

TOMORROW starts here.



Cisco *live!*

Firewall Architectures

BRKSEC-2021

Goran Saradzic

Technical Marketing Engineer

Guide to Icons



ASA Firewall



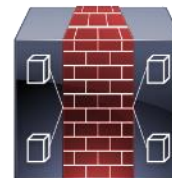
ASA1000V
Virtual Firewall
vASA



ASAv Firewall
(Virtualised ASA)



L3 Switch (Nexus 7K/Cat 6500)



Virtual Security
Gateway
Virtual Firewall

Agenda

- Introduction
- Physical vs Virtual Firewalls
- Firewall High Availability
- Clustering
- IPv6 Access Control
- Putting It All Together
- Summary and Conclusions



Introduction

Introduction

- This session was created new last year in response to feedback over the years from my previous session BRKSEC-2020 (Firewall Design and Deployment)
- Cisco has many different types of firewalls, this session will share good deployment options and things to avoid
- The intent of this session is to take a macro approach to the firewall
- Best practices and gotchas/caveats will be shared and discussed
- This session does not cover IOS firewall, Firewall Services Module (FWSM) or ASA Next Generation Firewall
- Please ask questions, we'll be moving fast



Physical Firewalls and Virtual Firewalls

Physical Firewalls:

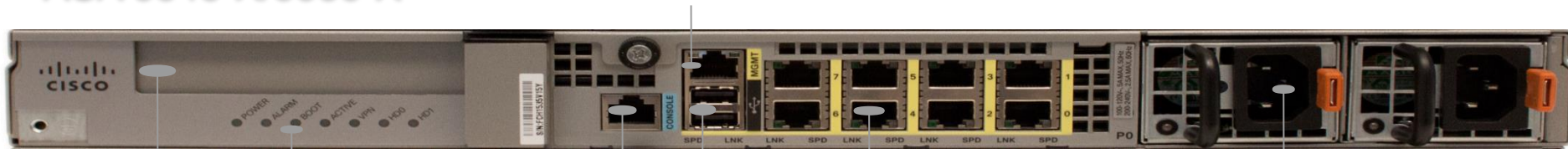
Service Modules and Appliances

- Cisco currently only has one service module firewall, the ASA SM for the Catalyst 6500-E
- SM firewalls have no physical interfaces and rely entirely on the existing switching infrastructure for packet flow
- It uses VLANs to redirect which packets are inspected or bypassed
- Appliance firewalls can be deployed in more places in the network but require physical cabling
- Additional services are available (e.g. remote access VPN) on physical firewalls that don't exist on blade firewalls (yet)
- Both types support multi-context mode
- Both types support routed mode and transparent mode firewalling

Physical Firewalls: ASA 5500-X Mid Range

- 1RU successor to ASA 5500 series (5510, 5520, 5540, 5550)
- Built in Crypto Acceleration card
- SSD slot for NGFW card
- Supports ASA clustering (2 units max) as of 9.1.4

ASA 5545-X/5555-X



Status LED's

I/O Expansion Slot

Serial Console

8 x 1GE Cu Ports

Redundant
Hot Swappable PSU

Physical Firewalls: ASA Service Module

- ASA SM supported only in Cat 6500-E chassis today
- Critical design around SVI placement for L3
- Up to 4 ASA SMs in one 6K chassis
- ~16gbs multiprotocol throughput per blade
- Runs ASA code
- No VPN support today except for management (future release)
- No clustering support today



Physical Firewalls: ASA 5585 Appliances

- 2 slots (2 RU): FW+FW, FW+IPS or FW+NGFW
- Top end 5585s provide 4 10GE ports (SFP)
- I/O card or additional IPS module will add 4 more 10GE ports
- 20 Gbps multiprotocol per appliance (5585-60)
- 10M connections per appliance (5585-60)
- BreakingPoint Test Results: <http://blogs.ixiacom.com/ixia-blog/cisco-asa-live-validation-with-breakingpoint-firestorm-ctm/>
- Miercom report here: <http://www.miercom.com/2011/06/cisco-asa-5585-x-vs-juniper-srx3600/>

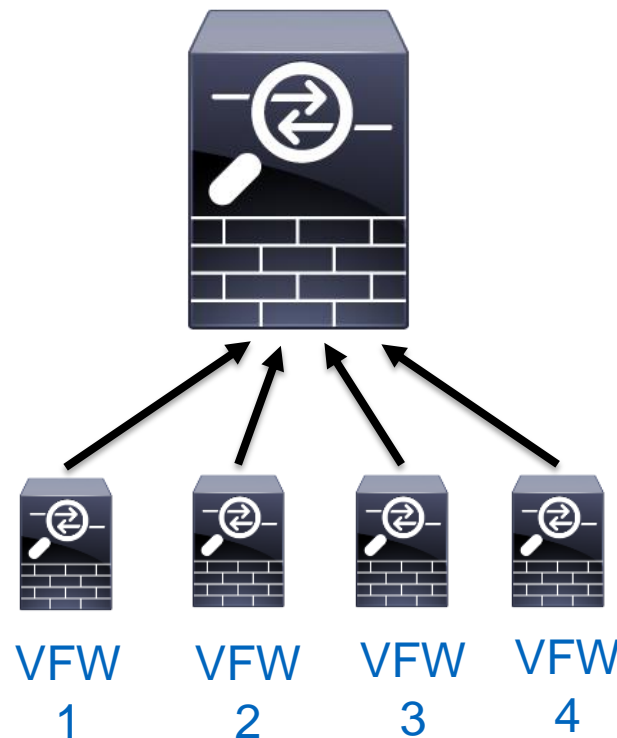


Virtualised Firewalls and Virtual Firewalls

- Two types: multi-context mode and virtual firewalls
- Multi-context mode was originally designed for SMT (Secure Multi Tenant) deployments and is a licensed feature
- Virtual firewalls are software-only firewalls running in a hypervisor
- Cisco has two virtual firewalls: the Virtual Security Gateway (VSG) and the ASA1000V
- Both require the Nexus 1000V distributed virtual switch and an “Advanced” license
- Virtual firewalls can be deployed rapidly with typical orchestration tools, etc. but there is an added layer of operational complexity
- Virtual firewalls are heavily dependent on available RAM and CPU on the host server
- We’ll cover virtual firewalls in the next section

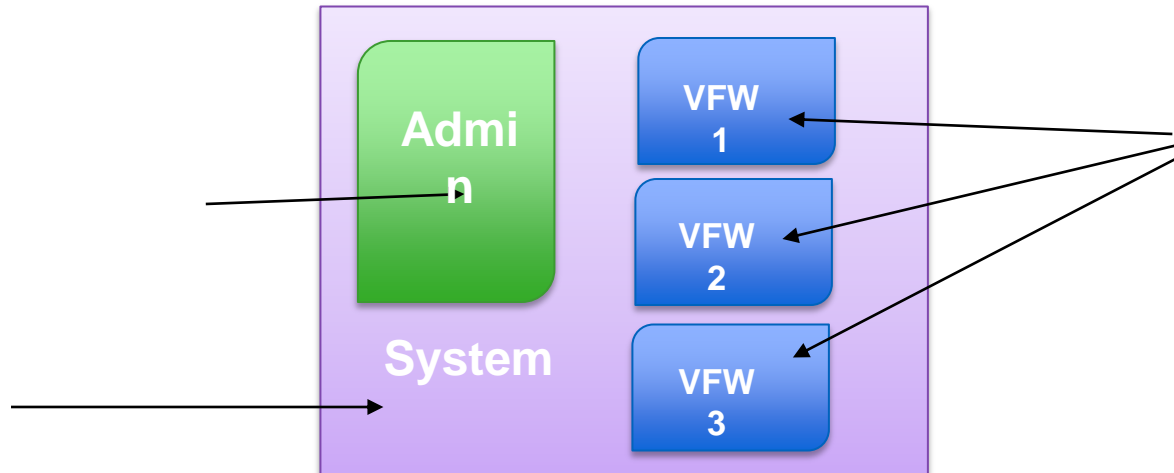
Virtualised Firewalls

- Multiple virtual firewalls in one physical chassis
- Each virtual firewall is considered a “context”
- Maximum number of virtual firewalls in one physical appliance is 250
- Physical interfaces are mapped to contexts and each context maps to a configuration
- Commonly deployed in VRF environments at intersection points



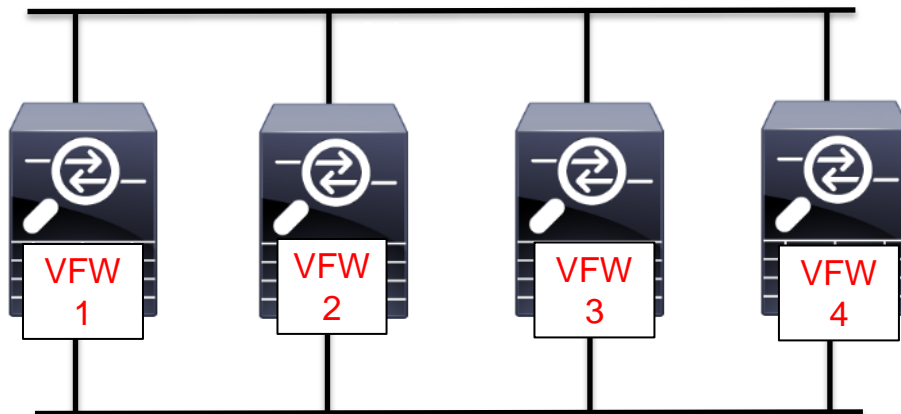
How the Virtualised Firewall is Configured

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



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

4 Virtualised Firewalls - Common Deployment



- Firewalls can be in transparent or routed mode or both (mixed mode 9.0+)
- Physical links are typically trunks but could be physical interfaces
- Contexts in routed mode can share VLANs, but not in transparent mode

Multi Context Mode Configuration

System Context Configuration

```
interface Ethernet0/0
!
interface Ethernet0/0.1
  vlan 10
!
interface Ethernet0/0.2
  vlan 20
!
interface Ethernet0/1
!
interface Ethernet0/1.1
  vlan 11
!
interface Ethernet0/1.2
  vlan 21
!
interface Ethernet0/2
!
interface Ethernet0/3
!
class default
  limit-resource All 0
  limit-resource ASDM 5
  limit-resource SSH 5
  limit-resource Telnet 5

!
admin-context admin
context admin
  allocate-interface Ethernet0/2 outside
  allocate-interface Ethernet0/3 inside
  config-url disk0:/admin.cfg
!
context vfw1
  allocate-interface Ethernet0/0.1 outside-vfw1
  allocate-interface Ethernet0/1.1 inside-vfw1
  config-url disk0:/context1.cfg
!
context vfw2
  allocate-interface Ethernet0/0.2 outside-vfw2
  allocate-interface Ethernet0/1.2 inside-vfw2
  config-url disk0:/context2.cfg
```


Multi Context Mode Configuration

Virtual FW 1 Context Configuration

```
ciscoasa/vfw1 (config)# show run
ASA Version 9.0
!
hostname vfw1
enable password 8Ry2Yjlyt7RRXU24 encrypted
!
interface inside-vfw1
 nameif inside
 security-level 100
 ip address 172.17.1.1 255.255.255.0
!
interface outside-vfw1
 nameif outside
 security-level 0
 ip address 10.2.2.1 255.255.255.0
```

To Virtualise the ASA or Not?

- Good fit for SPs who want to deploy a single appliance for multiple customers
- Good fit for VRF segmentation where VLANs map to VRFs
- Can't virtualise CPU or memory, careful for network surges
- Can't easily share interfaces in transparent (L2) mode
- Operationally more complex, management tools treat each context like a separate firewall
- Licensed feature \$\$\$
- Some features aren't compatible with virtualisation
- Can't easily "reboot" a context

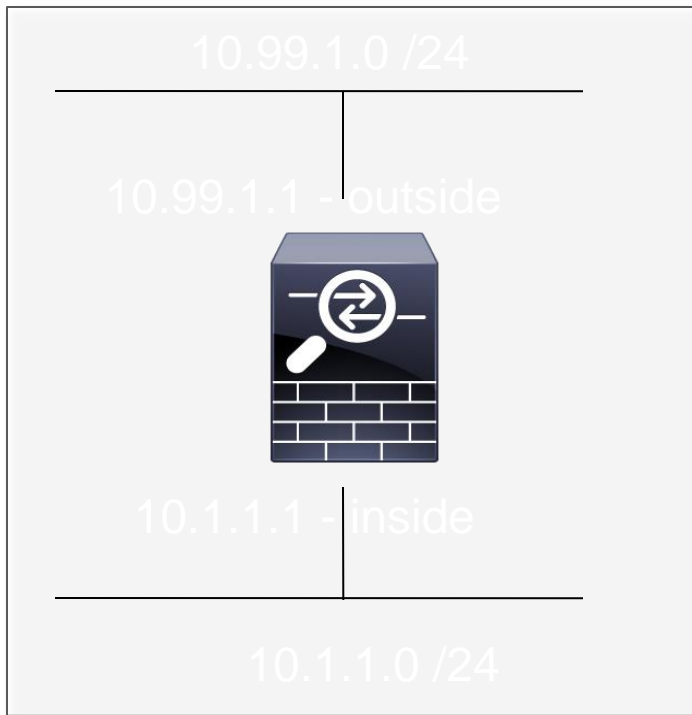


Deployment Modes

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
- **Service Tag Switching Mode** is for fabric integration where policy is enforced between two tags with no network interaction
- **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



```
hostname ciscoasa
!  
interface GigabitEthernet0/0  
 nameif outside  
 security-level 0  
 ip address 10.99.1.1 /24  
!  
interface GigabitEthernet0/1  
 nameif inside  
 security-level 100  
 ip address 10.1.1.1 /24  
!
```

What is a Transparent Mode Firewall?

