Cisco CSR 1000V: Functions, Features, Architecture, and Data Flow

Introduction

This study aims to primarily analyze the Cisco CSR 1000V and then compare it with leading virtual routing and network service platforms — Juniper vMX, Juniper vSRX, and VyOS — with a focus on their core functions, unique features, system architecture, data flow, protocols, and performance characteristics. The goal is to identify how each product supports enterprise, carrier, and cloud environments, particularly in hybrid-cloud, multi-tenant, and virtualized deployments, and to provide guidance for selecting the most suitable virtual router based on operational requirements.

The comparison follows a data-flow-centric and feature-based approach, examining:

- Must-have functions: dynamic routing, VPN, firewall, NAT, overlay networks
- Unique differentiators and specialized capabilities
- System architecture and internal data flow (control plane vs data plane)
- Protocols, signaling, and algorithm implementations
- Performance, resource requirements, and scalability
- Pros, cons, and operational considerations

Information is derived from vendor documentation, product whitepapers, and observed functionality, with an emphasis on practical deployment scenarios and operational insights rather than purely theoretical specifications.

The analysis shows that CSR 1000V provides full enterprise-grade routing functionality in virtual environments, with operational consistency across physical and virtual deployments. By comparison, vMX offers carrier-grade routing and NFV integration; vSRX emphasizes virtualized security and firewall throughput; and VyOS provides lightweight, open-source flexibility. Differences reflect each product's target audience, design principles, and deployment objectives, from enterprise hybrid-cloud to carrier/NFV and cloud-native security.

In conclusion, selecting a virtual router depends on deployment objectives, scale, and required features. CSR 1000V is ideal for enterprise hybrid-cloud integration and multi-service support. vMX excels in high-throughput carrier or NFV deployments. vSRX is suited for cloud-native security and multi-tenant firewalling. VyOS fits small- to medium-scale, cost-sensitive, or flexible open-source environments. Organizing features, architecture, and data flow in a structured comparison provides a data-driven framework for decision-making in virtual network design.

Overview

The Cisco CSR 1000V is a fully virtualized enterprise-class router that delivers Cisco IOS XE routing, VPN, security, and network services within cloud and virtualized environments. Instead of relying on dedicated router hardware, the CSR 1000V runs as a virtual machine on x86 servers or cloud platforms such as AWS, Azure, and Google Cloud. Because it uses the same software architecture and routing stack as physical Cisco routers (such as ISR and ASR platforms), it brings mature and feature-rich networking capabilities into cloud environments where hardware deployment is not possible. Its primary function is to extend WAN, VPN, MPLS, routing, and security connectivity into virtualized environments, enabling seamless hybrid cloud architectures, secure connectivity between on-premises networks and cloud workloads, and multi-tenant or service-provider environments that require flexible, scalable virtual routing capabilities.

At its core, the CSR 1000V behaves like any enterprise-grade router: it performs dynamic routing using protocols such as BGP, OSPF, EIGRP, and ISIS; it maintains routing tables, performs route selection, and exchanges prefixes with on-premises routers or cloud routing constructs. Beyond basic routing, it supports advanced technologies including VRF and MPLS, enabling segmentation and multi-tenant separation across virtual infrastructure. The router serves as a VPN gateway, supporting IPsec, DMVPN, FlexVPN, and SSL VPN to securely connect remote sites or data centers to cloud environments. It also integrates firewall capabilities through Cisco's Zone-Based Firewall model and provides NAT, DHCP, DNS, and other network services commonly needed when hosting or interconnecting workloads inside cloud networks. Additionally, the CSR 1000V can participate in hybrid environments by extending Layer-2 and Layer-3 connectivity using encapsulation technologies such as VXLAN, GRE, OTV, VPLS, and EoMPLS, making it possible to stretch networks across on-premises and cloud boundaries for use cases such as migration, failover, or multi-site application architectures.

One of the most significant advantages of the CSR 1000V is that it brings the full feature set of Cisco's physical router platforms into virtualized deployment models. Unlike basic cloud-native VPN gateways offered by public cloud providers, the CSR 1000V supports advanced routing, multi-protocol VPN, MPLS, multitenancy via VRFs, deep QoS functionality, and application visibility features such as Cisco AVC. Because it runs the same IOS XE operating system as Cisco's enterprise hardware, organizations benefit from operational consistency: the same CLI, APIs, SNMP, NetFlow, logging, and automation workflows apply across both physical and virtual routers. Another major differentiator is its support for network function virtualization (NFV); the CSR 1000V can operate as a virtual Route Reflector, virtual Broadband Network Gateway, or virtual Intelligent Services Gateway. This consolidation of traditional hardware-bound network roles into virtual machines makes it flexible and cost-efficient for

service providers or large enterprises. The router also supports VXLAN overlays and large-scale network segmentation that go far beyond the limitations of traditional VLAN models, enabling service providers to host many isolated tenant environments on shared infrastructure. Its virtual form also provides elasticity: administrators can scale compute, memory, or licensing throughput tiers depending on performance needs.

