



# SECURING THE NEXT GENERATION DATA CENTER

Leslie K. Lambert  
Juniper Networks  
VP & Chief Information Security Officer  
July 18, 2011



# JUNIPER SECURITY LEADERSHIP

## Market Leadership

- Data Center with High-End Firewall **#1** at 48%
- Secure Mobility with SSL VPN **#1** at 28%
- Intelligent Networking with Secure Routing **#2** at 22%

## Security Innovation

- Across device, network, application & virtual machine
- One Junos for Routing, Switching and Security
- Security and Mobile Threat Research Teams

## Proven Reach and Scale

- 24 of the Fortune 25 for secure connectivity
- Protecting 76% of smartphones worldwide
- GTM Scale with IBM, Dell, Ericsson & NSN

# THREE DRAMATIC CHANGES IN THE DATA CENTER PROVIDE SIGNIFICANT SECURITY OPPORTUNITIES

**53%**

Of companies have data center expansion and or consolidation projects planned in the next few years

**80%**

Of Enterprises have a virtualization program in place

**75%**

Of data center traffic will shift from client-server to server – server, growing from just 5% today

## **Mega Consolidation**

Efficiency improvements and simplified administration

## **Virtualization**

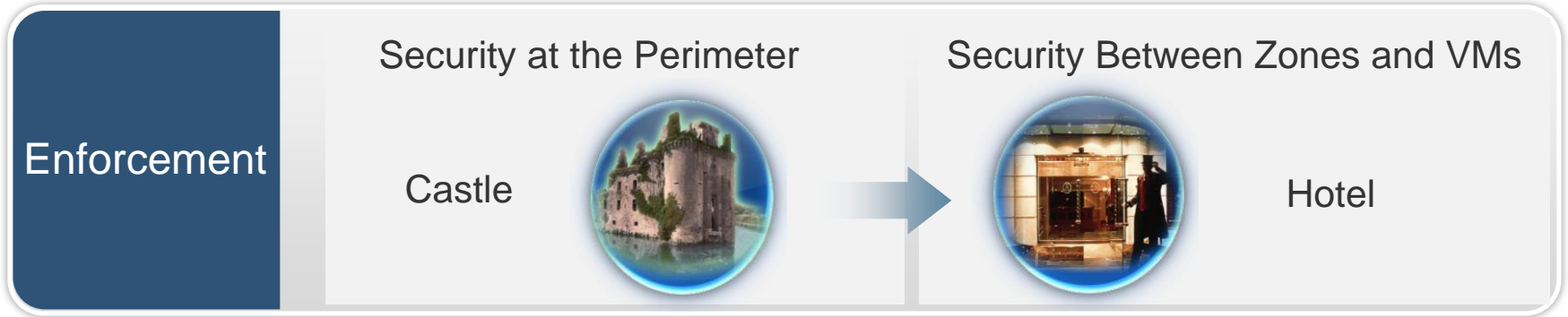
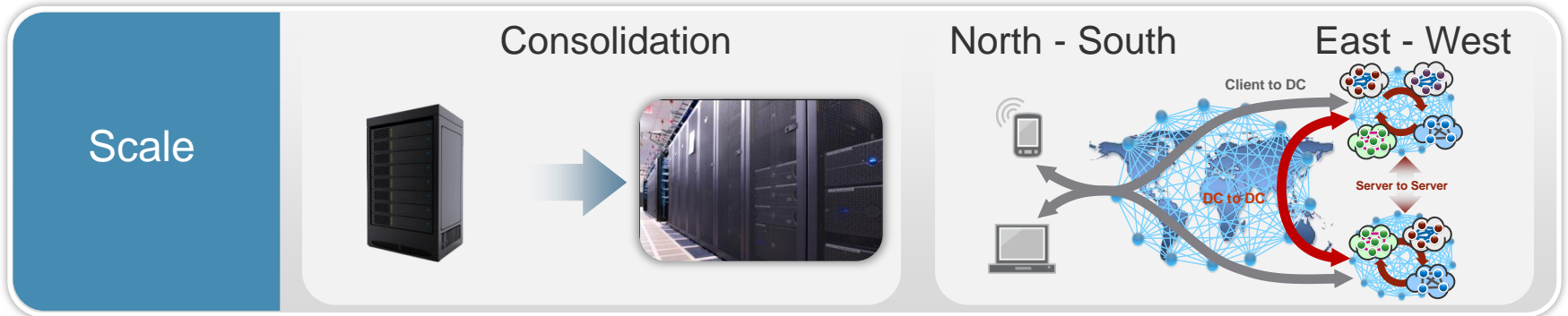
Cloud Services & Virtualization projects

## **Service Oriented Architectures**

Web 2.0 and Application Mashups

Sources: AFCOM Data Center Research, Gartner, KRC Research -

# DATA CENTER PARADIGM SHIFT



# KEY ISSUES FOR NEXT GEN DATA CENTER SECURITY





# DATA CENTER SCALE CONCERNS

## Customer Concerns



Scaling with data center growth



More efficient infrastructure



Dynamic VM security



Protecting online assets





# DATA CENTER SECURITY AT SCALE

## Data Center Solutions that Scale

Handling massive amounts of traffic as bandwidth continues to trend up with the SRX Services Gateway

Supporting multiple services in a single SRX system with the ability to run services concurrently

Best in class performance for VM to VM security with Altor acquisition and integration

Only company to offer coordinated security across physical and virtual environments

