Contrail for the Enterprise

Bringing Networks into the Cloud Era

Table of Contents

Executive Summary 3
Introduction 3
Limitations of Today's Network for Cloud Architectures 3
Scalability of the Network Edge 3
Lack of Programmatic APIs 4
Inability to Orchestrate Multi-Cloud/Hybrid Cloud Environments 4
Service Insertion Challenges 4
Introducing Contrail to Enterprise Networks 4
Key Features 5
What Functionalities Contrail Supports 6
Use Case #1 Virtualized Private and Hybrid Clouds 6
Time to provision network resources—*No agility* 7
Current data center architecture is hard to grow—*No scalability* 7
Networks are hard to manage and troubleshoot—No proactive monitoring and reporting 8
Use Case #1 Contrail Solution for Virtualized Private and Hybrid Clouds 8
Use Case #2 Hybrid Cloud—Seamless Inter-Cloud Orchestration 9
Use Case #3 Dynamic Service Chaining 9
Conclusion 10
About Juniper Networks 10

List of Figures

Figure 1: Contrail high-level architecture overview 4
Figure 2: Traditional data center view 6
Figure 3: Virtualized data center view 7
Figure 4: Contrail solution for virtualized private and hybrid clouds 8
Figure 5: Contrail solution for dynamic service chaining in the data center 9

Executive Summary

Enterprises are challenged to adapt their IT infrastructure to the ever changing demands of dynamic business and application delivery. Many enterprises are interested in either rolling out new applications or migrating legacy applications to the cloud to be agile and adapt to rapidly changing business needs. Although compute resources within traditional data centers have evolved tremendously in the past decade with the use of advanced server virtualization techniques, storage and networking have been lagging and often presents a roadblock to deployment of dynamic applications that require agile and scalable infrastructure.

This white paper introduces Juniper Networks® Contrail solution to enterprise decision makers. If you are an enterprise seeking to make the most out of your IT infrastructure but are limited by current technologies, this white paper will help you to understand how Contrail provides a unique virtual network solution that helps you move into the cloud era.

Introduction

The networking challenges for a self-service, automated, and vertically integrated cloud architecture are being addressed in multiple ways. For example, the orchestration system can use VLANs or Virtual Extensible LAN (VXLAN) to divide the network by application or tenant, but this approach is not ideal because it creates scalability, CapEx, and manageability issues. Scalability and CapEx inefficiencies are the result of the inability to handle policies, security, and routing at scale, without making changes to physical switching infrastructure. Similarly, tenant/application state is embedded in the physical networking infrastructure, creating challenges with manageability.

To address some of the drawbacks inherent in the traditional approach, data centers are starting to adopt a centralized, software-defined networking (SDN) controller based on OpenFlow to program the physical switches in the service path. However, this approach this approach has drawbacks similar to VLAN based multi-tenant virtualization approach, namely scalability, cost, and manageability. OpenFlow requires the programming of flows. With thousands of virtual machines (VMs) in a data center and hundreds of flows, programming those flows in today's low-cost physical switching hardware becomes a scalability challenge or can only be alleviated through the use of expensive switching equipment with large tables for flow management. Additionally, this approach reduces your ability to manage the infrastructure, since the tenant/application state is programmed in the underlying hardware and a problem in one tenant/application can propagate to others.

Juniper Networks Contrail solves these automation, cost, scalability, and manageability problems by providing advanced networking features through a proactive overlay virtual network. All of the networking features such as switching, routing, security, and load balancing are moved from the physical hardware infrastructure to software running in the hypervisor kernel that is managed from a central orchestration system. This allows the system to scale while keeping the costs of the physical switching infrastructure under control, as the switching hardware has no state of the virtual machines or tenant/application and is only involved in routing traffic from one server to another. The Contrail system also solves the agility problem, as it provides all of the automation for provisioning of the virtualized network, networking services, and integration with cloud orchestration systems such as OpenStack and CloudStack using REST APIs.

