Extending Enterprise Security to Public and Hybrid Clouds in Healthcare

Juniper Security for an Ever-Evolving Healthcare Industry

Challenge

The healthcare market is migrating toward public or hybrid clouds much faster than expected, 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 healthcare firms 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 enforces and monitors security across public and hybrid clouds
- Extends security policies and technologies used in physical data centers to public and hybrid clouds
- Reduces the number of proprietary, feature-limited public cloud elements to deploy and manage

The migration to the public cloud is accelerating rapidly. A HIMSS 2016 survey predicts healthcare is expected to follow the global market trend in rapid growth in moving to the public cloud. This rapid adoption is primarily attributable to the public cloud's ability to deploy across geographies, its flexibility and scalability, its pay-per-use model and lower upfront costs, and its simplicity. However, enterprises with heavy investments in private data centers and concerns about the feasibility of public clouds tend to favor a hybrid approach, leveraging a combination of public clouds and existing physical data centers and private clouds. Regardless of the approach, the move to the cloud creates real concerns about security that need to be addressed to ensure a successful migration.

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 a paradigm shift in security that must be addressed.

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

Public Cloud Security Challenges

The popularity of public clouds is driven, in large part, by the dynamics and realities of the startup world. In 2016, the economics of deploying a physical data center with a dedicated IT admin no longer makes economic sense for most startups and small enterprises. Instead, they typically go with one of the more popular cloud platforms, deploy their infrastructure, and hire a DevOps resource in place of a traditional IT/security administrator.

While DevOps resources offer a mix of development and operational experience, they typically lack the deep security knowledge of traditional security administrators. 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 person and a serious requirement for any security platform.

Hybrid Cloud Security Challenges

Healthcare firms 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. Also, some healthcare firms 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 risking discrepancies between the physical data center and the cloud. Additionally, hiring cloud professionals or training existing IT 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 solutions that work together to solve the cloud security issue. The major elements of this solution are:

- Juniper Networks® SRX Series Services Gateways and Juniper Networks vSRX virtual firewall with integrated 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) to detect and block network intrusions
  - User-aware firewalls to analyze, log, and enforce access control based on user roles and groups
  - Application control and visibility with integrated Juniper Networks AppSecure 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 at the gateway
  - Support for Linux KVM, VMware, and AWS platforms (vSRX)
- Juniper threat defense, security intelligence in the cloud composed of Spotlight Secure threat intelligence and Juniper Networks Sky Advanced Threat Prevention.
- Spotlight Secure threat intelligence aggregates threat feeds from multiple sources to deliver open, consolidated, actionable intelligence to SRX Series firewalls. Spotlight Secure provides an open platform to deliver threat feeds to SRX Series and vSRX virtual firewalls for instant enforcement.
- Sky Advanced Threat Prevention is a cloud-based advanced anti-malware service with dynamic analysis (sandboxing) to protect against sophisticated unknown and "zero-day" threats. Integrated with SRX Series and vSRX virtual firewalls, Sky Advanced Threat Prevention provides a machine learning to improve verdict accuracy.
- 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. Security Director includes a customizable dashboard with detailed drill-downs, threat maps, and event logs, providing unprecedented visibility into firewall performance. It is also available as a mobile app for Google's Android and Apple's iOS systems to enable remote mobile monitoring.

