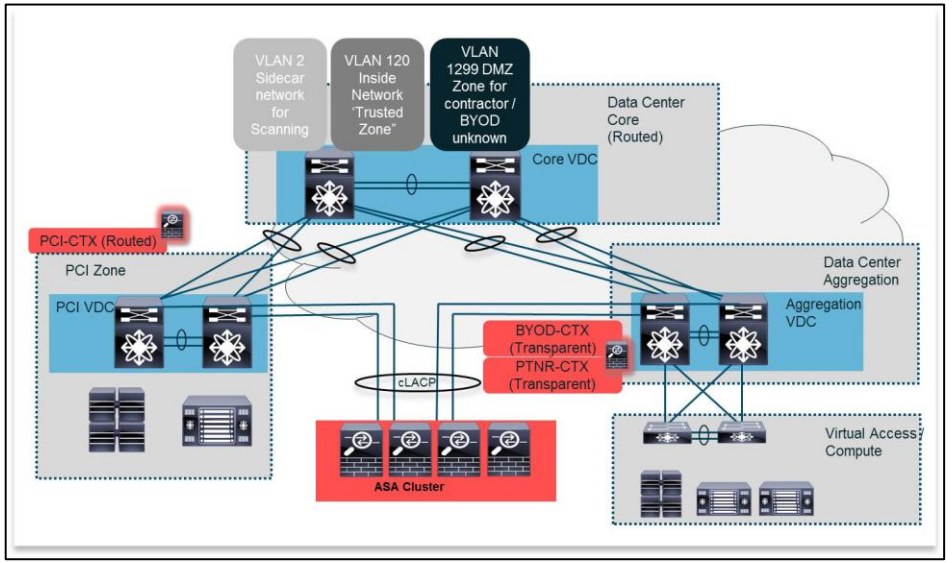
- **On Primary ASA: (after initial setup)**
  - ✓ 1 – Determine deployment mode –routed or transparent or both (mode multi)
  - ✓ 2 – Examine Interface Security logic
  - ✓ 3 – Interface Configuration(s)
    - EtherChannel / LACP / Redundant
    - Nameif / Security-level / IP addressing
    - VLAN tagging / sub-interfaces / trunk
  - ✓ 4 – Routing
    - Default route / static / routing protocols
  - ✓ 5 – NAT
    - Static and Dynamic Translations
    - Auto NAT & Twice NAT
  - ✓ 6 – ACLs
    - Interface ACLs
    - Global ACLs
    - ACL Simplification methods
- **Implement HA**
  - ✓ 6 – A/S, A/A



Deploying the ASA Cluster in Transparent L2 Firewall Contexts in the Data Centre

ASA Deployment Checklist (Data Centre)

- **Specific Items for ASA in the Data Centre**
  - ① – Verify deployment mode –routed or transparent or both (mode multi)
  - ② – Create Virtualised Firewalls where applicable
    - Multi-context Firewall common, especially for Multi-tenancy
  - ③ – Transparent Mode Firewalls
    - Deploying Transparent Mode
    - How Transparent Mode Works
  - ④ – Comparing Virtual and Physical Firewall Deployments for the DC based upon requirements
- **Implement Clustering**
  - ⑤ – Clustering Basics
  - ⑥ – Clustering deployment in the clinet.com Data Centre
- **Deploying ASAv (Virtual ASA)**
  - ⑦ – ESXI Deployment



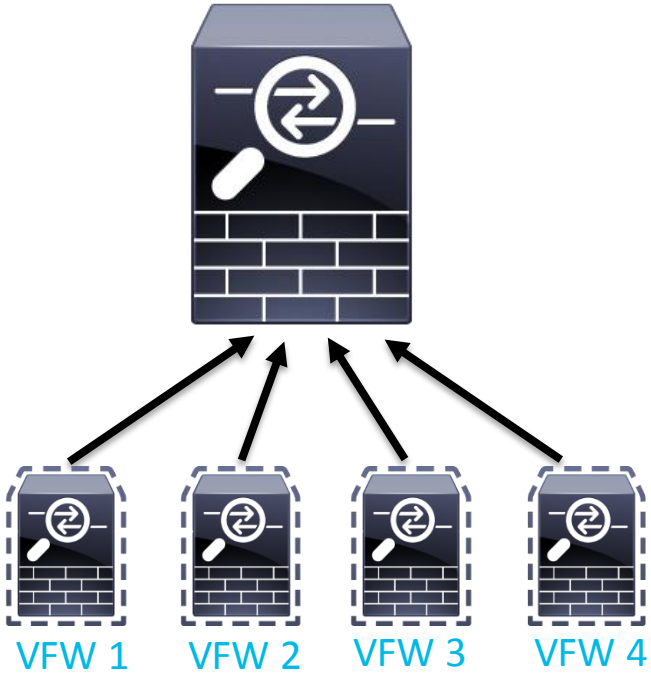
Review: Modes of Operation

- **Routed Mode** is the traditional mode of the firewall. Two or more interfaces that separate L3 domains – Firewall is the Router and Gateway for local hosts
- **Transparent Mode** is where the firewall acts as a bridge functioning at L2
  - Transparent mode firewall offers some unique benefits in the DC
  - Transparent deployment is tightly integrated with our 'best practice' data centre designs

- **Multi-context Mode** involves the use of virtualised firewalls (vFW), which can be either routed or transparent mode
- **Mixed (Multi-context) Mode** is the concept of using multi-context mode to combine routed and transparent mode virtualised firewalls on the same chassis or cluster of chassis'– Any ASA 9.x or Service Modules

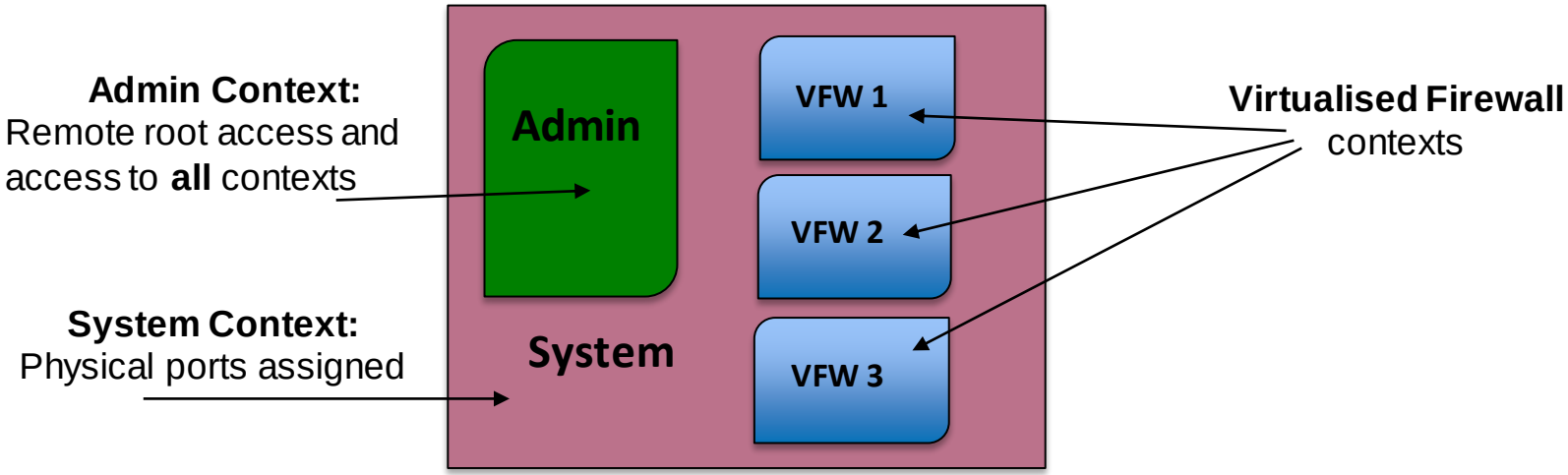
Virtualised Firewalls

- Multiple virtual(ised) firewalls (vFW) in one physical ASA chassis (or Cluster)
  - Meets network separation/ stateful filtering requirement(s) for regulatory compliance / multi-tenant use-cases
- Each virtualised firewall is considered a separate “context”
  - Each context has a separate Control Plane, Data Plane, dedicated config memory space and dedicated interfaces
    - Interfaces are not shared amongst contexts
    - Physical interfaces are mapped to contexts and each context maps to a configuration
  - Each context implements a unique, self-contained policy
- Maximum number of virtualised firewalls in one physical appliance is 250 (licensed feature)
  - Up to 250 vFW in an ASA Cluster



How the Virtualised Firewall is Configured

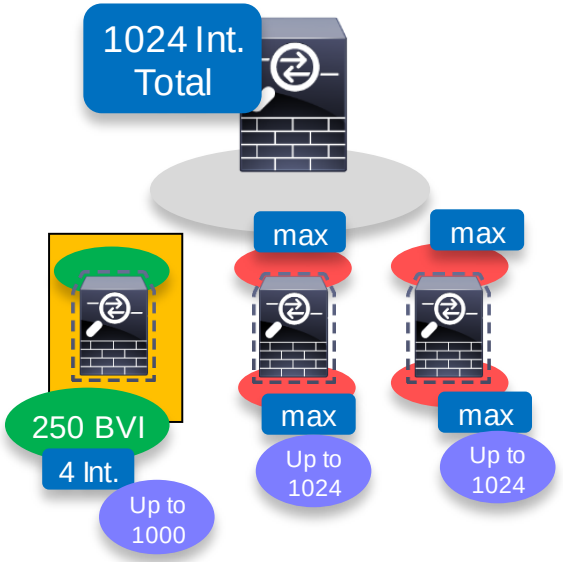
- Context = a virtualised firewall (vFW)
- All virtualised firewall configurations must define a System context and an Admin context



- There is no policy inheritance between contexts

ASA Multi-Context Mode Limits and Restrictions

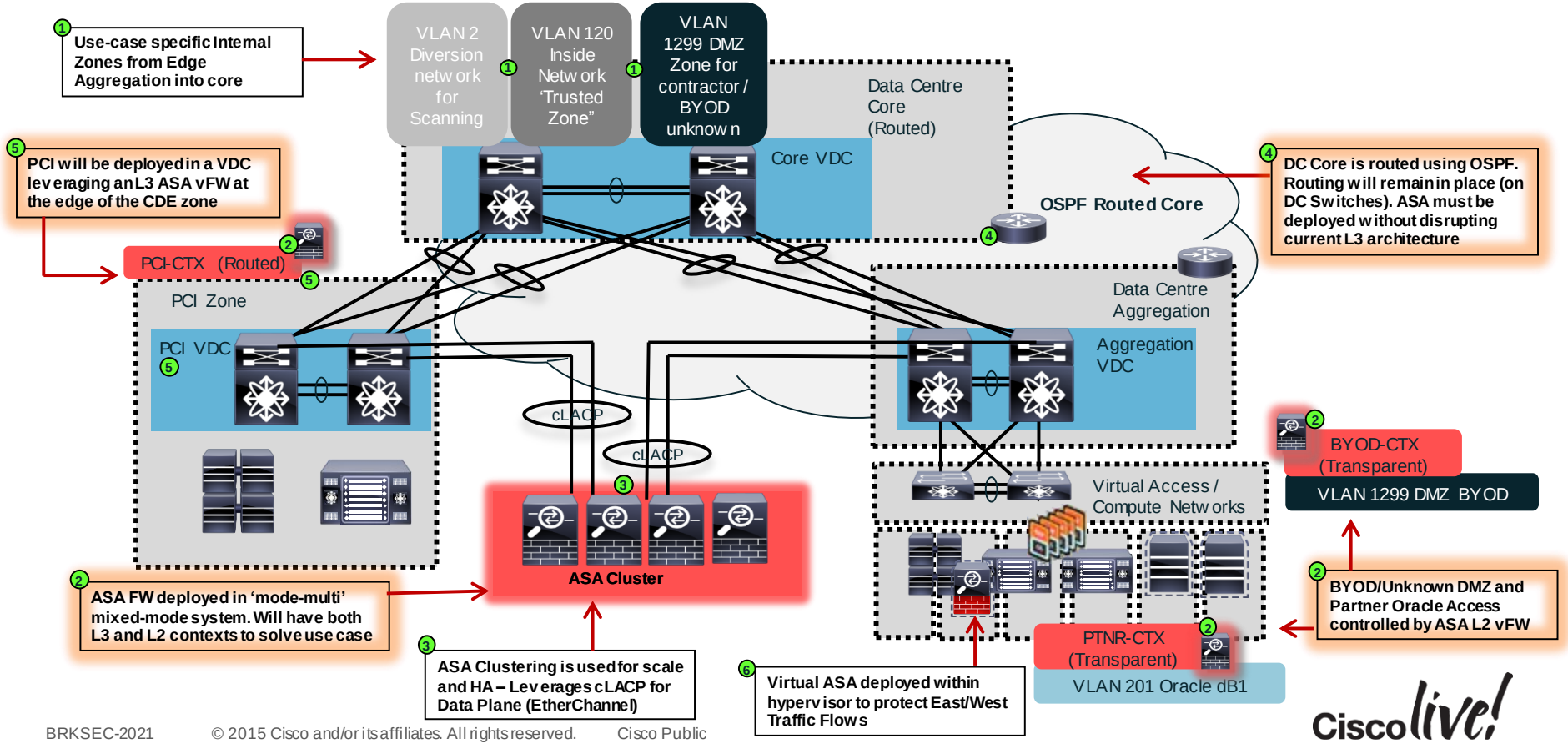
- Limits:
  - ASA physical limit of 1024 total interfaces/VLANs – Each vFW eats some of this total
    - Each transparent mode context is allowed 250 total bridge groups (9.3) each with up to 4 interfaces (VLANs) per context or transparent mode Firewall
    - Each routed-mode context is allowed up to the maximum number of remaining interfaces (of 1024)



- Restrictions:
  - Remote Access VPN is not yet supported (S2S is supported)
  - MAC addresses for virtual interfaces are automatically set to physical interface MAC
  - Admin context can be used for traffic, but grants privileges of whomever manages the Admin context to all other contexts, use with caution

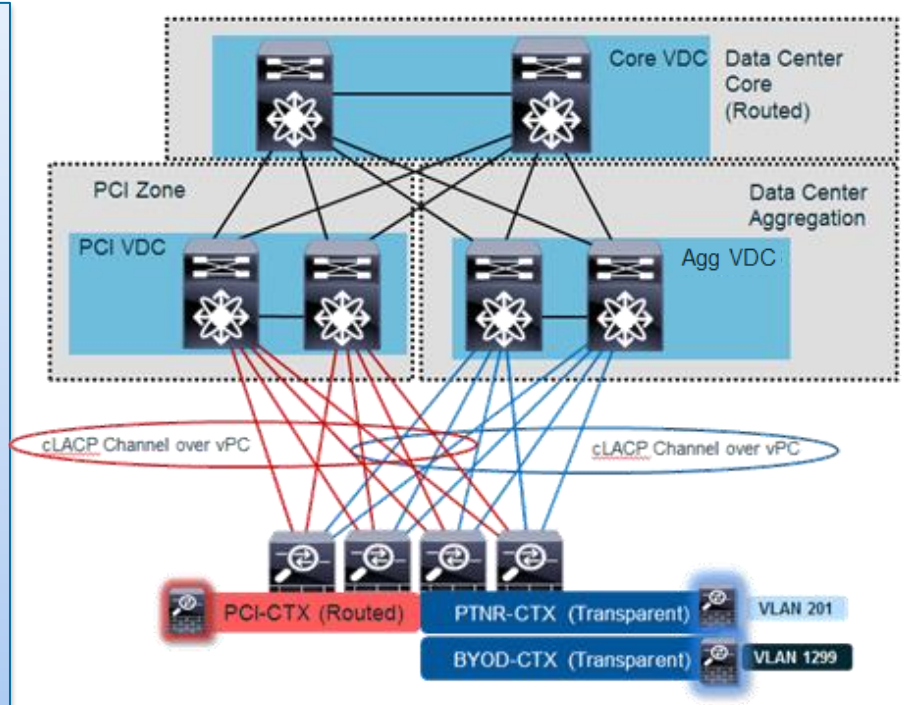
clinet.com Data Centre ASA Deployment

General Requirements



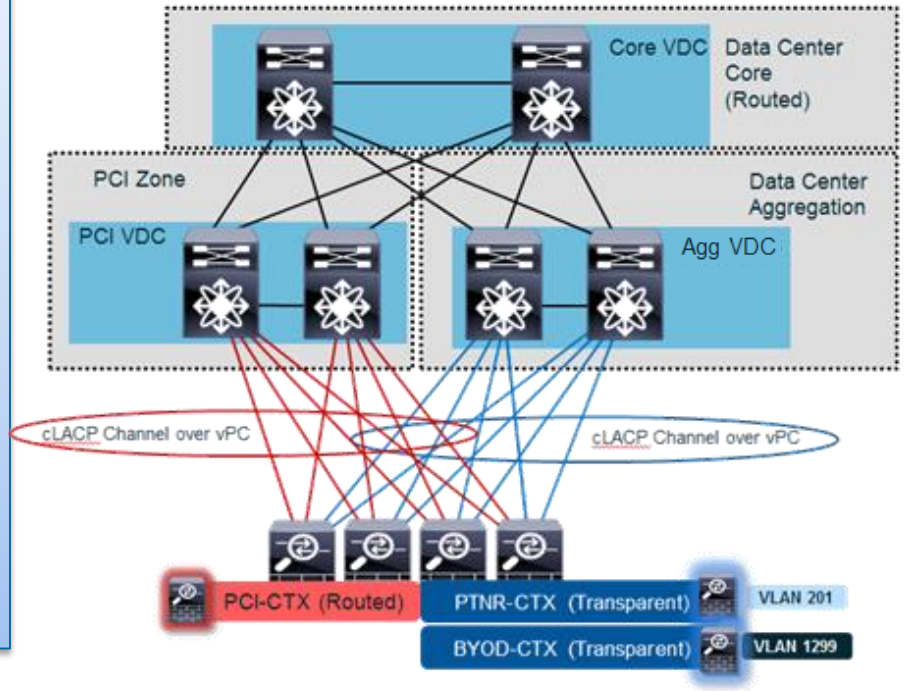
Deploying ASA Multi-Context

```
DC-ASA(config)#
mode multiple
! System Context Configuration
!  Allocate Interfaces for PTNR and BYOD
interface TenGigabitEthernet0/6
 channel-group 32 mode active
interface Po32.200
 vlan 200
interface Po32.201
 vlan 201
interface Po32.1200
 vlan 1200
interface Po32.1299
 vlan 1299
! Interface TenGig0/7 would have same config as T0/6
!
! Allocate Interfaces for PCI
interface TenGigabitEthernet1/0
 channel-group 31 mode active
interface Po31.1000
 vlan 1000
interface Po31.1001
 vlan 1001
! Interface TenGig1/1 would have same config as T1/0
! Allocate Interfaces for Cluster Control / Management
interface TenGigabitEthernet1/6
interface TenGigabitEthernet1/7
interface Management0/0
```



