
TOMORROW starts here.
cisco
Cisco live!

Security and Virtualisation in the Data Centre

BRKSEC-2205

Greg Gibbs

Network Consulting Engineer

CCIE #19084

Cisco live!

Abstract

BRKSEC-2205

The evolving complexity of the data centre is placing increased demand on the network and security teams to come up with inventive methods for enforcing security policies in these ever-changing environments. The goal of this session is to provide participants with an understanding of features and design recommendations for integrating security into the data centre environment.

This session will focus on recommendations for securing next-generation data centre architectures. Areas of focus include security services integration, leveraging device virtualisation, and considerations and recommendations for server virtualisation.

The target audience are security and data centre administrators.

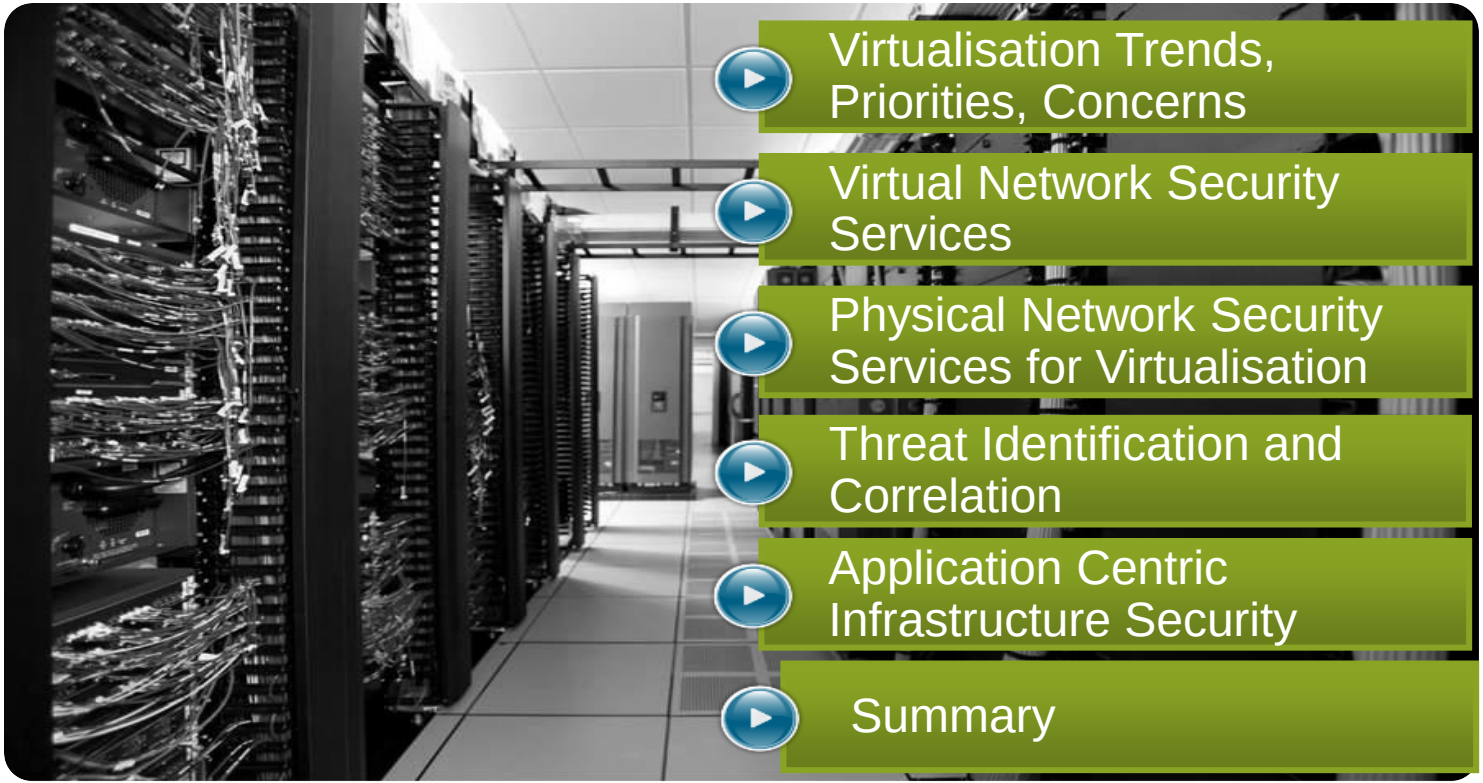
Related sessions are BRKSEC-2009 "Securing Cloud Computing" and TECSEC-2670 "Data Centre Security"

Session Objectives

- Discuss common virtualisation security concerns
- Gain an understanding on aligning physical and virtual network security resources
- Focus on tools available to unify policy enforcement for the virtual environment
- How to Increase overall visibility for virtual machine traffic flows
- Understand how security services can be integrated into the Application Centric Infrastructure

Security and Virtualisation in the Data Centre

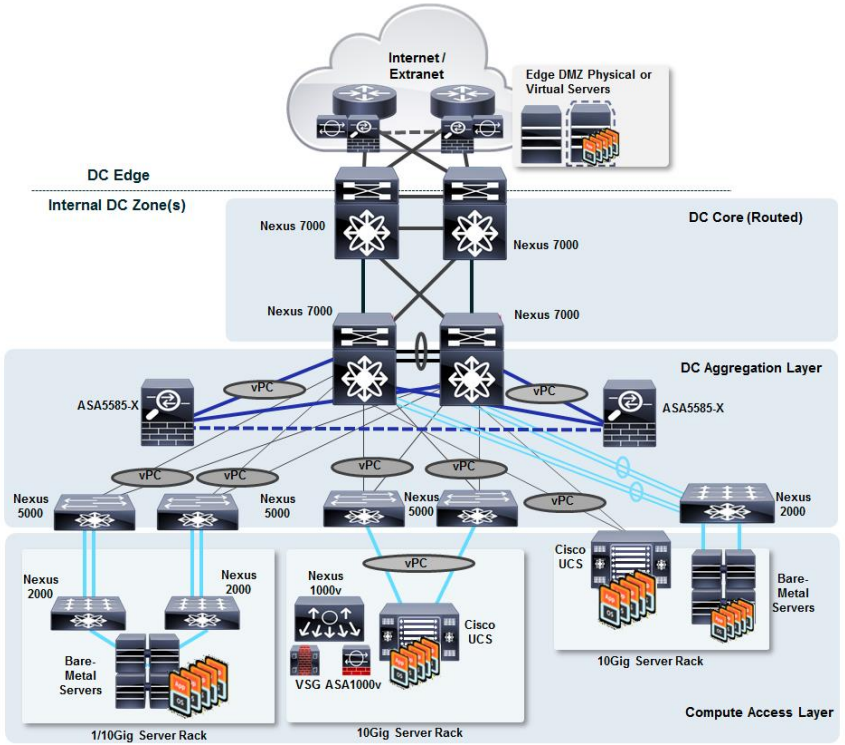
Agenda



- Virtualisation Trends, Priorities, Concerns
- Virtual Network Security Services
- Physical Network Security Services for Virtualisation
- Threat Identification and Correlation
- Application Centric Infrastructure Security
- Summary

Data Centre Architecture

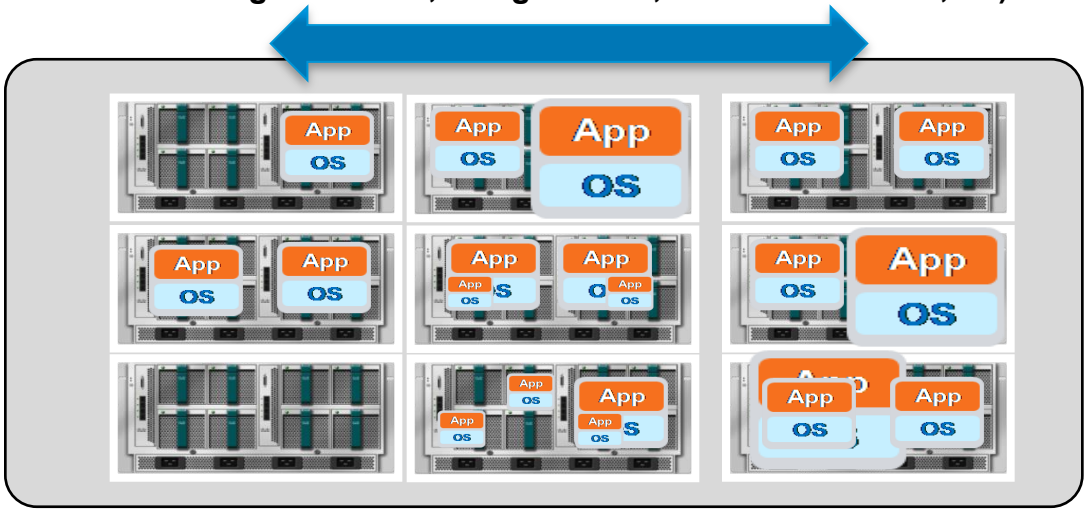
- Physical Network Fabric and Virtualisation
- DMZ network (physical or virtual workload) on DC edge that could securely leverage physical workloads or virtual workloads
- DC Core is Routed
- DC Aggregation layer contains Physical Security Services allowing the creation of internal zones / trust enclaves without crossing core (East-West) and crossing core (North-South) only when required
- Various End-of-Row/Top-of-Rack options represented between Aggregation and Compute/Access Layer
- Virtual Network and Security Services



Building an Efficient DC Fabric to Scale

Starting Point – The Compute Workload Domain

Scaling and Distribution of the Workload (Striping servers and VM's amongst the rack, along the row, between the rows, …)

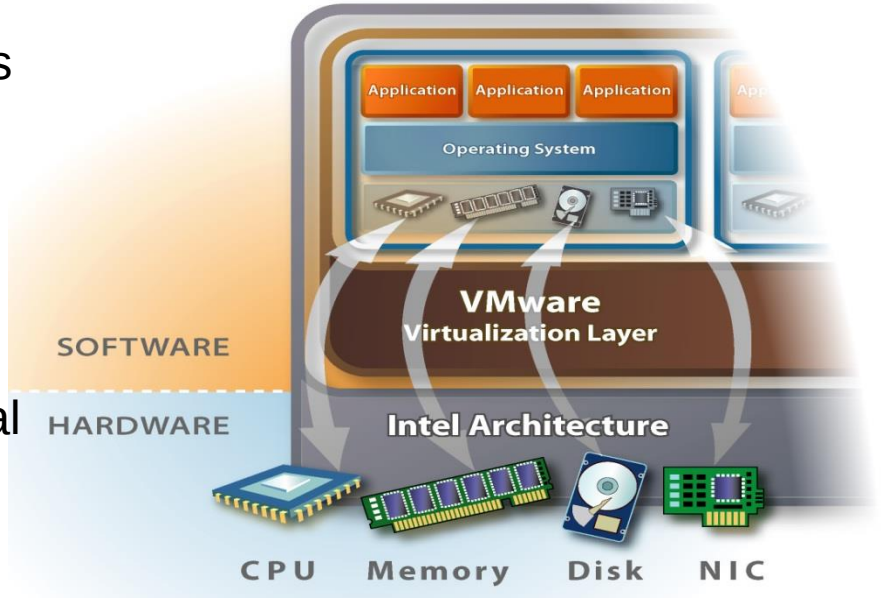


Scaling of the Workload Capabilities (Number of Servers and VM's)

- Architectural Goal is balanced between the need to scale the application workload capabilities and provide availability and manageability of the network fabric
- Improving the efficiency of the Data Centre requires a more scalable and flexible network fabric design

Server Virtualisation

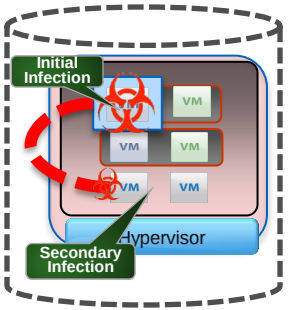
- Single physical server hosting multiple ***independent*** guest OS and applications
- Hypervisor ***absracts*** physical hardware from guest OS and applications
- Partitions system resources: CPU, Memory, Disk, Network
- Application & OS encapsulated as virtual machine



Common Virtualisation Concerns

Policy, Workflow, Operations

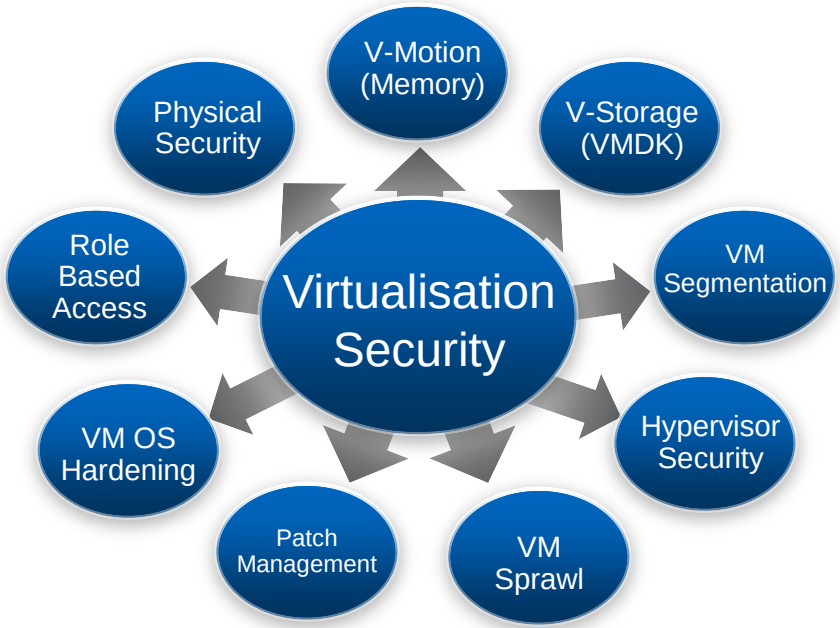
- Unified Policy Enforcement
  - Applied at physical server—not the individual VM
  - Impossible to enforce policy for VMs in motion
- Operations and Management
  - Lack of VM visibility, accountability, and consistency
  - Difficult management model and inability to effectively troubleshoot
- Roles and Responsibilities
  - Muddled ownership as server admin must configure virtual network
  - Organisational redundancy creates compliance challenges
- Machine and Application Segmentation
  - Server and application isolation on same physical server
  - No separation between compliant and non-compliant systems…



Virtualisation Security

Virtualisation Attention Deficit Disorder

- Collateral hacking?
- Segmentation?
- Side channel attacks?
- Visibility?
- Threat identification and defence?
- What about Hypervisor Hyperjacking?



Simple, Effective, Achievable

Segmentation

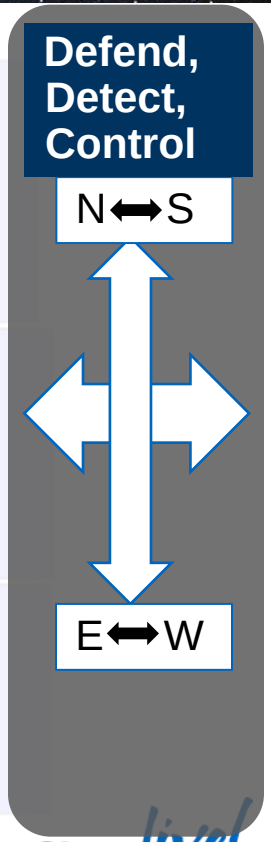
- **Establish boundaries:** network, compute, virtual
- **Enforce policy** by functions, devices, organisations, compliance
- **Control and prevent unauthorised access** to networks, resources, applications

Threat Defence

- **Stop** internal and external **attacks and interruption of services**
- **Patrol** zone and edge **boundaries**
- **Control information** access and usage, prevent data loss and data modification

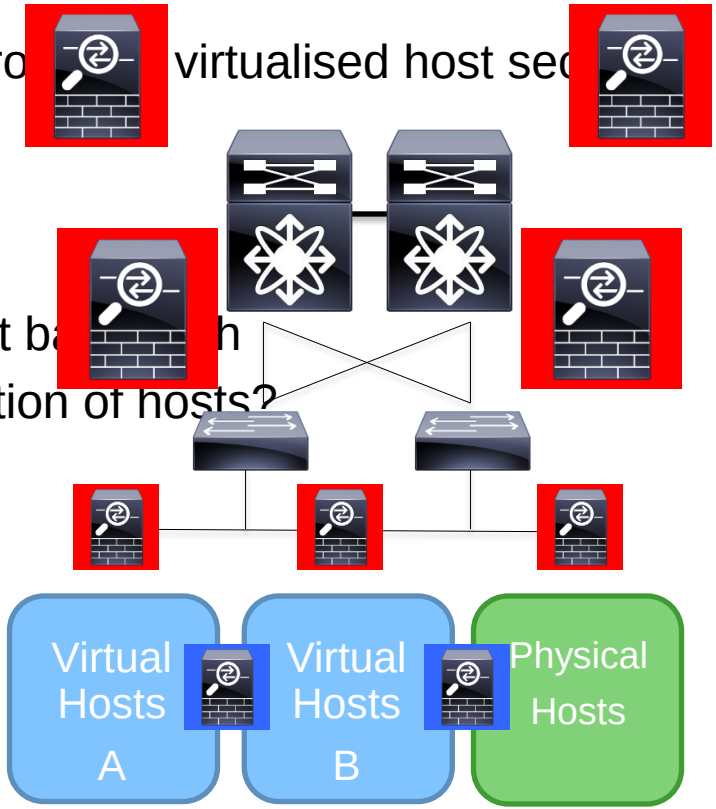
Visibility

- Provide **transparency** to usage
- Apply **business context** to network activity
- **Simplify** operations and compliance reporting



Centralised or Decentralised Firewalls or Both?

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



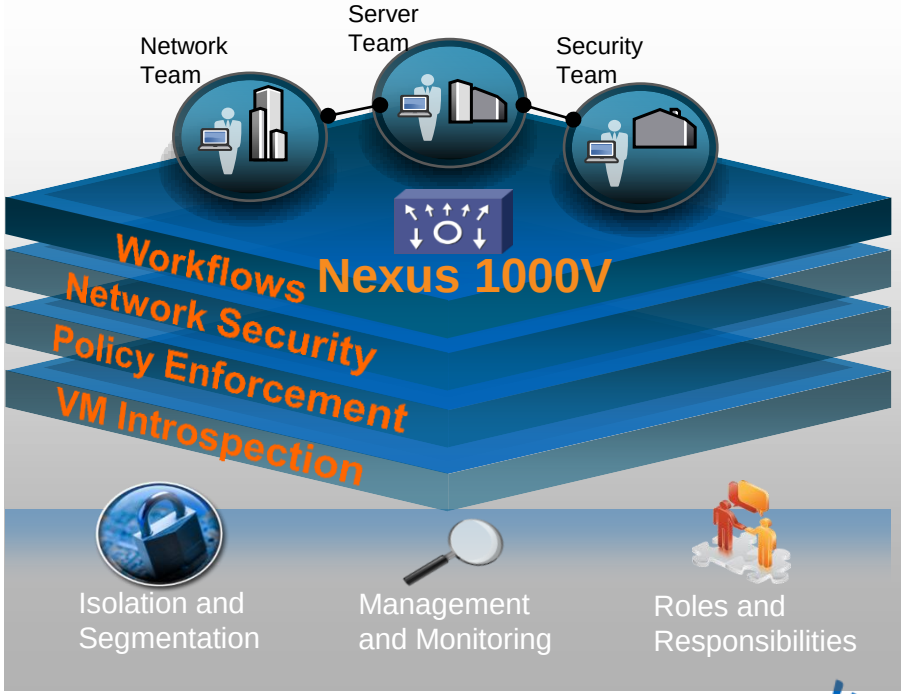
Virtual Network & Security Services

Managing Virtual Networking Policy

Virtual Switches: Example Nexus 1000V

Nexus 1000V

- Non-disruptive operational model to maintain current workflows using Port Profiles
- Maintain network security policies with isolation and segmentation via VLANs, Private VLANs, Port-based Access Lists, Cisco Integrated Security Features
- Ensure visibility (VM Introspection) into virtual machine traffic flows using traditional network features such as ERSPAN and NetFlow



Port Profiles

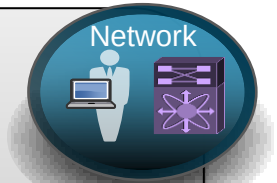
Port Profile –> Port Group

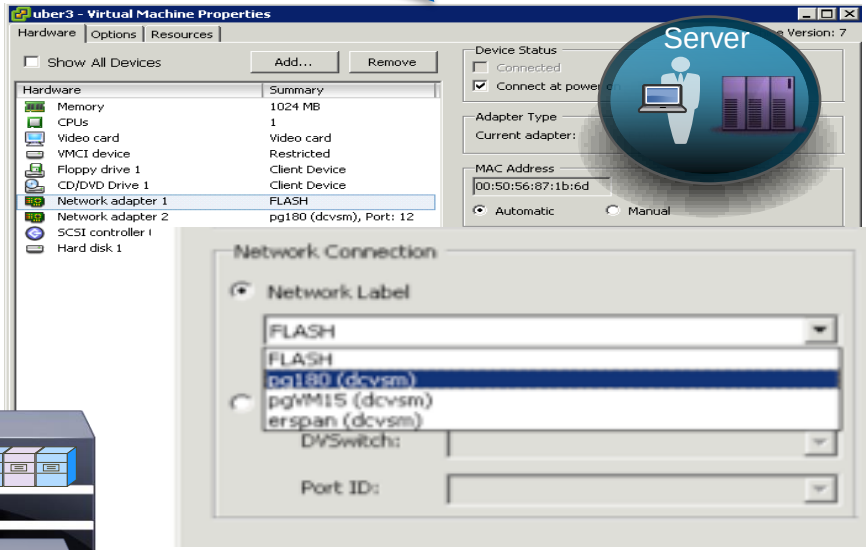
vCenter API

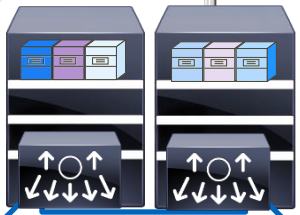
```
port-profile vm180
  vmware port-group pg180
  switchport mode access
  switchport access vlan 180
  ip flow monitor ESE-flow input
  ip flow monitor ESE-flow output
  no shutdown
  state enabled

interface Vethernet9
  inherit port-profile vm180

interface Vethernet10
  inherit port-profile vm180
```







vMotion
Policy Stickiness

Nexus 1000V supports:

