

ENTERPRISE AT HOME FOR FINANCIAL SERVICES

Keeping remote workforces secure

Challenges

Financial organizations need to keep remote users connected and productive while ensuring business continuity and security. Endpoint protection and a simple VPN back to headquarters is not enough; what's needed is a comprehensive, connected security strategy.

Solution

By combining Mist Wi-Fi and Mist Edge with Juniper Connected Security, financial organizations can extend the AI-driven Enterprise into employees' homes. With zero-touch provisioning, Juniper security hardware and Mist Wi-Fi access points can be deployed remotely, without a technician.

Benefits

- Gain AI-driven insights into remote user experiences, simplifying deployments with zero-touch provisioning
- Eliminate overlay VPN technologies while extending the enterprise network into employee homes
- Monitor business Wi-Fi to secure and segment business and personal traffic on the network
- Keep threats in check with advanced security services
- Cultivate a dynamic, flexible, adaptable network

According to a recent Gartner CFO survey, nearly a quarter of respondents said they will move at least 20% of their onsite employees to permanent remote positions.¹ This transformation will complicate a financial services industry where going to an office has been the norm for decades. Further, some power users may require the higher degree of security than an office setting provides.

Suddenly, IT teams at finance organizations have a brand new, complex challenge they need to solve; namely, how do they keep remote users connected and productive while ensuring business continuity and security? IT leadership knows that endpoint protection and a simple VPN back to headquarters is not enough. What's needed is a comprehensive, connected security strategy.

Financial organizations must keep their networks secure while maintaining the flexibility to scale rapidly to support ever-changing traffic patterns and satisfy a constantly expanding remote workforce. And they must be proactive in tackling challenges quickly and efficiently to ensure continuity of operations.

The Challenge

Financial organizations around the globe have experienced a sudden and significant increase in remote staff, overloading traditionally configured VPNs. While routing all endpoint traffic through an organization's core network infrastructure simplifies security by centralizing and concentrating defenses, it also increases traffic volume, potentially slowing access to resources and negatively impacting the remote user experience.

In today's environment, there is a real need for organizations to provide fast, reliable connections, ensure data is secure, and scale dynamically to meet escalating business demands.

The Juniper Networks Enterprise at Home Solution

By combining Mist Wi-Fi and Mist Edge with Juniper Connected Security, financial organizations can extend the AI-driven Enterprise into employee homes to provide the necessary level of protection. With the Juniper Networks® Enterprise at Home solution, financial organizations can deploy Juniper security hardware and Mist Wi-Fi access points using zero-touch provisioning (ZTP) to roll out managed networking equipment without requiring a visit from a technician. Juniper's cloud-based management solution provides the scalability to meet the needs of even the largest deployments.

¹ Gartner Press Release: Gartner CFO Survey Reveals 74% Intend to Shift Some Employees to Remote Work Permanently, April 3, 2020, <https://www.gartner.com/en/newsroom/press-releases/2020-04-03-gartner-cfo-surey-reveals-74-percent-of-organizations-to-shift-some-employees-to-remote-work-permanently2>

Features and Benefits

- **Gain AI-driven insights into the user experience at home and in remote offices.** With Mist, IT teams can proactively troubleshoot and resolve issues from anywhere, using the Marvis Virtual Assistant, proactive anomaly detection, and Dynamic Packet Capture.
- **Simplify deployments with zero-touch provisioning.** With ZTP, there's no need for a technician to go onsite to install and configure the equipment. The user simply plugs in the Mist access point and the Juniper Networks® SRX Series Services Gateways firewall, and they come to life—even in a home. The IT department gains immediate insight into the user experience and, in most cases, will be able to identify and resolve any problems autonomously, managed in the cloud.
- **Eliminate overlay VPN technologies while extending the enterprise network into employees' homes.** With Mist Edge, finance organizations can securely extend their organizational service set identifier (SSID) and authentication services to remote offices, wherever they are. By installing an access point and enabling Mist Edge, organizations can extend their network to any user's remote location or home.
- **Easily monitor business Wi-Fi and keep corporate traffic safe.** Using Mist Wi-Fi with Mist Edge is an add-on to a user's existing home setup, effectively separating home use and business traffic. From a security standpoint, this walls off traffic between the business and other users in the home. If another member of the household accidentally downloads a lateral threat via phishing, the business remains safe.
- **Increase security and segment business traffic, ensuring a quality user experience with Juniper Connected Security.** In addition to Wi-Fi and a superior user experience, Juniper Connected Security provides powerful tools that financial organizations can extend into an employee's home network. SRX Series Services Gateways bring compact and robust firewalls to enable secure SD-WAN, Juniper Advanced Threat Prevention, and cloud-based orchestration, supporting any deployment needs. Juniper enables organizations to segment their employees' home networks, completely separating organizationally provided equipment from any personal devices on the home network.

