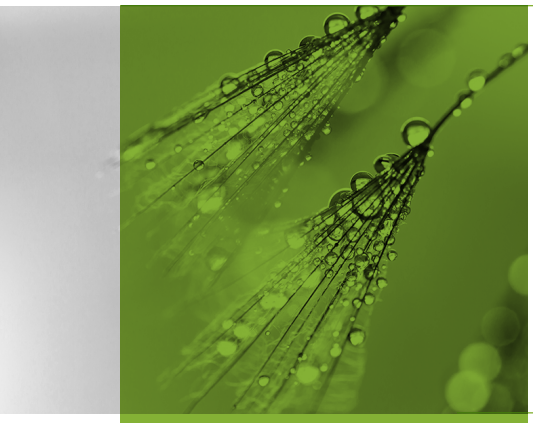

ADVANCED SECURITY SERVICES FOR CLOUD-DELIVERED MISSIONS

Scale and secure your hybrid and private clouds

Challenge

AWS environments must be able to connect multiple VPCs in different regions and deploy next-generation firewalls (NGFWs) and advanced malware and threat remediation services to secure the VPCs. Native AWS modules provide limited connectivity and lack VPN and advanced security initiation capabilities.

Solution

A transit VPC or full-mesh VPN solution using next-generation vSRX Virtual Firewalls with Juniper Sky ATP delivers advanced connectivity and enhanced security in AWS deployments.

Benefits

- *Enables connectivity between VPCs*
- *Enforces security policies between VPCs and inbound-outbound traffic*
- *Implements next-generation firewall services in VPCs*
- *Secures VPN deployments with compliant advanced security services offering malware and threat intelligence from Juniper Sky ATP*
- *Reduces complexity and enables large-scale deployments*
- *Provides centralized management*

The basic building block of data centers in an Amazon Web Services (AWS) environment is a virtual private cloud (VPC), which acts as a virtual data center in the cloud. Migrating from a traditional data center to a cloud-delivered mission services environment while ensuring security, compliance, and visibility into multi-VPC deployments within AWS is a significant challenge.

The Challenge

Securing mission-critical application workloads with real-time inline protection is difficult and lacks visibility into migration and operations within a cloud environment.

When data no longer resides behind an on-premises firewall, as is the case with public and hybrid clouds, it introduces new risks that must be addressed. Additionally, as customers adopt a hybrid cloud approach to ensure access to best-of-breed solutions, the need to centrally manage security policies is more critical than ever.

Amazon Web Services (AWS) places a significant emphasis on security, and Juniper Networks delivers advanced L7 security features such as application firewall, intrusion prevention system (IPS), security intelligence (SecIntel), and advanced threat prevention (ATP) to provide customers with comprehensive security for their AWS deployments. This solution also addresses the needs of traditional physical deployments whose security administrators want to extend their policies to public or hybrid cloud deployments.

The Juniper Networks AWS Security Solution

Juniper Networks offers solutions that overcome the native AWS limitation on multi-VPC connectivity while providing advanced security with Security Technical Implementation Guide (STIG)-compliant security services delivered to transit VPC deployments that comply with on-premises data center and cloud workload requirements.

Transit VPC Solution

Juniper's transit-secure VPC solution lets operators seamlessly add NGFW services and connectivity to both large and small multi-VPC AWS deployments. This model, recommended by AWS, uses Juniper Networks® vSRX Virtual Firewall to provide higher level integrated security and high-performance routing capabilities. The transit VPC solution uses a hub-and-spoke topology where every VPC connects to a special "transit VPC" that serves as a central hub for internal traffic, on-premises data centers, or the Internet.

Deploying a vSRX Virtual Firewall in the transit VPC delivers NGFW services (IDS/IPS, application firewall, and advanced threat prevention) to the VPCs, as well as secure connectivity and routing between them. The BGP routing protocol, used over IPsec VPN service (VPNS), facilitates dynamic routing between VPCs, dramatically simplifying network management and minimizing the number of connections needed to connect networks across VPCs and the physical corporate data center.

Juniper Sky ATP Solution

Juniper Sky™ Advanced Threat Prevention leverages Juniper Networks SRX Series Services Gateways and a cloud-based service component for all management, configuration, and reporting.