- Transparent Firewall (L2) mode provides an option in traditional L3 environments where existing services can't be sent through the firewall
- Very popular architecture in data centre environments
- In L2 mode:
 - Routing protocols can establish adjacencies through the firewall
 - Protocols such as HSRP, VRRP, GLBP can pass
 - Multicast streams can traverse the firewall
 - Non-IP traffic can be allowed (IPX, MPLS, BPDUs)
 - Allows for three forwarding interfaces, inside and outside and DMZ
 - NO dynamic routing protocol support or VPN support
 - Specific design requirements, reference Configuration Guide for details

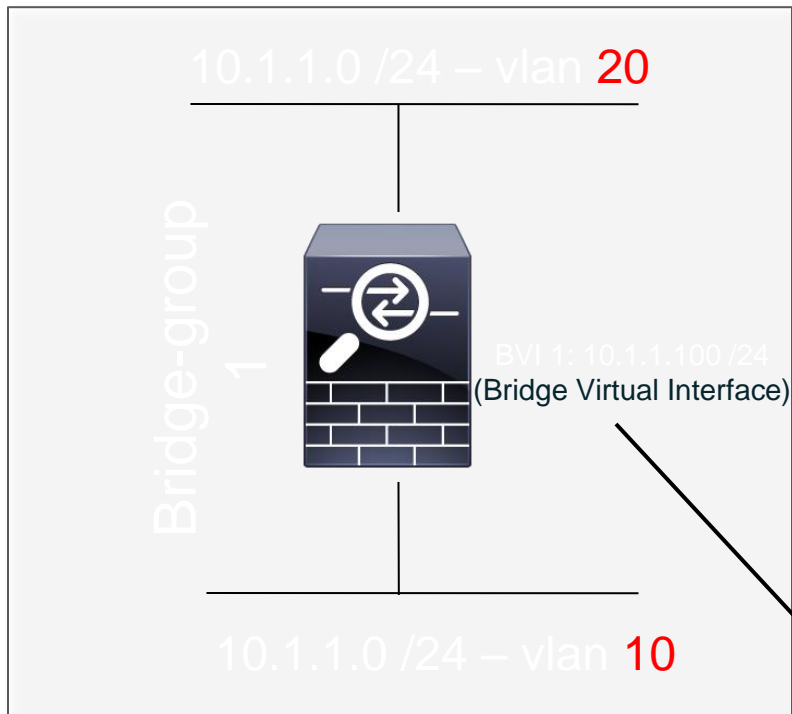
How Does Transparent Mode Work?

- Firewall functions like a bridge (“bump in the wire”) at L2, only ARP packets pass without an explicit ACL
- Still can use traditional ACLs on the firewall
- Does not forward Cisco Discovery Protocol (CDP)
- **Same** subnet exists on all interfaces in the bridge-group
- **Different** VLANs on inside and outside interfaces
- In addition to Extended ACLs, use an EtherType ACL to restrict or allow L2 protocols

Transparent Mode Requirements

- A BVI address is **required** for both management and for traffic to pass through the transparent firewall
- Set default gateways of hosts to L3 on far side of firewall, NOT the management IP of firewall
- Up to 4 interfaces are permitted per bridge-group
- In multi-context mode an interface can not be shared among contexts (virtual firewalls)

Transparent Mode Configuration (2 Interfaces)



```
firewall transparent
hostname ciscoasa
!
interface GigabitEthernet0/0
vlan 20
nameif outside
security-level 0
bridge-group 1
!
interface GigabitEthernet0/1
vlan 10
nameif inside
security-level 100
bridge-group 1
!
interface BVI1
ip address 10.1.1.100 255.255.255.0
```

What is STS Mode Firewall?

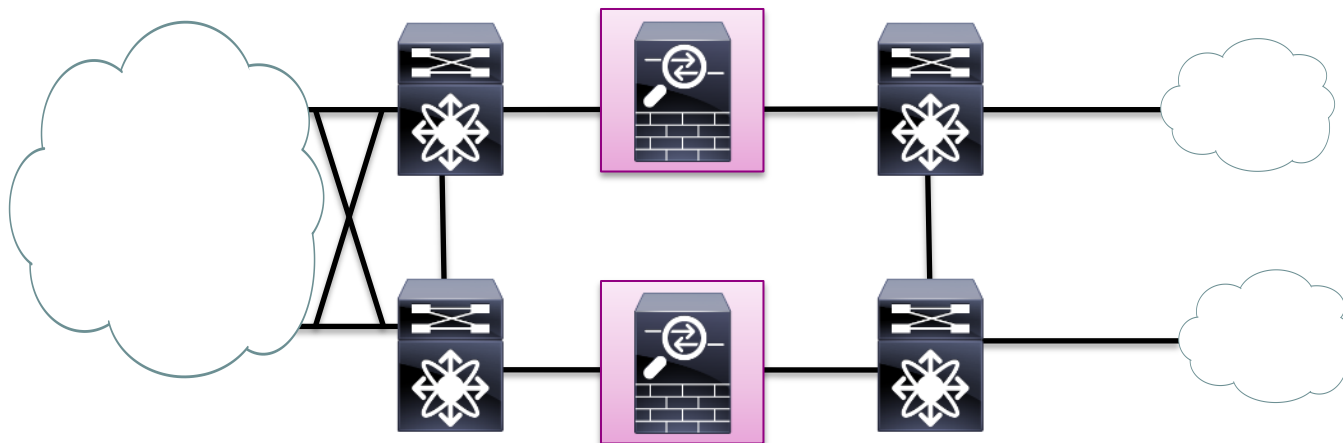
- ASA security policy on packets between two VxLAN tags
- Similar to Transparent Firewall (L2) mode with no tables for tracking MAC address (no network interaction)
- The Fabric can take over network interaction and add stateless filtering in Nexus 9000 series switches
- ACI integration leverages STS mode with ASA hardware and ASA v
- ASA is 'stitched' or 'graphed' into communication between two EPGs (end point groups) with out changes to IP settings fronting the app
- Same supported feature notes apply as in Transparent Firewall mode



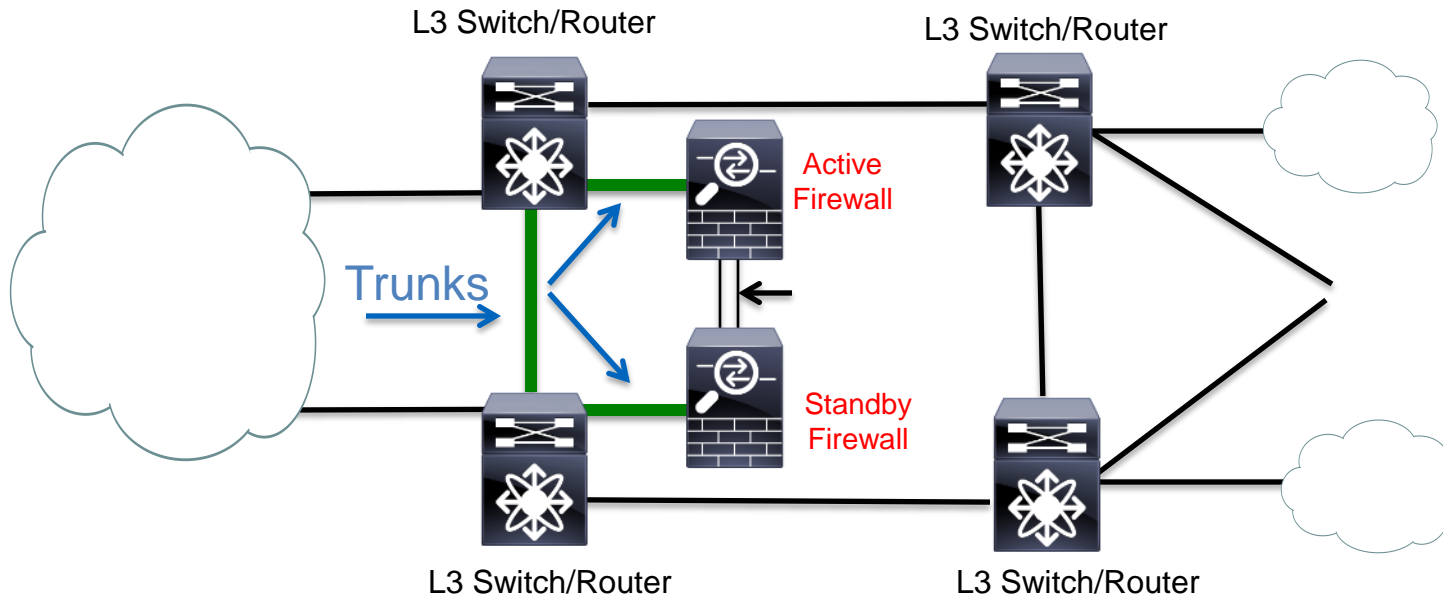
Transparent Mode FW Architecture

L2 FW Between Two L3 Devices

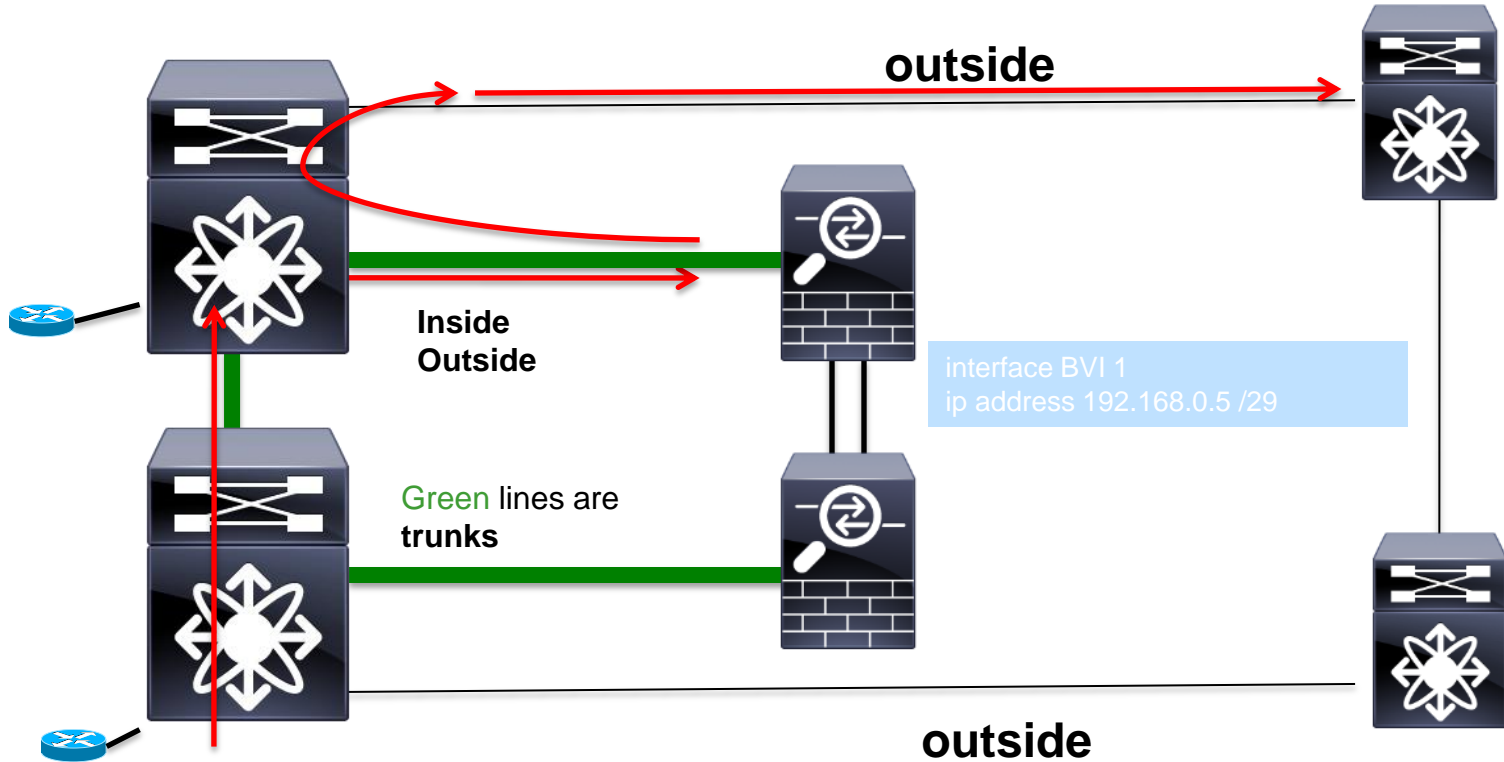
- These are L3 point-to-point links that connect to the routed core
- Stateful inspection point is required a L2 firewall between L3 links
- Firewall is processing at L2 (VLANs) while L3 services are unaffected if permitted by firewall access control list (ACL)



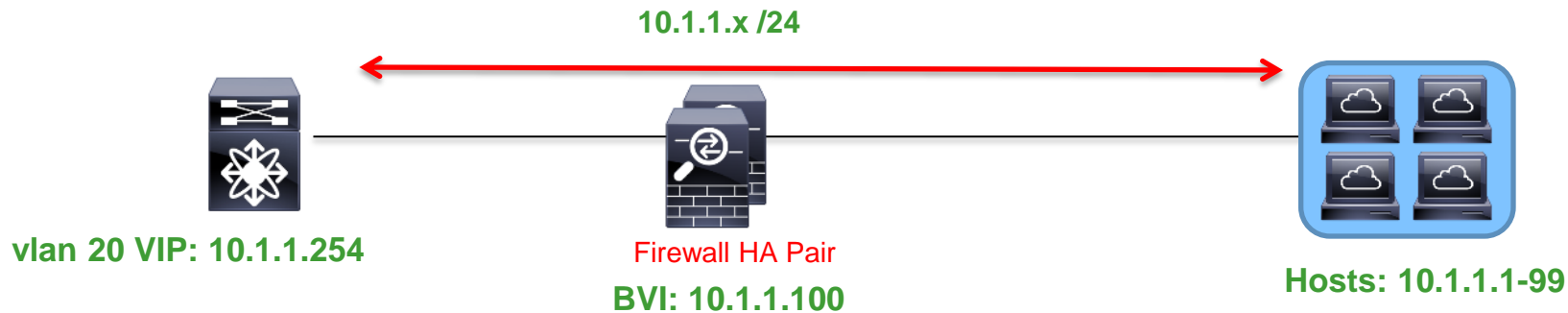
L2 FW Logical View



L2 FW Detailed View



Data Centre: ASA L2 FW – Design #1



- ASAs in transparent mode with upstream L3 gateway
- Server gateway on **outside** of firewall
- Firewall is L2 adjacent and in path to hosts
- Segmentation through VLAN assignment

