Extending Enterprise Security to Public and Hybrid Clouds

Juniper Security for an Ever-Evolving Market

Challenge

Enterprises are increasingly migrating to public or hybrid deployments, creating an immediate need to extend the level of security found in traditional networks to the new cloud landscape.

Solution

With a broad portfolio of physical and virtual firewalls, centralized single-pane-of-glass management, and threat intelligence, Juniper helps enterprises seamlessly secure physical data centers, private clouds, and public clouds by extending simple yet comprehensive protection to the ever-evolving market.

Benefits

- Significant CapEx and OpEx savings through investment protection, lower TCO, and lower learning costs
- Simple, intuitive management for enforcing and monitoring security across public and hybrid clouds
- Extension of security policies and technologies used in physical data centers to public and hybrid clouds
- Reduction in the number of proprietary, feature-limited public cloud elements to deploy and manage

The migration to public cloud is accelerating rapidly. In fact, Gartner predicts that the global market for public cloud is expected to reach $204 billion in 2016. This rapid adoption is primarily attributable to the public cloud's ability to deploy across geographies; its flexibility, scalability, and simplicity; and its pay-per-use model and lower upfront costs. However, enterprises with heavy investments in private data centers and concerns about the security of public clouds tend to favor a hybrid approach, leveraging a combination of public clouds and existing physical data centers and private clouds. Regardless, the move to the cloud creates a different risk model that needs to be addressed to ensure the protection of an organization's network.

The Challenge

No new technology is without its pitfalls, and the cloud is no exception. When data no longer resides behind an on-premises firewall, as is the case with public and hybrid clouds, it introduces new risks that need to be taken into account. Additionally, as customers adopt a multi-cloud approach to ensure access to best-of-breed solutions, the need to centrally manage security policies is more critical than ever.

For example, Amazon Web Services (AWS), the most popular public cloud platform with 57% market share, employs a simple IP-level or port-level restriction approach at each instance level. This is a far cry from the granular control and advanced security features that network and security administrators need and use in their physical deployments.

Public Cloud

The popularity of public clouds is no longer restricted to the startup world; their adoption has spread across the full business spectrum to include large enterprises as well. While AWS enjoys the majority of cloud provider market share, solutions such as Microsoft's Azure, Google's Google Cloud Platform (GCP), and IBM's SoftLayer are making significant inroads. Other cloud providers such as Oracle Cloud and Rackspace are also gaining market traction.

Today, the economics of deploying a physical data center with dedicated administrative staff no longer makes economic sense for most enterprises. Instead, they typically opt for one of the more popular cloud platforms, deploy their infrastructure, and hire DevOps personnel in place of a traditional network/security teams.

While DevOps resources offer a mix of development and operational experience, they typically lack security expertise. They are expected to possess good scripting skills and are usually tasked with additional responsibilities such as software build management. Since network security is only a small part of their job description, DevOps individuals need a simple security solution that they can easily configure, monitor, and upgrade. With the rise of infrastructure automation platforms such as Chef and Puppet, programmability is top of mind with every DevOps team and a serious requirement for any security platform.

Hybrid Cloud

Enterprises that want to move to the cloud but have heavy investments in physical data centers prefer the hybrid cloud model, which allows them to leverage the flexibility and economics of public cloud while maintaining more control. Also, some enterprises are legally required to hold certain data on premise. A hybrid approach allows extremely sensitive data to be stored in private data centers while offloading the rest to the cloud.

Migrating to a hybrid cloud is not without its own set of challenges. New security policies must be set up for the public cloud deployment, adding management overhead and introducing discrepancies between the physical data center and the cloud. Additionally, hiring cloud professionals or training existing personnel for cloud security adds to operational expenses and takes time.

