Secure Cloud Connectivity for Virtual Private Networks

Field trial with Third Party DWDM system

Table of Contents

Executive Summary

Cloud-based solutions have taken center stage for enterprises as they prepare to roll out new applications and services, and they are challenging the traditional way network services are designed and delivered. Security, performance, and reliability are key concerns when it comes to any cloud service, with enterprise IT owners demanding the same level of security, performance, and reliability as achieved with VPNs. This situation creates an opportunity for innovative service providers to deliver secure and reliable cloud network access via VPNs by offering connectivity to multiple public cloud providers. Service providers' secure cloud connectivity provides enterprises with the ability to leverage several cloud provider solutions while still experiencing the same high performance, reliability, and security similar to enterprise VPN networks.

This paper describes how secure connectivity to public cloud networks provided by the service provider can address the security, performance, and reliability needs of enterprise customers as they deploy large-scale cloud services. Juniper Networks, as an industry networking leader, offers enhanced and open standards-based SDN and Network Function Virtualization (NFV) solutions to meet the networking service needs of the service provider, the public cloud provider, and the enterprise business.

Introduction

Over the last few years, the hybrid/public cloud computing model has gained increased acceptance in the enterprise business community as a means to provide quick, low-cost, and scalable services. The availability of SaaS, PaaS, IaaS, and many other variant services from the cloud offers flexible choices that meet varying business needs. The key driver for cloud adoption is the ability to provide "always-on access to applications" with increased application availability at a large scale, in a quick and secure fashion, and at an overall reduced cost.

Merging Secure Private Networks with the Cloud

The agility and scale of today businesses means providing enterprise-grade network services when deploying cloud-based solutions.

Enterprise network owners do not compromise on security, latency, reliability, and performance when deploying cloud-based solutions.

Service providers have the opportunity to deliver new world cloud-based managed services.

Enterprise IT owners worldwide use VPNs to meet the connectivity needs of their businesses with security, performance. and availability. As these enterprise owners look to deploy cloud-based solutions more extensively, they expect a similar experience; in essence, they are looking for enterprise-grade network services when connecting to the public cloud. However, many businesses connect to public cloud providers over the Internet. Recent industry research[1] indicates that security, reliability, low latency, and predictable performance are priorities for enterprise business owners as they build private clouds or deploy a hybrid cloud model.

Service providers have an opportunity to address some of the service gaps that exist in the public cloud services chain today. Services that extend the performance metrics of their VPN, offering to provide connectivity to the hybrid/public cloud infrastructure, are desperately needed by performance-conscious enterprise organizations. Consequently, service providers are looking at ways to define and deliver managed services in this new agile and open, multivendor services driven-market. On the technology side there are several innovative solutions surfacing on the market to meet the virtualized, on-demand availability and growth needs of the enterprise. As the demand grows for open and agile solutions on a large scale, virtualizing the network, storage and compute resources in an integrated fashion have become a critical need. Today's network architecture experts are stepping up to integrate increased virtualization in an effort to improve the time to market for service delivery in a dynamic and automated environment.

This paper reviews how service providers can leverage their deployed physical architecture with Juniper and seamlessly integrate virtual solutions with SDN and service chaining with NFV as they apply to offering a secure cloud interconnect service over a VPN and support the enterprise's IT needs with a hybrid cloud model.

Network Transformation

Network Design Trends

Business model transformation continues to drive network and service innovation. Service providers have continually adapted and evolved their service portfolio in a competitively fierce and dynamic market. Their networks have evolved from supporting POTS (plain old telephone service) to Internet-age distributed applications that require packet transport. For the last few decades, the trend of network consolidation to deliver many services on one network has been the defining force for network architecture and services. Accelerated global demand for mobile communications over the years has also driven service providers to continually evolve and upgrade network capacity and services to deliver high-speed, low-latency, and highly reliable solutions. Over the same period, enterprise businesses have made

[1] IDG survey report [70% respondents say No 1 barrier to deploying cloud solutions in security concern] www.idgenterprise.com/report/idg-enterprises-cloud-computing

major investments in building in-house IT infrastructure and a supporting VPN to meet their ever-increasing information needs. Traditional outsourcing meant using managed services and network resources from service providers while outsourcing application development and maintenance for compute and storage needs from IT integrators. Today's distributed application-driven service trends have resulted in IT transformation that fundamentally needs the network platform to evolve to be simple, open, and agile. The virtualization benefits seen in compute and storage resources models have led to large geographically distributed virtual data centers. For networks to elastically adapt to the virtualized compute and storage resources in the data center, the next wave of innovation must focus on bringing virtualization to a much larger scale in the network design and operations.

