Streamlining Security Deployments with Juniper Validated Designs

Deploy more quickly and confidently, improve outcomes, and save valuable time

Discover how Juniper Validated Designs (JVDs) for security can help you design and deploy an optimal networking solution

Explore security JVDs →

The challenge

Navigating the complex landscape of security deployments

As networks become increasingly complex and distributed, IT professionals face evolving security challenges that span multiple domains. Network and security teams must protect information, infrastructure, and services from both legacy and emerging threats amid mounting pressures. They are tasked with deploying effective security solutions by maintaining consistent postures across all segments, adapting to changing threat landscapes, managing increased traffic without compromising performance, ensuring regulatory compliance, and implementing Zero Trust models—all while avoiding operational disruption.

The capabilities you need

Operationalize security across the entire network

Security operators taking on architectural transformations must do so without compromising the user experience or increasing the risk of unauthorized access to applications and data. Security JVDs help you operationalize security, adopt Zero Trust architectures, and protect the business everywhere—from the edge to the data center and back.

JVDs are comprehensive, end-to-end blueprints for deploying Juniper solutions in your network

Scalability

Validated designs are built out based on customer input and requirements and are tailored to meet specific common use cases at maximum scale.

Reliability

Because JVDs are prescriptive designs used by multiple customers across various industries, all JVD customers benefit from lessons learned through lab testing and real-world deployments.

Velocity

JVDs have clearly defined performance profiles to help you make informed decisions about your network, resulting in up to 9x faster deployments.

Predictability

JVDs undergo a rigorous testing framework to achieve validation with ongoing, automated verification in each new release.

JUNIPER NETWORKS

www.juniper.net

The answer

JVDs for security

JVDs for security offer a transformative approach to network security design, deployment, and operation by addressing the challenges you face while delivering substantial business value and lower risk.

Current JVDs for security:

Juniper Scale-Out Stateful Firewall and CGNAT for SP Edge

Top-tier routing and security on Multiservice Edge and Broadband Edge deployments

Juniper Scale-Out Stateful Firewall and Source NAT for Enterprise

Boost MX platforms with scalable architecture and service flexibility

Data Center Next-Generation Firewall Use Case

Comprehensive next-generation firewall solution for data centers

WAN Edge for SRX Series Firewall

Optimize WAN edge with SRX devices and Juniper Mist WAN Assurance

Scale-Out IPsec Solution for Enterprises

Get high-speed, high-rate security using MX Series routers

Scale-Out IPsec Solution for Mobile Service Providers

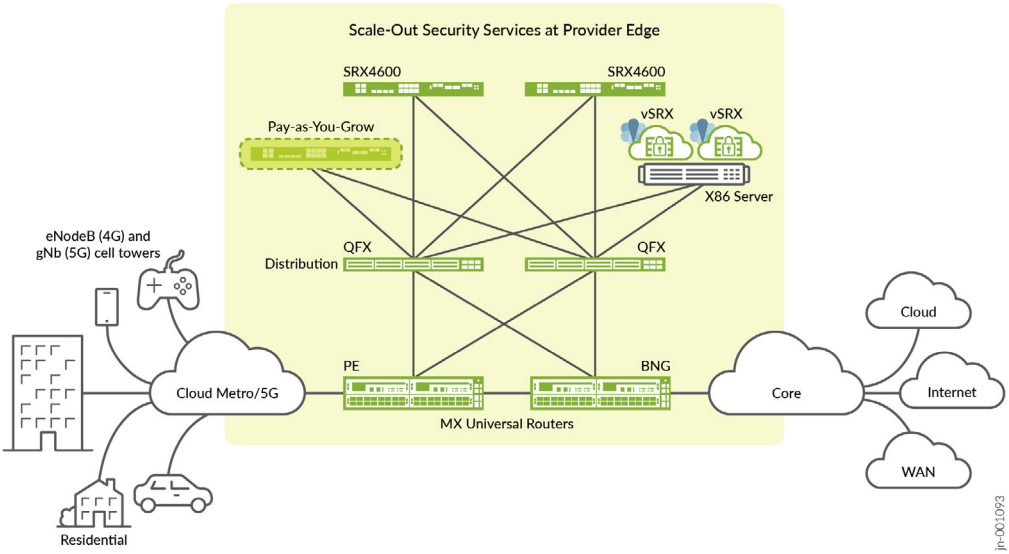
Handle unpredictable traffic growth, ensure seamless service delivery with robust security

How it works

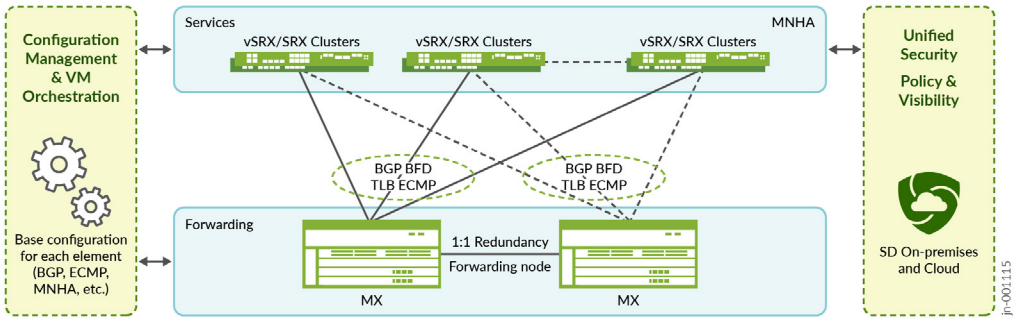
The transformative power of security JVDs

JVDs offer a robust solution to the challenges of network security design and deployment, providing a clear pathway to enhanced operational efficiency, strategic alignment, and more secure platforms.

