FORTINET

WHITE PAPER

Remote Working Is the Next Normal

How to Stay Secure and Efficient Using FortiVoice Unified Communications

Introduction

The coronavirus has forced millions of corporate and government employees to work from home, and has created challenges for many companies that did not plan effectively for a majority-remote workforce. In order to maintain productivity, companies not only need a fast adoption of communications tools to ensure business continuity but they also need to help remote employees deal with the new way of working—securely.

Adjusting to Secure Remote Work

Working remotely has become acceptable in many organizations, but COVID-19 forced a majority of companies into scenarios where a majority or all employees are remote. Even when lockdown orders due to the pandemic are lifted, an overall shift toward remote work shows no signs of reversing in the long term. A recent Gartner survey found that 74% of CFOs have already reported they intend to make the shift to remote work for some employees a permanent one. All organizations need to adjust their infrastructure and invest in best-in-class communications technology that is reliable, flexible, and secure, regardless of whether employees are working remotely or in the offices.

Cybersecurity Risks for Remote Workers

Having a sizable number of employees working remotely can be a major change for organizations and presents numerous challenges in cybersecurity. The popularity of employees using their own devices for work and the availability of insecure network access also increase the risk of attacks like phishing and malware. Most security breaches are attributable to human errors, and in a remote environment, organizations are unquestionably more prone to users' mistakes and more likely to experience security gaps. Organizations need a secure and reliable communications solution that is easy to use and effective for employee collaboration.

41% of employees are likely to work remotely even after the pandemic, increased from 30% before the pandemic.[1]

90% of IT professionals believe remote workers post a security risk in general and over 54% think that remote staff poses a greater risk than onsite employees.[2]

Fortinet Unified Communications for Teleworkers

The Fortinet FortiVoice Unified Communications platform provides secure and comprehensive communications with integrated voice, conferencing, fax, and mobility support, enabling organizations to communicate and collaborate easily and securely. Its intuitive web-based portal simplifies management of your calling routing and preferences. The softclient for mobile and desktops helps preserve employee productivity while working remotely.

Use Cases for Remote Workers

Even before COVID-19 impacted many organizations, the workplace evolved significantly in the last decade and employees no longer have to be tied to their office desks. The Fortinet Unified Communications solution is designed to support a variety of use cases that enable employees in any size business to stay productive and collaborative, whether they are in their offices or teleworking.

Using Remote Extensions with Personal Devices

A remote extension is a physical number, such as a cell phone or landline, that can be configured as an extension within FortiVoice. When a caller dials an office extension number, the call will automatically be routed anywhere in the world based on the settings, or a receptionist can easily transfer calls to a proper remote user. These remote extensions are ideal for people constantly on the go.

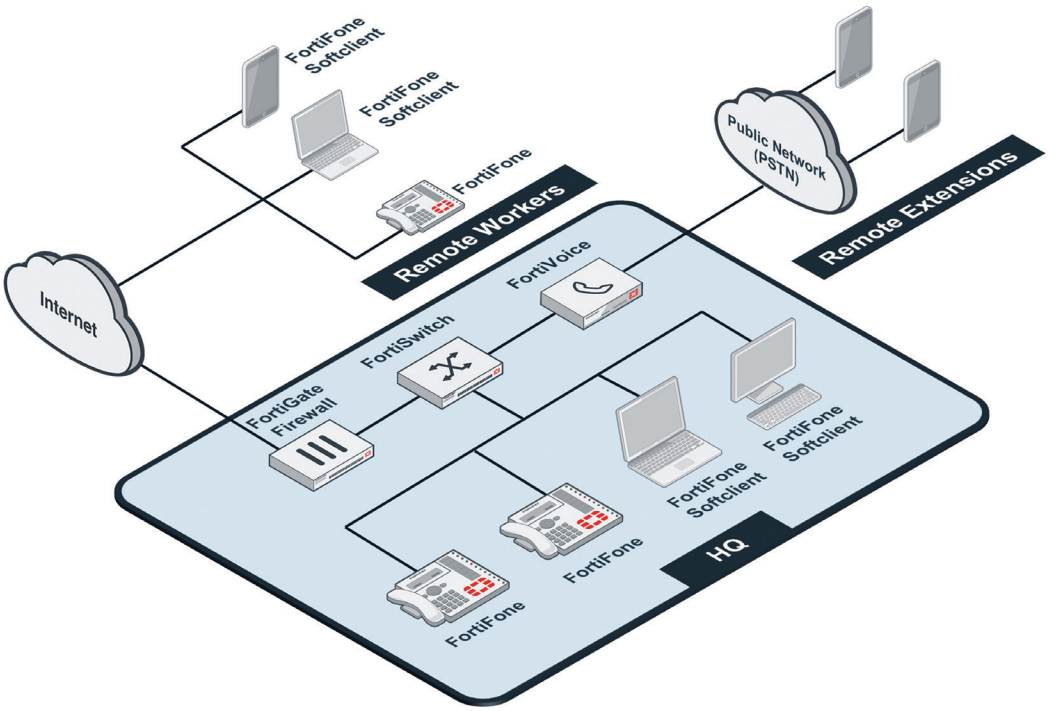

Figure 1: FortiVoice provides a number of solutions for staying securely connected while remote: Mobile softclient, Desktop softclient, External extensions, and Remote extensions.

