CLOUD-NATIVE CONTRAIL NETWORKING

Product Overview

Service providers and enterprises are evolving to cloud-native using the same technologies as the public cloud providers to achieve greater agility, flexibility, and improved economics across a hybrid-cloud ecosystem. Cloud-Native Contrail Networking (CN2) is a Kubernetes-native SDN that secures and automates virtualized Infrastructure as a Service (IaaS) and multiple containerized application clusters into an integrated network. With support for OpenStack and Kubernetes orchestration, CN2 delivers hybrid-SDN for a consistent NetOps and infrastructure-as-code model that is open, simple, and secure, allowing organizations to migrate to cloud-native at their own pace.

Product Description

Service providers and enterprises rely on the cloud-native operational model to run scalable applications in modern, dynamic environments such as private, public, and hybrid clouds. Beneath and alongside the cloud and cloud-native abstraction and platforms, legacy systems and applications must communicate with dynamic and ephemeral workloads across a physical network connecting end users, legacy systems, applications, and partners.

Cloud-native API-driven microservice architectures increase development, IT, and service agility, but they pose a networking challenge requiring massive API communication running over the network. Such networking infrastructure must be secure, automated, scalable, reliable, and programmable to deliver on the promise of cloud-native agility, elasticity economics, and digital-age expectations of service assurance. With Juniper® Cloud-Native Contrail Networking™ (CN2), organizations can extend Kubernetes to simplify DevOps and to orchestrate containerized microservices with intent-based declarative provisioning and APIs. By adding automation for security, management, and more through CN2, organizations can focus on developing and delivering innovative technology products and services to their customers quickly.

CN2 is a cloud-native, SDN solution that automates the creation and management of virtualized networks to connect, isolate, and secure cloud workloads and services seamlessly across private and public clouds. Using the standard Neutron interface and Container Network Interface (CNI), CN2 integrates with all OpenStack, OpenShift, and Kubernetes distributions delivering hybrid SDN orchestration for virtualized switching, routing, security, Network Address Translation (NAT), load balancing, and more.

CN2 preserves investments in existing orchestration platforms, licenses, skills, and processes. It provides dynamic end-to-end virtual networking and security for cloud-native containerized workloads, as well as virtual machine (VM) workloads, across multicluster compute and storage environments, from a single point of operations. It is well suited to the requirement of hard multitenancy for single or multicluster environments shared across many tenants, teams, applications, or engineering phases. It scales well in tenants, virtual networks, policies, and compute nodes, where AT&T, eBay, NTT, and Workday, for example, use it to manage virtual networking in clusters of thousands of nodes.

CN2 operates with centralized control over a distributed set of vRouter forwarding planes on all worker nodes in the cluster. CN2 offers advanced networking but with simplified configurations and management for features like overlay and underlay forwarding; service chaining; federation of gateways, controllers, VNF workloads; remote-edge compute clusters; and dynamic network learning. Its carrier-grade feature set is why tier-1 service providers like British Telecom, Deustche Telekom, Etisalat, and Saudi Telecom rely on CN2 for telco cloud.

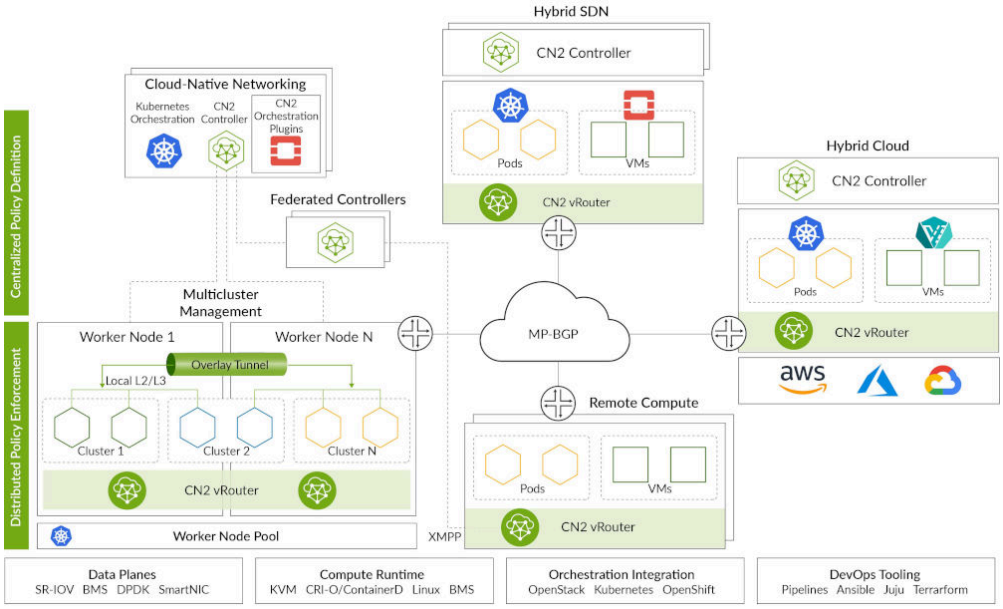

Figure 1: CN2 supports distributed policy enforcement with centralized policy definition.