In some cases, an enterprise may require additional hardware on site due to compliance issues or the financial impact of downtime. Juniper provides best-in-class security with the SRX Series firewalls that can connect to traditional broadband or terrestrial links for primary or backup traffic. Optionally, the SRX Series firewalls can include Power over Ethernet (PoE) to power devices such as phones and access points.

Juniper can provide the tools needed to support these efforts, saving time and money—all while increasing network reliability and security beyond what is available in traditional Wi-Fi solutions typically found at home.

- **Keep threats in check with advanced security services.** Now more than ever, security devices need to keep pace with the increased network load. Juniper's full suite of advanced threat capabilities, like next-generation firewall (NGFW) services and intrusion prevention system (IPS), helps maintain a safe and secure end-user experience by allowing security policies to scale at the rate of demand, minimizing network risk. Using SRX Series firewalls, IT teams can install additional security on premises to protect the network against threats. These advanced security services can safeguard business traffic while being able to separate business and personal traffic for privacy purposes. In some situations, an enterprise may need to have hardwired hardware or use proprietary protocols that require tunneling to function. The robust routing platform available with the SRX Series makes this possible.
- **Cultivate a dynamic and flexible network that can adapt as needs change.** Adding powerful solutions like SD-WAN and LTE backup is a great way to be prepared to scale quickly and easily, without having to rip and replace existing infrastructure. Juniper can help financial organizations adapt to changing traffic patterns, ensuring they have always-on connectivity and prioritization for business traffic. All of this can be provisioned with ZTP and is managed in the cloud.

By combining the insights-driven expertise of Mist with the security and traffic engineering of the SRX Series firewalls, employee productivity and security are enhanced.

