DATA SHEET

# Vyatta Service Edge

## Redefining the service edge

The enterprise Wide Area Network (WAN) landscape is rapidly transforming. The 'core' and 'branch' are being redefined in new contexts. The branch—whether offices or remote workers—is more far-reaching than it used to be. As application digitization progresses, the core stretches into core-plus-edge to house and process distributed data.

Enterprises are aiming to get ahead—and stay ahead—of these multifaceted and dynamic requirements. As far as is practical, the business demands of enterprises are not solely met by traditional WAN use cases. More than just a replacement of their existing solutions, organizations are looking to adjust network architecture and network operations tools and processes.

Conversely, Service Providers (SPs) recognize that a modern WAN approach is only efficient if integrated well with the underlying network infrastructure. For all its benefits, the adoption of software-defined and novel combinations of existing site-transport types will continue to accelerate. Furthermore, to be of value, related managed services must offer a more tailored WAN management for each organization's needs. SPs want to be efficient with these new paradigms to lower costs, achieve operational simplicity, and improve portfolio differentiation.

A modern WAN strategy mandates an agile approach, and Vyatta® Service Edge is designed with that in mind. From overlay to underlay, emerging technologies to existing solutions, Vyatta Service Edge creates the right packages for enterprises, SPs, and Managed Service Providers (MSPs) alike to simplify combinations of WAN deployments—whether on net or off net. Moreover, it allows for composing and deploying unique new services to drive differentiation and strengthen competitiveness.

Vyatta Service Edge brings together Ciena's proven Vyatta NOS, including new edge servers, and Cirrus Orchestrator management and orchestration services. It also combines one of the highest performing operating systems in the industry, a flexible orchestration platform, and a cost-optimized operating model better tuned to the new demands of the WAN from the cloud to the edge. This integrated approach is critical to cultivating a WAN ready to adapt to changing conditions—today and tomorrow.

### Highlights

- Brings together the established Vyatta Network Operating System (NOS), including new edge servers, and the Cirrus Orchestrator's management and orchestration services
- Accelerates the adoption of traditional WAN, software-defined, and cloud designs with proven NOS
- Offers platform choice, available in a series of physical, virtual, and cloud platforms
- Leverages one of the industry's most flexible and customizable service templates and parameters through Cirrus Orchestrator
- Delivers a cost-optimized, agile operating model for the evolving needs of the WAN from the cloud to the edge, regardless of whether it is on net or off net

### Telco-grade, proven, and trusted

Ciena's Vyatta NOS is trusted by some of the largest global Tier 1 SPs and enterprises. It is a highly scalable, purpose-built data-forwarding plane for extending the WAN and edges across clouds in a broad series of physical, virtual, and cloud platforms—all using identical software.

### High-performance plane support

The Vyatta NOS can assign multiple vCPUs to each forwarding and control/service plane while leveraging patented technology. This configuration not only maximizes performance but also reduces resource contention. As a result, as the service and control plane scales, the data plane follows suit while diminishing the demand for compute memory and storage, optimizing the utilization of the underlying hardware infrastructure.

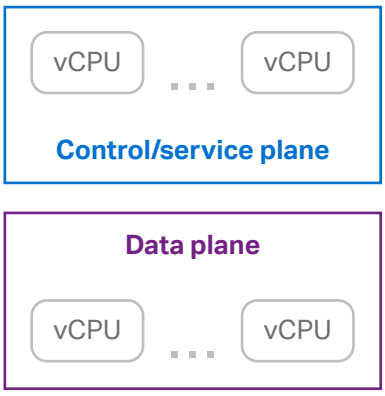


*Figure 1. Vyatta NOS high-performance architecture*

Even though the planes' performance scales independently, the NOS also improves packet processing across silicon and general compute architectures, significantly reducing capital and operating costs.