## Relevant Data Center Technologies



**SRX Security Service Gateways**



**AppSecure Software**





# VISIBILITY AND CONTEXT CONCERNS

## Customer Concerns



Visibility into Web 2.0 threats



Control of application usage



Secure mobile user access



Scalable policy enforcement & management







# VISIBILITY FOR BETTER SECURITY

## Data Center Visibility

Visibility and control for data center application usage with AppSecure

Identifying User ID and location with Unified Access Control

Security insight for application borne web 2.0 threats

Control over generation of new VM images with Altor

Integrated policy management with Junos Space Security Design Application

## Relevant Data Center Technologies



AppSecure Software



Unified  
Access  
Control

ALTOR  
A Juniper Networks Company



SRX Security  
Service  
Gateways





# ENFORCEMENT CONCERNS

## Customer Concerns



Control of VM to VM traffic



Maintain Security Compliance



Ability to securely move workloads between servers



Manage physical and virtual security domains



# ENFORCING SECURITY POLICIES IN VIRTUAL AND PHYSICAL ENVIRONMENTS



## Data Center Enforcement Solutions

Uniform policy management for physical and virtual environments

Policies that can move with the VM, regardless of the physical server

Simplified policy management with Junos Space Security Design Application

Enforcement at the device, network, virtual machine and application

## Relevant Data Center Technologies



**SRX Security  
Service Gateways**



**AppSecure Software**



# DATA CENTER SECURITY PORTFOLIO



Junos Space Platform for Automation and Innovation

## SRX Services Gateways



## Integrated Security Services



## Virtual Machine Security

**ALTOR**  
A Juniper Networks Company

STRM Threat Detection and Log Management

# ADDRESSING THE EVOLVING THREAT LANDSCAPE

## Customer Priorities



Visibility into web 2.0 threats



Control of application usage



Rapid response to new threats



Scalable policy enforcement & management



## Juniper Security Solutions



AppSecure Software



SRX Security  
Service  
Gateways



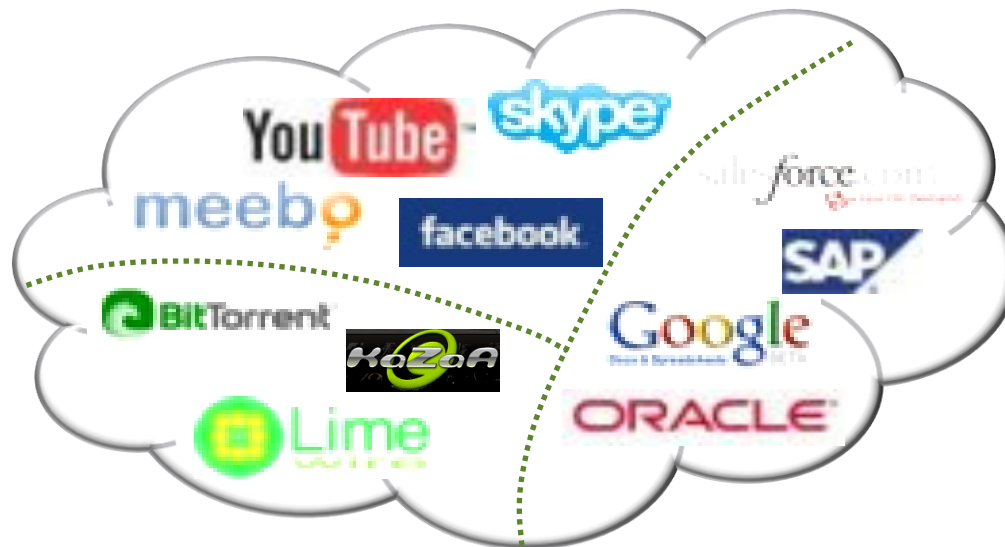
Copyright © 2011 Juniper Networks, Inc. [www.juniper.net](http://www.juniper.net)



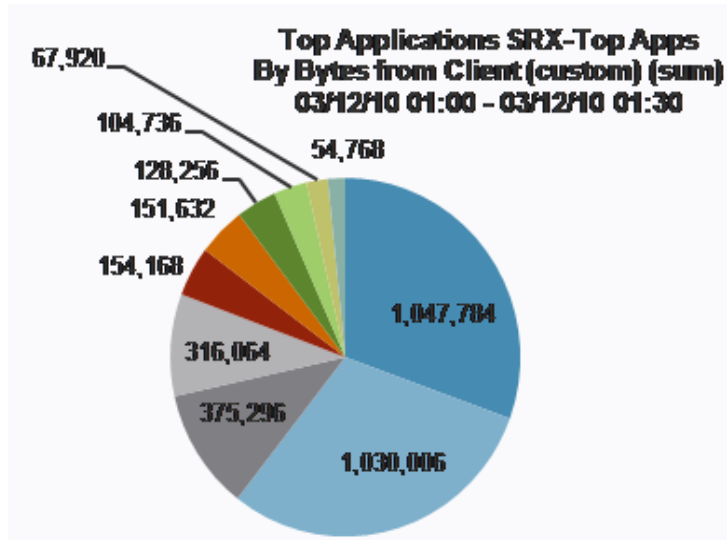
Security Research Teams

# APPSECURE: APPLICATION VISIBILITY AND ENFORCEMENT

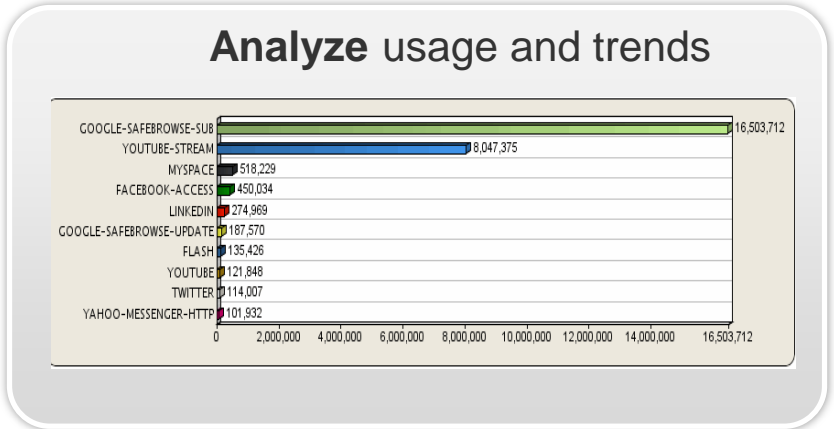
Juniper's AppSecure solution uses a combination of Application Signatures and Protocol Decoders to accurately identify 700+ Applications