Limitations of Today's Network for Cloud Architectures

Enterprises are confronted with many strategic data center and cloud networking issues as their business units challenge them to deliver IT-as-a-service applications that can be self-serviced by the developers. They are also demanding infrastructure that allows for elastically scalable and dynamic applications, usage-based billing to departments, and support for hybrid public/private cloud environments.

Scalability of the Network Edge

Transformation of data centers is continuing with gradual replacement of physical ToR switches with virtual switches built into the hypervisor within the "compute" server itself.

As VLAN (or VxLAN) based dynamic multi-tenant data traffic spreads over entire data center cluster over time, inevitably, many VLANs (or VxLANs) get provisioned within ToR switching layer, and as a consequence, scalability issues arise due to limited switching/forwarding and policy enforcement capacity of ToR switches.

Solution to this switching layer scalability problem is to shift VLAN information and associated switching/forwarding/policy enforcement functions to physically routed network, using overlay network virtualization, however this approach requires use of physical or software gateways to route traffic between VLANs (or VxLANs)

Lack of Programmatic APIs

Enterprises have to deal with multiple silos of disconnected management and operations systems for application orchestration, server virtualization, storage virtualization, and network provisioning. Since most application and infrastructure management is moving towards the use of an integrated orchestration system like VMware, OpenStack, and CloudStack, it is essential to present programmatic APIs (e.g., REST APIs) as an interface to the network instead of CLIs.

Inability to Orchestrate Multi-Cloud/Hybrid Cloud Environments

Existing networking approaches do not lend themselves to the seamless creation of new workload and/or the transport of workloads across multiple clouds/hybrid clouds. Lack of API compatibility and the federation of orchestration platforms are a major gap that inhibits different autonomous systems to securely cooperate for workload migration.

Service Insertion Challenges

Traditional appliance-centric network services require physical network elements to be reconfigured for any workload migration, and it takes an unacceptably long time to provision new service capacity and upgrade services. In addition, there is not any uniform management model (programmatic APIs) for services provided by different vendors and third parties including VM security, firewall, Network Address Translation (NAT), and VPN.

Introducing Contrail to Enterprise Networks

Contrail is a scale-out networking stack that creates virtual networks while seamlessly integrating with existing physical routers and switches. It automates service chaining of virtualized or physical network services, orchestrates networks across public, private, and hybrid clouds, and provides advanced analytics capability for automation, visualization, and diagnostics.

