

Cloud Network Security

End to End Cloud Overview

Session 17007

Thursday, March 5, 2015:

3:15 PM-4:15 PM

Issaquah A (Sheraton Seattle)

Junnie Sadler – jrsadler@cisco.com

Kevin Manweiler - kmanweil@cisco.com

#SHAREorg



SHARE is an independent volunteer-run information technology association that provides **education**, **professional networking** and **industry influence**.



Abstract



- This session focuses on the components that make up the network component of Data Center security and the challenges imposed by the Cloud and how they are addressed.

Complete your session evaluations online at www.SHARE.org/Seattle-Eval



Learning Objectives



On completion of this session participants will be able to...

- Understand the basic components and features that make up network security
- Understand the challenges that Cloud introduces and what options are available to deal with them
- Understand the challenges that Virtualization introduces and how to deal with them

Complete your session evaluations online at www.SHARE.org/Seattle-Eval



Agenda

Cloud Network Security Challenges
Cloud Network Security Components
Cloud Network Segmentation
Security Compliance

Complete your session evaluations online at www.SHARE.org/Seattle-Eval

THE NEWS

Follow +1 Like YouTube RSS

Search articles & products



24

NEW ARTICLES
TODAY

FEATURES

REVIEWS

PRODUCTS

SHOWS

VIDEO ^{NEW}

ABOUT

TIP US

FORUMS

JOIN A
CREW

SECTIONS

Science

Culture

Web & Social

Gaming

Policy & Law

Apps & Software

Apple

Android

SEE ALL

TRENDING

Chinese Hackers
Target U.S. Media—
Wall Street Journal
& N.Y.T. breached...

Super-critical
Java Zero-Day
Exploits Two Bugs...

Android web

LinkedIn

Facebook

ALERT

Financial Institution DDoS attacks: no break in sight

Hacker group expands targets

DDoS attacks

Executive Order on
Cybersecurity

Cloud Data Center Security Challenges

Complexity



- Too many different security components
- No easy way of collecting data and correlate
- Integration is a nightmare

Compliance



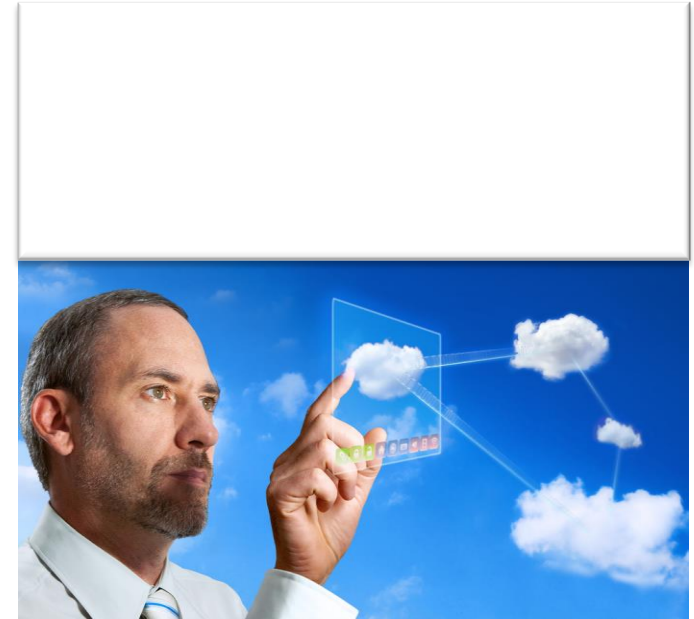
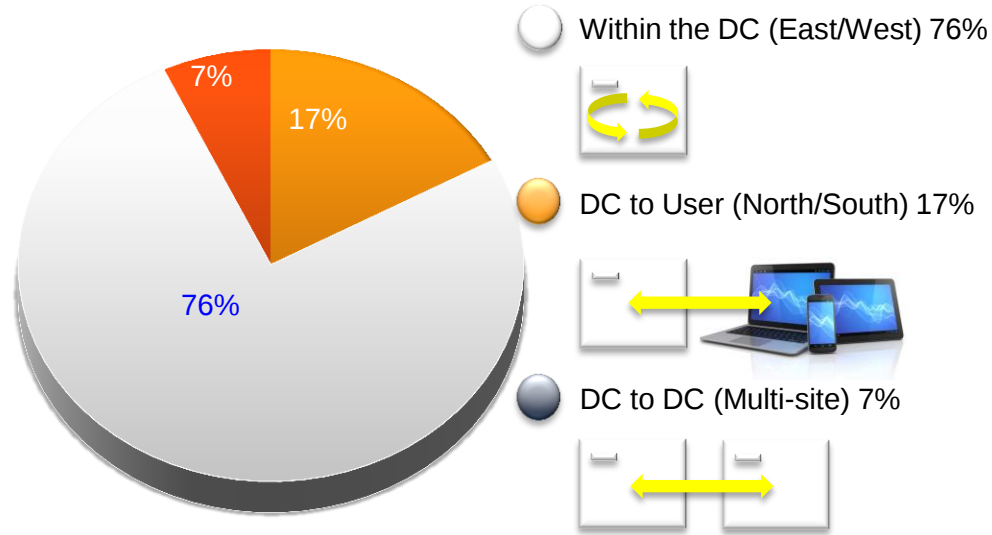
- Growing Regulatory Requirements: PCI, HIPAA, FISMA
- Little to No Guidance On How to Meet New Standards
- Huge non-compliance fines

Visibility



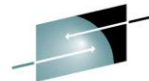
- Need to know complete context
- Utilize global intelligence with data analytics
- Behavioral analysis and forensic investigations

Security Must Be Part of The DC/Cloud Architecture



Complete your session evaluations online at www.SHARE.org/Seattle-Eval

Tenant Requirements of the Cloud Provider



Regulatory compliance

Is my Cloud Provider able to ensure compliance with regulations such as PCI, HIPAA, or FISMA?

Secure Multi-Tenancy

Can my Cloud Provider safeguard my workloads, protect sensitive data, and maintain complete isolation to prevent compromise?

End-to-End Visibility

Can I see my cloud environment as part of my DC, including access to forensic and remediation data?

Privileged user access

Can my Cloud Provider ensure that only my authorized users have access to my cloud environment?