# APPTRACK: APPLICATION VISIBILITY FOR INFORMED RISK ANALYSIS



**View** application by protocol, Web application, and utilization



Web 2.0 application visibility



App usage monitoring

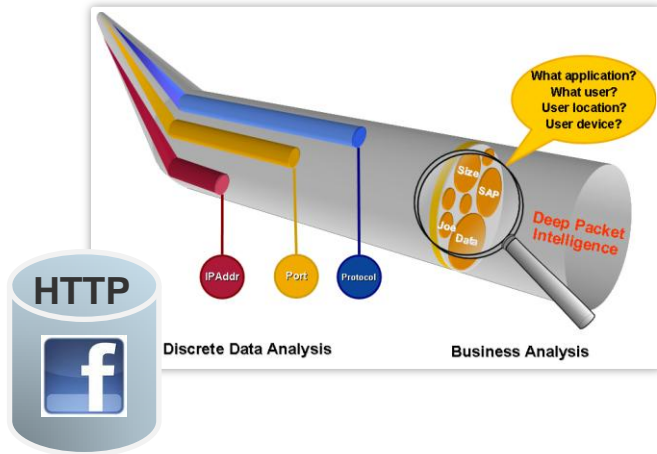


Scalable, flexible logging & reporting

**Customize** application monitoring

**Log and report** across security solutions and systems

# APPLICATION FIREWALL: BEYOND JUST FW OR APP CONTROL



## Control & Enforce Web 2.0 Apps


**Inspect** ports *and* protocols


**Uncover** tunneled apps


**Stop** multiple threat types

**Control** nested apps, chat, file sharing and other Web 2.0 activities

From Zone	To Zone	Name	Source Address	Destinatio...	Application	Dynamic...	Action	NW Servi...	Log/Count
AppPC	LAN	Allow-HTTP-Special	any	any	junos-http	FACEBOOK	permit	EP	None
					Any		deny	None	
AppPC	LAN	Block-SSH-Nonstandard	any	any	SSH	Any	deny	EP	None
					Any		permit	None	

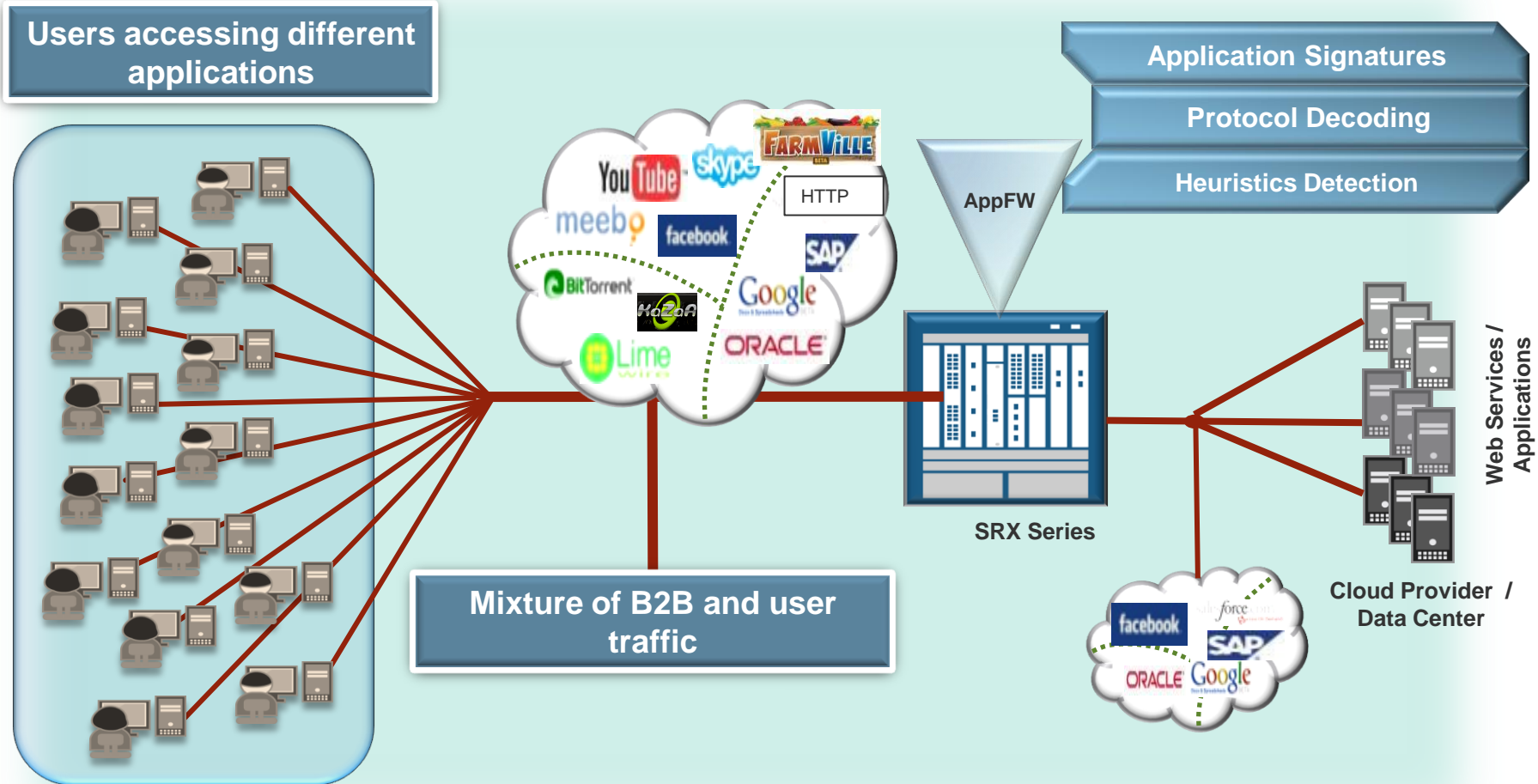
 Dynamic application security

 Web 2.0 policy enforcement

 Threat detection & prevention



# APPFW DEMO



# SECURING DATA CENTERS - BOTNET & DOS THREAT MITIGATION WITH APPDDOS



Botnet detection & remediation



DoS monitoring & remediation



On-going anomaly detection

Protect Valuable On-line Business

**Detect and mitigate** botnet activity

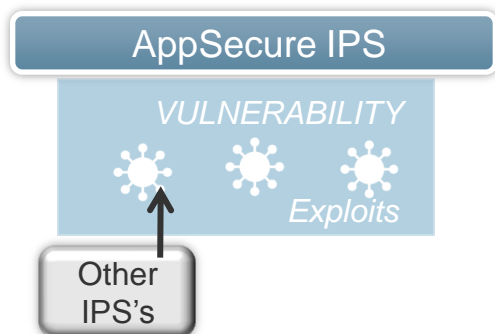
**Uncover** misuse of routine Web functionality