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

Nexus 1000V Security Features

Laying the Foundation

Switching	▪ L2 Switching, 802.1Q Tagging, VLAN Segmentation, Rate Limiting (TX) ▪ IGMP Snooping, QoS Marking (COS & DSCP)
Security	▪ Virtual Service Domain, Private VLANs w/ local PVLAN Enforcement ▪ Access Control Lists (L2–4 w/ Redirect), Port Security ▪ Dynamic ARP inspection, IP Source Guard, DHCP Snooping
Provisioning	▪ Automated vSwitch Config, Port Profiles, Virtual Centre Integration ▪ Optimised NIC Teaming with Virtual Port Channel – Host Mode
Visibility	▪ VMotion Tracking, ERSPAN, NetFlow v.9, CDP v.2 ▪ VM-Level Interface Statistics
Management	▪ Virtual Centre VM Provisioning, Cisco Network Provisioning, CiscoWorks ▪ Cisco CLI, Radius, TACACs, Syslog, SNMP (v.1, 2, 3)

Virtualised Network Services

Nexus 1100 Platform

Virtual Services Supported

- N1KV VSM (vSphere) 
- Virtual Security Gateway (VSG) 
- Network Analysis Module (NAM) 
- DC Network Manager (DCNM) 

Virtual Services

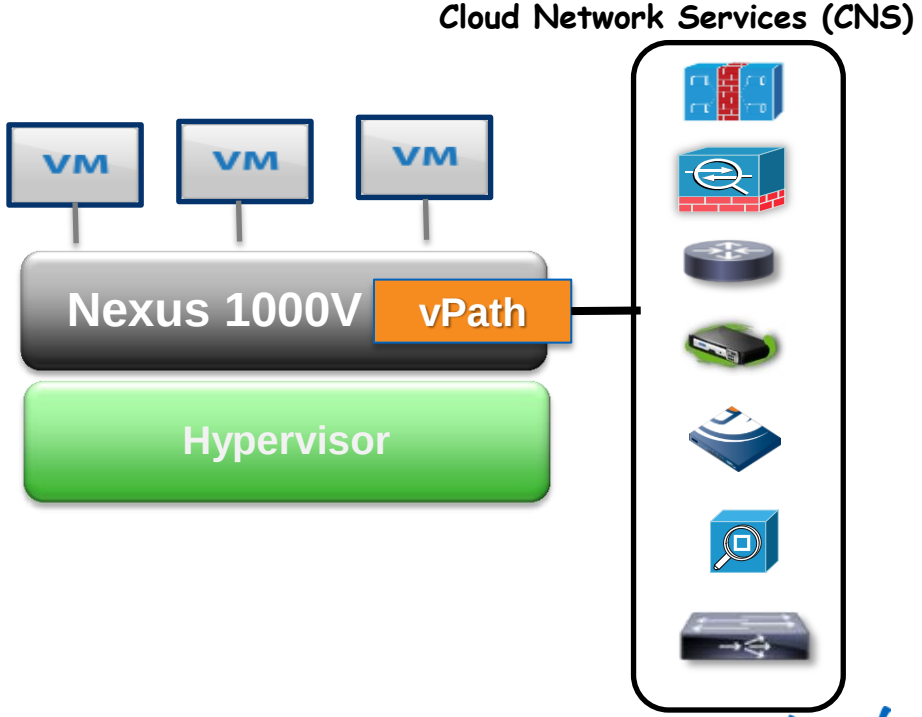
- N1KV VSM (Xen, Hyper-V, KVM) 
- VXLAN Gateway
- ASAv, vWAAS, CSR
- Netscaler VPX
- Imperva Web App FW

Note: Any Virtual Service can be solely deployed on N1100 series.

vPath Enables Chaining of Network Services

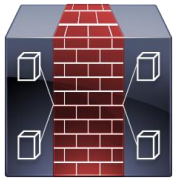
vPath is Nexus 1000V data plane component:

- Topology agnostic service insertion model
- Service Chaining across multiple virtual services
- Performance acceleration with vPath e.g. VSG flow offload
- Efficient and Scalable Architecture
- Non- Disruptive Operational Model
- VM Policy mobility with VM 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 Hyper-V
- Both are managed via Virtual Network Management Centre (VNMC) / Prime Network Services Controller (PNSC)
- Both are licensed per CPU socket
- They are complementary to each other, require the Nexus 1000V Virtual Distributed Switch and utilise a new forwarding plane, **vPath**



Virtual Security Gateway

ASA 1000V

vPath Service Chaining

- ASA 1000V and VSG
  - vservice node ASA1 type asa
    - ip address 172.31.2.11
    - adjacency l2 vlan 3770
  - vservice node VSG1 type vsg
    - ip address 10.10.11.202
    - adjacency l3
  - vservice path chain-VSG-ASA
    - node VSG1 profile sp-web order 10
    - node ASA1 profile sp-edge order 20
  - port-profile type vethernet Tenant-1
    - org root/Tenant-1
    - vservice path chain-VSG-ASA

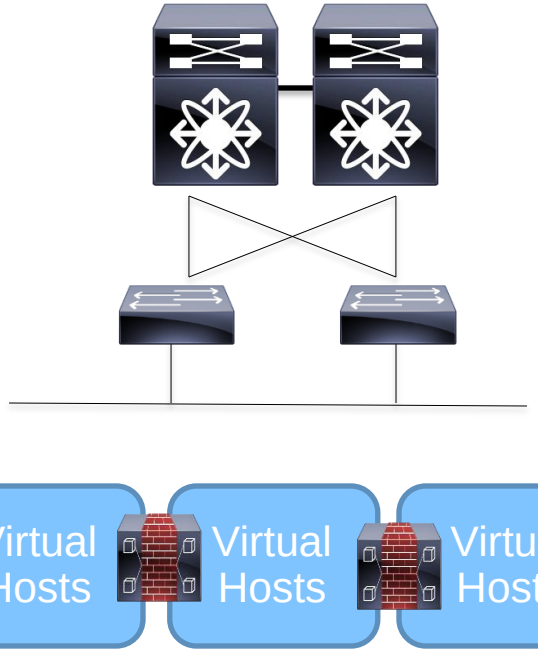
Defining the Service Node on Nexus 1000V

Chain the Service Nodes
Order is inside to outside

Enable the Service Chain Per Port-Profile

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



VSG Attributes

vCenter VM Attributes

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

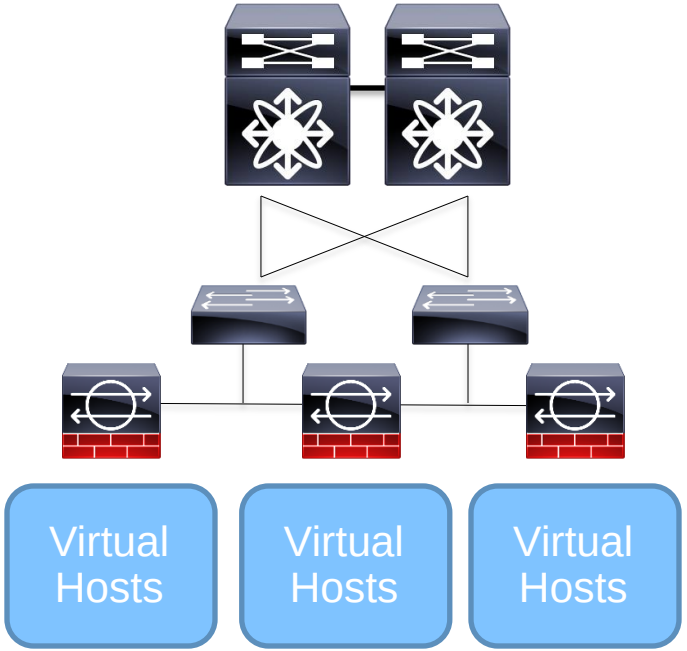
VM attribute information collected is used for enforcing security policy

Security Policy Profile

- Defined/Managed by VNMC / Prime NSC
- Bound to Cisco Nexus 1000V VSM port-profile

The ASA 1000V Cloud Firewall

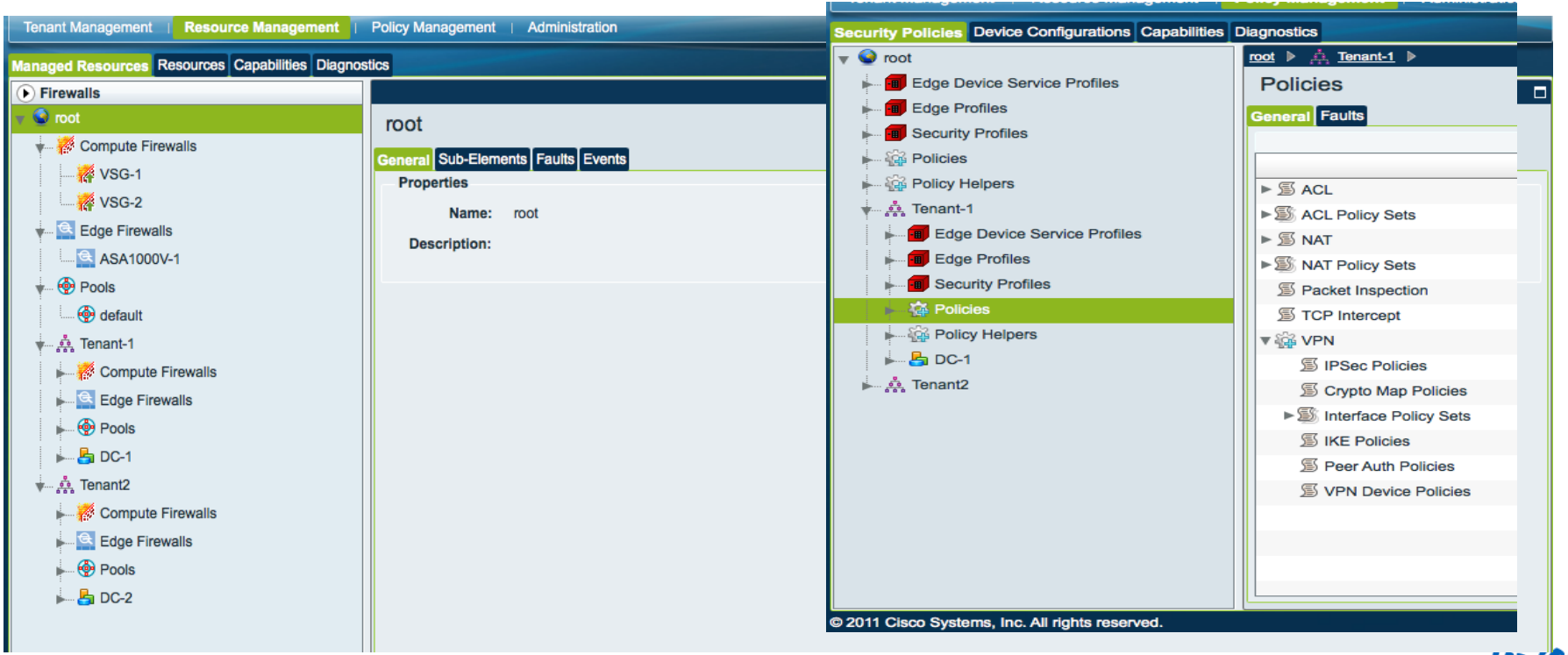
- ASA 1000V is a software-only version of an ASA appliance—an edge firewall with **limited features**
- Runs ASA codebase in a virtual machine in L3 mode only
- Supports S2S IPSEC VPN (not RA VPN)
- Can be deployed in active/standby HA
- Management via ASDM or VNMC/PNSC but not both
- Not a replacement for physical appliance!



4 interfaces: inside, outside, failover and management

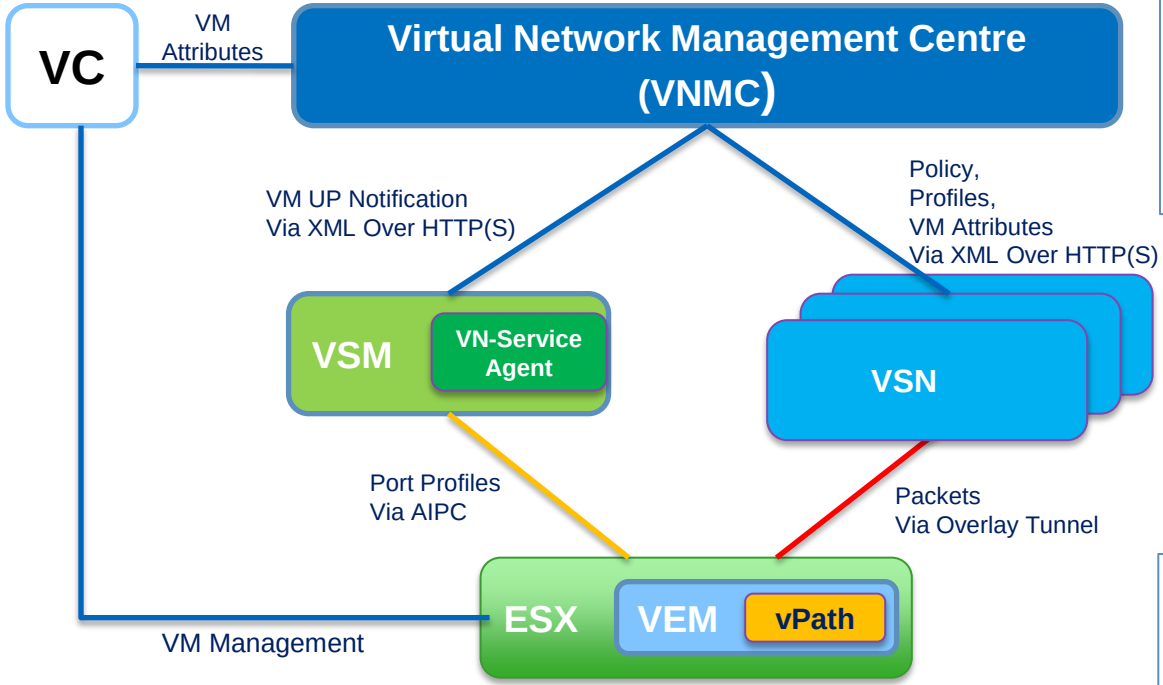
Virtual Network Security Policy Engine

VNMC



Virtual Services Architecture

Provides a Framework for Building Virtual Network Services



Virtual Network Management Centre (VNMC)

Centralised Management Plane - VM
Policy Management (PIP and PAP)
Multi-Device Management
vCenter Integration – VM Attributes
North Bound XML API
Multi-Tenant

Virtual Service Node (VSN)

Distributed Service Plane - VM Service Processiong
VSNs – VSG, vWAAS. ASA1000V..
Multi-Instance

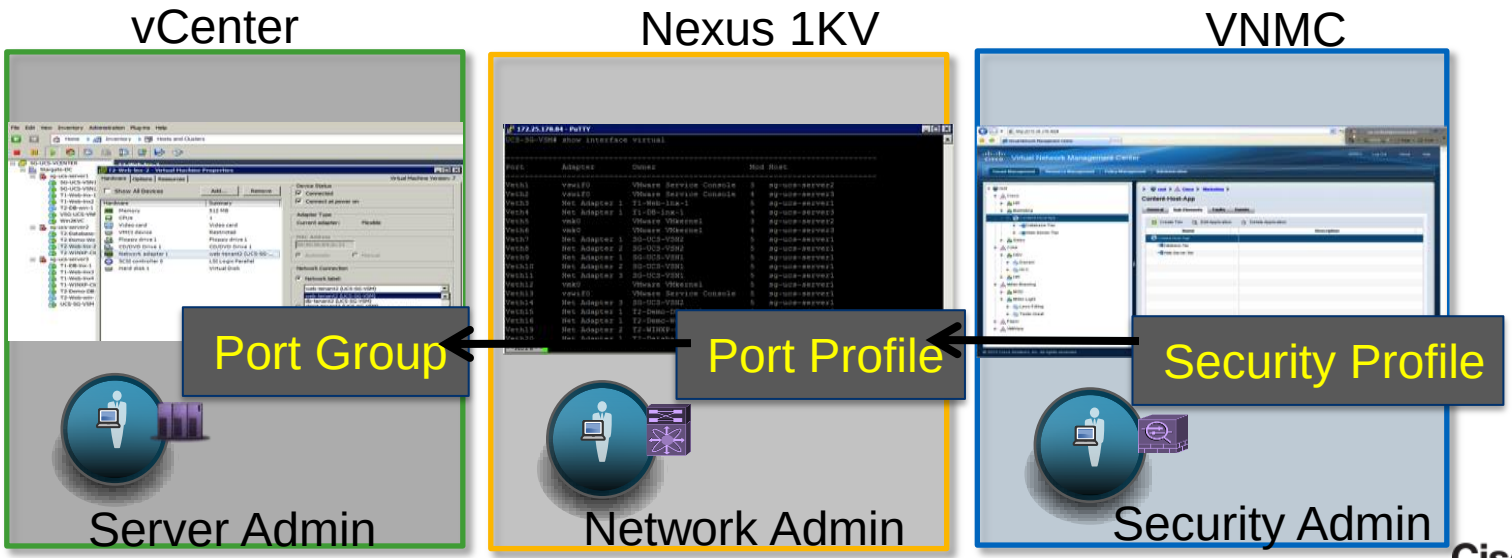
vPath

Distributed Data Plane - Embedded in VEM
vPath API – re-usable for multiple services
Multi-Tenant

Policy Workflow

Server, Network, Security

- Mitigate Operational errors between teams
- Security team defines security policies
- Networking team binds port-profile to VSG service profile
- Server team Assigns VMs to Nexus 1000V port-profiles



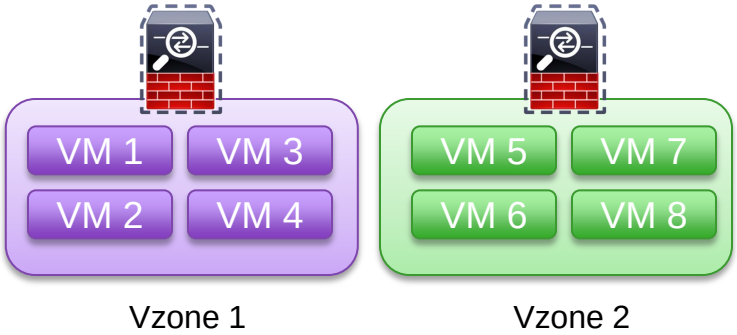
Introducing the Virtualised ASA (ASAv)

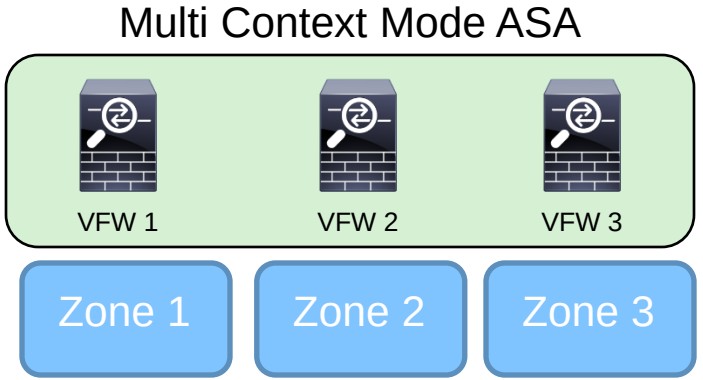
- Scheduled release spring 2014
- Developed due to customer feedback for a complete ASA firewall running as a virtual machine
- Nexus1000V not required
- Will support VMWare first then other hypervisors
- ASA feature parity (with some exceptions)
- No support for:
  1. ASA clustering
  2. Multi context mode
  3. Etherchannel interfaces
  4. Active/Active Failover (requires multi context mode)

ASAv Firewall
(Virtualised ASA)

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

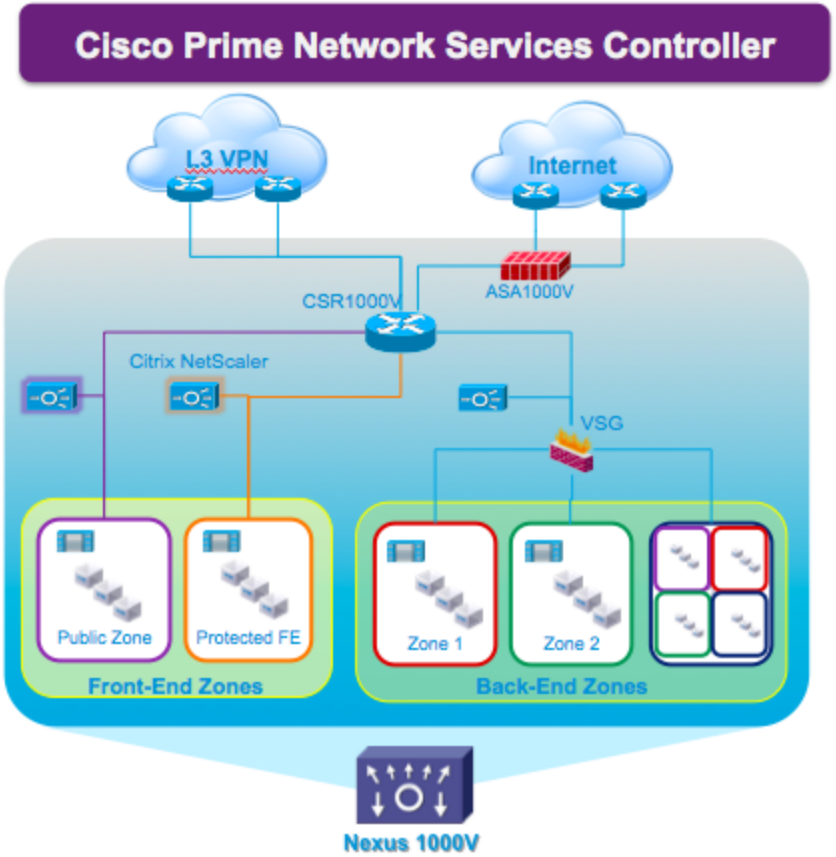
Comparing Cisco Virtual Firewalls

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/PNSC	Managed by VNMC/PNSC only
Full ASA code, CLI, SSH, REST API	Uses ASA code, CLI, SSH	Minimal config via CLI, SSH

