Juniper Networks
IP Routers & Security Solutions
Tendencias Tecnologicas

Cuauhtemoc Trejo M.
TAM Juniper Networks Mexico

Ctrejo@juniper.net
The Internet is Changing…Today:

Devices

Intelligence

Connectivity

limited WAN User experience

LAN User experience

Services

Connectivity
The Industry Has Two Choices

Continue growing service-specific private networks & a commoditized Internet…

Private Networks
- Control over security, quality...
- Expensive
- No inter-carrier connectivity

Public Internet
- Global connectivity
- Low cost
- No control over security, quality...

…OR migrate to a single infrastructure that delivers quality, security & reach

Single Network
- Segregated, uniquely managed virtual networks
- Assured end-to-end experience

Infranet
- Private IP/VPNs
- Email
- Web
- VoIP
- Gaming
- Video Conferencing
The Internet is Changing…:

- Connectivity
- Connectivity Services
- Assured WAN User experience
- Assured LAN User experience
- Services
- Connectivity
- Intelligence
- Devices
Intelligent Services – a Challenge and an Opportunity

Network Security becomes an integral part of the intelligent Network Services layer

Building the WorldWide LAN:
- Netscreen Technologies
- Peribit Networks
- Red Line Networks
- Funk Software
## Secure and Assured Portfolio

<table>
<thead>
<tr>
<th>Product</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Routing</strong></td>
<td>Deliver high levels of security, uptime and performance with simplified operations in converged IP and IP/MPLS infrastructures through professional-grade routers based on the advanced, modular JUNOS operating system.</td>
</tr>
<tr>
<td><strong>Application Acceleration</strong></td>
<td>Improve and control application performance for users accessing centralized and web-based applications across a wide area network to improve user satisfaction while lowering infrastructure cost and complexity.</td>
</tr>
<tr>
<td><strong>Session Border Controller</strong></td>
<td>Extends the reach of IP telephony beyond a single network by providing the advanced security, protocol interworking, NAT traversal and Quality of Service mechanisms required to interconnect two VOIP networks for seamless call control and completion.</td>
</tr>
<tr>
<td><strong>Intrusion Detection and Prevention</strong></td>
<td>Provide zero day protection against worms, Trojans, spyware, keyloggers, and other malware by identifying and stopping network &amp; application-level attacks as well as giving visibility to potential rogue servers and applications, and other violations.</td>
</tr>
<tr>
<td><strong>Secure Access SSL VPN</strong></td>
<td>Eliminate the need for client access software, changes to internal servers, and costly ongoing maintenance &amp; desktop support while providing added security through endpoint validation agents.</td>
</tr>
<tr>
<td><strong>Integrated Firewall/IPSec VPN</strong></td>
<td>Integrated security devices with Stateful firewall and IPSec VPN, including models with integrated IDP at the Data Center or integrated Antivirus, Web Filtering and wireless access at the branch office.</td>
</tr>
</tbody>
</table>
Global Commercial Customer Base
Includes 25 of the largest 28 service providers

Americas
- AT&T
- Qwest
- Focal
- Cable & Wireless
- Worldcom

EMEA
- France Telecom
- Colt
- Deutsche Telekom

APAC
- Hanaro Telecom, Inc.
- Korea Telecom
- China Telecom
- Chunghwa Telecom
- NTT Communications
- KDDI
- SingTel
- Telstra
Research & Education Customers

National Networks

North America
- Abilene - Internet2
- CA*net4 - Canada
- And 5 other National R&E Networks

Europe: GÉANT + 10 National R&E Networks

Asia: APAN + 3 National R&E Networks

Regional & Campus Networks

North America
- 16 GigaPoPs
- 13 Supercomputer Centers & National Labs
- 50+ Universities
- Several State Government Nets
- Several K-12 Systems

Europe
- 14 GigaPoPs
- 1 Supercomputer Center
- 30+ Universities & Research Labs

Asia
- 20+ Universities & Research Labs

Latin America
- 1 GigaPoP
- 1 University
EMEA R&E Networks

Planned national access speeds to
the pan-European backbone
(October 2001)