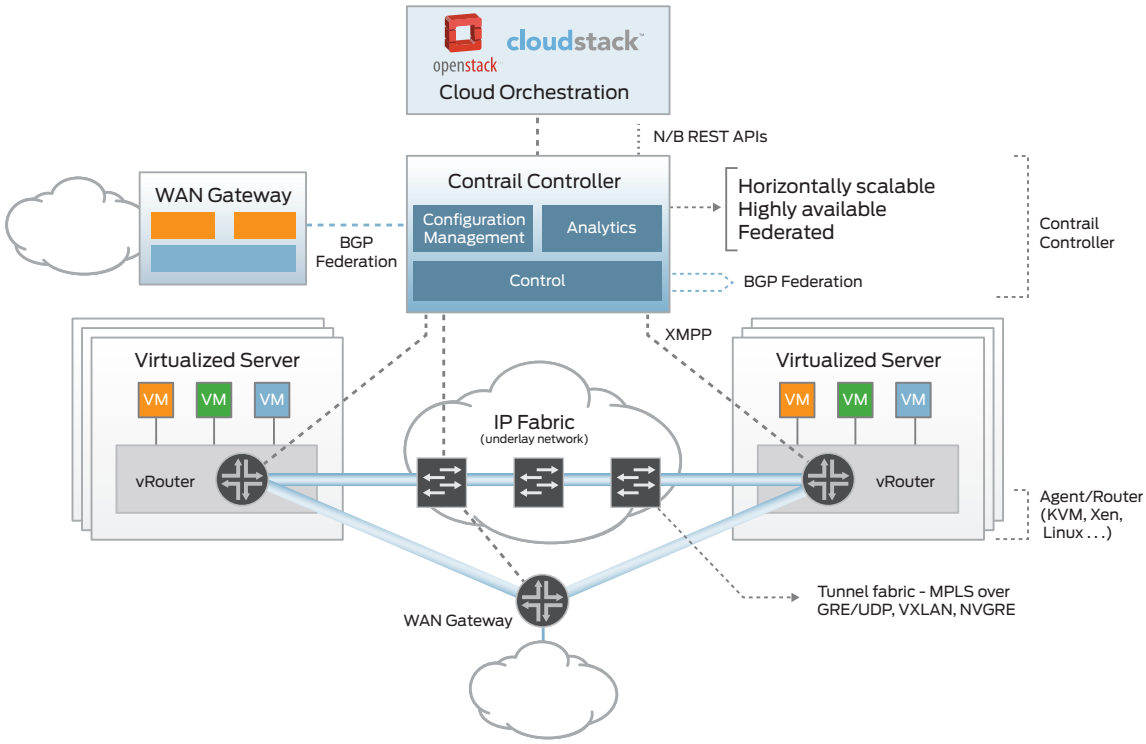

Figure 1: Contrail high-level architecture overview

Contrail is comprised of the following key components:

Contrail Controller integrates with open cloud orchestration solutions (i.e. OpenStack, Cloudstack) and with SP OSS/BSS systems. It sits between the orchestration system and network devices (physical underlay, virtualized appliances) and communicates via published RESTful APIs. Contrail control nodes have 3 main functions:

- **Configuration**: accepts request from an orchestrator for provisioning a VM and assign a network to the same. It converts this high level request into a low level request that can be understood by network elements.
- **Control**: interacts with the network elements using XMPP and maintains network state by interacting with its peers using industry standard BGP to ensure network resiliency and uptime.
- **Analytics**: collects, stores, correlates and analyzes information across network elements. This information includes statistics, logs, events and errors, can be consumed by end user or network applications through Contrail's northbound REST API and can be analyzed with SQL style queries.

Contrail vRouter is part of the compute node which gets reachability information from the control plane and ensures native L3 services for host-based virtual machines. Each vRouter is connected to at least 2 control planes to optimize system resiliency.

Key Features

- **Switching and Routing**: Hypervisor forwarding plane provides line-rate routing and switching in a multitenant virtualized environment that is completely decoupled from the underlying physical fabric switches.
- **Load Balancing**: Load balancing is built right into the hypervisor forwarding plane for the balancing of traffic across application tiers or network services.
- **Security**: Policy enforcement and security groups are built directly into the hypervisor forwarding plane. Application-aware firewall services are delivered in software using Juniper Networks JunosV Firefly (a virtual firewall-based feature of the market-leading SRX Series Services Gateways), and distributed threat prevention is delivered in software using Juniper Networks Junos® WebApp Secure.
- **Elastic, Resilient VPN**: Contrail delivers L3VPN, E-VPN, site-to-site IPsec, and SSL VPN in software.
- **Gateway Services**: Juniper Networks MX Series 3D Universal Edge Routers or EX Series Ethernet Switches can be used as a physical gateway to provide seamless connection to legacy workloads and non-virtualized physical services without the need for a separate software gateway element. This provides interoperability with most routing equipment that supports L3VPN or E-VPN with appropriate data encapsulation standards.
- **High Availability**: Contrail is configured in Active-Active cluster mode, and each vRouter is connected to a set of control planes and get same routing table and ACLs.
- **Analytics Services**: Rich visualization and diagnostics of virtualized and physical networks, these services provide real-time and historical infrastructure analytics that can be consumed through REST APIs.
- **API Services**: REST API for configuration, operation, and analytics for seamless integration with cloud orchestration systems such as CloudStack and OpenStack, or service provider operations and business support systems (OSS/BSS). This also includes virtual path connection (VPC) API compatibility for seamless deployment of applications in a hybrid environment (private cloud and public/Amazon Web Services, for example).

