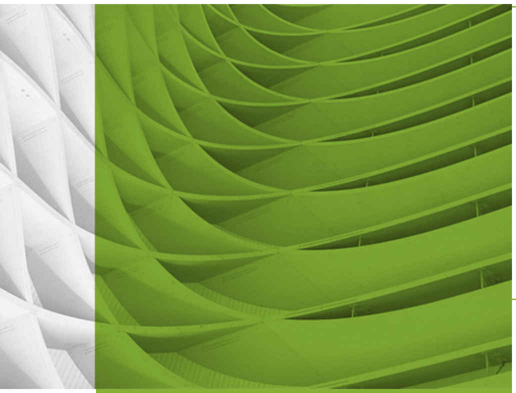

JUNIPER ZERO TRUST DATA CENTER SOLUTION BRIEF

Operationalize Security Services Across Centers Of Data At Your Own Pace With Juniper's Connected Security Distributed Services Architecture

Traditional data centers are moving from a few centralized data centers to multiple distributed centers of data across a region or around the world. As a result, the organization's data resides in more places, making it harder to secure.

Regardless of where the data resides, maintaining its security is paramount. By introducing a new extensible architecture and extending the same zero trust single policy framework to centers of data, Juniper evolves "firewall" to "firewalling" for the network, bringing security to every point of connection and empowering organizations to operationalize the architecture transition and implement zero trust at their own pace.

The Challenge

Without full visibility and unified policy management, achieving operational simplicity and maintaining security in distributed data centers is a difficult balancing act. Internal and external security threats continue to increase and sophisticated malware add to the pressure enterprises and service providers face almost daily.

Firewalls, which have largely been perimeter technology, must evolve to "firewalling" as a security fabric that's woven throughout the network to secure every point of connection. For modern networks, firewalls need to become an extensible enforcement node that intelligently and dynamically grows with the scale and performance needs of the network.

Juniper's Connected Security Distributed Services Architecture

Juniper's Connected Security Distributed Services Architecture, a new extensible architecture, uniquely integrates security services with Juniper routing infrastructure. The architecture balances millions of security service flows across multiple hardware or software security instances, removing the boundary of a fixed chassis with a limited number of slots. This unique, extensible approach gives you the ability to mix and match service plane devices (physical, virtual, or container form factor) with the existing forwarding and distribution architecture. By decoupling the forwarding layer and services layer, you can:

Challenge

Traditional data centers are transitioning to distributed centers of data. With this architectural shift, achieving operational simplicity and maintaining security are often at odds. When an organization's data is more distributed, it's harder to secure.

Solution

Juniper's experience-first approach and modern architecture secures and operationalizes the data center by extending security services across centers of data and empowering enterprises and service providers to implement zero trust at their own pace.

Benefits

Security through a unified policy management that follows users, devices, and applications across any network in a hybrid, multicloud environment Unlimited scalability and flexibility High-performance forwarding capacity and scalable services Industry's highest-performance, cloud-security solution