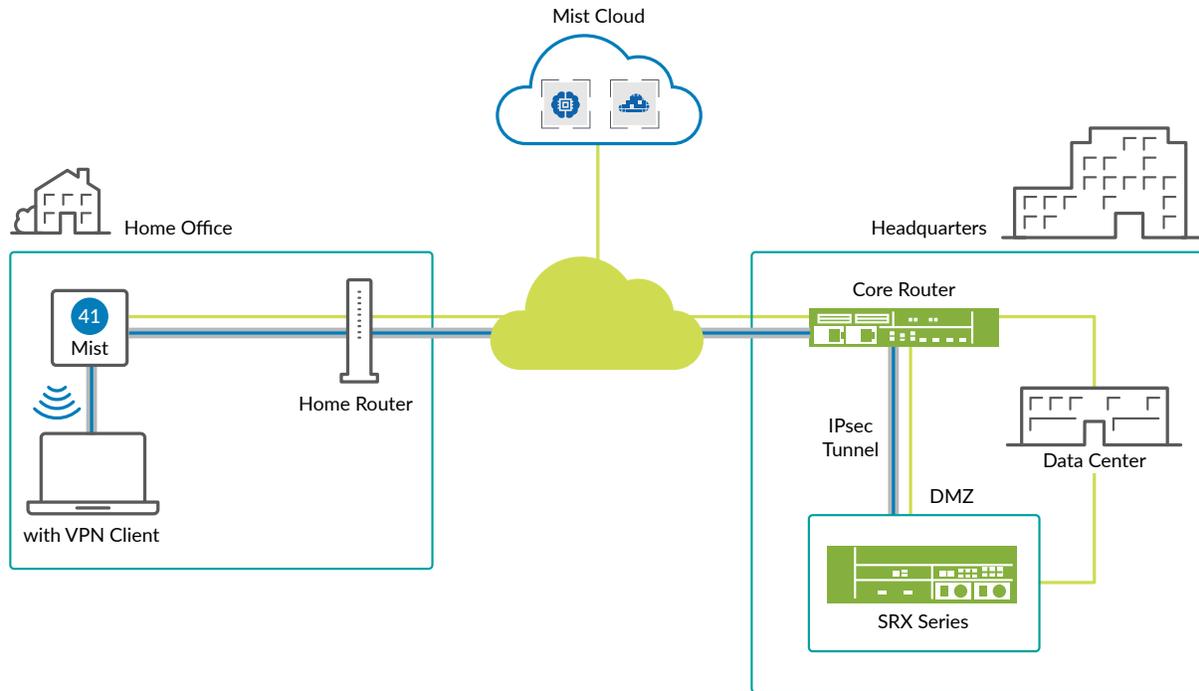


Figure 1: Mist Wi-Fi for Remote Workers solution

Solution Components

Mist Wi-Fi for Remote Workers

Deploying a Mist Wi-Fi access point in a remote office or an employee's home helps finance organizations leverage AI-driven insights to boost productivity. With Mist's Marvis AI engine, user experience and network issues and anomalies will be proactively identified, with root causes determined and resolved, either automatically or with user-driven actions. This increases network efficiency and allows IT teams to remotely troubleshoot home networks with ease.

Mist empowers organizations to secure their distributed access network, including employees working from home. By scaling with the agility of a microservices cloud, Mist Wi-Fi ensures that even the largest work-from-home deployments can be managed efficiently.

If remote workers already have a client-based VPN solution in place, the AI-driven Wi-Fi can easily be extended into their homes by simply plugging a Mist access point into their broadband router. This gives organizations unprecedented insight into the user experience, enabling automation that saves time and money while increasing network reliability.

The following table includes an example of hardware and software specifications for the Mist Wi-Fi for Remote Workers solution.

Product Code	Solution Description
AP41-US	Premium performance gigabit Wi-Fi Wave 2 access point (4x4:4) with adaptive Bluetooth low energy array for advanced location-based services and built-in internal antenna—U.S. deployments only.
APBRU	Universal AP bracket for T-rail and drywall mounting for indoor access points (included inside the box).

Extending the Enterprise with Mist Edge

The Mist Edge microservices platform helps eliminate costly and complex overlay VPN technologies while extending the enterprise network into employees' homes. Deployed in conjunction with Mist Wi-Fi access points, Mist Edge helps finance organizations securely extend their wireless and authentication services to remote locations anywhere in the world.

Managing the employee edge allows organizations to maximize traffic security while ensuring the best possible quality of experience (QoE) for the employee. Mist Edge can apply traffic shaping to ensure that traffic is treated rationally, allowing for business continuity while maintaining privacy.

The following table includes an example of the hardware and software specifications for the Extending the Enterprise with Mist Edge solution.