The CSR 1000V runs on a hypervisor or cloud compute instance, forming a virtualized network appliance composed of several logical components. At the base of the architecture is the virtualization layer, consisting of the host hardware, hypervisor (VMware ESXi, KVM, Hyper-V, or cloud-native hypervisors), and virtual NICs that map the CSR's interfaces to virtual networks or physical uplinks. Above this sits the Cisco IOS XE operating system, which houses two primary functional engines: the Virtual Route Processor (vRP) and the Virtual Forwarding Processor (vFP). The vRP is responsible for all control-plane operations such as running routing protocols, maintaining adjacency relationships, computing routing tables, and managing VRFs and MPLS label distribution. The vFP handles data-plane operations, including forwarding packets, enforcing QoS, performing NAT, switching and bridging, encapsulating or decapsulating tunneling protocols, and supporting overlay and Layer-2 extension technologies. A rich suite of integrated network-service modules runs alongside these engines, providing VPN termination, firewall enforcement, NAT services, DHCP and DNS capabilities, application monitoring, and overlay network functions. All these components interact through the IOS XE software architecture, giving the CSR 1000V predictable performance and feature parity with Cisco's hardware routers.

CSR 1000V offers an extensive set of network services designed to replicate and enhance traditional router and security appliance capabilities in virtual environments. Its security feature set includes IPsec VPN capabilities for site-to-site tunnels, remote-access VPN options, and dynamic multi-site VPN technologies like DMVPN and FlexVPN that support scalable and resilient hub-and-spoke or full-mesh topologies. Integrated security functions include the Cisco Zone-Based Firewall for stateful traffic filtering, standard ACLs, and AAA integration for identity-based access control. Beyond security, the router supports full NAT functionality, enabling translation of cloud workloads or tenant networks, and offers DHCP and DNS services suitable for cloud-hosted subnet environments. For multi-site or multi-cloud architectures, the router supports Layer-2 and Layer-3 extension technologies such as VXLAN, VPLS, OTV, and EoMPLS, which allow the stretching of VLANs or VRFs across geographically distributed environments. In carrier or service-provider contexts, the CSR 1000V can function as an MPLS CE or PE router, support VRF-based segmentation for tenants or departments, and act as a virtual Route Reflector. Additional NFV capabilities allow it to fulfill roles such as virtual Broadband Network Gateway or virtual Intelligent Services Gateway, reducing the need for specialized physical equipment.

Management of the CSR 1000V is consistent with Cisco's broader networking portfolio since it uses the same IOS XE operating system found in physical routers. Administrators can

manage it through traditional CLI via SSH, programmatic interfaces such as NETCONF, RESTCONF, and REST APIs, and monitoring protocols including SNMP, Syslog, NetFlow, and telemetry streaming. Its integration with cloud environments is flexible, as the router is available in public cloud marketplaces and supports standard hypervisor environments for private clouds. In SD-WAN mode, the CSR 1000V participates in Cisco's SD-WAN fabric, enabling centralized orchestration, policy management, and dynamic application-aware routing across WAN links. This means traffic can be intelligently steered across multiple tunnels or network paths based on real-time network health, application requirements, or business-defined intent. Because its management ecosystem mirrors that of Cisco ISR and ASR routers, organizations benefit from configuration consistency, operational familiarity, and reduced training overhead.

CSR 1000V is delivered with tiered licensing that governs throughput, feature sets, and advanced capabilities. Licenses such as IP Base, Security, AppX, and AX determine which features are enabled, ranging from basic routing to full VPN, firewall, application awareness, and MPLS capabilities. Performance varies depending on the number of allocated vCPUs, memory, and the underlying hypervisor platform. As a software-based forwarder, its throughput is inherently tied to virtual CPU speed and virtualization overhead, meaning that while it delivers impressive performance for a VM, it cannot match the raw forwarding power of high-end dedicated hardware routers. Nevertheless, it offers flexibility by letting administrators scale the VM size or license tier as bandwidth or service requirements grow. VM requirements generally include multiple vCPUs, moderate memory allocations, and several virtual NICs, making it feasible to deploy on a wide range of server infrastructures or cloud instance types.

