The purpose of a network is to move packets in a fast and secure manner. In fact, delivering the most advanced, open, and programmable network security platform is crucial for operational efficiencies, reliability as well as security efficacy, where Juniper’s SRX is positioned for operational efficiencies, reliability, as well as security efficacy, scalability. SRX’s throughput range is from 700Mbps up to 1Tbps, and 100m concurrent sessions. Available in virtual, appliance and chassis form factors, SRX is uniquely positioned for operational efficiencies, reliability as well as security efficacy, delivering the most advanced, open, and programmable network security platform that can be deployed as a data center firewall or a next generation firewall.

Juniper’s point of view on security
The purpose of a network is to move packets in a fast and secure manner. In fact, security is all about time – the speed of your firewall, the time it takes to respond to threats, and the efficiency factor – where time is money. View the chalk talk on Partner Center or Sales Central.

Virtual security: vSRX
vSRX in a virtual machine format with HA, multi-platform support and integrated automated management functionality.

Full Stateful Firewall
SRX in a virtual machine format with HA, multi-platform support and integrated automated management functionality.

Rich Routing & Networking
VPN connectivity and routing features in a flexible virtual machine format based on proven Junos OS foundation.

Advanced Security Services
Integrated UTM including IPS, full anti-virus, anti-spam, Web-filtering, content filtering and AppSecure.
**Spotlight Secure Threat Intelligence Platform**

Spotlight Secure is an open platform for threat detection and advanced malware prevention. It enables any number of intelligence sources to be aggregated and optimized through Security Director, then streamed directly to the SRX enforcement points using dynamic address groups. This enables continual updates without change/commit requirements. It is the fastest way to get threat intel directly to the firewall for immediate protection and risk reduction of data exfiltration.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open</td>
<td>Customer has choice to use any feed</td>
</tr>
<tr>
<td>Scalable</td>
<td>Robust, scalable architecture supports thousands of firewalls</td>
</tr>
<tr>
<td>High Capacity</td>
<td>Capacity for &gt;1M data feed entries, including IPs, URLs, and domains</td>
</tr>
<tr>
<td>Adaptable</td>
<td>Efficient resource utilization</td>
</tr>
</tbody>
</table>

**What to sell by use case**

**Domain**
- Data Center
- Edge
- Branch

**Use case**
- Private Cloud
- Transactional
- CDN
- High Performance Data Center
- Secure Visibility and Control
- Secure Communication
- Botnet / C&C detection
- Secure browsing

**Product**
- vSRX
- High End SRX
- IPS
- AppSecure (includes IPS)
- High End SRX
- Spotlight Secure
- UTM
- AppSecure (includes IPS)
- Branch SRX or vSRX
- Spotlight Secure
- UTM
- UTM
- UTM

**Service Provider: Sell Through**
- Service Provider's Customer
  - Secure Router
  - SP MSSP
  - SDN/NFV
  - vSRX
  - High End SRX
  - vSRX
  - Branch SRX
  - vSRX/Contrail
  - High End SRX

**Service Provider: Sell To**
- Mobile Service Provider
  - LTE Sec Gateway (VPN)
  - PCRF Roaming Firewall
  - Secure Router/Integrated Security Appliance
- Service Provider Subscribers
  - SDN/NFV
  - vSRX
  - Branch SRX
- High Performance Data Center
  - vSRX
  - Branch SRX
  - vSRX/Contrail
  - High End SRX
  - IPS
Enterprise edge use case summary

**Customer Pain Points**
- Manual processes: Human error and misconfigurations can be extremely time consuming
- SSL traffic visibility: 25 to 70% of enterprise traffic is SSL. SSL reduces visibility; application layer attacks will go undetected due to lack of SSL visibility. SSL decryption capabilities are a must in order to track and monitor sophisticated malware or application layer attacks.
- Performance: 2048b SSL decryption at the gateway firewall will create performance challenges for the gateway devices
- Compromise: Either over provision or compromise on security specialty in case of smaller deployments