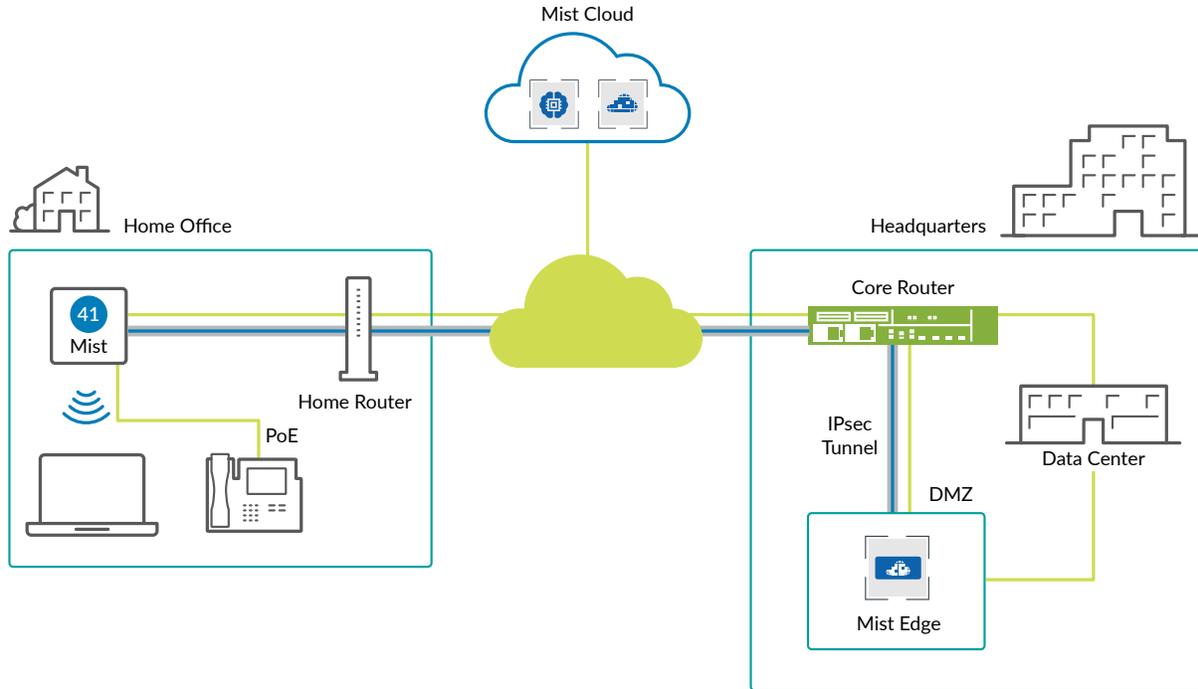


Figure 2: Extending the Enterprise with Mist Edge solution

Product Code	Solution Description
AP41-US	Premium performance gigabit Wi-Fi Wave 2 access point (4x4:4) with adaptive Bluetooth low energy array for advanced location-based services and built-in internal antenna—U.S. deployments only.
APBRU	Universal AP bracket for T-rail and drywall mounting for indoor access points (included inside the box).
SUB-ME-1S-1Y	Mist Edge Subscription for one year for one access point (data tunneling service).

Juniper Connected Security with Mist

Juniper Connected Security with Mist helps to easily monitor business Wi-Fi and keep corporate traffic safe, ensuring a quality experience by separating personal and business data. In addition to delivering reliable Wi-Fi user experiences with Mist access points, Juniper Connected Security brings powerful tools that can be extended into an employee’s home network. The compact and robust SRX Series firewalls enable secure SD-WAN, Juniper Advanced Threat Prevention, cloud-based orchestration, and even LTE backup to support any deployment needs. Optionally, Mist Edge can be added to extend organizational SSID and authentication services to remote locations.

Juniper enables financial organizations to segment their employees’ home networks, completely separating organizationally provided equipment from personal devices. At

the same time, the organization can provide QoE by applying traffic shaping to ensure that traffic is treated rationally, allowing for business continuity while maintaining privacy.

The following table includes an example of the hardware and software specifications for the Juniper Connected Security solution.

Product Code	Solution Description
AP41-US	Premium performance gigabit Wi-Fi Wave 2 access point (4x4:4) with adaptive Bluetooth low energy array for advanced location-based services and built-in internal antenna—U.S. deployments only.
APBRU	Universal AP bracket for T-rail and drywall mounting for indoor access points (included inside the box).
SRX340-SYS-JB	SRX340 Services Gateway, which includes hardware (16GbE, 4x MPIM slots, 4 GB RAM, 8 GB flash, power supply, cable, and RMK) and Junos® operating system software base (firewall, NAT, IPsec, routing, MPLS, and switching).

Juniper can support any deployment needs, ensuring business continuity while maintaining security and privacy. At Juniper Networks, we help our customers maintain a safe and secure end-user experience now and for the future.

