HYBRID MESH SECURITY: MANAGE SECURITY ANYWHERE AND EVERYWHERE

Discover Juniper's simple and seamless management experience

Challenge

As architectures such as SASE, zero trust, and hybrid mesh emerge, organizations must adopt them without a complex ramp-up process. Ops teams must handle the complexity of managing disparate security tools, which break visibility and lack consistent policies across architectures.

Solution

Juniper Hybrid Mesh Security powered by Security Director Cloud enables organizations to secure their architecture with consistent security policies across any environment, expanding zero trust across the network from the edge into the data center and to applications and microservices.

Benefits

- *Benefit from a simple, seamless management experience delivered in a single UI*
- *Manage security anywhere with unified policy management that follows users, devices, and applications wherever they go*
- *See what's happening on the network and keep it protected with complete visibility and consistent security*
- *Secure every point of connection on the network to safeguard users, applications, and infrastructure*

Solution Brief

As distributed workforces become more prevalent and new architectures emerge, securing the network edge is more critical than ever to ensure users can access the data and applications they need when they need them.

In securing an organization's distributed workforce, cloud-delivered security is not enough. Every organization must start by putting employees first, allowing them to securely access the data and applications they need to do their jobs effectively while streamlining processes. Unbroken visibility from client to workload, security assurance, and a single policy framework are essential tools to help secure a remote workforce.

The Challenge

As new architectures such as Secure Access Service Edge (SASE), zero trust, and hybrid mesh continue to emerge, organizations must adopt these new architectures without a long, complex ramp-up process.

Right now, organizations are likely to experience serious challenges when looking to adopt these new architectures due to disparate security management consoles that break visibility and lack consistent security policies across environments. Managing multiple security management tools can cause operational headaches for Ops teams in addition to what they already experience in their day jobs. They must manage these disparate architectures and fill in the visibility gaps while keeping the network protected, supporting the remote workforce, and ensuring business consistency.

The Juniper Hybrid Mesh Security Solution

The first step towards a streamlined architectural transition and the key to ensuring a great user experience is a simplified security management experience designed and tailored to meet the needs of security teams.

Juniper® Security Director Cloud, a simple and seamless management experience, addresses these challenges. Delivered in a single UI, Security Director Cloud connects organizations' current deployments with their future architectural rollouts. Management is at the center of the Juniper Connected Security strategy and helps organizations secure every point of connection on their network to safeguard users, applications, and infrastructure. Juniper meets our customers where they

are on their journey and helps them leverage their existing investments. Teams are empowered to transition to their preferred architecture at a pace that is best for business by automating their transition with Security Director Cloud.

Juniper Hybrid Mesh Security powered by Security Director Cloud enables organizations to secure their architecture with consistent security policies across any environment—on-premises, cloud-based, cloud-delivered, and hybrid—and expands zero trust across the network from the edge all the way into the data center and to the applications and microservices. With Security Director Cloud, organizations have unbroken visibility, policy configuration, administration, and collective threat intelligence all in one place.

Security Director Cloud provides a hybrid mesh security architecture so organizations can see what's happening on the network and keep it protected with complete visibility and consistent security from client to workload, at the edge, and into the data center. It enables organizations to manage security anywhere and everywhere, on-premises, and in the cloud and from the cloud, with unified policy management that follows users, devices, and applications wherever they go.

Features and Benefits

Security Director Cloud

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.

Juniper Secure Edge

Juniper Secure Edge secures the remote workforce anywhere with the fast, reliable, and secure access they need. Organizations can deliver full-stack Secure Services Edge (SSE) capabilities, including Firewall-as-a-Service (FWaaS), Secure Web Gateway (SWG), Cloud-Access Security Broker (CASB) with Data Loss Prevention (DLP), and advanced threat protection to protect access to Web, Software as a Service (SaaS), and on-premises applications. It provides users with security that follows them wherever they go.

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. Data isn't bifurcated—Security Director Cloud provides a single vantage point to see how data and access are protected without having to dig through a bunch of dashboards.

