Build an SDN-Enabled Network with Juniper Networks Contrail

Automate the creation of agile and open cloud networks to rapidly deliver new services in the enterprise

Challenge

The enterprise network must be agile, secure, cost-effective, and accessible to employees anywhere, anytime. Today's enterprise network infrastructure, however, is often static and requires special IT skills to deploy and make changes, hindering productivity and slowing business expansion.

Solution

Contrail is a cloud network automation platform that allows businesses to implement secure multitenant enterprise environments and dynamically establish virtual overlay networks that connect both physical and virtual functions.

Benefits

- Fosters innovation by simplifying SDN implementation, cloud deployment, network orchestration, and VNF operation
- Allows enterprises to use shared physical infrastructures by securely segmenting each department with virtual overlay networks
- Enables enterprises to host VNFs in various locations
- Connects virtualized workloads residing in private and public clouds, helping enterprises migrate to a hybrid cloud

Modern enterprises and their underlying infrastructures must be agile, flexible, and scalable enough to adapt to emerging trends such as the mobile workforce, labor mobility, and ubiquitous connectivity—all while reducing transport and communication costs. "Cloudifying" IT systems is an increasingly popular way for enterprises to address these challenges, remain relevant, and be competitive.

SDN is an integral part of this "cloudification" process, as it can dynamically create and/or migrate networks to where resources are allocated, applications are hosted, and connectivity is needed. In addition, SDN can segregate various departments within enterprises by setting up dedicated virtual overlay networks, isolating communications for each. For enterprises to take full advantage of next-generation technologies, SDN-related solutions must support an agile and flexible hybrid cloud.

The Challenge

Enterprises must remain competitive to expand their business, regardless of vertical or application. In order to increase top-line growth, businesses must be able to introduce new features, services, and/or applications faster than the market itself. It is critical that these technologies, which enterprises implement with their core business applications, foster innovation and help businesses achieve faster time-to-market to retain existing customers and attract new ones. When combined with agile network infrastructure, the cloud allows enterprises to implement "fail fast" fundamentals and structures to minimize the risk of introducing new features and services while allowing new ideas and innovation to flourish.

For enterprises, reducing operational expenses is just one of the advantages of using virtualization to move their IT systems to the cloud, enabling them to consolidate redundant hardware-based systems deployed by individual departments. However, while these dedicated systems can be consolidated, centralized, and shared, a clear segmentation between individual departments must be maintained to ensure security.

In addition, enterprises adopting a mobile workforce paradigm must extend that same flexibility and agility to branch offices, enabling them to quickly commission and decommission new locations while maintaining existing security policies and without incurring the extra resource, workforce, and transport costs normally associated with such moves. Along with a mobile workforce, this instant and movable office environment lets the enterprise be more productive.

Unfortunately, current IT and networking infrastructure is often static, causing a disconnect between nomadic employees and the stationary work place. The inability to provide these nomadic employees with an efficient and consistent work environment offering ubiquitous connectivity and instant and secure access to applications negatively impacts the business's competitiveness and growth.

To overcome these challenges, a new breed of technologies—including virtualization, SDN, and Network Functions Virtualization (NFV)—must be utilized. These technologies enable enterprises to migrate their IT infrastructure to a private or public cloud, depending on the

Business Need	Challenge
Deploy new services and/or applications rapidly	Rigid and static network infrastructure
Optimize operational costs	Redundant hardware-based infrastructures defined by departments
Establish secure communication between departments	Shared and common network infrastructure
Rapidly deploy new offices	Complex and expensive replication of hardware resources at each office location
Freely choose private or public cloud, depending on services and/or applications	Lack of networking tools to connect between cloud properties
Seamlessly connect overlay and underlay	Additional and specially configured gateway
Leverage the performance of existing physical underlay	Limited performance of gateway

applications. Furthermore, businesses must be able to migrate virtualized workloads—as well as the virtual overlay networks attached to those workloads—across private and public clouds with the click of a button to maintain continuous communication. This requires seamless connectivity between virtual overlay and physical underlay networks while maintaining the existing underlay network infrastructures.

