FORTINET

WHITE PAPER

El trabajo remoto es la próxima normalidad

Cómo mantenerse seguro y eficiente con el uso de las comunicaciones unificadas de FortiVoice

Introducción

El coronavirus ha obligado a millones de empleados corporativos y gubernamentales a trabajar desde casa, desafiando a muchas empresas que no planificaron de manera efectiva una fuerza laboral mayormente remota. Para mantener la productividad, las empresas no solo necesitan una rápida adopción de herramientas de comunicación para garantizar la continuidad del negocio, sino que también deben ayudar a los empleados remotos a entender la nueva forma de trabajar, de manera segura.

Es probable que el 41 % de los empleados trabaje de forma remota incluso después de la pandemia, en comparación con el 30 % antes de la pandemia.[1]

El 90 % de los profesionales de TI considera que los trabajadores remotos representan un riesgo de seguridad en general y más del 54 % piensa que el personal remoto representa un riesgo mayor que los empleados en el sitio.[2]

Adaptarse al trabajo remoto seguro

Trabajar de forma remota fue aceptado en muchas organizaciones, sin embargo, el COVID-19 forzó a la mayoría de las empresas a situaciones en las que la mayoría o todos los empleados están a distancia. Incluso cuando se levante la orden de encierro debido a la pandemia, el cambio general hacia el trabajo remoto no parece que vaya a revertirse en el largo plazo. Una encuesta reciente de Gartner encontró que el 74 % de los directores financieros (CFO) ya informaron que tienen la intención de hacer que el cambio al trabajo remoto para algunos empleados sea permanente. Todas las organizaciones deben adaptar su infraestructura e invertir en la mejor tecnología de comunicaciones que sea confiable, flexible y segura, independientemente de si los empleados trabajan de forma remota o en las oficinas.

Riesgos de ciberseguridad para trabajadores remotos

Tener un número considerable de empleados que trabajan de forma remota puede ser un cambio importante para las organizaciones y presenta varios desafíos de ciberseguridad. La popularidad de los empleados que utilizan sus propios dispositivos para trabajar y la disponibilidad de acceso no seguro a la red también aumentan el riesgo de ataques de tipo suplantación de identidad y malware. La mayoría de las violaciones de seguridad se pueden atribuir a errores humanos y, en un entorno remoto, las organizaciones se encuentran sin duda más propensas a los errores de los usuarios y es más probable que experimenten violaciones de seguridad. Las organizaciones necesitan una solución de comunicación segura y confiable que sea fácil de utilizar y eficaz para la colaboración de los empleados.

Comunicaciones unificadas de Fortinet para trabajadores remotos

La plataforma de comunicaciones unificadas FortiVoice de Fortinet ofrece comunicaciones seguras e integrales que incluyen soporte de voz, conferencias, fax y movilidad, lo que permite a las organizaciones comunicarse y colaborar de forma fácil y segura. Su portal intuitivo basado en la web simplifica la administración de preferencias y del enrutamiento de las llamadas. El software para los dispositivos móviles y fijos (softclient) ayuda a preservar la productividad de los empleados al trabajar de forma remota.

Casos de uso para trabajadores remotos

Incluso antes de que el COVID-19 afectara a muchas organizaciones, el lugar de trabajo evolucionó significativamente durante la última década y los empleados ya no tienen que estar atados a sus escritorios de oficina. La solución de comunicaciones unificadas de Fortinet se diseñó para una gran variedad de casos de uso que permiten a los empleados de empresas de todos los tamaños ser productivos y colaborativos, ya sea en sus oficinas o mediante el trabajo remoto.