The Juniper Networks Public and Hybrid Cloud Security Solution

Juniper Networks offers a broad portfolio of products that work together to address the unique concerns of securing public and hybrid cloud environments. The major components of this solution are:

- Juniper Networks® SRX Series Services Gateways and Juniper Networks vSRX virtual firewall with integrated next-generation and unified threat management (UTM), which deliver:
  - Core firewall functionality with IPsec VPN and feature-rich networking services such as NAT and routing
  - Intrusion Prevention System (IPS) 2.0 to detect and block network intrusions
  - User-based firewalls to analyze, log, and enforce access control based on user roles and groups
  - Application control and visibility with integrated Juniper Networks AppSecure 2.0 to provide application-level analysis, prioritization, and blocking to safely enable applications
  - Antivirus, antispam, and Web and content filtering with UTM to protect against viruses, spam, and malicious URLs and content
  - Support for Linux KVM, VMware, AWS, and Azure platforms (vSRX)
- Sky Advanced Threat Prevention, a cloud-based advanced anti-malware service with dynamic analysis (sandboxing) to protect against sophisticated malware. Integrated with SRX Series and vSRX virtual firewalls, Sky Advanced Threat Prevention provides built-in machine learning to improve verdict efficacy and decrease time to remediation.
- Juniper Networks Junos® Space Security Director provides centralized, single-pane-of-glass management to deploy, monitor, and configure security features and polices across all SRX Series and vSRX virtual firewalls in the network. Policy Enforcer, a component of Security Director, provides an additional level of centralized intelligence for deploying and enforcing security policies on multivendor network elements such as switches, routers, wi-fi access points, and the like. Security Director includes a customizable dashboard with detailed drill-downs, threat maps, and event logs, providing unprecedented visibility into network security measures. It is also available as a mobile app for Google's Android and Apple's iOS systems to enable remote mobile monitoring.

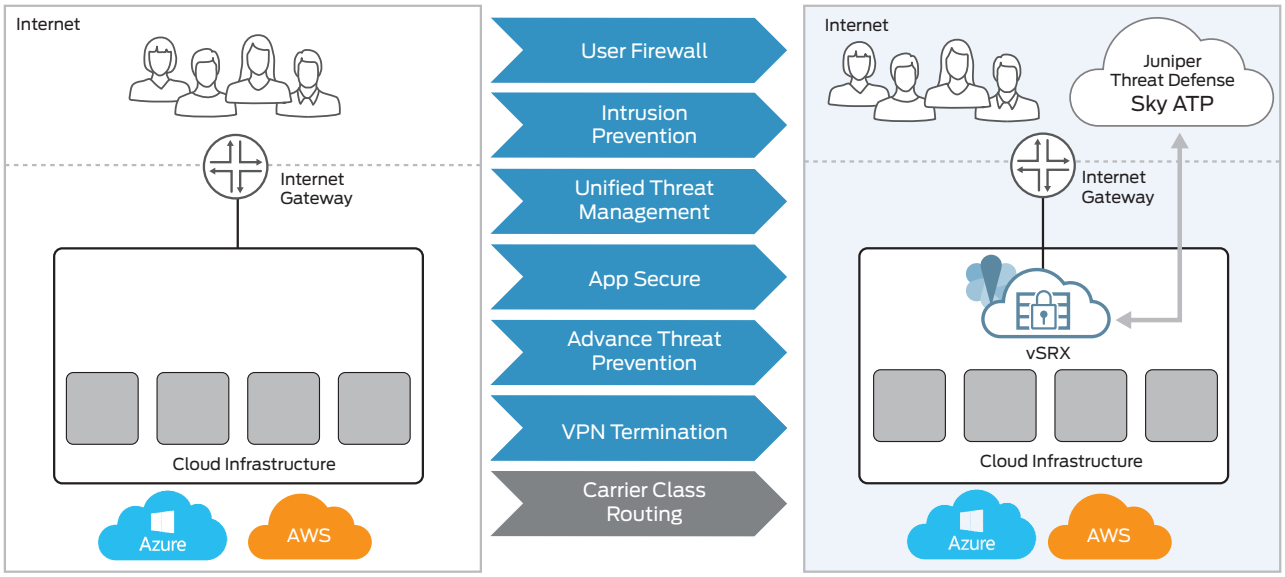

Figure 1: Juniper vSRX in a simple public cloud deployment (AWS/Azure)

Juniper's Solution for Securing and Simplifying Deployment in the Public Cloud (AWS and Azure)

Let's take a look at a simple AWS deployment comprising one virtual private cloud (VPC) with an Internet gateway and several EC2 instances to explore how the Juniper solutions deliver comprehensive security for the cloud. In a simple cloud deployment, a Juniper Networks vSRX virtual firewall can be easily incorporated between the Internet gateway and the VPC, facilitating comprehensive security, routing, and VPN services. Similarly, in a Microsoft Azure deployment, a vSRX can be added to the virtual network to facilitate VPN termination and advanced security services.