The Juniper Networks Contrail Solution: Cloud Network Automation

Juniper Networks® Contrail is a simple, open, and agile cloud network automation platform that implements secure multitenancy, enabling dynamic service chaining in private, public, and hybrid clouds.

Contrail is available in two product lines: Contrail Networking and Contrail Cloud Platform.

- Contrail Networking, an open SDN solution that consists of Contrail Controller, a Contrail vRouter analytics engine, and published northbound APIs for cloud and NFV, improves business agility by delivering unique security, availability, performance, automation, and elasticity capabilities.
- Contrail Cloud Platform is a turnkey cloud orchestration and automation platform that consists of Contrail Networking, Juniper's OpenStack Distribution, Server Manager, and Ceph-based distributed storage.

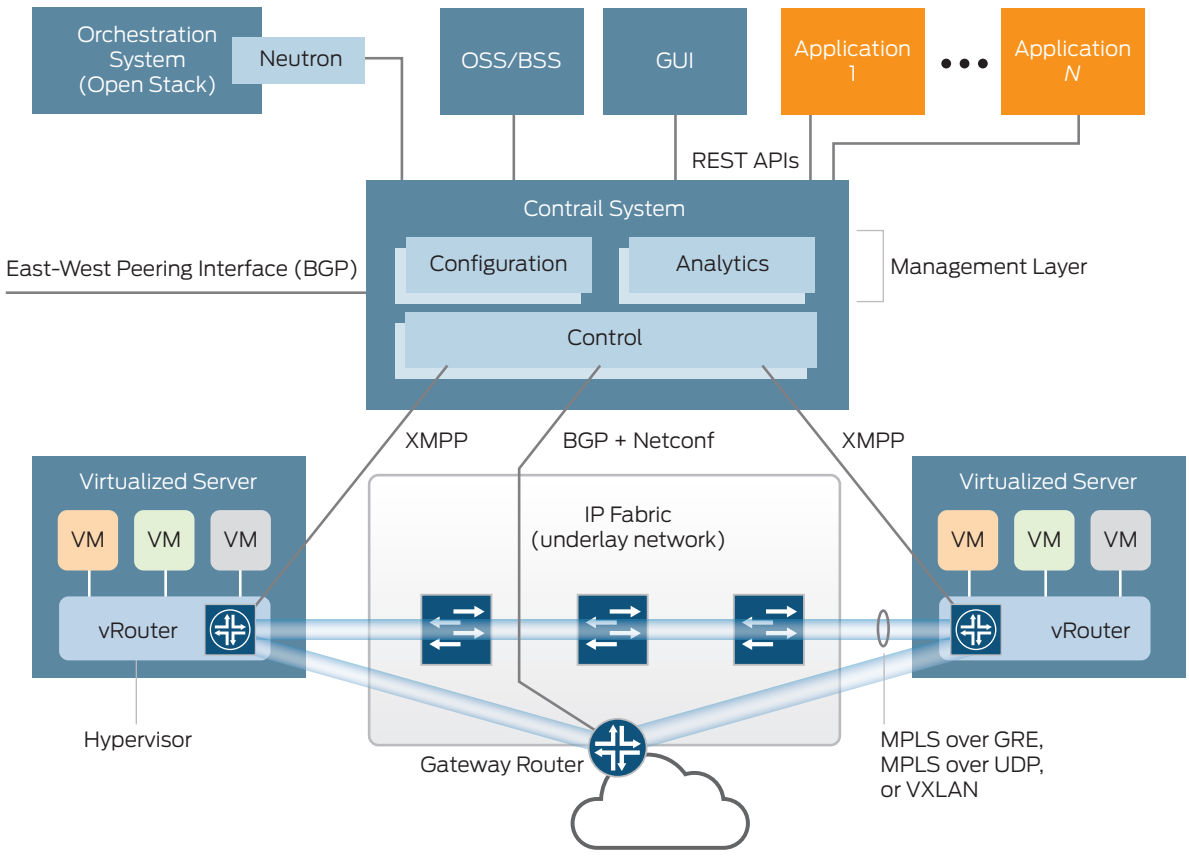

Figure 1: Juniper's Contrail overview

Fostering Innovation

Contrail Networking is based on OpenContrail, an Apache 2.0-licensed open-source project that demonstrates Juniper's commitment to openness, allowing anyone to participate in its ecosystem. As an open-source project, OpenContrail lets users contribute to and leverage the power of the community to enhance the product feature set. This allows enterprise users to customize and fine-tune Contrail Networking along with their cloud environments to serve their specific requirements, empowering them to offer granular applications to employees and customers.