Source: www.dante.net/geant/
The Abilene Network

The Abilene network consists of the states of AZ, CO, IA, ID, MN, MT, ND, NE, NM, OR, SD, UT, WA, and WY. It is provided to Internet2 as a charitable contribution of Qwest, which continues to assist in the operation of Abilene in those states.
Japan Gigabit Network

- Japan Gigabit Network (JGN) - nationwide, next generation network widely available for use at universities, research institutions, venture businesses & local governments in Japan.
- IPv6 service offered to the public and academic institutions in Japan since Fall 2001.
- "I appreciate Juniper Networks IPv6 implementation, as it provides us the same level of packet forwarding capacity, scalability as its IPv4. Also, it can run IPv4 and IPv6 simultaneously, while providing the interoperability with other IPv6 vendors' routers. I, especially, appreciate Juniper Network's prompt and adequate technical supporting to try to deliver the production-caliber quality operation."

Dr. Esaki, head of JGN IPv6 operation
v4 & V6 on a single infrastructure

ESnet Announcement 8/28/02

Department of Energy's Global Research Network Teams With Juniper Networks to Deploy Simultaneous IPv4 and IPv6 Operation

Delivers Scalability and Performance without Compromise to Advance Global Internet Expansion

- A single set of routers
- Simultaneous IPv6 implementation
Juniper IPv4 vs IPv6 Forwarding

- Both forwarding tables (IPv4 & IPv6)
  - Built by the Routing Engine
  - Stored in memory on the Forwarding Engine’s ASIC
- All forwarding decisions made in hardware
- Internet Routing Table
  - From University of Oregon Route Views Server
  - Approximately 112,000 Routes
TeraGrid

- Distributed Terascale Facility
- $53 Million NSF Funded Supercomputer Project
- Distributed across NCSA; Argonne; SDSC; Caltech
  - 8 Terraflops at NCSA (Illinois)
  - Petabytes of data at SDSC (California)
- Network has:
  - 6 T640s
  - 16 SONET OC-192 Circuits
  - 12 - 10 Gigabit Ethernet Links
Router platform selection

Two platforms in production for ~2 years
- Cisco 12416
- Juniper M160

One new (then unannounced) platform
- Juniper T640

Technical recommendation was for T640
- Significant improvement in performance
  - Longer ‘high-performance service’ lifetime
- Immediately scalable to 40-Gbps interfaces
- More compact (half rack)
- Newest technology

M5s required for OC-3c ATM support
Juniper Networks

M and T Architecture
Juniper M & T Series Routers

M-series
- M20
- M40e
- M320
- M7i/M10i

T-series
- T320
- T640

JUNOS
Common software and features
Across all platforms
Juniper Routers Advantage

**most Secure**
- Modularity for full router control while under attack
- Next Gen CLI for fast editing of filters while under attack
- Dedicated processing to support many filter terms without degradation

**highest Uptime**
- Strong attack defense ensures system stability
- Minor problems do not lead to system crashes
- Next Gen CLI prevents operator error
- Rescue config button for fast recovery

**excellent Performance**
- Predictable performance for voice, video and other time critical apps
- Comprehensive QOS functions to classify, prioritize and schedule traffic

**reduced Operational cost**
- One software train
- Multiple management tools, including J-Web
- XML-based API
- Restoration features
- Feature licensing
- Interoperability
ASIC Based Forwarding and Services

- All packet forwarding and advanced services are executed in hardware on a custom designed ASIC, not on a CPU.
- This ASIC is a programmable, high performance packet classifier and forwarding engine optimized for IPv4, IPv6, and MPLS.
- Acts as a centralized resource enabling breakthrough support for performance-based, enhanced services on all interfaces:
  - filter based forwarding, packet filtering, packet sampling, rate limiting, traffic policing, and port mirroring.
Design and Operations Simplicity

New Features and Functionality

Single Binary Image on All Platforms

Fewer variables and a simpler process mean less time is spent planning, provisioning, and deploying your networks