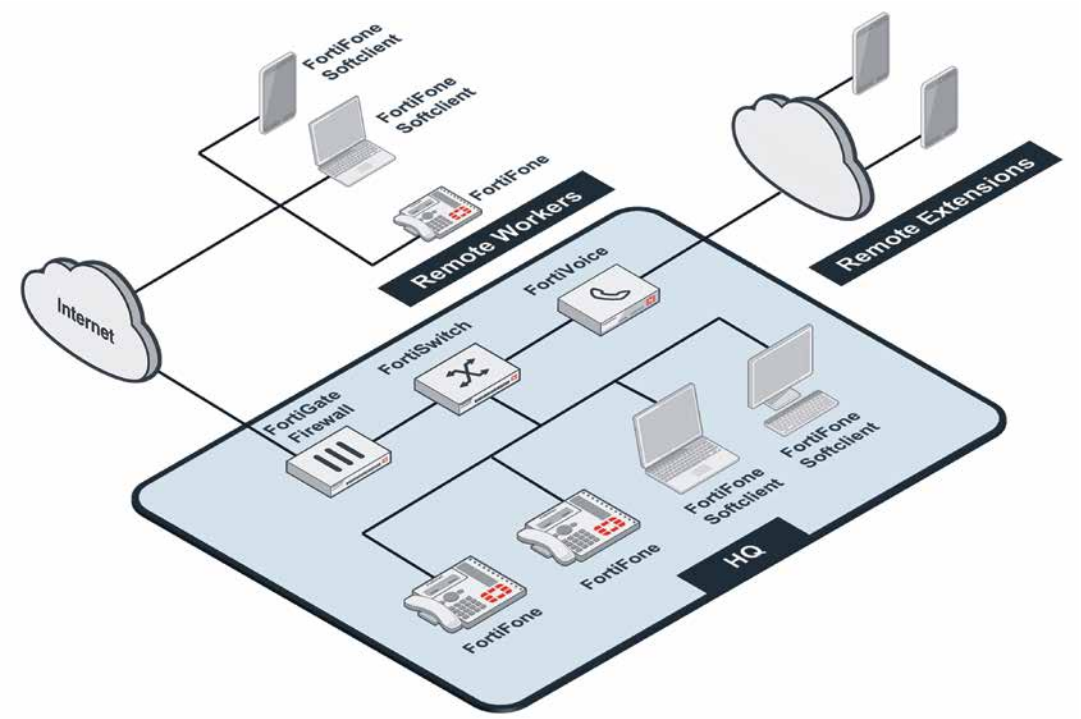

Figura 1: FortiVoice ofrece una serie de soluciones para permanecer conectado de forma segura mientras se está trabajando de forma remota: Mobile Softclient, Desktop Softclient, extensiones externas y extensiones remotas.

Uso de extensiones remotas con dispositivos personales

Una extensión remota es un número físico, ya sea un teléfono celular o fijo, que se puede configurar como una extensión dentro de FortiVoice. Cuando una persona que llama marca un número de extensión de oficina, la llamada se enruta automáticamente a cualquier parte del mundo según la configuración o bien una recepcionista puede transferir fácilmente las llamadas al usuario remoto correspondiente. Estas extensiones remotas son ideales para las personas que están constantemente en movimiento.

Uso de extensiones externas con teléfonos de FortiFone

Una extensión externa es idéntica a una extensión regular, sin embargo, existe fuera de la oficina física. Los empleados pueden llevar sus teléfonos IP de la oficina a casa y conectar los dispositivos en su red doméstica. Estas extensiones tienen las mismas características y funciones, incluidas las teclas de identificación, el aprovisionamiento automático y el control completo de llamadas, tal como en la oficina. Estos tipos de extensiones son las más adecuadas para los empleados que tienen oficinas permanentes en casa.

Uso de FortiFone Softclients para dispositivos móviles

Los clientes de software móviles (mobile softclients) son la solución híbrida perfecta para los usuarios expertos que están constantemente en movimiento y necesitan contar con las mismas características que las extensiones habituales en la oficina. Los mobile softclients se ejecutan en teléfonos Android o iOS y brindan a los usuarios aprovisionamiento automático, correo de voz visual, registros de llamadas para marcar con un clic y control completo de llamadas. Los softclients admiten conexiones de datos móviles y Wi-Fi. Cuando los usuarios están en la oficina, utilizan el Wi-Fi corporativo, pero cuando están en movimiento, se conectarán a puntos de acceso Wi-Fi (si están disponibles) o a la red de datos móviles para garantizar que las llamadas se conecten. El uso de un softclient en un dispositivo móvil brinda a los empleados todas las funciones avanzadas y la libertad de realizar y recibir llamadas en cualquier lugar.

	Ventajas	Desventajas
Extensión remota	■ fácil de configurar, solo requiere ingresar un número de teléfono físico en el sistema ■ no se requieren cambios en la red ■ no se requieren licencias	■ no hay identificación ■ no hay control de llamadas (transferencia, conferencia) ■ el correo de voz requiere llamar al sistema
Extensión externa	■ no se requieren licencias ■ la misma experiencia de usuario que con la extensión interna	■ la primera configuración requiere el ingreso de una dirección IP externa para extraer la configuración ■ los firewalls de terceros pueden causar problemas
Mobile Softclient	■ aprovisionamiento automático simple (escaneo de código QR) ■ funciones completas y control de llamadas ■ correo de voz visual ■ clic para marcar los registros de llamadas visuales	■ se requiere configuración de firewall ■ se requiere licencia
Desktop Softclient	■ funciones completas y control de llamadas ■ correo de voz visual ■ clic para marcar los registros visuales de llamadas	■ se requiere configuración de firewall ■ se requiere licencia

Uso de FortiFone Softclients para dispositivos fijos

El cliente de software para computadoras de escritorio (desktop softclient) se ejecuta en Windows y macOS y brinda las mismas funciones que cuando se utiliza el mobile softclient. Permite a un empleado utilizar fácilmente la misma extensión para hacer y contestar llamadas o unirse a una conferencia directamente desde una computadora o laptop. También es adecuado para oficinas en casa, ya que permite a los usuarios conectarse virtualmente a sus oficinas cuando no tienen la capacidad de conectar un teléfono físico. El uso de un softclient para dispositivos fijos es ideal para cualquier usuario que necesite la flexibilidad de estar conectado en la oficina, en casa o mientras viaja en carretera.