In a hybrid cloud deployment, the CSR 1000V often acts as a secure VPN and routing gateway between on-premises networks and cloud VPCs or VNets. It terminates VPN tunnels, exchanges routes with data-center routers, and performs NAT, firewall, and traffic steering for cloud workloads. In a cloud service provider environment, the CSR 1000V often serves as a multi-tenant virtual router, hosting dozens or hundreds of VRFs that separate customer networks from one another while providing each tenant with routing, VPN, and firewall services. Advanced overlay technologies such as VXLAN make it possible to scale these multi-tenant environments without exhausting VLAN space. In MPLS extension scenarios, a service provider deploys CSR 1000V instances within customer cloud environments as CE or PE routers, extending MPLS VPNs seamlessly into virtualized workloads. In all these cases, the CSR 1000V integrates routing, security, overlays, and network services under a single virtualized software platform.

End-to-End Data Flow Inside the Router

The following walkthrough assumes an incoming packet arriving from a cloud VPC/VNet, a hypervisor network, or a physical connection mapped through virtual NICs. In a real environment, multiple variations exist, but the following flow represents what is understood to be the universal internal data path.

1 - The data flow begins when a packet enters the CSR 1000V through one of its virtual NICs. These vNICs are presented to the VM by the hypervisor or cloud platform. At this point the packet is still part of the virtualized host's switching fabric, and no router-level processing has occurred. The hypervisor forwards the packet into the CSR's vNIC, delivering it to the IOS XE data plane.

2 - After entering the CSR 1000V, the packet is passed directly into the Virtual Forwarding Processor (vFP). The vFP is the router's data plane, responsible for all real-time packet forwarding.

As soon as the packet hits the vFP, several immediate actions occur:

- The vFP determines which router interface the packet belongs to. This involves mapping the vNIC to an IOS XE interface such as *GigabitEthernet1*, *Tunnel1*, or a subinterface with a VLAN tag.

- The ingress interface is mapped to a VRF, which determines the routing instance, table, and segmentation rules that apply to the packet.

- The vFP examines Layer-2 headers, removes VLAN tags if present, and identifies the encapsulation type.

3 - Before routing occurs, the packet is inspected against several policies. ACLs assigned to the interface are checked. If the ingress interface belongs to a security zone, the packet is evaluated against stateful firewall rules. This determines whether the packet is allowed to proceed. If the packet is destined for the router itself, CoPP (Control-Plane Policing) verifies whether it should be rate-limited or dropped.

4 - If the packet is allowed, the vFP performs a routing lookup. The vFP queries the FIB (Forward Information Base), which contains optimized forwarding entries built from the routing table (RIB). The FIB determines the next-hop IP, egress interface, and required encapsulations. If there is no matching FIB entry, the vFP contacts the Virtual Route Processor (vRP), which runs routing protocols, updates the RIB, and then pushes changes back into the FIB. Once the FIB is updated, the packet is processed again.

5 - Before the packet is sent out, several optional services may modify or further classify it.

- If NAT is configured, the vFP performs either source NAT, destination NAT, or PAT (Port Address Translation).

- The packet is then classified into a QoS policy: CoS/DSCP marking, rate-limiting or policing, and queuing decisions.

- If AVC (Application Visibility & Control) is enabled, the packet may be inspected for application identification before forwarding occurs.

- If the egress interface is a VPN tunnel, the packet is encrypted, new headers are added, and encapsulation transforms the packet into a secure payload.

- In MPLS deployments, the data plane applies label imposition (adding), label swapping (replacing), or label disposition (removing).

6 - Before exiting the router, the packet passes through outbound policy checks. If the packet crosses between zones, firewall rules are enforced again. Any egress ACL associated with the interface is applied. CSR verifies that forwarding complies with the VRF routing instance.

7 - Once the packet completes all processing steps, the vFP prepares it for transmission. CSR rebuilds the Layer-2 frame. For cloud platforms, this maps to the virtual NIC configuration. The vFP then delivers the packet to the egress vNIC. The hypervisor takes the packet from the vNIC and forwards it into either a VPC/VNet, a virtual switch or bridge, a physical NIC on a server, or another VM depending on the deployment. Thus completes the data flow path.