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

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

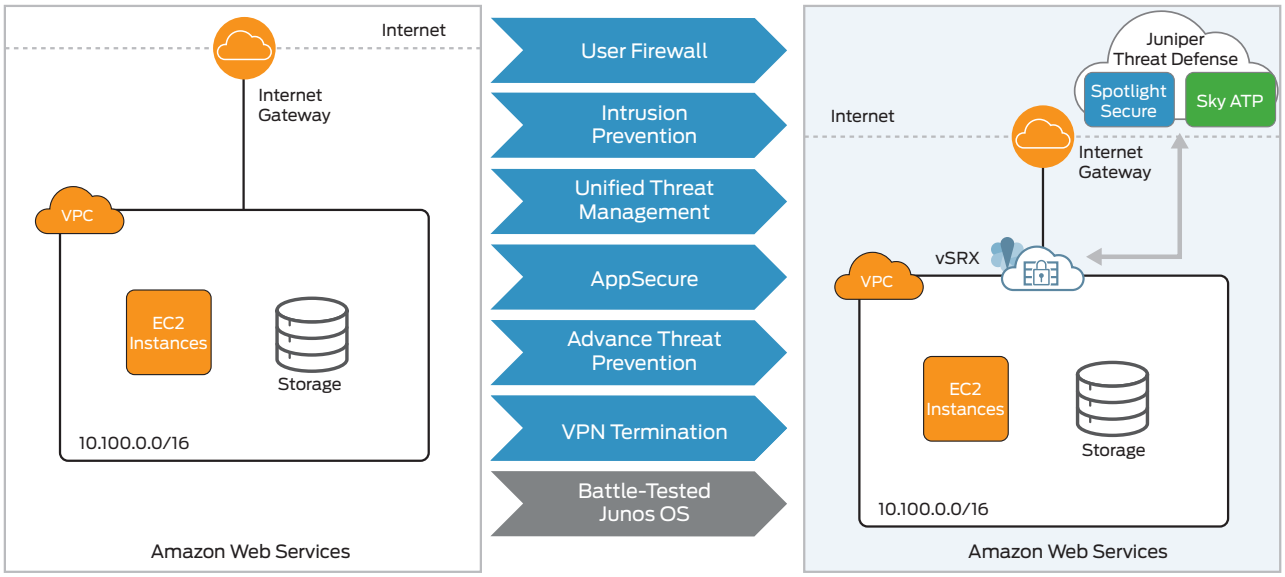

Figure 1: Simple vSRX deployment on AWS with one VPC

deployment, a Juniper Networks vSRX virtual firewall can be easily incorporated between the Internet gateway and the VPC, facilitating comprehensive security and VPN services.

In a more complex AWS deployment, a vSRX reduces the need for dedicated hardware components, consolidating them for easier management. Take, for example, an enterprise with multiple departments and hundreds of employees logging in to access infrastructure resources via a dedicated VPN. Some of the departments need to share resources while others don't. In AWS, intercommunication between VPCs requires a dedicated peering module. By default, all IP addresses within a VPC are in the private space (10.X.X.X). Internal resources wanting to access the public Internet require a dedicated NAT module for each VPC. In contrast, a vSRX on AWS can handle the task of VPN termination, NAT, and intercommunication between VPCs with multisite VPN (which is currently missing in AWS), dramatically simplifying the topology and reducing the number of elements to manage while enabling secure and granular control between VPCs (see Figure 2).

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—Expansion and Acquisition as well as Workload Distribution—and shows how Juniper solutions can address both the scenarios.

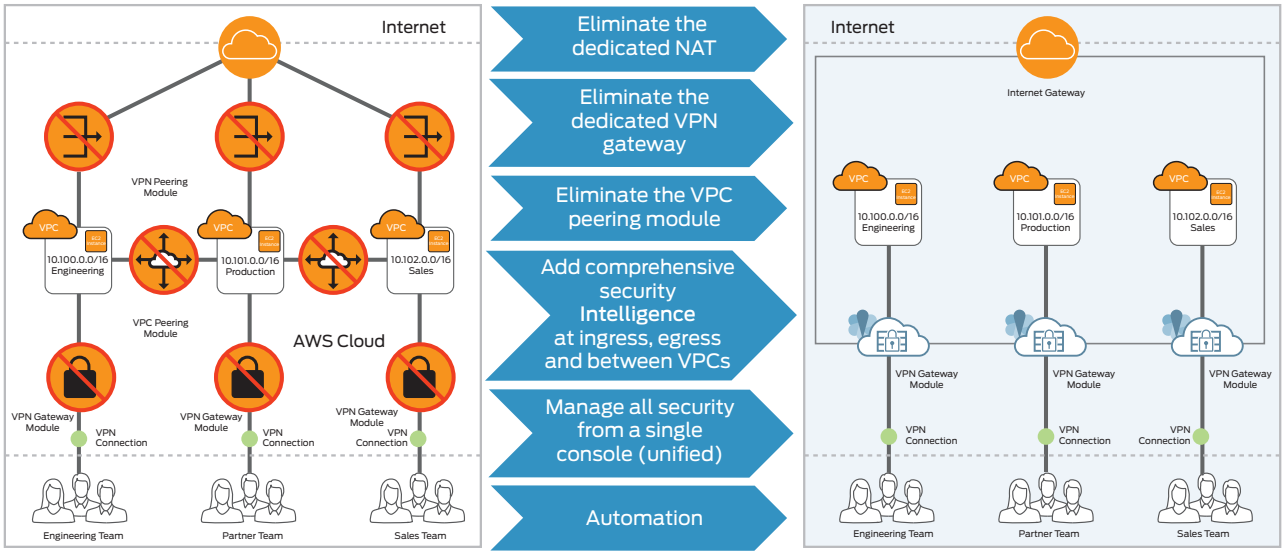

Figure 2: Comprehensive AWS deployment with multiple VPCs

Use Case 1: Healthcare Firm Expansion and Acquisition Adding new offices to a different geography	Use Case 2: Workload Distribution Distributing workloads across geographical locations
A healthcare provider with a physical data center in Colorado wants to expand its presence and decides to acquire another provider in the Midwest. • **Requirements:** - The company plans to consolidate several data centers into three — one each in the Midwest, the Mountain West, and Southwest. - Employees must be able to access the company's internal resources from their region. - Patients need to be redirected to their respective regions. - Essential services such as mail, active directory, file servers, and patient portals are replicated in all data centers, with data being synchronized in real time.	A new healthcare content video-streaming service anticipates more viewers in the U.S. East Coast between 7:00 and 10:00 PM. 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 patient experience in a cost-efficient manner without compromising patient privacy is critical. - Content and patient 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 patient details is unacceptable.