What Functionalities Contrail Supports

Feature	Description	Benefit
Network virtualization	A centrally managed abstraction that delivers all network functionality at the edge (typically, in the hypervisor) by creating an overlay network over any multivendor physical network	• Increases agility of the infrastructure through central management • Reduces costs by delivering complex network functionality in the virtualized networking layer instead of physical hardware
Programmability	Uses SDN as compiler to understand and translate abstract commands into specific rules/policies to automate provisioning of workloads, configure network parameters, and enable automatic chaining of services	• Hides complexities and low-level details of underlying elements (ports, VLANs, subnets, etc.) through abstraction to allow for effortless extensibility and simplified operational execution
Network function virtualization	Provides dynamic service orchestration including VM management, scale-out, load balancing of traffic, and service monitoring of any Juniper and third-party networking services	• Reduces service time-to-market, improving business agility and mitigating risk by simplifying operations with more flexible and agile virtual model
Big data analytics	Queries, ingests, and interprets structured and unstructured data to expose network knowledge using REST APIs and rich UI	• Enables better insight, proactive planning, and predictive diagnostics of infrastructure issues by employing both near-real-time and historical information on application usage, infrastructure utilization, system logs, network statistics like flows, latencies, jitter, etc.
Open system architecture	Supports standard-based protocols and open orchestration platforms to enable vendor-agnostic interoperability and automation Takes open concept to the next level by making source code available under the Apache v2.0 license	• Maximizes investment protection by eliminating the need for comprehensive refresh of infrastructure • Provides unmatched extensibility with ability to modify source code (learn more at www.opencontrail.org)
Visualization	Provides exception-based dashboard/UI with hierarchical presentation (virtual networks to individual flows) of real-time and historical network data	• Simplifies operations and decision making by providing a simple yet comprehensive view into infrastructure to help efficient correlation and orchestration across physical and overlay network components

Use Case #1 Virtualized Private and Hybrid Clouds

To be operationally agile, many enterprises deploy multitenant data centers (private clouds) that leverage virtualization to support dynamic applications with varying resource and compliance requirements. As enterprise data centers are evolving from traditional physical, virtual, and finally to fully automated clouds, they need to address the challenges associated with each phase of maturity. Contrail helps mitigate risk and deliver on the promise of a fully automated cloud environment.

In the traditional data center shown in Figure 2, banks of siloed servers dedicated to individual applications and VLANs are used to segment these networks. Orchestration is done manually by using complex rules on the routers, dedicated load balancers, and firewalls. This approach results in long lead times in new deployments and extreme inefficiency in the utilization of server resources.