### Advanced routing

The Vyatta NOS offers a feature-rich routing stack with full support for IPv4 and IPv6 dynamic routing protocols (BGP4/6, OSPFv2/v3, IS-IS, RIP), multicast, Policy-Based Routing (PBR), tunneling/VPN, and network services (DHCP, DNS). A comprehensive list is shown in the technical information section of this data sheet.

### Secure connectivity

The system's firewall features a robust IPv4/IPv6 stateful packet inspection to intercept and inspect applications, monitor network activity, and protect critical data. Furthermore, all primary security functions, like Access Control List (ACL) and Network Address Translation (NAT), are tied to the Deep Packet Inspection (DPI) engine, offering application-level protection and tooling.

### Application-aware native

Vyatta NOS can easily adopt an application-aware overlay natively integrated with its advanced routing and security suites. It employs application policies wherein matching application flows are assigned a set of thresholds—such as Quality of Service (QoS) traffic type and priority—and steered based on preferred forwarding paths to the internet, chosen overlay sites, selected links, or links in designated overlay groups.

Behind the scenes, Vyatta NOS has a robust suite of application-recognition and traffic-prioritization tools. It recognizes thousands of critical business-application signatures (for example, Microsoft 365) with DPI for later enforcing the configured business policies and steering traffic through the forwarding paths.

### A familiar, fully programmable software

The Vyatta NOS enables operators to interact with network elements in a familiar way. Operators accustomed to working with traditional routers and switches can use a standard CLI interface, while operators more comfortable with software can use Linux commands, including all embedded scripting functions, libraries (e.g., Python), and shells. The operating system can expose any function along any supported API—such as network configuration (NETCONF) and REST—regardless of which interface is used, so network operators can automate the deployment with their chosen DevOps tools.

### Platform examples supported by Vyatta NOS

Vyatta NOS can be deployed across physical, virtual, and cloud networking environments for maximum deployment flexibility.

Ciena's Edge Server family comes certified to deliver Vyatta NOS–powered edge services and applications. Both the 3844 and 3848 leverage a patented technology for combining the advanced network functions and the hypervisor at the host layer to maximize hardware performance.

The 3844 and 3848 both have a 1 Rack Unit (1U) form factor for WAN or Local Area Network (LAN), with port speeds ranging from 1 Gb/s up to 10 Gb/s. Both models have Ethernet ports that can support Small Form-Factor Pluggable (SFP) or SFP+ connectivity and RJ-45 connections, enabling fiber or copper connectivity.

Ciena's 3844 Edge Server is a 1RU rackmount 4-core device powered by an Intel Xeon processor, with 10x 1GbE RJ45 and 4x 10/1G SFP+ interfaces.

*Figure 2. Ciena's 3844 Edge Server*

Ciena's 3848 Edge Server is a 1RU rackmount 8-core device powered by an Intel Xeon processor, with 10x 1GbE RJ45 and 4x 10/1G SFP+ interfaces.

*Figure 3. Ciena's 3848 Edge Server*

Vyatta NOS can also be deployed as Virtual Network Function (VNF) using network virtualization technologies or as a cloud instance on Microsoft Azure.

## A wide variety of use cases

The Vyatta NOS supports a variety of use cases, addressing both traditional WAN and modern application-aware needs. The NOS can be deployed on Customer Premises Equipment (CPE), at data-center telco edges, and in the cloud—providing flexibility in deployments.

## Flexible CPE use cases

The solution reduces complexity and costs for SPs by consolidating CPEs and smartly using virtual services. Both the 3844 and the 3848, powered by Vyatta, can be used as physical CPEs at customer sites.

Alternately, a cloud CPE can aggregate these applications at the service provider's telco edge. A Layer 2 (L2) Network Interface Device (NID) or PON access at the customer site backhauls all traffic to the telco cloud. The L2 traffic terminates on the cloud CPE that provides all the capabilities of a physical CPE. Vyatta implements the same service chaining on the cloud CPE as it does on the physical device. This flexibility ensures the ability to respond rapidly to changing needs without compromising network infrastructure and without costly truck roll.