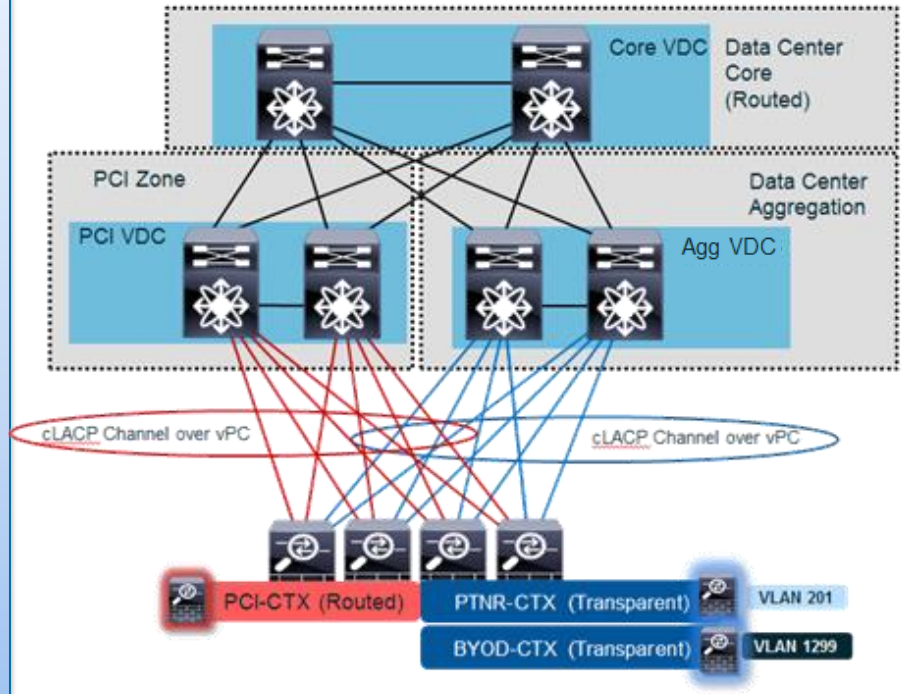
Deploying ASA Multi-Context (with Mixed Modes)

```
! Context Configuration
admin-context admin
context admin
  allocate-interface Management0/0
  config-url disk0:/admin.cfg
!
context PTNR-CTX
  !firewall transparent mode must be specified in the context
  allocate-interface Po32.200 oracle-txn
  allocate-interface Po32.201 oracle-net
  config-url disk0:/ptnr-ctx.cfg
!
context BYOD-CTX
  !firewall transparent mode must be specified in the context
  allocate-interface Po32.1200 byod-host
  allocate-interface Po32.1299 byod-list
  config-url disk0:/byod.cfg
!
context PCI-CTX
  allocate-interface Po31.1000 pci-outside
  allocate-interface Po31.1001 pci-inside
  config-url disk0:/pci-ctx.cfg
```



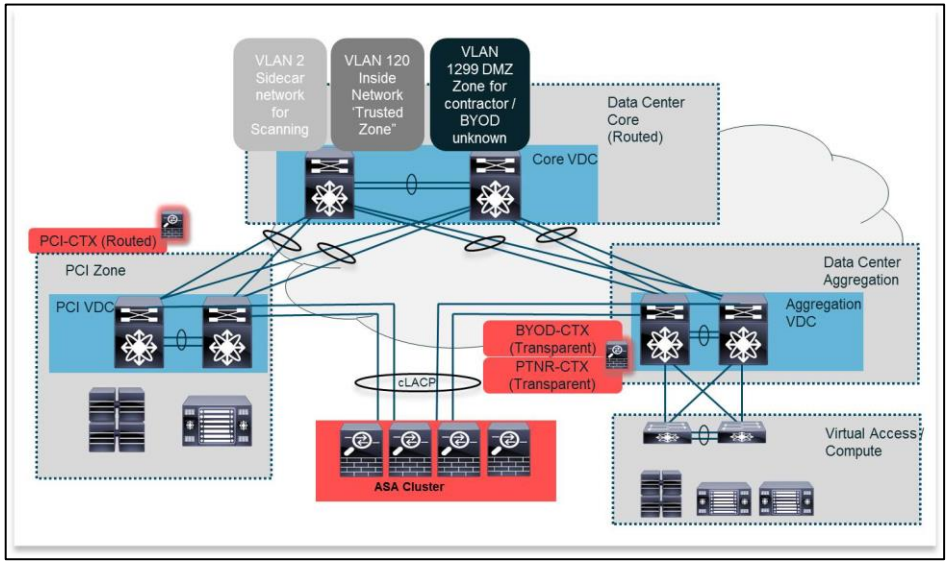
Deploying ASA Multi-Context

```
DC-ASA#

changeto context PTNR-CTX

DC-ASA/PTNR-CTX# show run

ASA Version 9.1
!
hostname PTNR-CTX
enable password 8Ry2YjIyt7RRXU24 encrypted
!
interface oracle-txn
 nameif outside
 security-level 0
 bridge-group 1
!
interface oracle-net
 nameif inside
 security-level 100
 bridge-group 1
!
interface bvi1
 ip address 172.16.25.253 255.255.255.0
```



ASA Deployment Checklist (Data Centre)

- **Specific Items for ASA in the Data Centre**
  - ✓ 1 – Verify deployment mode –routed or transparent or both (mode multi)
  - ✓ 2 – Create Virtualised Firewalls where applicable
    - Multi-context Firewall common, especially for Multi-tenancy
  - 3 – Transparent Mode Firewalls
    - Deploying Transparent Mode
    - How Transparent Mode Works
  - 4 – Comparing Virtual and Physical Firewall Deployments for the DC based upon requirements
- **Implement Clustering**
  - 5 – Clustering Basics
  - 6 – Clustering deployment in the clinet.com Data Centre
- **Deploying ASAv (Virtual ASA)**
  - 7 – ESXI Deployment



Review: 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 at L2
  - Transparent mode firewall offers some unique benefits in the DC

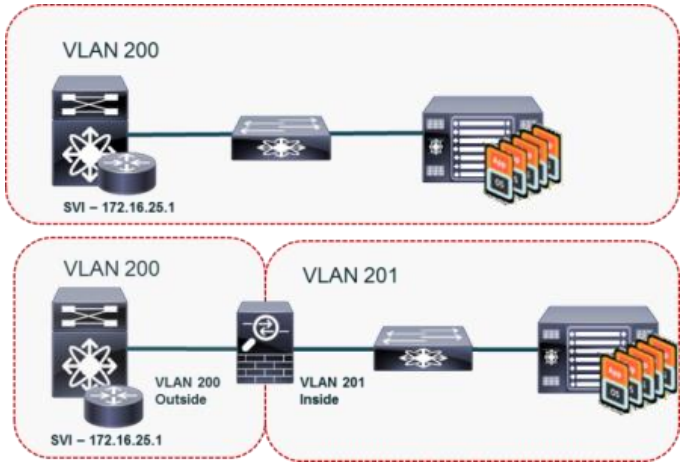
- **Multi-context** mode involves the use of virtual firewalls (vFW), which can be either routed or transparent mode
- **Mixed mode** is the concept of using virtualisation to combine routed and transparent mode virtual firewalls – ASA 9.x or Service Modules

Why Deploy Transparent Mode?

- Very popular architecture in data centre environments
- Existing Nexus/DC Network Fabric does not need to be modified to employ L2 Firewall!
  - Simple as changing host(s) VLAN ID
- Firewall does not need to run routing protocols / become a segment gateway
- Firewalls are more suited to flow-based inspection (not packet forwarding like a router)
  - 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)
- (CVD) most internal DC zoning scenarios recommend Transparent FW (L2) deployed versus Routed Firewall (L3)
  - L3 Use-cases still valid, especially in Multi-tenant and Secure Enclave architectures

Firewall - Transparent Mode

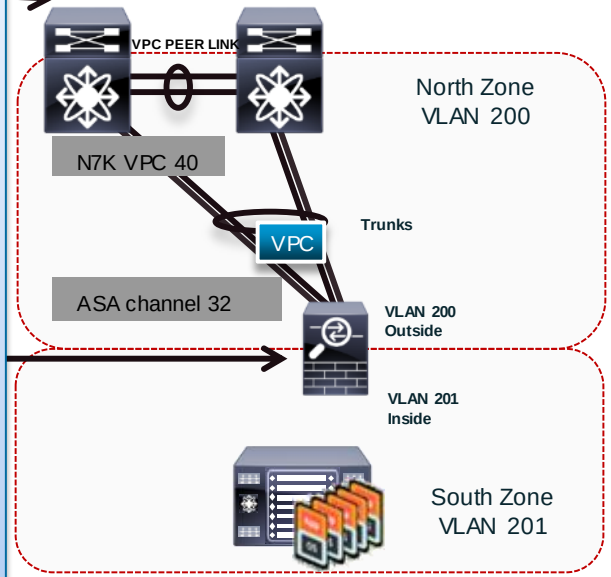
- Firewall functions like a bridge (“bump in the wire”) at L2
  - only ARP packets pass without an explicit ACL
- Full policy functionality is included, NAT, ACLs, Service Policy, NGFW/NGIPS, etc.
- Same subnet exists on all interfaces in the bridge-group
- Different VLANs on inside and outside interfaces
- Focus on specific ‘use-case’ when deploying transparent mode



ASA Connecting to Nexus with vPC (basic)

```
! NEXUS 7K Config
! Only one side of Configuration shown
interface Ethernet4/1
switchport mode trunk
channel-group 40 mode active
no shutdown
!
interface Ethernet4/2
switchport mode trunk
channel-group 40 mode active
no shutdown
!
interface port-channel40
switchport
switchport mode trunk
switchport trunk allowed vlan 1,200,201
vpc 40
!
vpc domain 10
 role priority 50
 peer-keepalive dest 10.1.1.2 source 10.1.1.1
vrf vpc-mgmt peer-gateway
```

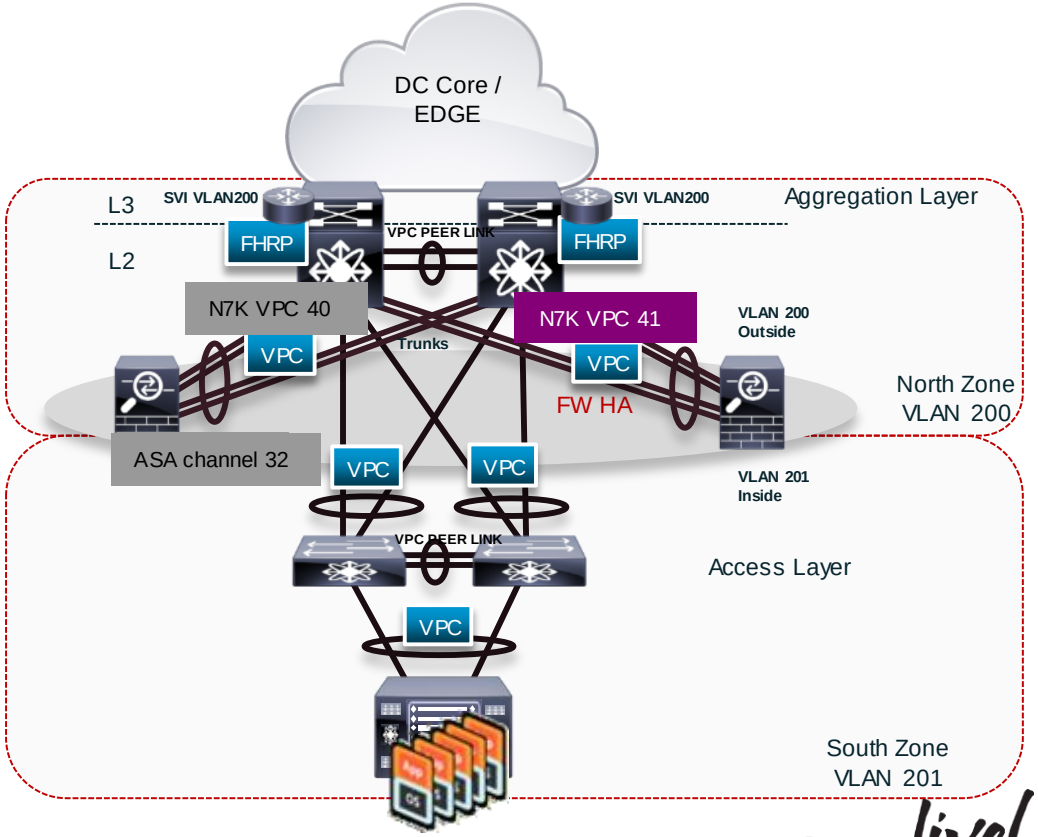
```
interface TenGigabitEthernet0/6
channel-group 32 mode active vss-id 1
no nameif
no security-level
!
interface TenGigabitEthernet0/7
channel-group 32 mode active vss-id 2
no nameif
no security-level
!
interface BVI1
ip address 172.16.25.86 255.255.255.0
!
interface Port-channel32
 no nameif
 no security-level
!
interface Port-channel32.201
 mac-address 3232.1111.0201
 vlan 201
 nameif inside
 bridge-group 1
 security-level 100
!
interface Port-channel32.200
 mac-address 3232.1111.0200
 vlan 200
 nameif outside
 bridge-group 1
 security-level 0
```



ASA Connecting to Nexus with vPC

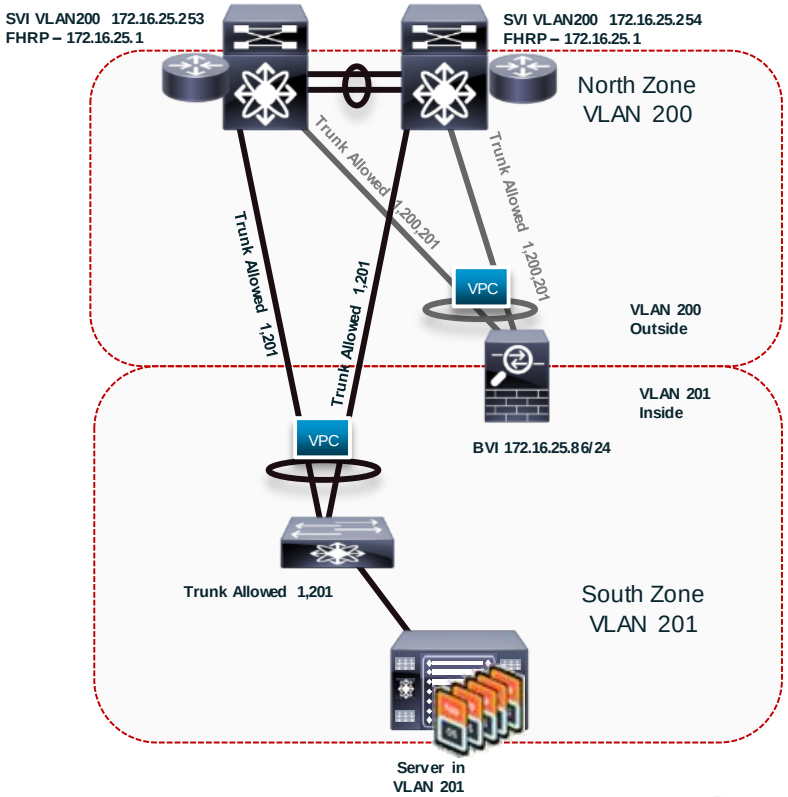
(Best Practices Shown)

- ASA connected to Nexus using multiple physical interfaces on vPC
  - ASA can be configured to failover after a certain number of links lost (when using HA over LAG)
- Note that vPC identifiers are different for each ASA on the Nexus switch **when using standard HA** (this changes with ASA clustering feature and cLACP [not yet shown])