Cisco Prime Network Services Controller (PNSC)

Version 3.2

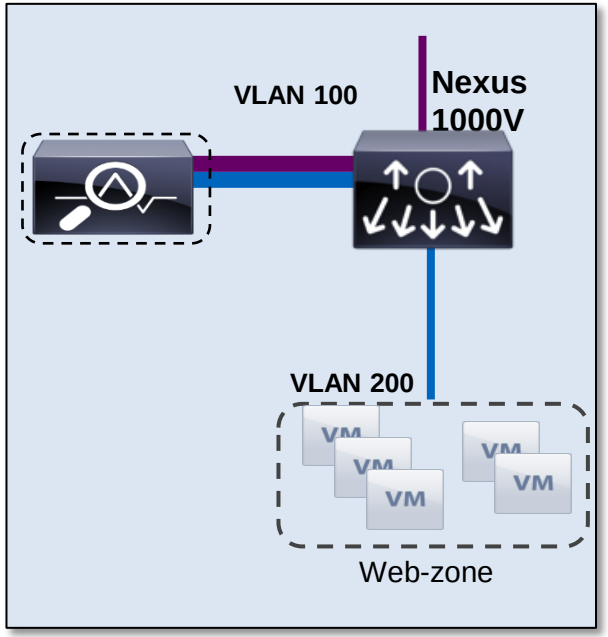
- Added feature support:
  1. Citrix NetScaler VPX/1000v
  2. CSR 1000v
  3. Dynamic Fabric Automation (DFA) Service Insertion
  4. Cisco Intelligent Automation for Cloud (IAC) integration

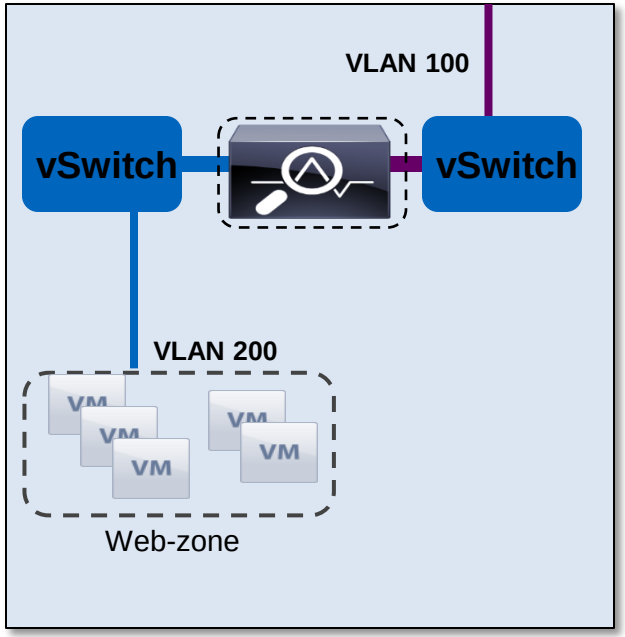


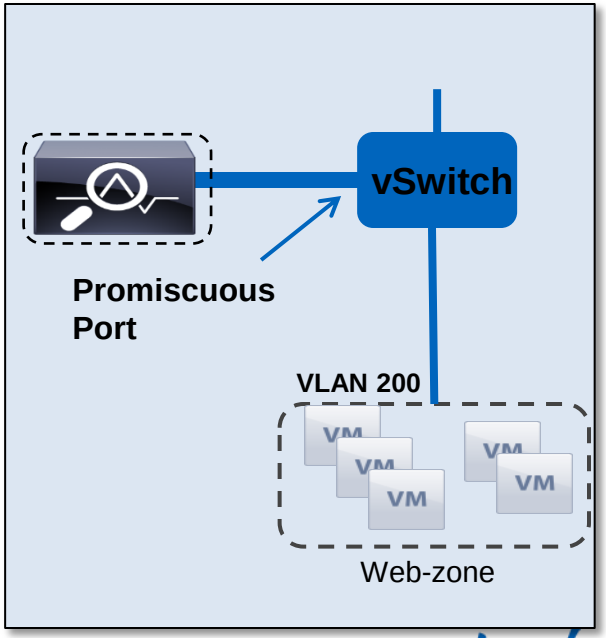
Virtual IPS

vIPS

Virtual Switch Inline and Passive Deployment Options



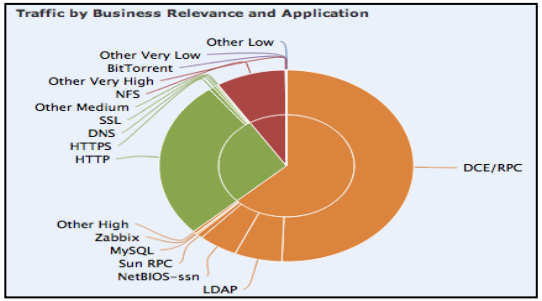




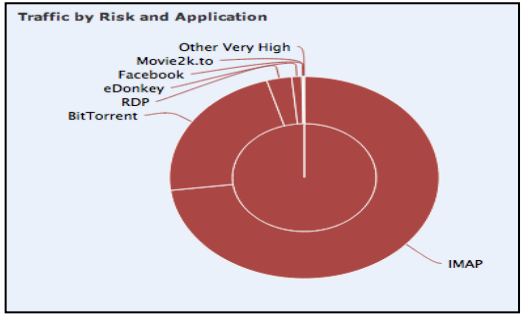
FireSIGHT Context Explorer

Application Security and Visibility

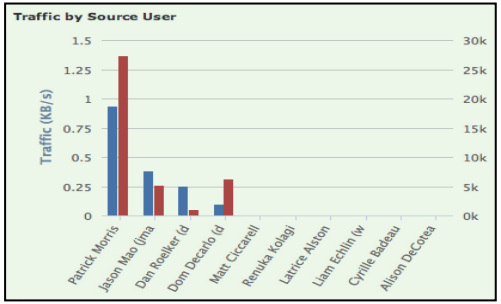
View all application traffic…



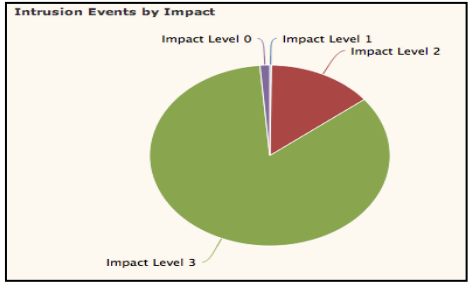
Look for risky applications…



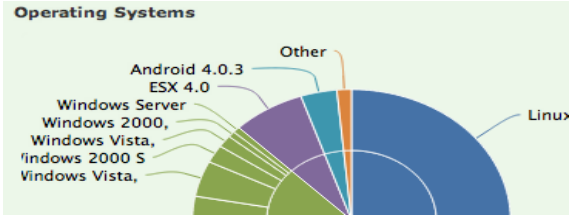
Who is using them?

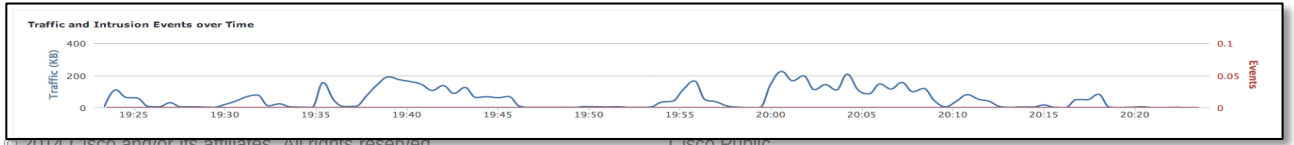


What else have these users been up to?



On what operating systems?





Application Security & Visibility

Geo Location Information

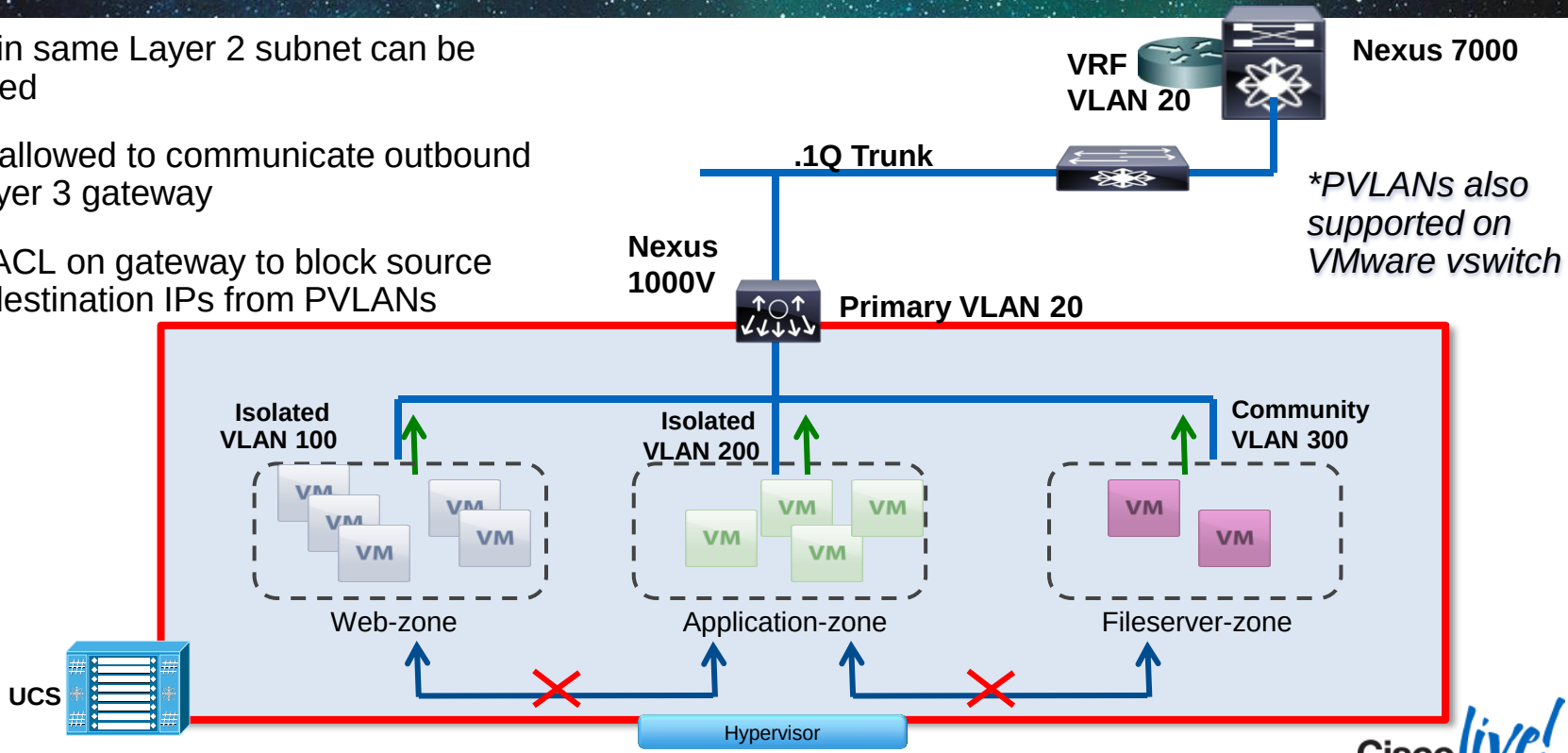



Deployment Example

Layer 2 Segmentation

PVLANs for VM Isolation

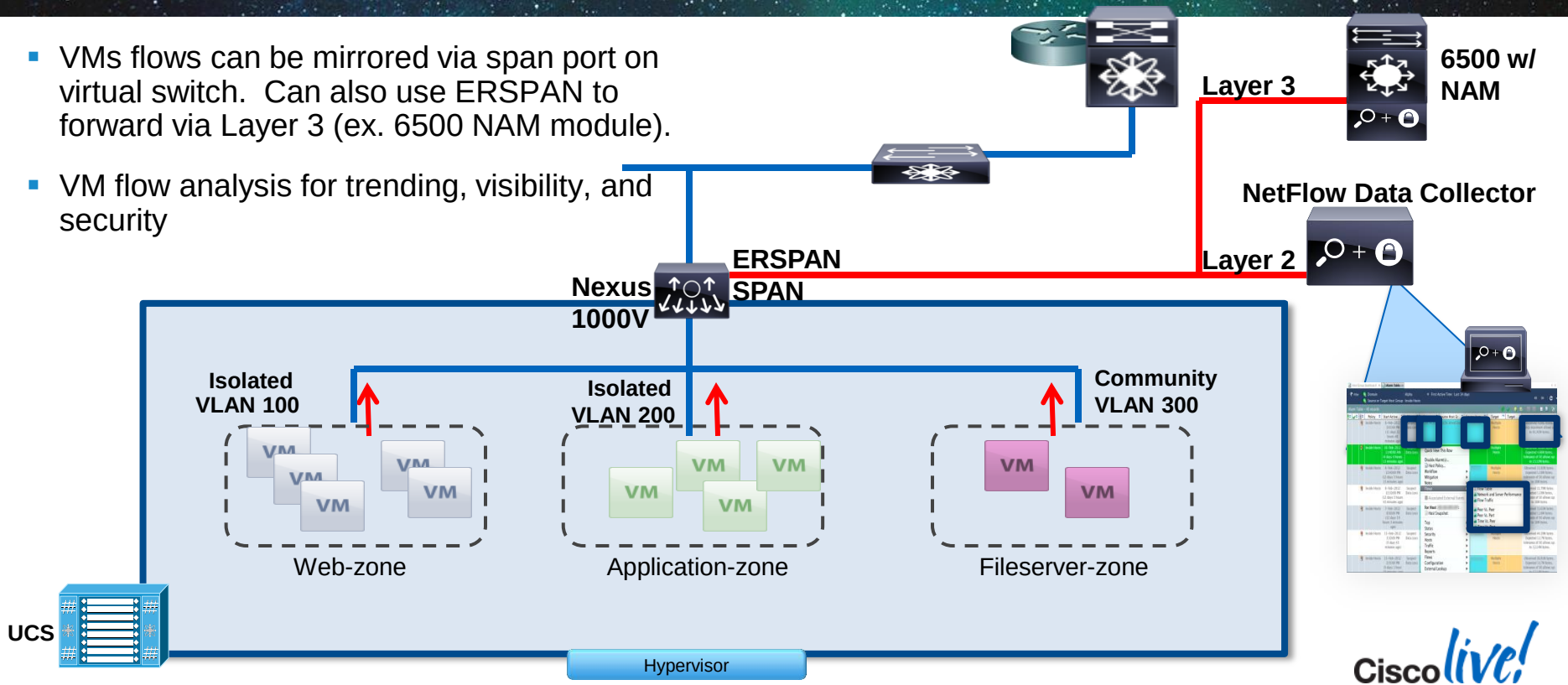
- VMs in same Layer 2 subnet can be isolated
- Only allowed to communicate outbound to Layer 3 gateway
- Use ACL on gateway to block source and destination IPs from PVLANs



VM Visibility

NetFlow for VM Network Behaviour Analysis

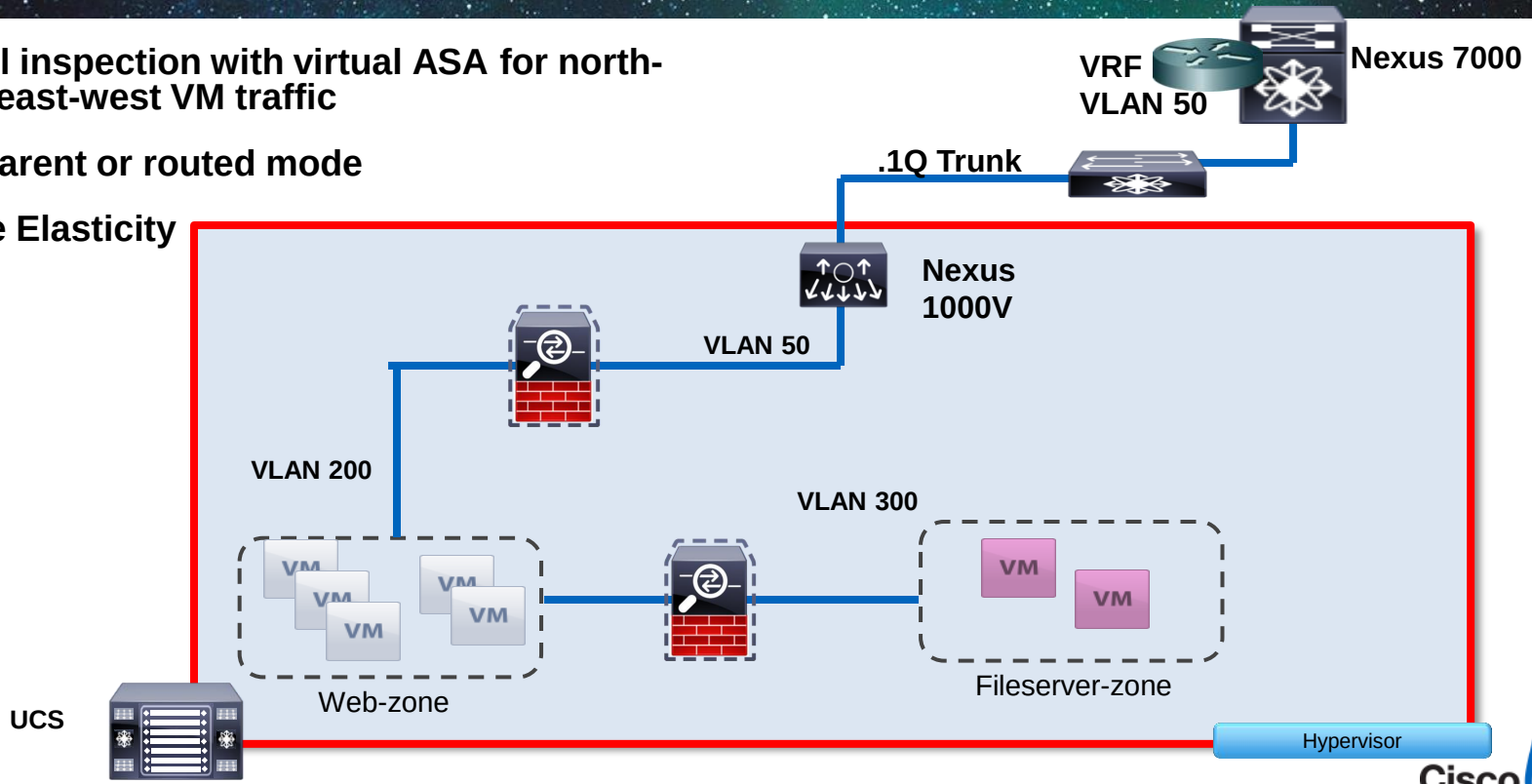
- VMs flows can be mirrored via span port on virtual switch. Can also use ERSPAN to forward via Layer 3 (ex. 6500 NAM module).
- VM flow analysis for trending, visibility, and security



Application Security & Visibility

ASAv

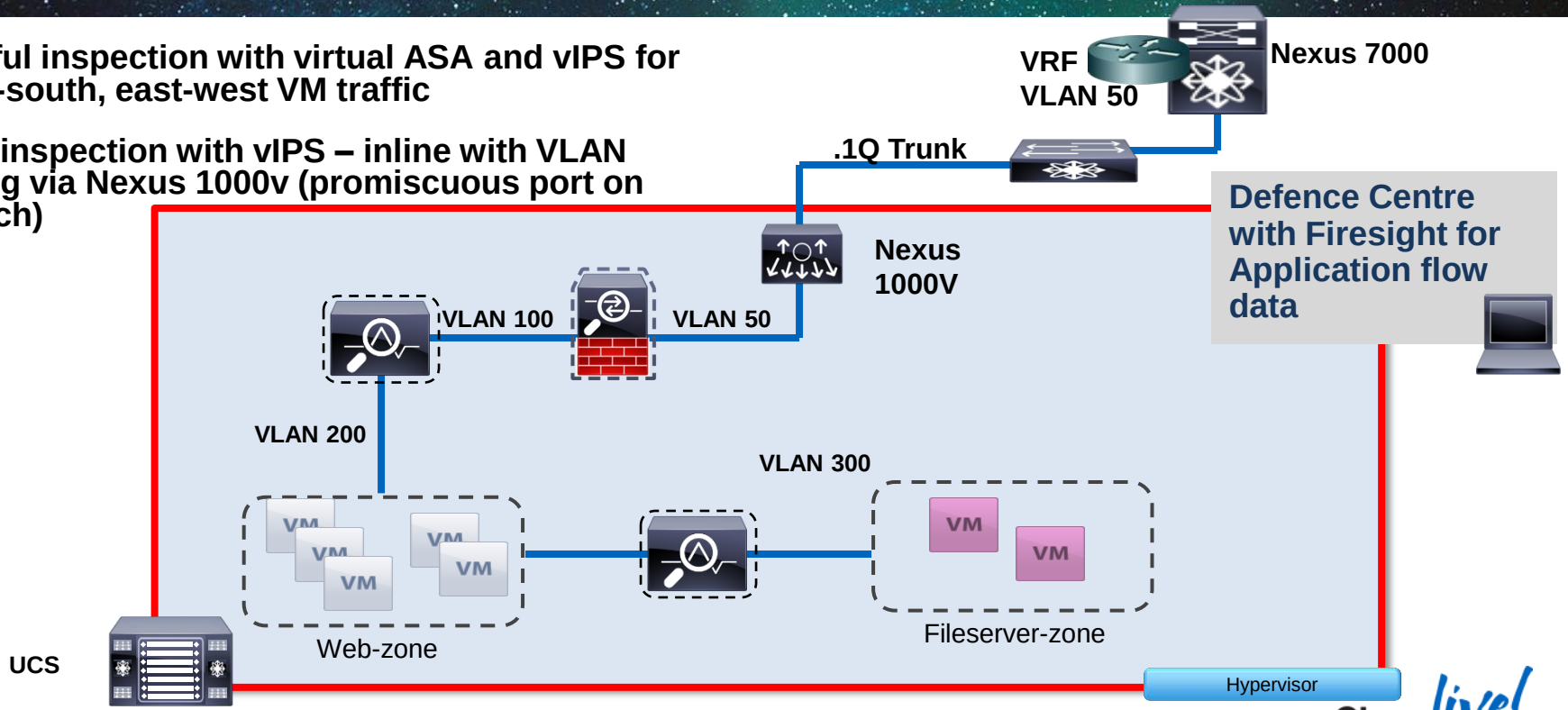
- **Stateful inspection with virtual ASA for north-south, east-west VM traffic**
- **Transparent or routed mode**
- **Service Elasticity**