**Juniper Solution**
- Juniper SRX-3000 Series
- AppSecure: Application control and IPS with SSL decryption (Forward and reverse proxy)
- IPS: Protects hosts from known vulnerabilities
- UTM (AV, Anti SPAM, content filtering)
- Threat Intelligence Platform: Detects and protects from data exfiltration
- Cross sell / up sell
  - EX2200 and EX3200 Ethernet switches
  - High-end SRX Series and router at central location
  - Spotlight Secure for bot detection

**Competitive Advantage**
- Check Point
  - Limited advanced routing and networking support
  - Often more expensive
  - Customer support issues
- Cisco
  - Competing product lines from Cisco creates lot of confusion for the customer
  - Closed models to lock in customers
  - Multiple management consoles
- Fortinet
  - Extremely poor performance when services other than firewall are turned on
  - Performance drops 93% when SSL decryption is enabled (worst in NSS SSL performance test)
  - Not shipping 100Gbps Interface yet
  - Deceiving datasheet numbers
- Palo Alto Networks
  - Closed application signatures (limits Layer 7 visibility)
  - Extremely expensive solution for commodity features such as application ID and user ID
  - Weak IPS functionality

**Qualifying Questions**
- How much time does your operations team spend on change management, rule audits and other similar activities?
- How many applications are running SSL? What percentage of your traffic is SSL?

**Power Position**
- Carrier class reliability
- Supports all use cases for scale (.7 to 300 Gb/s), and form factor (appliance, chassis, virtual)
- Open signature, supports any third party threat feed and supports open standards
- Best SSL decryption with minimal performance impact on 2048b ciphers (NSS Labs)
- Network and security unified via JunOS & automation

Branch and secure router use case summary

**Customer Pain Points**
- Lack of security resources: SMBs often must share/combine security and networking resources
- Regulations with huge fines: In US Privacy Bill of Rights; EU Data Privacy Act; Canada PIPEDA; Australia Privacy Management bill are but a few
- Attacker are targeting SMBs: Attackers consider SMBs to be easier targets than large enterprises

**Juniper Solution**
- Consolidate routing, switching, and next generation firewall functionality on a Branch SRX
- Scale from 700 Mbps to 10 Gb/s
- User-based policy through AD integration
- App and web control; URL filtering
- Connect multiple locations using IPv6/psec tunnels
- Cross sell / up sell
  - vSRX (Firefly Perimeter)
  - EX2200 and EX3200 Ethernet switches

**Competitive Advantage**
- Check Point
  - Requires additional routers; does not support PoE
  - Cannot support MPLS and IPv6 on same box
- Cisco
  - Lacks next generation firewall features for small branch deployments (for less than 1 Gb/s)
  - Models below ASAS512 (equivalent to the SRX240 but 5 times more expensive) does not support application control and visibility
- Fortinet
  - A compromise between security and performance
  - Customers are required to purchase switch and router at the branch location, which adds to the cost.
- Palo Alto Networks
  - Very expensive
  - Limited routing and MPLS support on the box
  - Unable to provide on-box/box automation to bootstrap, configure, manage and retire the firewall

**Qualifying Questions**
- How many branch locations do you have?
- Do you need advanced routing capabilities? (MPLS/ BGP)
- Do you want to encrypt communication between two branches or between a branch and a head office?
- Do you need application visibility?
- Do you need botnet and/or malware detection?
- What apps do you have running in your branch offices?
- How do you know these web 2.0 applications are authorized and malware free?