Complete your session evaluations online at www.SHAKE.org/Seattle-Eval

Impact

- Revenue loss
- Loss of reputation
- Damaged customer relationships
- Significant Fines and Fees
- Litigation or Arbitration

Detection is Key to Response and Recovery



85% of attacks begin compromising their target within minutes

60% of attacks begin exfiltrating data within hours

85% of attacks are not discovered for weeks or months

59% of attacks are not contained for weeks or months **AFTER** discovery



Complete your session evaluations online at www.SHARE.org/Seattle-Eval

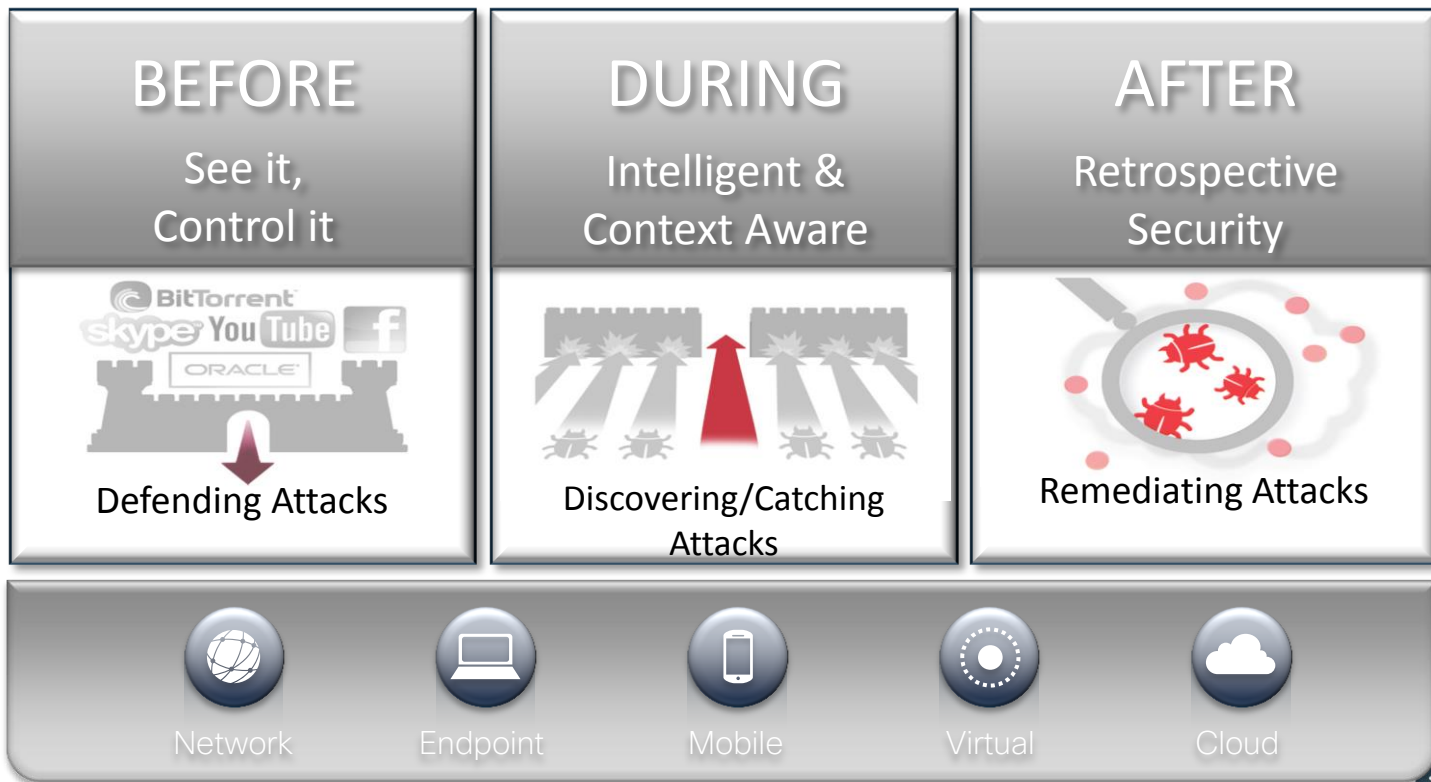
Source: Verizon 2012 Data Breach Investigation Report



Network Security Components

Complete your session evaluations online at www.SHARE.org/Seattle-Eval

Implications for Security Process and Technology



Complete your session evaluations online at www.SHARE.org/Seattle-Eval



Implications for Security Process and Technology



BEFORE

See it,
Control it



Defending Attacks

DURING

Intelligent &
Context Aware



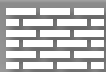
Discovering/Catching
Attacks

AFTER

Retrospective
Security



Remediating Attacks



FIREWALL



IPS



MALWARE
PROTECTION



VPN



WEB



NETWORK
ANALYSIS



CONTEXT



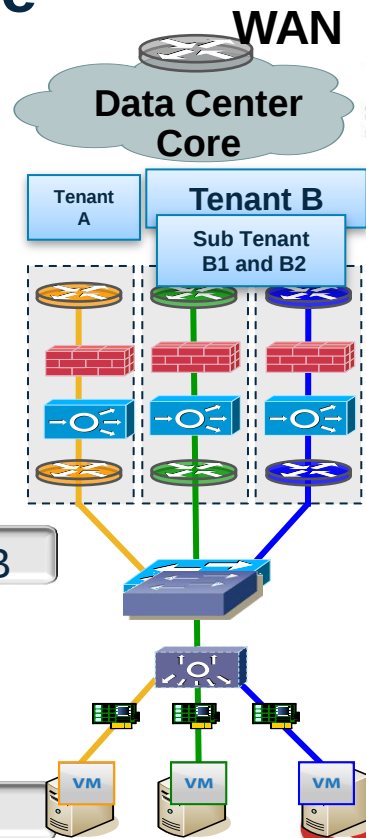
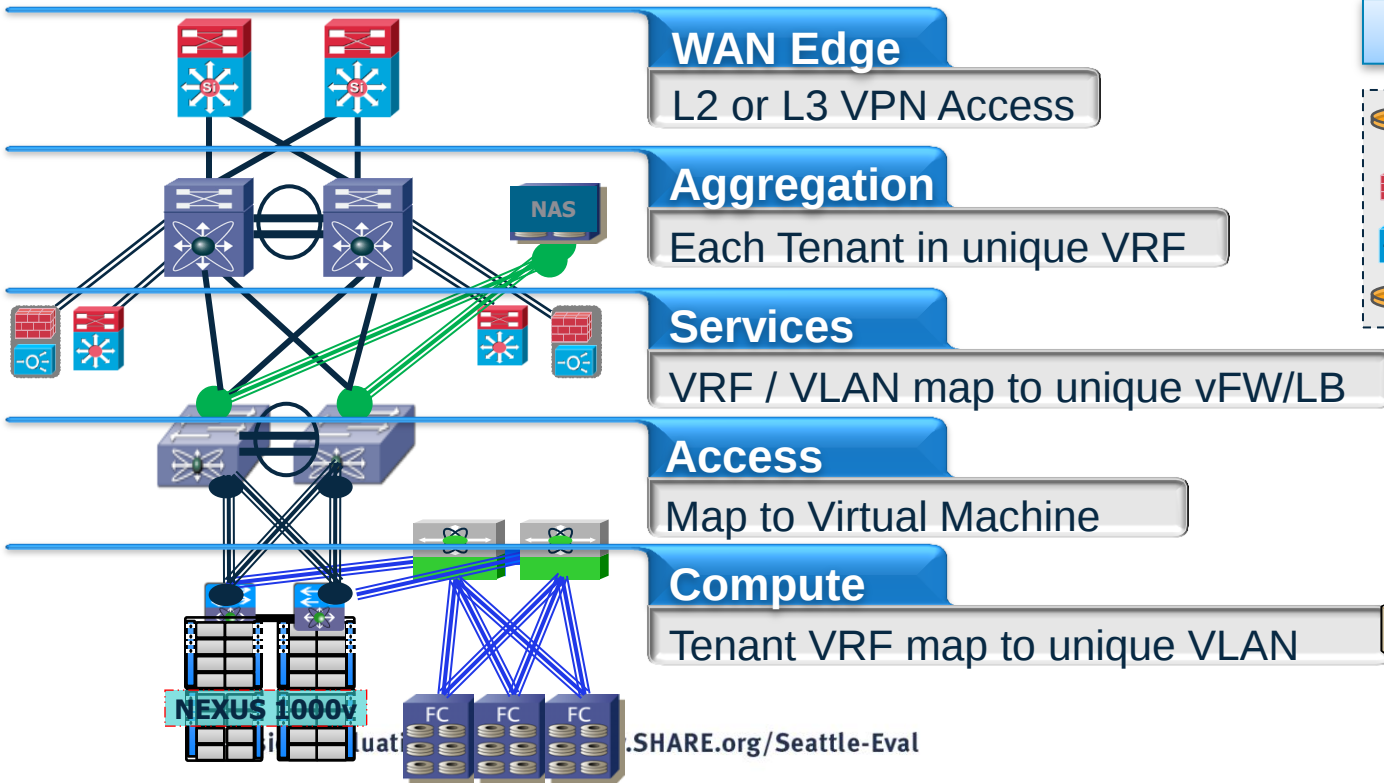
EMAIL

