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

* Source Infonetics Research 3Q10
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

Scale

Consolidation

North - South

East - West

Visibility

More information

Better Security Decisions

User ID
Application
Device
Location

Security at the Perimeter

Castle

Security Between Zones and VMs

Hotel
KEY ISSUES FOR NEXT GEN DATA CENTER SECURITY

- Enforcement
- Scale
- Visibility
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

Data Center Fabric
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**

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
- SRX Security Service Gateways
- Junos Space

Copyright © 2011 Juniper Networks, Inc.  www.juniper.net
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

Junos SPACE

Junos PULSE
DATA CENTER SECURITY PORTFOLIO

Junos Space Platform for Automation and Innovation

SRX Services
Gateways

Integrated
Security Services

Virtual Machine
Security

STRM Threat Detection and Log Management

SRX Services
Gateways

Integrated
Security Services

Virtual Machine
Security

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
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

Analyze usage and trends

Customize application monitoring

Log and report across security solutions and systems

Web 2.0 application visibility

App usage monitoring

Scalable, flexible logging & reporting
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

Dynamic application security

Web 2.0 policy enforcement

Threat detection & prevention
APPFW DEMO

Users accessing different applications

Mixture of B2B and user traffic

Application Signatures
Protocol Decoding
Heuristics Detection

Web Services / Applications

Cloud Provider / Data Center

SRX Series

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

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

Botnet detection & remediation

DoS monitoring & remediation

On-going anomaly detection
PROVIDING DEEP PACKET INSPECTION -- IPS

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 IPS**

- **VULNERABILITY**
- Exploits
- Other IPS’s

**On-going threat protection**

**Mobile traffic monitoring**

**Custom attack mitigation**
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
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
SECURITY IMPLICATION OF VIRTUALIZATION

Physical Network

Firewall/IDS Sees/Protects All Traffic Between Servers

Virtual Network

Physical Security is “Blind” to Traffic Between Virtual Machines
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

1. VLAN Segmentation

VLANs offer no granular security

2. Agent-based

Agents are very costly to manage at scale

3. Hypervisor-based

In the hypervisor = maximum performance and security
# HYPERVERSOR-BASED VS. VLANS

<table>
<thead>
<tr>
<th>REQUIREMENT</th>
<th>Juniper vGW</th>
<th>VLANs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security per Virtual Machine (VM)</td>
<td>✔</td>
<td>✗</td>
</tr>
<tr>
<td>Integrated Intrusion Detection</td>
<td>✔</td>
<td>✗</td>
</tr>
<tr>
<td>Hypervisor Protection</td>
<td>✔</td>
<td>✗</td>
</tr>
<tr>
<td>Auditing of hypervisor access</td>
<td>✔</td>
<td>✗</td>
</tr>
<tr>
<td>Monitoring of all inter VM traffic</td>
<td>✔</td>
<td>✗</td>
</tr>
<tr>
<td>VM Introspection</td>
<td>✔</td>
<td>✗</td>
</tr>
</tbody>
</table>
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
- 1st Purpose-Built Virtual Firewall
- "VMsafe Certified" by VMware
- 5 Patents Pending

Most Innovative Company
RSA® Conference 2010

2010 SIIA CODiE FINALIST

BEST OF INTEROP

FINALIST AWARD
SECURITY AND VIRTUALIZATION
VGW – AUTOMATED VM PROTECTION

- VM Introspection
- Compliance Assessment
- Inter-VM Visibility

- HVX Status
  - vCenter Link Active
  - 14 Secured VMs
  - 2 Unsecured VMs
  - 6 Secured VMs with Default Policy

- Compliance Status for All Machines

- Top Talkers for All Machines

Copyright © 2011 Juniper Networks, Inc.  www.juniper.net
Automatically classify VMs and assign them to the correct protection policy.
COMPLIANCE

Be notified of any configuration and security state changes
VISIBILITY – VM INSPECTION

A searchable inventory of VM configurations
INTEGRATED WITH JUNIPER DATA CENTER SECURITY

- **VM1**, **VM2**, **VM3**
- **vGW**
- **Juniper EX Switch**
- **Juniper SRX with IPS**
- **Central Policy Management**
- **Firewall Event Syslogs**
- **Netflow for Inter-VM Traffic**
- **Zone Synchronization**
- **Traffic Mirroring to IPS**
- **Network**
- **STRM**
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