**Power Position**
- Reduce TCO via advanced routing (MPLS), switching, next gen firewall and UTM firewall on a single box
- Increased reliability with automation for bootstrapping, policy configuration, and other operational management processes
- Simplified administration: Centralized management, autoup, and dynamic hub and spoke VNP functionality reduces overhead.
- Zero Touch Provisioning: Junos automation framework allows enables zero touch provisioning

Next Gen Firewall Chalk Talk

**SRX model comparison quick view**

<table>
<thead>
<tr>
<th>SRX Model</th>
<th>Bandwidth (Gb/s)</th>
<th>Concurrent sessions (k)</th>
<th>Connections Per Second</th>
</tr>
</thead>
<tbody>
<tr>
<td>SRX100</td>
<td>.7</td>
<td>32</td>
<td>1,800</td>
</tr>
<tr>
<td>SRX110</td>
<td>.7</td>
<td>32</td>
<td>1,800</td>
</tr>
<tr>
<td>SRQ210</td>
<td>.85</td>
<td>64</td>
<td>2,200</td>
</tr>
<tr>
<td>SRQ220</td>
<td>.95</td>
<td>96</td>
<td>2,800</td>
</tr>
<tr>
<td>SRQ240</td>
<td>1.8</td>
<td>256</td>
<td>8,500</td>
</tr>
<tr>
<td>SRX550</td>
<td>5.5</td>
<td>375</td>
<td>27,000</td>
</tr>
<tr>
<td>SRX650</td>
<td>7</td>
<td>512</td>
<td>35,000</td>
</tr>
<tr>
<td>SRX1400</td>
<td>10</td>
<td>1,000</td>
<td>70,000</td>
</tr>
<tr>
<td>SRX3400</td>
<td>30</td>
<td>3,000</td>
<td>150,000</td>
</tr>
<tr>
<td>SRX3600</td>
<td>55</td>
<td>6,000</td>
<td>270,000</td>
</tr>
<tr>
<td>SRX5400</td>
<td>240*</td>
<td>28,000</td>
<td>450,000</td>
</tr>
<tr>
<td>SRX5600</td>
<td>480*</td>
<td>100,000</td>
<td>450,000</td>
</tr>
<tr>
<td>SRX5800</td>
<td>1,000*</td>
<td>100,000</td>
<td>450,000</td>
</tr>
</tbody>
</table>

* with SRX Express Path feature enabled

---

CPE/Datacenter LTE Security Gateway

Customer pain points
- Manual processes: Creates human error and misconfigurations which can be extremely time consuming and can cost a fortune.
- Multiple vendor, multiple technologies and interoperability issues: SDN, virtualization and cloud create unique challenges for the datacenter to integrate and automate the entire workflow.
- Compromise: Customers are forced to compromise between security, performance, reliability, availability and automation.

Juniper Solution
- Juniper SRX-5000 series with IPS, centralized management and event correlation
- Rich ISSU, ISHU, revert back and self protecting configuration features enable ease of operations and minimal downtime
- SRX is still the only firewall that is shipping 100GBe

Cross sell / up sell
- vSRX (Firefly Perimeter)
- MX 280/480
- QFX 5100/3600

Competitive advantage
Check Point
- Lack of automation (auto provision and config)
- Extremely expensive solution for old technology
- Not shipping 100GBe interface yet

Cisco
- Cisco 5585 requires customer to rip and replace if customer requires different SSP (security card)
- 100GBe interface is not available.

F5
- Weak UDP performance
- Unreliable: often reboots when under DoS attack
- Firewall only solution; does not support IPS

Fortinet
- Poor performance when services are turned on
- No 100GBe interface production experience

Palo Alto Networks
- Unable to support 100 million sessions
- Lacks datacenter experience and scalability
- Does not support 100GBe interface

Qualifying questions
- What percentage of your servers are virtualized?
- How many applications are running SSL? What percentage of your traffic is SSL?
- How much time does your team spend on change management, rule audits and similar activities?
- Will you want to leverage IPv6 and/or dynamic routing protocol capabilities on your firewall?
- Do you required 100GBe interface?
- Do you expect downtime for upgrades and updates?
- How are you securing your virtual workloads?