Data Centre: ASA L2 FW – Design #2

Firewalls for Intra-VDC Traffic

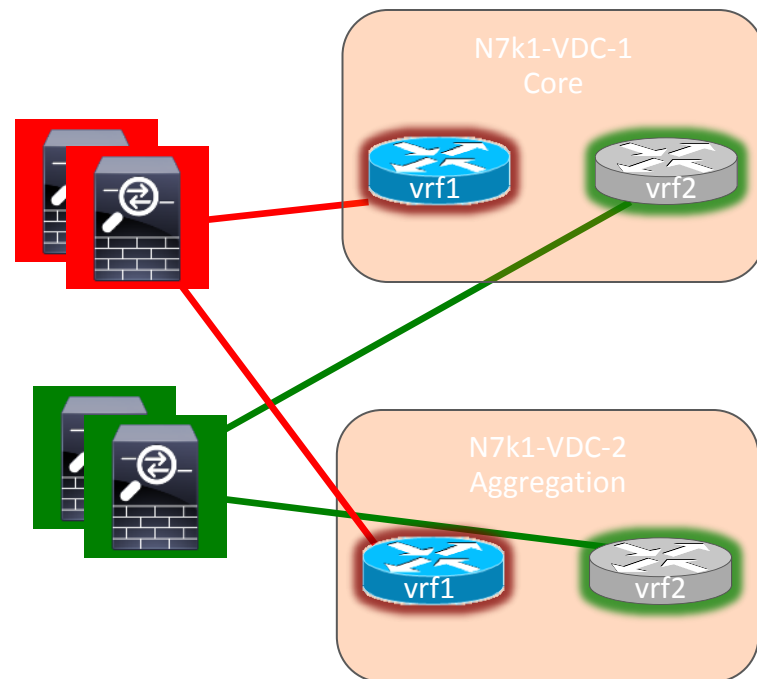


- ASA in either L2 or L3 mode, L2 is optimal in most cases
- Add VRFs on Cat 6500 or Nexus 7K for segmentation
- Server gateway **inside** of firewall
- Minimises firewall failures, route around failures if needed

ASA L2 FW – Design #3

Firewalls for Inter-VDC Traffic

- Transparent (L2) firewall services are “sandwiched” between Nexus VDCs
- Allows for other services (IPS, LB, etc) to be layered in as needed
- ASAs can be virtualised to for 1x1 mapping to VRFs
- Useful for topologies that require a FW between aggregation and core
- Downside is that most/all traffic destined for Core traverses FW; possible bottleneck, etc.
- Firewalls could be L2 or L3

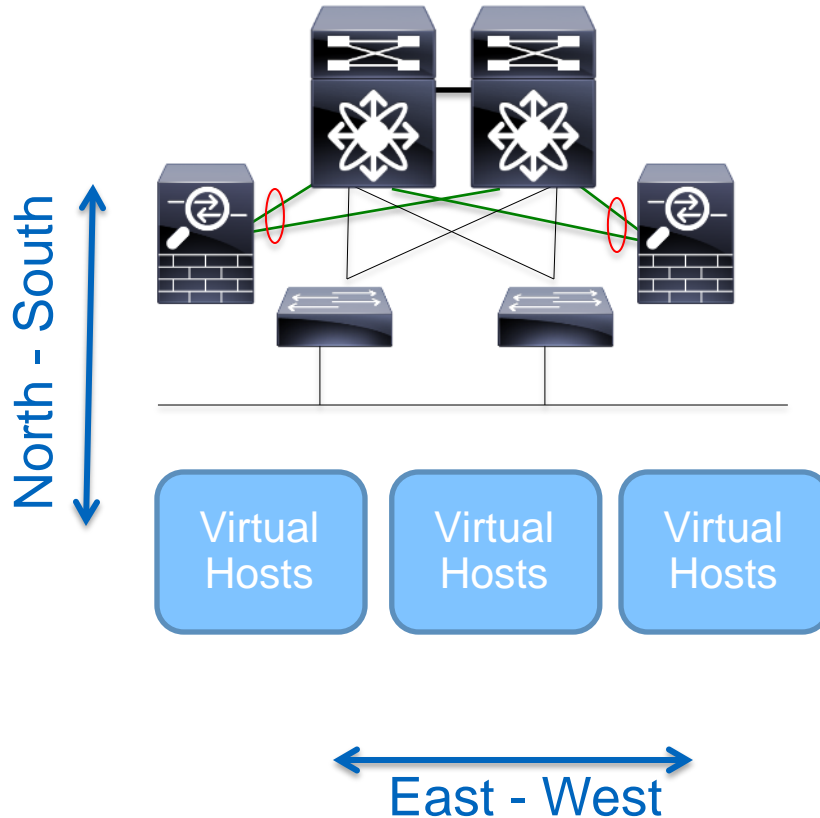




Virtual Firewalls

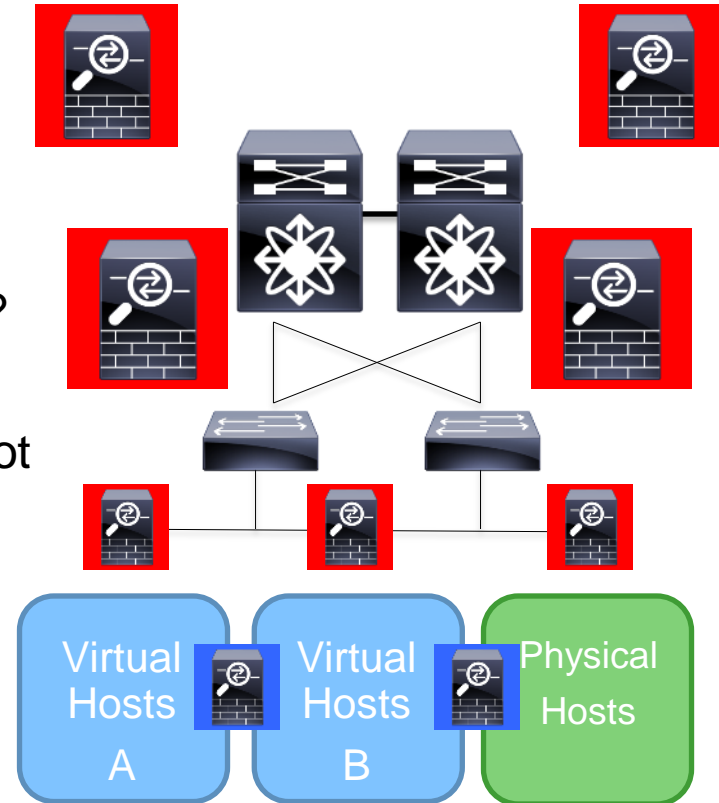
What are North-South and East-West Flows?

- North-South (N-S) flows are typically flows to and from Access layer to Aggregation Layer and Core
- East-West (E-W) flows typically stay either within a zone or between zones and often server to server traffic



Centralised or Decentralised Firewalls or Both?

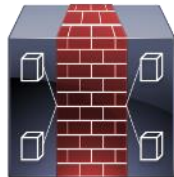
- Centralised firewalls are the traditional approach to virtualised host security
- Often a transitional architecture
- Firewalls in the core, aggregation or edge?
- Big challenge is scalability
- Usually the limiting factor is connections not bandwidth
- How to handle a requirement for L2 separation of hosts?
- How to address virtual host mobility?



Cisco's VPath Virtual Firewalls

VSG and ASA1000V

- Cisco has two virtual firewalls: the ASA 1000V and the Virtual Security Gateway (VSG)
- Each runs as a virtual machine in VMWare or HyperV
- Both are managed via Virtual Network Management Centre (VNMC)
- Both are licensed per CPU socket
- They are complementary to each other and require the Nexus 1000V Distributed Virtual Switch and utilise a new forwarding plane, **vPath**



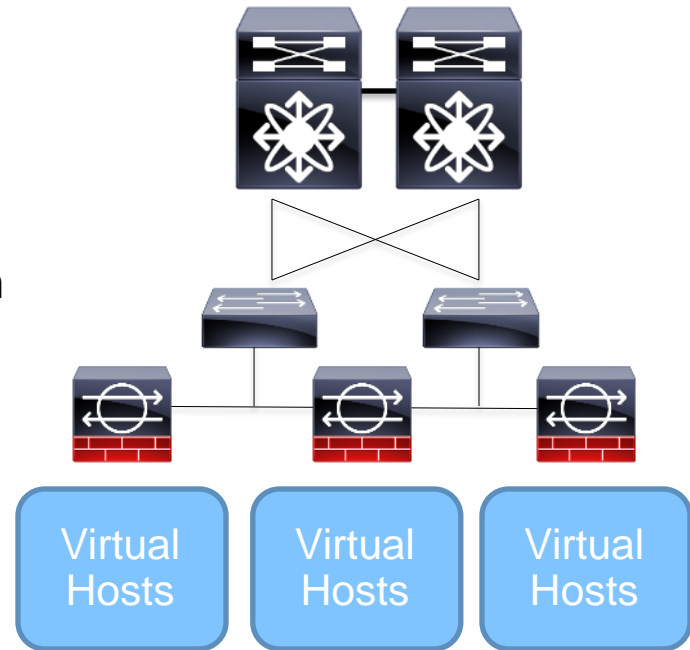
Virtual Security Gateway



ASA
1000V

The ASA1000V Cloud Firewall

- ASA1000V is a software-only version of an ASA appliance—an edge firewall with **limited features**
- Runs ASA codebase in a virtual machine in L3 mode only
- Supports S2S IPSEC VPN (not RA VPN)
- Can be deployed in active/standby HA
- Management via ASDM or VNMC but not both
- Not a replacement for physical appliance!



4 interfaces: inside, outside, failover and management

Introducing the Virtualised ASA (ASA v)

- **Scheduled release spring 2014**
- Developed due to customer feedback for a complete ASA firewall running as a virtual machine
- No Nexus1000V requirement
- Will support VMWare first then other hypervisors
- Has all ASA features with some exceptions
- No support for:
 1. ASA clustering
 2. Multi context mode
 3. Etherchannel interfaces
 4. Active/Active Failover (requires multi context mode)



ASA v Firewall
(Virtualised ASA)

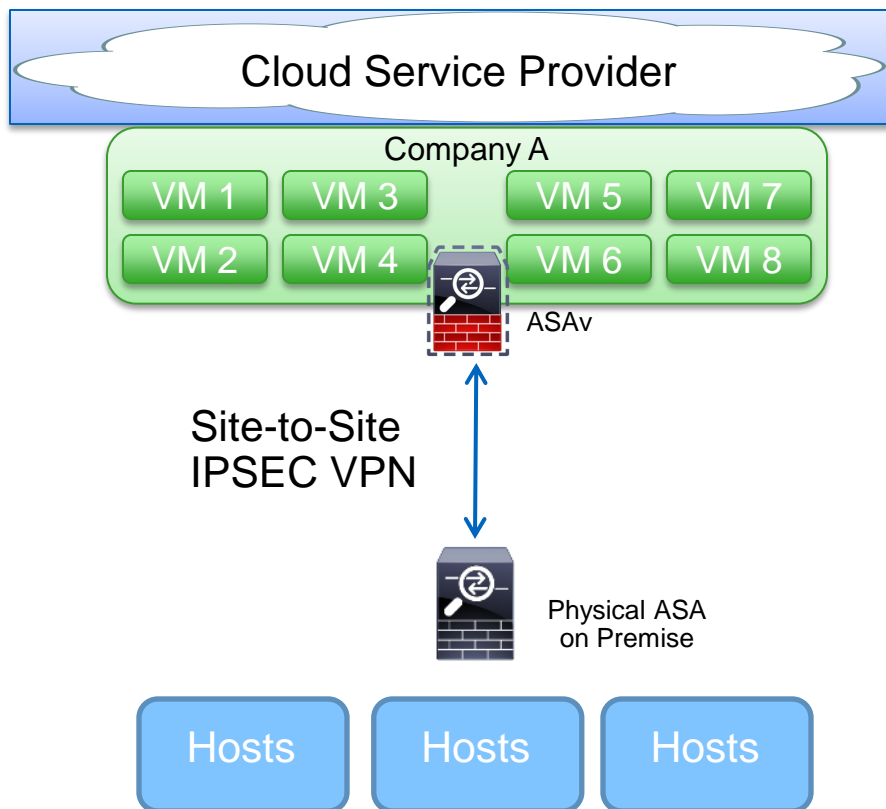
ASAv: A Deeper Look

- Supports ALL features of hardware ASA except those noted previously
- At release will be running ASA 9.2 code and features
- Up to 10 interfaces (VMWare maximum)
- Flexible licensing –based on vCPU usage, intended to simplify
- Managed like a hardware ASA: CLI, ASDM or Cisco Security Manager (CSM)
- Adds VXLAN support (up to 200)
- REST API allows for programmatic deployment and management