Enhancements to Contrail Networking can be integrated into the Contrail main trunk by upstreaming code from an enterprise's internal development or DevOps team's private repository. Furthermore, as a community-driven SDN solution that provides access to multiple feature sets, Contrail allows enterprises to leverage other users' enhancements. The ability for enterprises to contribute back to Contrail's main trunk fosters innovation through the breadth of the contributing community.

Although the development of Contrail Networking is driven by the OpenContrail community, Juniper provides technical assistance and fully supports both the open-source project and the commercial product, giving enterprises the confidence that they can implement mission-critical applications with this open-source-based SDN solution.

Optimizing Network Resources

Enterprises recognize that conventional segmented network designs serving individual departments are rigid and expensive, as they require redundant physical systems that may not be fully utilized. To overcome this inefficient use of resources, enterprises are using virtualization technologies to implement converged network designs that let various departments share a common network.

While this shared network resource achieves the desired flexibility and cost reduction, IT must now consider the challenge of securely isolating departments over the common network infrastructure to protect sensitive information. Contrail Networking solves this problem by implementing secure virtual overlay networks to logically separate departments.

This multitenancy capability, called a virtual private cloud (VPC), allows individual departments to establish one or more private, isolated L2 networks. A department's virtual overlay network allows each virtualized workload to communicate with other virtualized workloads in the same department; since networks are isolated from each other, a workload of one department cannot communicate with a workload of another department unless specifically allowed by policy.

Furthermore, Contrail Networking's secure multitenancy capability enables enterprises to seamlessly integrate their virtualized workloads in both public and private clouds, creating hybrid cloud environments and shielding employees and customers from the networking constructs while effectively abstracting the network.

The ability to implement secure virtual private overlay networks in a hybrid cloud environment empowers enterprises to freely migrate virtualized workloads between public and private clouds. This flexibility lets enterprises fine-tune serving locations for each virtualized workload with respect to cost, latency, resource availability, and other constraints.

Facilitating Business Expansion

SDN-enabled "cloudification" using Contrail Networking allows enterprises to expand their business. For example, using Contrail Networking's dynamic service chaining function, enterprises can move from owning and operating physical network appliances such as firewalls, intrusion detection and prevention (IDP),