Power Position
- Reliability: In-service software and hardware upgrades reduces downtime
- IPv6 and advanced routing: JunOS routing features strong IPv6 and dynamic routing protocol support
- Automation reduces the time and resources required for day to day operations
- Open Standards: supports third party threat feed, allows customers to write their own signatures
- Network and security unified via JunOS and automation

Mobile/broadband service provider use case summary

Customer Pain Points
- Privacy: clear test data may expose network element for the carrier; results in privacy liability
- Revenue impact due to unreliability: voice and streaming application may be impacted the most because of unreliable firewall and that may prevent carriers from providing aggressive SLA or even worse can result in subscriber churn. Subscriber retention is cheaper than getting the new subscribers.
- Manual provisioning: Leads to human error and misconfigurations, can be extremely time consuming and cannot be automated
- DoS/DDoS: Huge issue for service providers and specially mobile carriers.
- Explosive growth in data and subscriber in mobile network with little tolerance for traffic delays. Data growth demands more infrastructure which results in more CAPEX and OPEX with no additional revenue.

Juniper Solution
- (i)Gi and roaming firewall to protect Mobile subscribers and provide value add services.
- LTE Security Gateway for encryption for firewall and signaling protection scale up to 300 Gbps which can go up to 1 Tbps with service offload.
- SRX5000 supports up to 100GBe interface which allows customers to scale without adding network complexity.
- Rich ISSU, ISHU, revert back, self protecting configuration features enables operations ease and minimal downtime

Cross sell / up sell
- vSRX (Firefly Perimeter)
- MX 280/480
- QFX 5100/3600
- Contral as SDN Controller

Power Position
- Reduce OPEX: Only Juniper has underlying JUNOS for switching, routing and security.
- Reliability: Juniper SRX S4 series tested for stringent reliability (6-nines), <14 seconds of downtime per year. ISSU and ISHU provides an easy way to upgrade the firewalls with the downtime of few seconds.
- Additional revenue opportunity with VCPE/CEPE: New gen firewall services, router and T1 connectivity in the same platform.
- Only 100GBe interface shipping today
- Reduce complexity with end-to-end MPLS tunnel from core to subscribers
- Reduce complexity in automation: JunOS for security, switches and routers eliminates complexity for service chaining and automation by providing consistent commands and features that can programmed and reused

Mobile-European carrier use case summary

Customer Pain Points
- DoSRD: Have you got outages due to DDOS on Gi interface?
- Are you planning to upgrade to 100GBe?
- What are your subscriber growth projections?
- LTE Security Gateway
- Do you trust interconnect points such as third party RAN & GRX cloud carrying clear text data?
- Are you planning to implement femto cells/ small cells? If so, how are you going to encrypt the data?
- Roaming Firewall
- How are you protecting your mobile phones, radio network and EPC from threats such as DDoS?
- Datacenter
- Would you require automation to provision firewall and automate rule creation and configuration?
- CPE/VcPE
- Are you planning to add additional subscriber services such as parental control?
- Are you planning to add security services?

Qualifying questions
- (i)Gi- Firewall
  - Have you had outages due to DD0S on Gi interface?
  - Are you planning to upgrade to 100GBe?
  - What are your subscriber growth projections?
- LTE Security Gateway
  - Do you trust interconnect points such as third party RAN & GRX cloud carrying clear text data?
  - Are you planning to implement femto cells/ small cells? If so, how are you going to encrypt the data?
- Roaming Firewall
  - How are you protecting your mobile phones, radio network and EPC from threats such as DDOS?
- Datacenter
  - Would you require automation to provision firewall and automate rule creation and configuration?
- CPE/VcPE
  - Are you planning to add additional subscriber services such as parental control?
  - Are you planning to add security services?