◆ CLI enhancements (access controls, command line completion, context sensitive help, rich set of show commands, etc.)
◆ Industry-standard management protocols (XML, SYSlog, and SNMP)
◆ User-friendly configuration syntax: hierarchical (easy to read), editor supports local scoping, and comments/inactive command support
Physical Interface Cards (PICs)

Mix and Match PICs enable maximum configuration flexibility

- Each FPC has 4 PIC slots, any PIC can go into any slot
- Example: an M10 can be configured with OC-48 SONET, Gig-E, Fast-E, DS-3, and OC-12 SONET
- PIC choices include: Fast-E, Gig-E, T1, DS-3, OC3 (SONET & ATM), OC12 (SONET & ATM), OC-48 SONET, OC-192 SONET, 10 Gig-E
Flexible PIC Concentrators (FPC)

- Multiple interface media per FPC slot
- PIC hot insert/removal
- Adding additional flexible PIC controllers (FPCs) adds additional shared memory
  - Available to any interface in the system
  - There is never a possibility of “memory starvation”
Software Usability and Operations

- **Command Line Interface**
  - User & group access control
  - Flexible config management
  - Commit & rollback
  - Hierarchical, easy to read

- **Protocols & Tools**
  - SNMP v1, 2 (v3 in 5.4)
  - Telnet and FTP
  - Syslog and NTP
  - TACACS+ and RADIUS
  - SSH and SCP
  - Ping and Traceroute

```c
interfaces {
    fxp0 {
        unit 0 {
            family inet {
                address 10.0.0.20/24;
            }
        }
    }
}
routing-options {
    static {
        route default {
            gateway 10.0.0.1;
            retain;
            no-readvertise;
        }
    }
}
```
IPv6 Available Features

- Supported on all M-series and T-series platforms

**Addressing & Forwarding**
- Forwarding in hardware
- Addressing
  - Link, site, global
  - Stateless autoconfiguration
- Neighbor discovery
- IPv6 Packet Filtering
- EUI 64 Autogeneration
- Unicast RPF
- FBF and CBF for IPv6
- Destination/Source Class Usage

**Routing Protocols**
- IS-IS
- OSPFv3
- MP-BGP over v4/v6
- RIPng
- Static
- IPv6 VPN (RFC2547bis)
- PIM v2
- MLD

**Operations & Transition**
- Common support
- ICMPv6
- SNMP over v6 + MIBs
- IP applications
  - Ping, telnet, ssh, ftp...
- Transition
  - Configured tunnels
  - Dual stack
  - Transport IPv6 in MPLS
Service-Built M7i router

- **Leverages production proven technology**
  - Internet Processor II technology
  - Feature rich JUNOS 6.0 software

- **Uses existing M5/M10 PIC’s**
  - Broad set of interfaces available (45)
  - Provides investment protection

- 2 Rack Units high

- Four configurations:
  - 4 open slots, 2 x FE fixed
  - 4 open slots, 2 x FE fixed, adaptive services module
  - 4 open slots, 1 x GE fixed (SFP)
  - 4 open slots, 1 x GE fixed (SFP), adaptive services module

Ideal for:
- PE services, low density PoPs
- Carrier class head office CPE
M7i with Adaptive Services Module

- Hardware-accelerated packet processing with programmable ASICs
  - Based on Adaptive Services PIC technology
  - High performance services
  - Optional, must be ordered with chassis
- J-Protect security toolkit
  - High speed NAT
  - High speed Stateful Firewall
  - High speed IPSec
- J-Flow accounting
  - High speed accounting
Security in the Intelligent Infrastructure

- The network infrastructure is becoming more intelligent
  - MPLS
  - “Infranet”

- The intelligent infrastructure provides end-to-end services to applications:
  - Quality of Service (QoS)
  - Security
  - Reliability
  - Measurement

- Every device in the path of packets needs to provide these services in tandem with all other devices
  - Security devices are no exception
J-series Services Router

- **J2300**
  - 2XT1/E1/Serial platform
  - 2 fixed FE LAN + 1 fixed 2 port card
  - 1 FE & 1 primary port active, additional w/license
  - 1 expansion slot for backup ISDN/dial interfaces