ASAv: Deployment Best Practices

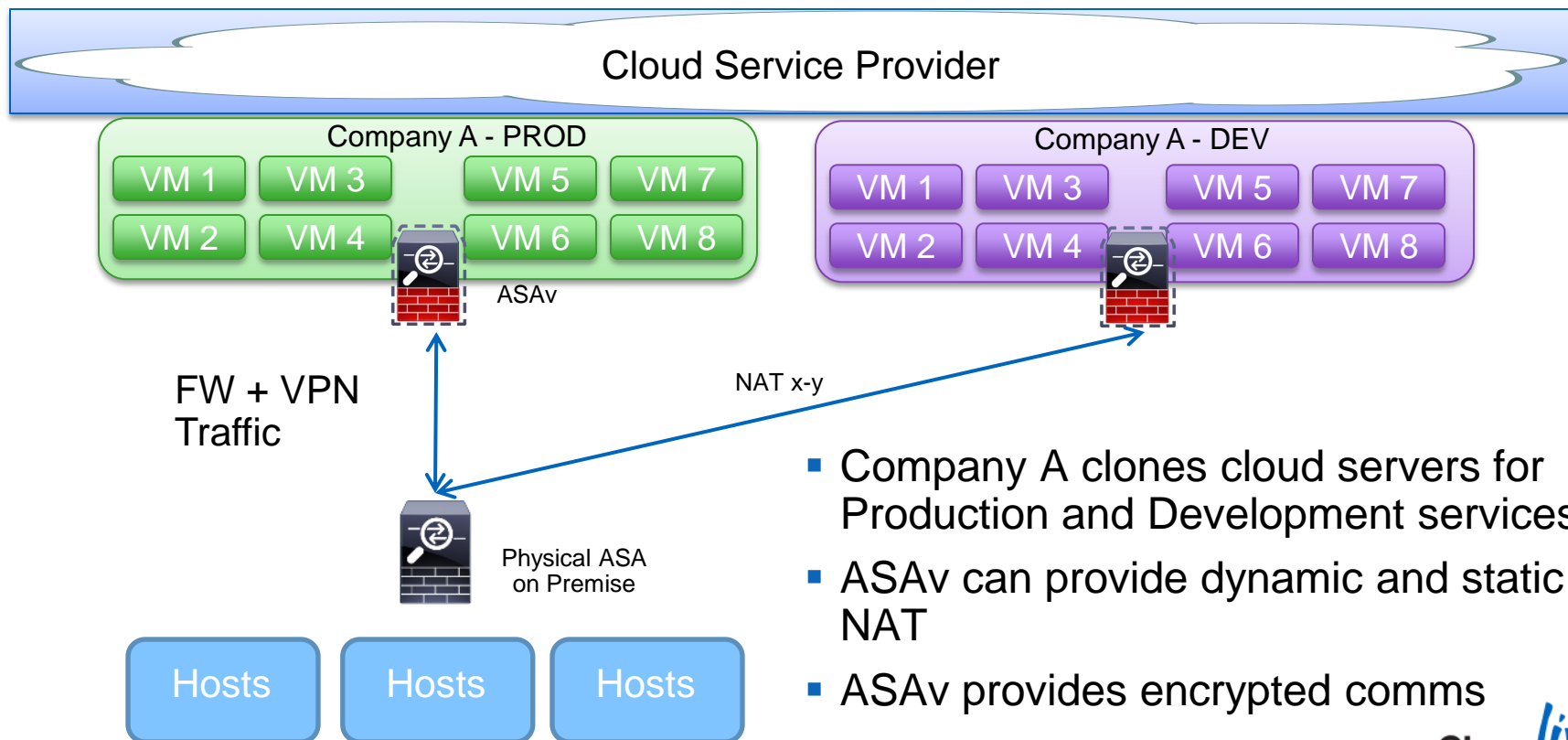
- Stateful inspection at the edge or for inter-VM traffic
- Routed (L3) or transparent (L2) mode firewall
- Multi-tenant environments
- Cloud environments that require scalable, on demand, stateful access control or remote access VPN
- Where ASA1000V is deployed today
- Performance is based on underlying hardware: single ASAv consumes 1 vCPU and 2GB of RAM
- Maximum of 4 vCPUs, licensed accordingly

ASAv Deployment: Public Cloud



- Company A has moved to virtualised cloud based servers
- Requires connectivity between existing hosts (physical or virtual)
- ASAv acts as default gateway to cloud servers, DHCP services etc
- S2S IPSEC VPN tunnel connects existing infrastructure to cloud
- Other VPN devices can establish S2S or RA VPN tunnels with ASAv

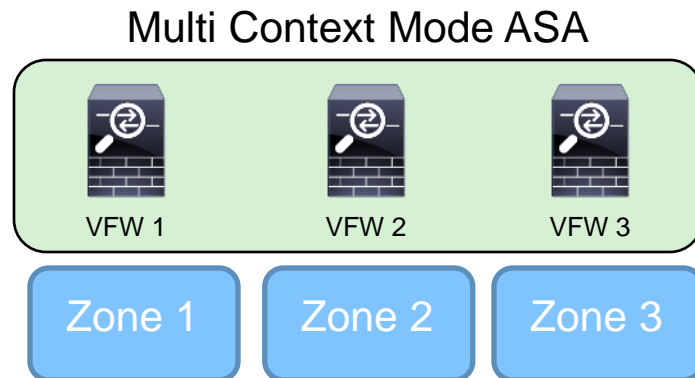
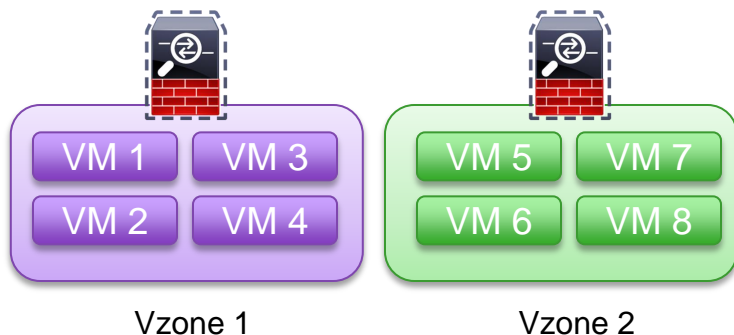
ASAv Deployment with NAT



- Company A clones cloud servers for Production and Development services
- ASAv can provide dynamic and static NAT
- ASAv provides encrypted comms

ASAv Deployment: Cloud Security FW+VPN

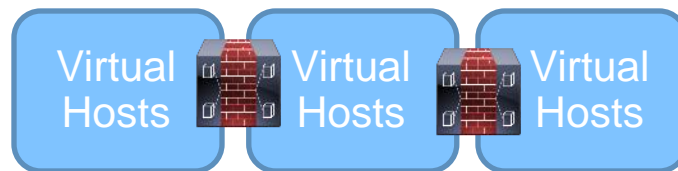
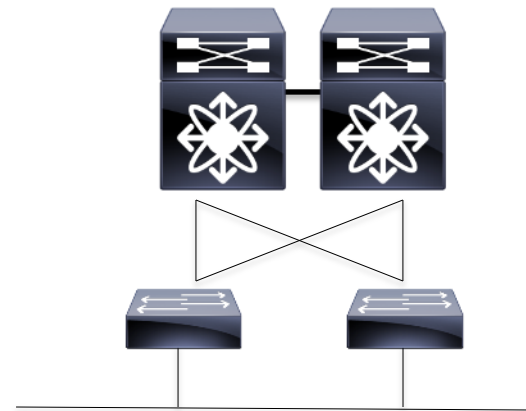
- Today multi context mode on ASA is used to provide firewall inspection for multi tenant and multi zone environments
- Trunks are typically used to transport zone and tenant traffic
- Challenge of E-W scale requires more firewall resources and scalable solution



- ASAv provides edge firewall and can scale for E-W buildout
- Each tenant or zone gets one or more ASAv for FW + VPN
- Scaled VPN termination for S2S and RA VPN clients

What is the Virtual Security Gateway?

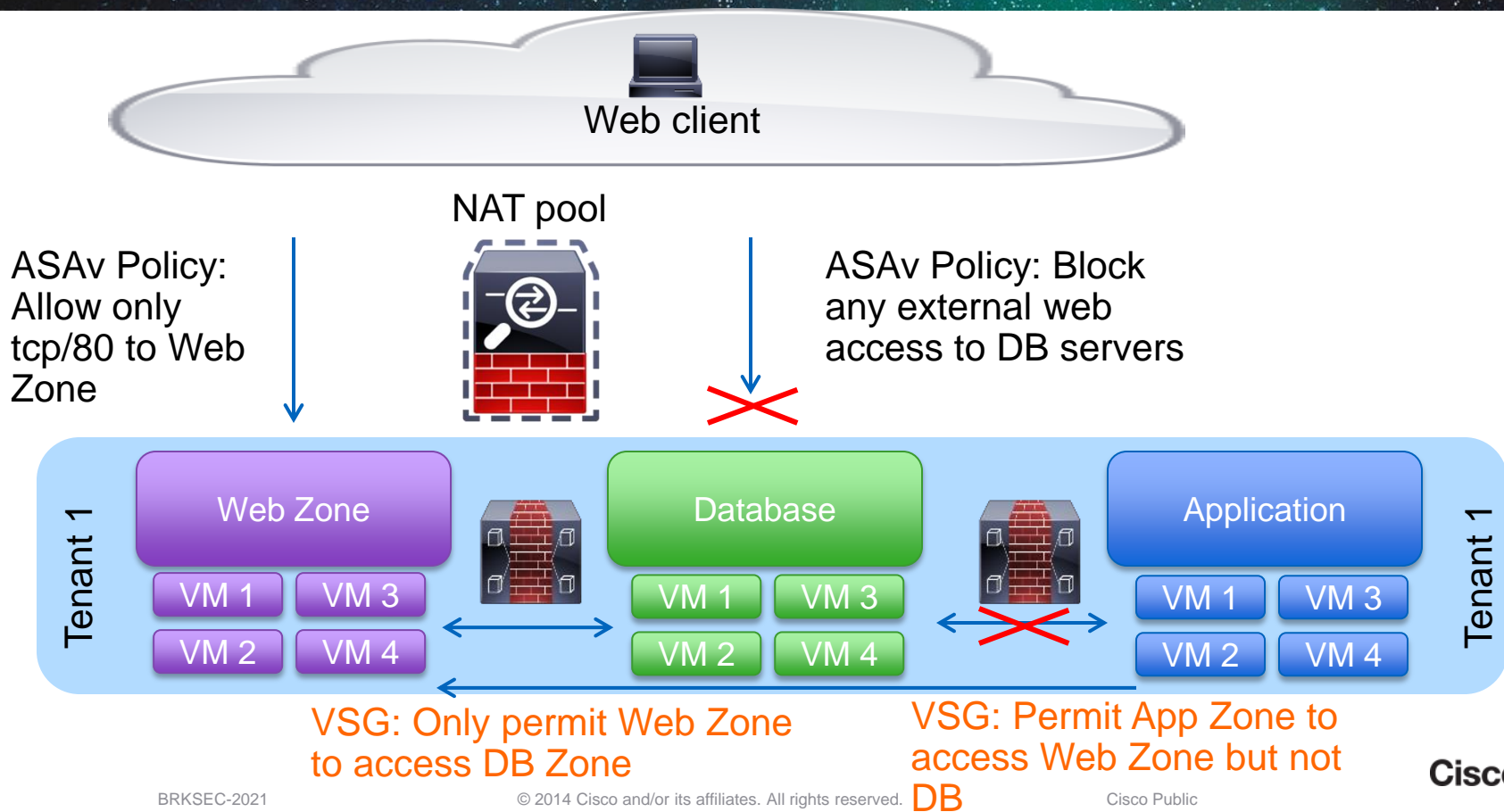
- VSG is a L2 firewall that runs as a virtual machine “bump in the wire”
- Similar to L2 transparent FW mode of ASA
- It provides stateful inspection between L2 adjacent hosts (same subnet or VLAN)
- It can use VMware attributes for policy
- Provides benefits of L2 separation for East-West traffic flows
- One or more VSGs are deployed per tenant



VM Attributes Used by VSG (Partial List)

Name	Meaning	Source
vm.name	Name of this VM	vCenter
vm.host-name	Name of this ESX-host	vCenter
vm.os-fullname	Name of guest OS	vCenter
vm.vapp-name	Name of the associated vApp	vCenter
vm.cluster-name	Name of the cluster	vCenter
vm.portprofile-name	Name of the port-profile	Port-profile

ASAv and VSG – 3 Tier Server Zone



ASAv and VSG Compared

	ASAv with 4 vCPU	Virtual Security Gateway
Throughput	1-2GB stateful	vPath
Max Concurrent Sessions	500,000	256,000
Max Conns/Sec	20,000	6K-10K (1vCPU/2vCPU)
S2S VPN Sessions	750	NA
AnyConnect® Sessions	750	NA

VSG Deployment Guide: http://www.cisco.com/en/US/prod/collateral/modules/ps2706/ps11208/deployment_guide_c07-647435.html

Comparing Cisco Virtual Firewalls

ASAv	ASA1000V (Edge)	Virtual Security Gateway
L2 and L3 mode	L3 routed mode only	L2 mode (transparent)
Dyn and static routing	Static routes only	No routing
DHCP server and client support	DHCP server and client support	No DHCP support
S2S and RA VPN	Supports site-to-site IPSEC	No IPSEC support
Managed via CLI, ASDM, CSM	Managed by ASDM and VNMC	Managed by VNMC only
Full ASA code, CLI, SSH, REST API	Uses ASA code, CLI, SSH	Minimal config via CLI, SSH



Deploying Firewall High Availability

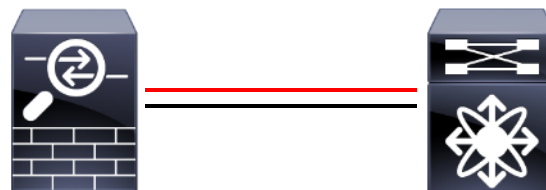
Firewall High Availability Options

- Like any other critical network device, firewalls must be deployed in a highly available manner
- This includes ports, links, data plane and control plane
- For over 15 years the standard for data plane redundancy has been the **Active/Standby** model
- **For:** no single point of failure, stateful failover
- **Against:** Deployed only in pairs, no sharing of load
- This section includes a deep dive on ASA clustering feature
- First let's explore port redundancy options

Interface Redundancy: Backup Interfaces

- Backup interfaces effectively aggregate two physical interfaces as one logical interface
- If one of the member interfaces goes down the other takes over (Active/Standby model)
- No link aggregation, only L1 redundancy
- Can only be deployed in pairs
- Up to 8 pairs of redundant interfaces can be configured

```
interface redundant 1
member-interface tengigabitethernet 0/6
member-interface tengigabitethernet 0/7
nameif inside
ip address 10.1.1.2 255.255.255.0
```



Red line is active link
Black line is standby link

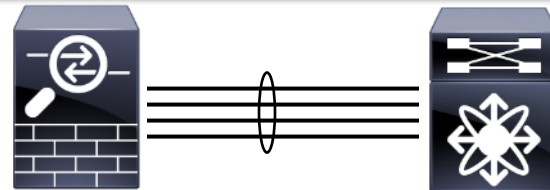
Interface Redundancy: Port Channels

- Port channel support was added to the ASA in 8.4 (2011)
- Best practice: Utilise Link Aggregation Control Protocol (LACP) where possible
- LACP dynamically adds and removes (if necessary) links to the port channel bundle
- Up to 8 active links and 8 standby links are supported in the channel*
- Link aggregation benefit
- Best practice in a Nexus DC is to use Virtual Port Channels (vPC)

* This expands from 8 to 16 in 9.2 release (spring 2014)

```
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
nameif inside
ip add 10.1.1.2 255.255.255.0
```

Actively negotiate LACP with switch



'Show Port-channel Summary' on ASA

Flags: D – down

P - bundled in port-channel

I - stand-alone s – suspended

H - Hot-standby (LACP only)

U - in use

N - not in use, no aggregation/nameif

M - not in use, no aggregation due to minimum links not met

w - waiting to be aggregated

Number of channel-groups in use: 1

Group	Port-channel	Protocol	Span-cluster	Ports
-------	--------------	----------	--------------	-------