Complete your se

SHARE
Seattle 2015

Simplified Cloud Reference Architecture

Secured and Private VPN
MPLS or IPsec / SSL

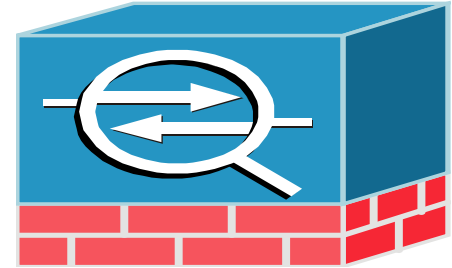


FW - Firewall



The workhorse of network security

Acts as a packet filter - allows the “good” packets through and discards the “bad”



Complete your session evaluations online at www.SHARE.org/Seattle-Eval



FW – Firewall (2)

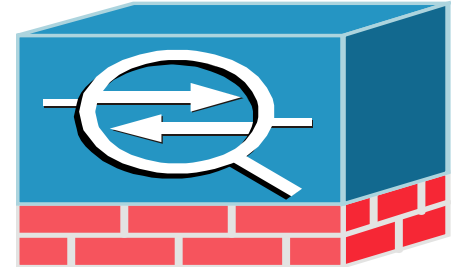


Can perform Network Address Translation (NAT) and Port Address Translation (PAT)

Translates “inside” (protected) address to an “outside” (unprotected) address

For TCP traffic also randomizes sequence starting ID's to help prevent hijacking

Can act as a VPN termination point



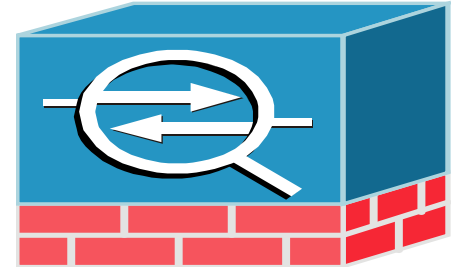
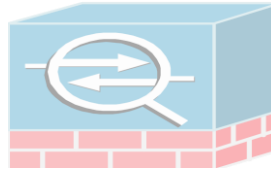
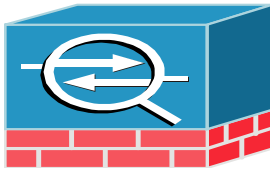
Complete your session evaluations online at www.SHARE.org/Seattle-Eval



FW – Firewall (3)

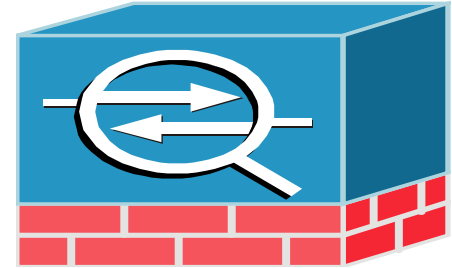
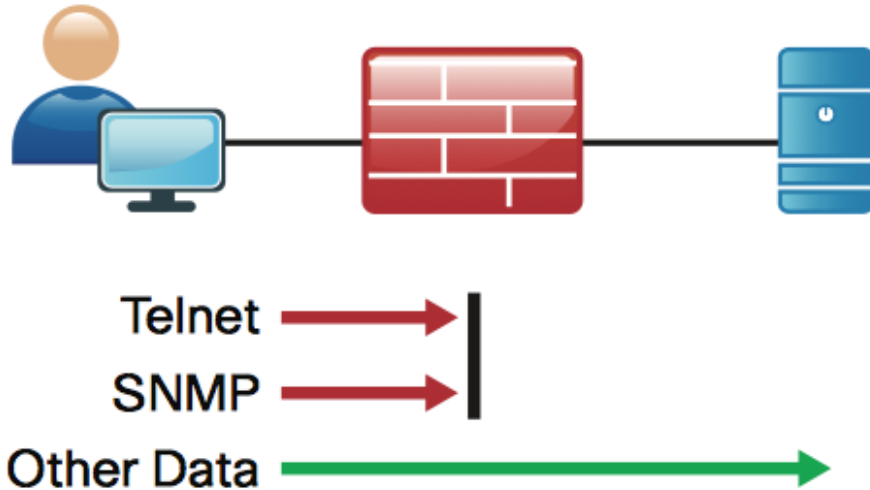
Can be deployed in High Availability mode – 1 active and 1 standby.

“Stateful” firewalls require symmetric traffic flow; ie, if it goes out one side it has to come back the same way.