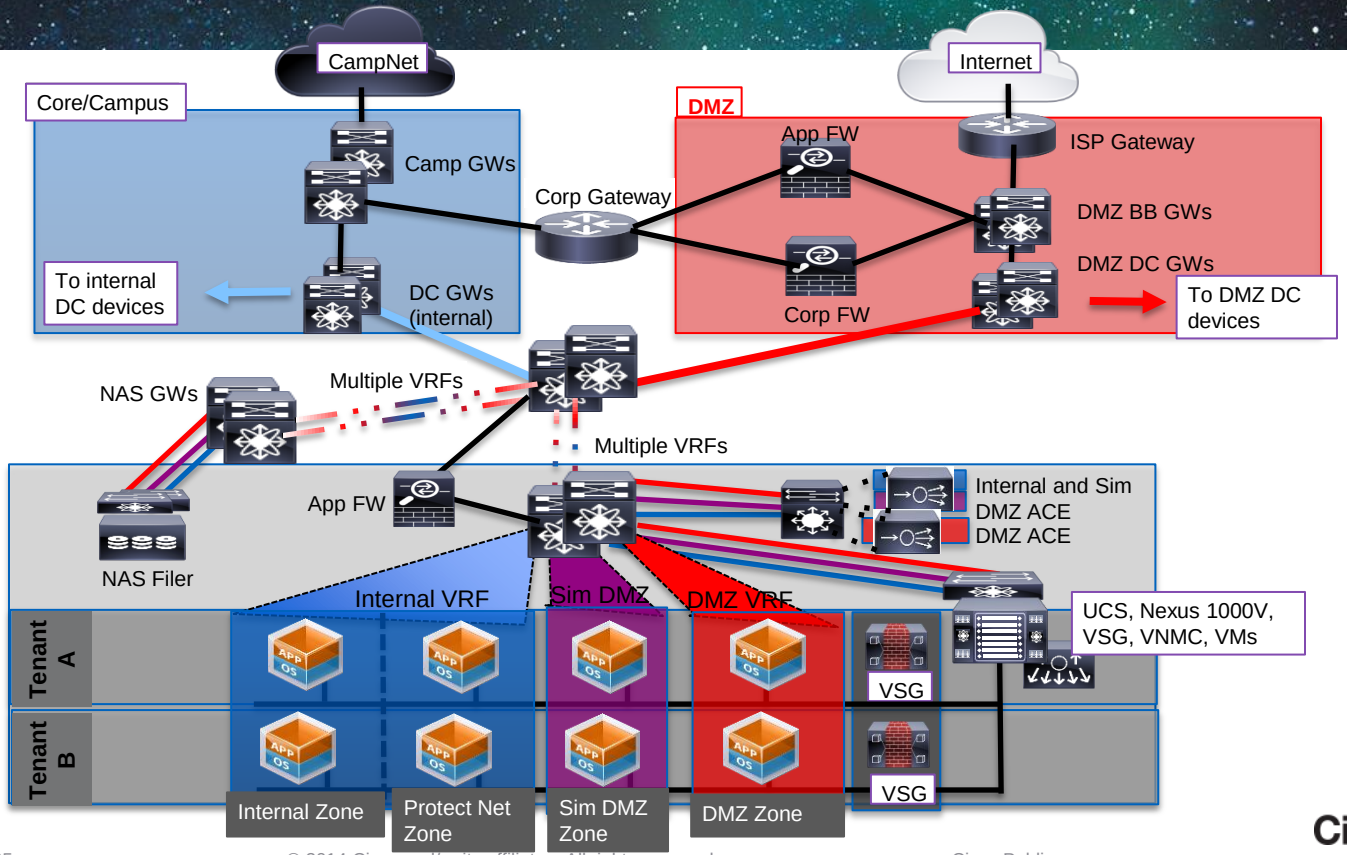
Application Security & Visibility

vIPS

- **Stateful inspection with virtual ASA and vIPS for north-south, east-west VM traffic**
- **Deep inspection with vIPS – inline with VLAN pairing via Nexus 1000v (promiscuous port on vswitch)**



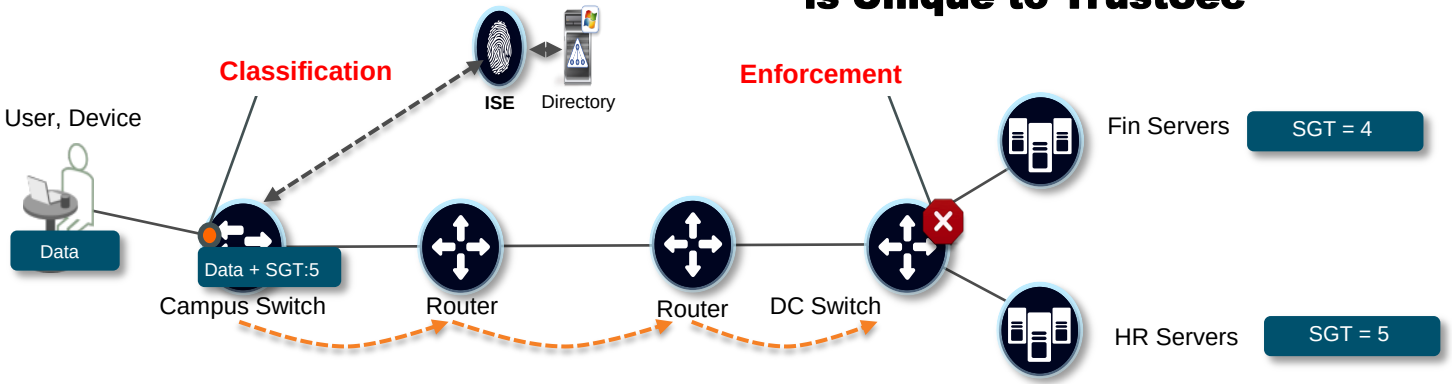
Virtualised DMZ



Physical Security Services for Virtualisation

What is TrustSec?

Tagging Data for Security Policy Control is Unique to TrustSec



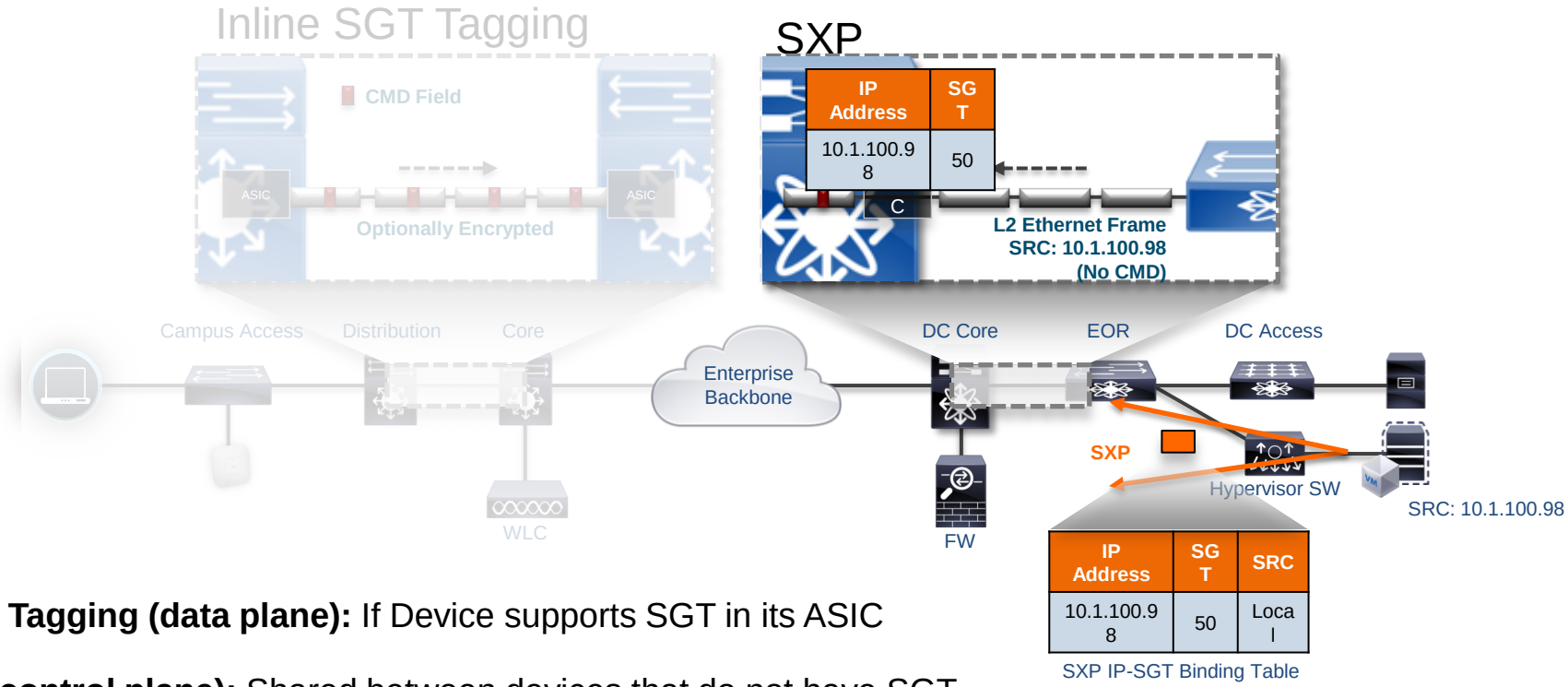
Users and Systems are **Classified** into Security Groups based on Context. Traffic is then Tagged with the Security Group ID

- Tags can be applied to individual users, servers, networks or network connection traffic
- Forwarding, filtering, inspection and other decisions can be based upon TrustSec Tags
- Provides virtual network segmentation, flexible access control and FW rule automation

Why TrustSec ?

- Simplifies Security Policies, Access Control & Segmentation
- Automates Cisco FW rule admin in Cisco DC & network environments
- Leverage your switching and routing infrastructure for Security
- Distributed Enforcement with Massive Scale.
- Consistent Segmentation for Physical and Virtual Workloads
  - Nexus 1000v – Static SGT Mapping (IP, Port Profile) & SXP
- Separation of Duties: Server, Network and Security Admin.

How is the SGT Shared?



- **Inline Tagging (data plane):** If Device supports SGT in its ASIC
- **SXP (control plane):** Shared between devices that do not have SGT-capable hardware

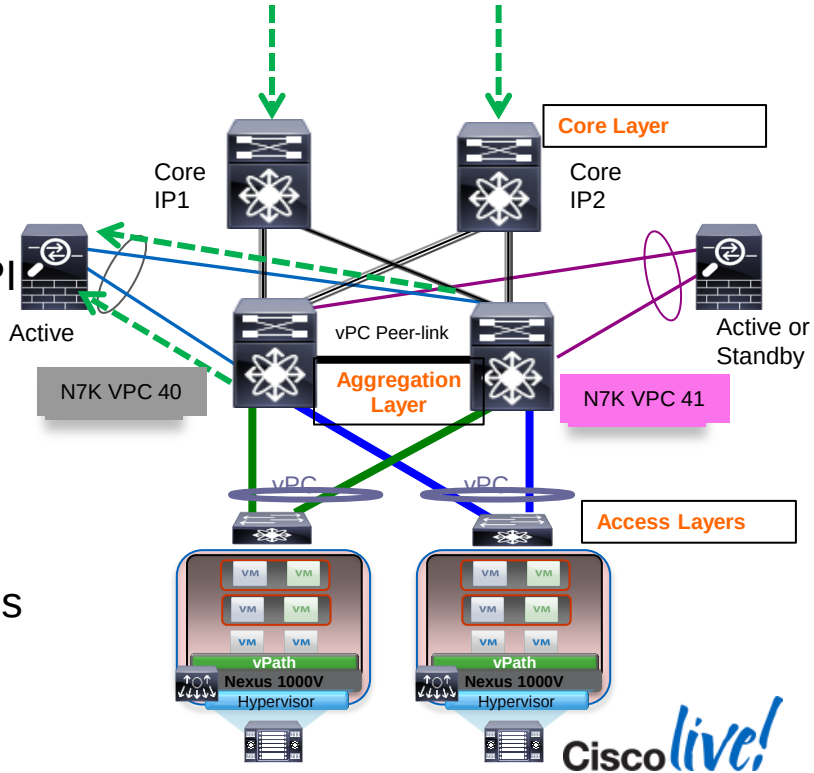
More on TrustSec Architecture

- TECSEC-2760 – Data Centre Security
- BRKSEC-2690 - Deploying Security Group Tags
- BRKSEC-2663 - Before. During. After. Cisco's Integrated Security Strategy

ASA Firewalls and the Data Centre Fabric

Data Centre Aggregation Layer

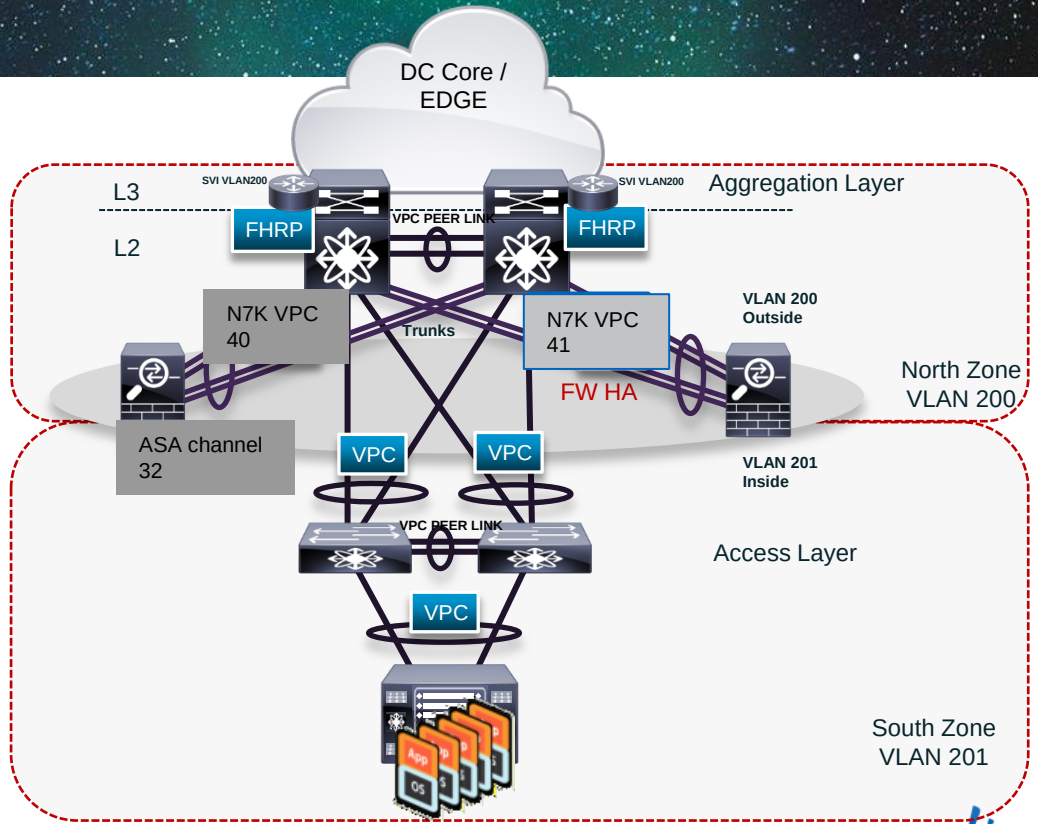
- ASA and Nexus Virtual Port Channel
  - vPC ensures all active links utilised (eliminates blocked STP links)
  - Unique integration with ASA and Nexus (LACP)
- IPS module relies on ASA connectivity –provides DPI
- Validated design to provide segmentation, threat protection, visibility
- Note that vPC identifiers are **different** for each ASA (*changes with clustering feature)
- Transparent (recommended) and static routed modes
- Works with both A/S and A/A failover



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)
- Note that vPC identifiers are **different** for each ASA on the Nexus switch (this changes with ASA clustering feature and cLACP)

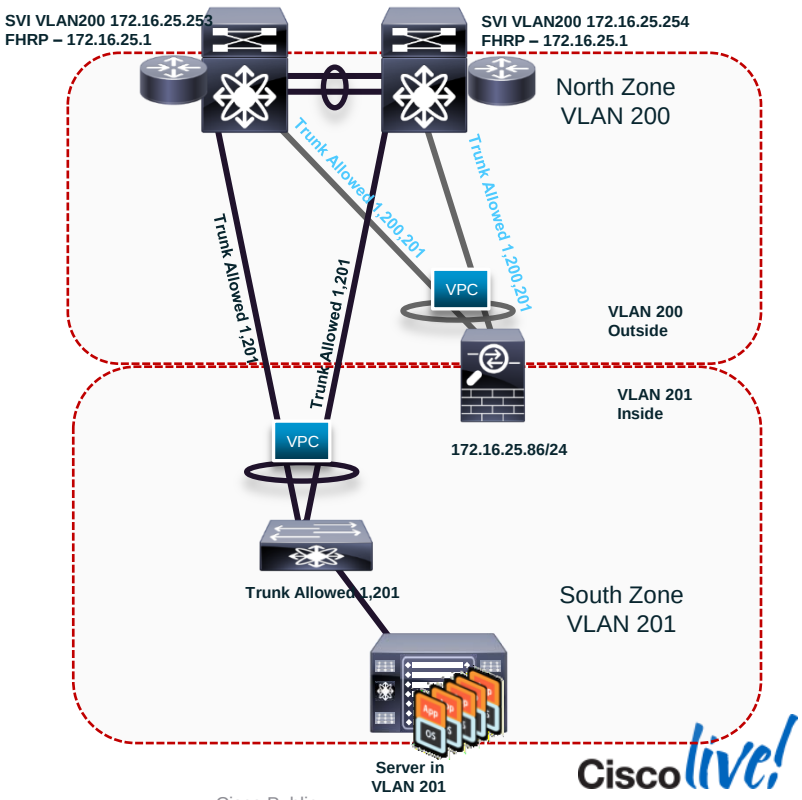


Transparent Mode Configuration in the DC

Two Interfaces

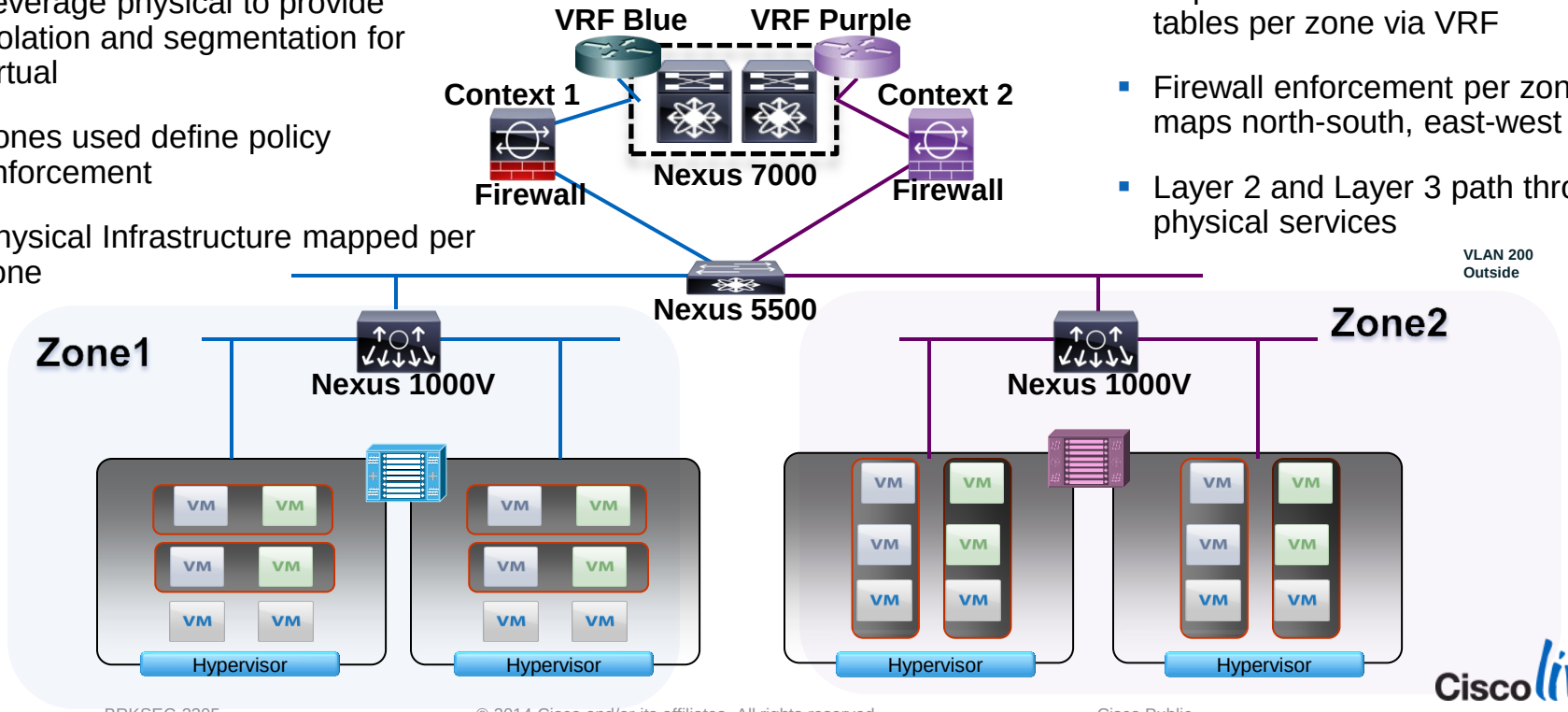
```
interface
TenGigabitEthernet0/6
channel-group 32 mode
active vss-id 1
no nameif
no security-level
!
interface
TenGigabitEthernet0/7
channel-group 32 mode
active vss-id 2
no nameif
no security-level
!
```

```
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 3232.1111.3232
 vlan 201
 nameif inside
 bridge-group 1
 security-level 100
!
interface Port-channel32.200
 mac-address 3232.1a1a.3232
 vlan 200
 nameif outside
 bridge-group 1
 security-level 0
```



