Contrail Security

Product Overview

Contrail Security, a member of the Contrail product family, is a simple, open, fully distributed cloud security solution that allows users to protect applications running in any virtual environment. 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 every time.

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 into—and manageability across—hybrid cloud environments.

Product Description

Chief Information Security Officers (CISOs) and security administrators are faced with an ever-increasing list of threats to their applications, whether they are deployed in development, staging, production, or public cloud environments; running on bare-metal servers (BMS), on virtual machines (VMs), or within containers; or orchestrated by OpenStack, Kubernetes, or OpenShift. Workload mobility in modern cloud environments exacerbates the problem, adding a new level of difficulty for securing workloads that migrate frequently.

As a result, the network perimeter is now blurred, rendering traditional perimeter-based application security measures insufficient, inflexible, and extremely cumbersome and costly to manage. The current decentralized, distributed, and democratized application development model, spurred by the rise of containerized infrastructure and the availability of cloud infrastructure, both public and on-premise, demands a similarly democratized and agile solution for securing the applications themselves. Developers must be able to express their application security requirements, while security administrators must be empowered to overlay those requirements with additional rules and policies transparent to the developers.

Juniper® Contrail™ Security introduces a new paradigm for expressing, enforcing, and visualizing security rules and policies. Working with various cloud orchestration platforms such as OpenStack, Kubernetes, and VMware, and integrating with L7 firewalls to provide a comprehensive security solution, Contrail Security leverages advanced analytics to provide deep insights into application security with easier diagnostics, rich reporting, custom application development, and machine automation.

Architecture and Key Components

Contrail Security includes two key components: the Contrail Security Controller and the Contrail Security vRouter.

Contrail Security Controller

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

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 comprised of three software components:

- **Configuration:** The configuration component provides APIs to invoke Contrail Security functionality and functions 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, and it programs 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.

Features and Benefits

Key Features

- **Intent-driven policy:** Contrail Security allows tenants and administrators to express security requirements in plain English, without relying on network coordinates to write policies.
- **Tag workloads and expressions:** Policy statements are written using tag expressions that describe application attributes, replacing the traditional method of using network coordinates. This relieves administrators and tenants of having to know and monitor dynamic, ever-changing network coordinates.
- **Fully distributed firewall:** Contrail Security deploys a vRouter enforcement component on every host where application workloads may be launched. The vRouter is embedded in the cloud infrastructure; there is no need for tenants to modify their applications to take advantage of Contrail Security. The vRouter provides up to L4 security in a fully distributed manner on every host.
- **Redirect to L7 firewall:** Contrail Security provides the ability to subject select traffic to L7 firewalls in a completely dynamic and programmatic fashion.
- **Analytics:** Contrail Security offers a rich framework for collecting various application, infrastructure, network, and security analytics over various supported ingestion protocols. Applications written on top of the analytics collection framework can extract meaningful insights from collected data.
- **Visualization:** Users can visualize traffic flows across different applications and application components, as well as associated security policies including adherence and violation status.

Key Benefits

- **Multidimensional policy statements:** Contrail Security provides the ability to write, review, and approve policies once and apply them universally in all environments, dramatically reducing the number of policy statements, simplifying manageability, and significantly containing security costs.
- **Comprehensive security:** Up to L7 security via connectivity and firewalling provides complete, end-to-end protection from a single pane of glass. Additionally, L4 through L7 security is fully distributed and available on every host, minimizing the attack surface as much as possible.
- **Actionable insights, visibility, and visualization:** Users gain complete visibility into various aspects of application, infrastructure, network (underlay and overlay), and security from a single pane of glass and via a single product.
- **Lower risk, greater compliance:** Contrail Security offers a complete, end-to-end, modern approach that defends against various lateral and external threats, lowering risk and significantly improving compliance.

Key Functionality

- **Open source and open standards across heterogeneous environments:** Contrail Security eliminates the need to rip and replace or change any tenant application workloads by installing a kernel-resident software enforcement element on the host (rather than guest application VMs). This provides fully distributed firewalling up to L4. It also integrates with, and can redirect select traffic to, several L7 firewalls.
- **Intent-driven (software-defined) security:** Contrail Security allows for security intent to be specified in plain English via tag expressions without needing to specify networking constructs. The Contrail Security Controller translates this high-level intent into specific security ACLs.
- **Visualization:** Contrail Security provides a rich interface for gaining deep visibility into traffic flows, mapping them to application topologies. The interface also correlates observed traffic with corresponding security policies and observed volumes. Successive levels of granularity may be selected to gain the appropriate visibility.

- **Analytics:** The Contrail Analytics Engine is designed for very large-scale ingestion and querying of structured and unstructured data, including specific aspects such as application usage, infrastructure utilization, system logs, security events, security logs, and network statistics like flows, latencies, and jitter. Several ingestion channels/means such as GPB, syslog, IPfix, sFlow, and SNMP are supported. All ingested data is deposited in highly available Cassandra databases for later retrieval and processing. A high-level query interface, as well as REST APIs and a rich GUI, can be used to extract the information exposed by the Analytics Engine.

  By providing both real-time and historical information, the Analytics Engine helps users gain better insights to easily diagnose issues within the infrastructure. Users can also employ REST APIs and modern techniques like Hadoop to write custom applications for reporting and/or infrastructure automation.

  Contrail Security also provides certain value-added applications that leverage the analytics framework to correlate the overlay with the underlay and detect statistical anomalies, among other features.

Contrail Security Use Cases

Contrail Security gives both service providers and enterprises dynamic and scalable network virtualization, and 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 reusing 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
- Maintain insights and the ability to query past records for historical research and compliance purposes

Specifications

System Recommendations and Operating Environment

- Orchestration systems: OpenStack, Kubernetes
- Hardware: 64-bit dual x86 processor, minimum memory 12 GB RAM
- Storage: 30 GB Serial Advanced Technology Advancement (SATA), Serial Attached SCSI (SAS), or solid-state drive (SSD); volume storage: 2 disks with 2 TB SATA
- Network: 1 GB interface card (1)
- OS: Linux OS (CentOS, RHEL 6.4, Ubuntu 13.x)

Ordering Information

What to Buy

This product adheres to the Juniper Care Software Advantage pricing model. Be advised of the following items that constitute an order:

- Select a software license based on the number of sockets required. The license is either subscription (fixed term) or perpetual (unlimited term).
  - A subscription software license includes Juniper Care Software Advantage, entitling you to software updates and upgrades, 24x7 remote technical support, and online support.
  - A perpetual software license excludes Juniper Care Software Advantage; the latter must be purchased.
- If your order includes a hardware product/platform, select a hardware license based on your networking, connectivity, and/or security requirements (e.g., interface options, I/O, services). You may need to purchase additional licenses in support of the base hardware license (e.g., power cables, network interface cards).
- If this is a virtual appliance/software product, you would not buy any hardware license from Juniper, but instead, procure the hardware elsewhere. For information on supported hypervisor(s) and VM requirements, please refer to the technical documentation for this product on our website (www. juniper.net) under the support section.

Juniper Networks products are sold directly as well as through Juniper partners and resellers. For more information on the Juniper Care Software Advantage business model, please visit www.juniper.net/us/en/products-services/sdn/contrail/. For information on how to buy, please visit www.juniper.net/us/en/how-to-buy.

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

1000621-001-EN Aug 2017