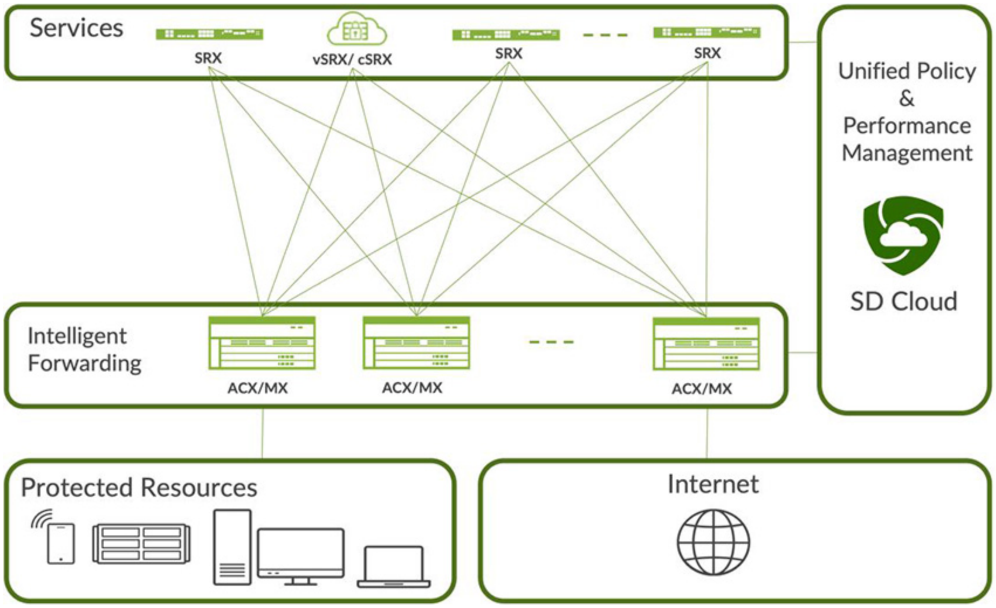

Figure 1: Overview of Juniper's Connected Security Distributed Services Architecture

- **Scale forwarding and distribution performance and services scale independently**—This approach allows service card capabilities to be available outside of the forwarding chassis (Figure 1) via a distribution layer. It also offers the capability to connect multiple forwarding devices directly or indirectly to the same remote services cards. Organizations gain tremendous agility and flexibility to independently scale the forwarding performance, and security services scale no matter how complicated and distributed the infrastructure. With a Connected Security Distributed Services Architecture, security services scaling and performance are no longer limited, and organizations can scale security services to cover all centers of data.
- **Eliminate single point of failure**—With a new form of redundancy of the forwarding path and remote service layer, organizations can use multiple forwarding devices to send traffic multiple remote service instances. This eliminates a single point of failure. Service is also consistent because all service devices are interconnected, and if one fails, the others will automatically balance the workloads.
- **Leverage the existing hardware investment in Juniper's forwarding devices**—Instead of investing in new equipment, you can repurpose the existing forwarding devices and gain the benefits of this highly scalable and high-performance architecture.

While Juniper offers the ability to scale, we recognize that traditional scale-out approaches often come with added operational complexity. With Juniper® Security Director Cloud, no matter how many firewall engines are added to the infrastructure, you can manage them as one logical unit, giving security administrators full visibility into where data resides, where users are, and who accesses what from where. Moreover, whenever a firewall engine is added to a new site, existing security policies can be rolled out automatically. Juniper's experience-first approach eases and simplifies administration, from policy management to version upgrades. With a Connected Security Distributed Services Architecture, security administrators achieve more without doing more.

Features and Benefits

Single policy framework from a single UI

Unified policy management from the edge to the data center means fewer policy gaps, more redundancy, elimination of human error, and a more secure environment. Administrators can manage all phases of the security-policy life cycle for firewall services and gain insight into sources of risk across the network from a single interface. They also can manage zero- touch provisioning from the same interface.

Industry Highest Efficacy Next-Generation Firewall

In 2023, Juniper received an "AAA" rating CyberRatings' Enterprise Network Firewall Report, demonstrating a 99.9% exploit block rate with zero false positives.

Juniper's Next-Generation SRX Series Firewalls deliver industry-leading threat protection and have been consistently ranked #1 for efficacy in every test for the past four years. The SRX4700, the latest addition to the SRX Series, delivers industry's highest firewall throughput performance per rack (1.4Tbps per rack with full support of 400GE port), protecting data centers by extending high-performance security to every point of connection on the network.

EVPN-VXLAN Support

Ethernet VPN–Virtual Extensible LAN (EVPN-VXLAN) configuration (EVPN Type 5 Route) is supported across all Juniper SRX Series Firewalls. Security is embedded across the entire EVPN-VXLAN fabric, everywhere your workloads are.

When policy enforcement points are embedded into the data center fabric, a network becomes truly threat aware, and security controls become composable. EVPN/VXLAN enables the SRX firewalls to be fully fabric-aware, which means the technical contexts defined by the network engineering team, such as tenant, virtual routing and forwarding (VRF), VXLAN network identifiers (VNIs), and others are shared with the SRX, providing visibility and understanding of a network setup and segmentation. Changes made to the network automatically propagate quickly via standard protocols, eliminating manual intervention.

