CommScope Enterprise Home Networking Solutions

As companies adjust to the new normal of mass telework, corporate decision makers are looking for simpler ways to extend network services securely and efficiently to remote workers.

Today, these remote workers are using a mixture of wired and wireless devices to access a host of corporate resources—transferring large amounts of data across the network on a daily basis. Business-critical applications such as email, messaging, voice, video, and cloud-based applications must all work seamlessly from the home office.

In this post-COVID-19 world, home networks need enterprise-level security and reliability, as well as the ability to support high-performance connectivity for a growing number of users. The CommScope Enterprise Home Networking solution offers a simple and secure way for enterprise IT organizations to extend on-premises access to an employee's home network.

Enterprises no longer need to rely on traditional home WAN and LAN architectures that are unable to support large numbers of dispersed remote workers. Nor do they need to implement expensive and complex solutions such as SD-WAN.

COMMSCOPE®

RUCKUS ®

The CommScope Enterprise Home Networking solution begins with a RUCKUS® access point (AP) located in the employee's home, such as the H510 or R510.

These industry-leading access points are particularly suited for this application because they provide both wireless and wired connectivity, together with CommScope's patented BeamFlex® technology.

The RUCKUS AP is simply connected to the employee's home router of choice (e.g., ARRIS® SURFBOARD®) for access to the internet. The control and data planes are then separated and connected to the RUCKUS Virtual SmartZone High Scale Controller (vSZ-H) and the Virtual SmartZone Data Plane Controller (vSZ-D) resident in the corporate data center. The connection is made using SSH (Secure Shell), GRE (Generic Routing Encapsulation), and IPsec (Internet Protocol Security) encrypted tunneling technology. This allows wireless and wired traffic to be securely tunneled from the access point in the home to the corporate data center—giving remote workers access to all of the resources as if they were physically connected to the LAN in the office. RUCKUS also provides APs and controllers that are Federal Information Process Standards (FIPS) certified for added security.

For secure onboarding of devices, the optional RUCKUS Cloudpath® software can automatically connect the employee device to the corporate network using X.509 certificate authentication. Cloudpath helps to establish granular policy-based access control for all users and all devices connecting remotely from home. To properly protect the corporate network, Cloudpath ensures the requisite on-device enforcement, such as enabling a firewall, installing certain applications, or updating anti-virus. A customer-provided RADIUS server may be used instead, if available.

In the home, non-corporate traffic can be bridged locally—creating a hybrid environment that gives the rest of the family the benefit of an enterprise-class network while keeping them segmented from the corporate network.

Finally, the optional RUCKUS Analytics software can be added for more efficient network management, operations, reporting, troubleshooting, and remediation. RUCKUS Analytics is a new breed of network monitoring tool designed to leverage machine learning and artificial intelligence.
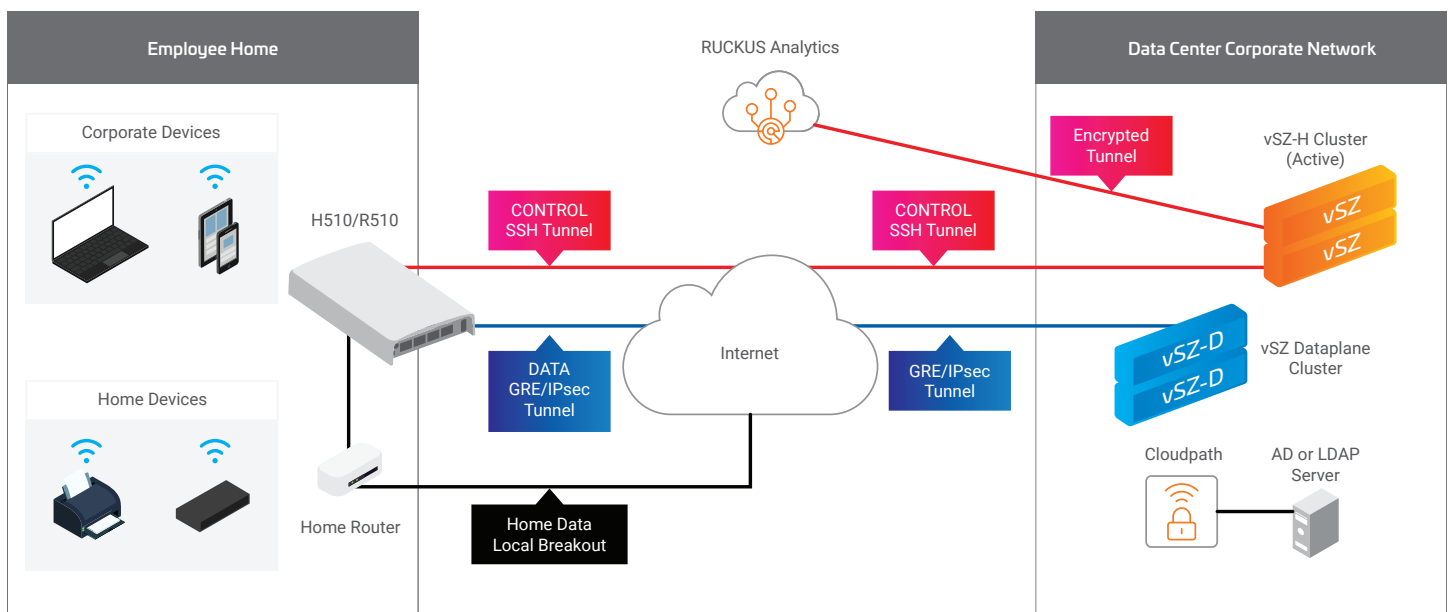
The CommScope Enterprise Home Networking Solution offers a number of advantages, from security and ease of operation to manageability

