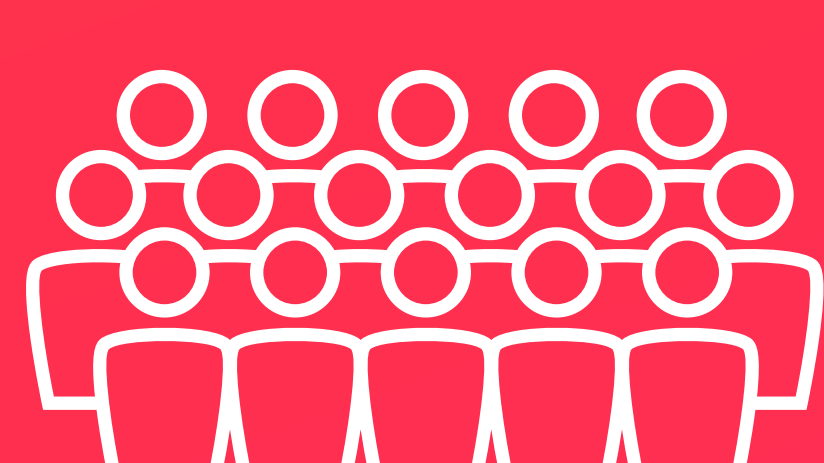# Secure remote working for SMB's

The transition to remote working opens users and companies up to a myriad of security threats including malware, all forms of phishing attacks and many more.

Fortinet has identified remote worker scenarios with three primary levels of connectivity.

Remote Users

Applies to most people in the company.

Need access to Email, Data & Applications whilst connecting remotely.

For Remote Users, a Virtual Private Network or VPN tunnel is needed to connect to the firewall back at the office. FortiGate customers already have high-performance VPN at their fingertips and can download FortiClient VPN agent for end points. The VPN client can be coupled with Fortinet's FortiToken providing additional security with two factor authentication.

Power Users

Applies to specific roles who spend extended periods of time on the corporate network.
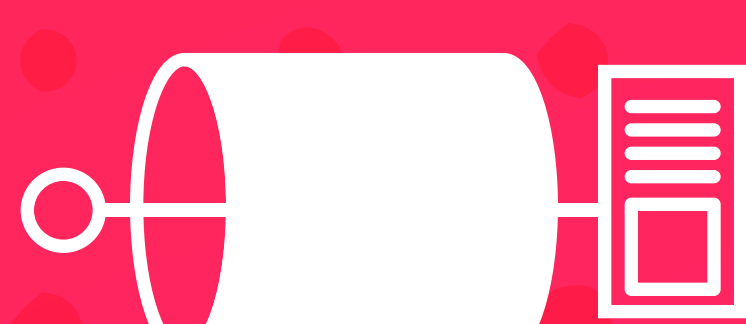
Need a consistent, secure always-on connection to the head-end firewall for multiple devices.

For Power Users, FortiAP can establish a secure connection back to the office and can be set up at home. While the traffic from that wi-fi connection can get the same security policies that the FortiGate provides. Wireless networks can be configured exactly as they are in the office, so that devices can be securely connected just as easily.

Super Users

An executive or user with access to the most sensitive company information.

Need highest levels of security or application performance for their work.

For this user a small FortiGate will provide the highest level of security, whilst also enabling the deployment of additional hardware like FortiAP. This effectively creates a small branch office for the employee. The FortiAPs and FortiGates can be delivered straight to the user and the configuration pushed directly to the units.