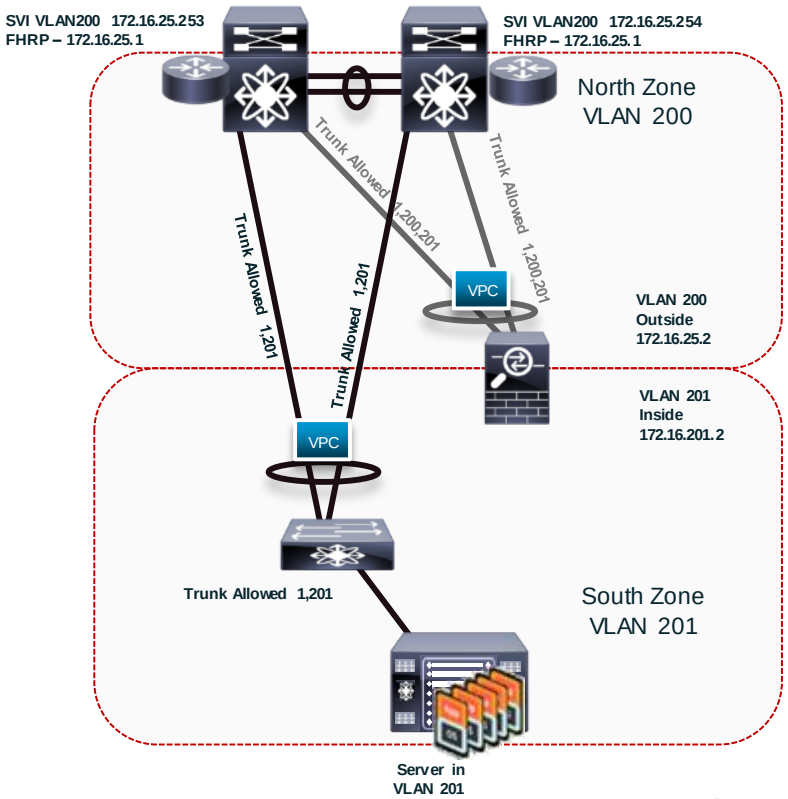
Transparent Mode Configuration in the DC (2 Interfaces)

```
interface TenGigabitEthernet0/6
channel-group 32 mode active vss-id 1
no nameif
no security-level
!
interface TenGigabitEthernet0/7
channel-group 32 mode active vss-id 2
no nameif
no security-level
!
interface BVI1
ip address 172.16.25.86 255.255.255.0
!
interface Port-channel32
 no nameif
 no security-level
!
interface Port-channel32.201
 mac-address 3232.1111.0201
 vlan 201
 nameif inside
 bridge-group 1
 security-level 100
!
interface Port-channel32.200
 mac-address 3232.1111.0200
 vlan 200
 nameif outside
 bridge-group 1
 security-level 0
```



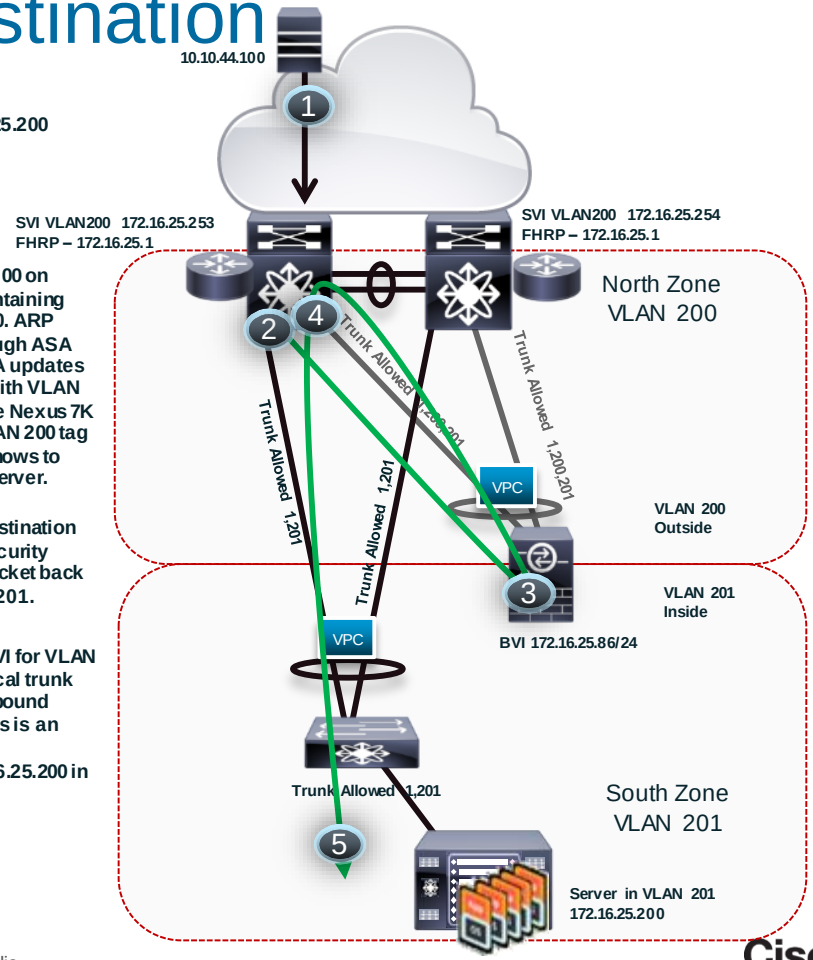
L3 Configuration in the DC (2 Interfaces)

```
interface TenGigabitEthernet0/6
channel-group 32 mode active vss-id 1
no nameif
no security-level
!
interface TenGigabitEthernet0/7
channel-group 32 mode active vss-id 2
no nameif
no security-level
!
interface Port-channel32
 no nameif
 no security-level
!
interface Port-channel32.201
 mac-address 3232.1111.0201
 vlan 201
 ip address 172.16.201.2 255.255.255.0
 nameif inside
 security-level 100
!
interface Port-channel32.200
 mac-address 3232.1111.0200
 vlan 200
 nameif outside
 ip address 172.16.25.2 255.255.255.0
 security-level 0
```



ASA L2 Mode: Local Destination

1. Session Request to server 172.16.25.200 from source 10.10.44.100
2. ARP request (or Lookup) 172.16.25.200 on VLAN 200– ARP Reply from ASA containing local MAC (outside) on VLAN tag 200. ARP request packet actually passes through ASA and on return trip to the N7K the ASA updates its MAC table with the server MAC with VLAN 201 (Inside). It forwards a reply to the Nexus 7K with the same server MAC and a VLAN 200 tag (rewritten). This is how the Nexus knows to direct traffic thru the ASA to reach server.
3. ASA receives packet with Server destination 172.16.25.200 and processes the Security policy. If allowed, it forwards the packet back to the Nexus 7K with a VLAN tag of 201.
4. Since Nexus 7K does not have an SVI for VLAN 201, it forwards packets across it local trunk which allows VLAN 201 tag – southbound towards the 5K. Source MAC address is an actual server MAC address
5. Request is delivered to Server 172.16.25.200 in VLAN 201



ASA L2 Mode: Remote Destination

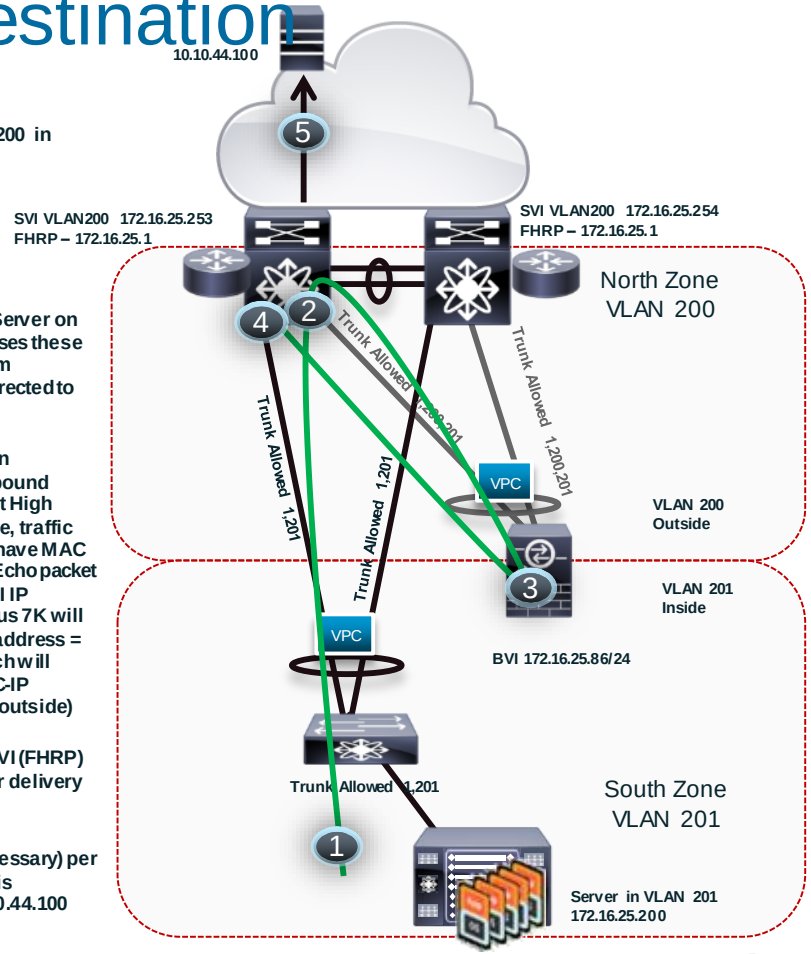
1. Return path from server 172.16.25.200 in VLAN 201 to remote destination 10.10.44.100

2. Packet received on Nexus 7K from Server on VLAN 201. MAC in table that processes these packets is ASA inside interface (from southbound example) Traffic is redirected to ASA (inside) VLAN tag 201

3. ASA receives packet with destination 10.10.44.100 and processes the outbound Security policy (if any). Since default High Trust interface to Low Trust interface, traffic should be allowed. If ASA does not have MAC Address in table, it sends an ICMP-Echo packet to 10.10.44.100 (sourced from its BVI IP Address) with TTL=1. FHRP on Nexus 7K will respond with Time Exceeded, MAC address = FHRP MAC VLAN 200 (Outside) which will update ASA MAC table with the MAC-IP Mapping of Nexus 7K on VLAN 200 (outside)

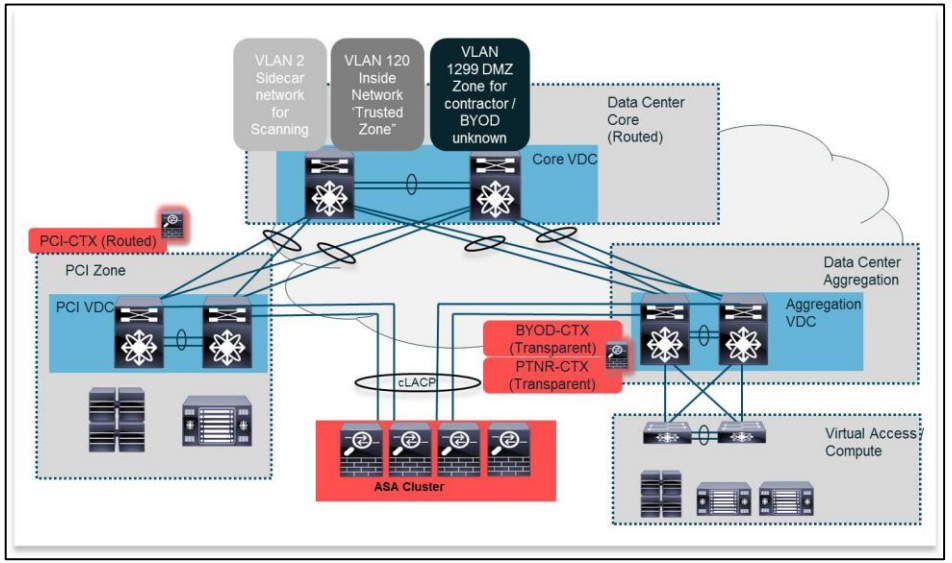
4. ASA forwards packet to Nexus 7K SVI (FHRP) address 172.16.25.1 on VLAN 200 for delivery to destination 10.10.44.100

5. Nexus executes ARP request (if necessary) per standard routing function. Request is forwarded towards destination 10.10.44.100



ASA Deployment Checklist (Data Centre)

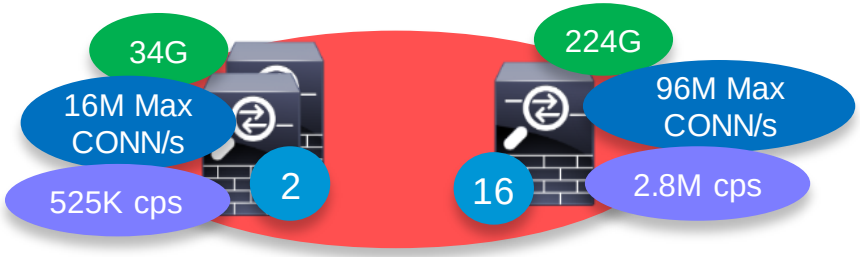
- **Specific Items for ASA in the Data Centre**
  - ✓ 1 – Verify deployment mode –routed or transparent or both (mode multi)
  - ✓ 2 – Create Virtualised Firewalls where applicable
    - Multi-context Firewall common, especially for Multi-tenancy
  - ✓ 3 – Transparent Mode Firewalls
    - Deploying Transparent Mode
    - How Transparent Mode Works
- **Implement Clustering**
  - 4 – Clustering Basics
  - 5 – Clustering deployment in the clinet.com Data Centre
  - 6 – Comparing Virtual and Physical Firewall Deployments for the DC based upon requirements
- **Deploying ASAv (Virtual ASA)**
  - 7 – ESXI Deployment



Cisco ASA Firewall Clustering Basics

- Designed to solve two critical issues with firewall HA:
  1. Aggregate firewall capacities for DC environments (BW, CPS, etc.)
  2. Provide dynamic N+1 stateful redundancy with zero packet loss
- Supported in routed (L3) and transparent (L2) firewall modes, both single and multi-context - Mixed Mode supported as well
- (NG)IPS module is fully supported in clustered firewall deployment
  - This adds NGIPS (FirePOWER) / NGFW / Device Context (FireSIGHT), etc. to ASA
    - Manages Asymmetric flows
- For ASA Clustering Deep-Dive watch recording of BRKSEC-3032 - Advanced - ASA Clustering Deep Dive

Cluster Scalability – ASA 9.2 Example (Real-World)



Bandwidth 70% Avg. → 100% with no Asymmetry*

Example 16 ASA5585-X SSP-60 at 20Gbps → 224Gbps of Real World TCP Throughput

Concurrent Connections 60%

Example 16 ASA5585-X SSP-60 at 10M → 96M concurrent connections

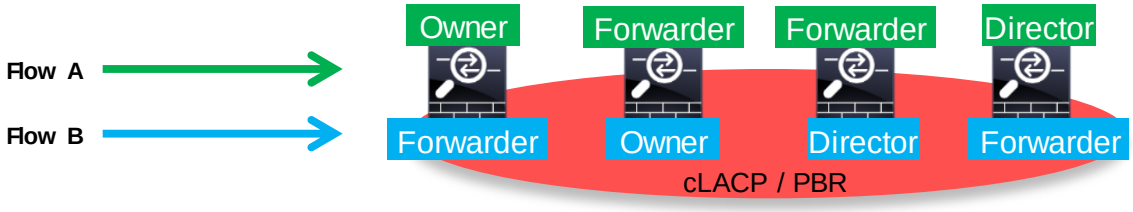
New Connection Rate 50%

Example 16 ASA5585-X SSP-60 at 350K CPS → 2.8M CPS

*Increasing scale can be accomplished by minimising Asymmetry – Symmetric LACP Hash is one good example – **src-dst IP or src-dst IP l4-port**

Clustering Roles

- Each firewall in the cluster has 3 roles defined:
  1. **Flow Owner** – the unit that receives the conn, registers with Director
  2. **Flow Director** – backup to the Owner and responds to lookup requests from the Forwarders – maintains a copy of state for individual Owner's flow
  3. **Forwarder** – receives a conn but does not own it, queries Director for Owner
  - Forwarders can derive Owner from SYN cookie if present (SYN-ACK) in Asymmetric scenarios or may query the Director via Multicast on CCL



Deployment Options

Overview on ASA Single-site clusters

- Load-balancing methods vs. Firewall mode, plus Context Mode options

Load Balancing	Firewall Modes and Features		
	Transparent	Routed	Multiple Contexts
Individual Interface L3 Method ECMP/ PBR	N/A*	✓	✓
Spanned Interface L2 ECLB	✓	✓	✓

- * Must configure spanned cluster to use Transparent firewall, L3 method warrants Routed firewall
- Multiple context mode is commonly utilised for both types of load-balancing scenarios

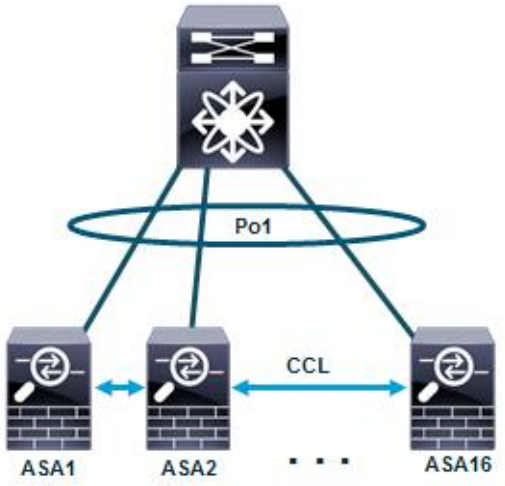
ASA Multi-Site Deployment Options

- Must Extend CCL over Data Centre Interconnect (DCI), no packet loss or re-ordering

Solution ID	ASA Version	Cluster type and switch designs	DC Integration
1	9.1.4	**Individual** Mode (ECMP)	**Router Sandwich**
2	9.2.1	**Spanned** / Transparent Firewall in Identified vPC designs **A. Extended Peer-link** (VPC) over DCI **B. Split Ether-Channel** between Data Centres	**Router Sandwich**
3	9.3.2	**Spanned** / Transparent Firewall (**Split Ether-Channel**)	**ASA between Apps and their First Hop**
4	Future	**Spanned /** Routed Firewall (**Split Ether-Channel**)	**ASA as a First Hop**

What is cLACP and What Does it Do?

