SOLUTION BRIEF

Acceso remoto seguro para su fuerza laboral a escala

Resumen Ejecutivo

Las organizaciones se enfrentan a diferentes situaciones potenciales de emergencia como epidemias, inundaciones, huracanes y cortes de energía. La implementación de un plan de continuidad comercial es esencial para garantizar que la organización sea capaz de mantener la operación ante la adversidad y prepararse para posibles desastres.

Una consideración importante para las organizaciones que desarrollan un plan de continuidad comercial es que la organización puede no ser capaz de mantener las operaciones normales en el sitio. La capacidad de apoyar a los empleados que trabajan de forma remota es esencial para garantizar tanto la continuidad del negocio como la seguridad. Las soluciones de Fortinet ofrecen una solución integrada para soportar el teletrabajo. Los firewalls de próxima generación (NGFW) FortiGate tienen soporte integrado para redes privadas virtuales (VPN) IPsec, lo que permite a los trabajadores remotos conectarse de forma segura a la red de la empresa. Con la protección de punto final, proporcionada por FortiClient, y la autenticación multifactor (MFA) con FortiAuthenticator, las organizaciones pueden soportar de forma segura el trabajo remoto y mantener la continuidad del negocio.

La capacidad de respaldar de manera segura a una fuerza de trabajo remota es un componente esencial del plan de continuidad del negocio y recuperación ante desastres de cualquier organización. Una organización puede ser incapaz de mantener las operaciones normales en el sitio, debido a un corte de energía o un evento similar, o una epidemia o inundación puede hacer que sea peligroso para los empleados viajar a las oficinas.

En estos escenarios, una organización debe ser capaz de soportar conectividad remota segura a la red corporativa. Para más de 400.000 clientes de Fortinet, su tecnología ya implementada contiene esta funcionalidad. Los FortiGate NGFW tienen soporte integrado para VPN IPsec, lo que permite una conectividad segura para los empleados que trabajan desde sitios de trabajo alternativos.

El trabajo remoto disminuye el tiempo improductivo de los empleados en un promedio del 27%.[1]

Los empleados remotos trabajan un promedio de 16,8 días más por año que los empleados en el sitio.[2]

El 85% de los empleados afirman que alcanzan la máxima productividad cuando trabajan de forma remota.[3]

Permitir el trabajo remoto aumentó la retención de empleados en el 95% de las organizaciones.[4]

Asegurando la fuerza de trabajo remota con FortiGate NGFWs

Las VPN IPsec y SSL integradas en cada FortiGate NGFW ofrecen un modelo de implementación extremadamente flexible. Los trabajadores remotos pueden aprovechar una experiencia sin determinar el cliente u obtener acceso a funciones adicionales a través de un cliente robusto integrado en la solución de seguridad de punto final FortiClient. Los usuarios avanzados y los superusuarios se beneficiarían de implementar un FortiAP o un FortiGate NGFW para obtener capacidades adicionales.

Las soluciones de Fortinet están diseñadas para ser fáciles de usar desde la compra inicial hasta el final de la vida útil. Los FortiGate NGFW y los puntos de acceso inalámbrico FortiAP incluyen la funcionalidad de implementación sin contacto. Los dispositivos desplegados en sitios remotos se pueden configurar previamente antes de su envío, lo que permite la configuración automática en el sitio, lo que garantiza la continuidad del negocio y el soporte para el teletrabajo.

El Fortinet Security Fabric aprovecha el sistema operativo Fortinet común y un entorno abierto de interfaz de programación de aplicaciones (API) para crear una arquitectura de seguridad amplia, integrada y automatizada. Con el Fortinet Security Fabric, todos los dispositivos de una organización, incluidos los implementados de forma remota para admitir el teletrabajo, se pueden monitorear y administrar desde un solo panel de control. Desde un FortiGate NGFW o una plataforma de administración centralizada FortiManager implementada en el entorno de la sede, el equipo de seguridad puede lograr una visibilidad completa de todos los dispositivos conectados, independientemente de su situación de implementación.

En el caso de un desastre natural u otro evento que interrumpa las operaciones comerciales normales, una organización debe ser capaz de hacer una transición rápida a una fuerza laboral totalmente remota. La Tabla 1 muestra el número de usuarios de VPN concurrentes que cada modelo de FortiGate NGFW puede admitir.

Más allá de ofrecer cifrado de datos en tránsito, a través de una VPN, las soluciones de Fortinet ofrecen una serie de otras características que pueden ayudar a una organización a proteger su fuerza de trabajo remota. Estas características incluyen:

- **Autenticación multifactor.** FortiToken y FortiAuthenticator permiten la autenticación de doble factor de empleados remotos.
- **Prevención de pérdida de datos (DLP).** FortiGate y FortiWiFi proporcionan funcionalidad DLP para trabajadores remotos, que es esencial para los ejecutivos de teletrabajo con acceso frecuente a datos confidenciales de la empresa.
- **Protección avanzada ante amenazas.** FortiSandbox ofrece análisis de malware y otro contenido sospechoso dentro de un entorno de espacio aislado antes de que llegue a su destino.
- **Conectividad inalámbrica.** Los FortiAP proporcionan acceso inalámbrico seguro en ubicaciones de trabajo remotas con integración total y administración de la configuración en un solo panel de control.
- **Telefonía.** FortiFone es una solución de telefonía segura de voz sobre IP (VoIP), cuyo tráfico está protegido, administrado y monitoreado por un FortiGate NGFW. Disponible en formato soft client y varias opciones de hardware.

