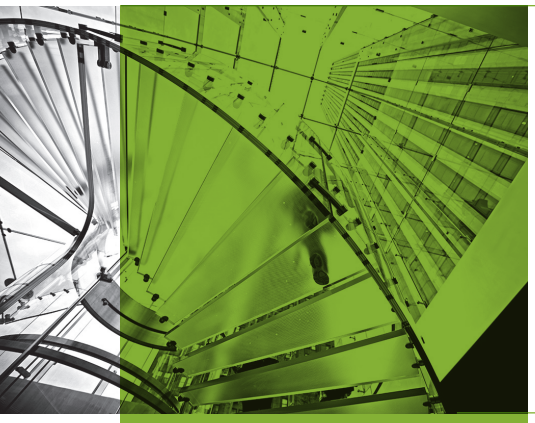

# EASILY CONNECT AND DELIVER NGFW SERVICES IN AWS MULTI-VPC DEPLOYMENTS

*Scale and secure your virtual private clouds*

***Challenge***

*AWS deployments that employ multiple VPCs need to easily connect them in different regions, and deploy enterprise network firewall and other shared services on the VPCs. Native AWS modules, however, are limited to providing basic connectivity within a single region and lack VPN initiation capabilities.*

***Solution***

*A Transit VPC or Full-Mesh VPN solution using the next-generation vSRX Virtual Firewall enables advanced connectivity and enhanced security in AWS deployments.*

***Benefits***

- *Enables connectivity between VPCs*
- *Enforces security policies between VPCs and inbound-outbound traffic*
- *Implements NGFW services in VPCs*
- *Reduces deployment complexity and enables large-scale deployments*
- *Provides centralized management*

*The basic building block of a data center in an Amazon Web Services (AWS) environment is a virtual private cloud (VPC), which essentially acts as a virtual data center in the cloud. Most AWS deployments evolve from a single VPC to multiple VPCs spread across numerous regions as the enterprise expands. The desire for data centers to be closer to end users, segmenting resources and tasks for which they are responsible, are common across most enterprises. However, with multi-VPC deployments, enabling connectivity between VPCs requires explicit peering using VPC peering modules, which are restricted to peering VPCs within a single AWS region and do not possess the ability to granularly filter or control traffic flowing between VPCs.*

## The Challenge

Adding VPC peering modules to enable connectivity between VPCs can often get complicated, adding considerable management overhead. Most AWS deployments also need next-generation firewall (NGFW) services in their VPCs to protect the cloud infrastructure it is hosting.

## The Juniper Networks Solution

Juniper Networks offers solutions that solve the native AWS limitation on multi-VPC connectivity while providing advanced security. These include:

1. Transit VPC, which is designed for larger deployments with AWS management roles distributed between many teams.
2. Full-Mesh VPN, which is designed for smaller deployments managed by a centralized DevOps team and requiring fewer hops, lower latency, and easier troubleshooting.

## Transit VPC Solution

Juniper's Transit VPC solution allows enterprises to seamlessly add NGFW services and connectivity to large multi-VPC AWS deployments. This deployment model, recommended by AWS, uses Juniper Networks® vSRX Virtual Firewall to move to the next level with integrated security and high-performance routing capabilities. The Transit VPC solution utilizes a hub-and-spoke topology where every VPC connects to a special "transit VPC" that serves as a central hub for internal traffic, as well as external traffic sent to the corporate on-premise data center or the Internet.

In this model, shared services are hosted in the transit VPC. Deploying a vSRX Virtual Firewall in the transit VPC delivers NGFW services (IDS/IPS, application firewall, advanced threat prevention) to the VPCs, as well as secure connectivity and routing between them. The BGP routing protocol is used over IPsec VPN service (VPNS) to facilitate dynamic routing between the various VPCs. This deployment mode dramatically simplifies network management and minimizes the number of connections needed to connect different networks across VPCs and the physical corporate data center.

When expanded to a hybrid cloud deployment with a corporate data center, a "direct connect" can be used to provide simple and direct connectivity between the corporate data center and the cloud data center on AWS. Backup VPN tunnels are established over the Internet between the corporate data centers and the vSRX in the transit VPC to facilitate redundancy. vSRX Virtual Firewalls are typically deployed in "Availability Zones" (AZs)—isolated locations within an AWS region—to deliver redundancy.

