Learn About  Service Provider Edge Security

The digital universe containing banking data, corporate financials, health information, tax statements, and personal photos and videos is doubling approximately every two years, according to USA Today. Within that changing digital universe, Internet service providers (ISPs) and telecom cloud providers are transforming their service delivery models, customer experience, and operations environment. During this enormous transformation undertaking, it is vital that network security be given top priority.

This Learn About provides an overview of the role security plays – particularly at the edge – within the ISPs’ evolving network and environment, with an emphasis on their mobile, residential, and business customers, and including security issues faced by today’s telecom cloud providers.

Network Protection and Security

Protecting a network is not merely implementing firewalls anymore, and it is no longer safe just playing defense. Today’s networks are subject to both active and passive attacks from various malicious sources that cause infection throughout the network. Active attacks, such as denial-of-service (DoS) attacks, IP address spoofing (or masquerade attacks), and malware created to target both physical and virtual machines (VMs), are the most complex security threats to manage because they target the control plane (the part of a network that carries signaling traffic and is responsible for routing) of network elements.

Security must be ingrained everywhere – in the protocols, the systems, the elements, the provisioning, and in the business surrounding the network. ISPs must implement security measures similar to those that financial institutions and governments use to protect their networks, devices, and data.

Network security is effective only if appropriate defensive mechanisms are established. Here are the most common categories of defensive mechanisms:

* Corrective mechanisms – Used to reduce the consequences of an incident by limiting the damage. They can be used during or after an incident. An example of a
corrective mechanism is restoring system backups to rebuild a compromised system.

- **Detective mechanisms** – Used to detect and react appropriately to any incidents that occur. In the event of an attack, a detective mechanism signals the preventative or corrective mechanisms required to fix the issue. Typically, network security monitoring, including intrusion detection service (IDS), is used to detect attacks on a network and its supporting communications infrastructure.

- **Deterrent mechanisms** – Used to reduce attacks on a network. Similar to a no trespassing sign, deterrent mechanisms reduce the threat level by informing potential attackers that there will be adverse consequences for them if they persist in their actions.

- **Preventive mechanisms** – Used to strengthen a network against incidents usually by reducing and eliminating vulnerabilities. For example, strong authentication of users makes it less likely that unauthorized users can access the network, and more likely that users are positively identified.

### Universal Edge Service Provider Network Security

An enhanced broadband network gateway (BNG) brings services and access methods together on a common platform, or a universal edge platform. The Juniper Networks MX Series 3D Universal Edge Router portfolio supports a universal set of services, enabling service providers to eliminate service silos, integrate community Wi-Fi access to provide an enriched residential subscriber experience, and consolidate their edge networks onto a single universal edge platform. Figure 1 shows a universal edge implementation example for a converged ISP network. Mobile IP, residential, and business services are consolidated onto a universal edge platform that provides universal access to any application from any device, anywhere.

![Figure 1: Converged Service Provider Network](image-url)
The MX Series routing platforms concurrently support routing, switching, security, and Layer 4 through Layer 7 services under one Junos operating system (Junos OS), and within one element management system (EMS), which reduces network complexity and operational costs. Additionally, MX Series routers such as the MX2020 – the highest-capacity and highest-throughput edge router available – address the steadily growing interest among ISPs for collapsed edge and core networks, and can satisfy those requirements as well.

**Router Security**

Many functions are performed by MX Series Routing Engines, from processing routing protocol updates, to driving the command-line interface (CLI) and running Junos OS. Given that the Routing Engine is critical for the operation of the router and the network, it must be protected from unwanted activities such as malicious traffic seeking to gain unauthorized access, unintentional routing protocol updates from neighboring devices, or even legitimate traffic that exceeds a given bandwidth limit.

Junos OS provides configuration automation tools that enable dynamic prefix lists, and as your network scales and changes, the security framework automatically changes and adjusts without requiring additional input from your network administrator.

**Mobile or Wireless Network Security**

The old network security model of securing the perimeter of a mobile network no longer works. In reality, network complexities and communications undermine security between internal and external environments, and mobile networks are vulnerable to both inside-out attacks and inside-in attacks. Most threats and attacks originate from the Internet (making interfaces to the Internet the most critical to secure), while other common sources of threats are compromised subscriber devices and roaming peers. Today, those in charge of network security have to assume zero trust among network elements, and ISPs want to operate their network as a single-enforced domain where every element – not just those at the perimeter – becomes a policy enforcement point.