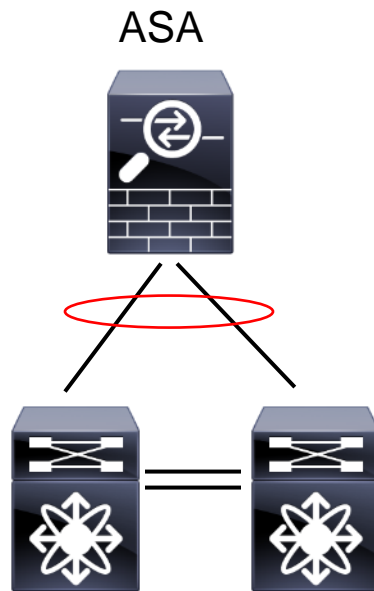
-----+-----+-----+-----+-----

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

Virtual Port Channels (VPC) and the ASA

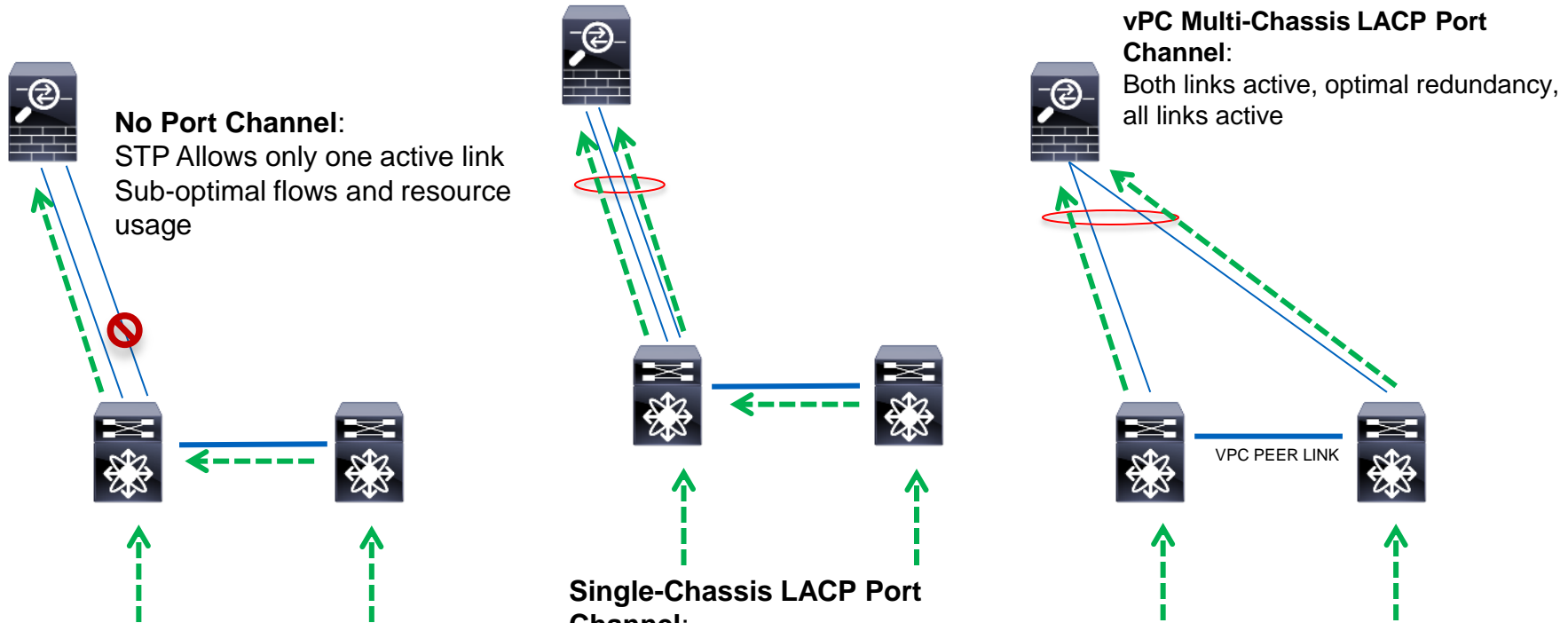
- Virtual Port Channels (vPC) are port channels where both links are actively forwarding traffic
- Typically deployed in the Data Centre
- VPC was created to solve two inherent network problems: Spanning-tree recalculation times and unused capacity in redundant L2 uplinks (due to STP blocks)
- No additional config required on ASA
- Supported with Nexus switches
- VPC Design Guide:

http://www.cisco.com/en/US/prod/collateral/switches/ps9441/ps9670/C07-572830-00_Agg_Dsgn_Config_DG.pdf



Nexus 5K/7Ks

Port Channel Options and Summary

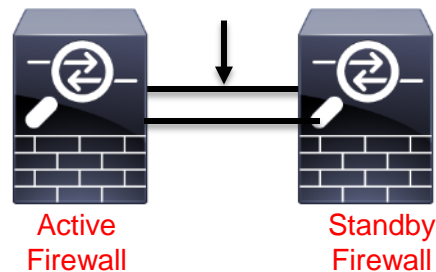




ASA High Availability

Legacy ASA Active/Standby Failover Model

- A **pair** of identical ASA devices can be configured in Failover
- Data interface connections must be mirrored between the units with L2 adjacency
- Virtual IP and MAC addresses on data interfaces move with the active unit
- Centralised management from the active unit or context
- Stateful failover “mirrors” stateful conn table between peers
- Active/Active failover requires manual traffic separation with contexts
- Stateful failover makes Active/Active impractical for scaling
- Failover delivers high availability rather than scalability!



Introducing ASA Clustering

- ASA Clustering was introduced in the 9.0 release (October 2012) to solve the problem of redundancy with scalability
- Allows for N+1 redundancy with a backup firewall for every active flow
- An ASA cluster is treated by the network as one logical firewall
- Configuration is synchronised among cluster members
- Three reasons to consider ASA Clustering:
 1. Redundancy – no single point of failure, actively using all cluster members
 2. Scalability – cluster can grow as requirements increase over time
 3. Asymmetric flow reassembly – the cluster maintains symmetry for all conns

ASA Clustering Design Guidelines

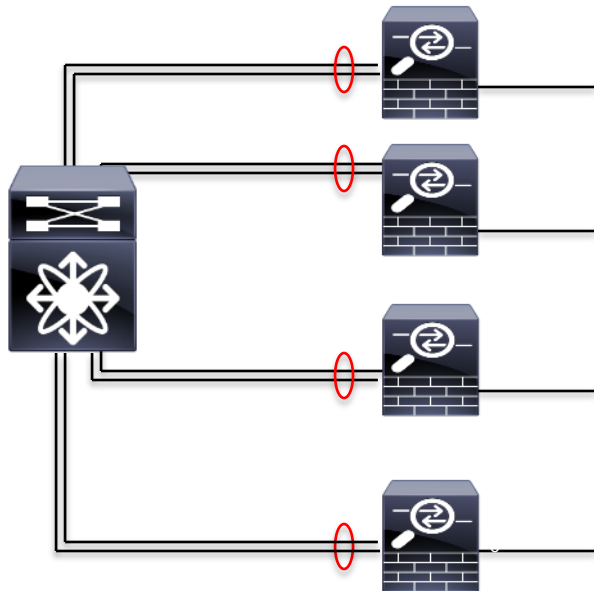
- Up to 8* ASAs (16 units 9.2.1+) are supported in a cluster (minimum of two) and all must be the same model, same SSPs, software and DRAM (only flash memory can differ)
- **Approximate maximum cluster throughput is ~ 70% of combined throughput and connections of units in the cluster**
- **Cluster control links must be sized properly for a load that is equal to or greater than the cluster data throughput (10G data requires 10G CCL)**
- Supported in routed (L3) and transparent (L2) firewall modes and multi context mode
- Requires at least one cluster control interface on ASA for cluster control plane – this is analogous to state and failover link in A/S today

* 5500-X clustering is max of 2 units

Clustering System Requirements

- Up to 8 ASA5580/5585-X in ASA 9.0 and 9.1
- Up to 16 ASA5585-X in ASA 9.2(1)+
- Up to 2 ASA5500-X in ASA 9.1(4)+
- Each ASA5580/5585-X member must have Cluster license installed
- Enabled by default on ASA5500-X except ASA5512-X without Security Plus
- 3DES and 10GE I/O licenses must match on all members
- Limited switch chassis support for control and data interfaces
- Catalyst 6500 with Sup32, Sup720, or Sup720-1GE and Nexus 7000 in ASA 9.0+
- Catalyst 3750-X and Nexus 5000 in ASA 9.1(4)+

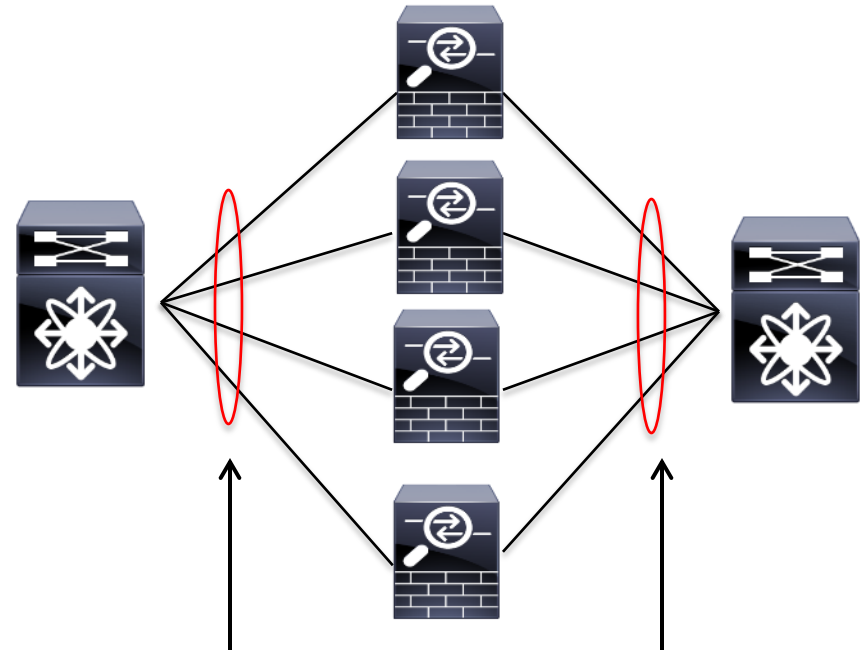
Clustering Best Practices – Control Plane



- Cluster control links must be sized accordingly (e.g. 10GE interfaces)
- Recommended to use a local port-channel on each ASA for link redundancy and aggregation
- Do NOT use a spanned port-channel for cluster control links
- Could also use ASA interface redundancy (backup interfaces) which supports up to 8 pairs of interfaces in an active-passive mode

Clustering Best Practices – Cat 6K Data Plane

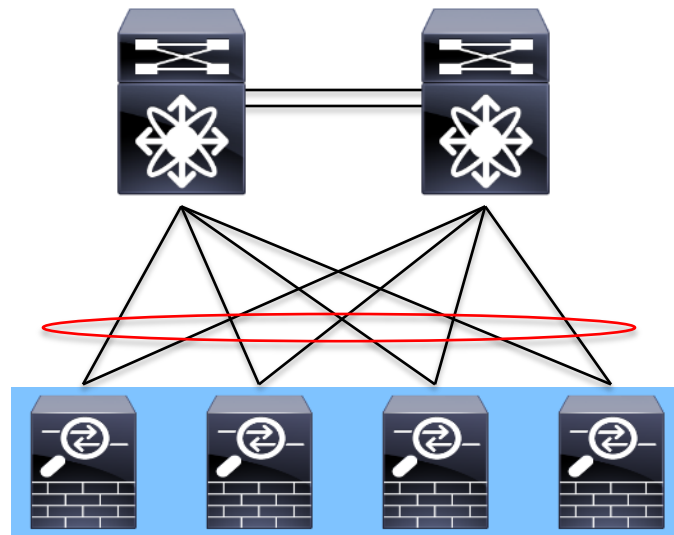
- ASA clustering relies upon stateless load balancing from an external mechanism
- Recommended method is to use a L2 spanned port-channel to a switch for ingress and egress connections
- BP is to use a symmetrical hashing algorithm like src-dest IP (the default)
- Could also use Policy Based Routing (PBR) or Equal Cost Multi-Path (ECMP); use both with Object Tracking L3 only
- Cat 6K VSS is supported with ASA clustering
- **Spanned port-channel will not come up until clustering is enabled!**



“Spanned” Port-Channels

Clustering Best Practices – Nexus 7K Data Plane

- Nexus 7K data centre offers advantages with clustering due to VPC feature
- All ASAs are dual homed to each 7K
- VPC ensures that a single link failure will have zero packet loss
- Enhancements to LACP such that ASA cluster appears as one logical firewall to rest of network
- Port channel provides packet forwarding
- ASAs in L2 or L3 mode



Basic Clustering Configuration

```
cluster group DC-SEC
```

```
key *****
```

← cluster members share the same key

```
local-unit asa1
```

← for cluster identification

```
cluster-interface Port-channel40 ip 99.99.99.1 255.255.255.0
```

```
priority 1
```

← lower is higher priority (no preempt)

```
console-replicate
```

```
health-check holdtime 3
```

```
clacp system-mac auto system-priority 1
```

```
enable
```

Clustering Data Plane Configuration

```
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
```

```
interface Port-channel 32
  port-channel span-cluster vss-load-balance
  no nameif
  no security-level
!
interface Port-channel32.101
  vlan 101
  nameif inside
  bridge-group 1

interface Port-channel32.102
  vlan 102
  nameif outside
  bridge-group 1
```