Juniper Sky ATP's progressive pipeline analysis engine performs a real-time cache lookup against a database of known threats, blocking malicious content inline. Suspicious files are subjected to a series of deep inspection steps that attempt to positively identify malware. Static analysis, combined with processing through multiple antivirus engines, attempts to identify the threat; if further analysis determines that the file is malware, its signature is added to the cache to ensure immediate identification of recurring threats in the future.

Dynamic analysis is performed in a sandbox environment, where threats are "detonated" and observed. Unique deception techniques elicit malware response and self-identification. Particularly elusive threats discovered at a more extensive analysis stage are identified, logged, and reported, and are easily mitigated by security operations staff. Infected hosts are automatically isolated and blocked from outbound network access by delivering an "infected host" feed to the SRX Series firewall.

Juniper Sky ATP maintains a list of compromised endpoints as data feeds (also called information sources) that include the IP address or IP subnet of the infected host, along with a threat level and recommended action. You can create security and apply policies that automatically perform enforcement actions on traffic entering or leaving these infected hosts. Juniper Sky ATP uses multiple indicators of suspicious behavior, such as a client attempting to contact a Command and Control (C&C) server or a client attempting to download malware, and it applies a proprietary algorithm to determine the infected host's threat level.

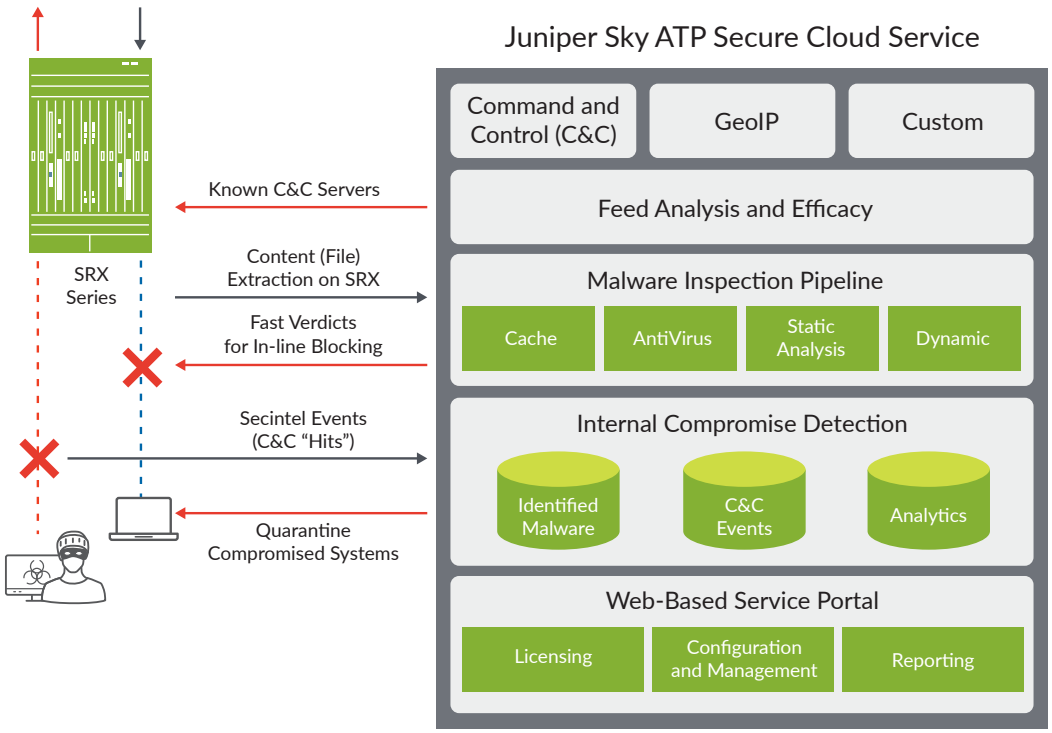

Figure 1: Juniper Sky ATP architecture

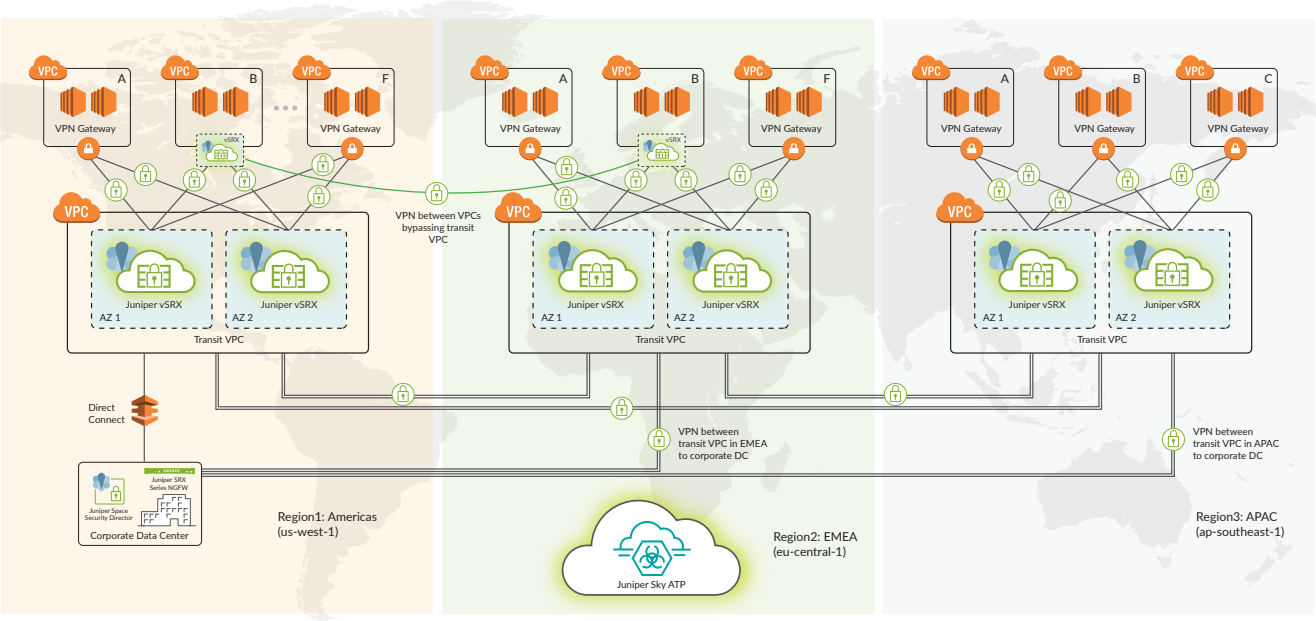

Figure 2: Juniper Sky ATP securing AWS transit VPC

Features and Benefits

- **Integrated security**: The vSRX Virtual Firewall is the only platform that can offer NGFW services, as well as routing and carrier-grade IPsec capabilities, on a single instance. This eliminates the need for switched port analyzer (SPAN) ports and multiple elements that add complexity to the deployments.