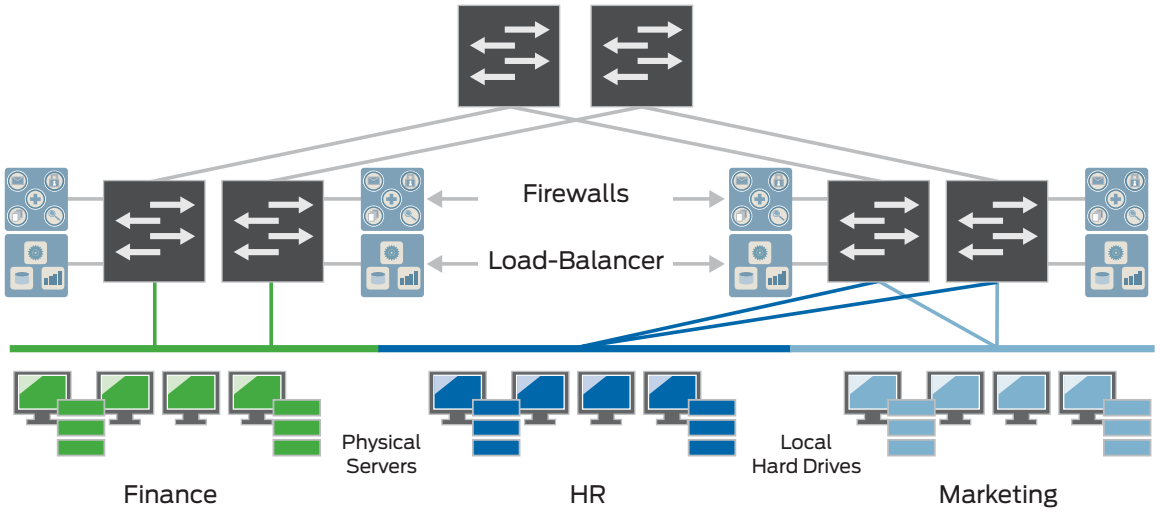

Figure 2: Traditional data center view

Virtualized data centers as shown in Figure 3 are fundamental to the success of next-generation IT evolution, where compute, storage, and network resources are completely virtualized and provisioned automatically to increase agility, provide increased utilization, and reduce overall TCO.

In a virtualized environment, enterprises have seen a significant reduction in cost of ownership and time to revenue as manual processes are automated, heterogeneous systems are converged, and operational processes become much less prone to error.

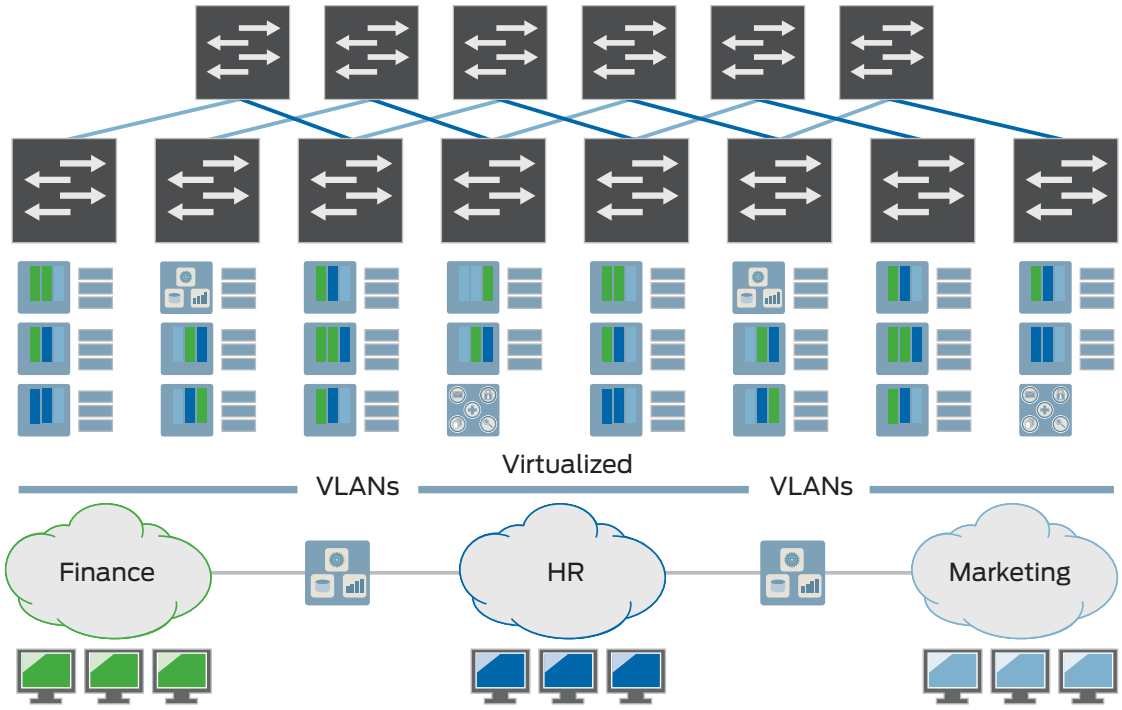

Figure 3: Virtualized data center view

In order to have a fully automated cloud environment, there are various challenges that an enterprise faces. Some of the biggest challenges are:

Time to provision network resources—*No agility*

Enterprises use a hypervisor as a base layer of their virtualized environments and a cloud orchestrator (CloudStack, OpenStack, etc.) to dynamically provision resources in the cloud and to the end user.