Features & Functions

A major differentiator of the CSR 1000V compared to other virtual or cloud-native routing solutions is the completeness of its feature set. Because the CSR runs the same IOS XE software as Cisco's physical ISR and ASR routers, it provides capabilities that are rare in virtual appliances. These include full MPLS L3VPN support with PE/CE roles, VRF-aware NAT and firewalling, scalable DMVPN and FlexVPN topologies, BGP route reflection, and service-provider-grade features such as advanced QoS, NBAR/AVC application visibility, and NFV roles like vBNG and vISG. Its ability to operate either in traditional IOS XE router mode or in SD-WAN mode adds further versatility, enabling it to serve both as a conventional enterprise router or as part of a controller-driven WAN fabric. The breadth and depth of functionality make the CSR 1000V stand out as one of the most capable and flexible virtual routers available.

Internally, the CSR 1000V processes packets using a virtualized architecture modeled after Cisco hardware platforms. Packets enter through a virtual NIC and are handed to the Virtual Forwarding Processor (vFP), which performs all data-plane operations such as packet forwarding, ACL checks, NAT translation, QoS classification, firewall enforcement, and tunnel encapsulation or decapsulation. The Virtual Route Processor (vRP) operates independently as the control plane, running routing protocols, maintaining adjacencies, computing routing tables, assigning MPLS labels, and updating the forwarding table that the vFP relies on. This separation mirrors the architecture of high-end Cisco routers, providing deterministic behavior, predictable performance, and the ability to support both fast-path forwarding and complex service-chain processing entirely within software.

High availability in virtual and cloud environments is another important aspect of the CSR 1000V's design. Although it does not support stateful redundancy like some hardware routers, it integrates seamlessly with hypervisor and cloud-based redundancy models. CSR pairs can use HSRP, VRRP, or GLBP for first-hop redundancy, and cloud-native load balancers or floating IPs can be placed in front of CSR instances to provide multi-AZ or multi-region failover. IPsec and DMVPN configurations can be built with redundant hub pairs, allowing tunnels to reestablish dynamically if a VM or cloud instance fails. Likewise, BGP-based failover or ECMP routing ensures continuity when one CSR becomes unavailable. These models provide highly resilient designs, ensuring that the CSR 1000V can function as a reliable WAN edge, VPN headend, or cloud gateway in any virtual deployment.

Performance and throughput on the CSR 1000V depend largely on the virtual CPU resources allocated to the VM and the licensing tier purchased. Because forwarding is software-based, higher vCPU counts and SR-IOV NIC acceleration significantly improve packet processing rates. Cisco licenses throughput in tiers (e.g., 10 Mbps, 50 Mbps, 100 Mbps, 1 Gbps+, and multi-Gbps levels), which allows organizations to scale performance according to cost and workload demands. However, like all virtualized routers, CSR performance is bound by

the host system's capabilities—especially for cryptographic operations such as IPsec, where CPU-bound encryption limits throughput. Despite these limits, the CSR delivers competitive performance for a VM-based router and offers the advantage of elasticity: administrators can increase VM size or upgrade licenses as network requirements grow.

Relative to cloud-native routing services—such as AWS Transit Gateway, Azure VPN Gateway, or GCP Cloud Router—the CSR 1000V provides significantly more advanced networking and security capabilities. Cloud-native gateways typically support only static or BGP routing, limited VPN topologies, and constrained NAT or segmentation options. In contrast, the CSR 1000V offers full dynamic routing across multiple protocols, rich firewalling, deep QoS, multi-VRF separation, MPLS, DMVPN, FlexVPN, and advanced overlay tunneling. This makes it ideal for complex enterprise or service-provider environments where precise routing control, multi-tenant segmentation, hybrid architectures, or WAN optimization policies are required. While cloud-native solutions provide simplicity and managed operation, the CSR provides depth, configurability, and the operational fidelity needed to replicate sophisticated on-premises network designs in the cloud.

In SD-WAN mode, the CSR 1000V becomes part of Cisco's SD-WAN fabric, enabling centralized management, encrypted fabric overlays, and application-aware routing through the vManage, vSmart, and vBond controllers. This allows organizations to use the same CSR instance either as a traditional router or as a full SD-WAN edge node, depending on deployment needs. For overlays, the CSR supports a comprehensive suite of tunneling and encapsulation technologies—VXLAN, GRE, IPsec + GRE, OTV, VPLS, and EoMPLS—allowing it to extend broadcast domains, VRFs, or routed boundaries across regions, clouds, or data centers. These overlays enable workload mobility, multi-site clustering, hybrid data center expansion, and large-scale tenant separation. In MPLS deployments, the CSR can function as a PE or CE router, support label-switching data paths, or act as a virtual Route Reflector, enabling service providers to extend MPLS VPNs directly into virtualized cloud environments. Together, these capabilities showcase the CSR 1000V's flexibility and its ability to operate in enterprise, carrier, and multi-cloud networking architectures.