Physical to Virtual

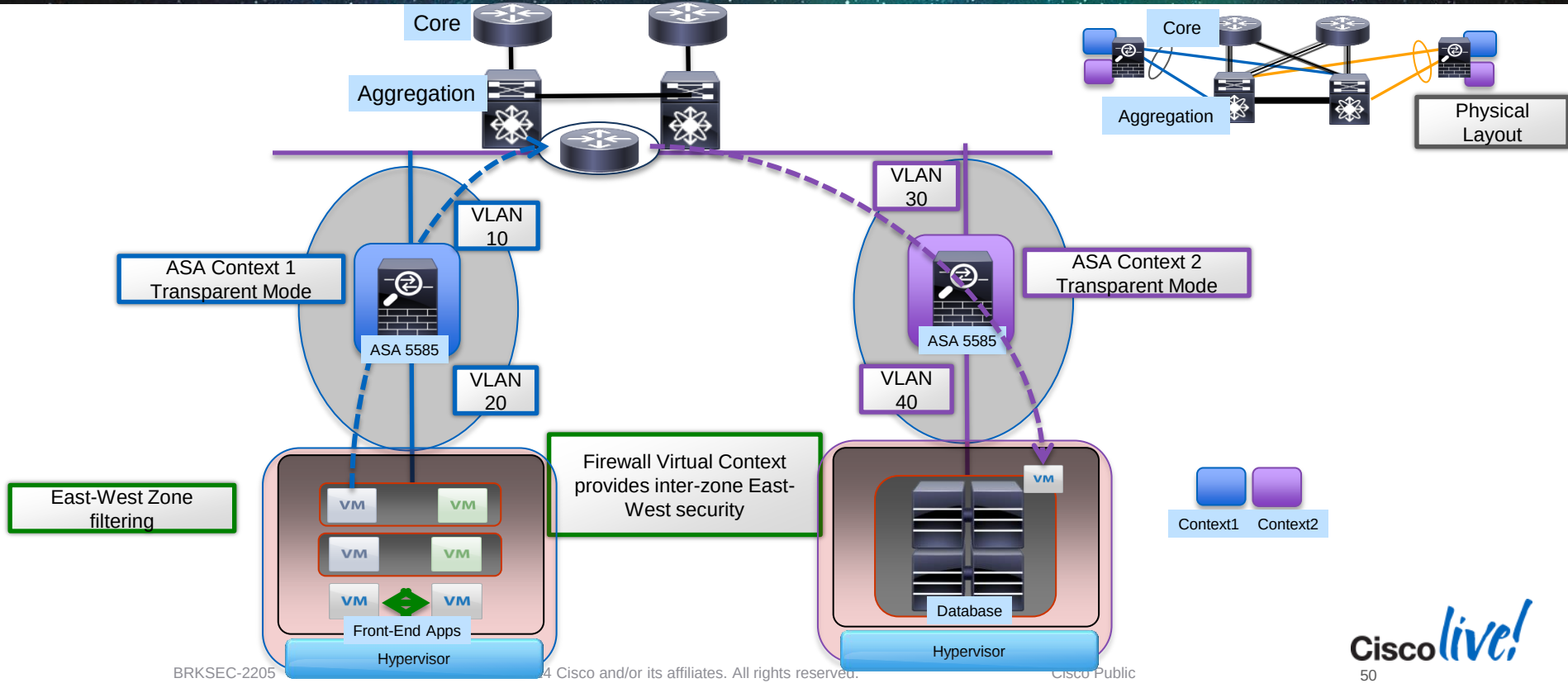
- Leverage physical to provide isolation and segmentation for virtual
- Zones used define policy enforcement
- Physical Infrastructure mapped per zone



- Separate and dedicated routing tables per zone via VRF
- Firewall enforcement per zone maps north-south, east-west
- Layer 2 and Layer 3 path through physical services

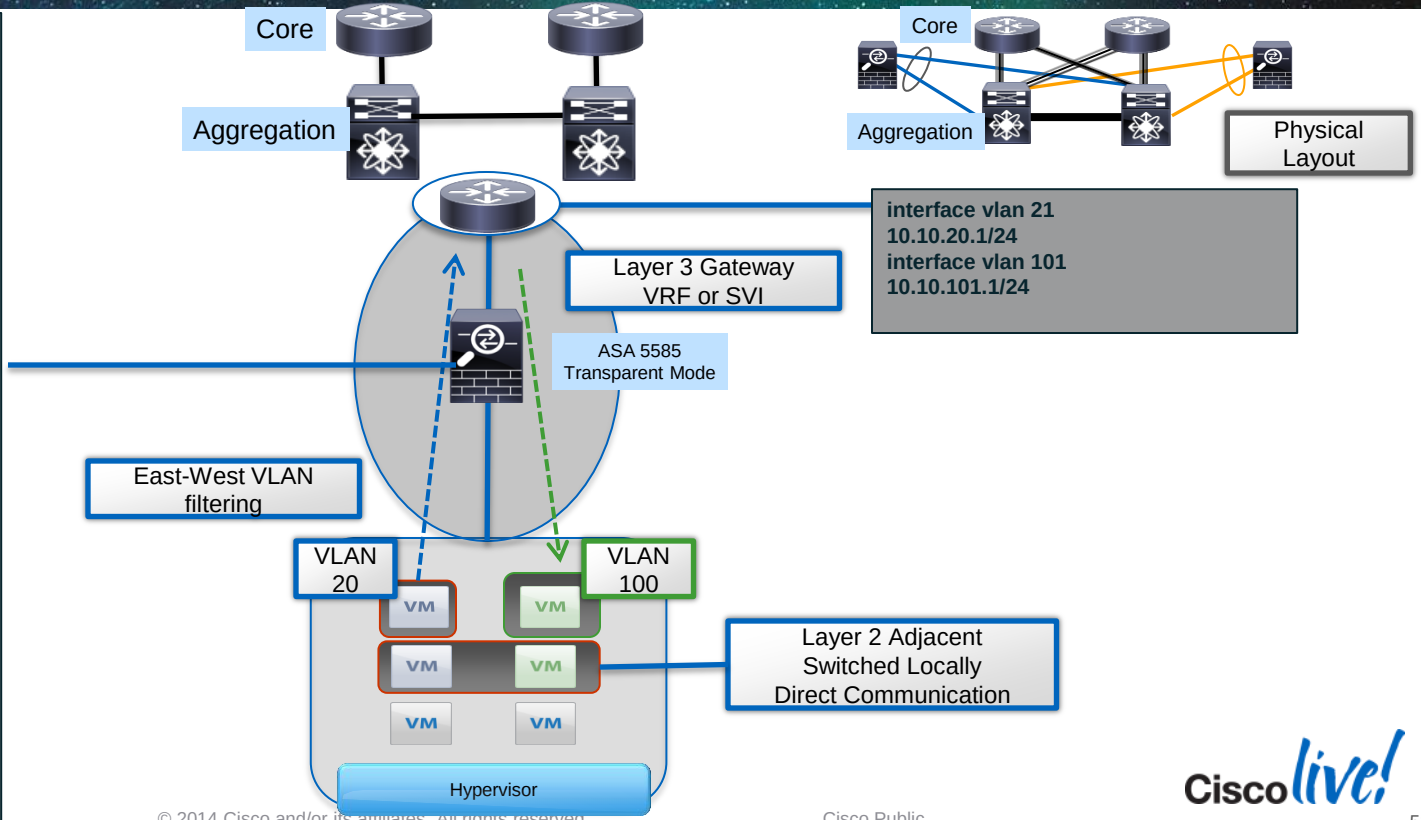
Firewall & Virtual Environment

ASA Virtual Contexts for Inter-Zone VM Traffic Flows



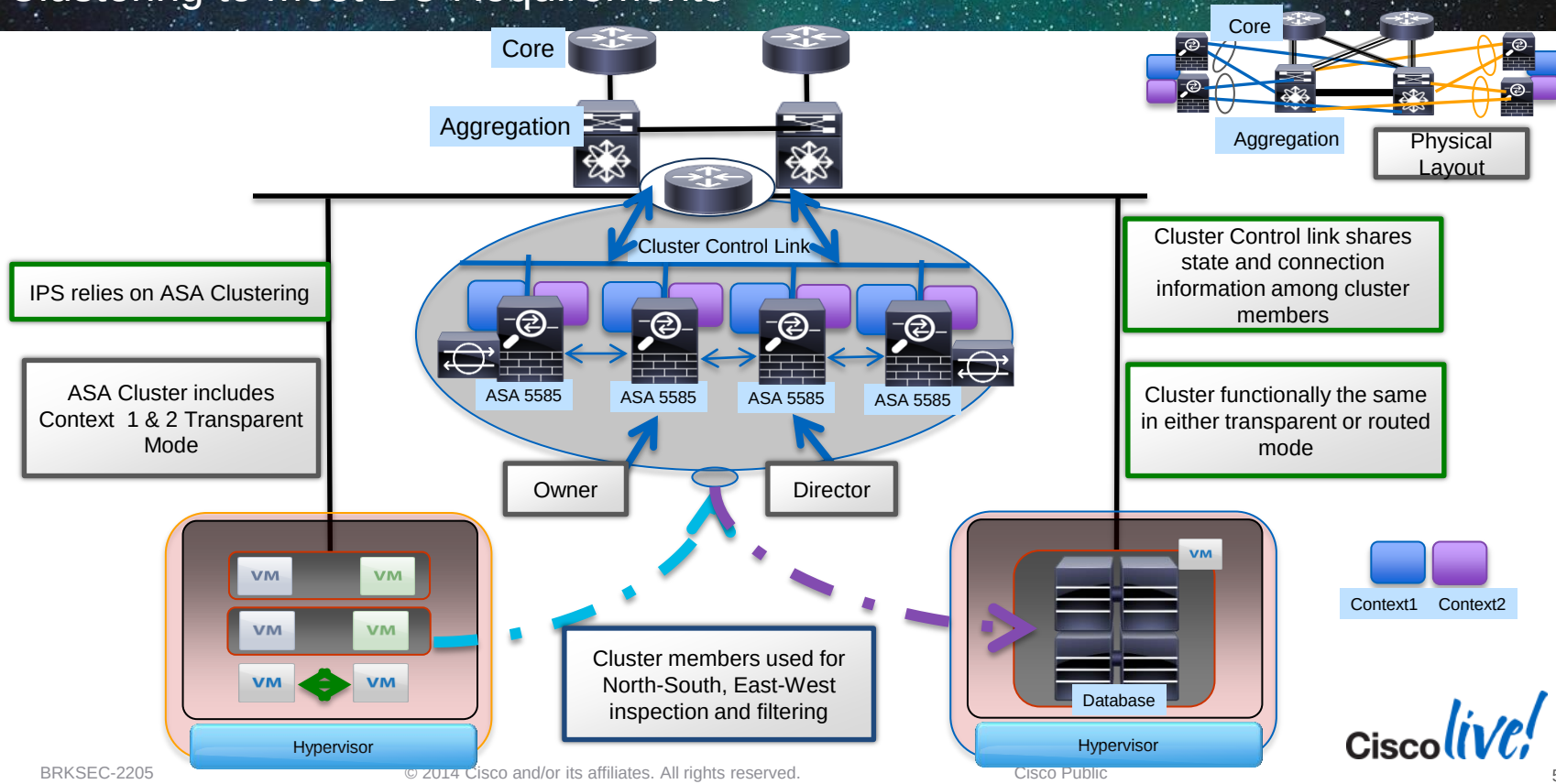
Inspecting Inter-VLAN VM Traffic Flows

```
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 10.10.101.254 255.255.255.0
!
interface Port-channel32
 no nameif
 no security-level
!
interface Port-channel32.20
 mac-address 3232.1111.3232
 vlan 20
 nameif inside
 bridge-group 1
 security-level 100
!
interface Port-channel32.21
 mac-address 3232.1a1a.3232
 vlan 21
 nameif outside
 bridge-group 1
 security-level 0
…
```



Firewall Clustering

ASA Clustering to meet DC Requirements

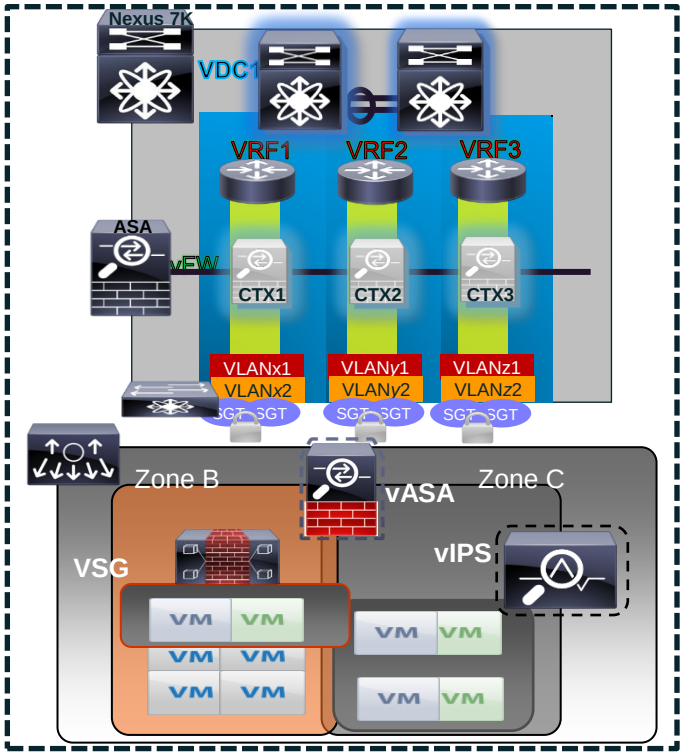


Physical to Virtual

Segmentation VRF-VLAN-Virtual

- Merging physical and virtual infrastructure
- Zones used define policy enforcement
- Unique policies and traffic decisions applied to each zone
- Physical Infrastructure mapped per zone
  - VRF, Nexus Virtual Device Context, VLANs, SGT

Segmentation Building Blocks



Enhanced Visibility and Threat Defence for the Data Centre

NetFlow Security Use Cases

- **Detecting Sophisticated and Persistent Threats.** Malware that makes it past perimeter security can remain in the enterprise waiting to strike as lurking threats. These may be zero day threats.

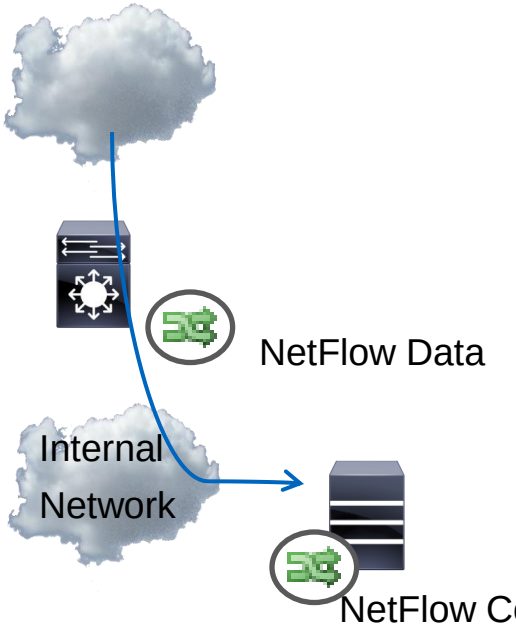
- **Identifying BotNet Command & Control Activity.** BotNets are implanted in the enterprise to execute commands from their Bot herders to send SPAM, Denial of Service attacks, or other malicious acts.

- **Uncovering Network Reconnaissance.** Some attacks will probe the network looking for attack vectors to be utilised by custom-crafted cyber threats.

- **Finding Internally Spread Malware.** Network interior malware proliferation can occur across hosts for the purpose gathering security reconnaissance data, data exfiltration or network backdoors

- **Revealing Data Loss.** Code can be hidden in the enterprise to export of sensitive information back to the attacker. This Data Leakage may occur rapidly or over time.

NetFlow in a Nutshell



Usage	• Packet count • Byte count	• Source IP address • Destination IP address	From/To
Time	• Start sysUpTime • End sysUpTime	• Source TCP/UDP port • Destination TCP/UDP port	Application
Port utilization	• Input ifIndex • Output ifIndex	• Next hop address • Source AS number • Dest. AS number • Source prefix mask • Dest. prefix mask	Routing and peering
QoS	• Type of Service • TCP flags • Protocol		

Cyber Threat Defence Solution Components

StealthWatch Management Console

Other tools/collectors

https

https

Cisco ISE

StealthWatch FlowReplicator

FR

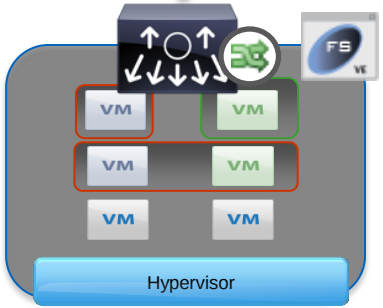
FC

StealthWatch FlowCollector

NetFlow

NetFlow

StealthWatch FlowSensor VE



NGA

NetFlow Generation Appliance

Cyber Threat Defence Solution

Use NetFlow Data to Extend Visibility to the Access Layer

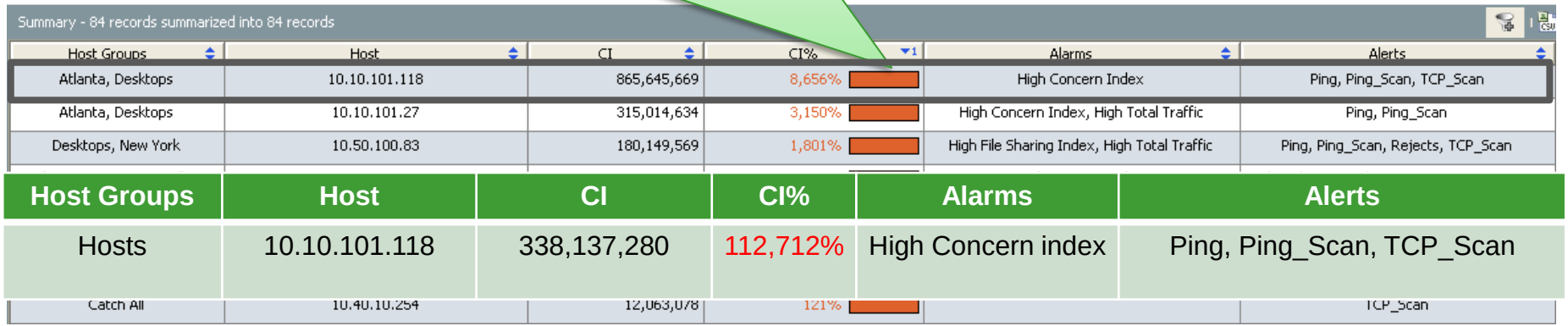
Enrich Flow Data With Identity, Events and Application to Create Context

Unify Into a Single Pane of Glass for Detection, Investigation and Reporting

Cisco CTD Solution

Attack Detection without Signatures

High **Concern Index** indicates a significant number of suspicious events that deviate from established baselines

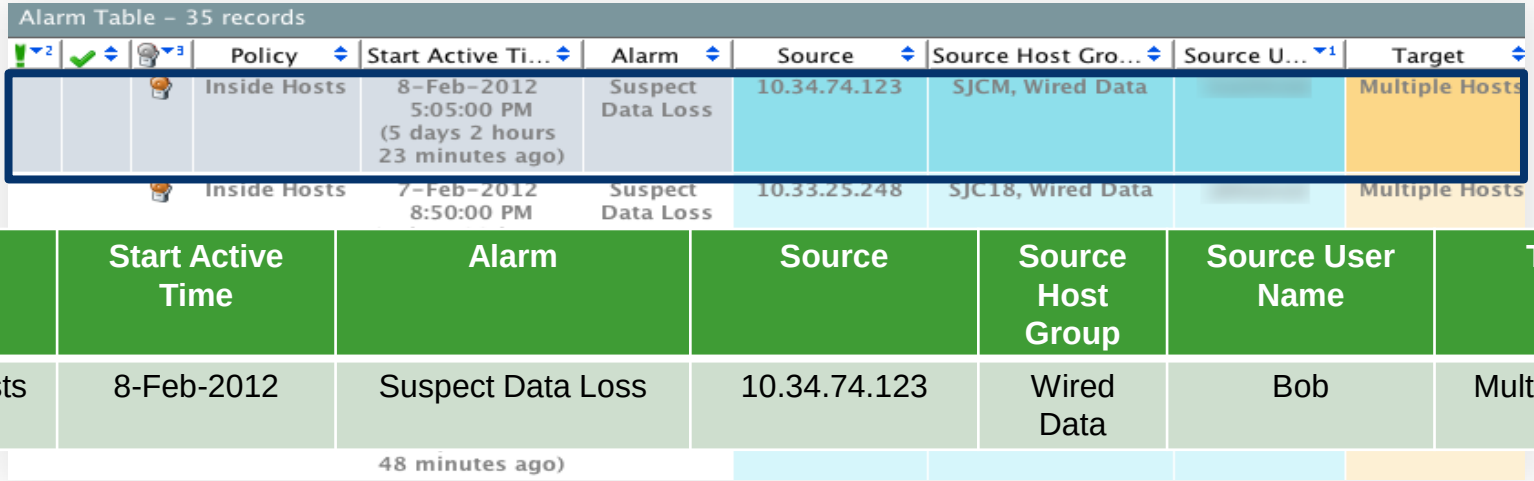


Host Groups	Host	CI	CI%	Alarms	Alerts
Hosts	10.10.101.118	338,137,280	112,712%	High Concern index	Ping, Ping_Scan, TCP_Scan

Monitor and baseline activity for a host and within host groups.