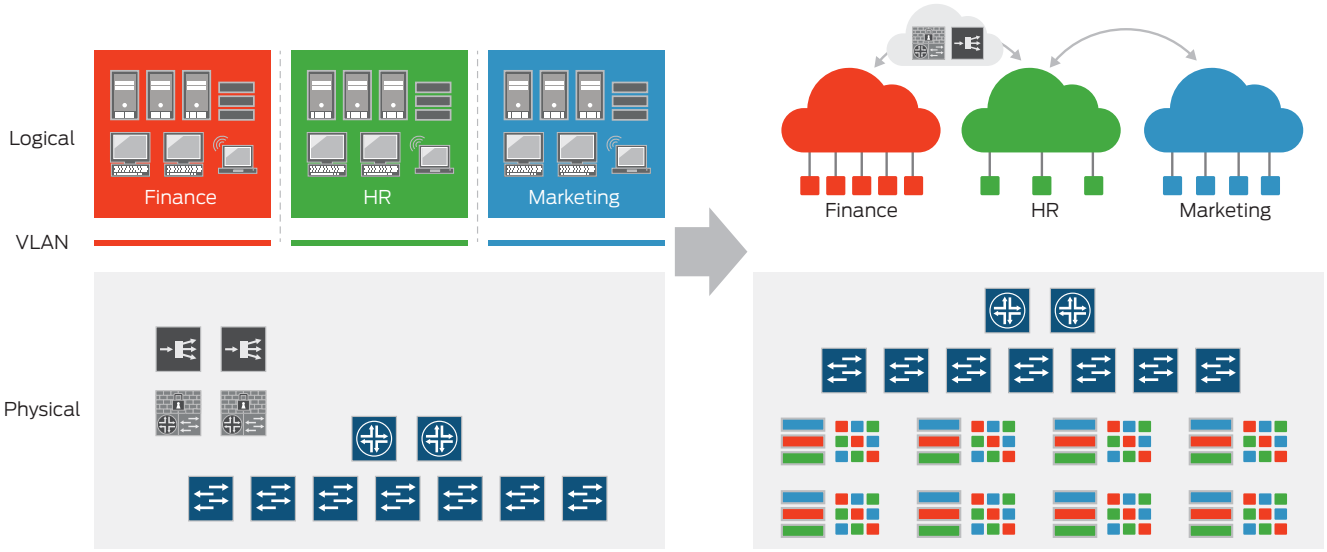

Figure 2: Migration of IT infrastructure

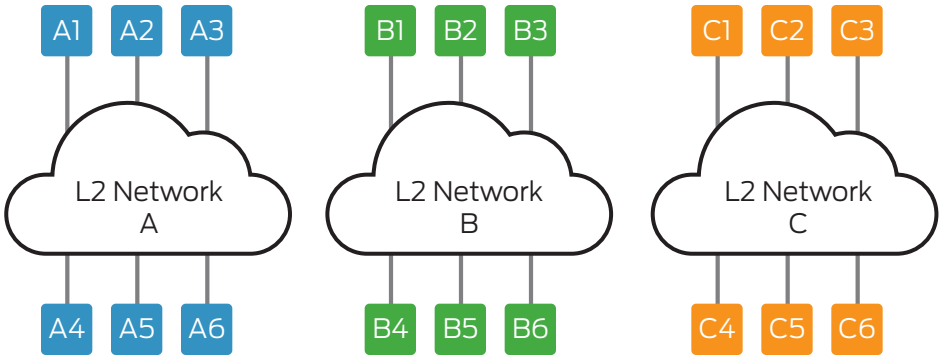

Figure 3: Secure multitenancy presented to departments

or Network Address Translation (NAT) systems from branch offices to cloud data centers as virtualized network functions (VNFs). Contrail Networking orchestrates the instantiation of the VNFs and steers traffic flows through a sequence of physical network appliances and VNFs. Hosting VNFs in the cloud gives enterprises significant flexibility and reduces the time required to implement new IT-related features by using turnkey, on-demand, and point-and-click service creation, eliminating the need for dedicated IT teams to manage and operate these features at every branch office.

This flexibility also applies to enterprises commissioning new branch offices, allowing nomadic employees to take full advantage of a regular corporate office environment anytime, anywhere. This, in turn, increases employee productivity and strengthens the competitive edge of enterprises that implement the SDN solution.

Realizing Hybrid Cloud

Contrail Networking uses mature, open, and standard-based protocols to set up networks to connect virtualized workloads located in public and private clouds. In this hybrid environment, traffic from a virtual overlay network must traverse a physical network to reach the other workload; therefore, a gateway router or switch is required to connect these two networking properties. In this scenario, the advantage of Contrail Networking is the use of BGP for the control plane—the same protocol used for MPLS L3VPNs and MPLS Ethernet VPNs (EVPNs).

Contrail Networking's architectural design lets enterprises use existing physical routers or switches as gateways, provided they support BGP. This eliminates the need to deploy new gateway appliances while maintaining the performance advantages of the existing router or switch over specialized gateway appliances. Enterprises do not have to compromise the performance of the underlay network, since the existing router or switch is not a bandwidth bottleneck. In addition, this eliminates the cost of purchasing and operating a specialized gateway appliance.

Features and Benefits

Open source: Contrail Networking is based on OpenContrail, an Apache 2.0-licensed open-source project that demonstrates Juniper's commitment to openness and allows all participants to contribute to its ecosystem as well as leverage the power of the community. This fosters SDN innovation and drives cloud adoption by providing enterprises with a platform built on open standards and APIs.