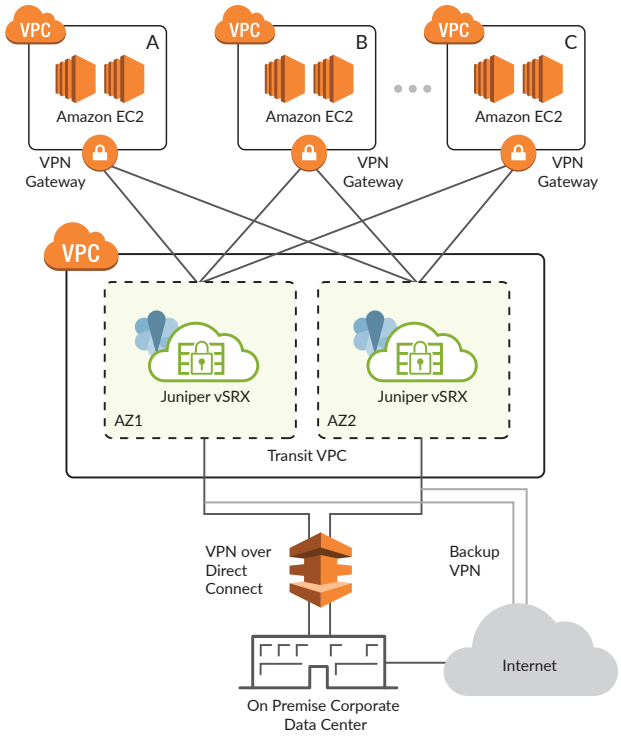


*Figure1: Transit VPC deployment in a hybrid cloud (single region)*

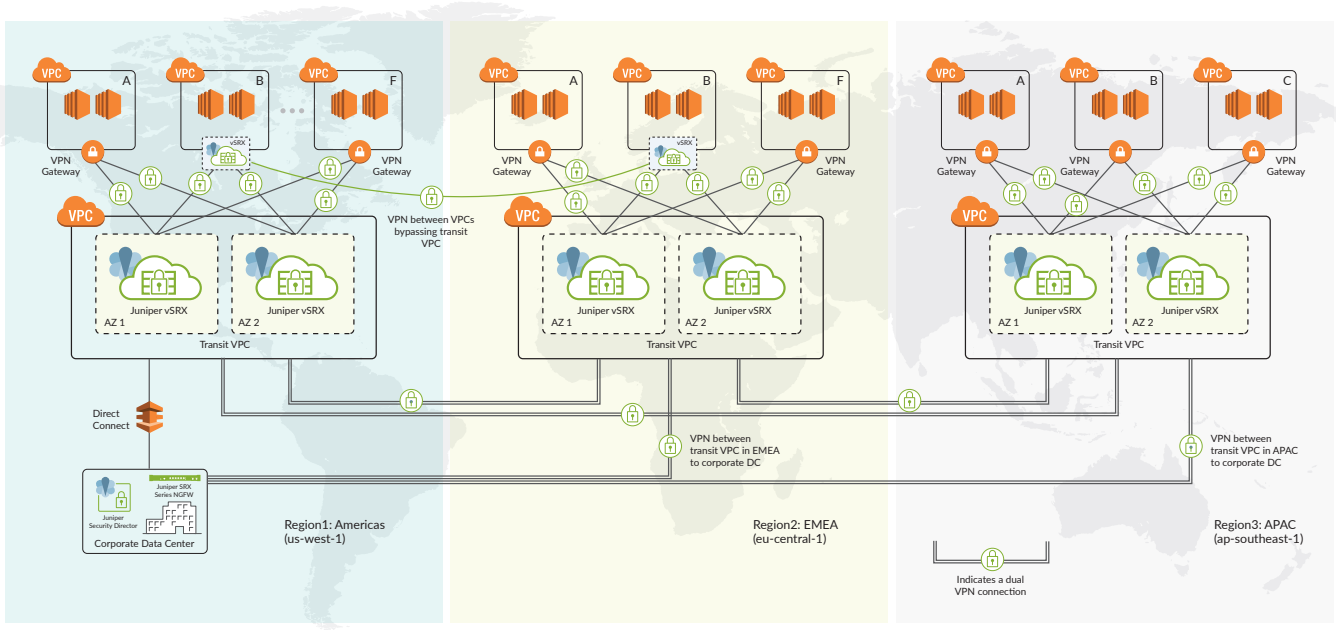


*Figure 2: Transit VPC deployment in a multi-region hybrid cloud deployment*

"CloudFormation" is a service on the AWS platform that manages orchestration and infrastructure using templates that describe all AWS resources that will be needed to provision and configure the deployment. Juniper offers an AWS CloudFormation template for Transit VPC deployments that helps customers deploy this solution in a matter of minutes within their AWS cloud data centers. Provisioning this template creates the necessary AWS modules such as VPC Classless Interdomain Routing (CIDR), subnets, Internet gateway, security groups, vSRX instances, Lambda functions, CloudWatch logs, and CloudWatch trigger rules. Lambda is a serverless compute service on the AWS platform that can be triggered by events that occur in that platform, such as adding a new VPC to the deployment. The Lambda functions created as part of this template handle polling for new AWS Virtual Gateways (VGWs) and initiate VPN connections from the vSRX to the VGWs. In the cloud formation template provided by Juniper, AWS VGWs are incorporated into each VPC to establish a secure VPN connection to the vSRX firewalls in the shared VPC. The vSRX can also be used in place of the AWS VGWs to facilitate a similar solution.

The Transit VPC supports several important use cases:

- Private Networking: Users can build a private network that spans two or more AWS regions.
- Shared Connectivity: Multiple VPCs can share connections to data centers, partner networks, and other clouds.
- Cross-Account AWS Usage: VPCs and the AWS resources within them can reside in multiple AWS accounts.