FW – Firewall

Black List

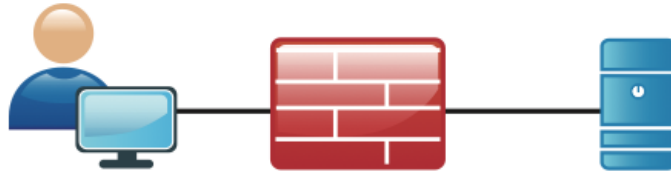


Let's all traffic pass by default

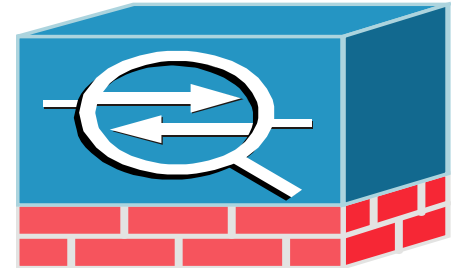
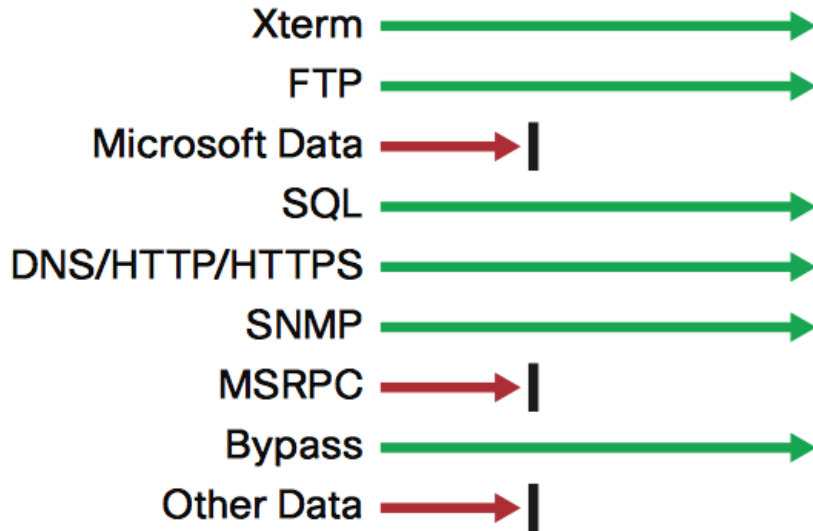
Complete your session evaluations online at www.SHARE.org/Seattle-Eval

FW – Firewall

White List



Denies all traffic by default except what is explicitly configured to be let through.



Creates more hassle for application deployment – all protocol/packet types must be enumerated in the change request

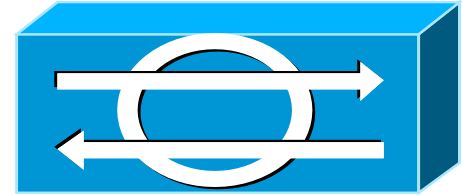
IPS – Intrusion Prevention System



Combination of IDS (Intrusion Detection System) and Firewall or Router.

IDS component monitors traffic and looks for anomalous or malicious traffic.

Logs information about the suspicious traffic and tries to prevent it with access-list or firewall rule dynamically.



Complete your session evaluations online at www.SHARE.org/Seattle-Eval



DDoS Traffic Scrubber

- Distributed Denial of Service (DDoS) traffic scrubbers help identify and divert suspicious traffic for further processing and cleansing
- Some versions divert and scrub traffic locally
- Other versions divert traffic to processing centers which scrub the traffic and return the clean traffic back to the data center. Usually performed with DNS diversion
- Example is Arbor's Prevail appliance and Arbor Cloud service



Complete your session evaluations online at www.SHARE.org/Seattle-Eval



ACLs - Access Control Lists



- Router feature to allow/block traffic on a per port basis
- First line of defense for routers
- Usually applied on User/Host/Edge facing ports
- Like Firewall rules, consist of individual configuration lines which are applied in order
- Can mix and match permitting some traffic while denying other traffic
- On most platforms performed by ASICs rather than the route processor (RP)



Complete your session evaluations online at www.SHARE.org/Seattle-Eval



User Credentials



- Access to network devices is protected with userid/password combination
- Uses TACACS or RADIUS protocol to communicate with a credentials server
- Access is usually via Telnet (weak) or SSH (strong)

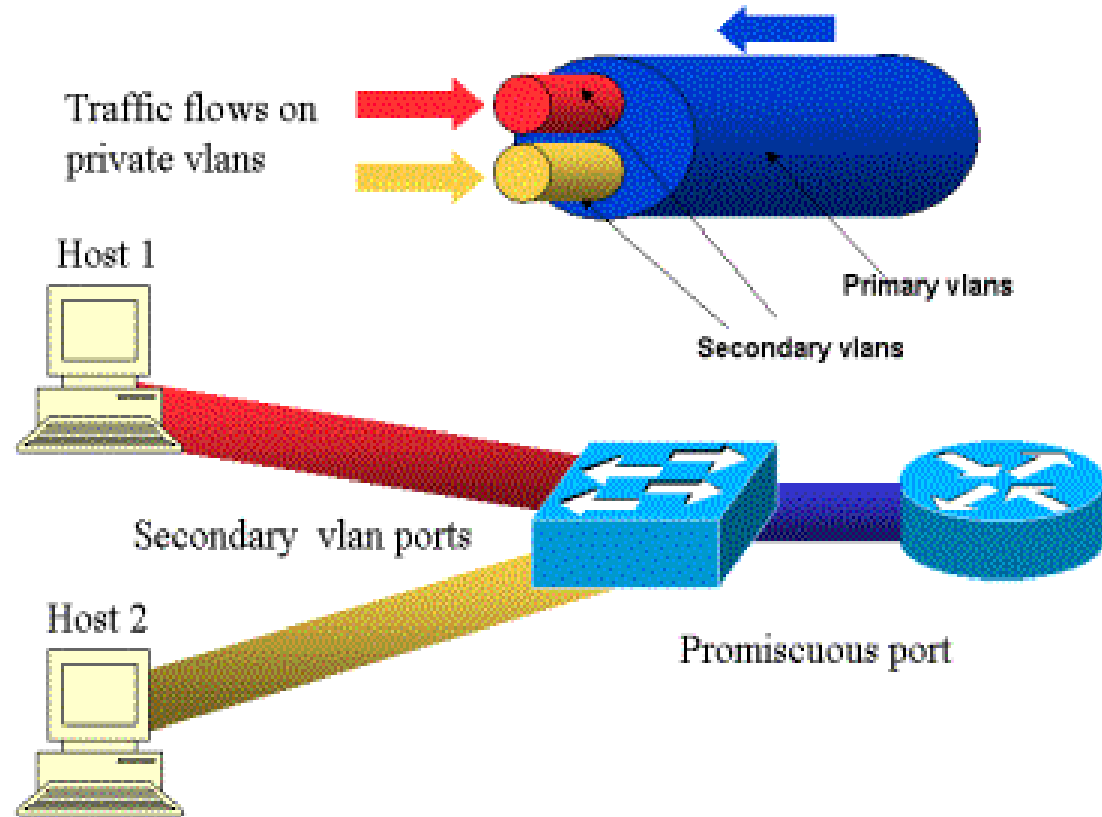


Complete your session evaluations online at www.SHARE.org/Seattle-Eval



Private VLANs

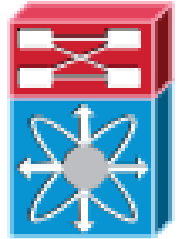
- Mechanism to provide isolation
- Cisco feature originally but open standard
- Different port types: Promiscuous, Isolated, Community