- **High-performance routing**: AWS allows 100 spoke VPCs to connect to a central transit VPC. The vSRX can support up to 128 virtual routing and forwarding (VRF) functions, providing the scale needed to take full advantage of a transit VPC deployment.
- **Centralized management and granular policies**: Juniper Networks Junos Space® Security Director provides intuitive and centralized management to configure and monitor security policies across the entire network. Each VPC can have a unique security policy, allowing granular control based on roles and responsibilities.
- **Ease of deployment**: Juniper's transit VPC solution can be easily deployed within minutes in an AWS environment using CloudFormation templates. A full-mesh VPN is easily deployed via Junos Space Security Director or through automation.
- **Lower licensing costs and TCO**: Pricing for the vSRX software licensing on the AWS marketplace is lower than similar competitive offerings. Also, the vSRX consumes significantly fewer AWS resources, which translates into lower operating costs.

Summary—Juniper Delivers Full Security Solution for AWS Deployments

Juniper Networks transit VPC and full-mesh VPN solutions can easily deliver secure connectivity, routing, and NGFW services in large, complex AWS deployments. This enables connectivity between VPCs and enforces security policies between VPCs and inbound-outbound traffic, implementing next-generation firewall services, reducing complexity, enabling large-scale deployments, and providing centralized management.

Next Steps

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

About Juniper Networks

Juniper Networks brings simplicity to networking with products, solutions and services that connect the world. Through engineering innovation, we remove the constraints and complexities of networking in the cloud era to solve the toughest challenges our customers and partners face daily. At Juniper Networks, we believe that the network is a resource for sharing knowledge and human advancement that changes the world. We are committed to imagining groundbreaking ways to deliver automated, scalable and secure networks to move at the speed of business.

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