- Orchestrators are able to provision compute and storage resources only.
- Network resources are hard to configure and often have to be provisioned manually. It takes days or even weeks to properly configure and provision a network for a VM, eventually causing a delay in application provisioning for the end user.

To improve data center agility, Contrail automates the overlay of network resources in a matter of seconds. It runs as a kernel module in the hypervisor to provide high-performance networking services, and it integrates with both OpenStack and CloudStack cloud orchestrators. This allows enterprises to roll out applications faster while reducing costs. Using Contrail, you get the true benefits of an agile, dynamic, and cost-effective cloud environment.

Current data center architecture is hard to grow—*No scalability*

There are various limitations on the technologies (VLAN, tree topology, etc.) used to design today's data center networks. These limitations, as mentioned below, affect the scalability of a network and are a bottleneck for running a dynamic and agile cloud environment.

- VLAN-based segmentation is only applicable on an L2 switching domain implemented on a set of network switches. A VM cannot move beyond an L2 domain without losing its network properties (IP address, policies, etc.), and this restricts it to a single L2 domain. This renders your VLAN unusable if you are looking to move your data across domains in a cloud environment.
- L2 domains have to be small for stability due to the weakness of underlying protocols (e.g., Spanning Tree Protocol). Hence, having an L2 domain span across an entire data center is technologically challenging.

- Traffic between VLANs has to go through an L3 router, which enforces the packet filtering rules. This creates large complicated filtering rule sets on the routers, and these are very hard to manage, resulting in errors and consequent outages.
- VLAN has a limit of 4,000 tenant networks per data center, which limits the number of network segments that can be created.

Contrail enables an agile data center by working as an overall and underlay network with IP connectivity. Figure 4 shows how Contrail's overlay network absorbs changes, enabling the movement of VMs that are supporting business services without any changes to the physical network properties. The overlay network can be either fully L3 or any combination of L2 and L3. This avoids application downtime if a VM has to be moved from one location to another. Also, any large L3 domain is much easier to manage, especially when all of the logical changes are absorbed by the overlay network. Virtual networks also negate the weakness of Spanning Tree Protocols that often result in network congestion and an outage. Since virtual networks work on L3, they have a 24-bit virtual network interface (VNI) construct that allows 16 million isolated tenant networks (virtual networks) in the data center as opposed to 4,096 tenant networks allowed by VLAN.

Networks are hard to manage and troubleshoot—No proactive monitoring and reporting

With enterprises moving to a cloud environment, there are new challenges in managing data center networks.

- It is hard to manage both L2 and L3 networks at the same time.
- IT has to invest in purchasing multiple tools to perform packet monitoring, troubleshooting the network, etc. that results in huge cost to the company.
- Multiple resources are required to manage these tools.

Contrail helps with planning and modeling by allowing you to monitor and analyze your network at a granular level. By providing historical and real time information, the analytics engine helps you manage both L2 and L3 networks, collect detailed network logs, perform on-demand packet capture and other functions from the same user interface. The data captured by Contrail helps a network administrator to configure the network for an optimal use, troubleshoot the network if there is a problem, set up alarms to detect any potential problems, and use historical information to plan for future growth. This helps to minimize the network downtime and also helps to reduce the cost of managing a data center.