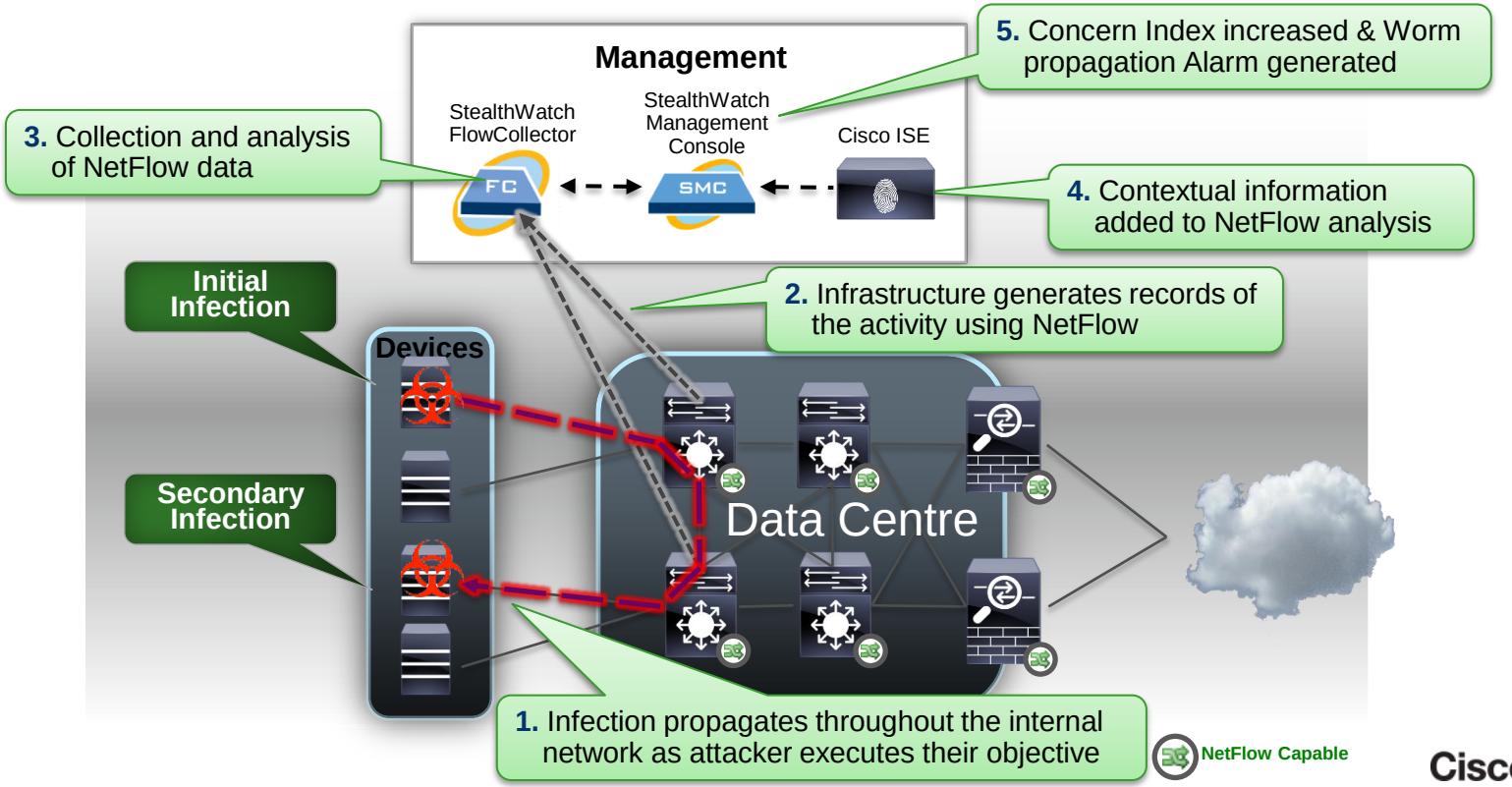
Identify Threats and Assign Attribution

Leveraging an Integration between Cisco ISE and Lancope StealthWatch



Policy	Start Active Time	Alarm	Source	Source Host Group	Source User Name	Target
Inside Hosts	8-Feb-2012	Suspect Data Loss	10.34.74.123	Wired Data	Bob	Multiple Hosts

Detecting Internally Spreading Malware

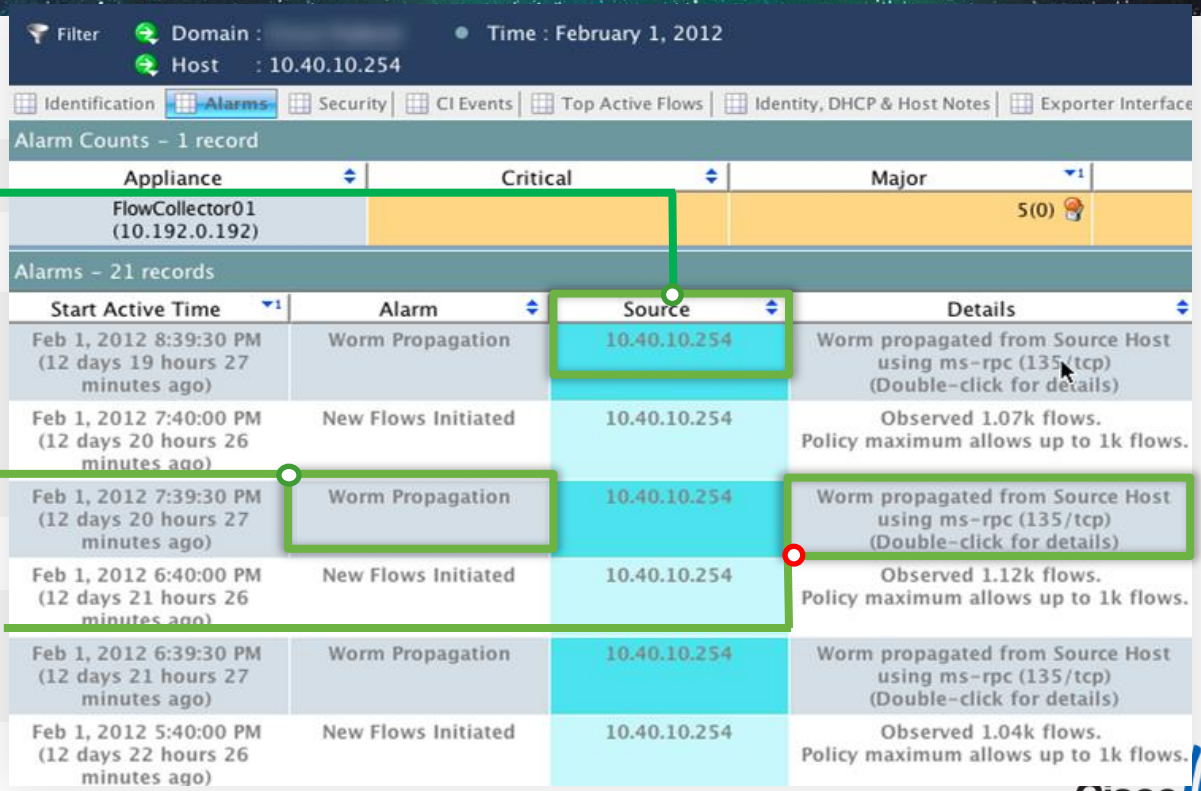


Detecting Internally Spreading Malware

IP Address

Alarm indicating this host touched another host which then began exhibiting the same suspicious behaviour

Suspicious activity that triggered the alarm

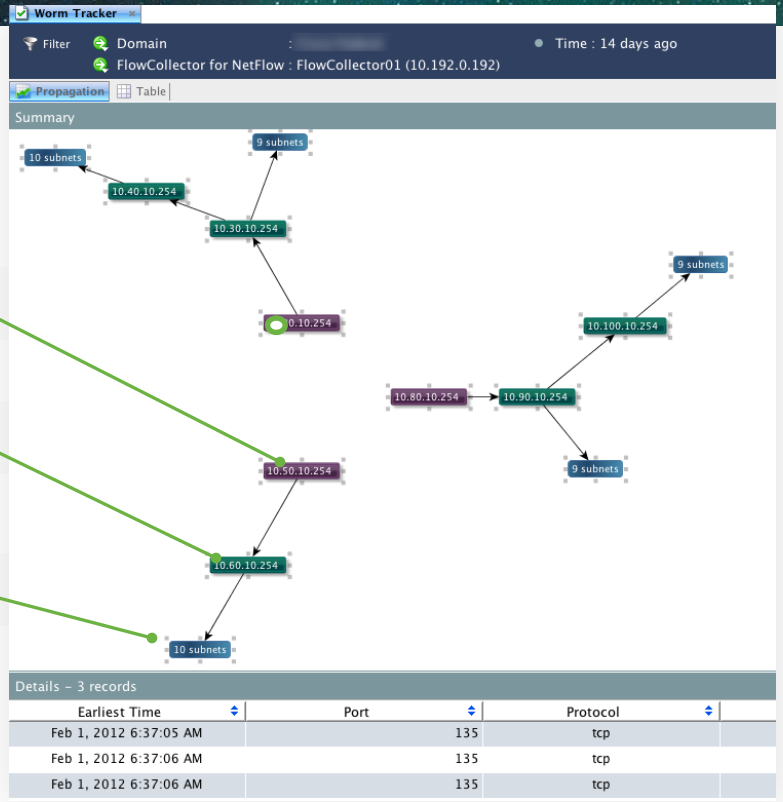


Infection Tracking

Initial Infection

Secondary Infection

Tertiary Infection



Summary

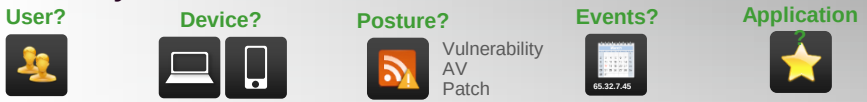
Leverages Cisco Network for Security Telemetry

NetFlow-enabled Cisco switches and routers become security telemetry sources

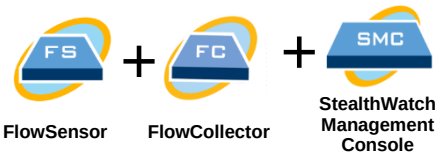
Cisco is the undisputed market leader in ***Hardware-enabled NetFlow devices***

Provides Rich Context

Unites NetFlow data with identity and application ID to provide security context



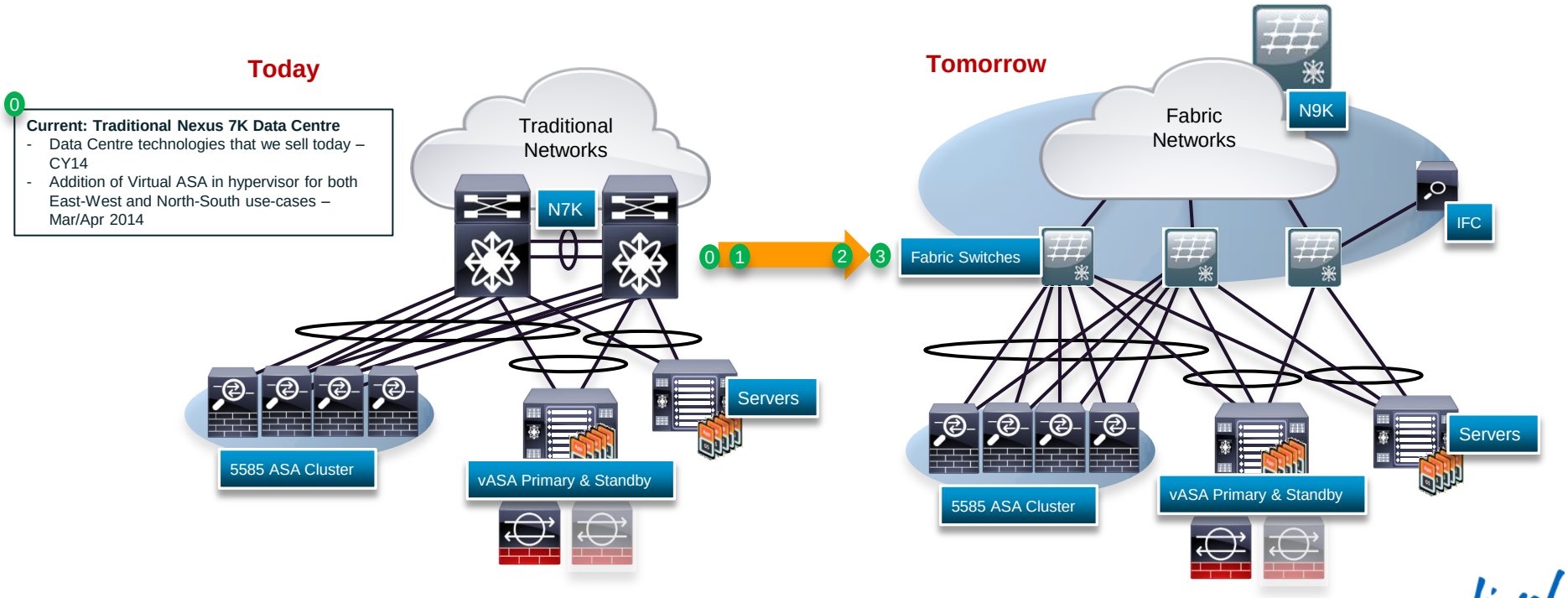
Provides Threat Visibility and Context



Single pane of glass that unifies threat detection, visibility, forensics analysis, and reporting

ACI Security Overview

Traditional Data Centre to Application-Centric Infrastructure Security (ACIS)



ACI Introduces Logical Network Provisioning of Stateless Hardware

Flat Hardware Accelerated Network

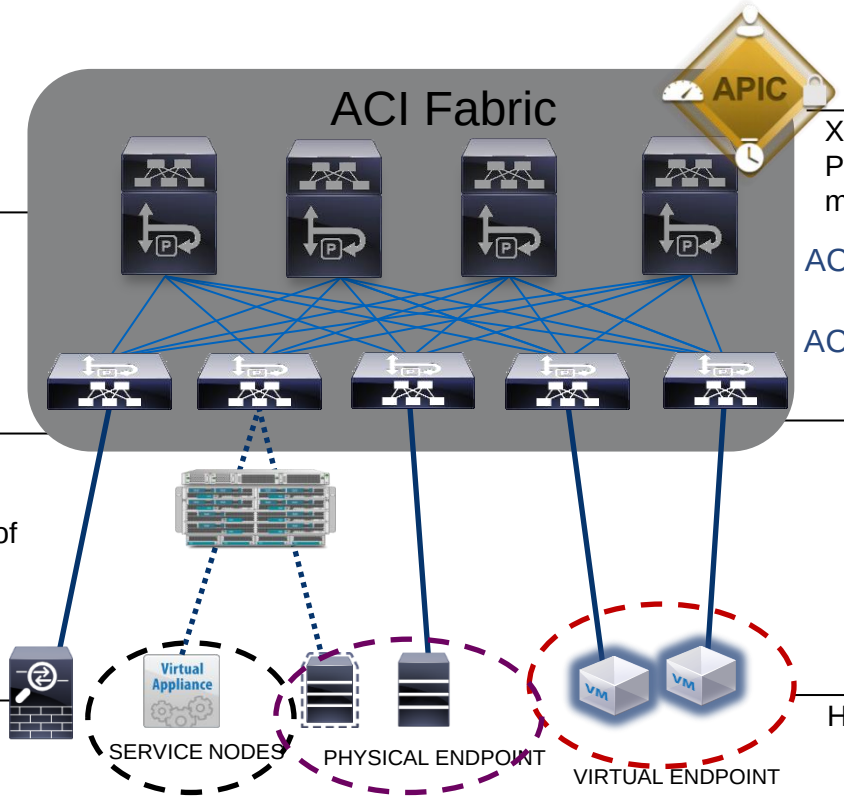
Full abstraction, de-coupled from VLANs and Dynamic Routing, low latency, built-in QoS

Flexible Insertion

Every device is one hop away, microsecond latency, no power or port availability constraints, ease of scaling

Unified Management and Visibility

ACI Controller manages all participating devices, change control and audit capabilities



Flexible Programmability

XML/JSON for Northbound API
Python scripting for custom device management

ACI Spine Nodes

ACI Leaf Nodes

Fabric Port Services

Hardware filtering and bridging; seamless service insertion, “service farm” aggregation

Logical Endpoint Groups by Role

Heterogeneous clients, servers, external clouds; fabric controls communication

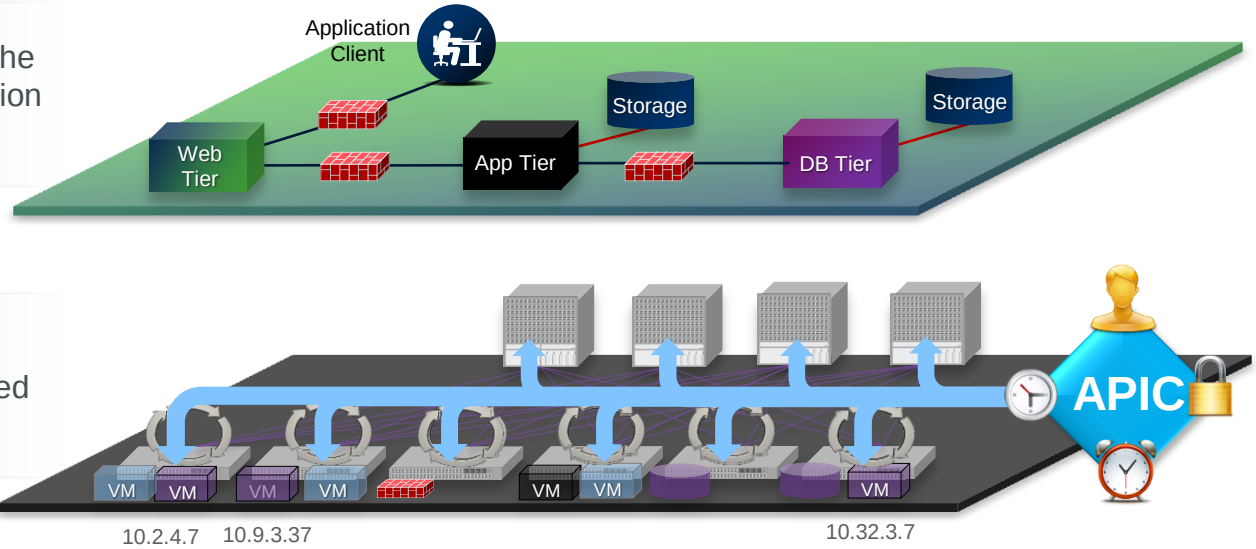



ACI Fabric Policy

Application Policy Model and Instantiation

Application policy model: Defines the application requirements (application network profile)

Policy instantiation: Each device dynamically instantiates the required changes based on the policies



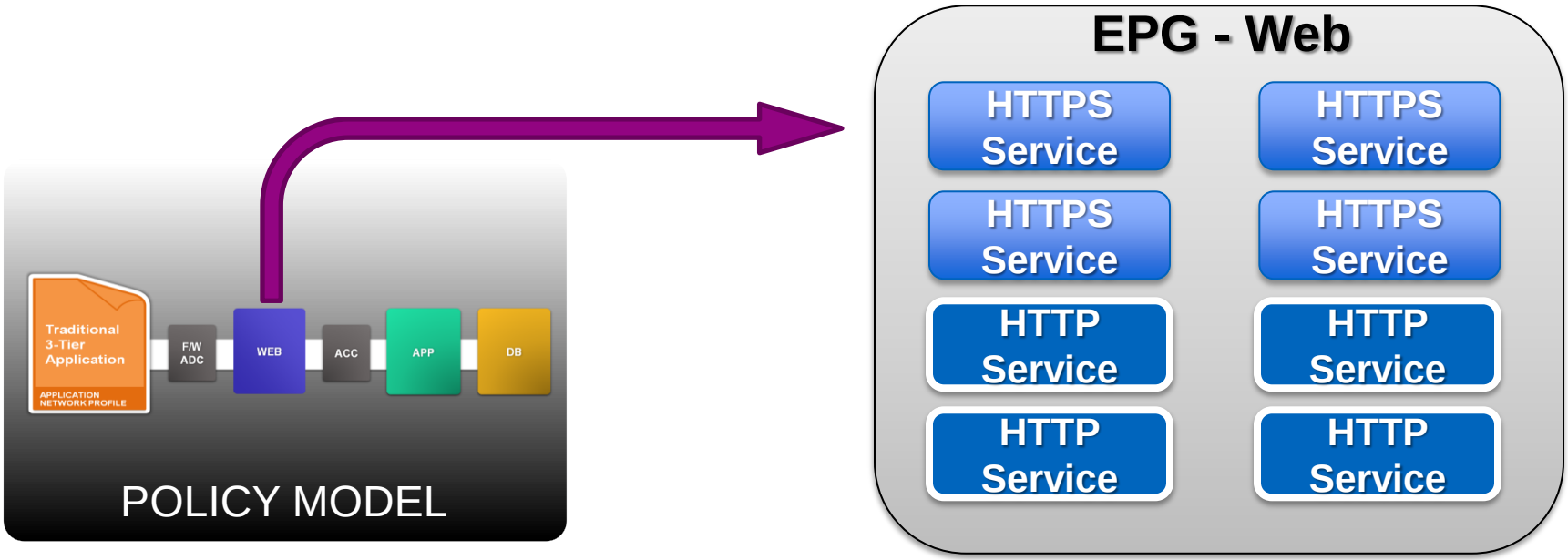
All forwarding in the fabric is managed through the application network profile

- IP addresses are fully portable anywhere within the fabric
- Security and forwarding are fully decoupled from any physical or virtual network attributes
- Devices autonomously update the state of the network based on configured policy requirements

What should be allowed to communicate
What should not be allowed to communicate
What should use an application service (Firewall, ADC)
What should have QoS, redirect, …, policies applied

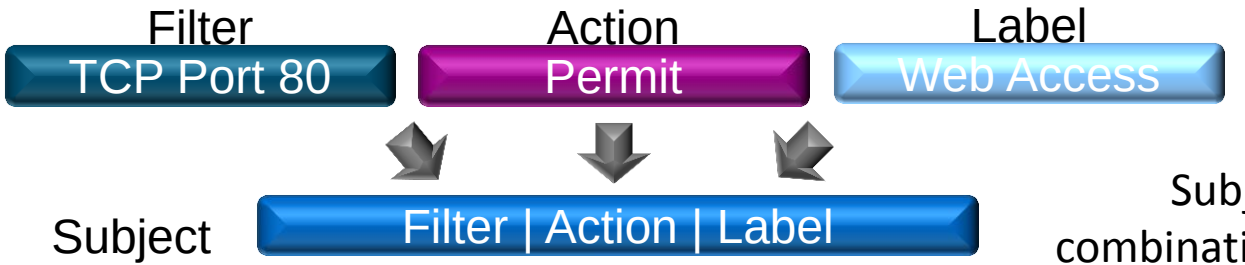
ACI Policy Model

Formalised Description of Connectivity



End-Point Groups (EPGs) are a grouping of end-points representing applications or application components independent of other network constructs.

