Secure Your Cloud with Consistent Policy and Threat Mitigation Using Juniper Contrail Security

Diminish risk to any applications in any cloud

Challenge

The lack of a comprehensive security solution is preventing enterprises and SaaS companies from rapidly identifying and mitigating threats traversing their cloud environments.

Solution

Contrail Security mitigates risk to applications running in any cloud environment by enabling traffic discovery with automated policy enforcement that stops the spread of inside threats.

Benefits

- Reduces risk from malicious traffic with application-to-application flow visibility and discovery across hybrid cloud environments
- Enhances operational efficiency using abstracted policies that prevent security policy proliferation
- Simplifies and automates policy definitions and management, enabling complex enforcement
- Provides a consistent security policy framework across multiple heterogeneous environments such as OpenStack, Kubernetes, bare-metal servers, and public clouds
- Blocks bad traffic at the host and redirects suspicious traffic to a next-generation L7 firewall to provide adaptive threat containment

Security administrators and operators are forced to deal with a wide variety of threats that put their applications at serious risk and, in extreme cases, lead to catastrophic damage to their business. There are numerous examples of simple attacks against well-established brands that have led to a loss of critical and confidential data, doing irreparable harm to the company-customer relationship.

While the attacks themselves can be simple, the threats they pose are complicated and hard to contain once a breach occurs. Operators need an effective, high-performance security solution that can scale with their growing needs to stop the spread of lateral threats.

The Challenge

Enterprises and Software as a Service (SaaS) cloud providers are constantly building and deploying new cloud-native applications across multiple public and private clouds in pursuit of limitless scale, flexibility, and agility. As these dynamic and disaggregated applications scale, their components get distributed across multiple heterogeneous clouds, blurring the perimeter of the environment on which these applications run.

This renders legacy security solutions ineffective in eliminating the lateral “east-west” spread of inside threats and malware. As these distributed applications move from development to staging to production environments, more operational siloes are created, presenting security administrators and operators with the burden of having to create and manage an exponentially growing number of security policies. To further complicate matters, security administrators and operators do not have clear visibility into how applications interact and communicate with each other, and this prevents them from applying the most effective threat prevention policies. All of these factors result in a situation where applications are left to run in a non-scalable, unmanageable, insecure, and opaque multicloud environment.

Addressing these issues effectively requires true application traffic discovery and policy flow visualization in order to eliminate any kind of application opacity.

The Juniper Contrail Security Solution

Juniper® Contrail® Security, a member of the Juniper Contrail product family, is a simple, open, fully distributed cloud security solution that allows users to protect applications running in any virtual environment. Contrail Security enables operators in any industry to secure their applications in any cloud at scale. Policies based on known application attributes defined by tags, labels, and other grouping constructs can be universally applied in various environments without having to rewrite them for every new environment.

Contrail Security further enhances the security framework by providing critical insights into traffic flows, establishing a new security paradigm that reduces the overall number of policies, simplifies enforcement, and provides greater visibility and manageability across hybrid cloud environments.

Contrail Security gives both enterprises and SaaS cloud providers dynamic and scalable network virtualization in the form of a distributed, intent-driven security solution that allows them to:

- Secure applications seamlessly across private and public cloud infrastructures
- Secure tenant isolation via network virtualization while allowing them to reuse policies across environments without rewriting them
- Account for workload mobility and the ever-expanding perimeter
- Redirect suspicious traffic to select L7 firewalls named by application owner or security administrator intent
- Unify connectivity and comprehensive security across heterogeneous environments
- Gain unprecedented visibility into application domains, including violators and violations, to proactively initiate remedial action

Solution Components

Contrail Security consists of two key components: Contrail Security Controller and Contrail Security vRouter.

Contrail Security Controller

The Contrail Security Controller provides a logically centralized but physically distributed control plane for the Contrail Security solution. It acts as an interface for defining and expressing security intent without relying on network coordinates for policy construct. The Security Controller translates abstract security descriptions into lower level security constructs (such as access control lists), which are then propagated to enforcement elements on every host where the application workloads are hosted.

The Contrail Security Controller includes northbound REST APIs that allow orchestrators and other management systems to interface with the Contrail Security solution.