**Adapt** security policy and QOS based on insights



**Benchmark** “normal” behavior to detect anomalies

# PROVIDING DEEP PACKET INSPECTION -- IPS



On-going threat protection



Mobile traffic monitoring



Custom attack mitigation

## Monitor & Mitigate Custom Attacks

**Detect and monitor** suspicious behavior

**Tune** open signatures to detect and mitigate tailored attacks



**Uncover** attacks exploiting encrypted methods



**Address vulnerabilities** instead of ever-changing *exploits* of the vulnerability



# APPSECURE SUMMARY



## 5 principles for delivering application security:

1. Protection at all points – user, network, applications
2. Scalable - application protection up to 100G performance
3. Application specific protection with comprehensive signatures
4. Tight integration with highly available, proven HW/OS infrastructure
5. Simplicity and scale for administration and management

# HIGHEST PERFORMING SECURITY PLATFORM

- SRX: The Integrated Services Platform of the future
- World's fastest Application Firewall – Up to 100G performance
- World's fastest Intrusion Prevention System

## SRX Series



150G firewall  
performance

100G  
Application firewall  
performance

30G IPS  
performance

4M concurrent  
sessions

---

# SECURING CLOUDS

## THE MARKET DYNAMICS

---

50% of the world's workloads will be virtualized by 2012

*-Gartner*

Virtualization is near de-facto architecture for clouds

*-GigaOM*

Security is a top concern for virtualization adoption

*– CDW Survey*

37% of large enterprises expect to adopt IaaS (cloud) in the next year

*-Yankee Group*



---

# VIRTUALIZATION SPECIFIC REQUIREMENTS

---

## Secure VMotion/Live-Migration

- VMs may migrate to a unsecured or lower trust-level zone
- Security should enable both migration and enforcement

## Hypervisor Protection

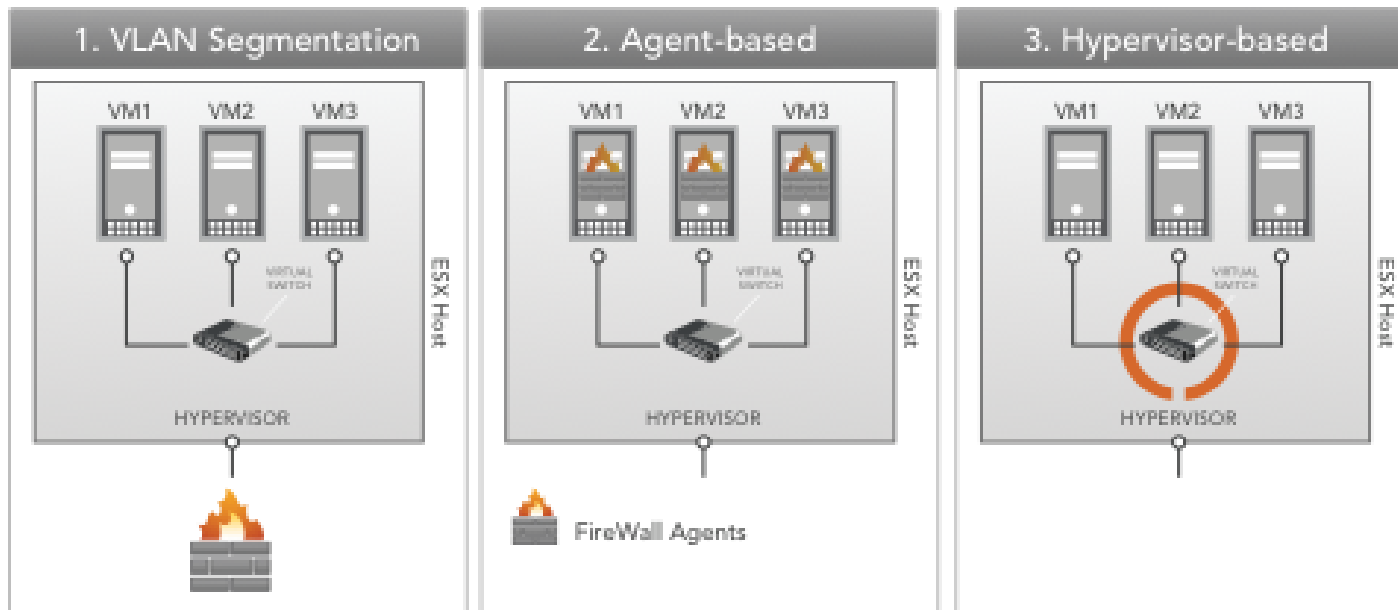
- New operating system means new attack surface
- Hypervisor connection attempts should be monitored

## Regulatory Compliance

- Isolating VMs, Access Control, Audit, etc.
- Segregating administrative duties inside the virtual network
- Tracking VM security profiles



# SECURING INTER-VM TRAFFIC



VLANs offer no granular security

Agents are very costly to manage at scale

In the hypervisor = maximum performance and security

# HYPERVISOR-BASED VS. VLANS

REQUIREMENT	Juniper vGW	VLANs
Security per Virtual Machine (VM)	✓	X
Integrated Intrusion Detection	✓	X
Hypervisor Protection	✓	X
Auditing of hypervisor access	✓	X
Monitoring of all inter VM traffic	✓	X
VM Introspection	✓	X