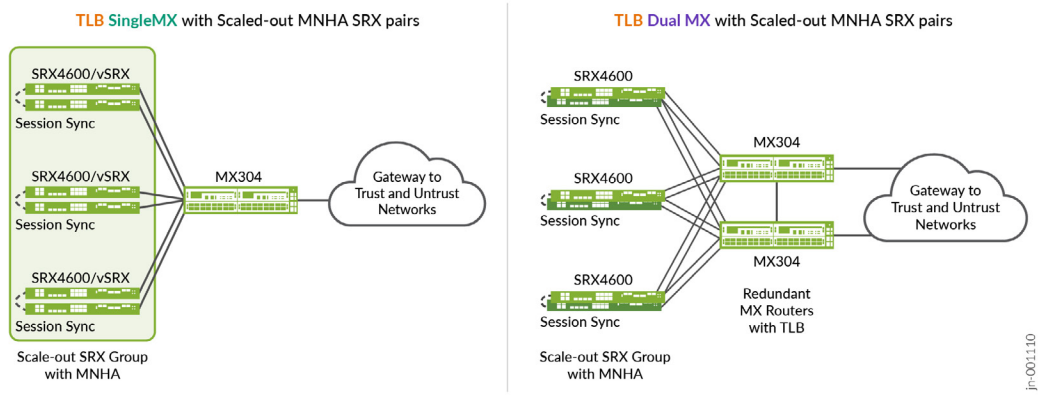
Juniper scale-out general architecture:



Juniper scale-out general architecture:



TLB – Dual MX with scaled-out MNHA SRX pairs:



Technologies and solutions used and tested:

ATP (Advanced Threat Prevention)	IDP (Intrusion Detection and Prevention)
CGNAT (Carrier-grade NAT)	CHASH (Consistent HASH)
MSE (Multi-Services Edge)	BFD (Bidirectional Fault Detection)
BBE (Broadband Edge)	ECMP
SFW (Stateful Firewall)	eBGP
MNHA (Multi-Node High Availability)	SD-WAN
SNAT (Source NAT)	Juniper QFX / MX / SRX / vSRX
AppID (Application Identification)	And many more…

Core capabilities

Next-generation firewalls (NGFWs) in data centers

Optimized performance: JVDs ensure that next-generation firewall deployments are optimized for high-throughput environments, maintaining security without compromising data center performance.

Scalable security fabric: The distributed security services architecture allows for horizontal and elastic scaling, enabling businesses to adapt their security posture as data center needs evolve.

Simplified management: JVDs provide templates for rapid-scale deployments, reducing the complexity of managing security across distributed data center environments.

WAN edge security

AI-driven insights: Juniper Mist WAN Assurance, integrated with JVDs, offers AI-powered visibility into WAN performance and security, enabling proactive issue resolution.

Seamless SD-WAN integration: JVDs for WAN edge incorporate security into SD-WAN deployments, ensuring protected connectivity without sacrificing agility.

Zero touch provisioning: JVDs enable rapid deployment of secure WAN edge devices, reducing time-to-value for new branch locations.

JVDs minimize operational costs while **reducing your IT burden and accelerating time to value**

Data center security

Comprehensive threat prevention: JVDs for data centers include advanced threat prevention measures, protecting critical assets from sophisticated attacks.

Microsegmentation: The validated designs enable fine-grained segmentation within data centers, limiting the potential impact of breaches.

Automated security operations: Integration with Juniper Apstra allows for automated security policy enforcement across the data center fabric.

Carrier-grade NAT (CGNAT)

Optimized address utilization: JVDs for CGNAT provide best practices for maximizing IPv4 address utilization while maintaining security and compliance.

Reduced P2P traffic issues: By incorporating Endpoint Independent Mapping (EIM-NAT), JVDs help mitigate common CGNAT-related issues with peer-to-peer applications.

IPv6 transition support: JVDs offer guidance on integrating CGNAT with IPv6 transition technologies, like MAP-T, for future-proofing network investments.

Our advantage

JVDs: faster, smarter, more secure

The JVD program develops solutions that reduce complexity for networking teams, helping them:

- **Qualify solutions faster** with tested architectures for building networks with well-documented capabilities and product/software release guidance
- **Reduce risk** with products, features, and topologies based on best practices and common use cases
- **Achieve predictable, repeatable results** with designs that have been validated at scale to ensure you will have faster, more reliable deployments

Why Juniper

The NOW Way to Network

Juniper Networks believes that connectivity is not the same as experiencing a great connection. Juniper's AI-Native Networking Platform is built from the ground up to leverage AI to deliver exceptional, highly secure, and sustainable user experiences from the edge to the data center and cloud. Additional information can be found at Juniper Networks (www.juniper.net) or connect with Juniper on X (Twitter), LinkedIn, and Facebook.

More information

Learn more about JVDs for security

To explore current JVDs for security, visit https://www.juniper.net/documentation/validated-designs/us/en/security

Take the next step

Connect with us
Learn how we can build what's next.
Contact us →

Explore solutions
Discover more about JVDs.
Explore solutions →

Read case studies
See how we help unlock growth.
Customer success →

More insights
Design and deploy optimal solutions.
Discover more →

Juniper Networks

www.juniper.net