Microsegmentation

Microsegmentation provides granular levels of segmentation and control at the app and workload levels and allows alignment of those segmentation policies across the edge and into the organization's data center environments, including cloud-native applications, to ensure no gaps are present. The impact of any successful threat is small and easy to identify quickly.

Juniper Cloud Workload Protection

Cloud-native application protection (CNAPP) defends both on-premises and cloud-native application workloads against advanced and zero-day exploits automatically as they happen. It shields application resources from lateral threat propagation and keeps business-critical services connected and protected.

Juniper Secure Connect

Zero Trust Network Access (ZTNA) gives remote users secure access to corporate and cloud resources, providing reliable connectivity and consistent security to any device, anywhere. Organizations can reduce risk by extending visibility and enforcement to users and devices wherever they are.

Security Director Insights

A single, comprehensive dashboard provides a complete picture of what's happening across the organization's environment and correlates threat detection information, including detections from third-party technologies. Orchestrated incident responses mitigate threats and address gaps in defense quickly.

Solution Components

SRX Series Firewalls deliver integrated Hybrid Mesh Security with application awareness, user identity, and content inspection for all deployments—physical, virtual, containerized, and as-a-service. In addition to next-generation firewall (NGFW) capabilities, the SRX Series Firewalls offer intrusion prevention, SSL inspection, URL filtering, and unknown threat detection, providing a single security platform that addresses a range of security requirements from a common architecture.

User Identification and Access Control: User Firewall

User identity is a core requirement of next-generation firewalls enabling administrators to create security policies that reflect business needs rather than network requirements. This flexibility provides a powerful mechanism for defining, managing, and refining security policies by creating firewall rules based on user identity rather than IP address.

Through Juniper's user firewall feature, an SRX Series Firewall can associate network traffic with a specific user by integrating directory services such as Active Directory. Organizations can define policies to allow application use based on individual users or user groups, enabling more powerful but straightforward

security controls. Through the user firewall, security policies can be expressed in terms of groups, allowing security policies to continue functioning as users are added or deleted from groups. In addition, the user firewall provides visibility into application usage at the user level rather than IP address, providing powerful insights into application traffic traversing the network. Security administrators can reduce the threat footprint by adjusting security policies to align application usage with security and business practices.

Application Identification and Control: AppSecure

The days of tying applications to traditional port-based communications are long gone. Today, new applications are designed to change ports and protocols dynamically. Some are designed to tunnel through services such as HTTP Web traffic. This means applications can be used anywhere, at any time the user needs. But empowering users to access applications anywhere poses a challenge in defending against a constantly changing threat landscape that directly targets applications and passes through traditional network-layer protections to protect the enterprise.

Juniper Hybrid Mesh Security offers a robust security platform that is well equipped to meet this challenge. At the core is Juniper Networks AppSecure, which offers complete visibility and control over applications on the network.

AppSecure quickly recognizes applications and surfaces the application name, description of the service, and inherent level of risk, regardless of port, protocol, or encryption method.

Offering deep application visibility and control, AppSecure provides the context that links application use to a user, regardless of location and device. Furthermore, AppSecure understands application behaviors and identifies vulnerabilities, enabling administrators to block risky applications before they can do any damage. AppSecure helps reduce an application's threat footprint by allowing the definition of granular security policies, such as the level of deep packet inspection required and which users or groups are allowed access.

Exploit Protection: Intrusion Detection and Prevention

The Juniper intrusion prevention system (IPS) is tightly integrated with SRX Series Firewalls to mitigate network and application exploits and protect against a range of attacks. Juniper's intrusion detection system (IDP) constantly monitors for new exploits against recently discovered vulnerabilities, keeping network protection up to date against the latest cyberattacks and stopping them at the exploit stage before they gain a foothold inside the network. Organizations can enable IDP signatures in detection-only mode or inline to block malicious traffic directly.

Real-Time Protection: SecIntel

Juniper's Security Intelligence (SecIntel) provides verified threat intelligence to all points of connection across the network to block malicious traffic, enabling a threat-aware network. To help reduce risk, SecIntel can be deployed on the SRX Series Firewalls to block malicious traffic originating from malicious IP addresses and domains without needing deep packet inspection. SecIntel's threat feeds are automated and constantly updated. Additionally, these feeds are scrubbed and verified by Juniper Threat Labs to maintain high detection efficacy and reduce false positives. SecIntel can help reduce the load on the network while making it more intelligent.