SPAN / rSPAN / Port Mirroring



- Used to copy packets from a port, set of ports, or VLAN on a network device
- Sends the traffic out a port (SPAN) or tunnels it (rSPAN)
- While used predominantly for sending copies of traffic to network Sniffers for troubleshooting, also used to send traffic to security monitoring and telemetry appliances and applications for DPI (Deep Packet Inspection)



NetFlow/JFlow



- Used to send information about traffic flows through the network.
- Basically collects information about source/destination traffic flows and packet counts

Date flow start	Duration	Proto	Src IP Addr:Port	Dst IP Addr:Port	Packets	Bytes	Flows
2010-09-01 00:00:00.459	0.000	UDP	127.0.0.1:24920	-> 192.168.0.1:22126	1	46	1
2010-09-01 00:00:00.363	0.000	UDP	192.168.0.1:22126	-> 127.0.0.1:24920	1	80	1



Other vendor
flow protocols:

Jflow / cflowd
NetStream
NetStream
Cflowd
Rflow
AppFlow
sFlow

Juniper
3Com/HP
Huawei
Alcatel-Lucent
Erricsson
Citrix
[multiple]

Complete your session evaluations online at www.SHARE.org/Seattle-Eval



Anti-spoofing/Unicast Reverse Path Forwarding



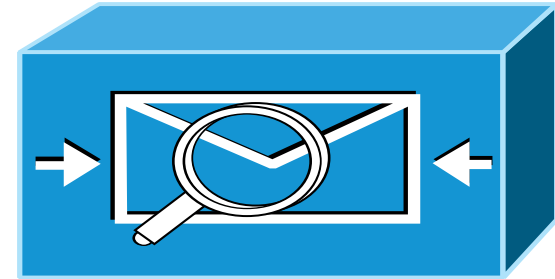
- Port check to ensure that users are who they say they are.
- Example: User is assigned an address in the 1.1.1.0/24 subnet but sends a Smurf attack to user 2.2.2.76 on subnet 2.2.2.0/24 using a source address of 2.2.2.111.
- When the first hop router receives the packet it checks to see that the source address of the packet is in the same subnet as assigned to the interface.
- If it doesn't match the packet is discarded.
- (note: this could be done using an access list but is easier to administrate – don't have to change if the subnet changes.

Complete your session evaluations online at www.SHARE.org/Seattle-Eval



ESA – Email Security Appliance

- Intercepts email and inspects it against attacks such as phishing, Spam, malware, embedded links, etc.
- Handles encrypting of outbound email



Complete your session evaluations online at www.SHARE.org/Seattle-Eval



Cloud Challenges

Complete your session evaluations online at www.SHARE.org/Seattle-Eval

Segmentation

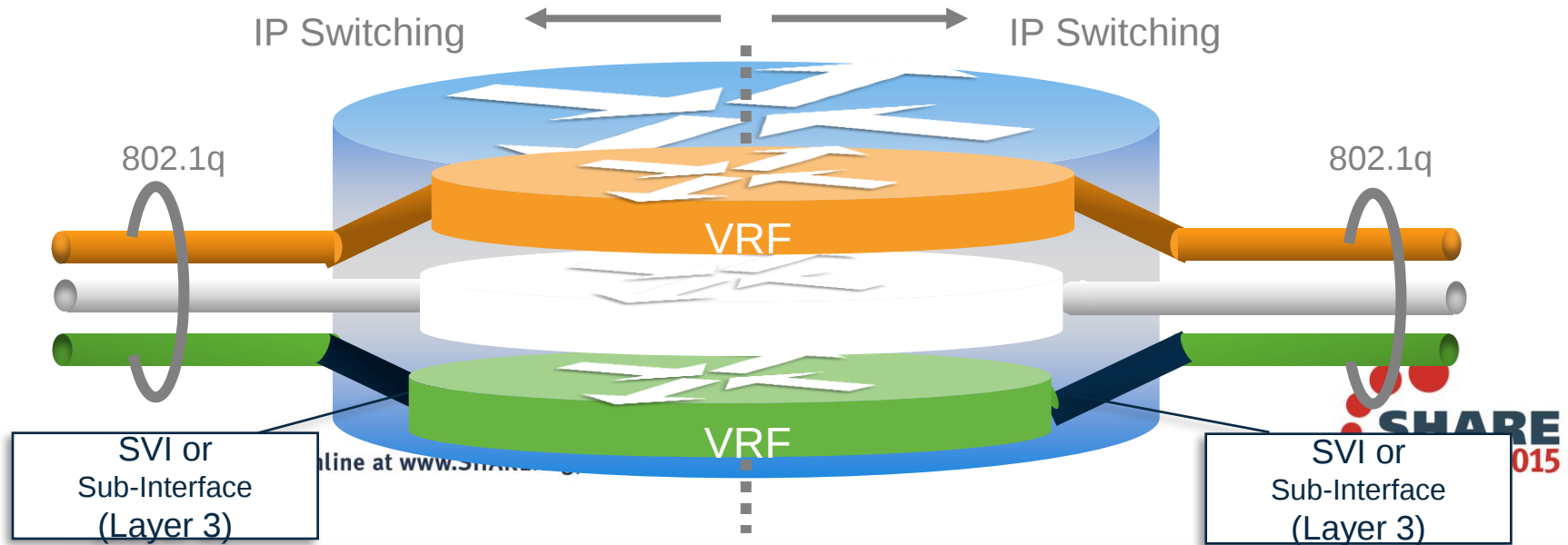
- Per-Tenant Isolation
 - *VRF-lite (virtual routing and forwarding) at aggregation layers provides per-tenant isolation at L3*
- Server-to-Server Traffic Denied By Default
 - *Separate dedicated per-tenant routing and forwarding tables ensure that all inter-tenant traffic within the data center is prohibited, unless explicitly allowed*
- Tagging provides ID-Based Segmentations
 - *VLAN IDs and the 802.1q tag provide isolation and identification of tenant traffic across the L2 domain*
- Segmentation for Compute, Storage, and Applications
 - *Compute Separation (vNICs, VLANs, Port Profiles)*
 - *Storage Separation (VSAN, LUN Masking)*
 - *Application Tier (Network Centric, Logical, and Physical segmentation with L2/L3 firewalling and security zoning)*

Complete your session evaluations online at www.SHARE.org/Seattle-Eval



WAN Edge – Core VRF's

VRF allows multiple instances of a routing table to co-exists within the same router. Due to the fact that routing instances are independent, they play a very crucial role in end-to-end separation of tenant traffic flows in a multi-tenant environment.