Comparative Analysis of Virtual Routing and Network Service Platforms

	CSR 1000V	vMX	vSRX	VyOS
Product Type	Enterprise-grade virtual router	Carrier-grade virtual router	Virtual firewall with routing	Open-source virtual router/firewall
Pros	Full enterprise feature set; operational consistency; hybrid-cloud & NFV-ready; SD-WAN support	High scale; carrier-grade routing; NFV integration; automation-ready	Strong security; multi-tenant overlay; cloud-native security	Free/open-source; highly customizable; lightweight; supports many tunneling protocols
Cons	Costly licensing; higher VM resource requirements; throughput lower than dedicated hardware	Complex; resource-heavy; primarily routing-focused	Less general-purpose routing features; focused on security	Limited enterprise/MPLS features; smaller community support; lower throughput

A general overview of four selected routers

	CSR 1000V	vMX	vSRX	VyOS
Routing Protocols	BGP, OSPF, EIGRP, IS-IS	BGP, OSPF, IS-IS	BGP, OSPF	BGP, OSPF, RIP, policy-based routing
VPN/Tunneling	IPsec, DMVPN, FlexVPN, SSL VPN; GRE, VXLAN, VPLS, OTV, EoMPLS	IPsec, MPLS VPN, GRE	IPsec/IKE, EVPN-VXLAN overlays	IPsec, GRE, OpenVPN, WireGuard, VXLAN
Overlay	VXLAN, VPLS, OTV, EoMPLS; VRF support	MPLS, VRF	EVPN-VXLAN overlays	VXLAN; VRF limited; multi-tenant via logical routing
Security/Firewall	Cisco Zone-Based Firewall, ACLs, AAA	Basic ACLs; relies on separate security appliances	NGFW, firewall policies, stateful inspection	Standard firewall and NAT; Linux iptables-based

A general assessment of each router's core features

	CSR 1000V	vMX	vSRX	VyOS
Architecture	vRP (control plane) + vFP (data plane) on VM; IOS XE; integrated network services	Control/data separation internally; Linux-based VM	VM with optimized firewall/data plane; integrated control plane	Monolithic Linux VM; control + forwarding in same OS; modular software services
Data Flow	Packet to vFP to NAT/firewall to overlay to forwarding to egress NIC; control plane in vRP	Packet to forwarding engine to MPLS/VPN to egress; control plane handles routing protocols	Packet to firewall/inspection to VPN termination to routing to egress; overlays handled	Packet to firewall/NAT to routing/overlay to forwarding; control plane updates routing tables dynamically

Architecture & Data Flow

	CSR 1000V	vMX	vSRX	VyOS
Resource Requirements	2–16 vCPUs, 4–32 GB RAM; multiple virtual NICs	2–16+ vCPUs, 8–64 GB RAM	2–16 vCPUs, 4–32 GB RAM	1–4 vCPUs, 1–8 GB RAM
Performance	Software forwarding limits throughput; overlay/NAT/VPN CPU-intensive	High throughput; scalable for large routing tables	Optimized for firewall throughput; inspection may limit routing	Lightweight; performance limited by VM resources
Computation	CPU-bound for VPN/firewall/overlay; scales with VM size	CPU-bound; high-throughput design	CPU-bound for inspection; optimized for security	Lightweight; minimal CPU/energy footprint

Performance & Resource Considerations

When evaluating virtual routing and network service appliances, several products stand out within the enterprise and service-provider ecosystem. Cisco CSR 1000V, Juniper vMX, Juniper vSRX, and VyOS represent four distinct approaches to virtualized networking, each meeting the baseline requirements expected of a modern virtual router while offering unique capabilities that align with their intended market segments. All four products provide essential must-have functionality: dynamic routing protocols such as BGP and OSPF, IPv4/IPv6 forwarding, VPN and tunneling capabilities, NAT and firewall support, and the ability to operate on standard hypervisors or cloud platforms. These foundational features allow each platform to serve as a viable virtualized equivalent of traditional hardware routers, enabling consistent network behavior in hybrid-cloud or fully virtualized environments.