# VGW & THE HYPERVISOR-BASED ARCHITECTURE: CLOUD AND MULTI-TENANT READY

## Enterprise-grade

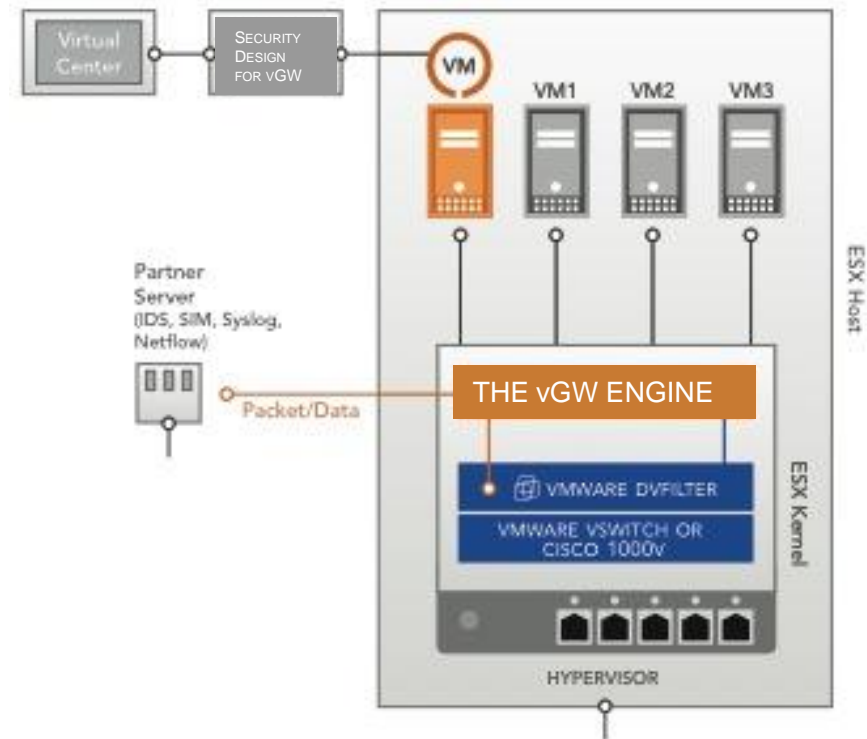
- VMware “VMsafe Certified”
- Protects each VM *and* the hypervisor
- Fault-tolerant architecture (i.e. HA)

## Purpose-built, Virtualization-aware

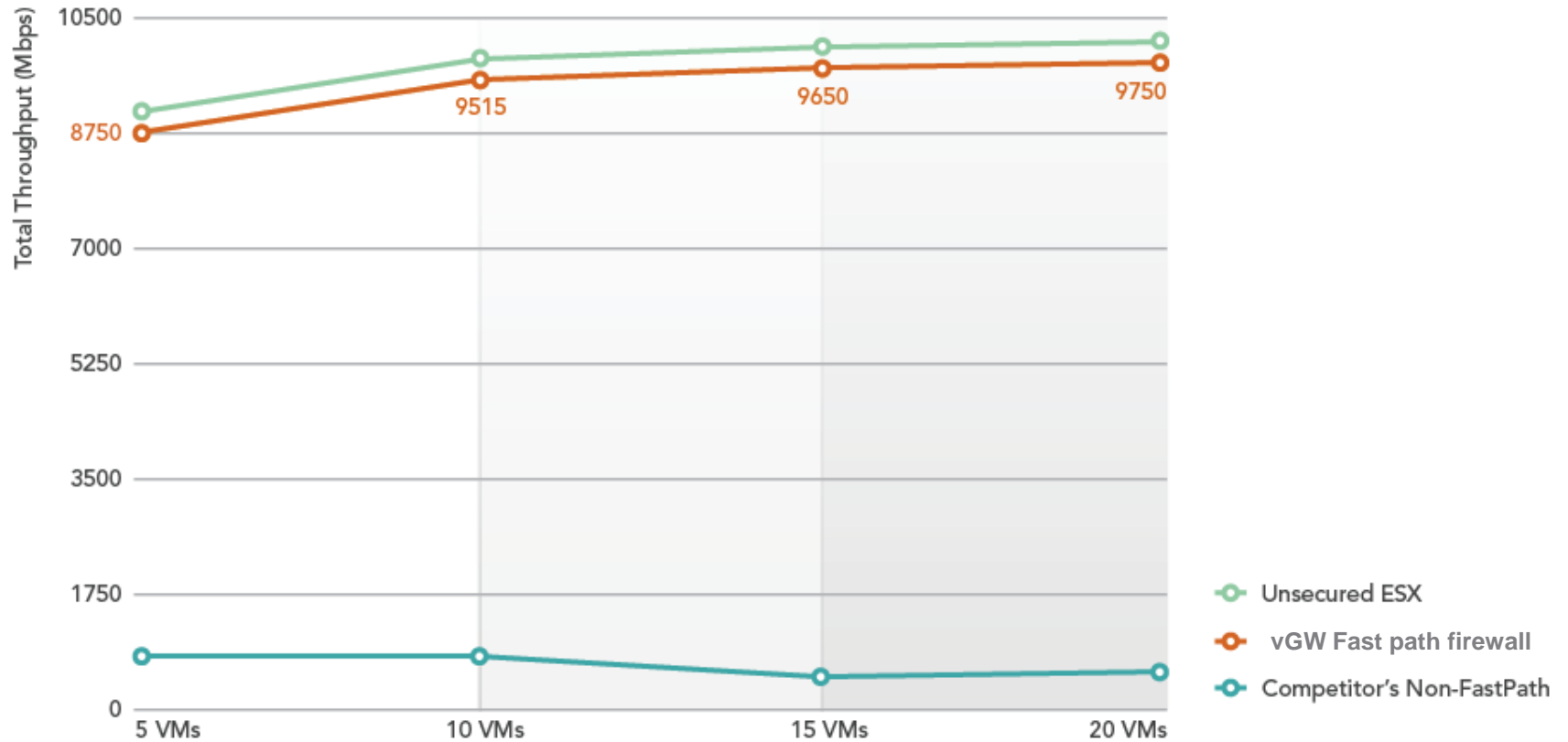
- “Secure VMotion” scales to 1,000+ ESX
- “Auto Secure” detects/protects new VMs

## Granular, Tiered Defense

- Stateful firewall and integrated IDS
- Flexible Policy Enforcement – Zone, VM group, VM, Application, Port, Protocol, Security state