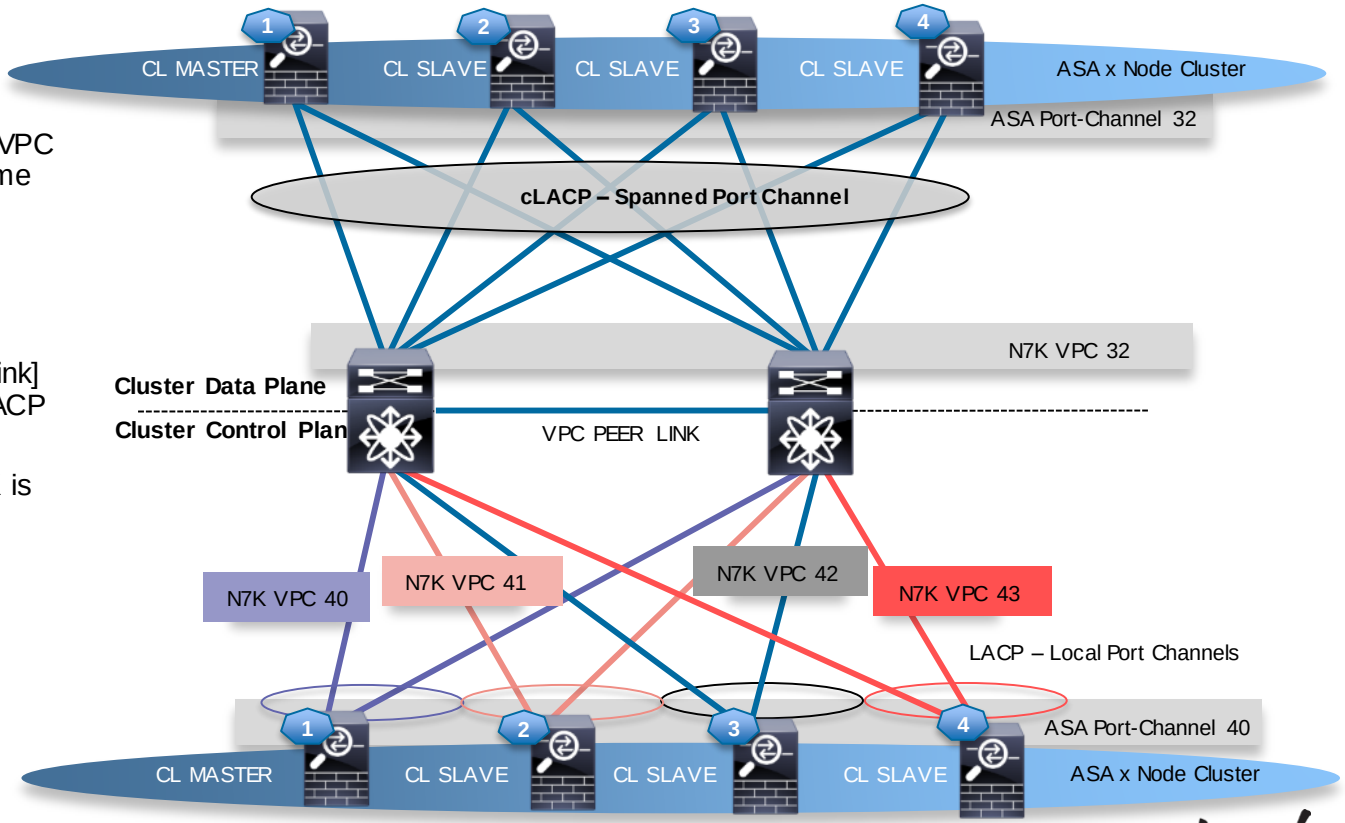
- The challenge for clustering is that LACP is defined to run between ***two devices only*** according to IEEE specification and may only have 8 interfaces forwarding data
- Requirement to support LACP over multiple ASA units in a cluster and make clustered ASAs able to interoperate with standard LACP devices **as one ASA**
- Provide Etherchannel re-configuration with traffic black-hole avoidance and load balancing at both link and device level during link failure or device failure
- Provide cLACP API to cluster CP to notify Etherchannel link status change and provide health monitoring
- cLACP recovery/redundancy between ASA units in the case of Master unit leaves cluster
- Extend the maximum number of active forwarding interfaces to 16 (or potentially greater)
  - 32-links Now Supported (16 active/16 standby in ASA 9.2)



Correct Use of EtherChannels When Clustering with VPCs

- **Data Plane** of Cluster MUST use cLACP (Spanned Port-Channel) VPC Identifier on N7K must be the same for channel consistency
  - ***ASA uses the 'span-cluster' command on channel***

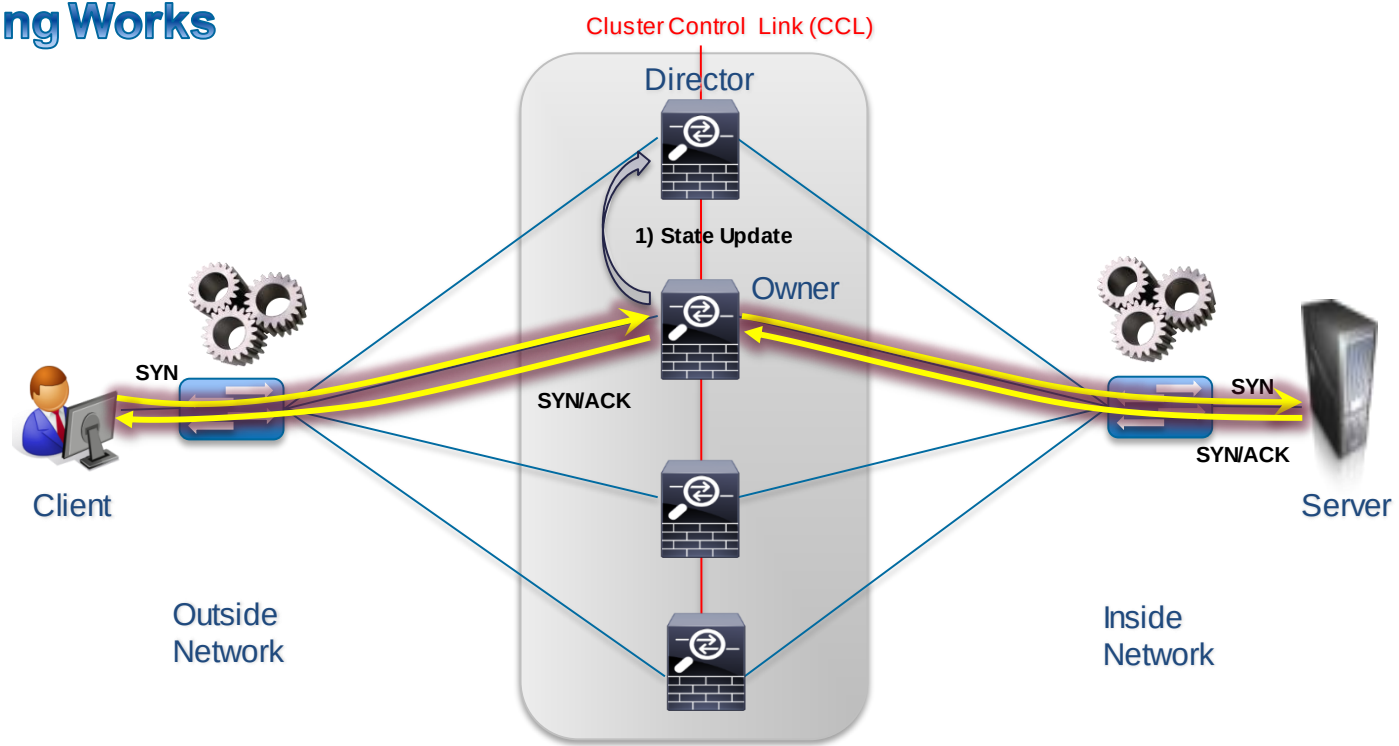
- **Control Plane** [Cluster Control Link] of Cluster MUST use standard LACP (Local Port-Channel)
- Each VPC Identifier on Nexus 7K is unique
- Port Channel Identifier on ASA is arbitrary
  - ***(max number 48)***



http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Data_Center/VMDC/ASA_Cluster/ASA_Cluster/ASA_Cluster.html

TCP Session: Symmetric Traffic

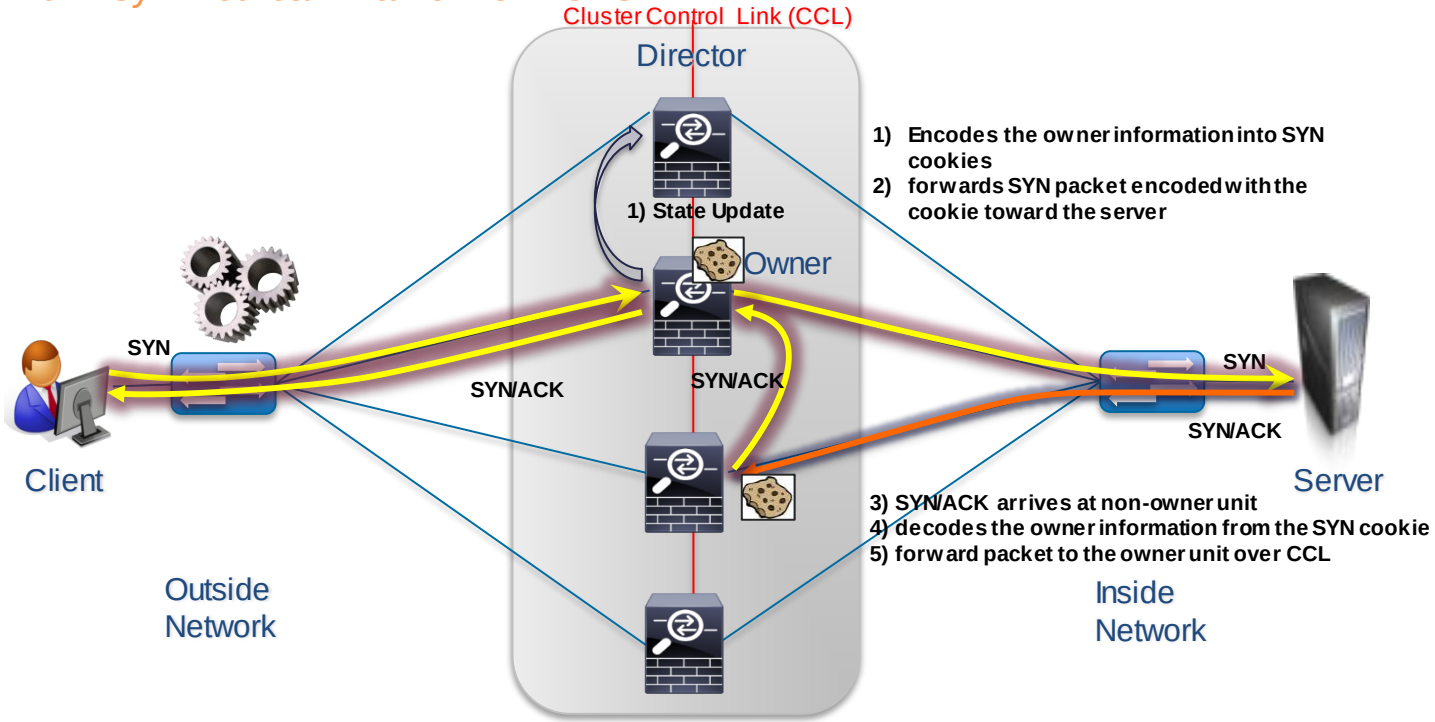
How Clustering Works



- State replication from Owner to Director, also serves as failover msg to provide redundancy should owner fail
- Director is selected per connection using consistent hashing algorithm.

TCP Session: Asymmetric Traffic

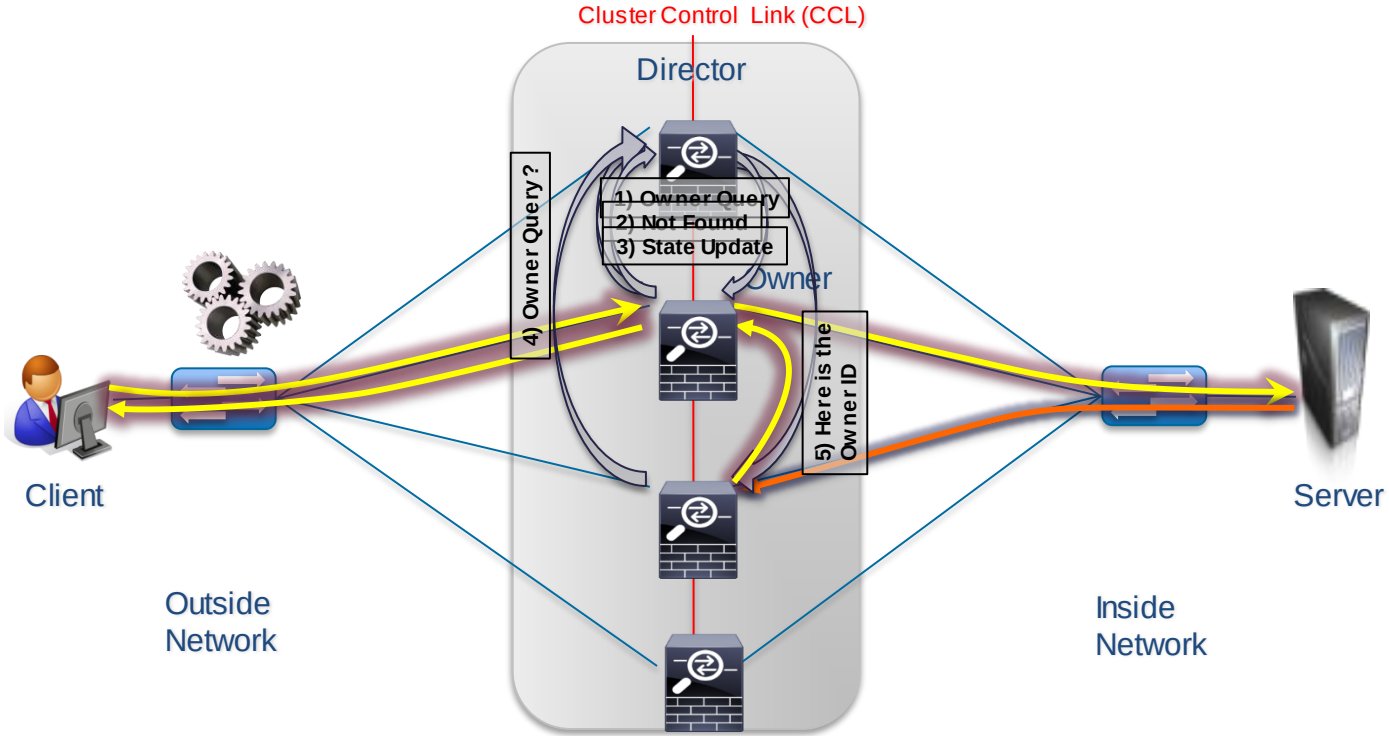
TCP SYN cookies with Asymmetrical Traffic workflows



It is possible that the SYN/ACK from the server arrives at a non-owner unit before the connection is built at the director.