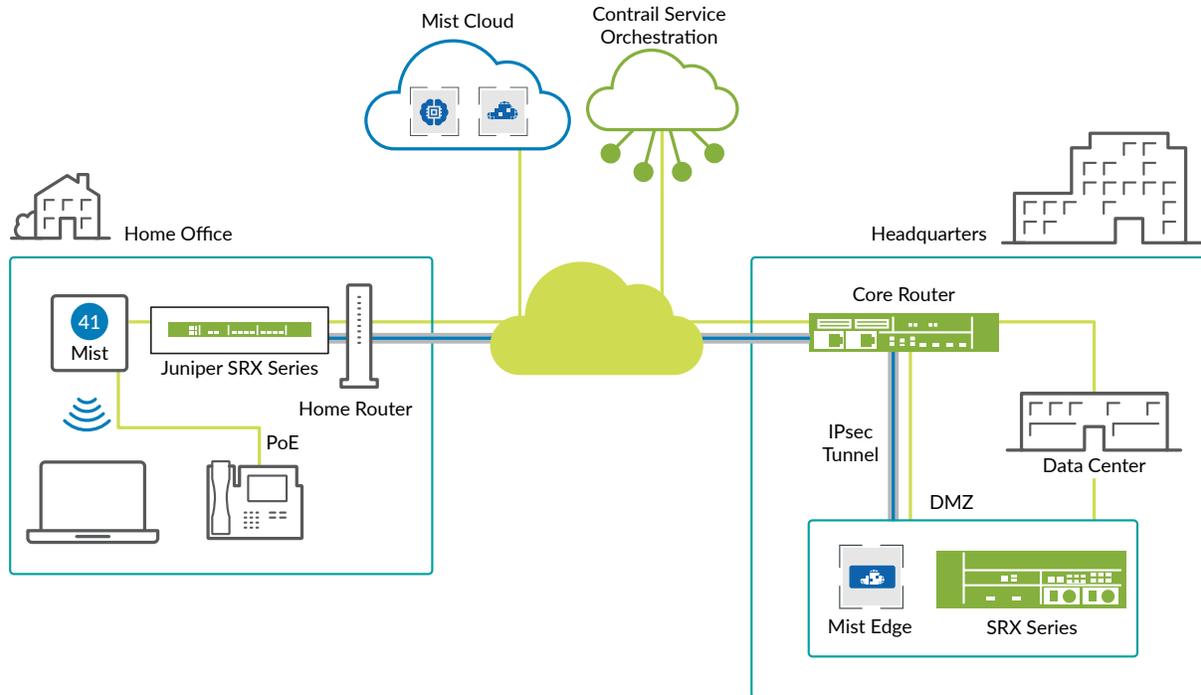


Figure 3: Juniper Connected Security with Mist

Enterprise at Home in the Real World

Recently, a Juniper customer in the financial industry came to us with a problem—how to support stock traders who suddenly needed to work from home. Their primary challenge: the staff needed to use an external device called a trading turret, a specialized telephony key system that requires an Ethernet connection and cannot run a VPN client. The trading turret is essential, as it allows stock traders to conduct business and connect their PCs to the corporate network. They needed to deploy a tactical solution that not only solved for these complexities but was plug-and-play for their nontechnical staff.

Juniper suggested deploying an SRX300 Services Gateway at each remote location and addressing the head-end capacity for small packets. We also recommended three pairs of SRX4600 Services Gateways at each of their international headquarter locations based on estimated traffic. To work at scale and to address the customer's requirements, Juniper's cloud management solution was selected to provide a basic management solution that offered simple ZTP from the cloud.

Each trader received a box containing the turret, the SRX300, and the necessary cabling, all color coded for easy installation. The traders followed the simple setup instructions (red cable

here, blue cable there) that initiated the ZTP process, and they were up and running in minutes. Within two weeks, the customer enabled approximately 500 traders and continues to bring more online. This is a great example of rapidly deployable business continuity combined with class-leading security.

Summary—Keeping the Remote Workforce Secure, Wherever They Are

Juniper is ready to help financial organizations gain insight into their remote user experience and employ automation to enhance and secure that experience. With Mist, Juniper Connected Security, SRX Series firewalls, and Juniper Advanced Threat Prevention, Juniper offers the tools needed to support the remote workforce, whether at home or on the move. These powerful solutions help organizations save time and money while increasing network reliability and security beyond what is available with traditional Wi-Fi solutions found in a typical home environment.

Next Steps

Contact your Juniper Networks representative for more information.

About Juniper Networks

Juniper Networks brings simplicity to networking with products, solutions and services that connect the world. Through engineering innovation, we remove the constraints and complexities of networking in the cloud era to solve the toughest challenges our customers and partners face daily. At Juniper Networks, we believe that the network is a resource for sharing knowledge and human advancement that changes the world. We are committed to imagining groundbreaking ways to deliver automated, scalable and secure networks to move at the speed of business.

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

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
Fax: +31.0.207.125.701