# PERFORMANCE AND SCALABILITY



vGW secures ESX with only a 3% overhead

# INDUSTRY RECOGNITION OF VGW

## Distinction

- 1<sup>st</sup> Purpose-Built Virtual Firewall
- “VMsafe Certified” by VMware
- 5 Patents Pending



Most Innovative Company  
RSA® Conference 2010



# VGW – AUTOMATED VM PROTECTION

logged in as Juniper [logout](#)

Main Network Firewall **Introspection** Compliance Reports Settings

Please See Status Screen

**JUNIPER NETWORKS**

**All Machines** VM Introspection Dashboard Status

**HVX Status**

- vCenter Link Active
- 1 HVX Security VMs Deployed
- 14 Secured VMs
- 2 Unsecured VMs
- 6 Secured VMs with Default Policy

**Compliance Status for All Machines**

Compliance Assessment

**Top Talkers for All Machines**

Inter-VM Visibility

Machine	Protocols	Total (Bytes)	In (Kbps)	Out (Kbps)	Internal (Kbps)	Avg (Kbps)
DemoVC	19247/tcp, https, llmnr, netbios-ns, vmware-hb	13.8M	3	9	18	31
Juniper Security Design HVX	37116/tcp, 37117/tcp, altor-agent, dns, http, https, ntp	9.99M	1	5	16	22
192.168.9.130 (ESX)	https, vmware-hb	832K	0	0	2	2
192.168.9.131 (ESX)	https, igmp, netbios-ns, vmware-hb	538K	0	<.001	1	1

# AUTOMATION

- vf.app\_count\_bad
- vf.app\_count\_known
- vf.app\_count\_unknown
- vf.application
- vf.description
- vf.firewall
- vf.group
- vf.has\_installed\_group\_policy
- vf.has\_installed\_policy
- vf.hotfix
- vf.monitored
- vf.name
- vf.os
- vf.secured
- vf.tag
- vf.type
- vf.vmsafeconfig
- vi.attribute
- vi.cluster
- vi.datacenter
- vi.folder
- vi.host
- vi.ipv4
- vi.memory\_inspection
- vi.name
- vi.notes
- vi.numvnic
- vi.os
- vi.pg\_security.forgedtransmits
- vi.pg\_security.macchanges
- vi.pg\_security.promiscuous
- vi.portgroup
- vi.portgroup.all
- vi.powerstate
- vi.resourcepool
- vi.vapp
- vi.vlan
- vi.vlan.all
- vi.vmci\_enabled
- vi.vmsafe\_configured
- vi.vmsafe\_dvfilter
- vi.vmwaretools.running
- vi.vmwaretools.uptodate
- vi.vswitch

## Add Group

Name:

Advanced

Matches:  All  Any

<input type="text" value="vi.name"/>	<input type="text" value="Matches RegE"/>	<input type="text" value="^UserWorkstation.*"/>	-	+
<input type="text" value="vi.os"/>	<input type="text" value="Contains"/>	<input type="text" value="XP"/>	-	+
<input type="text" value="vf.application"/>	<input type="text" value="Contains"/>	<input type="text" value="McAfee"/>	-	+
<input type="text" value="vi.cluster"/>	<input type="text" value="Equals"/>	<input type="text" value="Production"/>	-	+

The following 3 machines will be included in group:  
UserWorkstation-1, UserWorkstation-2, and UserWorkstation-3

Group Policy Attributes:

Policy Group

Priority:

Apply Policy:  Automatic  Manual

Automatically  
classify VMs and  
assign them to the  
correct protection  
policy

# COMPLIANCE

**All Machines**

[Refresh Interval: 60s, Last Update: 19:10:22]

0% 20% 40% 60% 80% 100%

[Show Rules](#)

