Best Practices: VPN Connectivity for Employees

Virtual Private Networks are secure links created between remote employee's devices and the corporate network. VPNs allow employees to remain connected to essential business applications and internal documents while not being physically present in the office.

Many businesses, nonprofits, healthcare providers and schools have transitioned their workforce to enable them to work from home, in the office, or support a hybrid work environment. To ensure networks remain secure, we have created a list of Best Practices for users to follow.

Meet With You Direct Supervisor and IT Administrator

Meeting directly with your supervisor and IT administrator will allow you to establish an understanding of what daily business activities can be completed remotely and what additional software or hardware tools may be needed to assist you to work remotely and remain efficient.

Setup and Test VPN Connectivity

Setting up VPN connectivity on your computer is typically a simple process with the help of your IT administrator. Turning on your VPN on your device ensures that you have access to the applications, systems, and network resources you need to connect to on a daily basis from your home internet connection. If your VPN is setup properly, working remotely should be the same as working in the office. Thoroughly test your VPN when it is setup to ensure that you have the needed access before you attempt to work remotely.

Update All Software to the Most Current Version

This is the ideal time to make sure that every software program is running its most current version. This includes VPNs. VPNs connect devices 24/7 unless programmed otherwise, so it is necessary to use the most updated version provided by your IT administrator.

Multi-Factor Authentication (MFA)

Multi-factor authentication is a secondary layer of security used to access critical profile information. Activating MFA for VPN protects the corporate network against credential theft by requesting additional information via SMS message or another secondary authentication source.

About Arista Cognitive Unified Edge

Arista's Cognitive Unified Edge (CUE) solutions help distributed enterprises optimize their networks while safeguarding their data and networks. CUE redefines enterprise networks with enhanced security and connectivity, flexible PoE switching, and Wi-Fi 6/6E offerings that work together seamlessly to ensure connectivity, protection, monitoring, and control across the entire network from headquarters to the network edge.

Centralized Cloud Based Management

- Visibility across globally dispersed networks & endpoints
- Zero touch deployment for hardware appliances
- Advanced alerting & reporting for CIPA compliance

Next Generation Firewall

- Next-gen firewall, with IPS, VPN & more
- Protection, encryption, control & visibility anywhere
- Onboard security for small network appliances & IoT devices
- Full security processing on-premises or in the cloud

WAN Optimization

- Secure, WAN-optimized connectivity for every location
- Seamless scalability with centralized policy management
- Optimal predictive routing technology for first packet, dynamic path selection

Wired Connectivity

- Scalable PoE compact switches with 12 to 48 ports
- Based on Arista's Extensible Operating System (EOS)
- Wire rate encryption/tunneling
- Multi-gigabit uplink speeds from 1 to 100 Gbps

Wi-Fi 6 Access Points

- Enterprise class Wi-Fi 6 and Wi-Fi 6E technologies
- Optimized performance to scale from 1 to hundreds of users per AP
- Multi-gigabit uplink choices based upon bandwidth needs
- Open, published APIs for integration with ITSM and monitoring tools

As employees continue to work from home, maintaining connectivity to business critical applications as well as their team members will help business operations move forward effectively.

Using a VPN allows access to important files so employees can continue to help their customers and business move forward.

Santa Clara—Corporate Headquarters
5453 Great America Parkway,
Santa Clara, CA 95054

Phone: +1-408-547-5500
Fax: +1-408-538-8920
Email: info@arista.com

Ireland—International Headquarters
3130 Atlantic Avenue
Westpark Business Campus
Shannon, Co. Clare
Ireland

Vancouver—R&D Office
9200 Glenlyon Pkwy, Unit 300
Burnaby, British Columbia
Canada V5J 5J8

India—R&D Office
Global Tech Park, Tower A, 11th Floor
Marathahalli Outer Ring Road
Devarabeesanahalli Village, Varthur Hobli
Bangalore, India 560103

Singapore—APAC Administrative Office
9 Temasek Boulevard
#29-01, Suntec Tower Two
Singapore 038989