Building Contracts



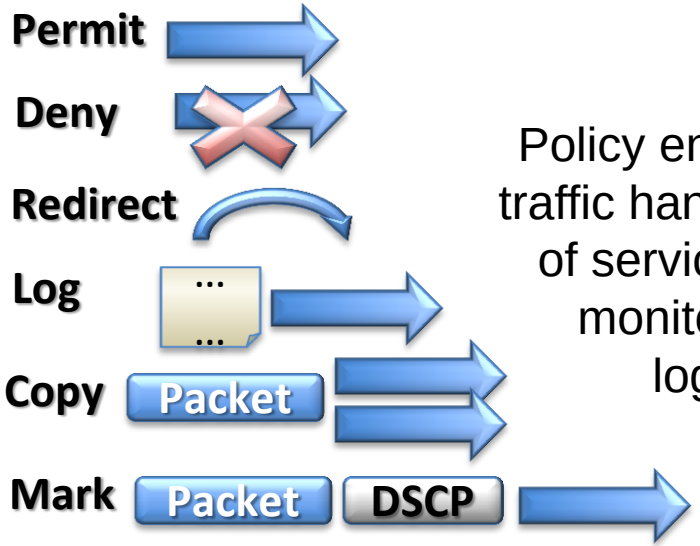
Subjects are a combination of a filter, an action and a label

Contracts define communication between source and destination EPGs

Contracts are groups of subjects which define communication between EPGs.

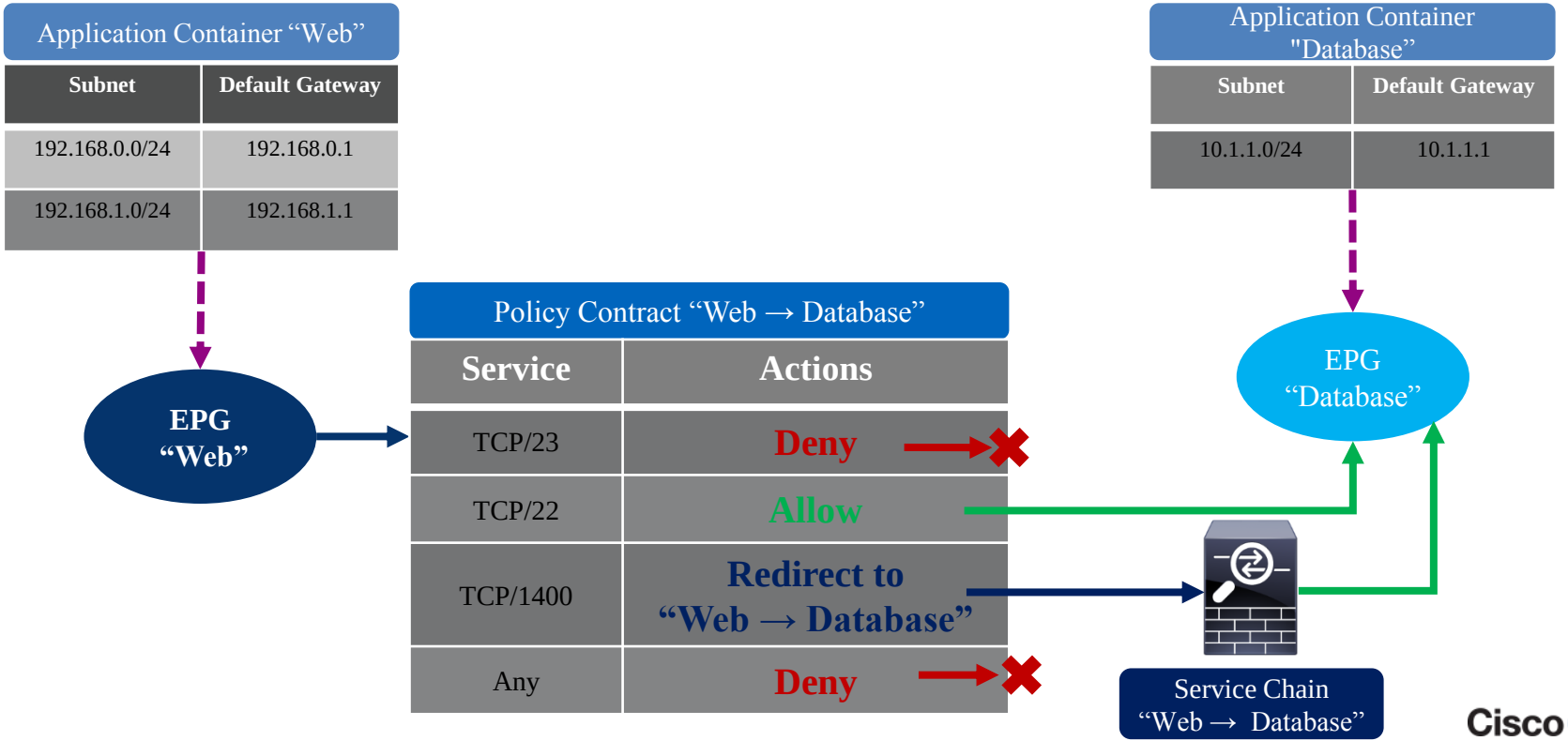
Policy Options: Actions

- There are six policy options supported:
- Permit the traffic
- Block the traffic
- Redirect the traffic
- Log the traffic
- Copy the traffic
- Mark the traffic (DSCP/CoS)



Policy encompasses traffic handling, quality of service, security monitoring and logging.

Inter-EPG Communication Example



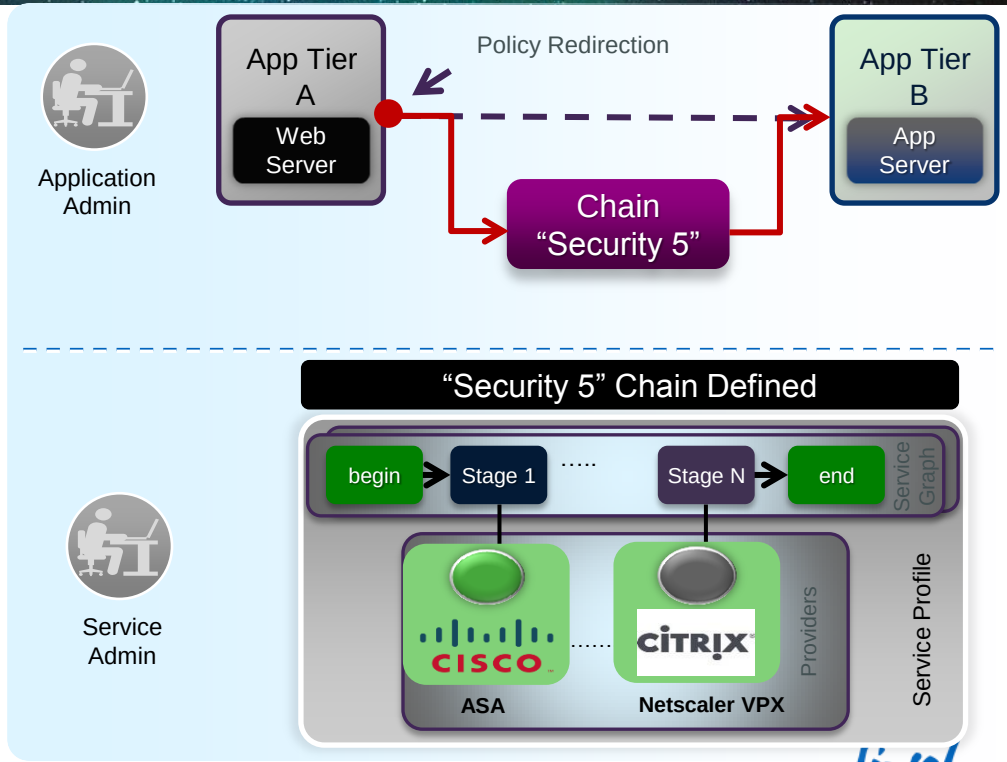



Service Insertion

ACI Layer 4 - 7 Service Integration

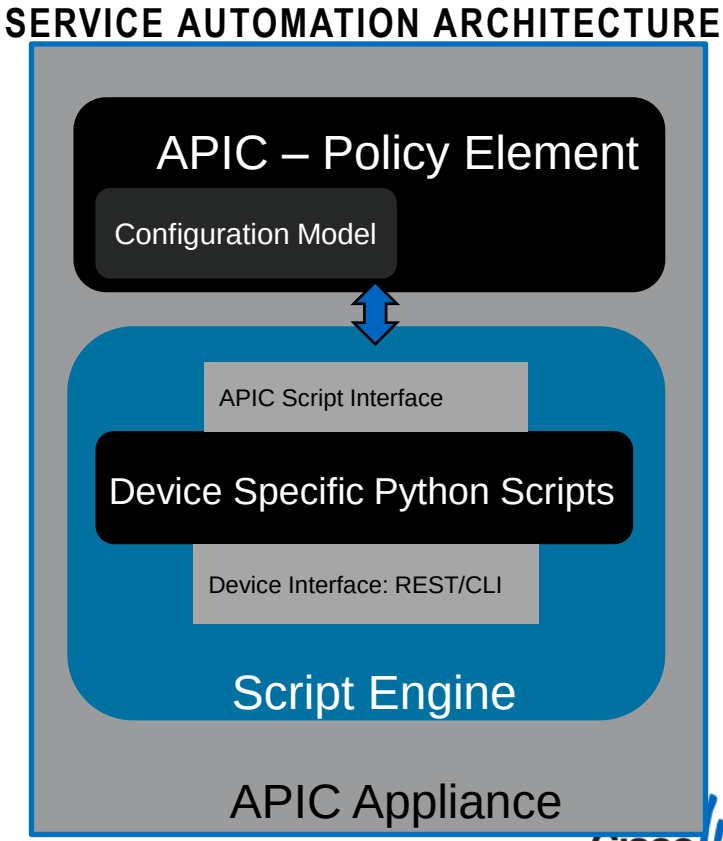
Centralised, Automated, and Supports Existing Model

- Elastic service insertion architecture for physical and virtual services
- Helps enable administrative separation between application tier policy and service definition
- APIC as central point of network control with policy coordination
- Automation of service bring-up / tear-down through programmable interface
- Supports existing operational model when integrated with existing services
- Service enforcement guaranteed, regardless of endpoint location



Device Package

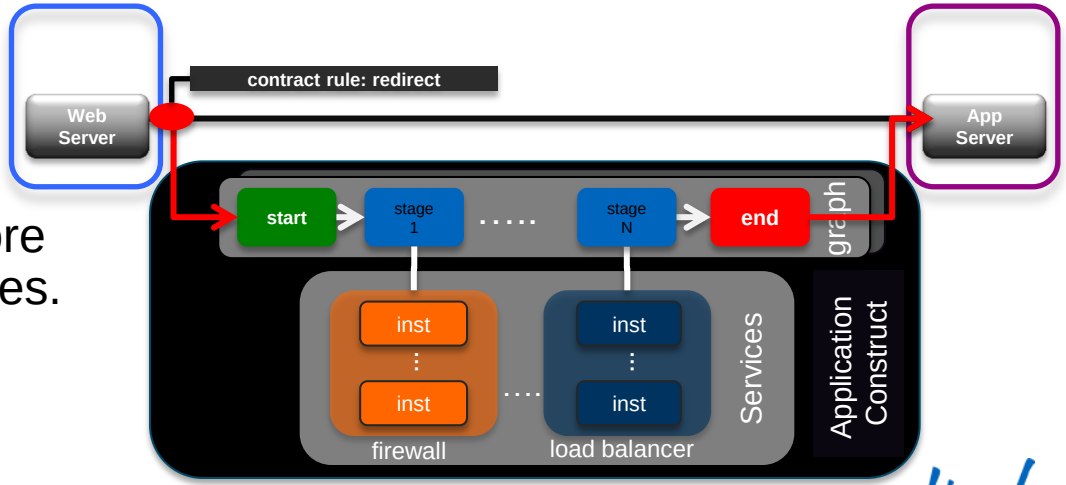
- Defines services appliances
- Lists service functions offered by the services appliance
- Provides scripts for driving service configuration
- Plan is to open the API so that anyone can create a device package and have a community similar to Puppet manifests or Chef recipes



Fabric Service Redirection

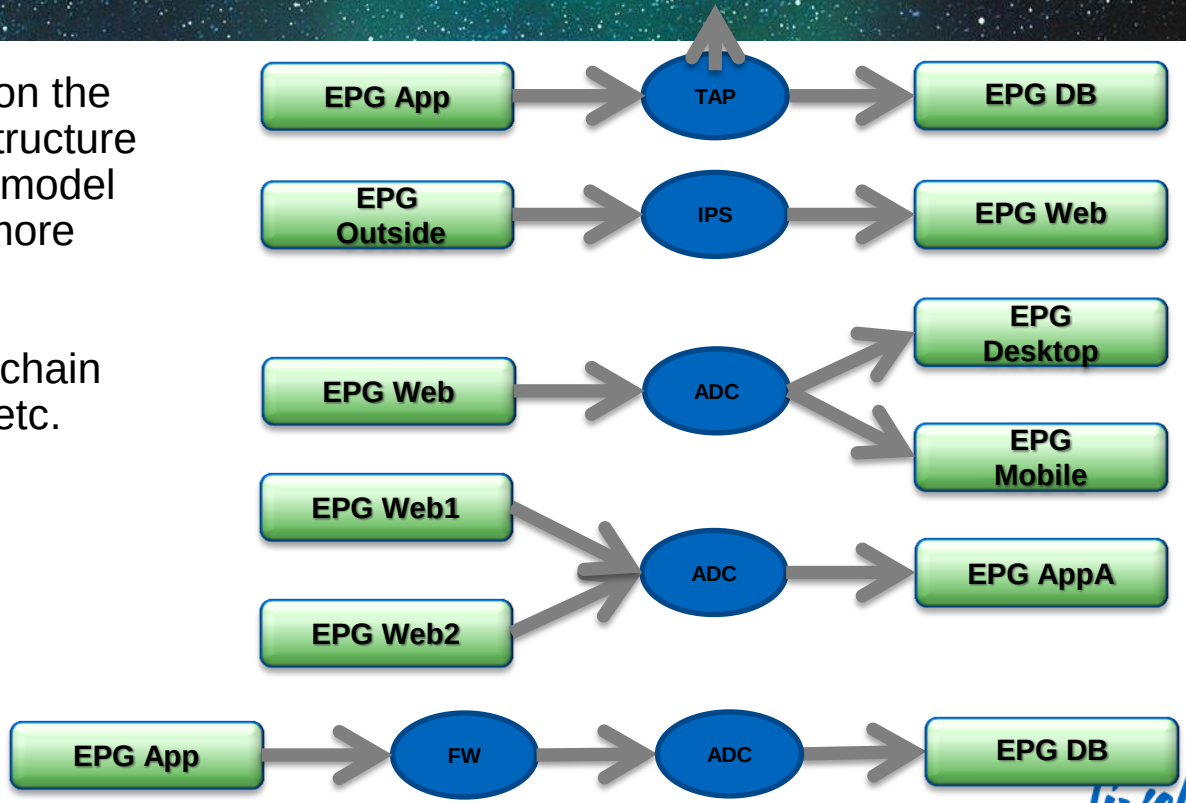
- Application-centric service graph simplifies and scales service operations
- Packet match on a redirection rule sends the packet into a services graph.
- A Service Graph can be one or more service nodes pre-defined in a series.
- Automated and scalable L4-L7 service insertion

Redirect Traffic to a services graph
Redirect [SRC, *] [DST, TCP 80] to FIREWALL_ADC_PROD



Service Graph Definition

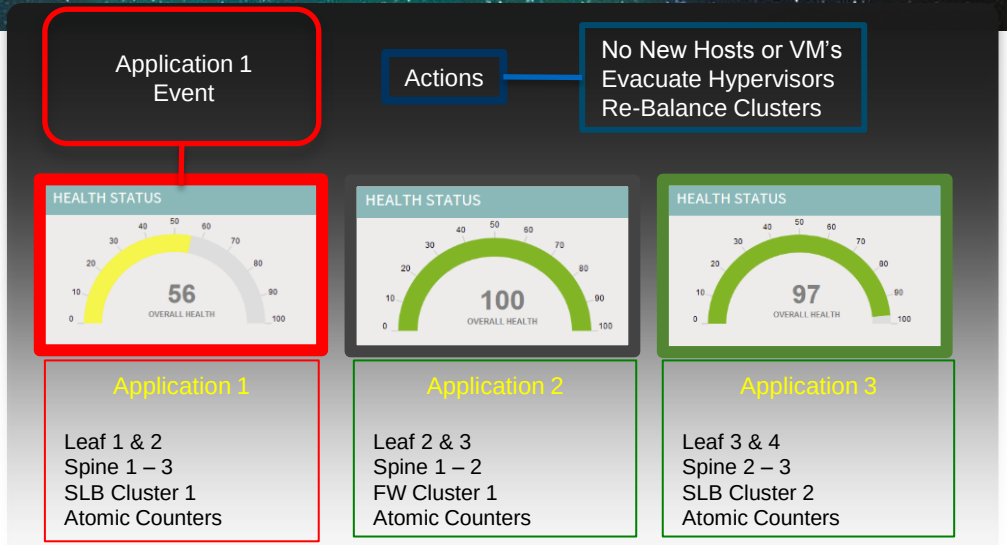
- Service Graphs are defined on the APIC. A service graph is a structure that defines the connectivity model between EPGs with one or more service nodes in between.
- The graphs can be a simple chain or involve splits, joins, taps, etc.
- Common services would be:
  - Firewall
  - IPS
  - TAP/Packet mirror
  - ADC/SLB



Service & Application Health

The Service Appliance can generate a health rating

- **Device:** Score the health of the Device on a scale from 0(failing)-255(working). It is up to the DeviceScript to define the meaning of the score, the IFC will simply report it to the user.
- **Virtual Device:** Score the health of the VDev on a scale from 0-255. Similar to the Device health score.
- **Service Capacity:** The capacity of the Device is typically defined by licensing and the DeviceScript needs to report capacity to the IFC to prevent over provisioning.
- **Service Availability:** Memory, CPU, cluster health, response time statistics as available on the service device or cluster.