The Contrail Security Controller is composed of three software components:

- **Configuration:** The configuration component provides APIs to invoke Contrail Security functionality, acting as a compiler that translates high-level descriptions of security intent into lower level security constructs.
- **Control:** The control component implements the BGP speaker for peering with gateways, programming lower level security constructs into enforcement elements on hosts via Extensible Messaging and Presence Protocol (XMPP).
- **Analytics:** The analytics component provides a framework for collecting data such as traffic flows, statistics, logs, and other system state information over various ingestion channels such as GPB, IPFix, SNMP, NetFlow, sFlow, syslog, and from enforcement elements on hosts via a protocol called Sandesh. All ingested data is stored in highly available Cassandra databases for querying via northbound REST APIs. Applications that derive meaning and insight from the collected data are also provided.

Contrail Security vRouter

The Contrail Security vRouter is an enforcement element installed on every host where application workloads may be instantiated. The vRouter has full ownership of logical interfaces present on every workload, whether a VM or container, enabling the vRouter to enforce security policies inline. The vRouter can also route selected traffic to L7 firewalls. Each vRouter communicates with a pair of control nodes to optimize system resiliency.

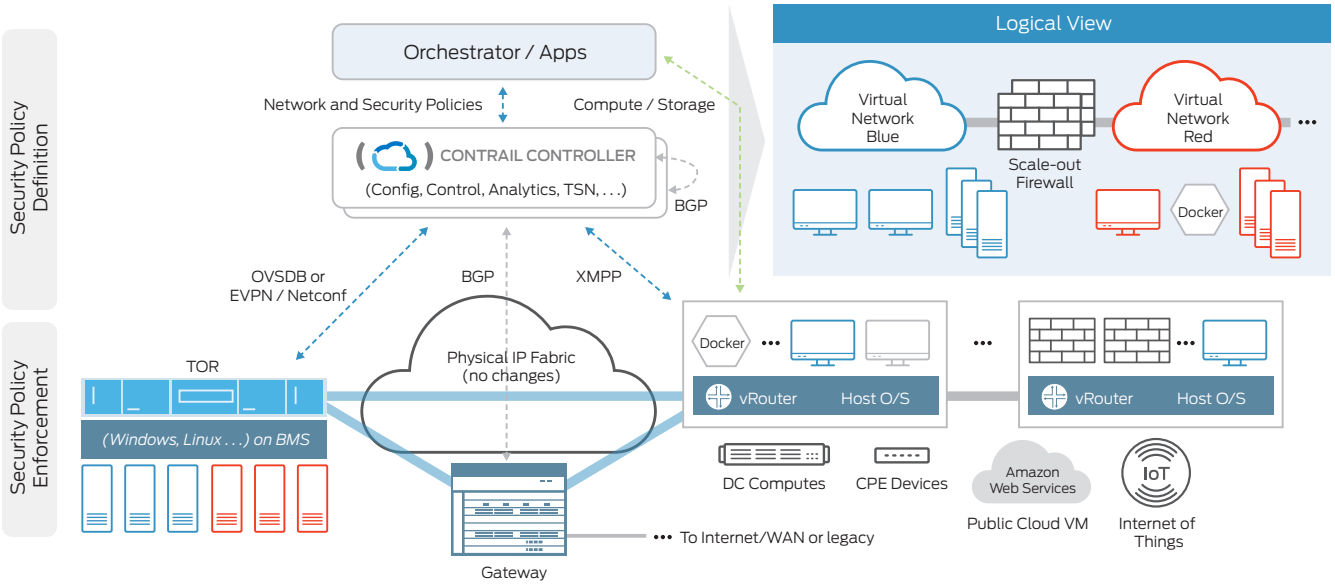

Figure 1: Contrail Security architecture

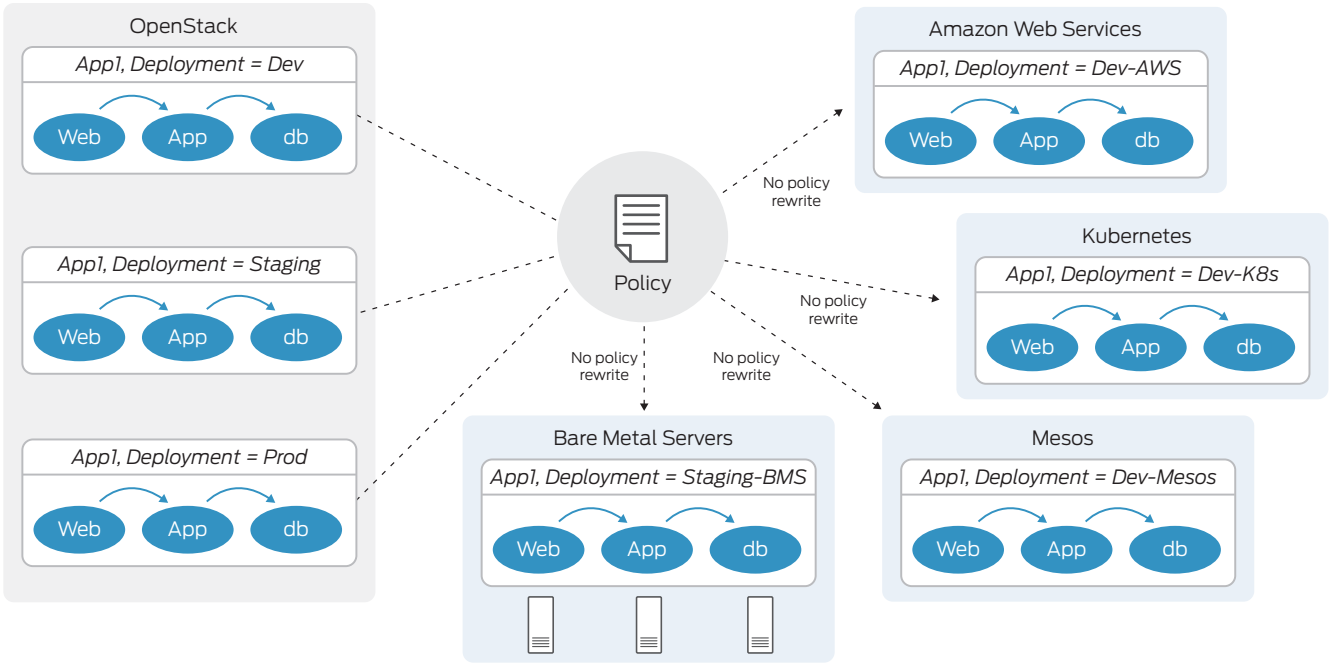

Figure 2: Consistent policy framework where policies are defined once and can be applied across multiple environments

Features and Benefits

- **Consistent intent-driven policy framework**: Using Contrail Security, operators can define and implement security policies using tags in plain English and scale it across multiple environments. The Controller takes these policies and enforces them on each compute node where the vRouter is installed, satisfying the intent of the operator. The need to define policies using IP address and VLANs is now eliminated.
- **Scalability and performance**: The Contrail Security Controller uses northbound REST APIs that can be integrated with popular orchestrators like OpenStack, Kubernetes, Mesos, VMware vCenter, and others. The distributed vRouter can protect workloads from inside threats, based on the intent-driven security policies defined by the operator. This protection can be extended by integrating Contrail Security with next-generation virtual firewalls to enable advanced security services, and to ensure that applications are protected.