Carrier-Class VPN to Cloud Evolution

Service provider networks designed for carrier-class availability, predictable performance, and latency are the connectivity foundation of enterprise networks large and small. These networks use varied forms of network virtualization to realize the benefits of resource pooling and network efficiency. Network virtualization can be at a link, device, and service level such as with Layer 2 MPLS and Layer 3 VPNs. Enterprise businesses lease virtual private links and network resources to build large-scale global VPNs. MPLS technology has been around for over a decade now, and MPLS-based VPNs are simple to implement, very scalable, and provide high performance along with low latency. Additionally, the security of these VPNs is unquestioned and something business customers have come to not only expect but assume. There has been a change, though, as today's enterprise customers look for complete IT solutions to meet the business agility needs at reduced cost. With the huge success and expanse of virtualized data centers and the low-cost availability of infrastructure, platforms, and applications as a service, enterprises look more and more at hybrid cloud-based solutions.

The network is a key infrastructure component of the overall hybrid cloud solution. Today, enterprise customers have to exit their VPN and use the public Internet to connect to a public cloud provider. In some cases, the public cloud provider can lease network resources from multiple service providers to connect a large enterprise's private clouds to its public cloud environment, creating hybrid cloud environments. The mixed solution poses potential issues in several areas, such as the following:

Security—Customers might not have a choice to devise or influence the security policies for their traffic flows in the public cloud or dictate the level of segregation of their applications from other tenants. Traditional security solutions have neither visibility into the traffic and virtual machine (VM) within the cloud, nor the ability to scale, preventing them from addressing the security needs of the underlying network and thereby exposing security risk.

Performance and Latency—Tunneling internal cloud traffic to an external firewall results in higher latency and affects the cloud performance, and the use of tunneling over the Internet reduces actual bandwidth availability. Internet latency is highly unpredictable as there are no SLA guarantees. While access to public cloud services can be acceptable for non-critical business applications, the enterprise customer needs predictable bandwidth availability and latency and expects a certain level of application performance for business-critical applications.

Reliability—For enterprise businesses to run critical applications in the public cloud, they need always-on access to applications with network reliability and availability similar to that available with carrier-class enterprise VPNs.

The enterprise business also has to work with multiple vendors to deploy hybrid cloud solutions. With the myriad of cloud solutions available and emerging, most medium to large business are expected to use a multitude of cloud solutions. By providing a secure and reliable cloud connection to many public cloud service providers, the communication service provider can help streamline and bring some consolidation into the cloud services chain. This consolidation not only streamlines service delivery but also impacts fault isolation and recovery in the event of failures along the services chain.

Network Agility with Virtualized Cloud Platform

Service providers are also looking at network virtualization solutions to increase network service agility and to reduce order-to-bill times resulting in a shorter time to revenue. The network security and performance gaps in hybrid cloud-based solutions pose a real opportunity for offering VPNs that extend to the public cloud or cloud VPNs that connect the enterprise private cloud to public cloud providers. This is also one domain where service providers are perfectly poised to provide a highly valued service and are looking to leverage SDN and NFV solutions to deliver this service.

Enabling Secure Cloud Connectivity

There can be many ways to integrate virtualized solutions to deliver secure public cloud connectivity to enterprise business customers. This section looks at how one service provider is seeking to introduce this service to its customers and integrate virtualized network functions to deliver scalable and customized managed services in a non-disruptive fashion.

The solution deployment is discussed in two main parts, with the first phase primarily for laying the foundation for secure hybrid cloud with the deployed physical architecture. The second phase is integrating a virtual firewall with Juniper Networks® Contrail Controller for enhanced agility, simplicity, and scalability. This phase also allows the service provider to be able to service-chain new network functions in the future and deploy customized solutions for the varying needs of its enterprise customers.

Phase 1: Adapting Physical Architecture for Cloud Connectivity

Service providers are perfectly positioned to provide the much-needed secure hybrid cloud connectivity to their enterprise VPN customers. Current network architecture optimized for maximum performance with physical workloads can easily be adapted to extend the VPN functionality to the cloud. With the extensively deployed Juniper Networks MX Series 3D Universal Edge Routers and leading-edge Juniper Networks SRX Series Services Gateways, a service provider can intelligently enable NNI connections to the cloud. And using standards-based MP-BGP peering with the cloud provider, the service provider can route critical business traffic over secure private links to various public cloud providers. Figure 1 shows a high-level architecture for secure public cloud connectivity.