Therefore, in order to better combat and contain security threats in the mobile network, ISPs are moving toward a more distributed architecture, with detection and enforcement enabled everywhere. As the threat environment morphs and accelerates, you can have automated and centralized security policies with decentralized enforcement on switches and routers driven by dynamic and real-time security updates. Using software-defined networking (SDN) and Network Functions Virtualization (NFV), you can detect threats and enforce security policies with a high level of automated security, unified threat detection, and real-time protection.

Juniper Networks provides the building blocks for a new security model and a vision for Software Defined Secure Networks (SDSN) as shown in Figure 2.

By using the Juniper Networks SRX Series Services Gateways (or the physical firewalls), and Juniper Networks vSRX virtual firewalls in combination with Spotlight Secure and Sky Advanced Threat Prevention (Sky ATP), you can organize and coordinate threat intelligence, while employing simple common-sense policies. And by upgrading the Gi/SGi firewall, ISPs can modernize the perimeter to become adaptable, and use cloud economics for instant intelligence leading to more effective detection.

Gi/SGi is an IP-based interface and reference point of a mobile network infrastructure that connects and exchanges data on the transmission plane between a gateway GPRS support node (GGSN) and external packet data networks, such as the Internet.
Table 1 lists Juniper’s comprehensive suite of products and how they centralize and automate security regarding threat intelligence.

<table>
<thead>
<tr>
<th>Secure Network Areas</th>
<th>Products</th>
<th>What Product Provides</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dynamic Adaptive</td>
<td>Security Policy Controller</td>
<td>Policy</td>
</tr>
<tr>
<td>and Policy Engine</td>
<td></td>
<td>Dynamically adapts policy and deploys in real time</td>
</tr>
<tr>
<td>Evolved Packet Core</td>
<td>Junos Space Security Director</td>
<td>Policy</td>
</tr>
<tr>
<td>SRX Series Physical</td>
<td>Detection, Enforcement</td>
<td>Consistent firewall capabilities, both physical and virtual</td>
</tr>
<tr>
<td>Firewall</td>
<td></td>
<td></td>
</tr>
<tr>
<td>vSRX Virtual Firewall</td>
<td>Detection, Enforcement</td>
<td></td>
</tr>
<tr>
<td>MX Series Routers</td>
<td>Detection, Enforcement</td>
<td></td>
</tr>
<tr>
<td>with Junos</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network Secure</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(supported with SDSN</td>
<td></td>
<td></td>
</tr>
<tr>
<td>products)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>QFX Series Switches</td>
<td>Detection, Enforcement</td>
<td></td>
</tr>
<tr>
<td>(supported with SDSN</td>
<td></td>
<td></td>
</tr>
<tr>
<td>products)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Juniper Cloud</td>
<td>Spotlight Secure Threat</td>
<td>Detection, Enforcement</td>
</tr>
<tr>
<td>Security</td>
<td>Intelligence</td>
<td></td>
</tr>
<tr>
<td>Sky Advanced Threat</td>
<td>Detection, Enforcement</td>
<td></td>
</tr>
<tr>
<td>Prevention</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Third-Party Cloud</td>
<td>Other vendors</td>
<td>Detection</td>
</tr>
<tr>
<td>Security Feeds</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

By combining SRX Series physical firewalls, vSRX Series virtual firewalls, Junos Space Security Director, Security Policy Controller, MX Series routers (with Junos Network Secure), and Juniper Networks QFX Series switches, ISPs can deploy a policy engine that communicates with their network, gathers analytics from network data, customizes the user interface to provide data correlation, and uses network edge as detection and enforcement points.
Residential Broadband Edge Security

Today’s residential broadband subscribers want personalized online digital experiences, with the freedom to use any device (from phones to tablets to gaming consoles to big-screen TVs) to consume, control, and share content at any location, at any time, and with high quality and resolution levels. With service providers offering IP-based data, video, and voice content to their subscribers on a myriad of devices, and making content easier to access, network security is a very significant issue from the point of view of both a subscriber and a service provider.

For residential subscribers with always-on connections, hacker attacks are a significant issue. Hackers can attempt to breach security at odd hours when no one is likely to notice, and these connections often use static IP addresses thereby making it easy for hackers to consistently return to the site to alter, refine, and exploit their attacks.

Therefore, residential broadband service providers need to meet two major security objectives:

* Defend their own network by shielding network resources and operations against malicious external parties, such as distributed denial-of-service (DDoS) attacks launched against, and from within, their network (IP address spoofing).