Fabric provides next generation of analytic functions

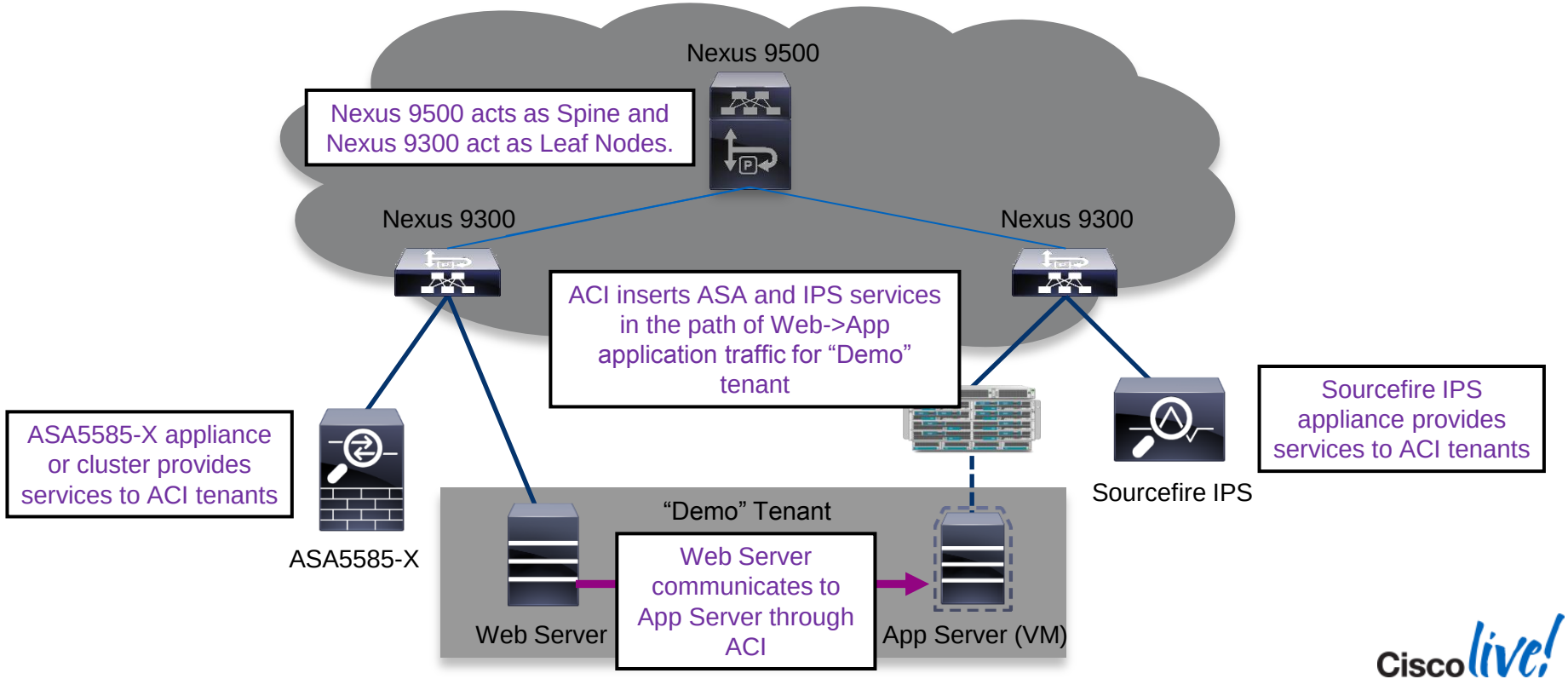
Per Application, Tenants and Infra:
- Health Scores
- Atomic Counters
- Latency
- Resources Consumption

Health Score tracks:
- Device
- Virtual Device
- Mem, CPU utilisation
- Service Capacity

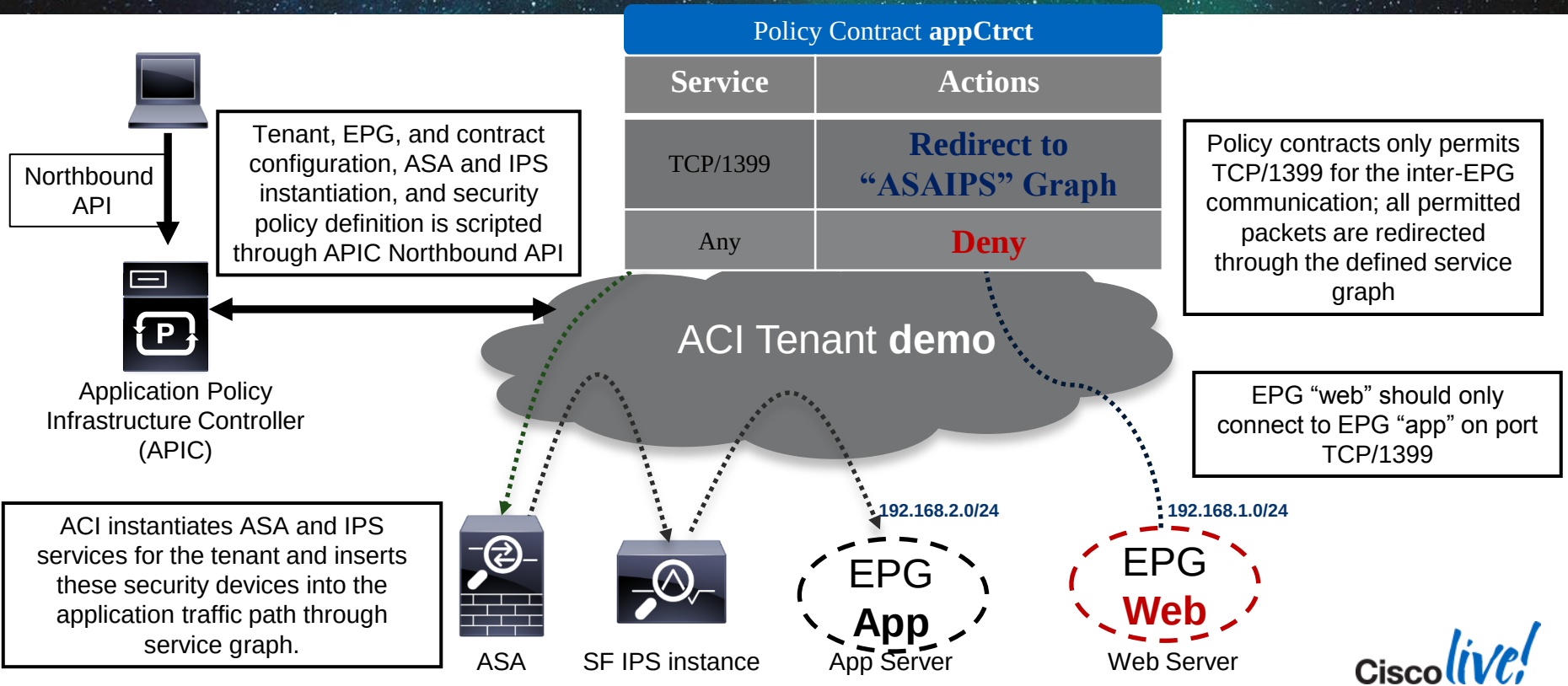



Demo Scenario

Physical Topology



Demo Flow



Demo: Application Centric Security




Summary

Summary

Defend, Detect, Control

- Virtual network services
  - Extend policy
  - Extend Visbility
  - Extend Workflow
- Leverage P-to-V fabric services to create unified policy
- Assume both internal and external threats
- ACI
  - Automatically instantiate security services and policies right with the application flows




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




Additional Slides

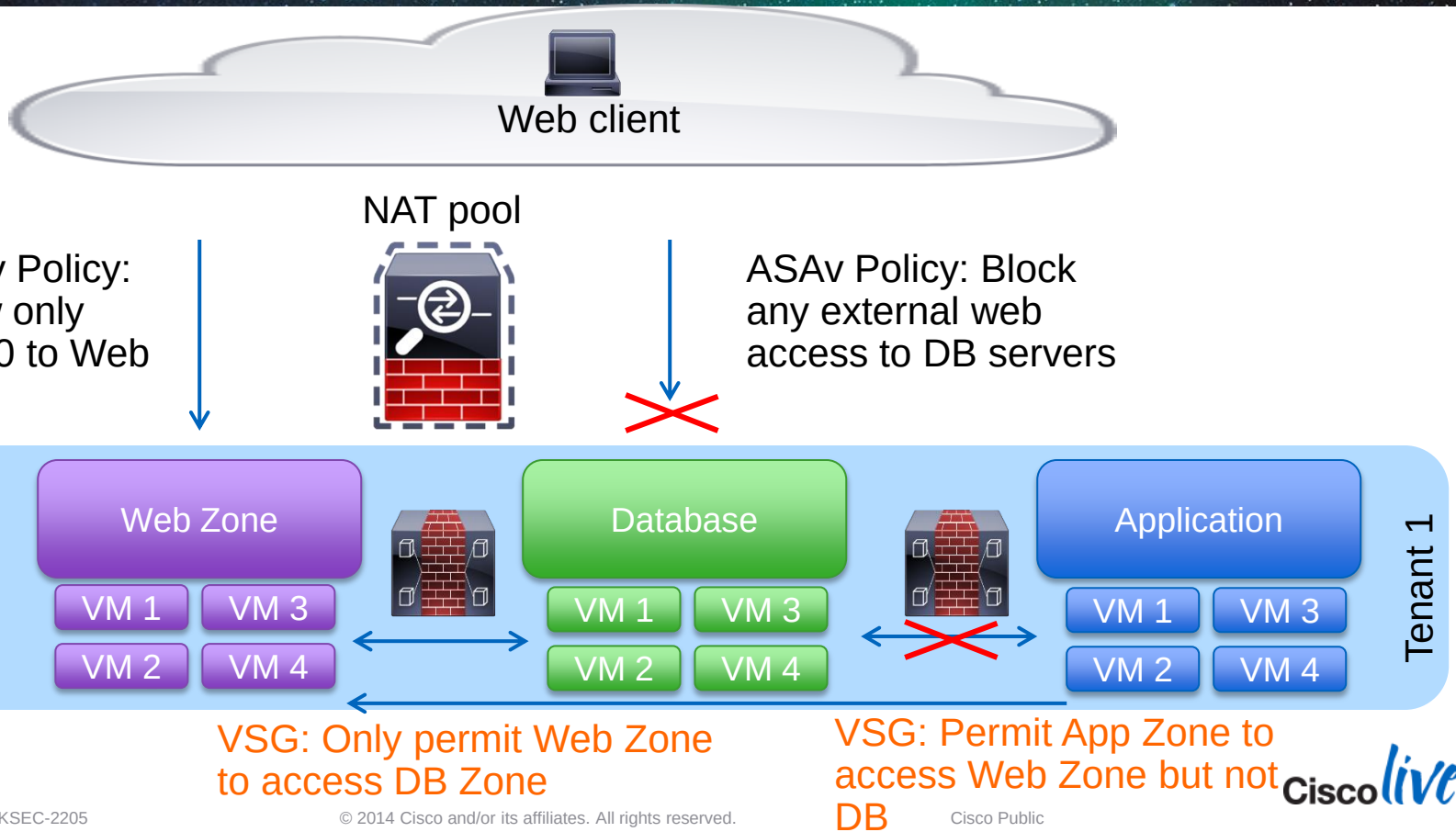
ASAv: Deployment Best Practices

- 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

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



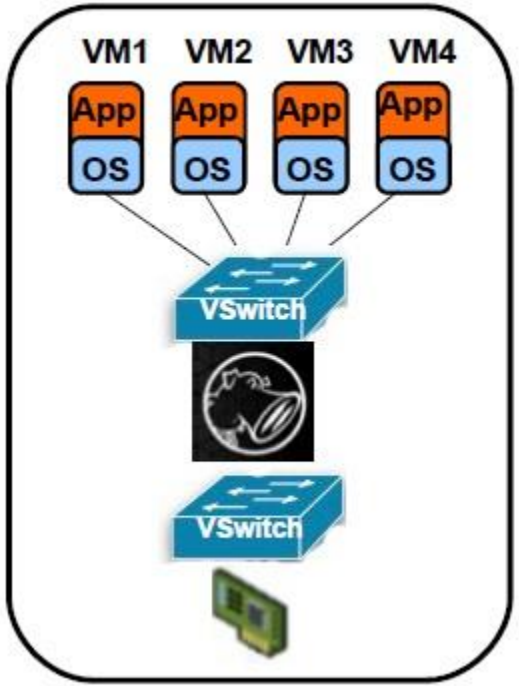
ASAv and VSG Compared

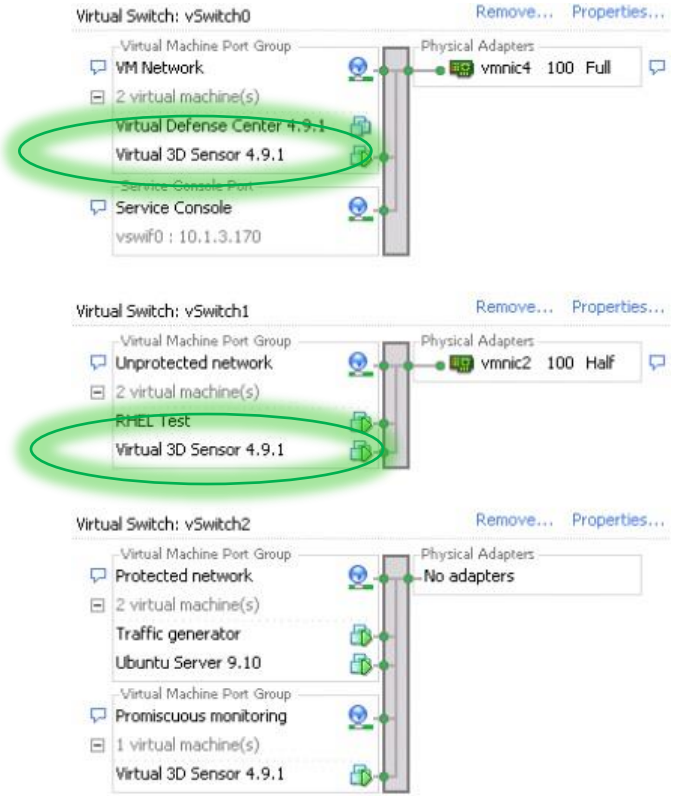
	ASAv with 4 vCPU	Virtual Security Gateway
Throughput	1-2GB stateful	vPath
Max Concurrent Sessions	500,000	256,000
Max Conns/Sec	20,000	6K-10K (1vCPU/2vCPU)
S2S VPN Sessions	750	NA
AnyConnect® Sessions	750	NA

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

Virtual Appliance

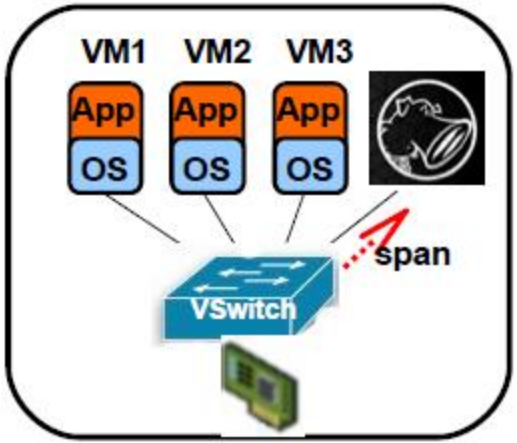
Inline

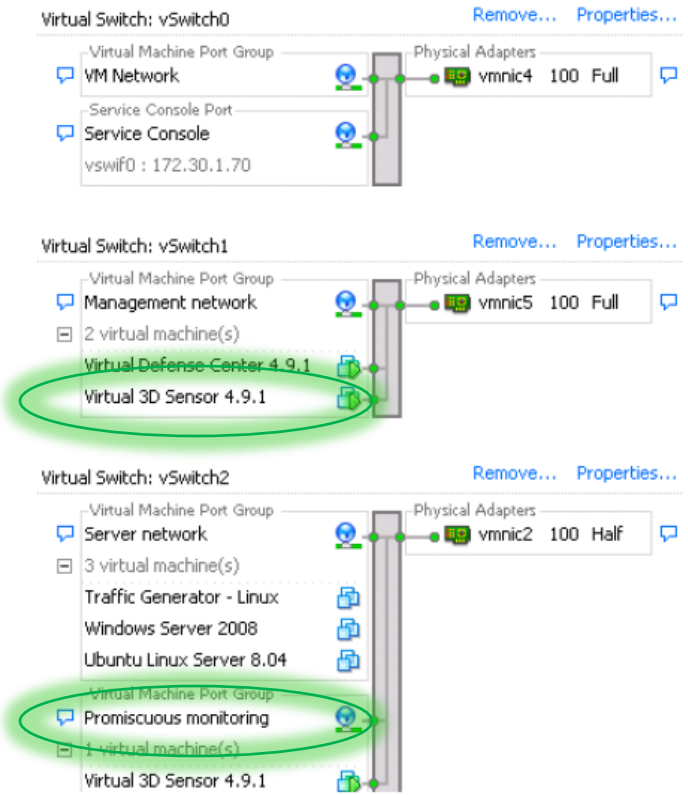




Virtual IDS

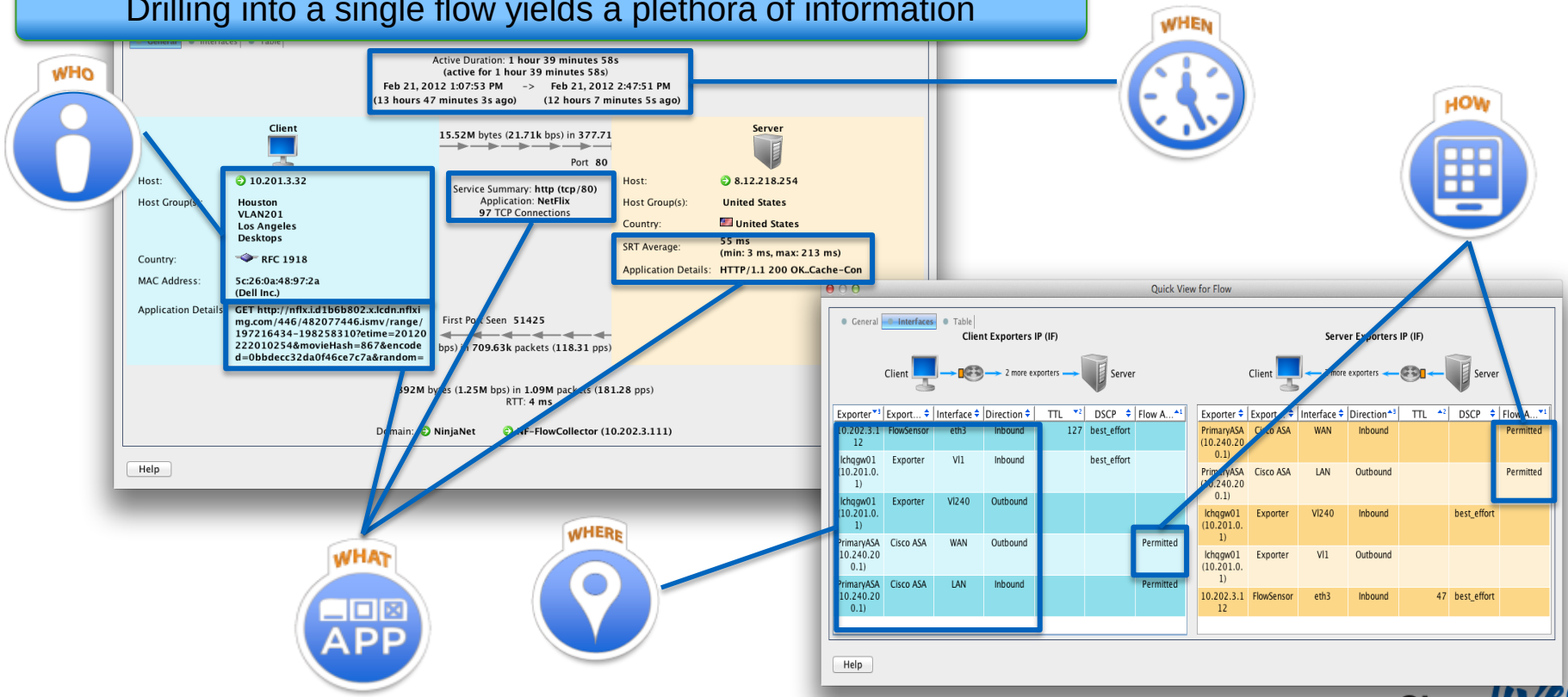
Passive





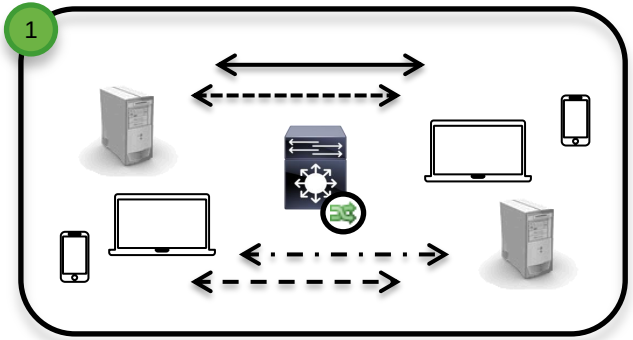
Cisco CTD Solution: Providing Scalable Visibility

Drilling into a single flow yields a plethora of information



Flow-based Anomaly Detection

1



Collect & Analyse Flows

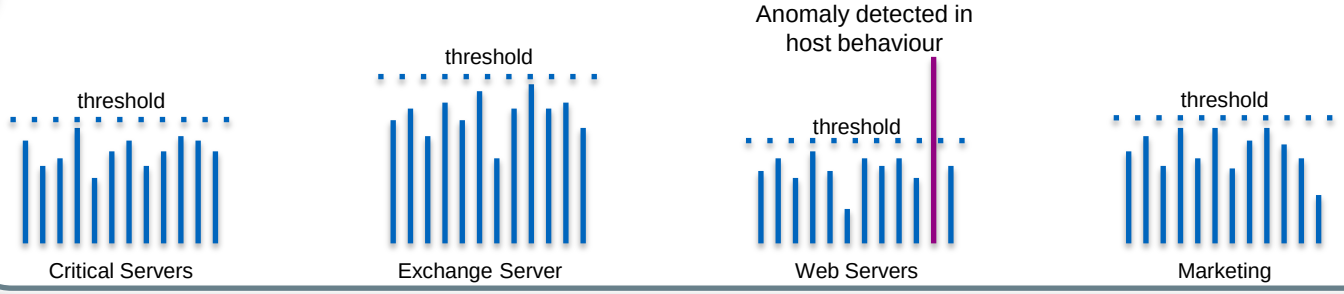
2

- # Concurrent flows
- Packets per second
- Bits per second
- New flows created
- Number of SYNs sent
- Time of day

- Number of SYNs received
- Rate of connection resets
- Duration of the flow
- Over 80+ other attributes

Establish Baseline of Behaviours

3



Alarm on Anomalies & Changes in Behaviour


CISCO
TM