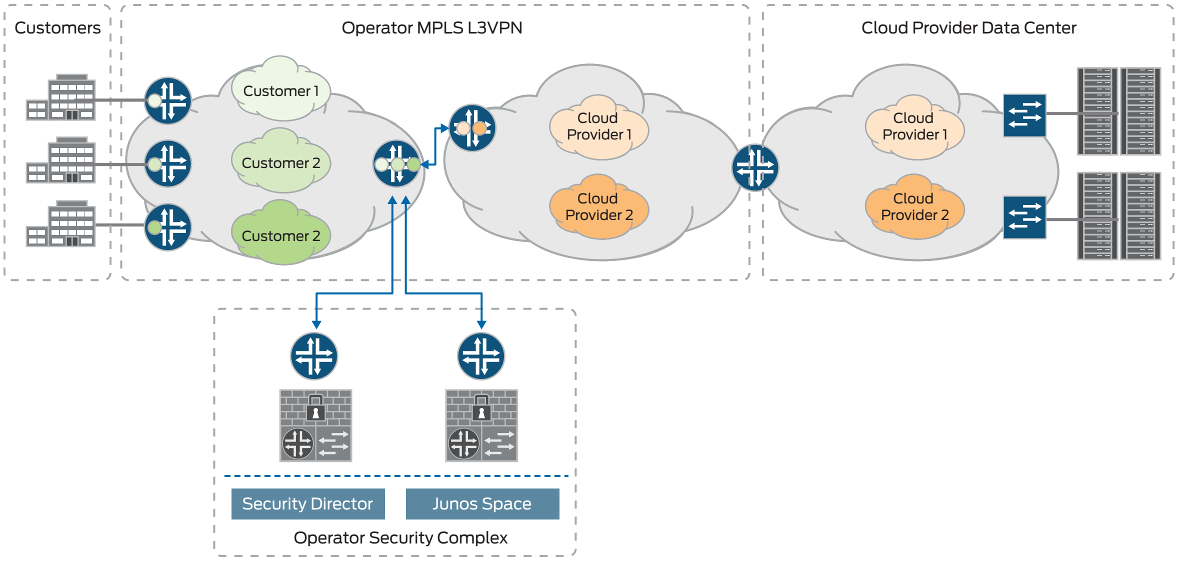

Figure 1: Secure cloud connectivity with physical workloads on the provider network

The MX Series router provides the scalable and intelligent MPLS VPN provider edge functionality. The MX Series enables service-level guarantee per customer by forwarding traffic based on appropriate QoS policies and assuring bandwidth based on traffic type. It also supports many inline services with the MS-MPC, carrier-grade NAT, and tunneling. The MX Series provider edge peers with the public cloud provider edge, and using MP-BGP, appropriate routes are installed in each customer VPN based on connectivity and service requirements from the enterprise to specific public cloud providers. The customer traffic is then forwarded to the security complex that includes the SRX Series gateway. The SRX Series gateway provides the extended high-performance stateful firewall. A zone per customer can be mapped to each customer's requirements and security policies.

Manageability and OSS integration are critical to any service delivery. Juniper Networks Junos® Space network management platform includes components to address both infrastructure routing needs and secure services delivery. Juniper Networks Junos Space Security Director provides a graphical and easy-to-use interface to provision and manage security policies per zone.for both the SRX Series and Juniper Networks Firefly Perimeter, Juniper's virtual firewall. The Junos Space integrated management system also includes Transport Activate to configure, manage, and monitor VPN connections.

Phase 2: Enabling Virtualized Secure Cloud Connectivity

Once the network's physical resources are put in place by the service provider for secure public cloud connectivity, a virtualized overlay network can be built to deliver the agility, scalability, and customized services needed at the virtual machine (VM) level, providing the most needed tenant level segregation. A virtualized security solution can deliver the agility needed to adapt to dynamic changes in traffic, protecting the enterprise data in a distributed applications environment

The integration of virtualized security solutions can be done in the security complex previously built out in the initial phase.

The agile and services-oriented nature of virtualization and cloud computing technologies demands security solutions that can dynamically safeguard virtual assets without sacrificing the level of performance, availability, and management control that network and security administrators have taken for granted in the physical world.