Virtual Extensible Local Area Network (VXLAN)



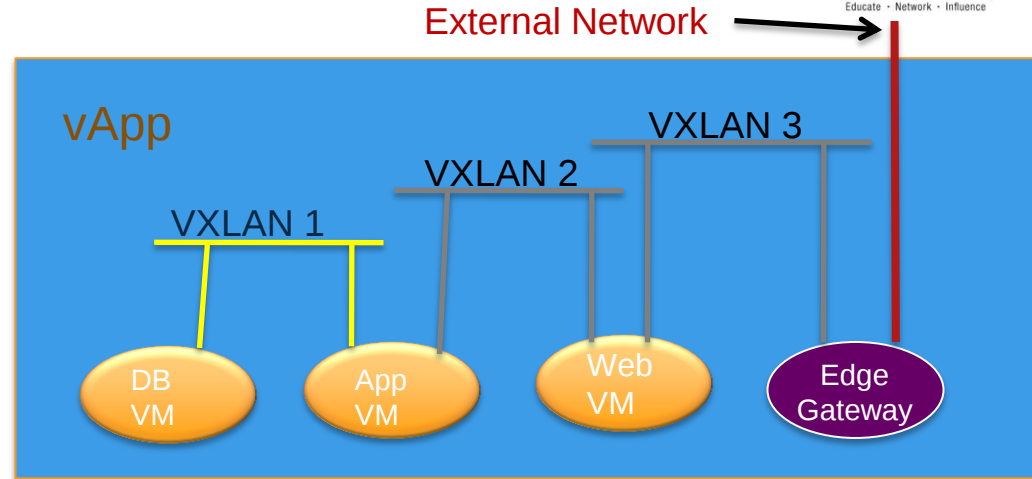
Offers virtual separation

Currently an IETF draft submitted by Cisco, VMware, Citrix, Broadcom and others

IP Multicast used for L2 broadcast/multicast

Can cross Layer 3

- Ethernet in IP Overlay
L2 frame encapsulated in UDP → 50 bytes overhead
- Uses 24bit VXLAN identified → 16M Logical networks



Outer MAC DA	Outer MAC SA	Outer 802.1Q	Outer IP DA	Outer IP SA	Outer UDP	VXLAN ID (24 bits)	Inner MAC DA	InnerM AC SA	Optional Inner 802.1Q	Original Ethernet Payload	CRC
--------------------	--------------------	-----------------	----------------	----------------	--------------	-----------------------	--------------------	--------------------	-----------------------------	---------------------------------	-----



session evaluations online at www.SHARE.org/Seattle-Eval



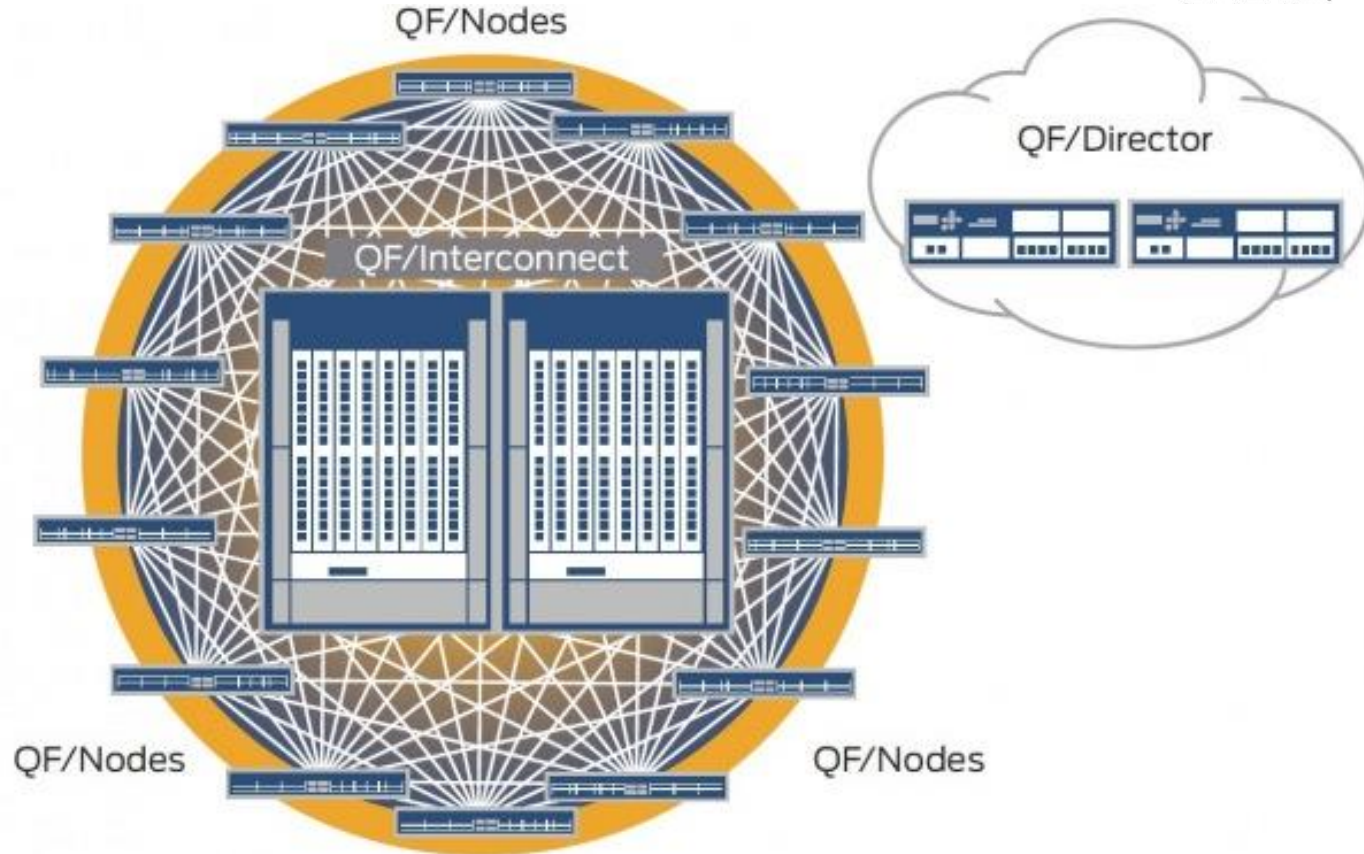
QFabric



Juniper's solution to linking devices together in a data center

Flattens out the network – makes everything a single tier

Used in IBM's Cloud



session evaluations online

Virtualization Challenges

Complete your session evaluations online at www.SHARE.org/Seattle-Eval

Question



What do all the network security devices listed above need to have in order to work?