Technical support: Juniper provides technical assistance and fully supports both the open-source project and Contrail Networking, giving enterprises access to Juniper's technical support and assuring enterprises that they can implement mission-critical applications with an open-source-based SDN solution.

Secure multitenancy: Virtualization allows multiple departments to share the same physical resources (servers, storage, network) within a common data center. Contrail Networking assigns logical resources to each department and connects virtualized

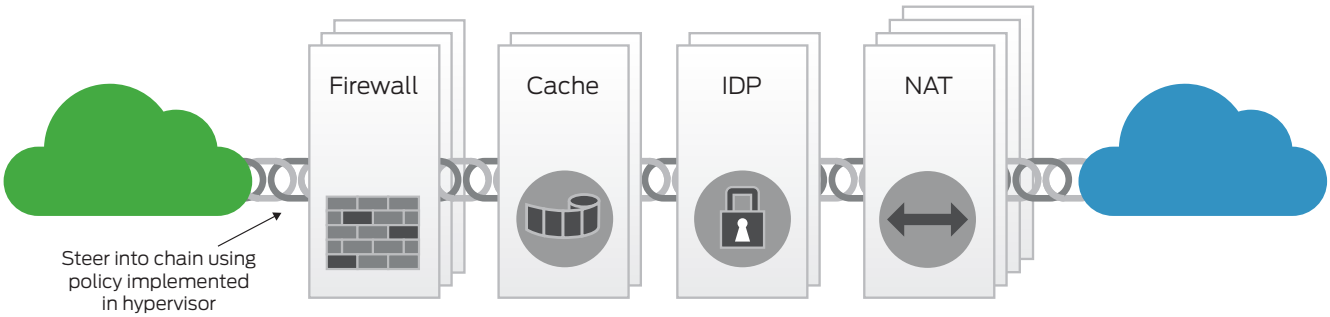

Figure 4: Dynamic chaining of VNFs between two networks

workloads using virtual overlay networks, which replace VLAN-based isolation and provide multitenancy in a virtualized data center. Each department can have one or more virtual overlay networks; each virtual overlay network is isolated from all others unless explicitly allowed by security policies.

Dynamic service chain: Contrail Networking can steer specific traffic flows through a series of physical or virtual network services such as firewalls, deep packet inspection (DPI), load balancers, IDP, or NAT.

Architectural advantages: Contrail Networking uses mature, open, and standards-based protocols—such as BGP and MPLS over User Datagram Protocol (MPLSoUDP), MPLS over generic routing encapsulation (MPLSoGRE), and Virtual Extensible LAN (VXLAN)—to set up virtual overlay networks. This allows Contrail Networking to integrate with physical network devices from any vendor, provided these devices work together to create an IP fabric for all computer resources within the data center.

High-performance gateways: Contrail Networking uses BGP to exchange routing information between control nodes and gateway nodes—Juniper Networks MX Series 3D Universal Edge Routers and/or QFX Series and EX Series Ethernet Switches, along with routers and switches from major networking vendors—to connect virtual overlay networks to physical networks as well as to attach non-virtualized servers or networking services to a virtual overlay network. The control node's ability to directly exchange routing information with the gateway eliminates the need to deploy an additional gateway software appliance in the virtual infrastructure, while maintaining the performance advantages of the existing router or switch. (See the Solution Components section for a description of the control node.)

Solution Components

Based on the principles of SDN, Contrail leverages BGP-signaled end system IP/VPNs to implement network virtualization overlays. These standards-based overlays, which span cloud boundaries, deliver a vendor-neutral approach for creating multitenant virtualized, containerized, and bare-metal cloud environments. Infrastructure analytics and visualization features provide insight into virtual and physical networks, simplifying operations and decision making with proactive planning and predictive diagnostic capabilities.