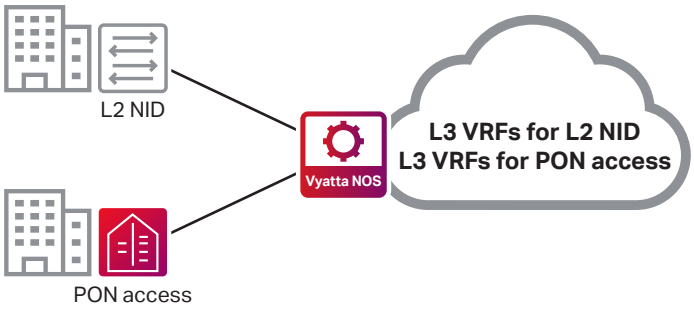


*Figure 4. Cloud CPE use case*

## Comprehensive WAN and cloud gateway capabilities

Gateways are foundational to the WAN, serving as crucial interconnection points within the network infrastructure. Vyatta NOS supports comprehensive gateway capabilities, including cloud, internet, multisite, and multiprotocol VPN. It incorporates numerous encrypted tunneling techniques, such as Generic Routing Encapsulation (GRE), IPsec concentrator, and Virtual Extensible LAN (VxLAN). Regarding cloud integration, Vyatta NOS is a NAT gateway for on-premises management experience within cloud instances. It also facilitates the extension of Ethernet VPN (EVPN) VxLAN overlays to customer premise locations.

## Monitoring and SLA enforcement

Vyatta NOS also supports path-monitoring policies within its application-aware suite. It uses path monitoring tools such as/including Bidirectional Forwarding Detection (BFD) to measure Service Level Agreement (SLA) requirements from active tunnels and paths—such as loss, delay, and jitter—to dynamically fail over to a better-performing link, load balance sessions, or even utilize all available site bandwidth to maximize throughput capacity.

Customers can tailor how an internet application fails over—either to another internet path or through a private VPN path. This ensures that all mission-critical applications perform their best to provide SLA-based resiliency and usability.

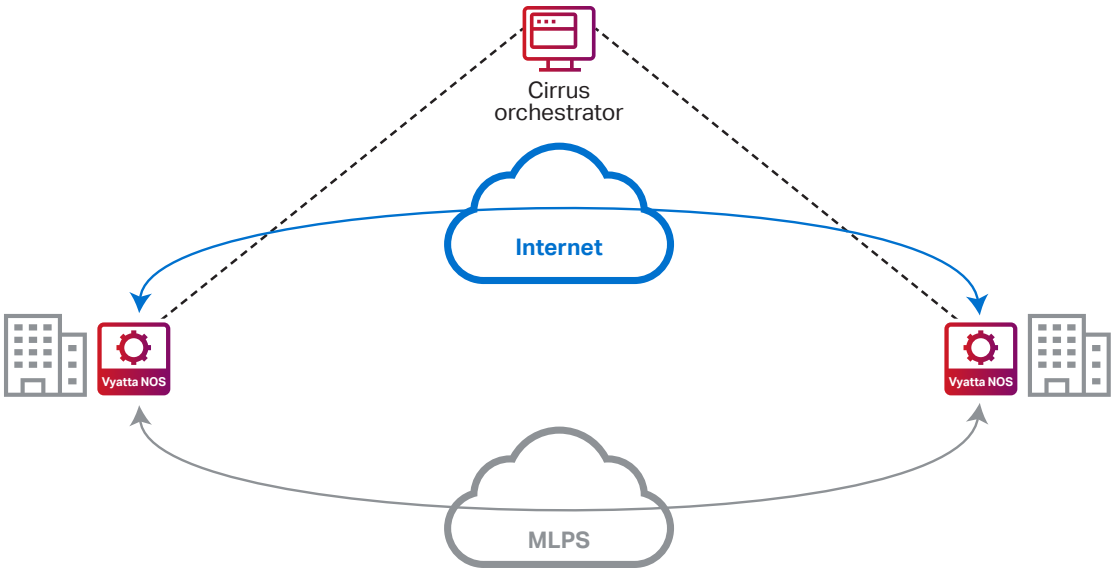


*Figure 5. Monitoring and SLA enforcement*

## Cirrus Orchestrator

Cirrus Orchestrator is designed to manage and orchestrate services for Vyatta NOS–powered devices. It offers various functions, including service template design, onboarding, Zero-Touch Provisioning (ZTP), monitoring, and analytics.