* Protect their subscribers against threats from outside networks.

By mitigating these security threats, ISPs can deliver a reliable and highly available service, which is key to growing their business, retaining the loyalty of subscribers, and maintaining profitability. Figure 3 shows a typical residential broadband network topology for IP-based data, video, and voice services.

![Residential Broadband Network Topology](image)

The MX Series 3D Universal Edge Routers with subscriber management software license provide an industry-leading broadband network gateway (BNG) that supports IPTV/video, broadband Internet, integrated voice, Layer 2/Layer 3 wholesale, and content services, among many other services. BNGs are located at IP edge points where they aggregate, authenticate, and terminate subscribers. Because the BNG acts as an initial service point, service providers primarily implement Layer 3 security. For downstream devices, ISPs need to carefully consider and implement Layer 2 and transport-related security.
In addition to physical MX Series routers, ISPs can also use Juniper Networks vMX (a virtual version of the MX Series 3D Universal Edge Router that runs as software on x86 servers) as a BNG. Services that were traditionally deployed on a physical MX Series router are easily provisioned and enforced in a vMX environment to deliver a consistent model of visibility and security, and can enable automated provisioning and context-sharing across virtual and physical security platforms.

**Business Edge Security**

The traditional method for service providers to provision services to business customers on the universal edge is by connecting through secure VPN tunnels or firewalls (see Figure 1). ISPs can use Junos VPN Site Secure to configure, set up, and apply security to IPsec VPN tunnels, and the Junos Network Secure software to provide stateful firewall services that integrate with the MX Series router to protect edge services. This configuration eliminates external firewalls that consume router ports and management resources, and can be used as a first line of defense in layered security architectures. ISPs can authenticate users by using methods such as token authentication (RSA SecurID), smart card authentication, machine authentication, and credential provider authentication.

For ISPs, protecting their infrastructure elements and services from targeted attacks is the utmost concern for securing the business edge. Table 2 lists several of the most common attacks along with measures to prevent them.

<table>
<thead>
<tr>
<th>Attack Type</th>
<th>Purpose</th>
<th>Preventative Measure</th>
</tr>
</thead>
</table>
| Unauthorized access                           | Attacker attempts to gain access to network infrastructure elements for reconfiguration, traffic redirection, or malicious traffic injection. | • Limit management access, including physical access and network access, to network elements such as loopback filters and allow/deny expressions for user groups.  
• Disable controls when not in use.  
• Implement secure communication for management access using SSH for system administrators, SCP (Secure Copy Protocol) to secure file transfers between local and remote host or between two remote hosts.  
• Hide infrastructure elements from end user. |
| Software and hardware security flaws within code | Attacker uses flaw to control, reconfigure, and manipulate code.         | Configure control protocols used in the network, such as IS-IS, OSPF, BGP, and so on, to mitigate hijacking threats. |
| Hijacking of management and network control communications | Infrastructure elements, used to run management routines and protocols, are accessed by attacker who then establishes new control and management sessions, or intercepts existing ones, to impact forwarding behavior. | For VPN and DIA (Direct Internet Access) services, the most vulnerable point of attack is located at the PE (provider edge) to CE (customer edge) interface connection. To mitigate, isolate failure domains by configuring PE to provider interfaces to dedicated line cards, then distribute users between several line cards, and police control plane traffic from each customer. |
| DDoS                                          | Attacker attempts to deny valid users access to network or server resources by using up all of the resources of the network element or server. DDoS attacks from multiple sources enable a much greater amount of traffic to attack the network. | Configure unicast reverse path forwarding (RPF) check in strict mode at the PE to CE interface and over all feasible paths to effectively block any traffic from prefixes that are not reachable through the configured interfaces. |
| DIA and IP address spoofing                    | Attacker attempts to hide the identity of the sender or impersonates another computing system. | Configure unicast reverse path forwarding (RPF) check in strict mode at the PE to CE interface and over all feasible paths to effectively block any traffic from prefixes that are not reachable through the configured interfaces. |
Today, many ISPs are deploying hosted private cloud services at the business edge, and transforming themselves into cloud-hosting service providers. According to an IDC study, the worldwide market for hosted private clouds is expected to reach over $40 billion by 2019 (https://www.idc.com/getdoc.jsp?containerId=259066). A hosted private cloud includes a dedicated hosted-private cloud and an on-demand private cloud. Hosted private clouds offer a cost-effective and robust solution to quality and reliability issues associated with the public cloud. They provide enhanced security and quality-of-service (QoS) features by bringing the cloud platform behind the firewall. Figure 4 shows the Juniper Networks universal edge solution for hosted private cloud over VPN.