Architecture and Key Components

CN2 has the following key components:

Modern, Kubernetes-Native Management and Control Plane

CN2's modernized control and management plane operates natively in Kubernetes to simplify its deployment and automate upgrades. Configurations are modeled with intent-based, declarative custom resources, extending Kubernetes and lending themselves well to infrastructure-as-code and GitOps. High availability and high scale are implemented in three or more nodes per cluster for carrier-grade production environments.

High-Performance CN2 vRouter Data Plane

CN2's vRouter forwarding plane delivers high-performance networking for VM, container, and bare-metal server workloads with kernel, Data Plane Development Kit (DPDK), and SmartNIC implementations to optimize CPU resources, space, and cost. The vRouter provides consistent, high-performance forwarding for both OpenStack and Kubernetes workloads to unify environments and simplify operations. Centrally managed and programmable, CN2's vRouter delivers distributed forwarding and security enforcement at the edge of the data center, cloud, and network to support low-latency, high-capacity applications.

CN2 Management Web GUI and Plug-Ins

CN2 has a plug-in for the open-source GUI. The Lens plug-in provides troubleshooting and debug tools across the multicluster that can work with any Kubernetes orchestration. A Web GUI further enhances CN2 and Kubernetes multicluster provisioning and simultaneous observability. Both GUIs are optional as are all analytics add-ons that provide Grafana dashboards. Users can choose the types of operations tooling that works best for them.

Key Capabilities

Cloud-Native Networking

Built upon a Kubernetes-native control plane, CN2 is cloud-native and Kubernetes-native, enabling SDN operations portability and a consistent experience across hybrid clouds and diverse orchestration distributions.

SDN for Hybrid and Mixed Orchestration

CN2 integrates any Kubernetes and OpenStack platforms into a hybrid SDN to support virtualized and containerized workloads and operational investments as organizations evolve to cloud-native and need to straddle hybrid, multicloud, and multivendor orchestration platform distributions.

NetOps-Driven Automation

CN2 is tested, qualified, and deployed using project Argo-based CN2 with Pipelines, a GitOps and Continuous Integration/Continuous Delivery (CI/CD) model for NetOps to deliver reliability engineering at hyperscaler speed. Networking infrastructure-as-code, provisioning workflows-as-code, and test/staging workflows-as-code using the CN2 Pipelines test suites simplify operator qualification and life-cycle management of CN2 with any Kubernetes distribution, custom environments, and custom workloads.

Multicluster Management and Scale

CN2 reduces the cost and complexity of multicluster operations, using a single CN2 instance to serve as the CNI for many Kubernetes clusters for intra- and inter-cluster connectivity as well as cluster load balancing to enhance performance and availability. The CN2 Web GUI also streamlines operations across user-defined groups of multiple clusters—by team, by deployment purpose, or by geography. In addition, network federation, Kubernetes federation, and Prometheus federation provide one-to-many centralized management and control to achieve operational scale and reduce costs for distributed and prolific multicluster deployments.

Edge and Remote Compute

Centrally managed and programmable, CN2's low-profile vRouter data plane supports edge "Remote Compute," a deployment model that simplifies cloud orchestration and operations for numerous space-constrained, distributed edge sites to deliver operational scale and reduced OpEx. This goes beyond the stretched OpenStack or Kubernetes cluster architecture to further optimize local network overlay-network gateways at each remote site without any distributed CN2 Controller software overhead.

Application-Aware Security and Service Chaining

CN2 features a logically centralized, policy-based rules engine to define, apply, and manage granular security policies that are enforced through the distributed fleet of vRouters on all cluster nodes. SecOps tasks of definition, application, and enforcement visibility are simpler and superior to Kubernetes Network Policy objects and complementary to optional service mesh policies. Using metadata, user-defined tags, and attributes, CN2's security and encryption mode simplifies security and privacy administration at scale with dynamic security policies that follow namespaces, services, and workloads across clusters.