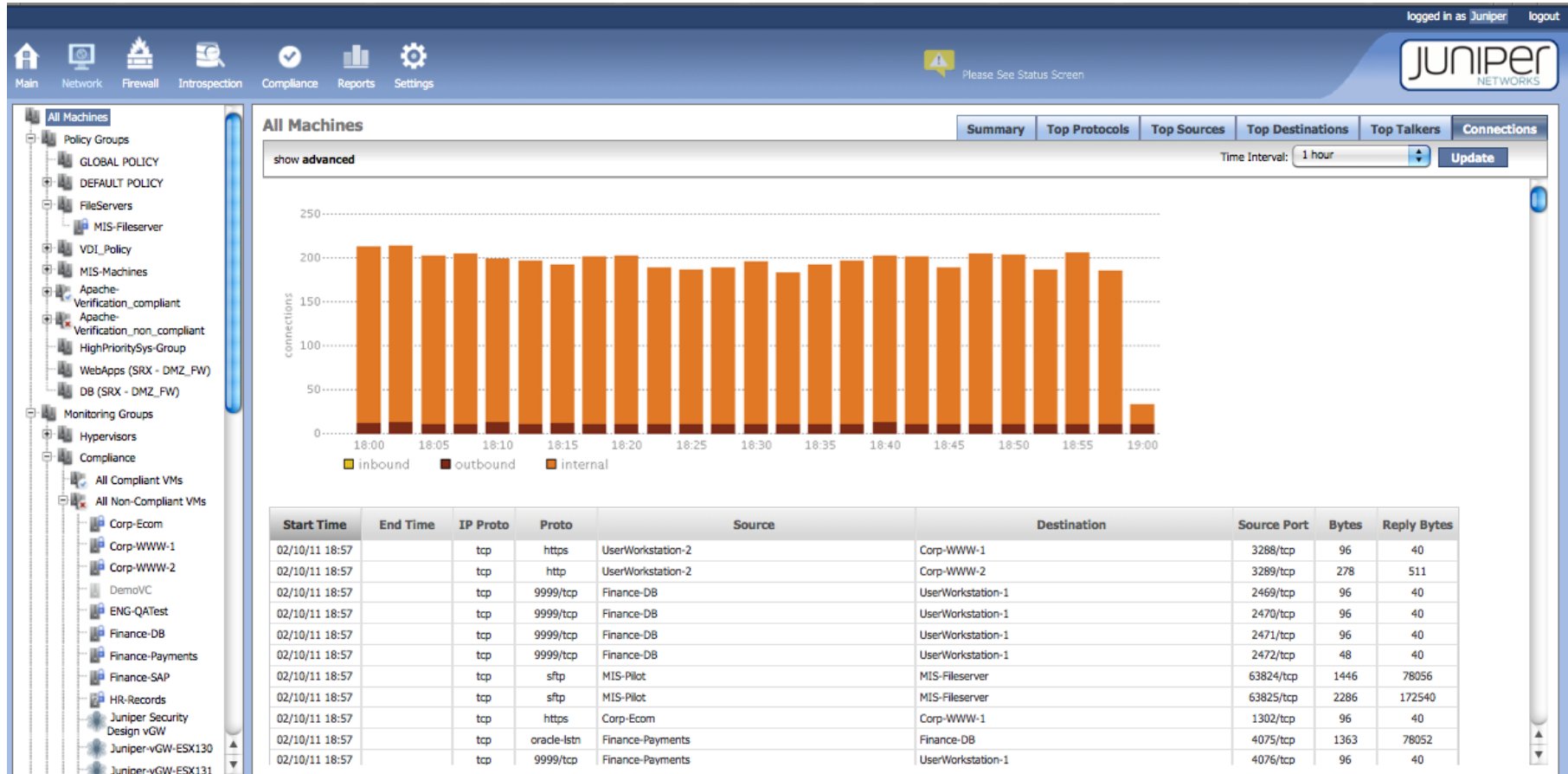
**Compliance Status of Selected VMs**

VM Name	Compliance Status	Rules
Filter: <input type="text"/>		
<a href="#">Corp-WWW-1</a>	64%	12
<a href="#">DemoVC</a>	72%	11
<a href="#">ENG-QATest</a>	72%	11
<a href="#">HR-Records</a>	72%	11
<a href="#">MIS-SDK</a>	72%	11

Be notified of any configuration and security state changes



# VISIBILITY – APPLICATIONS & USE



# VISIBILITY – VM INSPECTION

logged in as Juniper | logout

Main Network Firewall Introspection Compliance Reports Settings

Please See Status Screen

**JUNIPER NETWORKS**

**All Machines** Applications VMs Scan Status Scheduling

Data refers to 15 successfully scanned VMs out of 19.