- As the owner unit processes the TCP SYN, it encodes within the Sequence # which unit in the cluster is the owner
- Other units can decode that information and forward the SYN/ACK directly to the owner without having to query the director

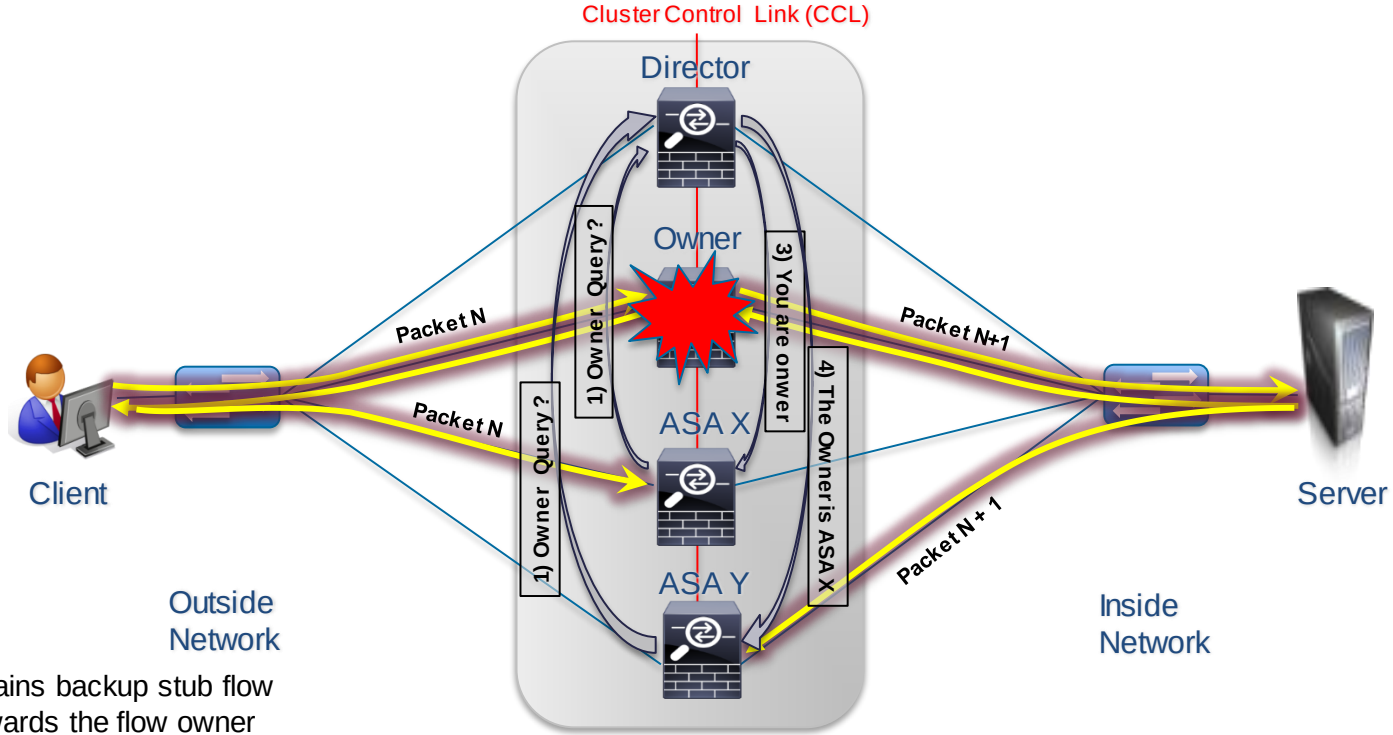
UDP Session: Asymmetric Traffic



- When a unit receives a UDP packet for a flow that it does not own, it queries the director to find the owner
- Thereafter, it maintains a forwarding flow. It can punt packets directly to the owner, bypassing the query to the director
- Short-lived flows (eg. DNS, ICMP) do not have forwarding flows

TCP Session: Recovery From Failure

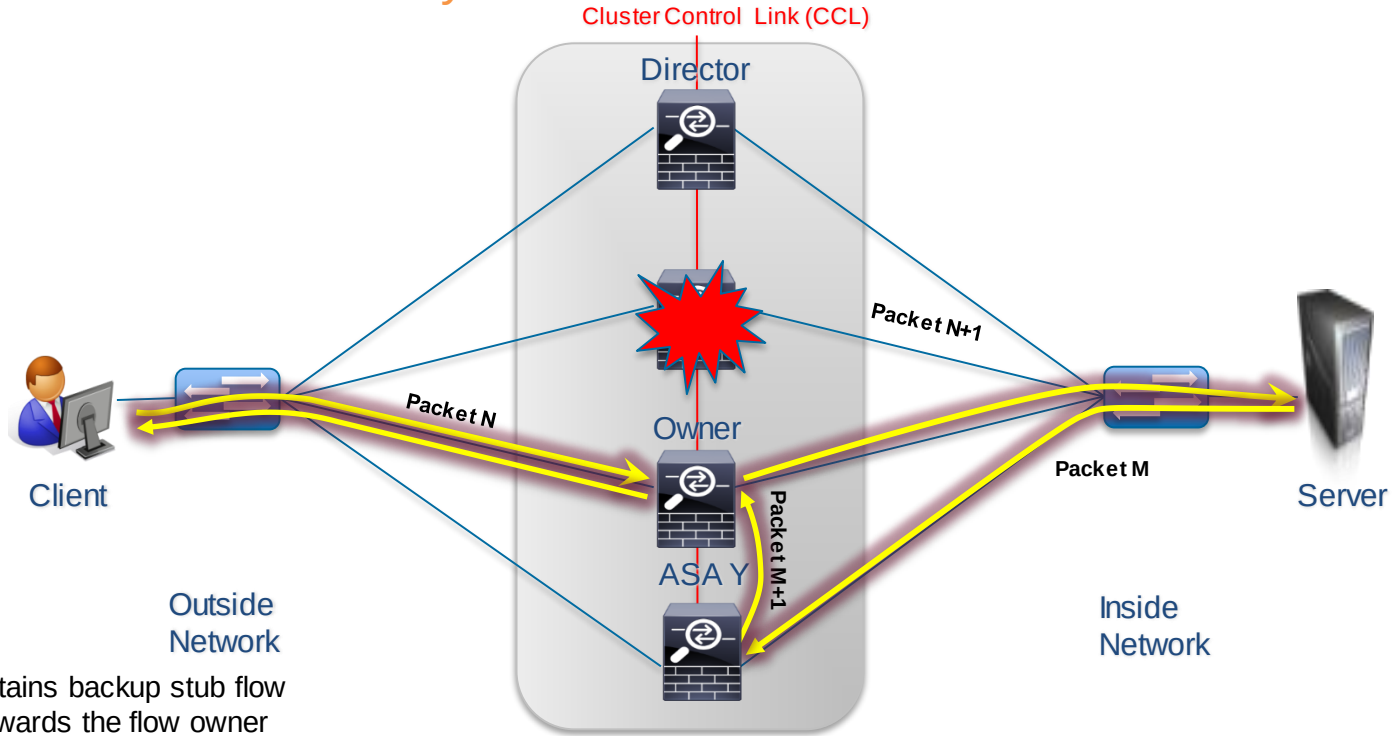
ASA Failover ⇔ Session Recovery



- Director unit maintains backup stub flow
- Redirects units towards the flow owner
- In case owner unit fails, director unit elects the owner
- Receives connection updates, so that they are up to date in case of owner failure

TCP Session: Recovery From Failure

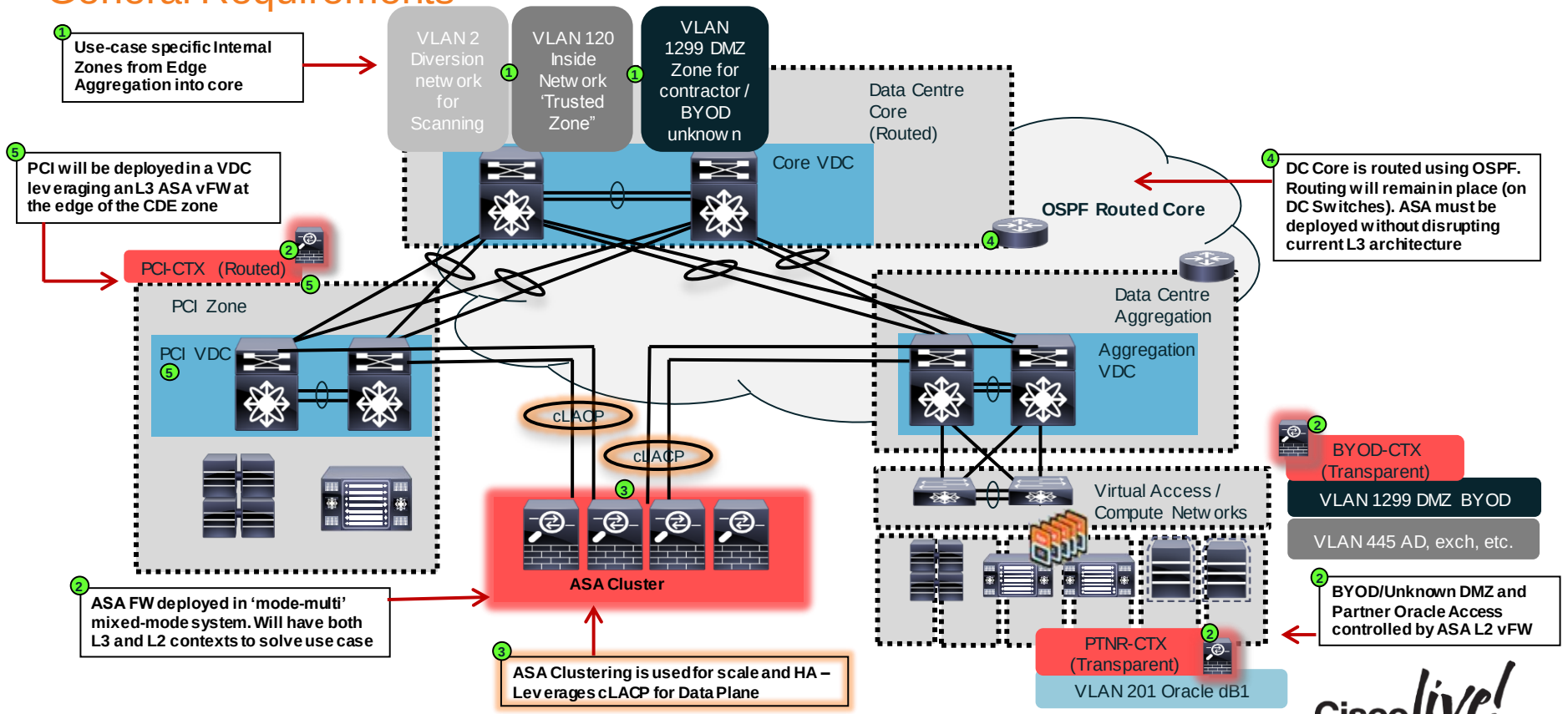
ASA Failover ⇔ Session Recovery



- Director unit maintains backup stub flow
- Redirects units towards the flow owner
- In case owner unit fails, director unit elects the owner
- Receives connection updates, so that they are up to date in case of owner failure

clinet.com Data Centre Physical ASA Deployment

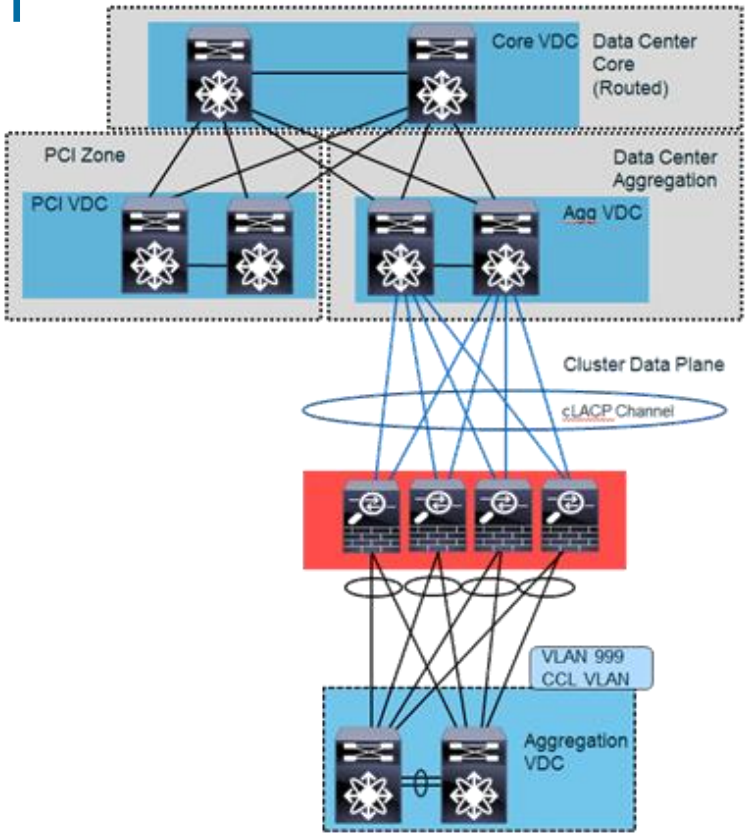
General Requirements



Basic Clustering Configuration

```
!Control Plane Configuration CCL - Once Per ASA
!
cluster interface-mode spanned
!
interface TenGigabitEthernet0/8
 channel-group 40 mode active
 no nameif
 no security-level
!
interface TenGigabitEthernet0/9
 channel-group 40 mode active
 no nameif
 no security-level
!
interface Port-channel40
 description Clustering Interface
```

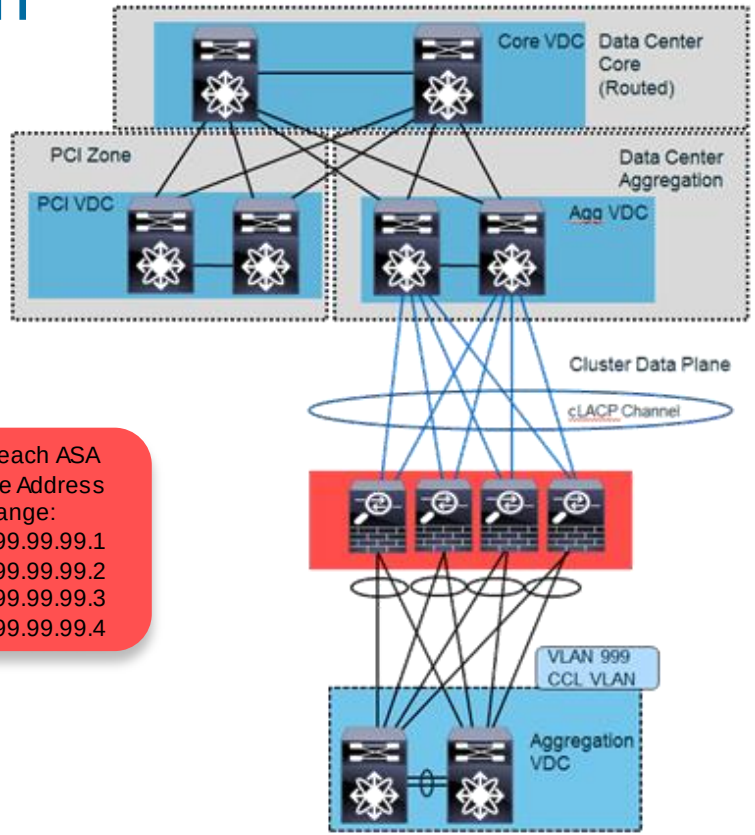
ASAs use a common channel-group for CCL.



Basic Clustering Configuration

```
! General Cluster Config - Once per ASA for CCL
cluster group DC-SEC
 key ***** (hidden)
 local-unit asa1
 cluster-interface Port-channel40 ip 99.99.99.1 255.255.255.0
 priority 1
 console-replicate
 health-check holdtime 3
 clacp system-mac auto system-priority 1
 enable
!Data Plane Configuration - On Master only
!
interface Po32
 port-channel span-cluster
interface TenGigabitEthernet0/6
 channel-group 32 mode active vss-id 1
 no nameif
 no security-level
!
interface TenGigabitEthernet0/7
 channel-group 32 mode active vss-id 2
 no nameif
 no security-level
!
interface BVI1
 ip address 10.101.10.200 255.255.255.0
```

Assign each ASA a unique Address in this range:
ASA1: 99.99.99.1
ASA2: 99.99.99.2
ASA3: 99.99.99.3
ASA4: 99.99.99.4

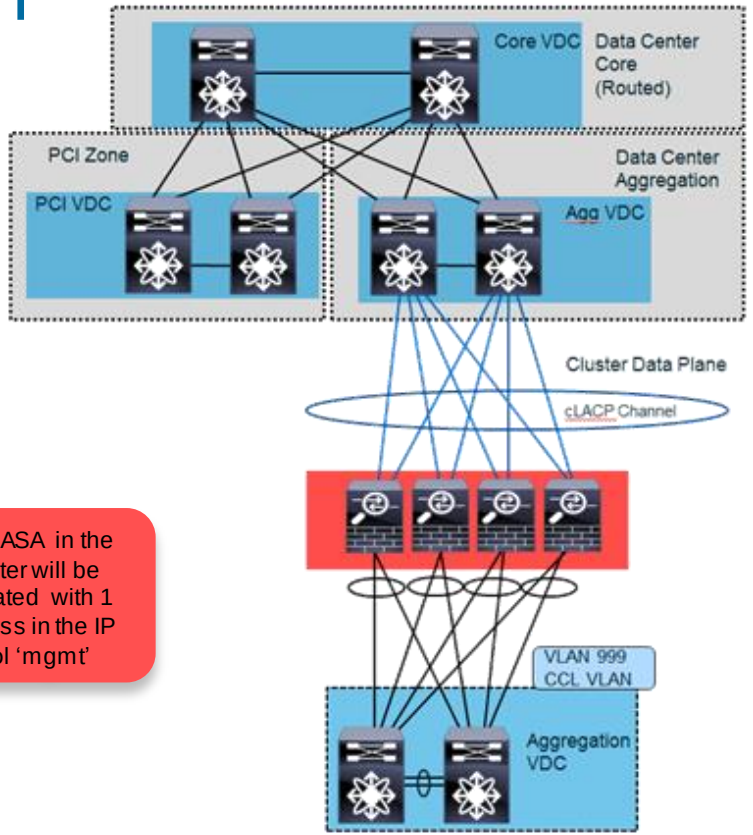


Basic Clustering Configuration

```
!Data Plane Configuration (cont.) On Master Only
!
interface BVI1
 ip address 172.16.25.252 255.255.255.0
!
interface Port-channel32.201
 mac-address 0001.0001.0201
 desc Oracle dB VLAN
 vlan 101
 nameif inside
 bridge-group 1
!
interface Port-channel32.202
 mac-address 0001.0001.0202
 vlan 102
 nameif outside
 bridge-group 1
!
!Management Configuration
ip local pool mgmt 172.26.246.253-172.26.246.254
interface Management0/0
 management-only
 nameif management
 security-level 0
 ip address 172.26.246.252 255.255.255.0 cluster-pool mgmt
```

Each ASA in the cluster will be allocated with 1 address in the IP pool 'mgmt'