Juniper Networks Firefly Perimeter addresses these demands by moving beyond the traditional security appliance with a virtual firewall based on the SRX Series code delivered in a VM form factor.Firefly Perimeter operates deep within the virtualized fabric, offering layers of defense as well as rich connectivity features based on the powerful Juniper Networks Junos operating system foundation including extensive routing capabilities, Network Address Translation (NAT), and VPN. Firefly Perimeter supports chassis clustering in both "active/active" and "active/passive" modes to support stateful failover of processed connections in the event of any failures. In addition, cluster members are able to span hyervisors, providing additional flexibility and high availability of the virtual appliance.Firefly Perimeter delivers granular security with segmentation capabilities that create clear demarcation between zones, departments, lines of business, users groups, and applications.

Firefly Perimeter also includes Juniper Networks Junos Space Virtual Director, an intuitive and easy-to-use life-cycle management application that enables administrators to automate provisioning and resource allocation of Firefly Perimeter VMs, easily scaling them to meet elastic demand. Junos Space Virtual Director provisioning capabilities include support for multiple centers, the ability to define template parameters as the number of virtual instances allowed, actual location integration with VMware, and the ability to allocate virtual resources per instance such as vCPU, vRAM, etc. Junos Space Virtual Director also supports the ability to bootstrap, thereby allowing newly instantiated VMs to be managed and registered with the Junos Space suite. The monitoring functions include the ability to group deployed Firefly Perimeter instances by predefined "smart groups" and provide virtual resources usage information. With Juniper Networks Contrail Controller and OpenStack Orchestrator, the service provider can fully virtualize the provisioning, configuration, and operations and maintenance of this extended secure cloud VPN service to the enterprise. Juniper Networks MX Series 3D Universal Edge Routers are SDN enabled and can act as gateways to the physical workloads in the rest of the service provider network to support the customer's overall VPN (Figure 2),

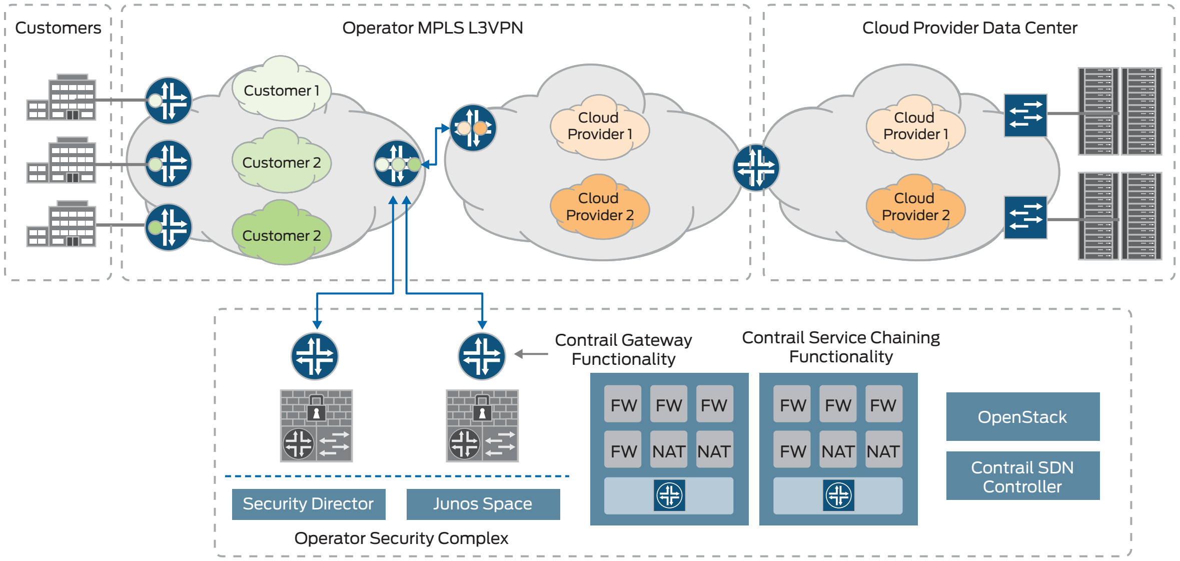

Figure 2: Hybrid solution with physical and virtual appliances to support both physical and virtual workloads

The statefull firewall functions and NAT functions are managed by Firefly Perimeter for customers ready for enhanced services provided by the virtualized solution.