Use Case #1 Contrail Solution for Virtualized Private and Hybrid Clouds

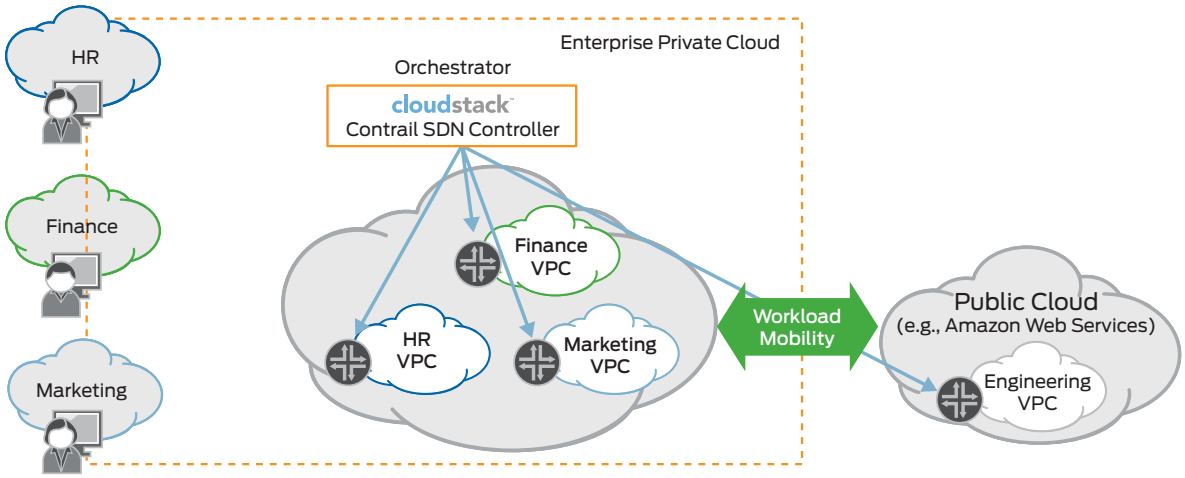

Figure 4: Contrail solution for virtualized private and hybrid clouds

Contrail is an open source technology and works with all hardware vendors and industry-leading orchestration platforms. It provides agility, scalability, and granular monitoring for data center networks, allowing the enterprise to build and consume a cloud environment most efficiently. By creating an L3 overlay network and avoiding the limitations of an L2 network, Contrail is also simplifying the end-to-end network, allowing you to manage your data center much more efficiently. It helps you cut down on management cost and also improves network uptime, reducing the time needed to roll out or migrate applications by reducing time to provision and deploy the network infrastructure. This leads to increased revenue, improved customer experience and loyalty, and more productivity for your employees.

Use Case #2 Hybrid Cloud—Seamless Inter-Cloud Orchestration

In addition to the physical workloads, enterprises today have to either choose a private cloud, a managed private cloud, or a public cloud to run their applications and workloads. Private clouds are more secure and rely on the enterprise's business model for quality of service (QoS) and reliability, whereas public clouds provide lower cost and easier capacity management for peak or transient workloads. This leads to two critical enterprise challenges:

- The first challenge is that workloads cannot talk to each other because most of the cloud vendors use proprietary technologies. As a result, enterprises are forced to choose a single cloud model for their workloads.
- The second challenge is the so called "Shadow IT" problem. Many development business units have their own IT budgets. Instead of going through their enterprise IT, these groups purchase a public cloud offering and spawn their workloads without IT, which often takes a long time to provision. This solves a short-term problem but involves several potential security and incompliance risks.

Figure 4 shows how Contrail enables multiple clouds or a hybrid cloud strategy. Contrail helps you create a virtual private cloud in a third-party cloud provider network, then extend it using your existing L3VPN link (or IPsec connection) to your existing data center, private cloud, or the legacy infrastructure in your branch office. Your workloads, be it on a branch office network, public cloud, in your data center, or in a private cloud, are now on the same virtual network and can access each other over a secure channel irrespective of which cloud they are on. This type of flexibility allows enterprises to choose multiple vendors, and it helps them negotiate better CapEx and SLAs. This also helps the enterprise IT organization get rid of "Shadow IT," and extend the organization's security policies to the workloads hosted on a third-party cloud provider network.

Use Case #3 Dynamic Service Chaining

Enterprise data centers are growing at a rapid pace and so is the cost to manage them. For maintaining security and compliance regulations, data centers and cloud environments have isolated tenant networks. Access to resources in these networks is given on a need-to-know basis and has to conform to various regulatory standards. Each of these networks has some sort of firewall, load balancer, data packet inspection (DPI), and intrusion detection and prevention service (IDS/IPS) attached to it. The problem with these services is:

- Even in their virtualized form, services take time to get provisioned and potentially cause delays, if a network needs to be updated, or a new service needs to be provisioned to these networks.
- There can also be network outages as a result of a new service being inserted or updated over time, which can be very cost prohibitive.