Secure encryption
- GRE or IPsec tunneling between the devices and the corporate network, thus removing the complexity and limitations of VPN concentrators.

Policy enforcement
- Cloudpath automatically and securely connects Wi-Fi and wired devices using X.509 certificate authentication. Head-less devices, such as printers, can also be authenticated since the solution is operating system independent.

Traffic segregation
- The RUCKUS GRE tunnel extends the subnet from the corporate LAN to the home corporate devices. Personal home traffic data is transmitted through local breakout (LBO) to the internet.

Access control
- Layer 2/MAC address Access Control Lists (ACL) can be defined per WLAN to restrict or allow specific clients.

Authentication
- The 802.1X EAP authentication method (also known as WPA2-Enterprise or WPA3-Enterprise) is a highly secure method for protecting the authentication process. The use of Dynamic PSK is also supported, giving administrators the ability to terminate individual accounts or devices with ease.

FIPS 140-2 Compliance
- RUCKUS APs and controllers support FIPS mode, which is compliant with the standards established by the National Institute of Standards and Technology (NIST).

URL filtering
- RUCKUS SmartZone controllers provide URL filtering to block access to inappropriate websites.

Wired and wireless coverage
- The RUCKUS R510 has an extra Ethernet port and the H510 contains four Ethernet ports to connect wired PoE network devices like company-provided IP phones or a printer.

Access point registration
- Automatically register access points to the controller to provide ease of deployment for the user, while preventing rogue connections.

Resiliency
- If connectivity with the controller should stop for any reason, existing connected clients will remain stable and can still transmit data.

Client isolation and rate limiting
- This feature can be set up per WLAN to isolate traffic and provide extra bandwidth for corporate data versus personal home data.

SmartMesh
- Multiple access points can form a mesh inside the home to provide better coverage if required for structurally complex interiors.

SmartCast
- RUCKUS unique queuing and scheduling techniques deliver reliable quality of service (QoS) to all clients in complex traffic mixes.

Cost-effective
- The CommScope Enterprise Home Networking solution is much simpler and less expensive than other solutions on the market today, such as SD-WAN.

Scalability
- Virtual SmartZone clustering will support up to 30,000 access points, 450,000 clients, and up to 60 Gbps of aggregate throughput per cluster.

Machine learning and AI
- RUCKUS Analytics machine-assisted software allows the network IT team to become more proactive in network management, operation, reporting, and troubleshooting.

Troubleshooting
- The virtual SmartZone controller assists in troubleshooting connectivity issues through the use of a call trace that visually shows the steps the client device has taken to gain access to the network. If there is a problem, the exact step where the failure occurred is identified.

High availability
- Redundancy is achieved through active instances in a regional controller cluster, and geographic redundancy is achieved through active-standby clusters in multiple regions.

Operating system independence
- Since a VPN client is not required on any device, the CommScope solution is operating system independent.

The COVID-19 pandemic has sparked a dramatic shift in data usage patterns and network demand for remote workers—prompting the need for more bandwidth and capacity. This increase in real-time traffic requires better QoS and coverage, without compromising security.

CommScope's Enterprise Home Networking solution combines proven capabilities to meet these challenging demands—offering the performance, simplicity, and flexibility that employees have come to expect. To learn more, please contact your local account representative.

COMMSCOPE®

RUCKUS®

commscope.com
Visit our website or contact your local CommScope representative for more information.