Virtual IP Address for the ASA cluster



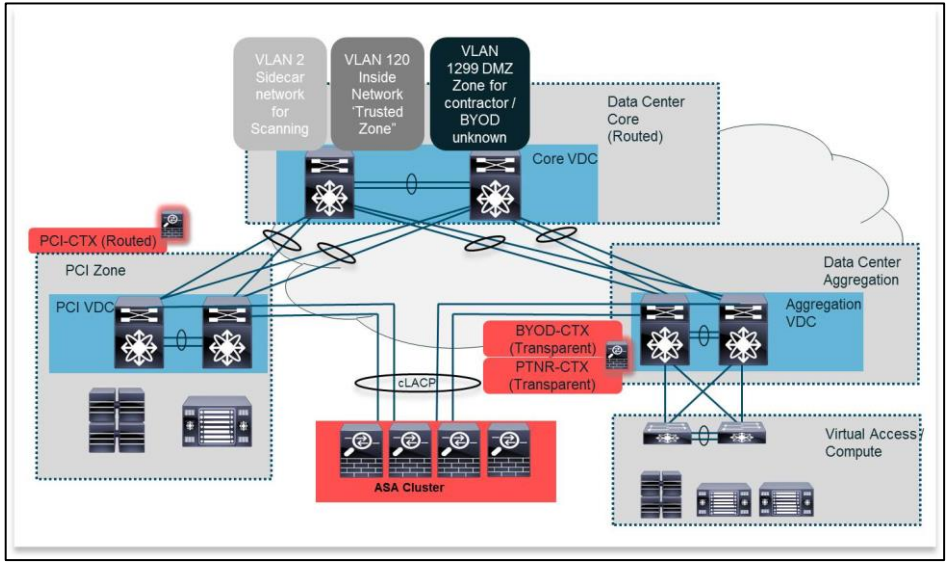
Port-channel Verification

```
asa(cfg-cluster)# sh port-channel summary

Number of channel-groups in use: 2

Group  Port-channel  Protocol  Span-cluster    Ports

------+-------------+---------+-----------+-----------------------

32     Po32(U)           LACP       Yes      Te0/6(P)    Te0/7(P)

40     Po40(U)           LACP        No      Te0/8(P)    Te0/9(P)
```

- Port channel 32 is the cluster data plane
- Port channel 40 is the cluster control plane—note that the CCL is not a “span-cluster” port-channel (best practice)
- Both are up as noted by the (U) and were negotiated via LACP
- Remember the spanned port-channel will not come up until clustering is enabled

ASA Deployment Checklist (Data Centre)

- **Specific Items for ASA in the Data Centre**
  - ✓ 1 – Verify deployment mode –routed or transparent or both (mode multi)
  - ✓ 2 – Create Virtualised Firewalls where applicable
    - Multi-context Firewall common, especially for Multi-tenancy
  - ✓ 3 – Transparent Mode Firewalls
    - Deploying Transparent Mode
    - How Transparent Mode Works
- **Implement Clustering**
  - ✓ 5 – Clustering Basics
  - 6 – Clustering deployment in the clinet.com Data Centre
  - – Comparing Virtual and Physical Firewall Deployments for the DC based upon requirements 7
- **Deploying ASAv (Virtual ASA)**
  - – ESXI Deployment 7



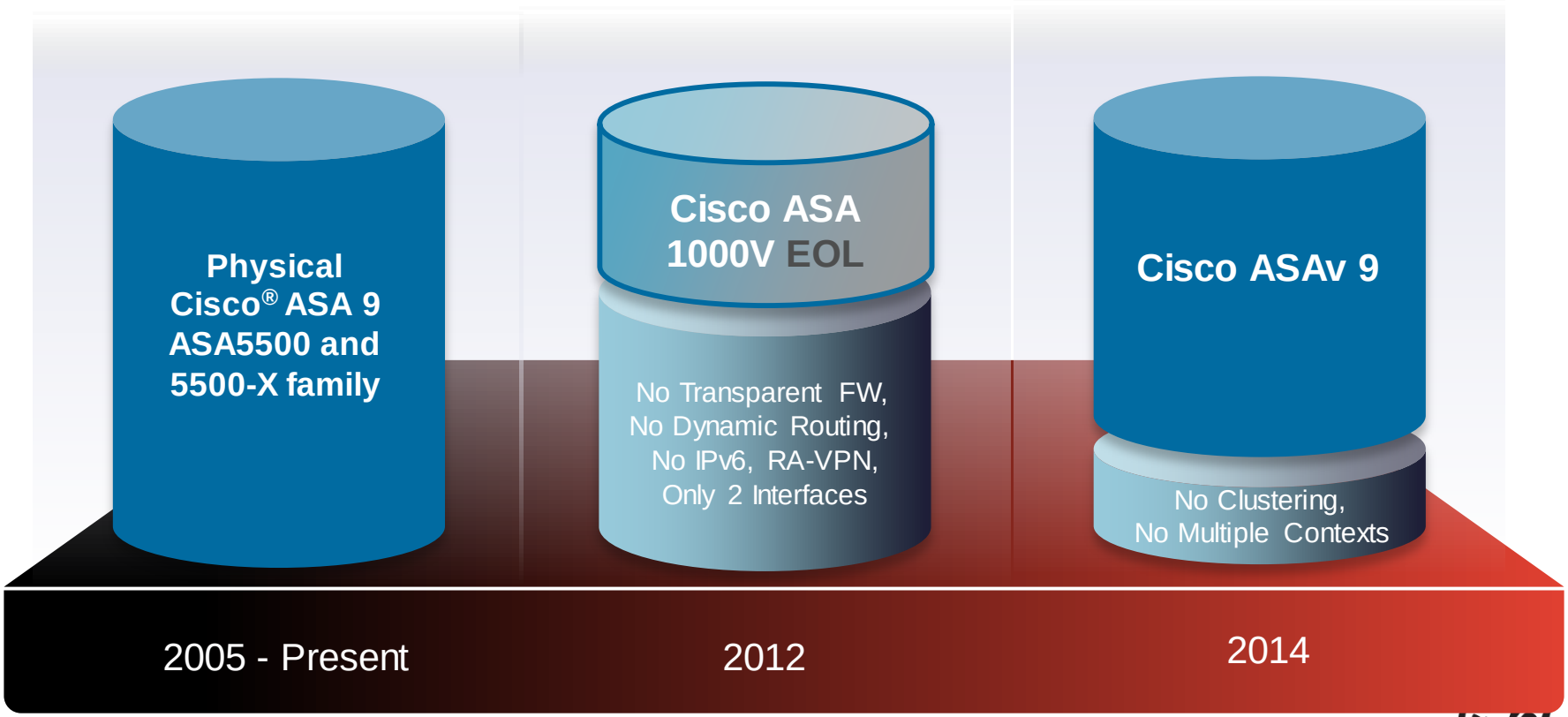
Deploying the ASAv Routed L3 Firewall in the Compute Layer

The Cisco ASAv Virtual Appliance

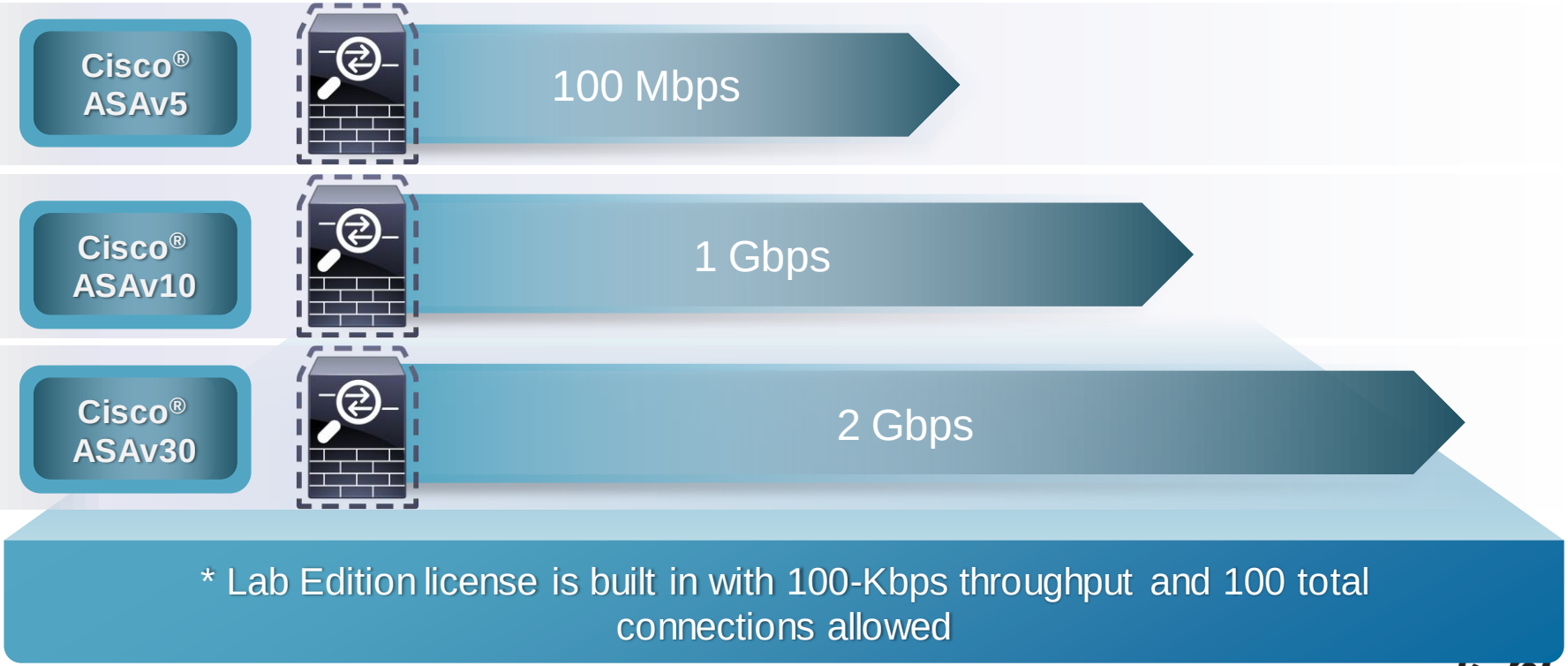
Cisco® ASAv Security Appliance

Brings proven Cisco security in physical environments to virtualised environments

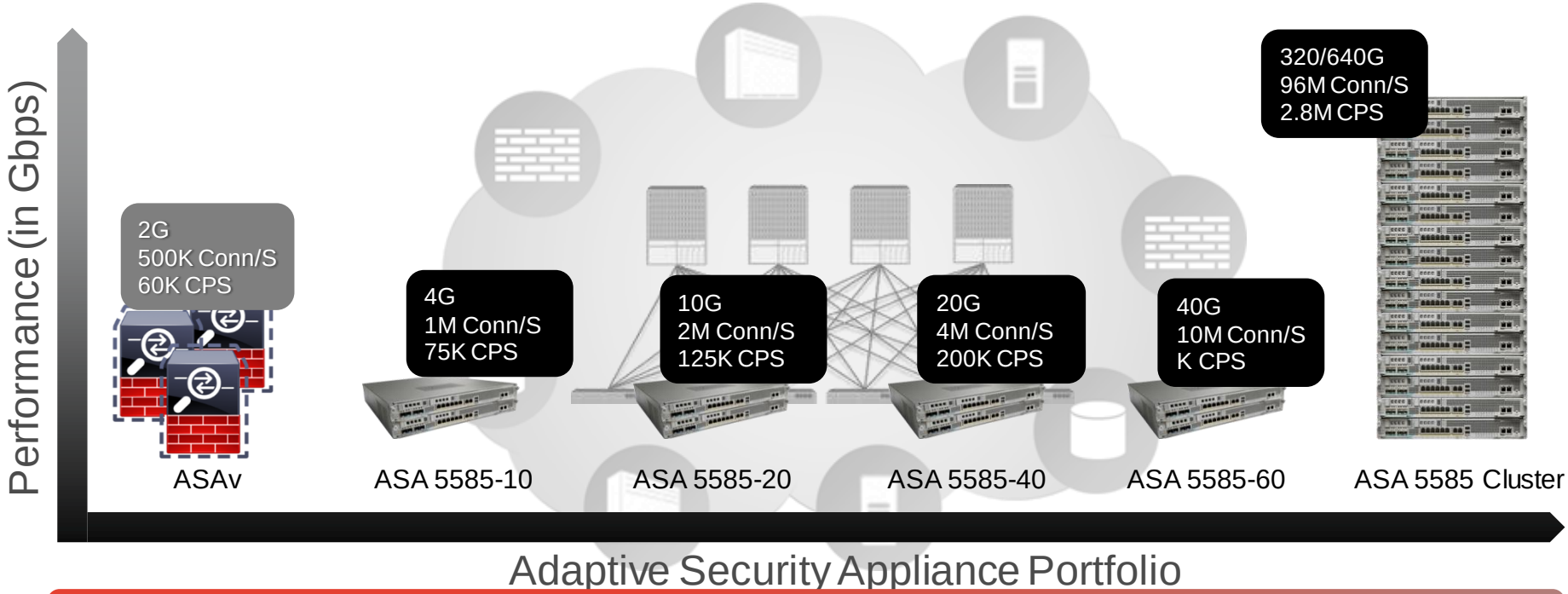
Cisco ASA Feature Comparison



Cisco ASAv Platforms



Cisco Adaptive Security Appliance in a Data Centre

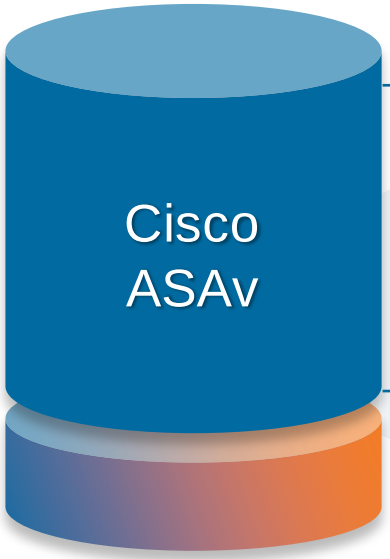


Purpose-Built for Agility, Scale, Programmability, and Application Awareness

Cisco live!

Cisco ASAv Firewall and Management Features

Cisco® ASA 9 Feature Set

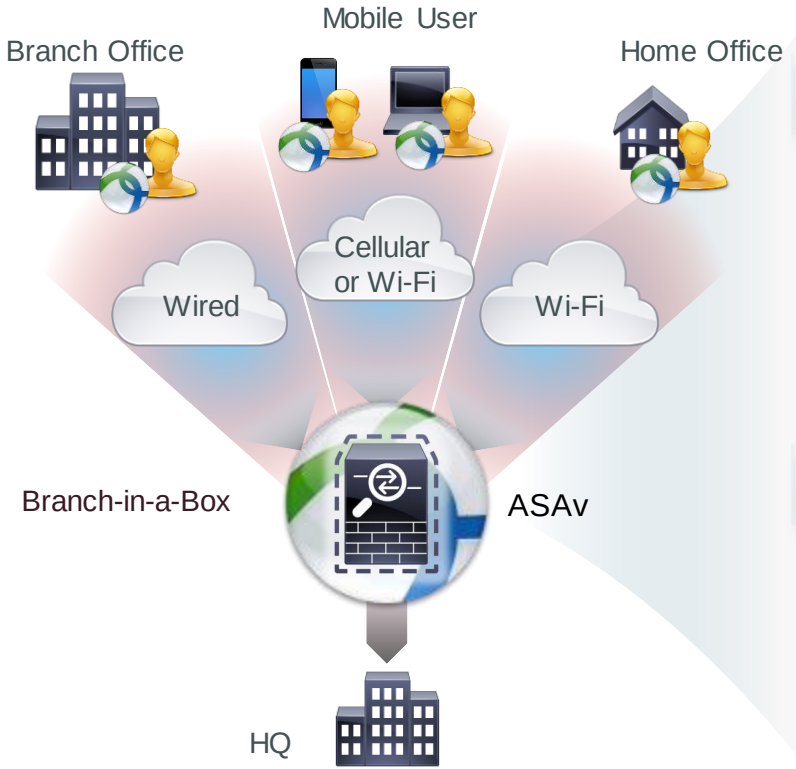


Removed clustering and multiple-context mode

- 10 vNIC interfaces and VLAN tagging
- Virtualisation displaces multiple-context and clustering
- Parity with all other Cisco ASA platform features

- SDN (Cisco APIC) and traditional (Cisco ASDM and CSM) management tools
- Dynamic routing includes OSPF, EIGRP, and BGP
- IPv6 inspection support, NAT66, and NAT46/NAT64
- REST API for programmed configuration and monitoring
- Cisco TrustSec® PEP with SGT-based ACLs
- Zone-based firewall
- Equal-Cost Multipath
- Failover Active/Standby HA model

Cisco ASAv RA-VPN Features



Remote-Access Client

- Cisco AnyConnect™ client
- Third-party client support with IKEv2 (RFC5996)
- TLS 1.2 update (new ciphers)
- Cisco TrustSec® SGT assignment
- Cisco® ISE change of authorisation

Clientless VPN

- Browser-based SSL tunnels
- Citrix and VMware VDI support
- Cisco ASAv can proxy for Citrix XenApp and XenDesktop

Note: All crypto features performed in software

Cisco ASAv Firewall Licensing Goes Smart

Cisco® Smart Solutions

License **Pooling**
Full Asset **Visibility**
Central Repository Portal

Options

Select the Following:
Performance: 100 Mbps, 1 Gbps, or 2 Gbps
Consumption Model: Perpetual
Procurable **Time-Based** Demos