Full fabric awareness gives security operators the situational awareness to respond to threats faster and reduce the blast radius of an attack to the smallest possible area using everything available to them, including the network.

URL Filtering

Users spend more than half their time browsing the Internet and using web-based tools. URL filtering enforces compliance needed by specific types of organizations. Administrators can block unwanted URL categories, such as gambling and malware sites, and re-categorize them at any time. URL localization across 200-plus geographies also keeps business traffic safe from threats.

Implement Zero Trust at Your Own Pace

Organizations are at different stages of implementing zero trust. They often face difficulties with the implementation due to shrinking budgets or bolt-on infrastructure that is too rigid to change.

The Connected Security Distributed Service Architecture allows organizations to easily add new forwarding and service devices, increasing the performance, scalability, or both, of security services without adding complexity and management overhead. Having network traffic spread across multiple service devices not only increases resiliency and performance, it also gives organizations the business agility to purchase devices as needed for business requirements. Flexibility is built into Connected Security Distributed Services Architecture so that organizations can take either big and small steps to improve the security scalability and performance at their data centers.

Solution Components

Security Director Cloud

Juniper Security Director Cloud enables organizations to manage security anywhere and everywhere, on-premises and in the cloud, with unified policy management that follows users, devices, and applications wherever they go. Policies can be created once and applied everywhere.

SRX Series Firewalls

Juniper Networks® SRX Series Firewalls protect data and applications and secure their access by enforcing and aligning policies across all data center environments, including private cloud, public cloud, and cloud-native, with physical, virtual, and containerized firewalls and follow-the-application policies. Never trust by default, always verify—with built-in zero trust, the SRX protects keys from compromise and substantiates Juniper-authentic software and product, mitigating the risk of data spoofing and supply chain attacks.

- **SRX 4000 and 5000 Series Firewalls**
  Juniper Networks SRX4000 and SRX5000 lines of next-generation firewalls protect mission-critical data center and campus networks for large enterprises, service providers, and cloud providers. They deliver IPsec VPN, fully automated SD-WAN, and easy policy management to make securing the network simpler and less prone to error. The next-generation firewalls integrate networking and security in a single platform to deliver industry-leading intrusion prevention and dynamic malware protection with high performance and scalability. The SRX4700 and SRX5000 line also act as a SD-WAN hub that delivers secure and resilient connectivity to today's cloud-centric businesses.
- **vSRX Virtual Firewalls**
  Juniper Networks vSRX Virtual Firewall offers the same features as physical SRX Series firewalls, including next- gen firewall capabilities, robust networking, and automated virtual machine life-cycle management, all in a virtualized form factor. Its highly dynamic and elastic nature is perfect for virtualized data centers with frequent additions and changes. It delivers security services scalable to match network demand and operates at speeds up to 200 Gbps..
- **cSRX Container Firewalls**
  Juniper Networks cSRX Container Firewall, offering the same features as virtual SRX Series firewall except the routing capacity, protects containerized applications and environments

with advanced security services. Purpose- built for containers, the cSRX next-generation firewalls can be spun up or down in less than a second, providing the agility needed to manage transitory container environments like Kubernetes.

Juniper Advanced Threat Prevention (ATP)

Juniper Advanced Threat Prevention is a threat intelligence hub and uses machine learning algorithms to provide complete advanced malware detection and prevention. Juniper Advanced Threat Prevention supports threat detection without breaking encryption and identifies compromised devices. When integrated with SRX Series Firewalls, it leverages a global threat database to deliver threat intelligence, dynamic malware analysis, encrypted traffic insights, and adaptive threat profiling. Advanced Threat Prevention protects against trojans, worms, ransomware, botnets, and IoT threats.

AI Predictive Threat Prevention

AI-Predictive Threat Prevention predicts and prevents malware on the wire by using AI to identify potential threats. It reduces false positives by filtering out non-threatening activities, reducing false-positive “noise” so the operations team can focus on more critical security tasks. In addition, AI Predictive Threat Prevention discovers dangerous threats in real time. Using AI keeps known threats and zero days off the network at line rate for the entire attack life cycle—not merely 24 hours, like other technologies—keeping the network safe from initial and subsequent attacks.