This orchestrator includes a library of standard templates that simplify onboarding and delivering new services. These templates assist SPs in describing the services they offer and configuring them in the domain language of that service. The templates translate the available options into well-defined device configurations without the operators needing to configure each device, thereby reducing the errors that can be introduced when manually converting requirements into device-specific configurations. This library of standard templates is one of the industry's most flexible and customizable in parameters.

Also, Cirrus Orchestrator is one hundred percent YANG-model driven and offers a customizable UX and zero-to-minimum GUI development for new features. Administrators can leverage built-in service workflows to create and deploy validated service designs quickly. The system also provides tooling for the service designers to develop and test the service bundles without needing a full deployment; when ready, they can upload the bundle into a Cirrus Orchestrator instance. Cirrus Orchestrator supports multiple services simultaneously, which can be added or upgraded in a live system at any time.

With ZTP, devices can be shipped to branch locations, powered up, and connected to the internet. Administrators simply need to register on a secure web portal to complete onboarding. Then, they can start managing deployment and configuration from a single pane of glass.

Cirrus Orchestrator also includes poll-based device monitoring. If an issue arises, operators can use the web interface to execute various networking options directly on the device and have full access to the diverse show and reset commands that Vyatta NOS offers.

While this orchestrator can be deployed on premises, it is mostly deployed in the cloud, where it can quickly scale up as needed. Cirrus Orchestrator has been shown to comfortably handle many thousands of end-customers or organizations through hierarchical multitenancy and role-based administrative capabilities.

**Platform examples supported by Vyatta NOS**

| | 3844 | 3848 |
|---|---|---|
| **Rack Units (RU)** | 1RU | 1RU |
| **CPU Cores** | 4 | 8 |
| **DRAM Memory (GB)** | 16 | 32 |
| **Storage (GB)** | 256 (SSD) | 512 (SSD) |
| **Ethernet Ports (GBE)** | (10) GbE RJ45, (4) 1/10GbE SFP+ | (10) GbE RJ45, (4) 1/10GbE SFP+ |
| **Virtualization (VNFs)** | 1 | 2-3 |
| **Power over Ethernet (PoE)** | Yes (4 Ports) | Yes (4 Ports) |
| **TPM 2.0** | Yes | Yes |
| **Dimensions (W x D x H)** | 430mm x 411mm x 44mm<br>16.93" x 16.18" x 1.73" | 430mm x 411mm x 44mm<br>16.93" x 16.18" x 1.73" |
| **Agency Approvals and Certifications** | CSA/UL - Canada and USA Certification<br>NOM and NICE – Mexican Certification<br>CE - EU Certification<br>VCCI - Japan Certification<br>RCM – Australia/New Zealand Certification<br>IRAM – Argentinian Certification<br>ICASA – South African Certification<br>EAC – Eurasian Certification<br>BSMI – Taiwan Certification<br>Ukrainian Certification | |
| **Emissions** | FCC Part 15 Class A | |
| **Safety** | CSA/UL | |
| **Environmental** | RoHS2 Directive | |
| **Operating Temperature** | 0°C to 40°C (32°F to 104°F) | |
| **Storage Temperature** | -40°C to 65°C (-40°F to 149°F) | |
| **Relative Humidity** | Non-condensing 5% to 90% | |
| **Supported hypervisors** | VMware ESXi<br>Red Hat KVM | |
| **Supported Public Clouds** | Microsoft Azure | |