Cisco Smart Workflow

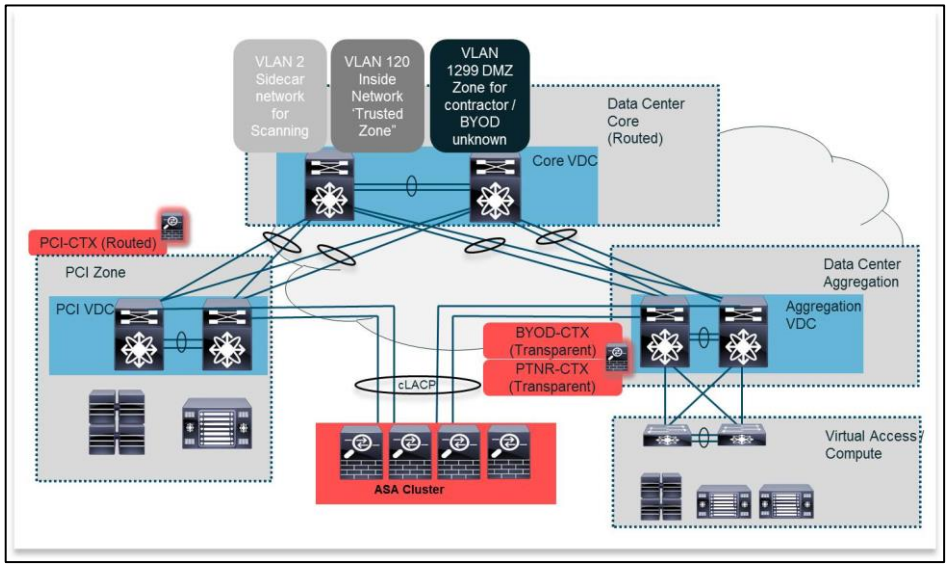
1. Customer places a Cisco ASAv order and creates the **Smart account**
2. Through Smart portal, **entitlements** allow them to generate a Smart **token**
3. The Smart **token** is entered on the Cisco ASAv through the **license** CLI command
4. Cisco ASAv then uses Call Home to send appliance info to the **Smart portal**

Enable Better Consumption Models and Streamline the Licensing Process

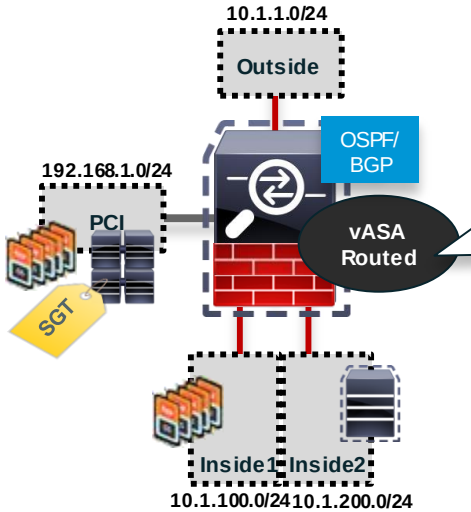
ASA Deployment Checklist (Data Centre)

- **Specific Items for ASA in the Data Centre**
  - ✓ 1 – Verify deployment mode –routed or transparent or both (mode multi)
  - ✓ 2 – Create Virtualised Firewalls where applicable
    - Multi-context Firewall common, especially for Multi-tenancy
  - ✓ 3 – Transparent Mode Firewalls
    - Deploying Transparent Mode
    - How Transparent Mode Works
- **Implement Clustering**
  - ✓ 5 – Clustering Basics
  - ✓ 6 – Clustering deployment in the clinet.com Data Centre
  - ✓ 7 – Comparing Virtual and Physical Firewall Deployments for the DC based upon requirements
- **Deploying ASAv (Virtual ASA)**
  - – ESXI and KVM Deployment

7



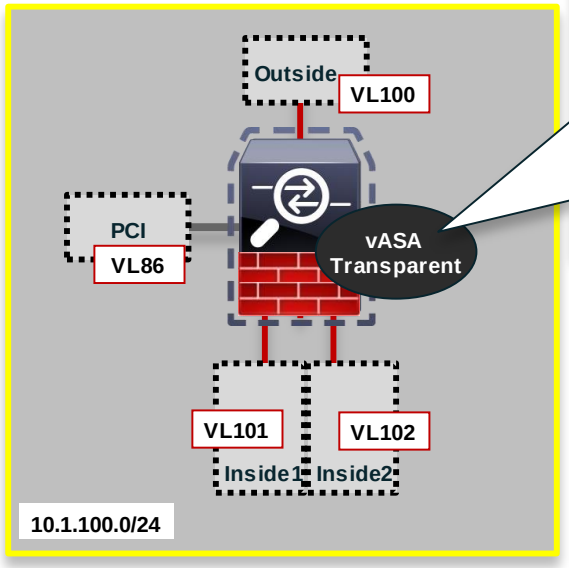
ASAv Deployment Scenario – Routed Mode



Routed Mode – Tenant edge use case

-First-hop gateway to hosts
-Capable gateway for all client hosts, VM or physical
-Scalable number of data interfaces
-Traditional Layer 3 Boundary in the network
-Dynamic Routing / IPv6 / NGE, etc.
-AnyConnect/SSL VPN Head-end or IPSec peer
-SGT Tagging Policy Enforcement capable
-REST API Orchestration – 60 second provisioning

ASAv Deployment Scenario – Transparent Mode

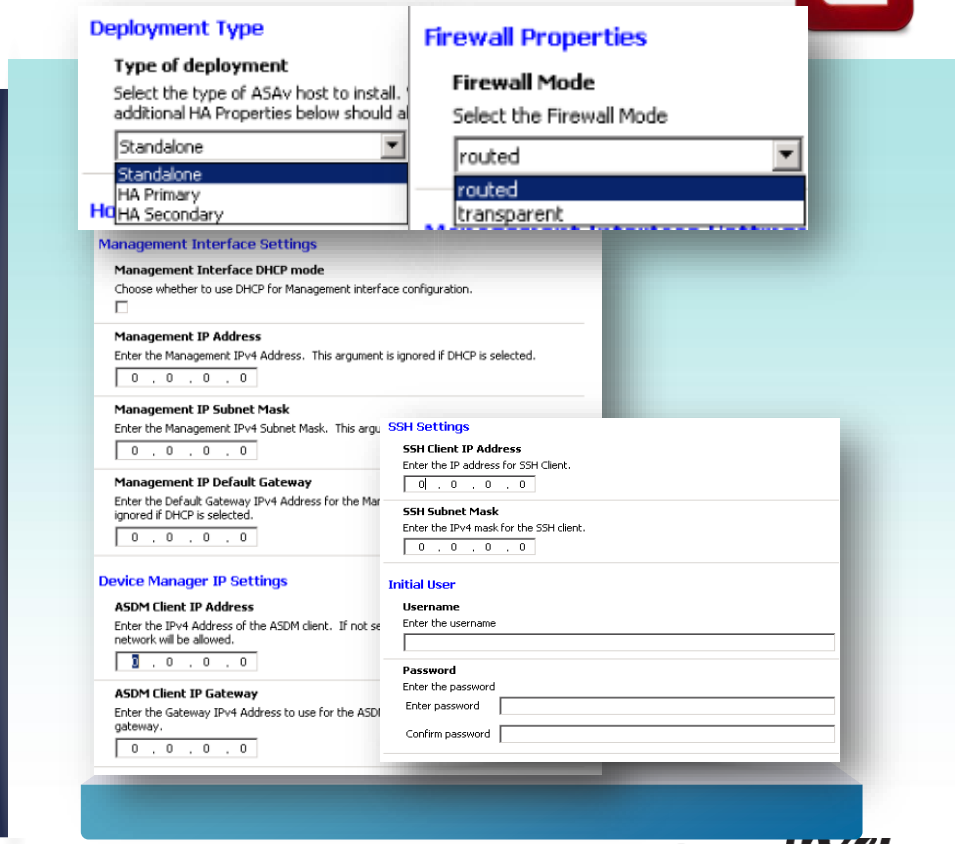


Transparent Firewall Use-case(s)

-VLAN Bridging up to 4 (sub-)interfaces per BVI
-Max 50 BVIs per ASAv30
- Intra-Subnet policies (VLAN)
-NAT and ACL available
-Non-disruptive PCI compliance
-Traditional Layer 2 boundary between hosts
-All segments in one broadcast domain (Subnet)
- REST API Orchestration – Same as Routed

Deploy Cisco ASAv on VMware ESXi

- Deploy OVF template and enter settings
  - Select firewall mode (L2 or L3)
  - Select performance
  - Management interface/Device Manager
  - Agent client IP/Gateway/Failover
  - SSH access and credentials
  - Smart license token and performance tier
- Verify vNIC interface mapping of
  - MGMT VLAN (M0/0) to Network Adapter1
  - Failover VLAN (G0/8) to Network Adapter10
- **Cisco® ASDM, SSH,** or **REST API** session can be used going forward to complete the configuration of the Cisco ASAv



Deploy Cisco ASAv on KVM

Cisco® ASAv on KVM is feature-equivalent to the VMware version in licensing, image signing, secure storage, and functions

- KVM adds **new packaging** and installation of Cisco ASAv
- Enables **Day-0 configuration**
- Linux distributions must have the following package versions:
  KVM/qemu **1.0**, Linux kernel **3.2**, glibc **2.15**, libvirt **0.9.8**
- Qualified with Ubuntu **12.04/14.04** LTS
- **Qcow2** image format is used for initial deployment, with capability to then **upgrade with .bin**

Day-0 Configuration

Allows you to predefine Cisco® ASAv configuration before it is launched.

- day0-config is a text file of Cisco ASAv configuration
- Must generate **day0.iso** image from day0-config and supply as second disk argument at launch
- Must use **no shutdown** command for Cisco ASA interfaces
- Example CLI:

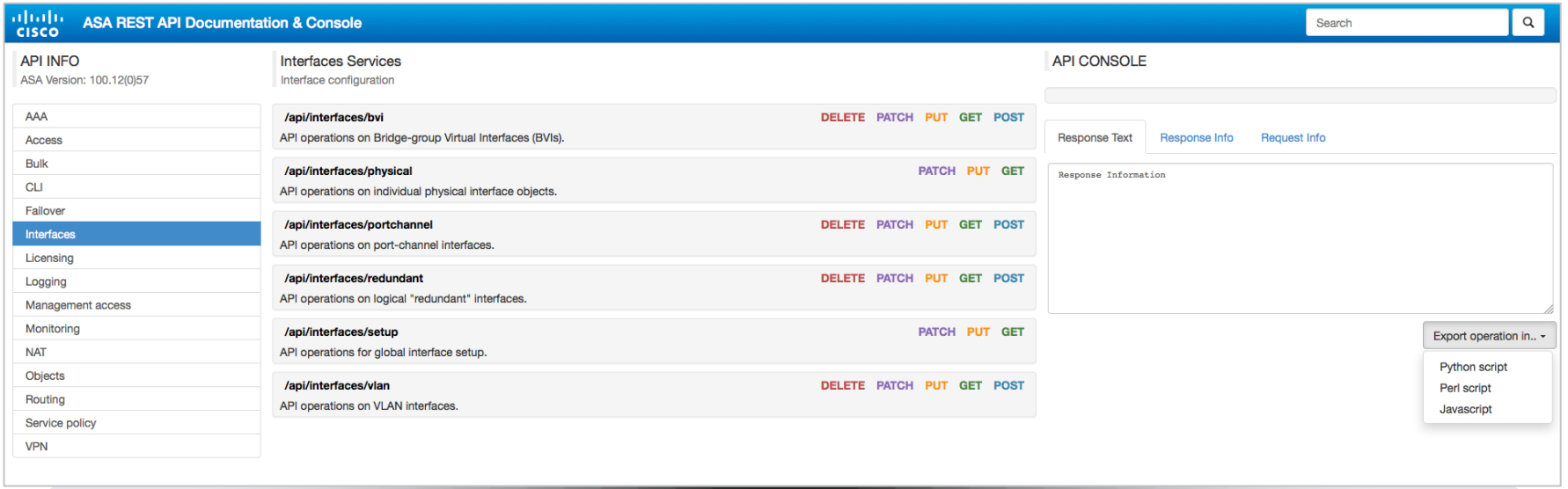
```
genisoimage -r -o day0.iso day0-config
```

```
hostname mylab-asav

Interface M0/0
nameif management
ip address 10.0.1.61 255.255.0.0
no shutdown

Interface G0/0
nameif inside
ip address 10.10.1.1 255.255.0.0
no shutdown

Interface G0/1
nameif outside
ip address 10.20.1.1 255.255.0.0
no shutdown

access-list inbound extended deny ip any any
access-list inbound extended deny icmp any any
access-group inbound in interface outside

crypto key generate rsa modulus 1024
aaa authentication ssh console LOCAL
username cisco password lab
ssh 10.30.0.0 255.255.0.0 management
ssh timeout 40
ssh version 2
```

Accessing and Configuring the Virtual ASA

- ASAv Bootstrapping – 2 options
  - Option 1: **https://***IP_address_of_management_interface***/admin**
    - No username / password needed
    - ASDM GUI will be used to run Startup Wizard
  - Option 2: Right-click the ASAv instance in the VM Inventory, and choose **Open Console**. Or you can click the **Console** tab.
  - Click in the console and press **Enter**.
  - ciscoasa> enable (Enable password is blank of course)
  - ASAv can now be configured just like a physical ASA
- **Note that there will be some time delays while the ASAv initialises for the first time**
- When the ASAv starts up for the first time, it reads parameters provided through the OVA file and adds them to the ASAv system configuration
  - It then automatically restarts the boot process until it is up and running
  - **This double boot process only occurs when you first deploy the ASAv**
- Once accessable from the network, you can also complete configuration using CSM, APIC, or the new ASA REST-API

Cisco ASA REST API Built-in Documentation



Reach API documentation through browser at, for example, https://10.0.1.61/doc

REST API Examples – Applies to any ASA

```
POST /api/access/out/inside/rules
{
  "permit": true,
  "sourceAddress": {
    "kind": "IPv4Address",
    "value": "192.168.1.1"
  },
  "destinationAddress": {
    "kind": "IPv4Network",
    "value": "172.16.171.0/24"
  },
  "sourceService": {
    "kind": "NetworkProtocol",
    "value": "ip"
  },
  "destinationService": {
    "kind": "NetworkProtocol",
    "value": "ip"
  },
  "active": true,
  "remarks": [],
  "position": 1
}
```

- Interface name
- Rule direction (**in** or **out**)
- **True** for permit or **false** for deny
- Source IP address
- Destination IP address
- Insert at position 1

Create an ACL Entry

```
GET /api/objects/networkobjects/DNS
{
  "kind": "object#NetworkObj",
  "selfLink":
"/api/objects/networkobjects/DNS",
  "name": "DNS",
  "host": {
    "kind": "IPv4Address",
    "value": "4.2.2.2"
  },
  "objectId": "DNS"
}
```

- Network object name
- Network object IP address

Retrieve an Object by Name

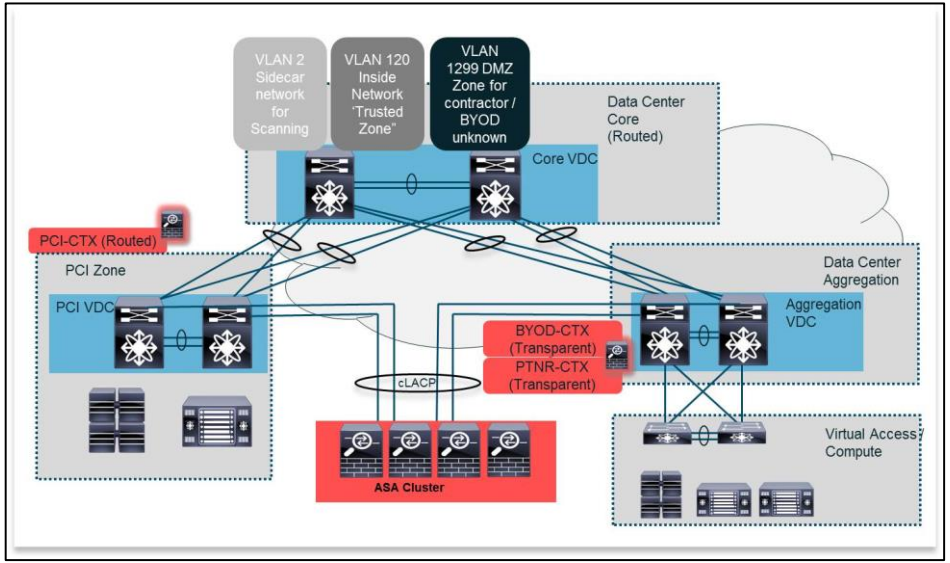
```
POST /cli
{
  "commands": [
    "show version | i Serial",
  ]
}
```

```
{
  "response": [
    "Serial Number: JMX09491111\n"
  ]
}
```