Source: Fortinet UK and https://partnerportal.fortinet.com/prm/English/s/assets?id=263930
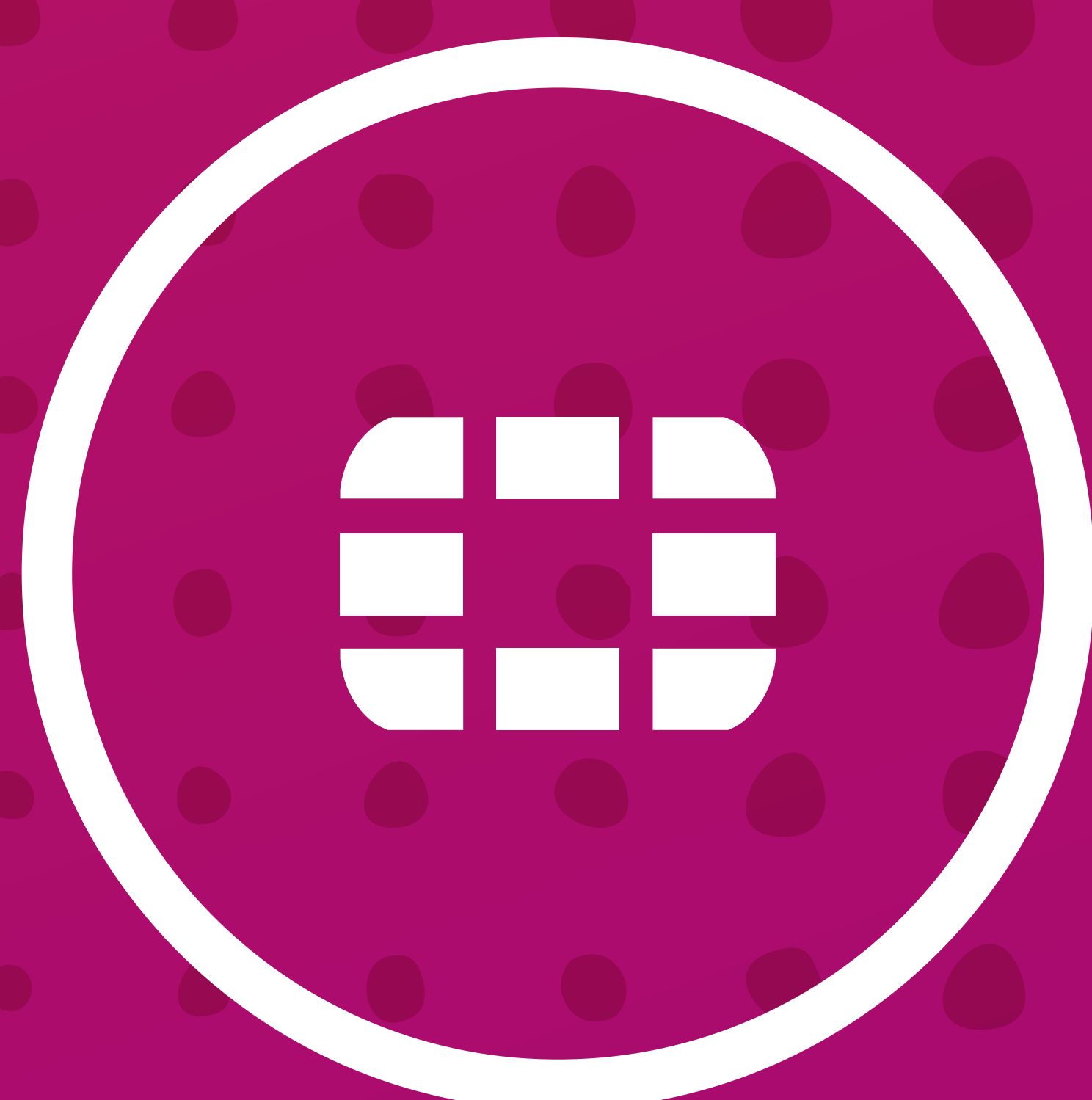
To support all users

The office they are connecting to needs a VPN Concentrator. Fortinet customers have this available for free as part of the FortiOS operating system. To help manage the many VPN clients deployed, FortiClient EMS, our endpoint management system can simplify larger deployments. For the two-factor authentication the office should have a FortiAuthenticator to coordinate this across all the FortiGates across the company.

For more information about Fortinet solutions for remote working visit:

www.fortinet.com/solutions/enterprise-midsize-business/network-access/teleworker-work-remote