Encrypted Traffic Insights

Encrypted traffic insights help you detect malicious threats hidden in encrypted traffic without decrypting and reencrypting the traffic.

SecIntel

SecIntel identifies and shuts down attacks across the network before they can do any damage, protecting users, applications, and infrastructure. Security threat intelligence feeds aggregate data from multiple sources, including Juniper devices, to deliver curated, consolidated, and actionable intelligence. These threat feeds are an essential component of a threat-aware network, allowing IT teams to improve visibility and security while continuing to reduce risk.

Table 1: Juniper Zero Trust Data Center solutions support multiple use cases

Use Case	Description	Benefits
Data Center WAN Gateway	Data center access protection, north-south traffic	• Enforce legitimate data center access • Stop threats from entering the data center • Align data center security policies with user access policies • Provide security without sacrificing performance
Intra-Data Center Firewall	East-west traffic and segmentation	• Allow microsegmentation between servers • Stop lateral movement • Enforce legitimate data movement between applications • Easily support and manage modern applications • Reduce complexity and OpE
Cloud and Data Center Interconnect	Application connectivity and data exchange	• Scale secure data transactions from cloud to cloud • Prevent threats from moving between data center locations • Reduce downtime
Public Cloud	Application access and data exchange	• Scale security across any and all clouds • Automate changing application security requirements • Seamlessly migrate to new infrastructure • Minimize time-consuming tasks and misconfigurations

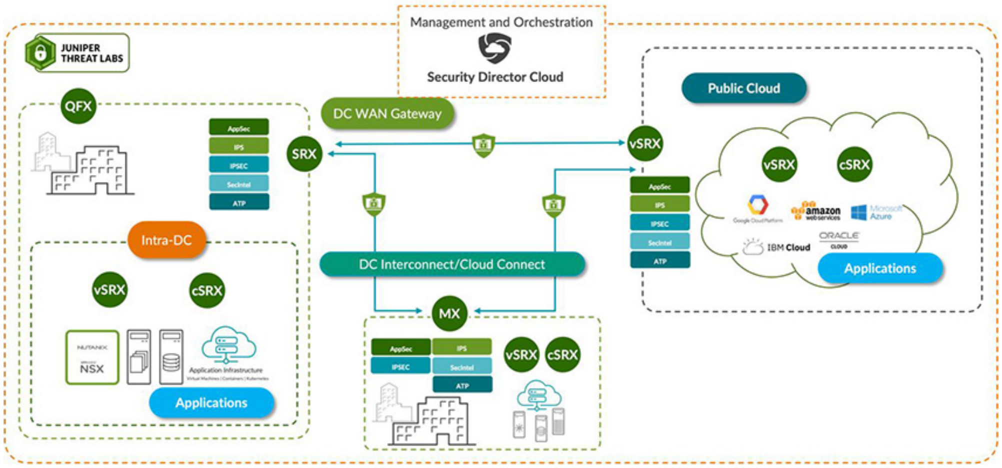

Figure 2: In the Juniper zero trust data center solution, Security Director Cloud manages multiple use cases

Summary—Operationalize a Zero Trust Data Center

As organizations make the architectural shift to centers of data, achieving operational simplicity and maintaining data security are paramount. Juniper's comprehensive Zero Trust Data Center solution with a Connected Security Distributed Services Architecture provides a secure pathway for organizations to make a seamless transition to zero trust. The new extensible architecture enables unlimited scalability and performance within a unified zero trust policy framework that supports security everywhere.

Organizations can operationalize security services everywhere and transition from firewall to firewalling the entire network. Security will reach every point of connection, delivering uncomplicated, fully operational Connected Security.

Next Steps

Visit https://www.juniper.net/us/en/security.html or contact your Juniper representative for more information on the Juniper Zero Trust Data Center solutions

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:**
+31.0.207.125.700