Port Channel Verification

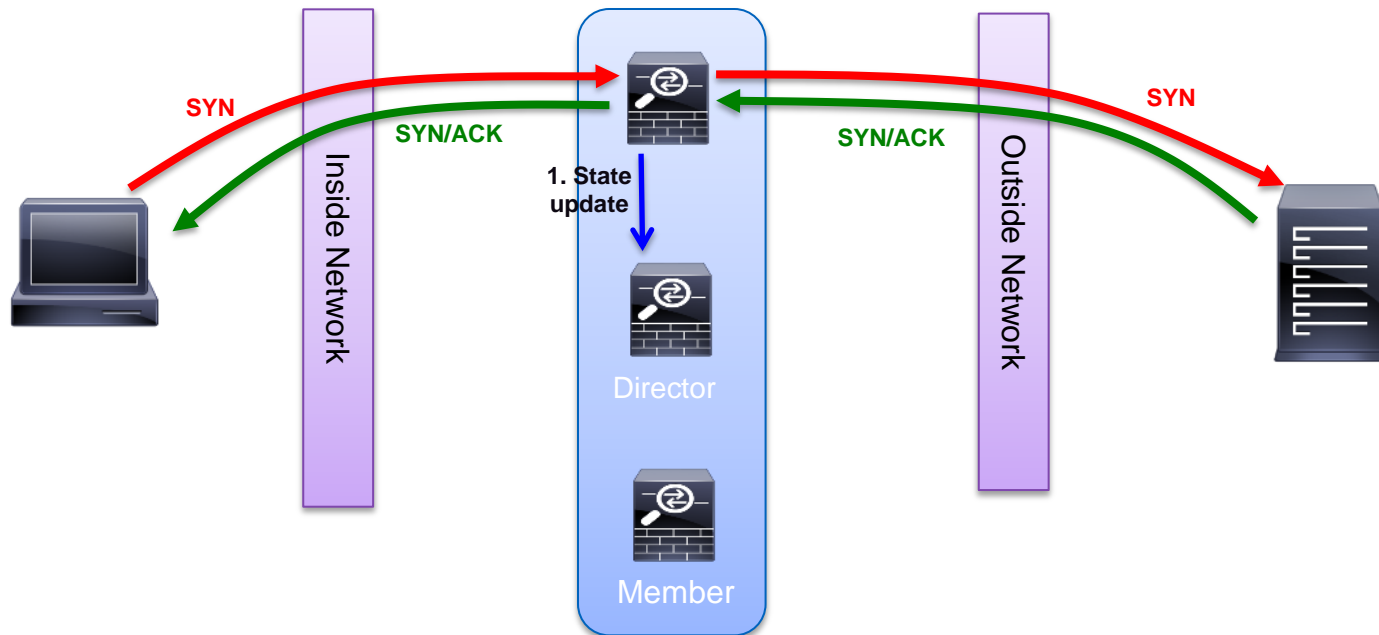
```
asa(cfg-cluster)# sh port-channel summary
```

```
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)

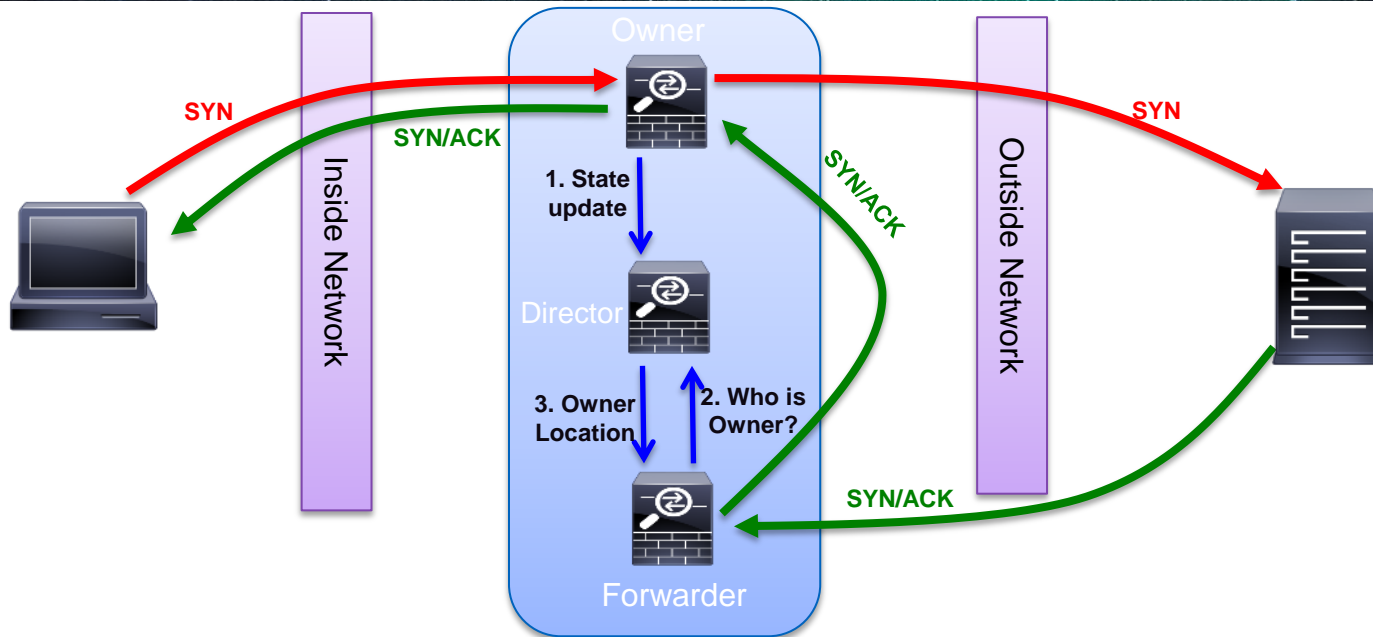
- Port channel 32 is the cluster data plane
- Port channel 40 is the cluster control plane—note that the CCL is not a “span-cluster” port-channel (best practice)
- Both are up as noted by the (U) and were negotiated via LACP
- Remember the spanned port-channel will not come up until clustering is enabled

TCP Session: Symmetric Flow



- State replication from Owner to Director, also serves as failover to provide redundancy should Owner fail
- Director is selected **per connection** using consistent hashing algorithm
- Director will act as backup should Owner fail

TCP Session: Asymmetric Flow



- Forwarder receives packet that it did not originate, queries Director
- Packet is forwarded via cluster control link to Owner who then forwards on to originating client and all subsequent packets are forwarded to Owner with no lookup
- This step is eliminated if the Owner can be derived via syn-cookies

Unsupported ASA Features with Clustering

- SSL and IPSEC remote access VPN (Site to Site VPN **is** supported)
- Legacy VPN load balancing is not supported for S2S VPNs
- Botnet Traffic Filter (BTF)
- DHCP Client, Server and Relay
- Unified Communications features and inspection engines
- WCCP
- ASA NGFW SSP
- Some application inspection features (see Release Notes)

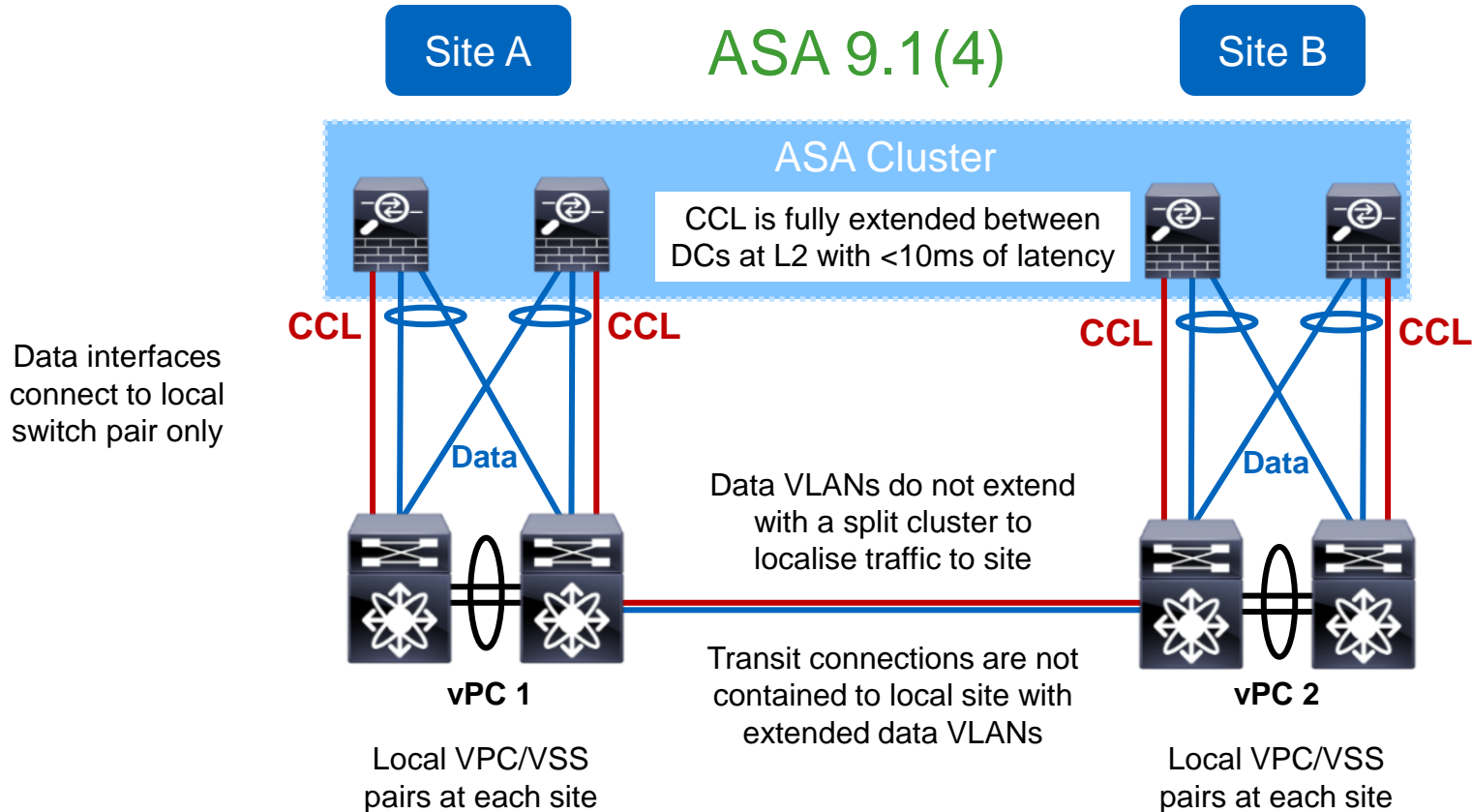


Advanced Cluster Deployments

Clustering Across Multiple Data Centres

- Until Dec 2013 ASA clustering was supported only in the **same** DC
- Increasingly customer requirements and interest were around spanning an ASA cluster across multiple DCs
- Geographically separated clusters are supported now with 9.1.4+ under these conditions:
 - Dark “Media” CCL with less than 10ms of one way latency
 - No packet overlays or loss
 - Routed (L3) firewall in individual interface mode only
 - ASA 9.2 (spring 2014) will extend Inter-DC clustering to Spanned Etherchannel mode
 - Transparent (L2) firewall only
 - Only the CCL can be used via dark media or overlay method, not data plane

Split or Single Individual Mode Cluster in Inter DC



ASA Clustering Best Practices Summary

- Use spanned port-channels for cluster data plane and local port-channels or interface redundancy for cluster control interfaces
- Use 'prompt cluster-unit state' to change prompt on firewall (e.g. asa1-master) to simplify operations and troubleshooting
- Cluster Master is for configuration replication only, all units are actively processing flows and backing up (forwarding) flows
- Size the cluster control link(s) to equal the largest data interfaces
- L3 cluster deployments will have unique L3 interfaces while L2 cluster deployments all interfaces will be the same

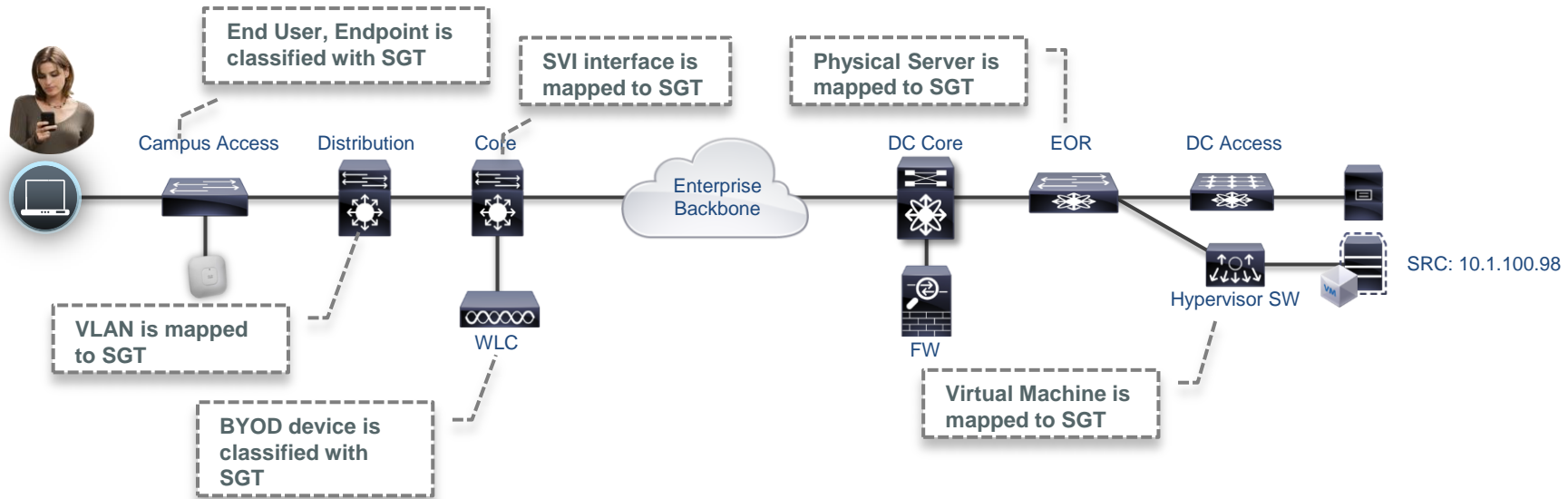


Security Group Tags

Cisco TrustSec and Security Group Tags

- Cisco created an architecture called TrustSec that uses tags in the IP header field to carry information for network based access control
- TrustSec is built upon a foundation that traffic is tagged at the edge and network devices enforce a global, consistent access policy throughout the network
- These tags are called Security Group Tags (SGT)
- ASA 9.0+ gives the ASA the capability to make policy decision based upon SGTs

Different Devices Can Assign SGTs



SGT eXchange Protocol (SXP)

- SGTs are supported in hardware
- SXP is a mechanism where devices can pull or push IP to SGT mappings from a native SGT device
- ASA supports SXP as a **listener** or a **speaker**
- ISE distributes PAC files to devices in a TrustSec domain
- SXP comms are encrypted using the PAC file (RADIUS)
- 5585-60 supports 100k IP to SGT mappings

SGT Mapping

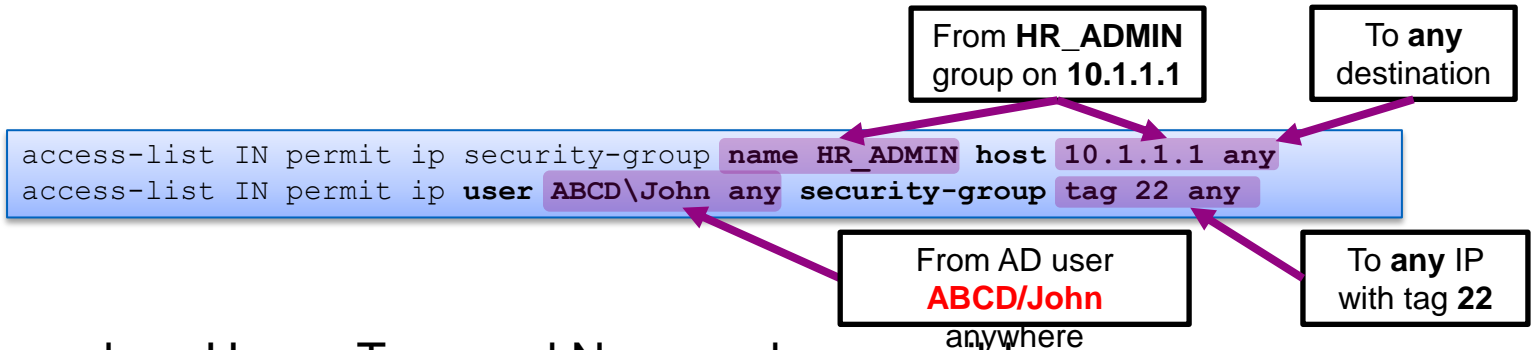
- Policy enforcement with Security Group Tags (SGTs) in ASA 9.0
 - Unique 16-bit value assigned to a certain role (SG Name)
 - Authenticated and mapped at edge switch, enforced on ASA in transit
 - Abstraction from IP address or specific identity schemes

Endpoint	Group Name	IP	SGT
HTTP Server	Server A	10.1.100.111	111
File Server	Server B	10.1.100.222	222
John Smith	Marketing	10.1.200.3	333

- Devices map IP↔SGT with Security tag eXchange Protocol (SXP)
 - ASA currently **does not** support in-line SGT frame headers

Using Identity and SG ACLs

- All entries still require IP information (could be any)
 - Identity for source only; SG Tags and Names can be source or destination
 - Names must resolve to tags, groups to users, user to IP addresses



- Syslogs show Users, Tags and Names when possible