Complete your session evaluations online at www.SHARE.org/Seattle-Eval



Answer



Traffic coming into the device
Visibility into what's going on

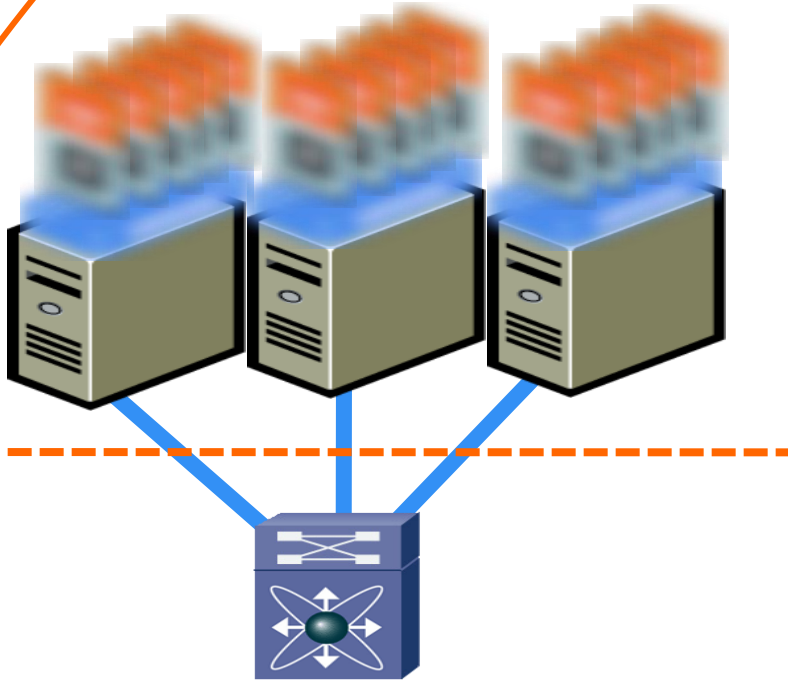
(yes, and power and connectivity....)

Complete your session evaluations online at www.SHARE.org/Seattle-Eval



Virtualized Devices

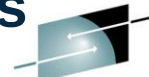
Boundary of network visibility



- No visibility to individual traffic from each VM
- Unable to troubleshoot, apply policy, or address performance issues

session evaluations online at www.SHARE.org/Seattle-Eval

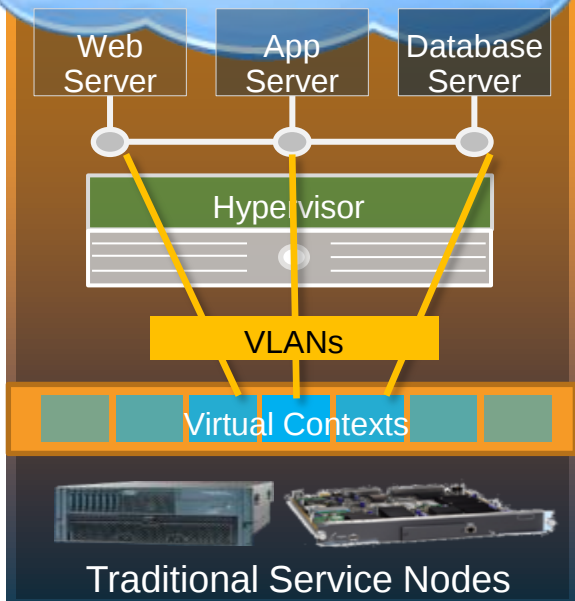
Two Solutions for Visibility and Policy on Virtualized Servers



SHARE
Educate • Network • Influence

1

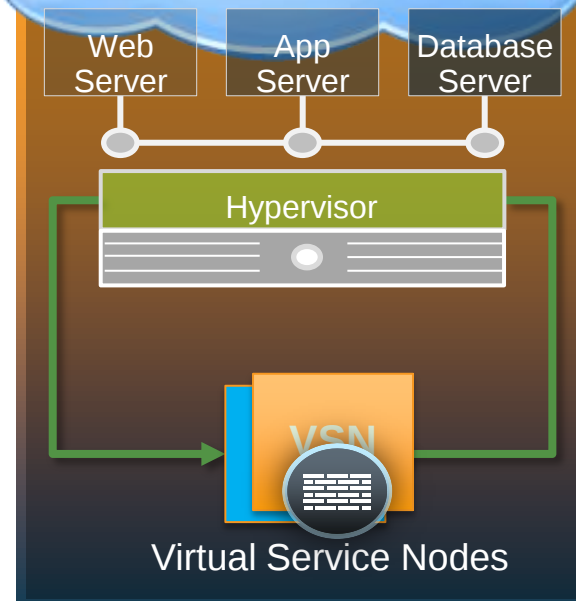
Redirect VM traffic via VLANs to external (physical) appliances



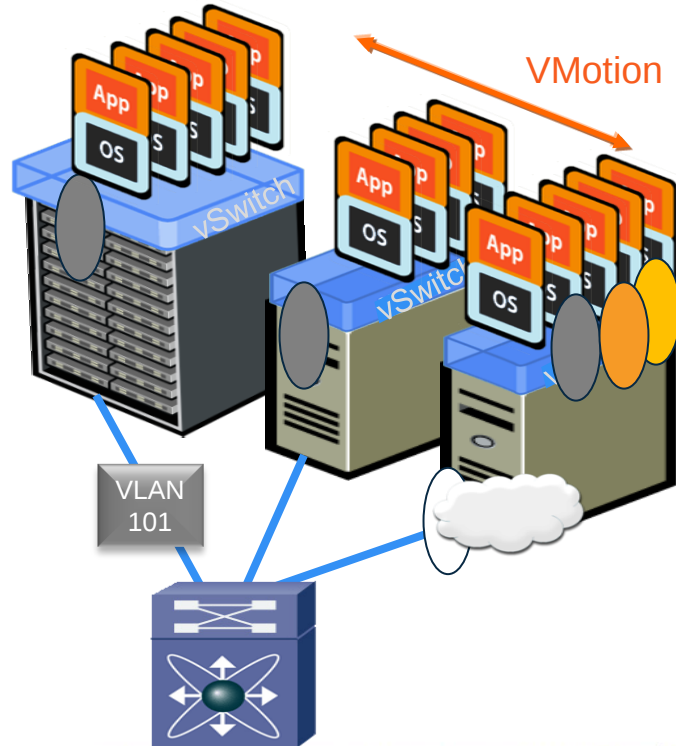
g/Seattle-Eval

2

Apply hypervisor-based network services



VMotion and locally switched traffic



session evaluations online at www.SHARE.org/Seattle-Eval

Problems:

- VMotion may move VMs across physical ports—policy must follow
- Impossible to view or apply policy to locally switched traffic
- Cannot correlate traffic on physical links—from multiple VMs
- Three solutions:
 - Virtual ports and VLAN's
 - VXLAN
 - VN-TAG and vPath