Using External Extensions with FortiFone Phones

An external extension is identical to a regular extension, however, it exists outside of the physical office. Employees can bring their office IP phones home and connect the devices in their home network. These extensions have all the same features and functions—including appearance keys, auto provisioning, and complete call control—as they function in the office. These types of extensions are best suited for employees who have permanent home offices.

Using FortiFone Softclients for Mobile

Mobile softclients are the perfect hybrid solutions for power users who are constantly on the go and require the same features as regular in-office extensions. Mobile softclients run on Android or iOS phones and provide users with auto provisioning, visual voicemail, click-to-dial call logs, and complete call control. The softclients support both Wi-Fi and cellular data connections. When users are in the office they are using the corporate Wi-Fi, but while on the go, they will connect to either Wi-Fi hotspots (if available) or the cell data network to ensure calls connect. Using a softclient on a mobile device gives employees all the advanced features and the freedom of making and receiving calls anywhere.

Using FortiFone Softclients for Desktops

The desktop softclient runs on Windows and macOS, providing all of the same functionality as using the mobile softclient. It allows an employee to easily use the same extension to make and answer calls or join a conference directly from a computer or laptop. It is also a fit for home offices, allowing users to connect to their offices virtually when they don't have the ability to plug in a physical phone. Using a softclient for desktop is ideal for any user who needs the flexibility to be connected in the office, at home, or while on the road.

Determining the right type of options for a remote workforce can sometimes be challenging, as every employee's function and needs are different. The key is to determine each remote user's requirements that are also supported by the company's secure infrastructure.

	Pros	Cons
Remote extension	■ easy to set up, only requiring physical phone number to be entered into system ■ no changes to network required ■ no licenses required	■ no appearances ■ no call control (transfer, conference) ■ voicemail requires calling into the system
External extension	■ no licenses required ■ same user experience as internal extension	■ first time set-up requires inputting of external IP address to pull configuration ■ third-party firewalls can cause issues
Mobile softclient	■ simple auto provision (scan QR code) ■ full features and call control ■ visual voicemail ■ click to call visual call logs	■ firewall configuration required ■ license required
Desktop softclient	■ full features and call control ■ visual voicemail ■ click to call visual call logs	■ firewall configuration required ■ license required

How to Deploy FortiVoice Secure Communications

Depending upon how network infrastructure is set up and what tools and hardware are needed to support teleworkers, administrators can utilize virtual private networks (VPNs) for devices to connect to FortiVoice, or they can allow external access from over the internet. The choice of solution varies depending upon the equipment put in place and the availability of configuration.

VPNs

VPNs provide a secure connection between locations, and provide many benefits for remote workers, including the following:

- All traffic is encrypted
- Easy for desktop applications, as FortiClient can be used
- Extensions are configured as internal on FortiVoice (no configuration changes required on the PBX)
- No ports are open in the firewall, therefore ensuring no unwanted access to the network

This solution provides an easy, secure connection, from which administrators can monitor and easily troubleshoot issues. However, if using an external IP phone, a FortiGate or VPN-capable equipment will be required at the remote location, which may not be available to users in all situations.

External Access

External access requires network administrators to open ports in the firewall and allow traffic into the internal network. In many situations this can be easier to deploy than a VPN and provide a number of benefits:

- Easily support any home user or mobile user
- Does not require firewall configuration or setup at remote locations
- Can share policies with Voice-over-IP (VoIP) trunks

FortiClient provides advanced endpoint protection, including secure remote access with built-in VPN, single sign-on, and two-factor authentication for added security.

FortiGate, the next-generation firewall, safeguards network access by providing organizations with advanced intrusion prevention, automated threat protection, and a single panel of visibility across the network.

When using external access, security can be a major challenge for some users. Signalling communication and audio encryption are equally important. FortiVoice supports SIP over TLS for the signalling as well as Secure RTP for encryption of audio, which can be easily enabled on the phone profiles.

Best Practices to Protect Business Communications

While many systems sit behind a firewall, unsolicited traffic can still make it into the network. In order to protect your system, it is best to restrict access as much as possible. This can involve using VPNs for external access or restricting inbound traffic to define IPs or geographical regions, if possible. It is also strongly recommended to use nonstandard ports for any inbound rules that you do require being open.

Best Practice #1: Securing Your Phone System

- Implementing password policies for voicemail and web access for administrators and users to ensure changing of default and simple passwords to more secure passwords
- Changing the default signaling ports to nonstandard ports, including HTTPS ports, when allowing remote access
- Disabling TFTP access or remote voicemail access on systems not required

Best Practice #2: Using FortiFone Mobile Softclient

- Utilizing FortiGate SIP ALG to control access and use nonstandard port to avoid traffic
- Enabling SIP over TLS and using SRTP encryption for secure communications between FortiFone softclient and FortiVoice

To learn more about Best Practices with Fortinet Unified Communications, visit FortiVoice Cookbook.

[1] "Gartner CFO Survey Reveals 74% Intend to Shift Some Employees to Remote Work Permanently," Gartner, April 3, 2020.

[2] "Remote Work Is the Future—But Is Your Organization Ready for It?" OpenVPN, accessed May 20, 2020.

May 21, 2020 1:14 PM

669643-0-0-EN

D:\Fortinet\Work\2020\May\052120\wp-remote-working