In a more complex cloud deployment, the vSRX can fill the roles of paid cloud features such as VPN gateways, NAT gateways, and VPC peering modules. Reallocating these tasks to the vSRX dramatically simplifies the topology, reducing the number of elements to manage and delivering better value for the customer.

Expanding Juniper Solution to Secure the Hybrid Cloud: Real-World Use Cases

The following section looks at the challenges and security requirements of two real-world use cases—Enterprise Expansion and Workload Distribution—and shows how Juniper solutions address both scenarios.

Simple and Secure Juniper Solutions for Enterprise Expansion and Workload Distribution

The following Juniper security solutions can be deployed to provide security for enterprise expansion and workload distribution use cases.

- A vSRX virtual firewall is installed in each AWS/Azure deployment to secure the instances and applications in the cloud. An SRX Series device/vSRX virtual firewall connects to the advanced threat defense system, Sky ATP, in the cloud and receives the latest threat information to help detect sophisticated malware.
- The vSRX is also used for IPsec VPN termination, multisite VPN, and NAT gateway functionality to facilitate and complement the AWS/Azure deployment.
- The vSRX gateways in the remote data center branches connect to the SRX Series firewalls at headquarters via IPsec VPN for secure data transportation.
- Junos Space Security Director centrally manages all security policies across the infrastructure. The vSRX virtual firewalls deployed in remote data centers register with Security Director, whether installed at headquarters or in the cloud.
- Once security policies are pushed to the remote vSRX devices, application data is synchronized across all data centers.
- New security policies are centrally added or updated from Security Director and deployed across all data centers.

Use Case 1: Enterprise Expansion Adding new branch offices to a different geography	Use Case 2: Workload Distribution Distributing workloads across geographical locations
A new e-commerce enterprise with a physical data center in San Francisco wants to expand its global presence and decides to open offices globally. • **Requirements:** - The company plans to add three new data centers—one each in Europe, APAC, and South America. - Employees must be able to access the company's internal resources from their region. - Customers need to be redirected to their respective regions. - Essential services such as mail, active directory, and file servers are replicated in all data centers, with data being synchronized in real time.	A new video-streaming enterprise anticipates more viewers in the U.S. east coast between 7 and 10 p.m. during November and December. Deploying a new physical data center or provisioning a virtual data center in a private cloud can be expensive to facilitate such intermittent usage. • **Requirements** - A high-quality user experience in a cost-efficient manner without compromising customer privacy is critical. - Content and customer data need to be replicated. - The data center must be able to scale higher or lower based on demand. - Loss of service due to any failures is unacceptable. - Leaking copyrighted content or customer details is unacceptable.