Despite this shared baseline, each solution diverges significantly in focus and specialization. Cisco CSR 1000V distinguishes itself by delivering nearly full feature parity with Cisco's physical ISR and ASR routers through the IOS XE software stack. This makes it uniquely suited for enterprises seeking consistent operational behavior between on-premises hardware and cloud-hosted routing services. Its strengths include comprehensive multi-VRF segmentation, MPLS PE/CE capabilities, advanced VPN technologies such as DMVPN and FlexVPN, integrated firewall and NAT services, and extensive overlay support including VXLAN, VPLS, GRE, and OTV. CSR 1000V also supports SD-WAN mode, allowing it to operate either as a traditional router or as part of a controller-driven WAN fabric. In hybrid-cloud and multi-tenant designs, its ability to combine routing, security, overlays, and network services within a single virtual appliance is a major differentiator.

Juniper's vMX targets a different niche, offering a virtualized version of the MX Series universal routing platform commonly deployed in service provider networks. While it supports the same core routing features as CSR 1000V, its uniqueness lies in its carrier-grade scalability, automation readiness, and suitability for NFV deployments that require high-throughput, large routing tables, and heavy MPLS operations. It excels in large-scale ISP or cloud-provider topologies rather than multipurpose enterprise environments. In comparison, Juniper vSRX is designed primarily as a virtual firewall with integrated routing, VPN, and security services. Its strengths include high-performance packet inspection, advanced security policies, NGFW capabilities, and support for EVPN-VXLAN overlays that combine security with multi-tenant network segmentation. Rather than functioning as a general-purpose router, vSRX is optimized for securing cloud workloads and enforcing policy in virtualized data centers or distributed cloud environments.

VyOS represents a different design philosophy: a fully open-source virtual router and firewall platform that provides a rich set of routing, VPN, NAT, and firewall features without licensing costs. It supports a wide array of tunneling and overlay mechanisms—including IPsec,

GRE, VXLAN, OpenVPN, and WireGuard—and offers flexible customization through its Linux-based architecture. Although it lacks some of the advanced MPLS, multi-VRF, and service-provider grade capabilities found in CSR 1000V and vMX, VyOS offers excellent value for environments where cost control, open-source tooling, and adaptability are priorities. It is widely used in labs, automation-driven environments, smaller enterprises, and cloud deployments that require basic routing and security without heavy feature complexity.

Overall, the comparison illustrates that while all four solutions meet core routing and virtualization requirements, their unique features reflect divergent product philosophies. Cisco CSR 1000V emphasizes enterprise consistency, rich multi-service functionality, and hybrid-cloud versatility. Juniper vMX targets high-scale, service-provider routing needs, whereas vSRX focuses on virtualized security and NGFW capabilities within cloud-native architectures. VyOS provides a flexible, cost-efficient open-source alternative for organizations that prioritize customization and accessibility over deep enterprise or carrier-grade networking features. Together, these distinctions help clarify which product aligns best with different architectural, operational, and organizational priorities.

References

[1] Cisco Systems, Inc. Cisco CSR 1000v and Cisco ISRv Software Configuration Guide. “Cisco CSR 1000v Series Cloud Services Router Overview,” last modified April 15, 2020. Available: https://www.cisco.com/c/en/us/td/docs/routers/csr1000/software/configuration/b_CSR1000v_Configuration_Guide/b_CSR1000v_Configuration_Guide_chapter_00.html

[2] Cisco Systems, Inc., Cisco CSR 1000v Series Cloud Services Routers — “Release Notes for Cisco CSR 1000v Series, Cisco IOS XE 3S”, last accessed November 29, 2025, Available: https://www.cisco.com/c/en/us/td/docs/routers/csr1000/release/notes/csr1000v_3Srn.html

[3] Cisco Systems, Inc., Release Notes for Cisco CSR 1000V Series, Cisco IOS XE Amsterdam 17.2.x, first published April 15, 2020. Available: https://www.cisco.com/c/en/us/td/docs/routers/csr1000/release/notes/xe-17/csr1000v_rn-17-2.pdf

[4] Juniper Networks, “Juniper vSRX Virtual Firewall,” HPE Store product page. Available: https://buy.hpe.com/us/en/networking/network-security/firewalls/juniper-firewall-products/juniper-vsrx-virtual-firewall/p/1014920022

[5] Juniper Networks, vMX Virtual Router Datasheet, “vMX Virtual Router,” accessed November 22, 2025. Available: https://www.juniper.net/us/en/products/routers/mx-series/vmx-virtual-router-datasheet.html