Determinar el tipo correcto de opciones para una fuerza laboral remota algunas veces puede ser desafiante, ya que la función y las requerimientos de cada empleado son diferentes. La clave es determinar los requerimientos de cada usuario remoto que también sean compatibles con la infraestructura de seguridad de la empresa.

Cómo implementar las comunicaciones seguras de FortiVoice

Dependiendo de la configuración de la infraestructura de red y de las herramientas y el hardware necesarios para apoyar a los trabajadores remotos, los administradores pueden utilizar redes privadas virtuales (VPN) para que los dispositivos se conecten a FortiVoice o pueden permitir el acceso externo desde Internet. La elección de la solución varía dependiendo del equipo instalado y la disponibilidad de configuraciones.

VPNs

Las VPNs proporcionan una conexión segura entre ubicaciones y ofrecen muchos beneficios para los trabajadores remotos, que incluyen los siguientes:

- Todo el tráfico es cifrado
- Facilidad para usar aplicaciones de dispositivos fijos debido a que se puede utilizar FortiClient
- Las extensiones se configuran como internas en FortiVoice (no se requieren cambios de configuración en el PBX)
- No hay puertos abiertos en el firewall, lo que garantiza que no haya acceso no deseado a la red

FortiClient cuenta con protección avanzada para endpoints, que incluye acceso remoto seguro con VPN incorporada, inicio de sesión único y autenticación de dos factores para mayor seguridad.

FortiGate, el firewall de siguiente generación, protege el acceso a la red al ofrecer a las organizaciones prevención avanzada de intrusiones, protección automatizada contra amenazas y un solo panel de visibilidad de toda la red.

Esta solución proporciona una conexión fácil y segura, desde la cual los administradores pueden monitorear y solucionar problemas fácilmente. Sin embargo, si utiliza un teléfono IP externo, necesitará un equipo compatible con FortiGate o VPN en la ubicación remota, el cual puede no estar disponible para los usuarios en todas las situaciones.

Acceso externo

El acceso externo requiere que los administradores de red abran puertos en el firewall y permitan el tráfico en la red interna. En muchas situaciones, esto puede ser más fácil de implementar que una VPN con varios beneficios:

- Admitir fácilmente a cualquier usuario doméstico o móvil
- No se necesita la configuración ni la instalación de un firewall en las ubicaciones remotas
- Se pueden compartir políticas con troncales de Voz sobre IP (VoIP)

Al utilizar el acceso externo, la seguridad puede ser un gran desafío para algunos usuarios. El cifrado del audio y la comunicación de la señalización son igualmente importantes. FortiVoice admite SIP sobre TLS para la señalización, así como RTP seguro para el cifrado de audio, que se puede habilitar con facilidad en los perfiles del teléfono.

Mejores prácticas para proteger las comunicaciones de la empresa

Si bien muchos sistemas se encuentran detrás de un firewall, el tráfico no solicitado aún puede ingresar a la red. Para proteger su sistema, es mejor restringir el acceso tanto como sea posible. Esto puede implicar el uso de una VPN para acceso externo o restringir el tráfico entrante para definir IPs o regiones geográficas, si es posible. También se recomienda encarecidamente utilizar puertos no estándar para cualquier regla de entrada que necesite estar abierta.

Mejor práctica #1: protección de su sistema telefónico

- Implementar políticas de contraseñas para el correo de voz y el acceso a la web para administradores y usuarios con el fin de garantizar el cambio de contraseñas predeterminadas y simples a contraseñas más seguras
- Cambiar los puertos de señalización predeterminados a puertos no estándar, incluidos los puertos HTTPS, cuando se permita el acceso remoto
- No es necesario deshabilitar el acceso TFTP ni el acceso al correo de voz remoto en los sistemas

Mejor práctica #2: uso de FortiFone Mobile Softclient

- Utilizar FortiGate SIP ALG para controlar el acceso y usar un puerto no estándar para evitar el tráfico
- Habilitar SIP sobre TLS y utilizar el cifrado SRTP para comunicaciones seguras entre FortiFone Softclient y FortiVoice

Para obtener más información sobre las mejores prácticas para las comunicaciones unificadas de Fortinet, visite FortiVoice Cookbook.

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

[2] "Remote Work Is the Future—But Is Your Organization Ready for It?", OpenVPN, consultado el 20 de mayo de 2020.

enero 22, 2021 2:51 p. m.

669643-0-0-ES

wp-remote-working_ES