CN2's security features are further extended and enhanced by Juniper Networks® vSRX Virtual Firewall and Juniper Networks cSRX Container Firewall. These are virtualized and containerized next-generation stateful firewalls that complement CN2's service chaining and insertion capabilities. Service chaining is also compatible with third-party firewalls and virtualized network functions (VNFs). Moreover, Juniper Connected Security products help organizations safeguard their entire estate, data, and users through a threat-aware network. Juniper Cloud Workload Protection shields cloud-native workloads from zero-day threats, and Juniper Advanced Threat Prevention service protects against known and unknown threats while assessing and verifying server and workload risk, even in encrypted traffic.

Unmatched Advanced Networking Services

Embedded services like BGP as a Service (BGPaaS), native equal-cost multipath (ECMP) (without kube-proxy), and vRouter L2 multilink bonding and L3 multihoming eliminate the cost and complexity of integrating third-party products and simplify the delivery of advanced services. Typical cloud-native bolt-ons such as ingress controller, multi-NIC capabilities, load balancing, and firewalls are built in. Controller support for internal and external BGP (iBGP and eBGP) InterAS options seamlessly extends the network into existing MPLS networks to simplify legacy integrations.

Enhanced Observability

With optional and configurable analytics for monitoring and troubleshooting, CN2 provides enhanced observability with plug-and-play usability for some of the most popular open-source projects like Prometheus, InfluxDB, Grafana, FluentD, and ElasticStack for ease of use, platform flexibility, and low cost. Traffic mirroring and flow analytics can be used for situational awareness, troubleshooting, and regulatory compliance.

Ultra-Fast, High Performance

The CN2 vRouter forwarding plane delivers high-performance networking for VM and container workloads with kernel, DPDK, and SmartNIC implementations. This delivers an assured application experience while preserving valuable CPU resources for revenue-generating services. An eBPF form factor of CN2 vRouter is in limited tech preview.

Key Benefits

- **Simple**: Automates Day-0 to Day-2 cloud networking using a NetOps model for CI/CD to simplify life-cycle management delivering quality, stability, and always-on reliability. CN2 is easy to try in simplified Kubernetes environments like minikube and cloud-based Terraform automated deployments.
- **Cloud-Native**: Protects and integrates existing VNF workloads, tools, and operations into a hybrid OpenStack and Kubernetes cloud to reduce training requirements for internal teams, speed time to market for new services, and lower costs while seamlessly evolving to cloud-native.
- **Operationally Consistent**: Unifies operational expertise and processes to enable workload portability and operational independence across a hybrid-cloud ecosystem to improve economics and deliver partnership flexibility, simplicity, and choice.
- **DevOps-Friendly**: Enables larger multipurpose and multitenant clusters to be elegantly secured through isolation and still benefit from overlapping network addressing for consistency and conflict avoidance. Additionally, all of CN2's configuration can be partitioned and managed as code alongside various applications driven by GitOps. This model streamlines DevOps and improves application security policy design and compliance.
- **Advanced**: Automates and simplifies cloud networking with highly scalable overlays and service chaining without limiting protocol support or requiring distributed routing protocol agents with complex configuration. CN2 easily federates to share virtual networks and routes using standards-based BGP with other CN2 instances, workloads, and external devices.

CN2 Use Cases

Enterprises and service providers can use CN2 to:

Deploy Distributed 5G Edge Clouds

- Deliver 5G enhanced Mobile Broadband (eMBB), massive Machine Type Communications (mMTC), and Ultra-Reliable Low-Latency Communications (URLLC) services distributing high-performance, low-profile remote compute cloud networking to the network edge
- Contain cluster sprawl with multicluster management and federation
- Operationally scale and simplify highly distributed edge clouds with Juniper Apstra collapsed-fabric integration

Secure Networking in the Cloud

- Mitigate lateral attacks and unrestricted cluster connectivity using dynamic networking policy to isolate network segments and traffic within and across clusters
- Distribute security policy at the edge using microsegmentation to protect worker node traffic, user data, and applications
- Partition and isolate namespaces, services, and pod networking to reduce your applications' exposure to external networks
- Manage security policy at scale using global security policies across multicluster networks
- Extend and enhance security features through the Juniper Connected Security and zero touch security portfolios of physical, virtual, and containerized Juniper Networks SRX Series firewalls, Juniper Cloud Workload Protection, and Juniper Advanced Threat Prevention (malware protection)

Simplify Hybrid Cloud and Multicloud

- Simplify Kubernetes operations with a common network services model and API across multiple cloud and on-premises deployments
- Simplify operations across OpenStack, OpenShift, and Kubernetes and multiple distributions with this hybrid SDN tool and its consistent model, API, and operational experience