For enterprises with large deployments in multiple regions, the same solution can easily scale to support a global transit network (see Figure 2). The enterprise may have both physical and AWS deployments in some regions and only AWS data centers in others. In those scenarios, all transit networks across the various regions can be connected to the headquarters as well as to each other over IPsec VPNs to facilitate this secure global transit network. Running BGP enables shared services in each region and dynamic routing between them. In cases where VPCs in one region must keep data in sync with VPCs in other regions—for instance, financial data shared between finance teams in the Americas and Europe—vSRX firewalls can be deployed in those locations and optionally bypass the transit network to establish secure channels between them via VPN connections.

In most large organizations, every team would typically prefer to define and maintain their own AWS resources and security policies. By using a vSRX in each VPC, unique security policies can be easily enforced at the VPC level—a critical requirement when the responsibilities are distributed between different teams.

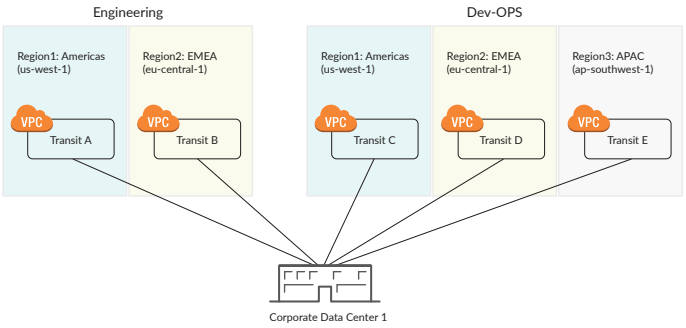


*Figure3: Transit VPC deployment managed by different teams*

## Full-Mesh VPN Solution

An alternative to the Transit VPC solution is the Full-Mesh deployment in which every VPC is connected to every other VPC by secure VPN connections. In this deployment, a pair of vSRX virtual firewalls reside on each VPC and connect to the vSRX firewalls on every other VPC, enabling secure connectivity and advanced security between them. This deployment provides the key benefit of enabling granular security policies for each VPC and delivering a truly global deployment solution that is not limited by AWS regions. Also, by skipping a central hub, the Full-Mesh deployment model reduces the number of hops in the network, resulting in lower latency and fewer potential bottlenecks. By using Juniper Networks Junos Space® Security Director, all vSRXs across different VPCs and remote networks, regardless of AWS regions or accounts, can be easily managed from a single, centralized pane-of-glass manager.

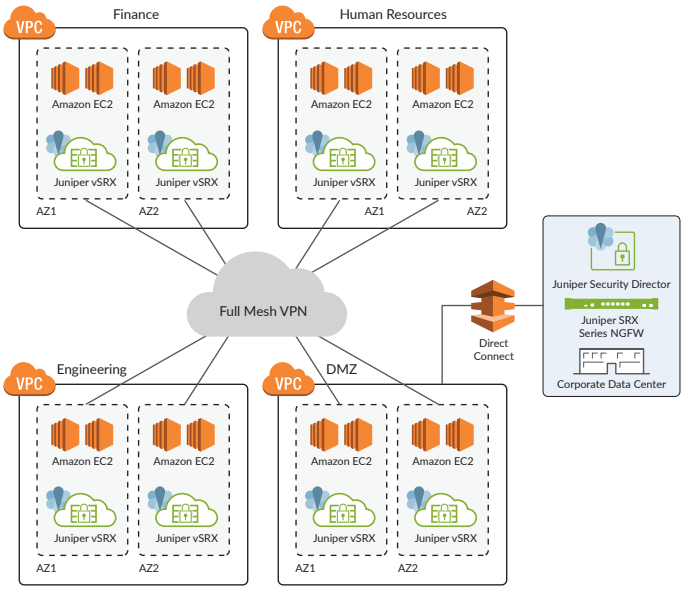


*Figure 4: Juniper Full-Mesh VPN solution*

## Key Benefits

- **Integrated security:** vSRX Virtual Firewall is the only platform that can offer NGFW services, in addition to the routing and carrier-grade IPsec capabilities on a single instance. This eliminates the need for Switched Port Analyzer (SPAN) ports and multiple elements which add complexity to the deployments.
- **High-performance routing:** AWS allows for 100 spoke VPCs to connect to a transit VPC. vSRX can support 128 virtual routing and forwarding (VRF) functions, which support the scaling requirement needed to take full advantage of a transit VPC deployment.
- **Ease of deployment:** Juniper's Transit VPC solution can be easily deployed within minutes in an AWS deployment using CloudFormation templates, while a Full-Mesh VPN can be easily deployed via Security Director or through automation.
- **Centralized management and granular policies:** 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.
- **Lower licensing costs and TCO:** vSRX software licensing costs on the AWS marketplace are lower than similar offerings from competitors like Cisco, Palo Alto Networks, and Check Point. Also, the vSRX consumes significantly fewer AWS resources, which translates to lower operating costs.

## Summary

Juniper Networks Transit VPC and Full-Mesh VPN solutions can easily deliver secure connectivity, routing, and NGFW services in complex or large AWS deployments.

### 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

Juniper Networks | Engineering Simplicity