- **Application policy configuration and flow visualization**: Contrail Security offers the ability to easily orchestrate and configure application security policies using templates and wizards. Contrail Security's dashboard offers deep insights into and visualization of intra- and inter-application interaction and communication. Contrail Security leverages machine learning that can detect and discover anomalies within the environment.

Contrail Security addresses the needs and challenges of virtually any organization (see Table 1).

Table 1: Contrail Security Features and Benefits

Business Needs/Challenges	Contrail Security Solution
Simplify policy across the environment	Reduced risk from malicious traffic with application-to-application flow visibility and discovery across hybrid cloud environments.
Visualize traffic between the applications	Enhanced operational efficiency by using abstracted policies, preventing rule proliferation.
Reduce operational complexity	Simplified and automated policy definition and management, enabling complex policy enforcement.
Scale security for any environment	Consistent security policy framework across multiple heterogeneous environments such as OpenStack, Kubernetes, bare-metal servers, public clouds, etc.
Protect applications beyond east-west security policies	Adaptive threat containment by blocking bad traffic at host and redirecting suspicious traffic to next-gen L7 firewall.

Summary—Simplifying Security in the Cloud

Contrail Security simplifies operations by applying unified, consistent, and intent-driven security policies through APIs, seamlessly interoperating with existing security controls and environments. Furthermore, Contrail Security adaptively responds to any threat from inside or outside the cloud by sitting close to application workloads and enforcing policies using a highly scalable and performant enforcement module.

With Contrail Security, Juniper Networks is transforming the way enterprises and SaaS cloud providers protect, manage, and monitor their cloud-native applications in multicloud and multiplatform environments.

Next Steps

For more information about how Juniper Contrail Security can help your organization, please visit www.juniper.net 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

3510623-001-EN Aug 2017