Automate VNF/CNF Deployments Through Service Chaining of Any Network and Security Service

- Provide service orchestration of any Juniper or third-party network and security service (physical or virtual)
- Instantly add, update, delete reachability for ephemeral telco workloads (5G, radio access network (RAN), etc.) through BGPaaS
- Insert waypoint advanced network services (next-generation firewall, IPsec, source NAT, destination NAT, etc.) with on-demand service chain insertion
- Provide virtualized subscriber or business edge with chaining of services, including deep packet inspection (DPI), security (firewall, anti-DDoS), proxies, and caching

Key Features

Table 1: Key Features

Features	Feature Description
Advanced Networking	
Routing and bridging	Juniper has a full suite of L2 (EVPN, VLAN, VXLAN) and L3 (eBGP, iBGP, MP-BGP, MPLS) services to deploy full-featured, scalable networking solutions. Integration into existing data center fabrics and MPLS backbones is seamless.
Traffic mirroring and flow analytics	Statistics collection and monitoring of flows bring greater visibility into the behavior of the traffic and policy conformance in your cluster. Traffic can be mirrored to virtual and physical devices for integration with external analysis platforms.
Hub/spoke and mesh virtual networks topology	CN2 constructs logical network topologies using flexible, virtual network routers. This mechanism enforces network isolation into virtual networks that are more elegant than security policies and shared easily through network federation.
Layer 3 multihoming	vRouter utilizes multiple next hops in the forwarding table when multiple uplinks in the underlay are present. Routing protocols can be leveraged in the hypervisor for dynamic load balancing and failure protection.
BGPaaS for containers and VMs	BGP as a Service is delivered locally on the hypervisor to establish BGP connections from the container or VM and proxies these advertisements to the rest of the network. This provides dynamic network reachability of network functions and applications in the cluster.
Load balancing	CN2 vRouter load balancing for services is L4 native, non-proxy load-balancing-based on ECMP. This includes Kubernetes services type load balancer not available with other CNIs. The instance-ip (service-ip) is linked to the ports of each of the pods in the service. This creates an ECMP next-hop in CN2 and traffic is load-balanced directly from the source pod. CN2 also includes an add-on option for an Ambassador Ingress in Kubernetes for L7 load balancing and OpenStack LBaaS. It is fully compatible with other Ingress controllers as well.
Selective overlay tunneling	Overlay tunneling (MPLS over UDP, MPLS over GRE, or VXLAN) abstracts the physical underlay to scale networks with isolation, policy, and security. Utilize direct underlay routing to selectively bypass overlay tunnels and directly access physical networking resources.
High-performance forwarding	High-performance vRouter networking includes kernel, DPDK, and SmartNIC implementations. Reference the list of supported network interface partners for more details.
SDN gateway	CN2 interoperates with most physical or VM-based routing and switching equipment that supports L3VPN or EVPN with the appropriate overlay network encapsulation standards (VXLAN, MPLSoGRE, MPLSoUDP). This includes interoperability with Juniper Networks MX Series Universal Routers and QFX Series Switches, as well as other vendors' devices to seamlessly connect to the WAN or legacy networks and workloads.
Monitoring	Optional analytics based on Prometheus and Grafana integrate with existing cloud ecosystem components, providing a centralized platform for robust insight into SDN operations, cluster health, and diagnostics. Optional flow monitoring employs InfluxDB. Besides native Grafana dashboards, monitoring is simplified in the optional Contrail Lens plug-in and Web GUI.
Troubleshooting	CN2 collects cluster health, network statistics, and flow data which is then aggregated and presented through the CN2 Web GUI for troubleshooting. CN2 also exposes a number of logging, introspect, and tracing features for deep troubleshooting, resulting in faster serviceability and mean time to repair (MTTR).
Advanced Security	
Microsegmentation	Networking and security policies are defined centrally, then applied to network objects through labels and enforced at the distributed vRouter, providing security enforcement at each virtualized and containerized workload.
Multitenant and namespace network isolation	The use of tenant domains and L3 VPNs to create virtual networks inherently provides a secure segregated environment, where virtual networks cannot talk to each other without policies. Securely partitioned clusters using virtual routing and forwarding (VRF) and namespaces optimize flexibility, agility, and compute across multiple applications, users, teams, and tenants.
Label-based security policy	Going beyond rudimentary Kubernetes NetworkPolicy, CN2's additional security and firewall rules create flexible and granular policies using metadata, tags, and attributes (vs. routing/IP info alone) to create a layer of abstraction for finer grained isolation that is simpler to design and configure (e.g., isolation between development, test, and production).
Drop/deny alerting and visibility	Flow records and alert logs on CN2 policies provide visibility and audit compliance (e.g., no flow) to quickly identify potential security threats and optimize traffic flows.
Service chaining transparent insertion of L7 next-generation firewall (NGFW)	Policy-driven, dynamic, service chaining helps users easily creates and deliver flexible security services (e.g., steering traffic to a vSRX/cSRX NGFW).
VPN services	VPN services include MPLS over GRE, MPLS over UDP, VXLAN overlays implementing network slicing in the cluster.
Advanced Federation and Multicluster	
One CN2 to many clusters CNI and analytics	A single CN2 SDN cluster configured to manage many Kubernetes clusters improves operational efficiency and reduces cluster sprawl.
Edge/remote compute	Centralized CN2 SDN cluster management of remote vRouter worker nodes (e.g., distributed edge clouds) improve operational efficiency and reduce costs.
Multicluster policy federation for network/security	Using CN2 with KubeFed allows a single primary Kubernetes control plane to coordinate multiple Kubernetes and CN2 clusters to simplify higher scale, multicluster networks and services.
BGP cluster-to-cluster peering	Open standards-based BGP with CN2's simplified peering configurations extends reachability between clusters and to the WAN providing end-to-end network and multicluster reachability and logically shared virtual networks.