```
%ASA-6-302013: Built outbound TCP connection 16 for outside:198.51.100.100/22
(198.51.100.100/22) (ABCD\Mary, 111:MKTG) to inside:10.0.0.2/20898 (10.0.0.2/20898) (1212)
```

Slide courtesy of Andrew Ossipov



IPv6

IPv6 and Cisco Firewalls

- Virtual Security Gateway supports IPv6
- ASA1000V **does not** support IPv6
- ASA code has supported IPv6 for many years and 9.0 release augments IPv6 features (ASA and ASASM)
- Very little performance hit with IPv6
- AnyConnect IPSEC VPN also support IPv6
- ASDM supports IPv6 addresses
- NAT46 and 64 support on ASA

Unified IPv4 and IPv6 ACLs

- Older ASA software used separate IPv4 and IPv6 interface ACLs:

```
access-list INSIDE_IPV4 extended permit ip host 10.1.1.1 any
ipv6 access-list INSIDE_IPV6 permit ip host 2001:DB8:1:1:1:1:1:1 any
access-group INSIDE_IPV4 in interface inside
access-group INSIDE_IPV6 in interface inside
```

"Any" depends on the ACL type

- ASA 9.0 and newer uses a single ACL for all IPv4 and IPv6

```
access-list IN extended permit ip host 10.1.1.1 any4
access-list IN extended permit ip host 2001::1 any6
access-list IN extended permit ip host 10.1.1.1 host 2001:DB8::10
access-list IN extended permit ip any any
```

Any IPv4

Any IPv6

Mixed IPv4 and IPv6
(Need NAT)

Any IPv4 or IPv6

- Configuration migration from earlier releases
 - Dual interface ACLs are merged
 - Contextual **any** conversion applies to ACLs only

Slide courtesy of Andrew Ossipov

ASA IPv6 Best Practices

- ACL to block unknown Router Advertisement (RA)

```
ipv6 access-list outsideACL permit icmp6 host fe80::21e:7bff:fe10:10c any router-advertisement
ipv6 access-list outsideACL deny icmp6 any any router-advertisement
access-group outsideACL in interface outside
```

```
interface vlan2
nameif outside
security-level 0
ipv6 address autoconfig
ipv6 enable
```

- Suppress ASA interface Router Advertisements

```
interface vlan2
ipv6 nd suppress-ra
```

<https://supportforums.cisco.com/docs/DOC-15973>

Summary and Conclusions

- Physical firewalls and virtual firewalls are complementary solutions
- Virtualised firewalls (multi context mode) provide a nice option for segmented networks (VRF Lite, MPLS, etc) and/or decentralised management
- Firewall clustering offers advantages over the traditional A/S model
- NSEL provides additional flow visibility over syslog events
- ASA policy can be built with user and group identity
- Security Group Tags offer an alternative scalable approach to network access control
- The ASA has robust IPv6 capabilities

Reference Links

- VPC Design Guide: http://www.cisco.com/en/US/prod/collateral/switches/ps9441/ps9670/C07-572830-00_Agg_Dsgn_Config_DG.pdf
- Virtual Multi-Tenant Data Center (2013) (VMDC) 3.01 Validated Design http://www.cisco.com/en/US/partner/docs/solutions/Enterprise/Data_Center/VMDC/3.0.1/DG/VMDC_3.0.1_DG.html
- Virtual Security Gateway (VSG) Deployment Guide http://www.cisco.com/en/US/prod/collateral/modules/ps2706/ps11208/deployment_guide_c07-647435.html
- TrustSec 2.0 Design and Implementation Guide http://www.cisco.com/en/US/partner/solutions/ns340/ns414/ns742/ns744/landing_DesignZone_TrustSec.html
- TAC Security Podcast http://www.cisco.com/en/US/solutions/ns170/tac/security_tac_podcasts.html
- ASA IPv6 Config Guide http://www.cisco.com/en/US/docs/security/asa/asa90/configuration/guide/route_ipv6_neighbor.html



Q & A

Complete Your Online Session Evaluation

Give us your feedback and receive a Cisco Live 2014 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 21 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



CISCO TM



Netflow Security Event Logging

NetFlow and Syslog for Visibility

- Syslog has been around forever, still has value
- Latest ASA syslog (9.1) Events Guide is 666 pages!
- Debug level syslog is a great way to DoS your syslog servers

- 8.2 code release (2010) introduced NetFlow v9 export option
- ASA NetFlow is called NSEL (NetFlow Secure Event Logging)
- NSEL is different than traditional NetFlow export in that the exports are not “sampled”

Syslog vs NetFlow on ASA

- Syslog on ASA only sends one event per packet
- NSEL is a stateful flow tracking method that only sends (“exports”) when specific conditions are met
- Syslog and NSEL both use UDP for transport
- ASA can be configured to use TCP for syslog (not recommended)
- Both syslog and NSEL can send to multiple collectors based on policy
- Syslog has 8 logging levels, NSEL does not

NSEL Best Practices

- NSEL has three options: Track flows as they are built, torn down, updated or **denied**
- Any or all can be combined into a NSEL export policy
- Events are usually time driven like traditional NF but can also be sent on state changes
- NSEL supported both IPv4 and IPv6 flows but not conversions (NAT46 or NAT64)
- For more information see the ASA Note for Flow Collectors:
<http://www.cisco.com/en/US/partner/docs/security/asa/asa91/system/netflow/netflow.html>

NSEL Configuration in CLI

- NSEL and syslog have overlapping events so the best practice is to disable the redundant syslog events
- Sample NSEL configuration:

```
asa(config)# flow-export destination inside 10.1.1.30 2055
!! Globally Defines the destination for export
asa(config)# policy-map global_policy
asa(config-pmap)# class netflow_class
asa(config-pmap-c)# flow-export event-type all destination 10.1.1.30
```


NSEL Configuration in ASDM

Firewall> Service Policy Rules> Edit

The screenshot displays the ASDM configuration interface for NetFlow. At the top, there are tabs for 'ASA CX Inspection', 'Connection Settings', 'QoS', 'NetFlow', and 'User Statistics'. The 'NetFlow' tab is active, showing the instruction: 'Match NetFlow events with any of configured NetFlow collectors.'

Flow Event Type	Collectors
-- All --	10.1.1.30

Buttons for 'Add', 'Edit', and 'Delete' are located to the right of the table.

An 'Edit Flow Event' dialog box is open in the foreground. It contains a 'Flow Event Type' dropdown menu with the following options: -- All -- (selected), Created, Denied, Updated, and Torn Down. Below this is a 'Collectors' section with a table:

Collector	end
10.1.1.30	<input checked="" type="checkbox"/>

A 'Manage...' button is located to the right of the collector table.

Collection Tools For Visibility

- In my external lab we use multiple tools from different vendors for visibility
- Lancope StealthWatch®, Arbor Peakflow® and Live Action® are a few
- My ASAs are combining syslog with NSEL data for more granular flow details

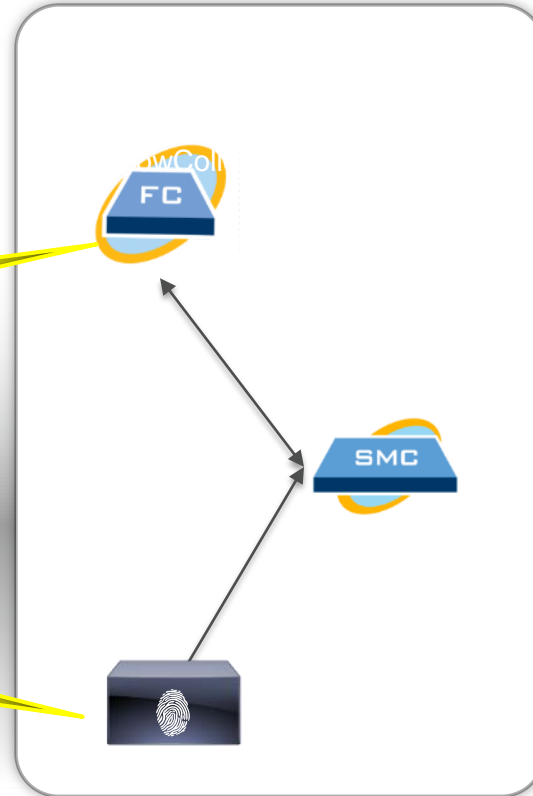
Summary - 9 records summarized into 9 records					
Host Groups	Host	CI	CI%	Alarms	Alerts
Desktops, Internal 3rd Party Managed Devices, By Location, Trusted Internet Hosts, Flickr	10.201.3.23	338,137,280	112,712%		Ping_Oversized_Packet
SMS Servers, External IPs, By Location, Flickr	(209.182.184.2)	103,869,936	1,039%		Excess_Clients, Excess_Servers, Ping, Rejects, Spoof, TCP_Scan, UDP_Scan
WebEx.com, By Function, By Location, Trusted Internet Hosts, Flickr	10.202.1.122	2,328,268	776%	High Concern Index, ICMP Flood	Ping_Oversized_Packet, Rejects
Firewalls, By Location, PGP Corp, Trusted Internet Hosts, Flickr	(10.192.0.1)	10,875,454	109%	High Concern Index	Ping, Ping_Oversized_Packet, Ping_Scan
Application Servers, By Location, Flickr	209.182.176.42	2,539,292	79%		Rejects, Spoof
WebEx.com, By Function, By Location, Trusted Internet Hosts, Flickr	(10.202.1.70)	1,083,341	76%		Rejects, UDP_Scan
Desktops, By Location, Trusted Internet Hosts, Flickr	(10.10.10.10)	409,118	75%		Rejects, UDP_Scan
Servers, Atlanta, Internal 3rd Party Managed Devices, Trusted Internet Hosts, Flickr	(10.201.0.1)	188,988	63%	Suspect UDP Activity	Rejects, UDP_Scan
By Location, PGP Corp, Trusted Internet Hosts, Flickr	(10.192.0.58)	186,579	62%		UDP_Scan

NSEL for Cyber Threat Defence (CTD)

- ASA NSEL data for deep visibility
- Cisco has an OEM relationship with Lancope's StealthWatch product
- Their console interface is used for monitoring, alerting and reporting

Correlate and display flow analysis with Identity information

Provides identity, profiling and context information through Cisco TrustSec solution



Easily Find All Traffic for a Given User

User

Device Type

Flow Table

Identity and Device Table - 541 records

Start Active Time	End Active Time	User Name	Host	Host Groups	Device Type	Domain Name	Network...
13-Feb-2012 12:27:38 PM (7 hours 6 minutes 32s ago)	Current	[REDACTED]	10.34.79.193	SJCM, Voice, Wireless Voice	Apple-iPhone	cisco.com	[REDACTED] (10.34.76.213)
13-Feb-2012 9:00:43 AM (10 hours 33 minutes 26s ago)	Current	[REDACTED]	10.34.74.123	SJCM, Wired Data	OS_X_SnowLeopard-Workstation	cisco.com	[REDACTED] (10.34.74.4)
13-Feb-2012 6:22:39 PM (1 hour 11 minutes 30s ago)	Current	[REDACTED]	10.35...		Apple-Device	cisco.com	[REDACTED] (10.32.37.6)
13-Feb-2012 3:30:25 PM (4 hours 3 minutes 45s ago)	Current	[REDACTED]	10.35...		Apple-Device	cisco.com	[REDACTED] (10.32.37.6)
13-Feb-2012 5:49:00 PM (1 hour 45 minutes 10s ago)	Current	[REDACTED]	10.3...				[REDACTED]
13-Feb-2012 5:41:05 PM (1 hour 53 minutes 4s ago)	Current	[REDACTED]	10.35.71.62	Catch All			[REDACTED] (10.32.37.6)
13-Feb-2012 5:26:20 PM	Current	[REDACTED]	10.35.71.62	Catch All			[REDACTED] down

Quick View This Row
for Host 10.34.74.123:
Host Snapshot

- Top
- Status
- Security
- Hosts
- Traffic
- Reports
- Flows
- Configuration
- External Lookup

- Flow Table
- Network and Server Performance
- Flow Traffic
- Peer Vs. Peer
- Peer Vs. Port
- Time Vs. Peer
- Time Vs. Port
- Host/Host Group Peer
- Host/Host Group Port

A Note on Cyber Threat Defence (CTD) and NSEL

- Flow Action field can provide additional context
- State-based NSEL reporting is taken into consideration in StealthWatch's behavioural analysis (concern Index points accumulated for Flow Denied events)
- NAT stitching deduplicates flow records from ASA and ASR1000
- Lack of TCP flags and bi-directional byte and packet counters limit effectiveness of NSEL only in detecting certain threats (ex. SYN Flood); suggested deployment is to use in combination with other NetFlow sources

Flow Action	Client Host	Translated Host	Client Host Groups	Server Host	Server Host Groups
Permitted	192.168.203.10	168.192.203.10	Web Servers	168.192.200.22	United States
Permitted	192.168.203.10	168.192.203.10	Web Servers	168.192.200.22	United States
Permitted	168.192.200.22	168.192.203.10	United States	192.168.203.10	Web Servers
Denied	192.168.203.10	168.192.203.10	United States	192.168.203.10	Web Servers
Denied	168.192.200.22	168.192.203.10	United States	192.168.203.10	Web Servers

Permitted through ASA

Denied by ASA



Nexus 1000V Basics

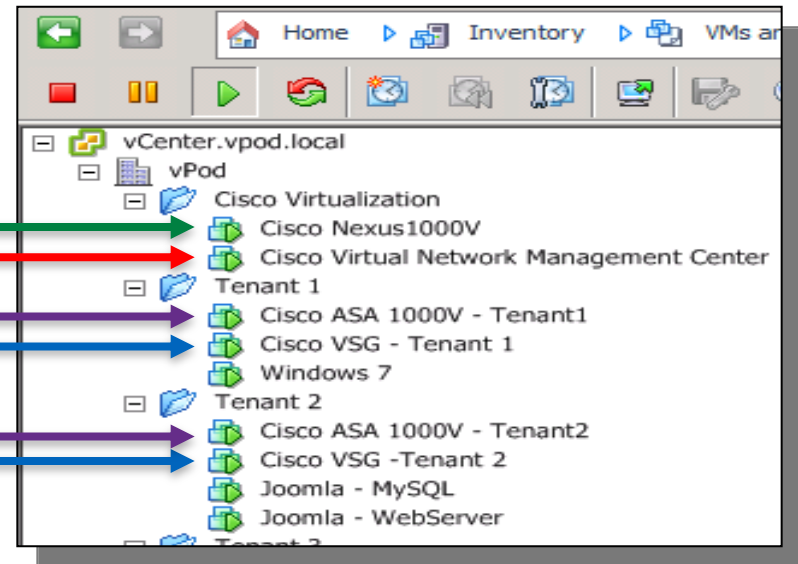
Cisco Virtual Components in VCenter

Nexus VSM

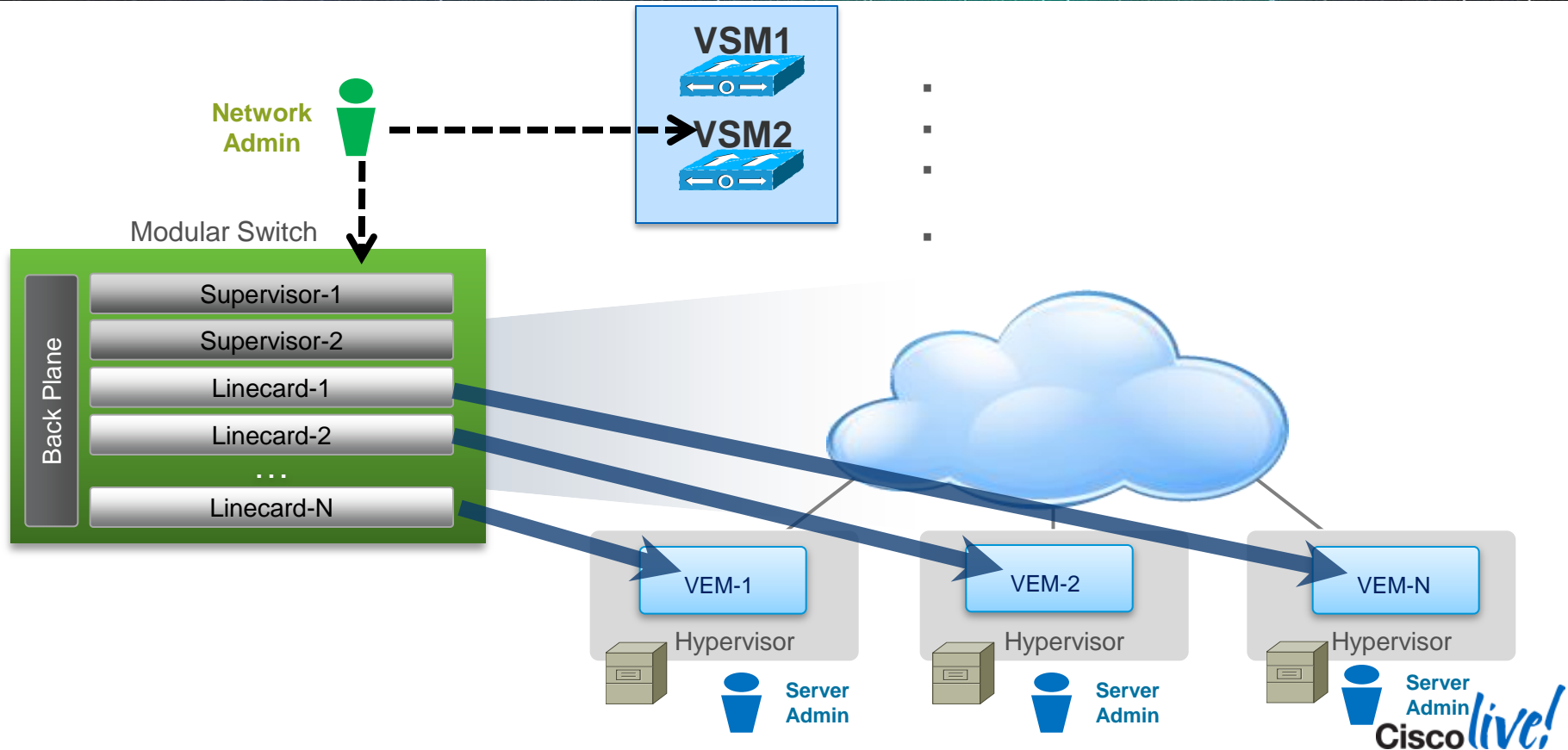
VNMC

ASA 1000V

VSG



Nexus 1000V Architecture



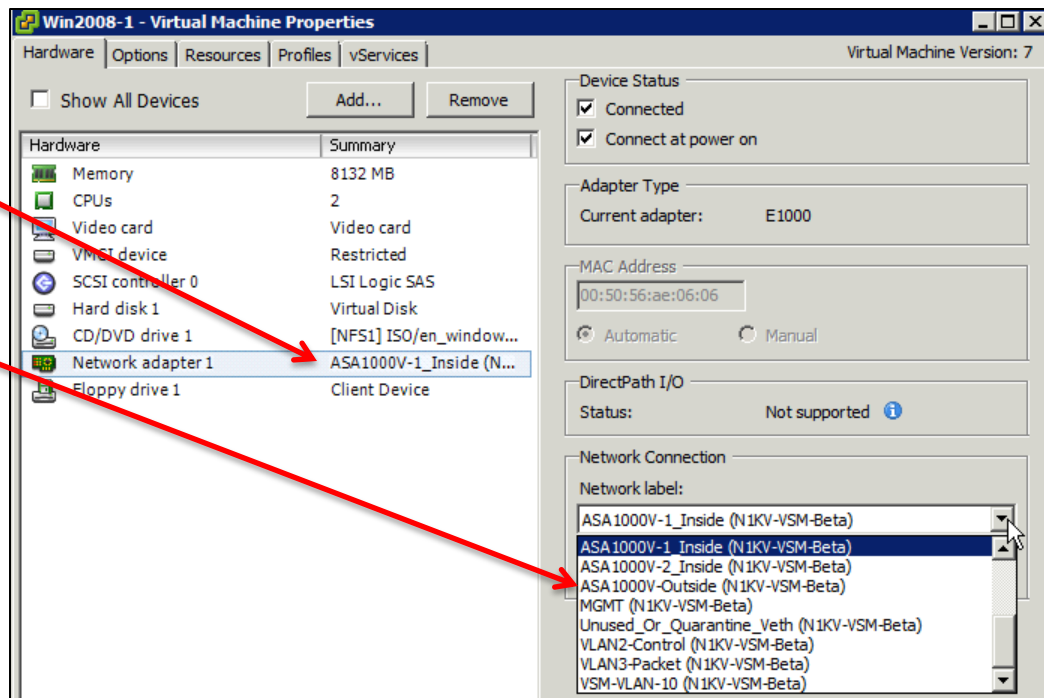
Nexus 1000V Architecture

port-profile type vethernet ASA1000V-1_Inside
switchport mode access
switchport access vlan 210
no shutdown
state enabled

port-profile type vethernet ASA1000V-Outside
vmware port-group
switchport access vlan 211
switchport mode access
no shutdown
state enabled

Nexus 1000V supports:

- ACLs
- Quality of Service (QoS)
- PVLANS
- Port channels
- SPAN ports



What is Vpath?

- vPath is the forwarding “brains” built into the Virtual Ethernet Module (VEM) of the Nexus 1000V
- It is an encapsulation that tags flows based upon attributes
- It has two main functions:
 1. Intelligent traffic steering
 2. Offload processing from virtual service nodes (VSN) to VEM
- vPath allows processing to be offloaded to Hypervisor for performance
- Currently only supported on VMWare today with future support for Hyper-V and others
- vPath is cornerstone for Cisco’s VSN delivery



Virtual Network Management Centre

Virtual Network Management Centre

- VNMC manages both ASA1000V policy and VSG policies and is built for multi-tenant environments
- Zones are building blocks for policy
- VNMC runs as a virtual machine, managed via web browser
- Virtual firewall policies are linked to virtual machine regardless of physical location and move
- Service chaining gives an order of operation to virtual firewalls
- Edge firewalls = ASA1000V
- Compute firewalls = VSG

VNMC Policy – Compute and Edge Firewalls

The screenshot displays the Virtual Network Management Center (VNMC) interface in a Windows Internet Explorer browser. The browser address bar shows `https://vnmc.vpod.local/#`. The interface includes a navigation bar with tabs for Tenant Management, Resource Management (selected), Policy Management, and Administration. Below this, there are sub-tabs for Managed Resources, Resources, Capabilities, and Diagnostics. The main content area is divided into a left-hand tree view and a right-hand configuration panel.

Tree View:

- root
 - Compute Firewalls
 - Edge Firewalls
 - Pools
 - Tenant1
 - Compute Firewalls
 - VSG - Tenant1
 - Edge Firewalls
 - ASA 1000V - Tenant1 (selected)
 - Tenant2
 - Tenant3

Configuration Panel: ASA 1000V - Tenant1

- Name: ASA 1000V - Tenant1
- Description: [Empty text box]
- HA Mode: High Availability Standalone
- Pool Name: [Not Assigned](#)
- States
 - Config State: applied
 - Association State: associated
- In case of failure, check: ! 0 ! 0 ! 0
- Buttons: Save, Reset

VSG

ASA1000V

VNMC VM Attributes in Zone Policy

The screenshot displays the VNMC interface for editing a vZone. The breadcrumb navigation shows 'Policy Management' > 'Service Policies'. The vZone is named 'WebZone' and is located under 'org-root/org-CustomerA'. The 'General' tab is active, showing the 'Name' as 'WebZone' and the 'Description' as 'Logical Zone for grouping all Web Servers'. Below this, the 'vZone Condition' section shows a table with one record: 'VM Name' contains 'Web'.

Tenant Management | Resource Management | **Policy Management** | Administration

Service Profiles | **Service Policies** | Device Configurations | Capabilities | Diagnostics

Edit

vZone

org-root/org-CustomerA

General | Events

Name:

Description:

vZone Condition ⓘ

+ Add Zone Condition PDF Excel Records: 1

Attribute Name	Operator	Attribute Value
VM Name	contains	Web

VNMC Security Policy Per Zone

The screenshot displays the Cisco Virtual Network Management Center (VNMC) interface. The top navigation bar includes "Tenant Management", "Resource Management", "Policy Management" (highlighted), and "Administration". Below this, a secondary navigation bar shows "Service Profiles", "Service Policies" (highlighted), "Device Configurations", "Capabilities", and "Diagnostics".

The left sidebar shows a hierarchical tree structure:

- root
 - Policies
 - Policy Helpers
 - CustomerA
 - Tenant-Sonali
 - Policies
 - Policy Helpers
 - Object Groups
 - Security Profile Dictionary
 - vZones**
 - AppZone
 - DBZone
 - WebZone

The right pane shows the configuration page for "vZones" under the "Tenant-Sonali" tenant. The "General" tab is selected, and the "Name" column lists the configured zones:

Name
AppZone
DBZone
WebZone

VNMC Security Policy

Edit

Edit (Allow-Web-Access)

org-root/org-CustomerA

General Events

Name: Allow-Web-Access


Description: Allow Web Access on Port 80

Rule Table

+ Add Rule | ↑ ↓ ↕ ⚙ Records: 6

Name	Source Condition	Destination Condition	Protocol	
Web-port80	Any	vZone Name eq WebZone	Any	Any
Allow_Web-DB-access	vZone Name eq WebZone	vZone Name eq DBZone	Any	Any
Allow_DB-Web	vZone Name eq DBZone	vZone Name eq WebZone	Any	Any
Allow-SSH	Any	Network Port eq 22 vZone Name eq DBZone	Any	Any
Block-DB-Access	Any	vZone Name eq DBZone	Any	Any
Explicit-Deny	Any	Any	Any	Any

VNMC Security Policy Rule

 Edit

ACL Policy Rule

org-root/org-CustomerA

General **Events**

Name:

Description:

Action to Take: **i** drop permit reset

log

Protocol: **i** Any

EtherType: **i** Any

Time Range: **i** Always

Source Conditions **i** Records: 0

Destination Conditions **i** Records: 1

+ Add Rule Condition		
Attribute Name	Operator	Attribute Value

+ Add Rule Condition		
Attribute Name	Operator	Attribute Value
vZone Name	eq	WebZone



CISCO TM