The universal edge solution seamlessly extends customer VPNs to cloud data centers. Cloud customer security is extended to virtual machines. The MX Series routers in a Virtual Chassis configuration provide collapsed layers of data center routing, switching, and security devices. As more and more customers embrace the agility and flexibility of automated provisioning for virtual private resources, the on-demand private cloud is trending toward becoming the standard operating model for hosted private clouds.

Figure 5 shows an example of a service provider offering virtual security services (DDoS and URL blocking) on demand to their customers by using a virtual high-end provider edge (vHEPE) router to connect the ingress (incoming) PE device and the URL blocking device (scrubber).
The condition, or origin, of the URL request traffic coming from the PE device to the HEPE device, determines the traffic’s destination. If the traffic:

- Is in a dirty virtual routing and forwarding (VRF) table, then the scrubber device begins filtering.
- Belongs to a blocking list, then some blocking messages are sent out.
- Belongs to an “allowed list” blocking list, then the traffic is first sent to the clean VRF table, and then forwarded to its original destination.

Similarly, for DDoS, if a server is under attack, dirty traffic with known signatures is dropped, while clean traffic is forwarded to its original destination.

In Figure 5, the vMX plays the role of a virtual HEPE, diverting traffic to the virtualized scrubber applications, which can be aligned with the virtual scrubber device to leverage the same cloud infrastructure and orchestration tool.

**Telecom Cloud Providers and Security**

By 2020, nearly 40% of the information in the digital universe will be touched by cloud computing providers (http://preservationmatters.blogspot.com/2014/05/the-digital-universe-in-2020-big-data.html). Telecom cloud providers provide cloud services (or Web services) over the Internet. The most common cloud service resources, collectively known by the acronym SPI, are:

- **Software as a Service (SaaS)** – A software distribution model designed for customers where applications are hosted by a service provider and made available to customers over the Internet. This represents the end result of cloud computing.
- **Platform as a Service (PaaS)** – Provides hardware and software tools, as well as operating services delivered over the Internet without downloads or installation, that can be used as a service by IT personnel to develop applications for end users.
- **Infrastructure as a Service (IaaS)** – Similar to PaaS providers; however, it hosts the infrastructure equipment used to support operations (such as storage, hardware,
software) on behalf of its customers, providing IT personnel more control over the OS of the business.

Threats to cloud platforms are ongoing and affect everyone who uses cloud services for business or personal reasons. Multilayer, multidomain security is critical for a telecom cloud deployment. Table 3 lists some of the biggest security issues and vulnerabilities specific to cloud computing and telecom cloud providers today.

### Table 3  Cloud Computing Security Issues

<table>
<thead>
<tr>
<th>Security Issue</th>
<th>Description/Example</th>
<th>Preventative/Corrective Measure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data breaches</td>
<td>An organization’s sensitive internal data is accessed as a result of malicious and intrusive action. For example, a new data breach called side channel timing exposure allows a user on one virtual machine (VM) to listen for activity that signals the arrival of an encryption key on another VM on the same host.</td>
<td>Implement secure hypervisor and VM operations.</td>
</tr>
<tr>
<td>Data loss or leakage</td>
<td>When a disk drive dies without the customer having a backup drive, and the customer has lost the key that unlocks their encrypted data.</td>
<td>Implement disk-level data protection using RAID, backup/replicated backup, data replication, and journaled/checkpoint-based replication.</td>
</tr>
<tr>
<td>Account/service traffic hijacking</td>
<td>Phishing, loss of passwords, and compromised credentials can lead to loss of control of an account. If an account in the cloud is hijacked, an attacker can use it as a base and take advantage of a customer’s reputation to enhance himself/herself at the customer’s expense.</td>
<td>Practice defense in depth, prohibit sharing of account credentials, and implement strong two-factor authentication.</td>
</tr>
<tr>
<td>Insecure interfaces and APIs</td>
<td>As layers are added to APIs to reach value-added services, increasing complexity might create additional exposure allowing attackers to circumvent policy.</td>
<td>Implement OAuth, an open authorization service for Web services that controls third-party access and is an Internet Engineering Task Force (IETF) standard.</td>
</tr>
<tr>
<td>Malicious insiders</td>
<td>A system is still vulnerable to inside attackers if encryption keys are not stored with the customer and are available only at data usage time.</td>
<td>Keep encryption keys on your own premises, not in the cloud.</td>
</tr>
<tr>
<td>Cloud services abuse</td>
<td>Attackers take advantage of a collection of a large number of servers to manipulate existing cloud services to launch DDoS attacks or add malware.</td>
<td>Plan how to detect inappropriate use, clearly define what constitutes abuse, and determine how to prevent it in the future.</td>
</tr>
<tr>
<td>Shared technology</td>
<td>A misconfigured operating system or application within the cloud’s shared infrastructure can lead attackers to compromise data beyond a customer’s immediate surroundings.</td>
<td>Institute an in-depth defensive and monitoring strategy for errant/destructive behaviors relating to storage, network, application, and user access.</td>
</tr>
</tbody>
</table>