**Operating Systems for All Machines**

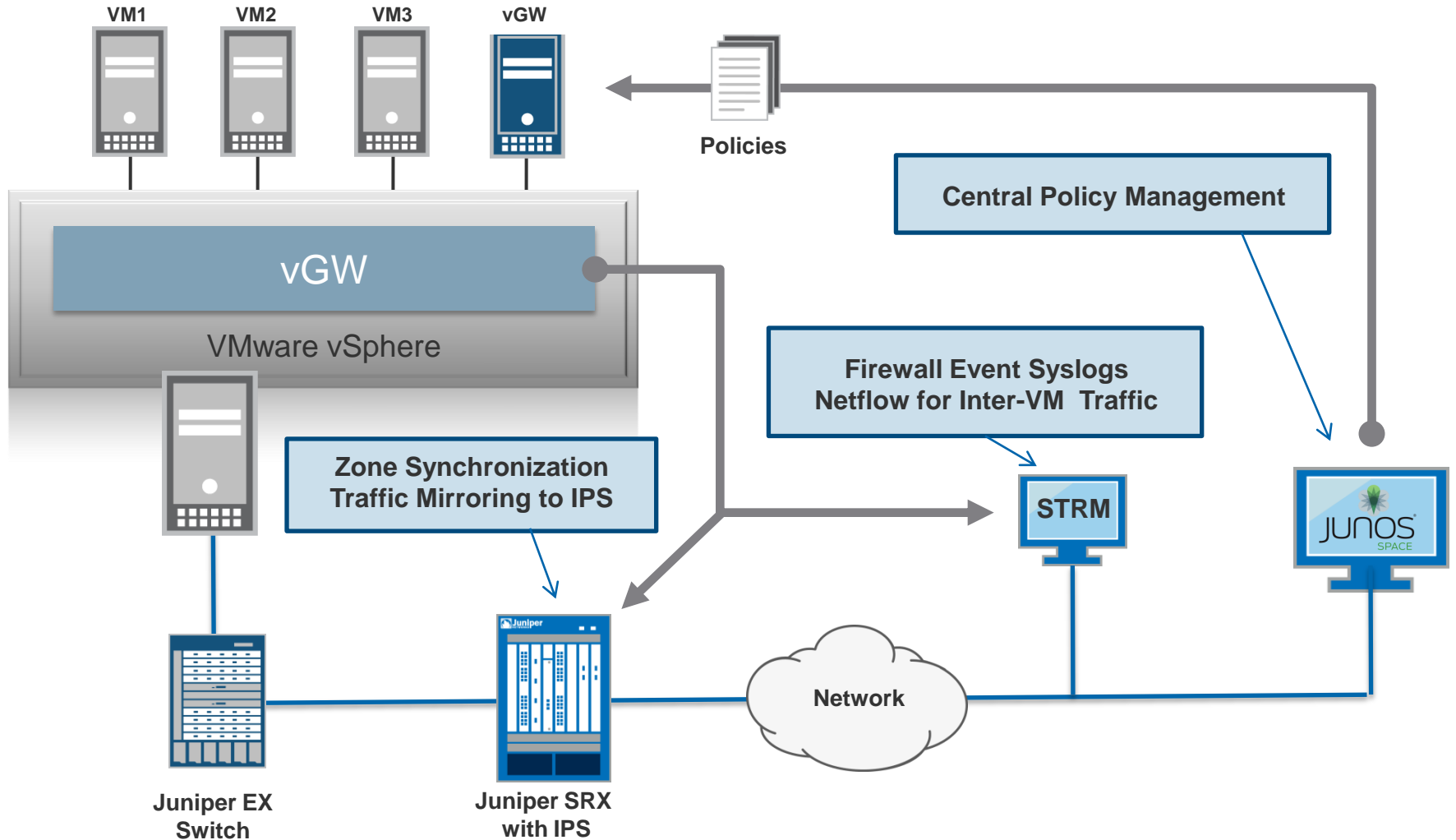
**Applications for All Machines**

**Applications**  Known  Unknown  Bad  Unclassified

Select	Class	Name	Version	Vendor	Install %
<input type="checkbox"/>	●	VMware Tools	8.3.2.1593	VMware, Inc.	93%
<input type="checkbox"/>	●	Strawberry Perl	5.12.1	Vanilla Perl Project	86%
<input type="checkbox"/>	●	WebFldrs XP	9.50.7523	Microsoft Corporation	20%
<input type="checkbox"/>	●	Kazaa File Sharing	3.2.7	Kazaa	13%
<input type="checkbox"/>	●	Microsoft .NET Framework 3.5 SP1		Microsoft Corporation	13%
<input type="checkbox"/>	●	Microsoft .NET Framework 3.5 SP1	3.5.30729	Microsoft Corporation	13%
<input type="checkbox"/>	●	WinSCP 4.2.7	4.2.7	Martin Prikyri	13%

**A searchable inventory of VM configurations**

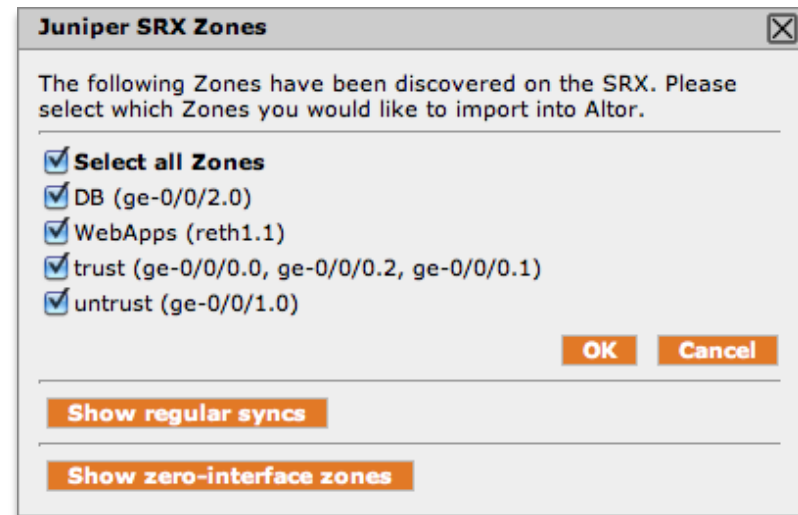
# INTEGRATED WITH JUNIPER DATA CENTER SECURITY



# SRX SERIES INTEGRATION

## Firewall Zones Integration

- Zone-Synchronization between SRX Series and vGW
- Benefits
  - Guarantee integrity of Zones on hypervisor
  - Automate and verify no “policy violation” of VMs
  - Empower SRX Series with VM awareness



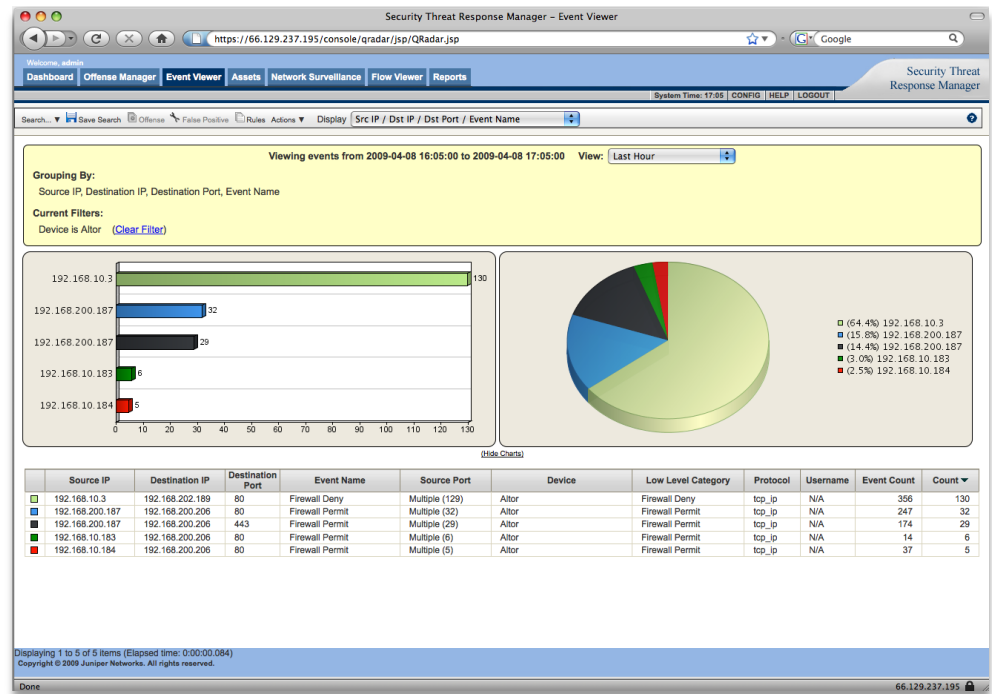
# STRM SERIES INTEGRATION

## Features

- Integrated physical and virtual compliance and threat management
- Consolidated logs and flow statistics

## Benefits

- Single-Pane of glass for the data center
- Increases ROI of STRM Series
- Fast and simple to configure



---

# SUMMARY

---

## vGW enables virtualization and clouds

- Hypervisor-based approach maximizes throughput & capacity
- Deep security experience results in administrative ease and scale
- Innovation makes enforcement granular and dynamic

## vGW as part of Juniper data center security

- Comprehensive protection for all workloads
- Extended security through several points of integration
- Part of a clear path to unified security administration

# SYRACUSE UNIVERSITY – PRIVATE CLOUD

## Deployment

Virtualized data center – Services to 22 departments  
Student data is hosted in the same infrastructure  
Security Infrastructure – Juniper FW, IDP, and STRM

## Challenge

Segregation in Multi-Tenant environment  
Trust-Level separation within departments  
Protect Sensitive Information

## Solution

vGW delivers guaranteed segregation of VMs  
vGW's Multi-tier Security Policy enables delegated administration  
STRM – Single-pane of glass for Threat Management





everywhere