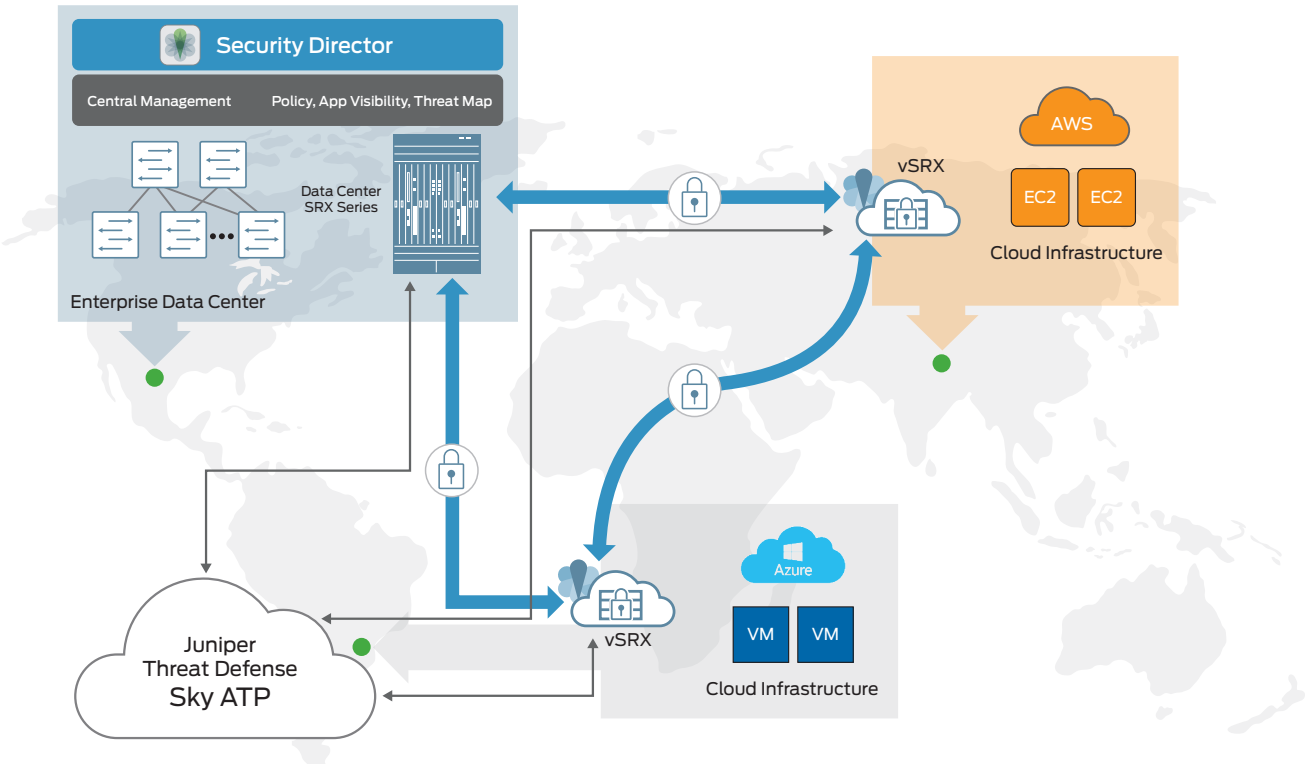

Figure 2: Juniper security solutions in a hybrid/multicloud deployment

Key Benefits Delivered by Juniper Security Solutions

Juniper security solutions deliver the following benefits in a public or hybrid cloud environment.

1. **Unified intelligent security**
   - The vSRX virtual firewall serves as a single point of enforcement. By leveraging security feeds from advance threat intelligence platforms in the cloud, such as Sky Advanced Threat Prevention, the vSRX can detect known and unknown threats while enforcing application security, intrusion prevention, and unified threat management.
2. **Centralized, simple, and intuitive management**
   - Junos Space Security Director provides intuitive and centralized management for monitoring security across entire network. The simple user interface means even new users can quickly become proficient. The mobile Security Director app, available for iOS and Android platforms, is accessible to security admins or CIOs who want to monitor security updates in their network remotely.
3. **Programmability**
   - With a wide range of programmatic APIs supported in Juniper Networks Junos operating system, DevOps resources can easily automate deployment and management activities through simple scripts, streamlining the entire workflow.
4. **Lower costs and shorter learning curves**
   - The ability to extend the familiar and well-known security policies used in the physical data center to private and public clouds is a critical benefit, allowing enterprises to leverage existing admins to manage cloud infrastructure. There is no need to hire new cloud experts.

Summary

Juniper Networks security solutions seamlessly extend across public and hybrid clouds without compromising flexibility and manageability. With highly evolved security intelligence and simple, centralized management and automation tools, Juniper makes it easy to monitor and enforce security across existing and new data centers.

Next Steps

For more information on Juniper Networks security solutions, please visit us at www.juniper.net/us/en/products-services/security and contact your Juniper Networks representative.

About Juniper Networks

Juniper Networks challenges the status quo with products, solutions and services that transform the economics of networking. Our team co-innovates with customers and partners to deliver automated, scalable and secure networks with agility, performance and value. Additional information can be found at Juniper Networks or connect with Juniper on Twitter and Facebook.

Corporate and Sales Headquarters
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or +1.408.745.2000
Fax: +1.408.745.2100
www.juniper.net

APAC and EMEA Headquarters
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: +31.0.207.125.700
Fax: +31.0.207.125.701

3510567-004-EN May 2017