# Vyatta NOS software features and protocols

**IPv4 routing**

Static Routing
Border Gateway Protocol Version 4 (BGPv4)
Open Shortest Path First Version 2 (OSPFv2)
Routing Information Protocol Version 2 (RIPv2)
Policy-based Routing (PBR)

**Multicast IPv4 support**

Internet Group Management Protocol Version 2 and 3 (IGMPv2 and IGMPv3)
Protocol Independent Multicast Sparse Mode (PIM SM)
PIM Source-Specific Multicast (SSM) Multicast Source Discovery Protocol (MSDP)

**IPv6 routing**

Static Routing
BGPv6
OSPFv3
RIPng
PBR

**Multicast IPv6 support**

PIMv6
MSDP
Multicast Listener Discover Versions 1 and 2 (MLDv1 and MLDv2)

**Encapsulation**

Ethernet
GRE
PPP over Ethernet (PPPoE)
802.1Q
QinQ

**Tunneling/VPN**

Virtual Extensible LAN (VXLAN)/ Virtual Tunnel End Point (VTEP)
Site to Site VPN (IPsec)
Remote VPN (L2TPv3, IPsec)
Dynamic Multipoint VPN (DMVPN) with Next Hop Resolution Protocol (NHRP)
Generic Routing Encapsulation (L2/L3 Bridging)
BGP VPN v4/v6 for Inter-AS options A, B, and C
EVPN route types 1,2,3,4, and 5
IP in IP (IPIP, IPIP6, IP6IP, and Simple Internet Transition)

**High availability**

VRRPv2 (IPv4 and IPv6)
VRRPv3 (IPv6)
VRRP Support with IPsec VPN
Bidirectional Forwarding Detection (BFD)
Link Aggregation Control Protocol (LACP)
Stateful Firewall/NAT Failover

**IP address management**

DHCPv4/v6 Server, DHCPv4/v6 Client
DHCPv4/v6 Relay
Dynamic DNS
DNS Hosting
DNS Forwarding

**NAT**

IPv4 to IPv4 (NAT44)
CG_NAT (NAT44(4))
IPv6 to IPv4 (NAT64)
Application-level Gateway (ALGs)

**Cryptographic algorithms**

Encryption: AES-256 (in CBC and GCM modes), AES-128 (in CBC and GCM modes), 3DES
Authentication: ECDSA, ECCSA, RSA
Integrity: SHA-256, SHA-384, SHA-512, SHA, MD5

**Firewall**

Stateful Inspection Firewall (v4/v6)
Zone-based Firewall (v4/v6)
Time-based Firewall (v4/v6)
Policy Rate Limiting

**Multiprotocol Label Switching (MPLS)**

Label Distribution Protocol (LDP)
Label Switch Router (LSR)
Label Edge Router (LER)
Resource Reservation Protocol (RSVP)
Ping
Traceroute

**QoS**

Hierarchical QoS
Policing
DSCP Classification
DSCP Marking
Weighted Round Robin (WRR)
Random Early Detection (RED)
Weighted Random Early Detection (WRED)
Strict Priority Queuing

**Application-aware capabilities**

Application-aware routing
Application-aware firewall
Application-aware QoS
Application-aware metrics (jitter, drop, delay)
Predefined application thresholds for common application categories

**Administration and authentication**

Integrated CLI
Web GUI
RESTful API
NETCONF/YANG
Telnet
SSHv2
RADIUS
TACACS+
X.509 digital certificate authorization

**Diagnostics, logging**

Remote Syslog
SNMPv1/v2/v3
SNMP for IPv6
Two-Way Active Measurement Protocol (TWAMP) client/server

**Port monitoring**

Switched Port Analyzer (SPAN)
Remote Switched Port Analyzer (RSPAN)
Encapsulated Remote Switched Port Analyzer (ERSPAN)

**Flow monitoring**

IPFIX export
NetFlow export