This secure cloud connectivity solution with the integration of Firefly Perimeter, Junos Space Virtual Director, and Contrail SDN Controller enables the service provider to deliver the following:

Highly customized environment: The service provider can provide a portal to the enterprise customer to view the security policies in place. The service can be tailored to allow customers to modify their environment and have control over the security policy that is tied in to their virtualized instance. Custom reports and security compliance data can be made available per customer virtual instance.

Transfer cost savings: A virtualized security solution enables the service provider to deliver to the customer enhanced features such as security monitoring and control. This also enables the service provider to offload some of the security functions that enterprise customers might have previously taken on at their own premises. The service offload by the service provider can lower both the CapEx and OpEx for the enterprise because the enterprise does not have to maintain the extended security infrastructure and service in-house.

Enhanced network agility: With a virtualized security solution, the enterprise can easily modulate the use of resources needed based on application needs. Virtual instances can be spawned on demand for popular services, and resources can be freed up for services that don't take off in the enterprise.

Integration of Future Services with Secure Cloud

With a virtualized secure cloud connect service, service providers can establish themselves as value providers into the cloud chain. They can build on providing a consolidated solution to their enterprise customers. The basic building blocks of the virtualized secure cloud interconnect lay the foundation for integrating advanced managed security functions in the security complex at the service provider POP. This functionality can be easily replicated in various geographical locations to provide a highly available, reliable, and scalable solution.

In the example discussed earlier, along with stateful firewall and NAT on Firefly Perimeter, additional virtual network functions (VNF) can be integrated with Contrail, and the service provider can implement new services in the service chain. Some examples of services that can be included are IDP, Juniper Networks Junos WebApp Secure, and Junos DDoS Secure.

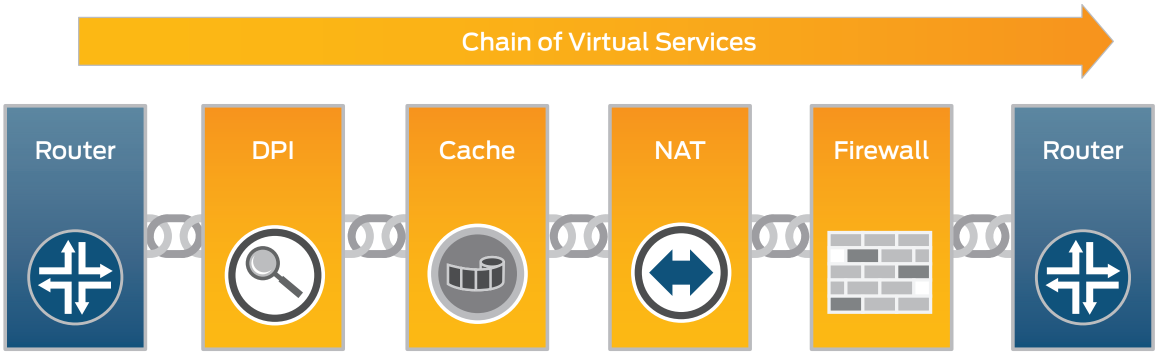

Figure 3: Integrate advanced security and bandwidth optimization services into the services chain

Juniper Networks Contrail Controller with OpenStack integration enables network function virtualization, and multiple services can be chained on demand per virtualized instance per customer (Figure 3). With an underlying mechanism based on standards- based BGP and NETCONF, the SDN overlay can smoothly integrate with the MPLS-VPN network architecture (Figure 4). The SDN Orchestrator can adapt to changing needs in the virtualized network and dynamically configure and modify services based on predefined network policies.