Power Position
- Reduce OPEX: Only Juniper has underlying JUNOS for switching, routing and security.
- Reliability: Juniper SRX S4 series tested for stringent reliability (6-nines), <14 seconds of downtime per year. ISSU and ISHU provides an easy way to upgrade the firewalls with the downtime of few seconds.
- Additional revenue opportunity with VCPE/CEPE: Next gen firewall services, router and T1 connectivity in the same platform.
- Only 100GBe interface shipping today
- Reduce complexity with end-to-end MPLS tunnel from core to subscribers
- Reduce complexity in automation: JunOS for security, switches and routers eliminates complexity for service chaining and automation by providing consistent commands and features that can programmed and reused

Competitive Advantage
Check Point
- Lack of automation (auto provision and config)
- Extremely expensive solution for old technology
- Not shipping 100GBe interface yet

Cisco
- Cisco 5585 requires customer to rip and replace if customer requires different SSP (security card)
- 100GBe interface is not available.

F5
- Weak UDP performance
- Unreliable: often reboots when under DoS attack
- Firewall only solution; does not support IPS

Fortinet
- Poor performance when services are turned on
- No 100GBe interface production experience

Palo Alto Networks
- Unable to support 100 million sessions
- Lacks datacenter experience and scalability
- Does not support 100GBe interface

Mobile-Europe carrier use case summary

Customer Pain Points
- DoSRD: Have you got outages due to DDOS on Gi interface?
- Are you planning to upgrade to 100GBe?
- What are your subscriber growth projections?
- LTE Security Gateway
- Do you trust interconnect points such as third party RAN & GRX cloud carrying clear text data?
- Are you planning to implement femto cells/ small cells? If so, how are you going to encrypt the data?
- Roaming Firewall
- How are you protecting your mobile phones, radio network and EPC from threats such as DDOS?
- Datacenter
- Would you require automation to provision firewall and automate rule creation and configuration?
- CPE/VcPE
- Are you planning to add additional subscriber services such as parental control?
- Are you planning to add security services?

Qualifying questions
- (i)Gi- Firewall
  - Have you had outages due to DD0S on Gi interface?
  - Are you planning to upgrade to 100GBe?
  - What are your subscriber growth projections?
- LTE Security Gateway
  - Do you trust interconnect points such as third party RAN & GRX cloud carrying clear text data?
  - Are you planning to implement femto cells/ small cells? If so, how are you going to encrypt the data?
- Roaming Firewall
  - How are you protecting your mobile phones, radio network and EPC from threats such as DDOS?
- Datacenter
  - Would you require automation to provision firewall and automate rule creation and configuration?
- CPE/VcPE
  - Are you planning to add additional subscriber services such as parental control?
  - Are you planning to add security services?

Power Position
- Reduce OPEX: Only Juniper has underlying JUNOS for switching, routing and security.
- Reliability: Juniper SRX S4 series tested for stringent reliability (6-nines), <14 seconds of downtime per year. ISSU and ISHU provides an easy way to upgrade the firewalls with the downtime of few seconds.
- Additional revenue opportunity with VCPE/CEPE: Next gen firewall services, router and T1 connectivity in the same platform.
- Only 100GBe interface shipping today
- Reduce complexity with end-to-end MPLS tunnel from core to subscribers
- Reduce complexity in automation: JunOS for security, switches and routers eliminates complexity for service chaining and automation by providing consistent commands and features that can programmed and reused

Competitive Advantage
Check Point
- Lack of automation (auto provision and config)
- Extremely expensive solution for old technology
- Not shipping 100GBe interface yet

Cisco
- Cisco 5585 requires customer to rip and replace if customer requires different SSP (security card)
- 100GBe interface is not available.

F5
- Weak UDP performance
- Unreliable: often reboots when under DoS attack
- Firewall only solution; does not support IPS

Fortinet
- Poor performance when services are turned on
- No 100GBe interface production experience

Palo Alto Networks
- Unable to support 100 million sessions
- Lacks datacenter experience and scalability
- Does not support 100GBe interface

More information for Juniper sellers:
Public information: www.juniper.net/security
Partner Center: https://www.juniper.net/partners/partner_center/
Sales Central: https://juniper.gosavio.com/