Contrail helps reduce the cost associated with buying and provisioning hardware, virtual network appliances, and services. It helps to dynamically provision any Juniper or third-party network service in a matter of minutes and connect virtual networks and support rollout of new or updated applications. Contrail provisions these network services on an x86-based VM and connects multiple virtual networks without any downtime required.

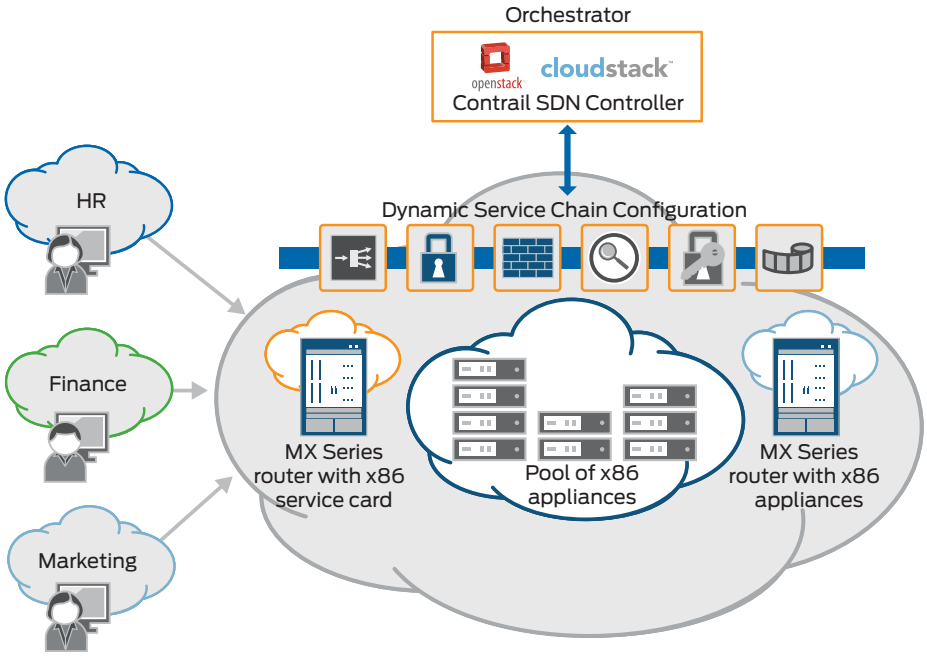

Figure 5: Contrail solution for dynamic service chaining in the data center

Conclusion

Juniper Networks Contrail is a scale-out networking solution that creates virtual networks while seamlessly integrating with existing physical routers and switches. It automates service chaining of virtualized or physical network services, orchestrates networks across public, private, and hybrid clouds, and provides advanced analytics capability for automation, visualization, and diagnostics.

Contrail brings advanced networking capabilities to the cloud and eliminates the barriers to cloud adoption by making the cloud dynamic and flexible. Today, Contrail is offering a unique and significantly differentiated approach that is built on a number of key benefits:

- Provides a simple way to connect physical networks with a virtual environment and provision underlying services, reducing the time, cost, and risk for customers when configuring the network
- Uses service chaining to make provisioning and management of network and security services such as JunosV Firefly easy, enhancing the efficiency and agility with which customers deploy and use network resources
- Eliminates the risk of vendor lock-in by leveraging a standards-based architecture that integrates with a wide variety of hypervisors, physical networks, and orchestration platforms, including compatibility with both CloudStack and OpenStack
- Seamlessly integrates with most industry switches and routers, including MX Series, EX Series, and QFX Series appliances, to provide customers with a quick and easy migration path to SDN without any disruption to underlying physical network architecture and investment
- Accelerates the connection of virtual resources and enables the federation of private, public, or hybrid cloud environments, increasing the speed of business and service innovation by making the network more dynamic, flexible, and automated
- Speeds up troubleshooting and diagnostics through unique analytics capability, enabling customers to more intelligently and efficiently manage their networks

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

2000528-001-EN Sept 2015