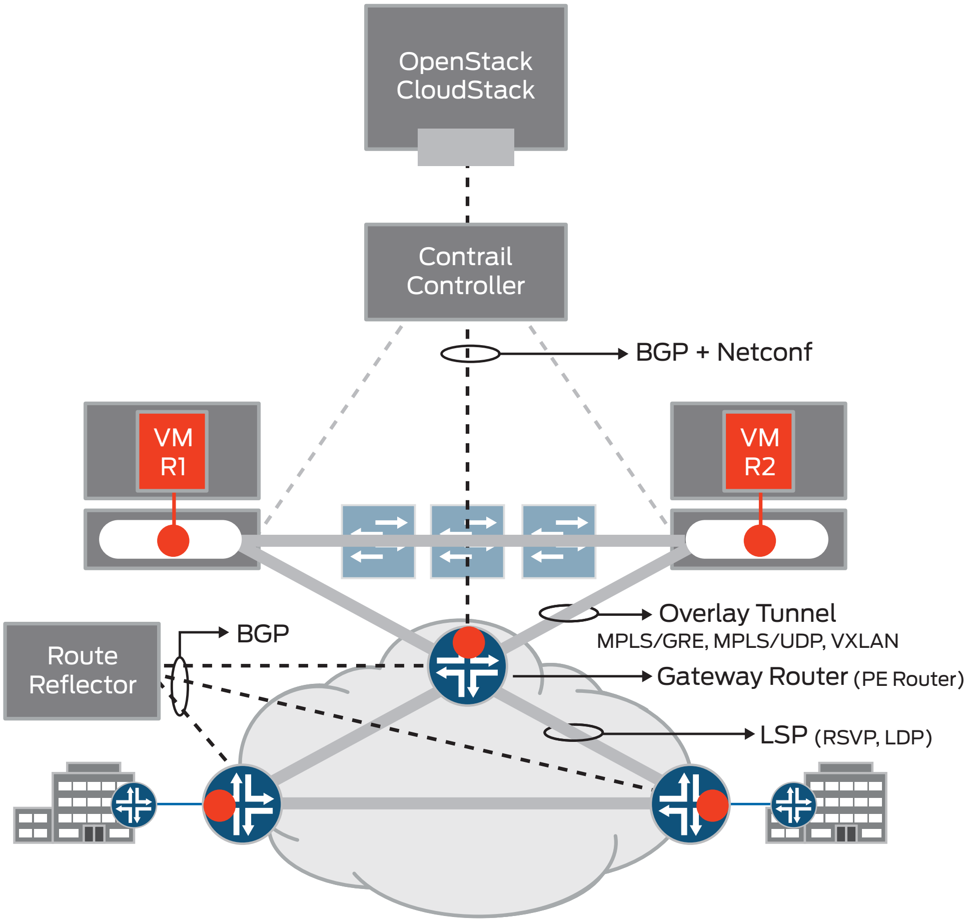

Figure 4: Juniper Networks Contrail Controller integration with MPLS VPN networks

With the Contrail Controller and Orchestrator, service chaining can be implemented—and these new services can be added to the virtualized environment in a customized fashion. Detailed statistics, security information, and reporting can also be provided per customer instance.

Juniper's vision for next-generation, SDN-enabled, virtualized networks is designed to help service providers evolve their network to cope with the elastic demands of their cloud-savvy business customers. The architecture is based on open standards and gives service providers the ability to integrate SDN/virtualization into their existing physical infrastructure. Service providers are expected to work with a hybrid (physical and virtual) network as they transform and evolve to deliver cloud-aware and cloud-based network services.

With Juniper's solution, service providers can accelerate network agility and fully utilize the ability to service chain and customize security policies per customer in an automated fashion. With the enhanced network agility, the provider can achieve reduced order to bill times at a large-scale, thereby accelerating revenue generation ultimately. The smooth integration of a virtualized solution into a physical network architecture also allows the service provider to deploy SDN in a small domain, gain deployment confidence with the solution, and find nondisruptive ways to integrate with the rest of the network and at a larger scale.

Conclusion

Today, service providers have the opportunity to insert themselves into the cloud services chain and evolve their network architecture to support the agility and distributed scalability of cost-conscious enterprise business customers. Juniper Networks is at the forefront of providing leading-edge, simple, agile, and open standards-based scalable solutions to meet the critical needs of today's enterprise. Juniper's solution is designed to help its customers create revenue by offering scalable systems and enabling network processes automation using open, standards-based network protocols. With Juniper's SDN framework and proven routing and security portfolio, service providers can seamlessly support the needs of physical and virtual solutions for years to come.

Bibliographic Citation and References

www.opencontrail.org

IDG survey report (70% of respondents say the number one barrier to deploying cloud solutions is security concern.) http://www.idgenterprise.com/report/idg-enterprises-cloud-computing

Infonetics research: Operators reveal where in their networks they plan to deploy SDN first. http://www.infonetics.com/pr/2013/SDN-and-NFV-Survey-Highlights.asp

About Juniper Networks

Juniper Networks is in the business of network innovation. From devices to data centers, from consumers to cloud providers, Juniper Networks delivers the software, silicon and systems that transform the experience and economics of networking. The company serves customers and partners worldwide. Additional information can be found at www.juniper.net.

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