Block Known Threats: Network Anti-Malware

Malicious files, including ransomware and adware, are becoming more prevalent from multiple attack vectors. These threats compromise network endpoints and make them vulnerable to data theft, including credentials and personally identifiable information (PII). Detecting and blocking malware and unwanted files at the network level before making it onto an endpoint is critical to safeguarding users, applications, and infrastructure against attacks.

Anti-malware protection combines cloud-based file reputation intelligence and malware signatures with the SRX Series Firewalls to deliver lightweight and fast security. The result is a highly effective perimeter defense against many known threats, which doesn't slow down users or the business.

Browsing Defense: Enhanced Web Filtering

Users spend more than half their time browsing the Internet and using web-based tools. Web traffic must be both legitimate and safe. At the same time, specific Web applications, such as online banking or healthcare, must remain private. Enhanced Web Filtering (EWF) allows administrators to block unwanted URL categories, such as gambling and malware sites and enables selective decryption to keep business traffic safe from threats. In contrast, users' personal traffic can remain private. EWF contains more than 180 URL categories that can be used within security policies on the SRX Series Firewalls to reduce attacks.

Encrypted Protection: SSL Proxy

SSL has become the universal method for authenticating websites and encrypting traffic between Web clients and Web servers.

Since SSL content is encrypted, users can download malware directly onto client endpoints. Since organizations have no visibility into SSL connections, they are blind to any threats transmitted over HTTPS into their corporate enterprise.

Juniper offers a powerful application-level SSL proxy that sits between client and server, intercepting encrypted traffic, terminating the session, and re-initiating the connection

towards the end destination. It can be used as an SSL "forward" proxy that sits between users on the corporate LAN and their access to the Internet, protecting the end client. It also intercepts HTTPS traffic by acting as a gateway at the enterprise perimeter and terminates encrypted traffic before impacting the organization. At that point, unencrypted traffic is immediately inspected to determine compliance with security policy, as set by the security team. Traffic is then handled by proactive malware engines that instantly block malware, thwarting any security breach.

The SSL proxy can be configured with exemptions that prevent traffic between specific URLs from being decrypted for user privacy protection. The exemptions can be set based on user groups, URL, or custom categories.

Unknown Threats: Advanced Threat Prevention (ATP)

Advanced Threat Prevention is Juniper's 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 decryption and surfacing 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.

Ensure Great User Experiences and Streamline Security Management

As organizations adopt new architectures such as SASE, zero trust, and hybrid mesh, they need a seamless solution to help them transition to their architecture of choice. The best place to start is with a simplified security management experience designed and tailored to meet the needs of security teams.

Juniper Hybrid Mesh Security powered by Security Director Cloud enables organizations to secure their architecture with consistent security policies across any environment—on-premises, cloud-based, cloud-delivered, and hybrid—and it expands zero trust to all parts of the network from the edge all the way into the data center and to the applications and microservices. With Security Director Cloud, organizations have unbroken visibility, policy configuration, administration, and collective threat intelligence all in one place.

Security Director Cloud provides a Hybrid Mesh Security architecture, so organizations see what's happening on the network and keep it protected with complete visibility and consistent security from client to workload, at the edge, and into the data center. It enables organizations to manage security anywhere and everywhere, on-premises, and in the cloud and from the cloud, with unified policy management that follows users, devices, and applications wherever they go.

Juniper meets customers where they are on their journey, helping them leverage their existing investments and empowering them to transition to their preferred architecture at a pace that is best for their business.

Next Steps

Visit www.juniper.net/security or contact your Juniper representative for more information on the Juniper Hybrid Mesh Security and Security Director Cloud 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.

JUNIPER NETWORKS | Driven by Experience™

APAC and EMEA Headquarters
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: +31.207.125.700
Fax: +31.207.125.701

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 | Fax: +1.408.745.2100
www.juniper.net

3510760-001-EN Aug 2022