However, in spite of the security threats, cloud security is being promoted as a benefit instead of an unknown and risky hindrance for cloud adoption. Telecom cloud providers must adopt a defense-in-depth strategy to ensure, protect, and secure data by implementing layers of security technologies and business practices. Service providers are building security into the platform at the IaaS level, similar to the way that customers expect power to be built into the platform.
Juniper Networks high-end SRX Series firewalls provide front-end security to telecom cloud data centers around the world. Combined with Juniper’s AppSecure and unified threat management (UTM) capabilities, the SRX Series provides an effective barrier between the outside world and sensitive telecom cloud applications and services. Within the data center, Juniper provides multiple layers of security-focused virtualized network functions (VNFs), such as the vSRX.

For example, public cloud service providers (which can host large numbers of VMs for their customers) can deploy the vSRX to protect their customers by placing the virtual firewall in front of each customer’s individual hosting environment, keeping the hosting environments separate from each other, as shown in Figure 6.

![Figure 6: Public Cloud Service Provider](image)

By combining Junos Space products (such as Security Director and Security Policy Controller), Juniper Networks Secure Analytics virtual appliances, and VMware products in the cloud infrastructure, along with virtualizing specific objects with vSRX, public cloud service providers can tailor security between network elements and offer security services to customers with multiple remote locations.

Traditional cloud architectures rely on relatively unsecure VLANs, where rogue or compromised network elements can impact other workloads. However, using the Contrail Cloud Platform to provide IP VPN (or IPsec VPN) connectivity between virtual objects, ensures that workloads and VMs can communicate only with predetermined network elements, resulting in a more highly secure virtualized network.

With the vSRX, public cloud service providers can provide their customers with the security required, both inside their virtualized data centers, and at the customer and business network edges.
Summary

ISPs face a wide-range of security issues originating from a multitude of known and unknown sources. ISPs must ensure that their infrastructure is secure and that their customers’ data and applications are protected. To protect the growing digital universe, ISPs must devise and follow a thorough, multilayered, and defense-in-depth approach to security by considering all information traversing the network and in the cloud, and not just threats solely identified at the perimeter and edge. A change in mindset is required – it’s not network security anymore, it’s secure networks!

Resources and References

This Day One book introduces you to all the fundamentals of the Juniper Networks Dynamic Subscriber Management solution and shows you how to get it up and running in a day:

This technical library includes everything you need to understand and configure for all aspects of Junos OS Broadband Subscriber Management and Services:

Eliminate threats at the network edge with industry-leading scalability and performance. Service providers can securely scale services while converging edge routing, switching, and security in a single MX Series 3D Universal Edge Router:

To understand why an open, scalable network architecture is essential for enhanced IT security in the cloud era, get our Networks That Know Security eBook. Read about how to safeguard virtual and physical workloads and get always-on protection to reduce vulnerabilities:

The Juniper-sponsored J-Net Communities forum is dedicated to sharing information, best practices, and questions about Juniper products, technologies, and solutions. Register to participate at this free forum:
http://forums.juniper.net/jnet.

The TechTarget network provides technology-specific websites where you can access industry experts, and independent content and analysis:
Today’s networks are subject to both active and passive attacks from various malicious sources that cause infection throughout the network. Security must be ingrained everywhere – in the protocols, the systems, the elements, the provisioning, and in the business surrounding the network. Learn about how to deploy security measures similar to those that financial institutions and governments use to protect their networks, devices, and data.

About the Author:
Susan McCoy is a Staff Engineer Technical Writer at Juniper Networks with over 20 years of experience writing and developing documentation for networking, telecommunications, manufacturing, and marketing.

© 2016 by Juniper Networks, Inc. All rights reserved. Juniper Networks, Junos, are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, and the Junos logo are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.