Cloud Security Standards and Compliance

Complete your session evaluations online at www.SHARE.org/Seattle-Eval

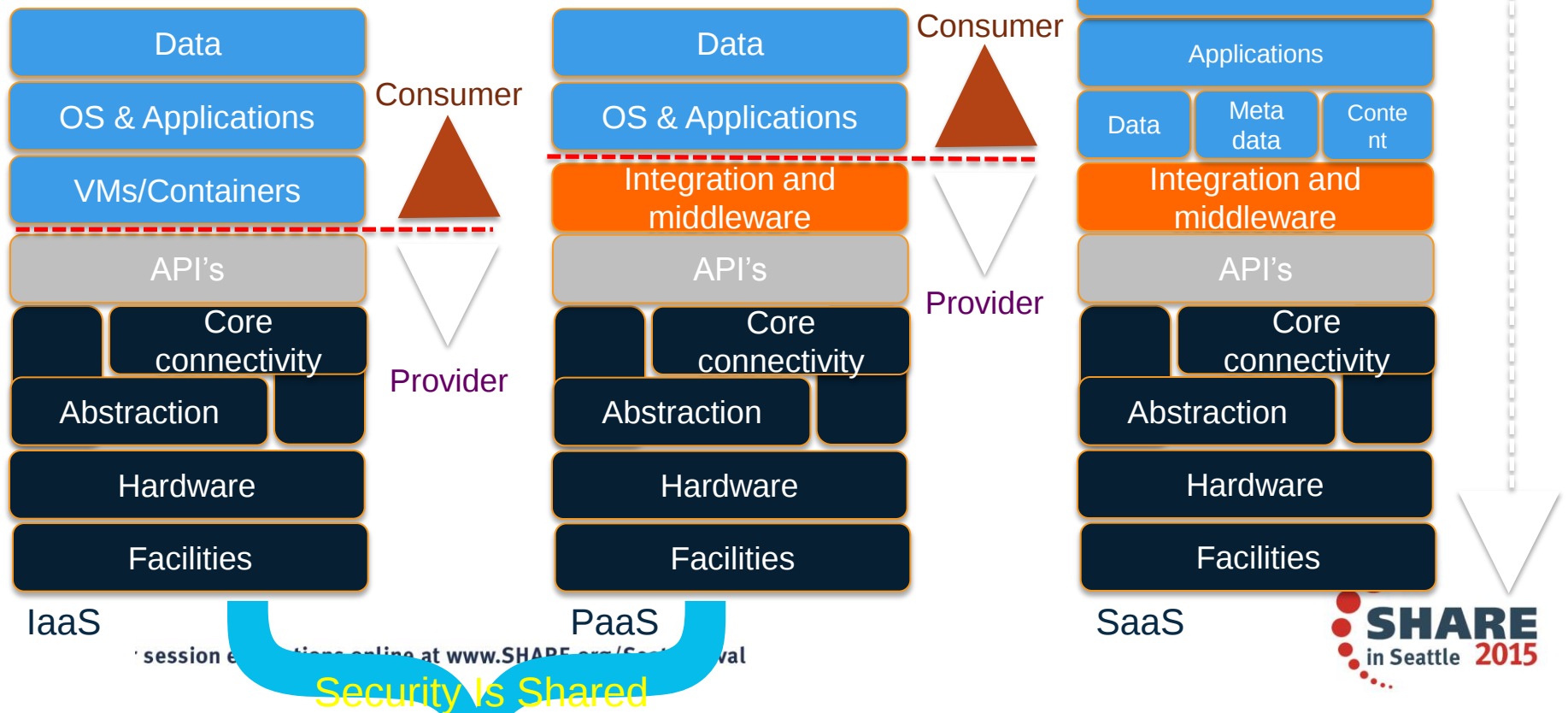
Control Ownership Clarity



SERVICE OWNER	SaaS	PaaS	IaaS
Data	Joint	Tenant	Tenant
Application	Joint	Joint	Tenant
Compute	Provider	Joint	Tenant
Storage	Provider	Provider	Joint
Network	Provider	Provider	Joint
Physical	Provider	Provider	Provider

*Controls represent the **common language** of information security and regulatory compliance between supplier and customer.*

Ownership Accountability



Compliance is NOT Security



- Compliance is currently one of the biggest drivers of security activity
- Compliance, however, does not equal effective security
- Many “compliant” organizations have experienced significant outages, compromises, and losses
- Even without incidents, compliance efforts can result in lost productivity and money
 - Redundant silos of compliance may exist within an organization
 - Compliance activities may be inefficient and poorly aligned or coordinated

Security = Compliance

Complete your ses:



Industry Standard Regulatory Compliance Guidance



There are different regulatory compliance laws for different market verticals:

- PCI DSS – For credit card data and processors
- HIPAA and related privacy laws – For health care segment
- FISMA and related government regulations – For government agencies and their service providers



Complete your session evaluations online at www.SHARE.org/Seattle-Eval



Cloud Security Alliance – Cloud Controls Matrix



CCM v3.0.1 DOMAINS

- AIS** Application & Interface Security
- AAC** Audit Assurance & Compliance
- BCR** Business Continuity Mgmt & Op Resilience
- CCC** Change Control & Configuration Management
- DSI** Data Security & Information Lifecycle Mgmt
- DSC** Datacenter Security
- EKM** Encryption & Key Management
- GRM** Governance & Risk Management

136 CONTROLS
Cloud Controls Matrix v3.0



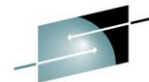
- HRS** Human Resources Security
- IAM** Identity & Access Management
- IVS** Infrastructure & Virtualization
- IPY** Interoperability & Portability
- MOS** Mobile Security
- SEF** Sec. Incident Mgmt, E-Disc & Cloud Forensics
- STA** Supply Chain Mgmt, Transparency & Accountability
- TVM** Threat & Vulnerability Management

133 CONTROLS
Cloud Controls Matrix v3.0.1

Complete your session evaluations online at www.SHARE.org/Seattle-Eval



Cloud Security Alliance – Cloud Controls Matrix



New or updated mappings to the following

- + AICPA 2014 Trust Services Criteria
- + Canada PIPEDA (Personal Information Protection Electronic Documents Act)
- + COBIT 5.0
- + COPPA (Children's Online Privacy Protection Act)
- + CSA Enterprise Architecture
- + ENISA (European Network Information and Security Agency) Information Assurance Framework
- + European Union Data Protection Directive 95/36/EC
- + FERPA (Family Education and Rights Privacy Act)
- + HIPAA/HITECH act and the Omnibus Rule
- + ISO/IEC 27001:2013
- + ITAR (International Traffic in Arms Regulation)
- + Mexico - Federal Law on Protection of Personal Data Held by Private Parties
- + NIST SP800-53 Rev 3 Appendix J
- + NZISM (New Zealand Information Security Manual)
- + ODCA (Open Data Center Alliance) Usage Model PAAS Interoperability Rev. 2.0
- + PCI DSS v3

Consolidation of redundant controls

Rewritten controls for clarity of intent, STAR enablement, and SDO alignment

Thank you! Stay Secure

Complete your session evaluations online at www.SHARE.org/Seattle-Eval