Ordering Information

Model Number Structure	Model numbers and descriptions
License tiers: • Standard • Advanced • Premium	S-CN-S1-* = standard tier, includes multitenant network overlays, service chaining for OpenStack or Kubernetes use cases. S-CN-A1-* = advanced tier, adds DPDK and SmartNIC vRouter, BGPaaS, remote compute architecture. S-CN-P1-* = premium tier, adds Juniper Apstra integration and containerized routing protocol process (daemon) (cRPD) support with vRouter routing. Apstra and cRPD sold separately.
CN2 with Pipelines (CI/CD support) • '1' without CN2 with Pipelines • '2' includes CN2 with Pipelines	S-CN-S2-* = S1 tier with CN2 with Pipelines full CI/CD support and CN2 test suite. S-CN-A2-* = A1 tier with CN2 with Pipelines full CI/CD support and CN2 test suite. S-CN-P2-* = P1 tier with CN2 with Pipelines full CI/CD support and CN2 test suite.
Class types	S-CN-*-C4-* = Certified and integrated OpenStack (Red Hat RHOSP, Canonical/Juju). S-CN-*-C3-* = Red Hat OpenShift Operator integrated. S-CN-*-C2-* = Pre-integrated K8s (Juju/Canonical, Rancher). S-CN-*-C1-* = Upstream Kubernetes. Integration may be self-tested with CN2 with Pipelines tier.
Subscription duration terms	S-CN-*-C1-1 = 1 year of support and software subscription. S-CN-*-C1-3 = 3 years of support and software subscription. S-CN-*-C1-5 = 5 years of support and software subscription.

Model Number Structure	Model numbers and descriptions
Examples sold per vRouter compute node (controller node not licensed)	S-CN-S1-C4-1 = standard tier license for 1 year for OpenStack. S-CN-S1-C3-5 = standard tier license for 5 years for OpenShift. S-CN-S2-C2-5 = standard tier with CN2 with Pipelines license for 5 years for Kubernetes. S-CN-A2-C2-1 = advanced tier with CN2 with Pipelines license for 1 year Kubernetes integrations such as Amazon EKS, and Kubernetes from Canonical or Rancher. S-CN-A2-C1-1 = advanced tier with CN2 with Pipelines license for 1 year Kubernetes integrations such as upstream K8s.

Juniper Networks products are sold directly as well as through Juniper partners and resellers. Please contact your Juniper account team or partner for licensing. For more information on how to buy, please visit: https://www.juniper.net/us/en/how-to-buy/form.html.

About Juniper Networks

At Juniper Networks, we are dedicated to dramatically simplifying network operations and driving superior experiences for end users. Our solutions deliver industry-leading insight, automation, security, and AI to drive real business results. We believe that powering connections will bring us closer together while empowering us all to solve the world's greatest challenges of well-being, sustainability, and equality.

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

www.juniper.net

APAC and EMEA Headquarters

Juniper Networks International B.V.

Boeing Avenue 240 1119 PZ Schiphol-Rijk

Amsterdam, The Netherlands

Phone: +31.207.125.700