- **J4300**
  - Nxt1/E1
  - 2 fixed FE LAN + 6 open interface slots
  - 1 FE port active, additional w/license

- **J6300**
  - DS3 platform
  - 2 fixed FE LAN + 6 open interface slots
  - Both FE ports active
  - Redundant power supply

I/O Cards: 2xT1, 2xE1, 2xSerial, 2xFE (J4300/J6300), DS3 (J6300)
Juniper Advantages for R&E Nets

- **JUNOS**
  - Running in production networks for 10+ years
  - High Performance IPv4; Scalable Multicast that works; IPv6 features and functionality
  - Same JUNOS on all M&T Series Routers

- **Hardware Performance**
  - Advanced Features at line rate

- **Routers that don’t get in the way of Network Research**
  - No performance or operational bottlenecks allow network researchers to focus on network research not router trouble shooting
Network Security: New Challenges

1. Merging Network Security into an intelligent network infrastructure

2. Disappearance of the Trusted Network. Users and their devices are always “inside”

3. Applications impose tougher demands on network equipment:

4. New types of endpoints, less trust and less control

5. Attacks target applications, spread quickly and are increasingly more difficult to detect
Security in the Intelligent Infrastructure

*Traditional Approach*

All devices need to participate in the intelligent infrastructure
Security in the Intelligent Infrastructure

Integrated Infrastructure

Internet

Integrated Routing, Firewall, VPN, DDoS, IPS/IDP, AV, etc.

ST Firewalls

IPS/IDP

Anti Virus

DMZ

Finance

HR

Sales

Department Servers

- Appliances remain popular by being a simple means of delivering security software, so much so that appliance products can be found that cover many different security applications. By 2007, 80% of all network security solutions will be delivered via a dedicated appliance.

- IDC believes that the market for threat management appliances remained strong because of the wide coverage of the products. IDC tracks these products in price bands ranging from a few hundred dollars to a few hundred thousand dollars. The appliances solve many enterprise security problems.

- IDC believes that there will continue to be new players in this market because there are low barriers to entry and strong demand for different types of appliances, especially regionally.

- Threat management appliances, especially UTMs, continue to be popular with small and medium-sized enterprises. This segment continues to be targeted by all of the appliance vendors because of the large number of potential customers.
Evolution of the Enterprise Gateway
Increasing Demands Require New Approaches

- Increasing use of small packet applications: multi-media, streaming media, VoIP, etc.
- Make traffic decisions with low latency to ensure applications are not affected
- Increasing demand for remote network connectivity: from home, on the road, on the go-PDA’s wireless
- Application vulnerabilities are on the rise, application attacks are growing in sophistication
Introducing NetScreen-Integrated Security Gateway (ISG) 2000

Best-of Breed Security in a Single Platform

• **Predictable Performance** –
  Next-Generation Security ASIC (GigaScreen³)
  • 2 Gbps Stateful Firewall - any packet size
  • 1 Gbps 3DES & AES IPSec VPN - any packet size
  • 1 Gbps+ IDP

• **Integration**
  • Core networking capabilities via ScreenOS – Security Zones & Virtual Systems, OSPF, BGP & RIPv2 routing, A/P & A/A High Availability
  • Security applications -- FW/Deep Inspection/VPN

• **Scalability**
  • New flexible architecture designed to accommodate future performance, capacity and functionality needs
    • Up to 28 ports, up to 500 VLANs,

• **Attack Protection**
  • Network attack protection, including DoS attacks (Screens)
  • Deep Inspection to protect against attacks in Internet-facing protocols
Forecast and assumptions (IDC)

Continuing expansion of the UTM security appliance.
Security event correlation married to UTM management.
Opportunities in small and medium-sized enterprises. The number of small and medium-sized companies is huge.
Addressing new applications such as voice, Web services, and storage networks.

Wireless (WLAN) security
Change in form factor. Security appliance form factors will continue to change. The standalone black box is beginning to be replaced by appliance blades or Cards.