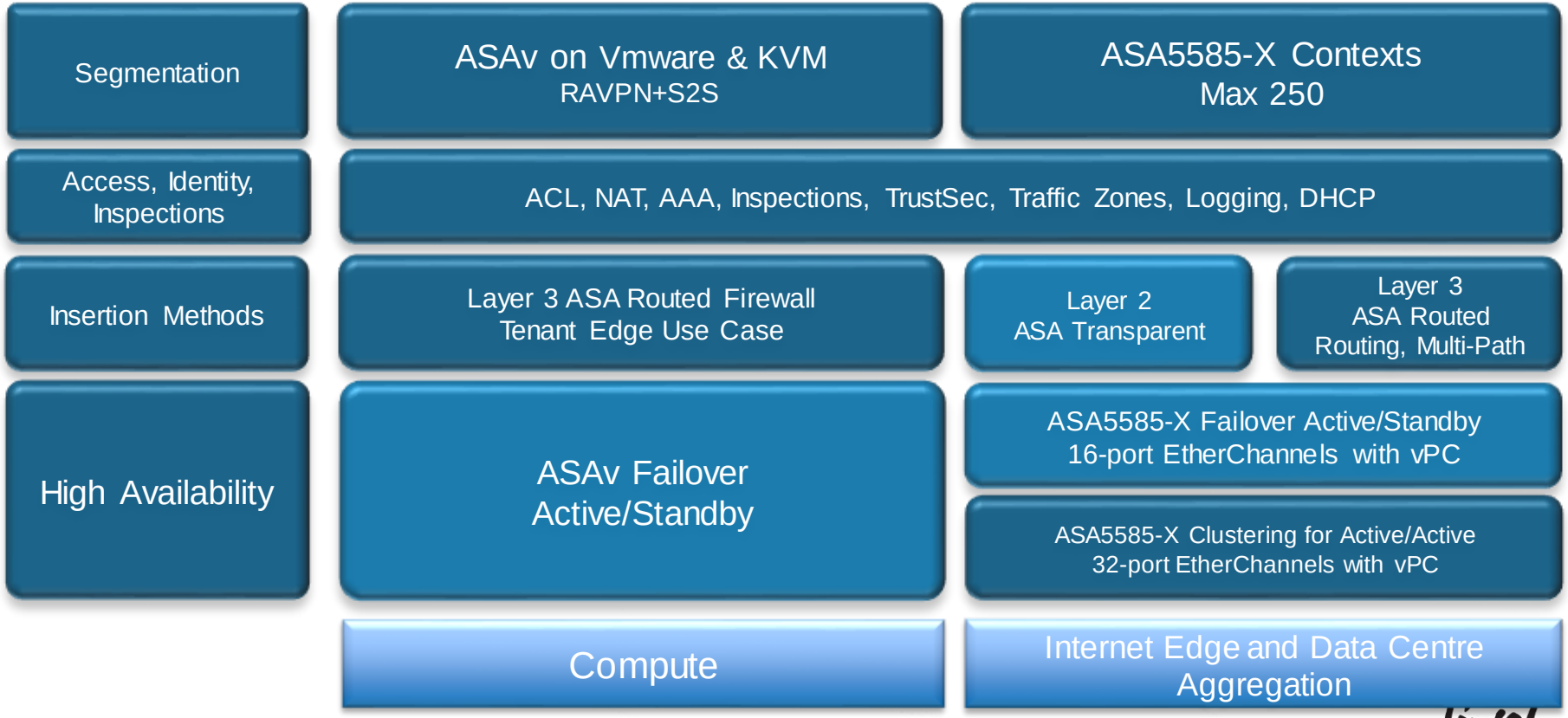
Execute Arbitrary Command

ASA Deployment Checklist (Data Centre)

- **Specific Items for ASA in the Data Centre**
  - ✓ 1 – Verify deployment mode –routed or transparent or both (mode multi)
  - ✓ 2 – Create Virtualised Firewalls where applicable
    - Multi-context Firewall common, especially for Multi-tenancy
  - ✓ 3 – Transparent Mode Firewalls
    - Deploying Transparent Mode
    - How Transparent Mode Works
- **Implement Clustering**
  - ✓ 5 – Clustering Basics
  - ✓ 6 – Clustering deployment in the clinet.com Data Centre
  - ✓ 7 – Comparing Virtual and Physical Firewall Deployments for the DC based upon requirements
- **Deploying ASAv (Virtual ASA)**
  - ✓ 7 – ESXI or KVM Deployment



Summary



Conclusions

- Cisco CVDs have guidance on firewall deployments in a Data Centre
- Physical firewalls and virtual firewalls are complementary solutions
- ASA's new routing, NSF, and traffic zone features enable better integration at the Internet Edge
- Firewall clustering offers advantages in the Data Centre deployments over the traditional failover A/S model
- Virtualised firewalls (multiple context mode) offer a nice approach to segmenting customers and allowing decentralised management
- ASAv platforms enable easy installation, training, licensing, and early scoping of security features and designs, before they go into production


Q & A
Cisco live!

Complete Your Online Session Evaluation

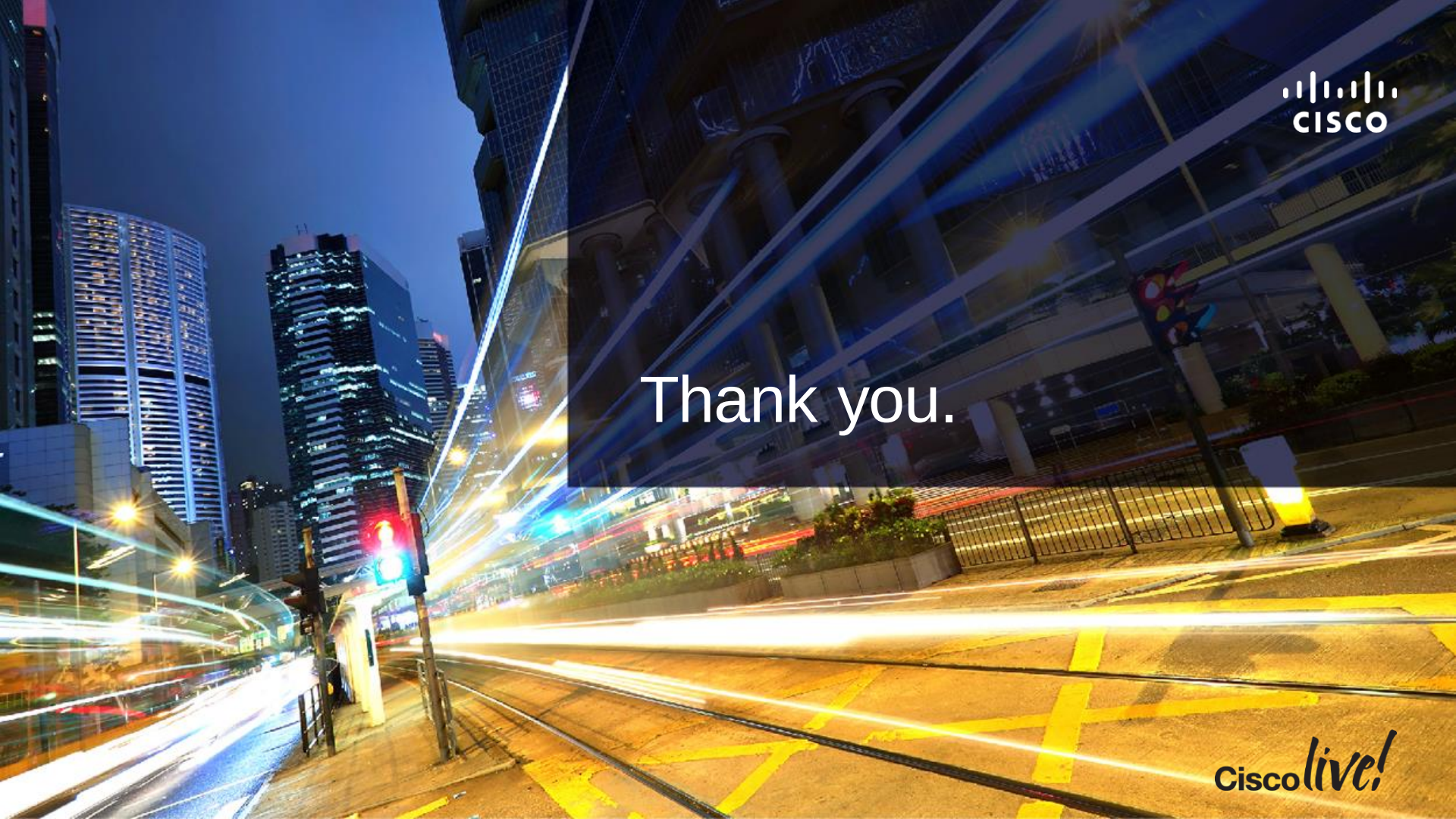
Give us your feedback and receive a Cisco Live 2015 T-Shirt!

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 http://showcase.genie-connect.com/clmelbourne2015
- Visit any Cisco Live Internet Station located throughout the venue

T-Shirts can be collected in the World of Solutions on Friday 20 March 12:00pm - 2:00pm

Learn online with Cisco Live!
Visit us online after the conference for full access to session videos and presentations. www.CiscoLiveAPAC.com


Thank you.
CISCO
Cisco live!


CISCO

Appendix

Global ACLs

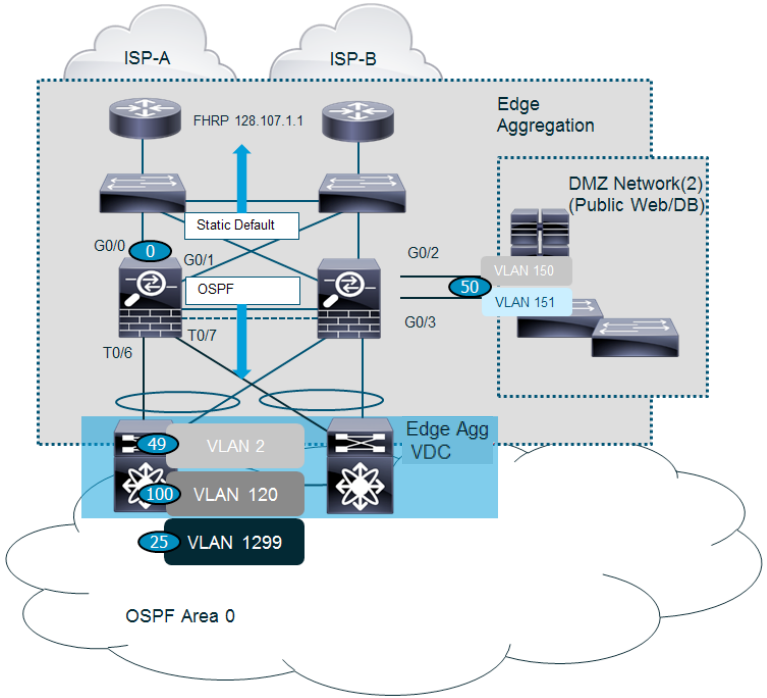
access-group name global

- The global ACL applies access control to **inbound traffic only on ALL interfaces**
  - Not replicated on each interface, so they save memory space
  - As long as a packet matches the source and destination IP addresses, the incoming interface is irrelevant
- Global access rules use the same architectural constructs as interface-specific access rules, so scalability and performance for global rules is the same as for interface-specific rules
  - Applies to transitory traffic, not Control Plane – **control-plane** argument and **global** argument are mutually exclusive
- ASA uses the following order to match access rules when only interface ACLs are configured:
  - Interface access list rules
  - Implicit deny ip any any interface access list rule (only on Interface ACL)
- ASA uses the following order to match access rules when both interface ACLs and the global ACL are configured:
  - Interface access list rules
  - Global access list rules
  - Implicit deny ip any any global access list rules (not on Interface ACL)

Deploying ASA Routing

Workaround for Nexus 7K vPC DRP Peering limitation

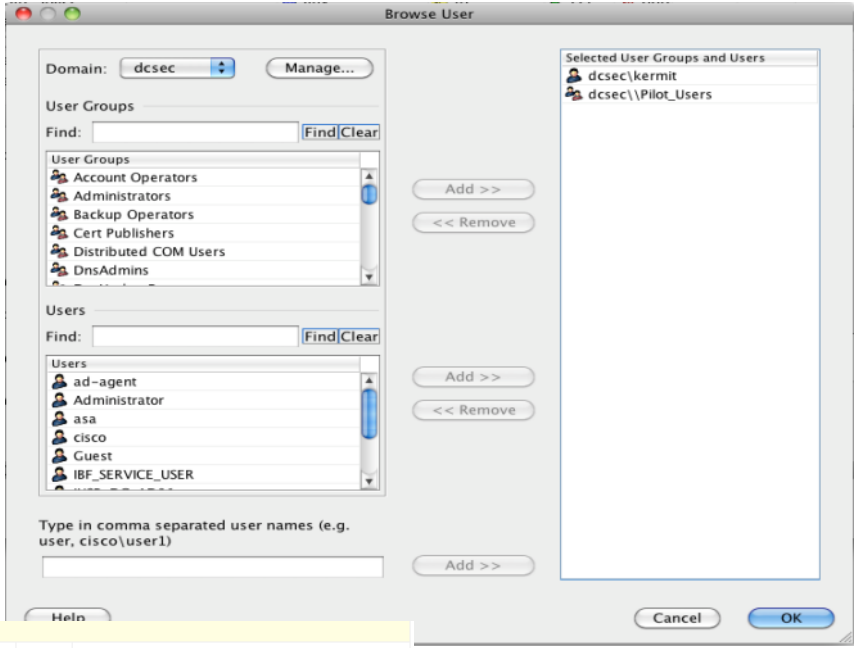
- Until NXOS 7.2, the limitation still exists which prevents dynamic route peering across vPC
- In order to use dynamic routing, follow this procedure to work around the limitation:
  - Create static routes on ASA that point to the HSRP address of the Nexus 7K SVI directly adjacent over the vPC
  - Create static routes on Nexus 7K that point to the Active IP address (or Cluster IP) on ASA
  - On both ASA and Nexus 7K, identify or implement the chosen DRP and use route redistribution to redistribute the static data into the DRP
  - Once the capability is released in NXOS, the DRPs can establish adjacency and the redistribution/static info may be removed.



Additional Policy Options

ASA Identity Firewalling

- 8.4.2> allows two new features: AD user and group import and FQDN in ACLs
- Requires use of an agent
- 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)



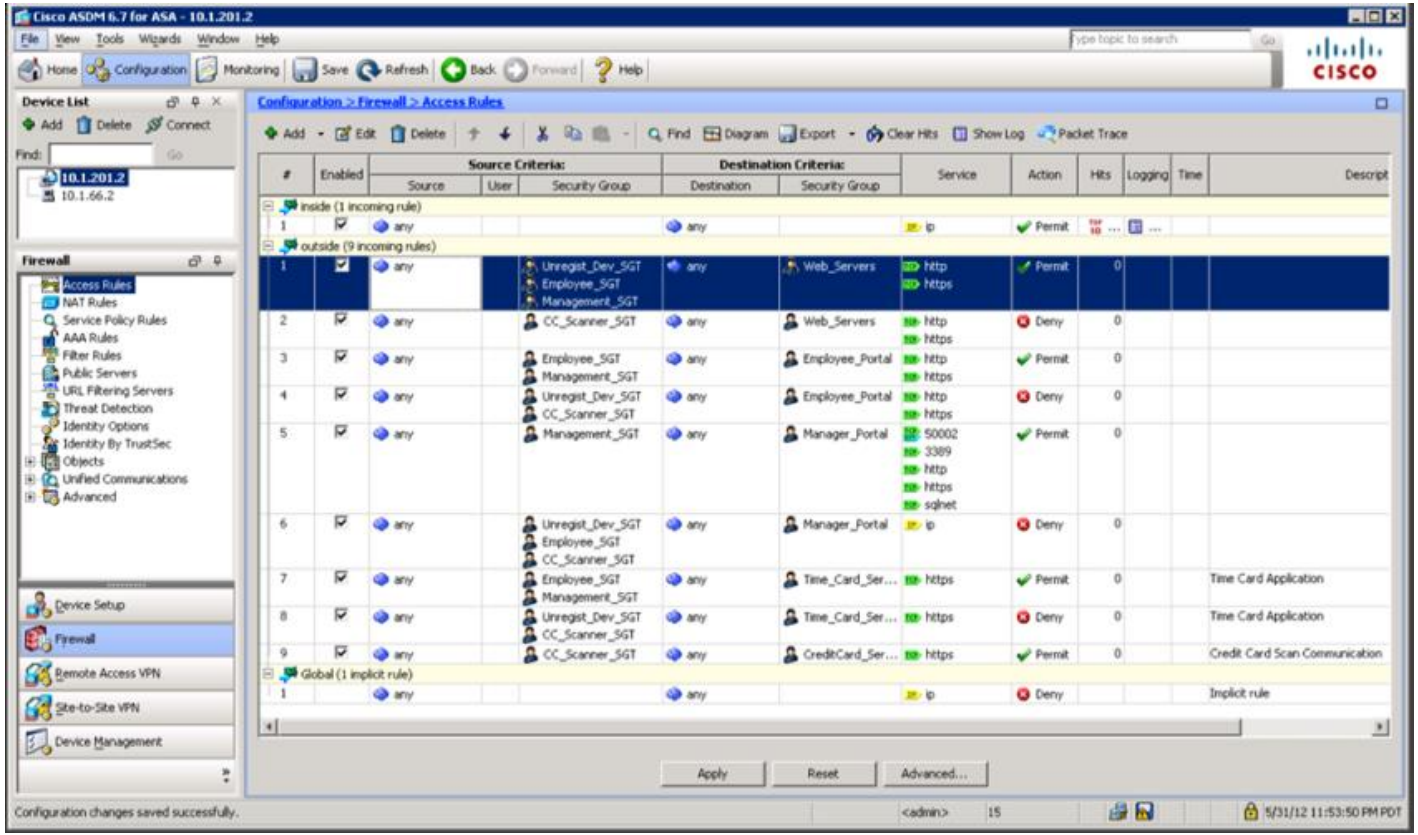
Global (8 rules)

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

SGT Firewall Policy

- BRKSEC-3690 Advanced Security Group Tags: The Detailed Walk Through
- BRKSEC-2690 Deploying Security Group Tags

Enforcing Traffic Policy on the ASA - SGFW




CISCO