Simple and Secure Juniper Solutions for Enterprise Expansion and Workload Distribution

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

- A vSRX virtual firewall is installed between the VPC and Internet gateway of each AWS deployment to secure the instances and applications in the VPC. An SRX Series device/vSRX virtual firewall connects to the advanced threat defense system in the cloud and receives the latest threat information to help detect unknown or zero-day attacks.
- The vSRX is also used for IPsec VPN termination, multisite VPN, and NAT gateway functionality to facilitate and complement the AWS deployment.
- The vSRX gateways in the remote data center branches connect to the SRX Series firewalls in the head office 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.

Key Benefits Delivered by Juniper Security Solutions

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

1. Enforcement point leveraging intelligent security
   - The vSRX virtual firewall serves as an intelligent 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, unknown, and zero-day 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 theentire 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.

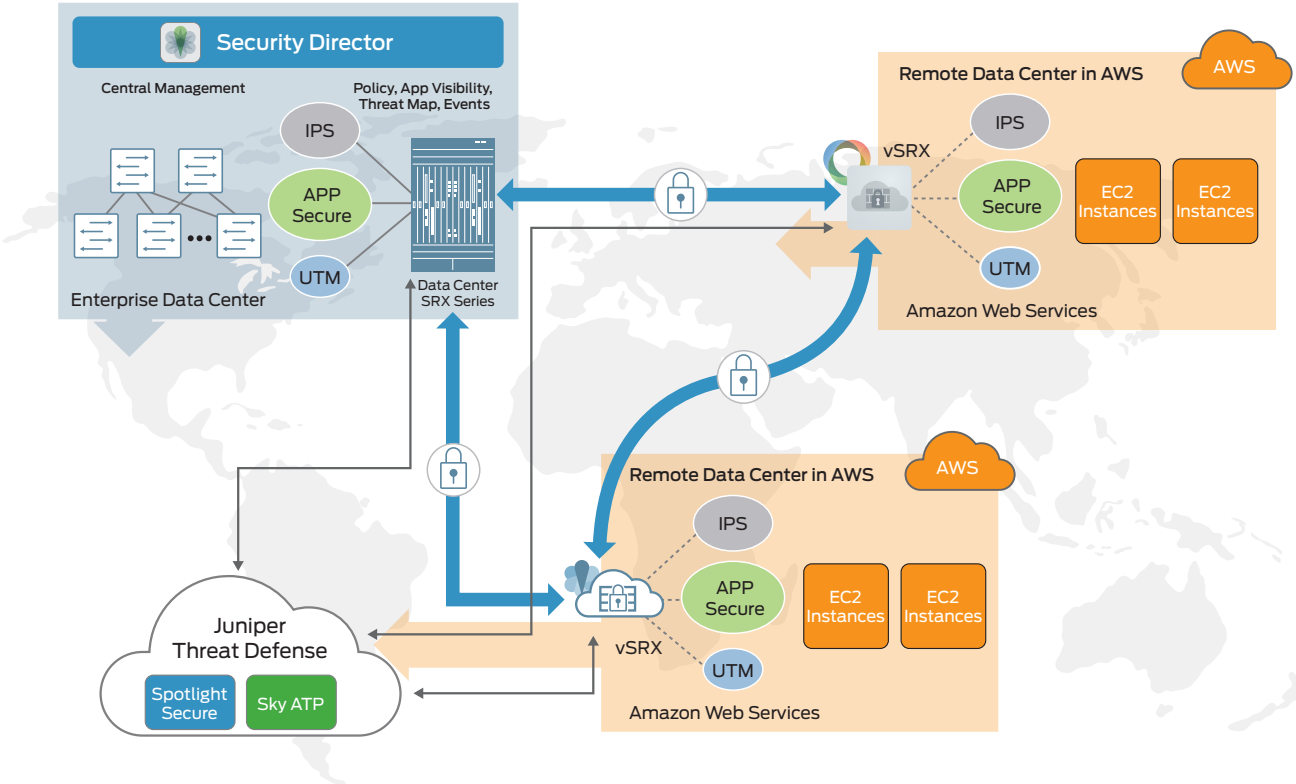

Figure 3: Juniper security solutions deployed in a hybrid cloud for the healthcare firm expansion and workload distribution use cases

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 IT admins to manage cloud infrastructure. There is no need to hire new cloud experts as your firm moves to the cloud.

Summary

Juniper Networks security solutions seamlessly extend across public and hybrid clouds without compromising flexibility and manageability. With highly evolved security intelligence and new 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

3510596-001-EN Nov 2016

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

3510596-001-EN Nov 2016