Firewall routers. boon or bane? The increasing incorporation of firewall technology into routers by networking vendors such as Cisco, Enterasys, and Juniper can be a blessing or a curse for the threat management markets.

More new players and no consolidation.
## SSG: New Family

<table>
<thead>
<tr>
<th>Maximum Performance and Capacity&lt;sup&gt;(1)&lt;/sup&gt;</th>
<th>SSG 550</th>
<th>SSG 520</th>
</tr>
</thead>
<tbody>
<tr>
<td>ScreenOS version support</td>
<td>ScreenOS 5.1</td>
<td>ScreenOS 5.1</td>
</tr>
<tr>
<td>Firewall performance</td>
<td>1 Gbps IMIX traffic</td>
<td>600 Mbps IMIX traffic</td>
</tr>
<tr>
<td>3DES VPN performance</td>
<td>500 Mbps</td>
<td>500 Mbps</td>
</tr>
<tr>
<td>Packets per second (64 byte packets)</td>
<td>600,000</td>
<td>300,000</td>
</tr>
<tr>
<td>IPS performance</td>
<td>500 Mbps</td>
<td>300 Mbps</td>
</tr>
<tr>
<td>Concurrent sessions</td>
<td>128,000</td>
<td>64,000</td>
</tr>
<tr>
<td>New sessions/second</td>
<td>15,000</td>
<td>10,000</td>
</tr>
<tr>
<td>Policies</td>
<td>4,000</td>
<td>1,000</td>
</tr>
<tr>
<td>Users supported</td>
<td>Unrestricted</td>
<td>Unrestricted</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Network Connectivity</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Fixed I/O</td>
<td>4x 10/100/1000</td>
</tr>
<tr>
<td>Physical Interface Module (PIM) Slots</td>
<td>6</td>
</tr>
<tr>
<td>Enhanced PIM Slots</td>
<td>4</td>
</tr>
<tr>
<td>WAN interface options</td>
<td>Serial, T1, E1, DS3</td>
</tr>
<tr>
<td>LAN interface options</td>
<td>SFP, FE, 10/100/1000</td>
</tr>
</tbody>
</table>
APM advisors report: Traffic Management

**Competition**

Taking a look at what should keep Packeteer awake at night, there are a number of monsters coming out of the closet. First of all, many of the other Ingress / Egress products are including various QoS mechanisms within their products. While there may not be an argument about whose traffic management is better than whose, it’s clear that most of the vendors are taking the approach we outlined in the APM Paper, which is that this is a feature and not a product.

**Best of Breed vs Breadth**

While any feature needs to work, there is a level of ‘good enough’ within traffic management that should be kept in mind. Basically, what ‘traffic shaping’ or queuing is providing is a prioritization scheme that provides bandwidth for the applications that should have it. Therefore any well-implemented scheme will manage congestion and improve response times for critical transactions.

Therefore the service points for Traffic Management are being defined by the application architecture rather than the network architecture.
Juniper’s Broad Product Portfolio
Meeting a Diverse Range of Requirements

- Central Policy-Based Management
- Secure Remote Access (SSL VPN)
- Access Routing
- Unified Access Control

- Integrated Firewall/IPSEC VPN
- Integrated Security Gateways
- Intrusion Detection and Prevention
- Secure Services Gateways

- Core and Aggregation Routing
- WAN Acceleration
- Application Acceleration
- VF-Series
Evolving Challenges and Requirements

Different Users with different relationship to business
Different Devices with different levels of IT control
Different Locations with different relationship to business

Need Access to Differentiated Information and Application Services

A New Security and Assurance Paradigm

Security throughout the computing environment
• Trust = binary → Trust = variable
• Perimeter Security → Pervasive Security

Increase Intelligence in the Network
• User/device separate from network → Blended
• Network level → network, application, device, user

Assurance throughout the computing environment
• Best Effort → Predictable Service Delivery
• Support quality → Enhance quality
Best in Class Platforms for Carriers and Enterprises

- Purpose-built platforms delivering performance, stability and control
- Applications and services supported at scale
- User and application aware
Secure + Assured + Open = Secured and Assured Solutions
Preguntas?