- **Contrail Controller** consists of the following components:
  - **Configuration nodes**, which are responsible for the management layer. Configuration nodes provide a northbound Representational State Transfer (REST) API that can be used to configure the system or extract system operational status. The instantiated services are represented by objects in a horizontally scalable database that is described by a formal service data model. Configuration nodes also contain an engine that transforms objects in the high-level service data model into corresponding lower level objects in the technology data model. Whereas the high-level service data model describes what services need to be implemented, the low-level technology data model describes how those services need to be implemented. The configuration nodes publish the contents of the low-level technology data model to the control nodes using the Interface to Metadata Access Point (IF-MAP) protocol.
  - **Control nodes**, which implement the logically centralized portion of the control plane. Not all control plane functions are logically centralized; some control plane functions are still implemented in a distributed fashion on the physical and virtual routers and switches in the network. Control nodes use the IF-MAP protocol to monitor the contents of the low-level technology data model, as computed by the configuration nodes, describing the desired state of the network. The control nodes use a combination of southbound protocols to make the actual state of the network equal to the desired state of the network. These southbound protocols include Extensible Messaging and Presence Protocol (XMPP) to control Contrail Networking's vRouters, as well as the BGP protocol to control physical gateways. The control nodes also use BGP for state synchronization when multiple control nodes are employed for scale-out and high availability reasons.
  - **Analytics nodes**, which are responsible for collecting, collating, and presenting analytics information for troubleshooting problems and understanding network usage. Each component of Contrail Networking generates detailed event records for every significant event in the system. These event records are sent to one of multiple instances (for scale-out) of the analytics node, which collates and stores the information in a horizontally scalable database using a format optimized for time-series analysis and queries. The analytics nodes have a mechanism that automatically triggers the collection of more detailed records when a certain event occurs; the goal is to determine the root cause of any issue without having to reproduce it. Analytics nodes provide a northbound analytics query REST API.
- **vRouter** is the forwarding plane of a distributed router, running in the hypervisor of a virtualized server. It extends the network from the physical routers and switches in a data center into a virtual overlay network hosted in the virtualized servers. The vRouter is conceptually similar to existing commercial and open-source vSwitches such as the Open vSwitch (OVS), but it also provides routing and higher layer services.

Business Need	Challenge	Contrail SDN-Enabled Solution
Rapidly deploy new services and/or applications	Rigid and static network infrastructure	Automate creation of agile and open cloud networks
Optimize operational costs	Redundant hardware-based infrastructures defined by departments	Consolidate networking infrastructures to be shared by multiple departments
Establish secure communication among departments	Shared and common network infrastructure	Segment each department over shared and common infrastructure
Rapidly deploy new offices	Complex and expensive replication of hardware resources at each office location	Allow network appliances to run as virtual network functions and be deployed with point-and-click operation from anywhere
Freely choose private or public cloud, depending on services and/or applications	Lack of networking tools to connect both cloud properties	Set up virtual overlay networks within both private and public clouds
Seamlessly connect overlay and underlay networks	Need for additional and purpose-built gateway	Set up virtual overlay networks between vRouter and existing high-performance switches and/or routers
Leverage the performance of existing physical underlay networks	Limited performance of purpose-built gateway	Eliminate the need for additional and purpose-built gateway by controlling existing high-performance switches and/or routers

Summary—Contrail Helps Enterprises Build an Open SDN-Enabled Network

If enterprises want to achieve their top-line growth objectives and stay competitive, they need to move their IT infrastructure to the cloud, delivering the flexibility, agility, and security required to provide users with anytime, anywhere access. This move to the cloud allows enterprises to innovate more quickly, develop and deliver new services faster, and reduce risks with a "fail-fast" methodology. These, in turn, increase productivity and facilitate faster business expansion.

Contrail is an SDN solution for implementing an open network in the cloud. It is enabling enterprises to achieve these significant objectives by creating secure multitenancy environments, and dynamically setting up virtual overlay networks that connect both physical and virtual networks:

- Foster innovation by simplifying SDN implementation, cloud deployment, network orchestration, and VNF operation
- Utilize shared physical infrastructures by securely segmenting each department with virtual overlay networks
- Host VNFs in various locations, including branch offices
- Connect virtualized workloads which reside in private and public clouds, furthering migration to a hybrid cloud
- Use existing physical underlay networks to connect with virtual overlay networks

Next Steps

For more information about Juniper Networks Contrail, please visit http://www.juniper.net/us/en/products-services/sdn/contrail/ or contact your Juniper 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

3510582-001-EN June 2016