Modelo	Usuarios de SSL VPN concurrentes	Usuarios de IPsec VPN concurrentes	FortiAPs administrados (Modo Túnel)
100E	500	10,000	32
100F	500	16,000	64
300E	5,000	50,000	256
500E	10,000	50,000	256
600E	10,000	50,000	512
1100E	10,000	100,000	2,048
2000E	30,000	100,000	2,048
All Larger Models*	30,000	100,000	2,048
*3300E supports 1,024 Tunnel Mode APs			

Tabla 1: Número de conexiones VPN concurrentes compatibles con varios modelos de FortiGate NGFW

Casos de uso para las soluciones de Fortinet que soportan trabajo remoto

No todos los empleados de una organización requieren el mismo nivel de acceso a los recursos de la empresa cuando trabajan de forma remota. Fortinet ofrece soluciones de teletrabajo a medida para cada trabajador remoto:

1. Teletrabajador básico. El teletrabajador básico solo requiere acceso a correo electrónico, internet, teleconferencia, intercambio limitado de archivos y capacidades específicas de funciones (finanzas, recursos humanos, etc.) desde su sitio de trabajo remoto. Esto incluye el acceso a aplicaciones de software como servicio (SaaS) en la nube, como Microsoft Office 365, así como una conexión segura a la red corporativa.

Los teletrabajadores básicos pueden conectarse a la organización utilizando el software de cliente VPN integrado FortiClient y verificar su identidad con FortiToken para la autenticación multifactor. Tenga en cuenta que los usuarios avanzados y los superusuarios volverían al perfil básico de teletrabajador cuando se movilicen desde su ubicación de trabajo remota.

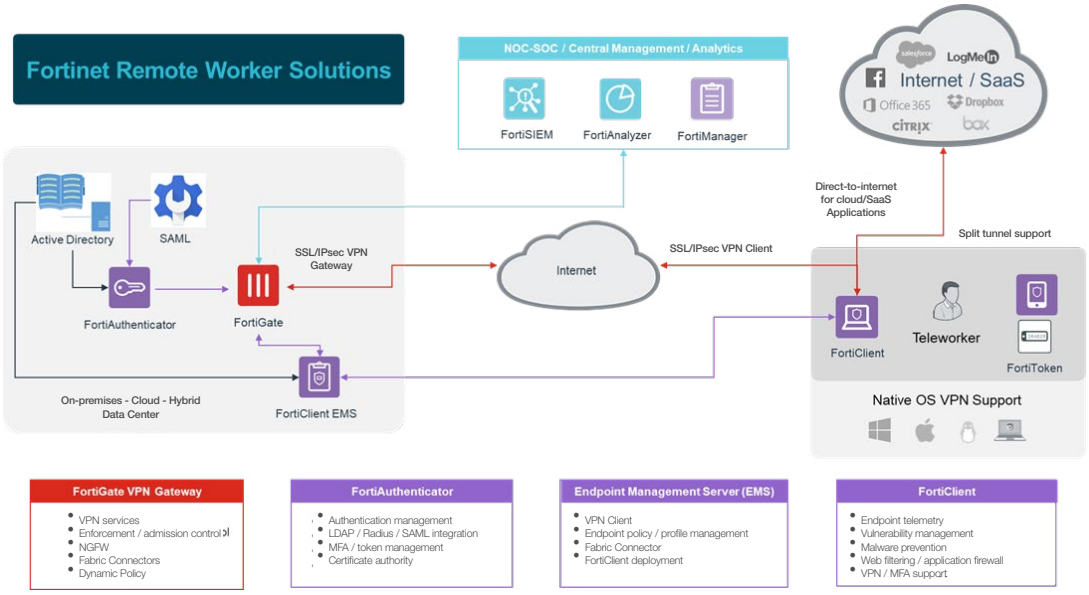

Figure 1: Notional Fortinet solution deployment for basic teleworker.

2. Usuario avanzado. Los usuarios avanzados son empleados que requieren un mayor nivel de acceso a los recursos corporativos mientras trabajan desde una ubicación remota. Esto puede incluir la capacidad de operar en entornos de TI múltiples y paralelos e incluye empleados como administradores de sistemas, técnicos de soporte de TI y personal de emergencia.

Para estos usuarios avanzados, la implementación de un punto de acceso FortiAP en su sitio de trabajo alternativo proporciona el nivel de acceso y seguridad que requieren. Esto permite una conectividad inalámbrica segura con un túnel seguro a la red corporativa. Los FortiAP se pueden implementar con aprovisionamiento sin contacto (ZTP) y serán administrados por los FortiGate NGFW en la oficina. Si un teléfono corporativo necesita ser implementado, simplemente puede conectarse al FortiAP para la conectividad de regreso a la oficina principal.

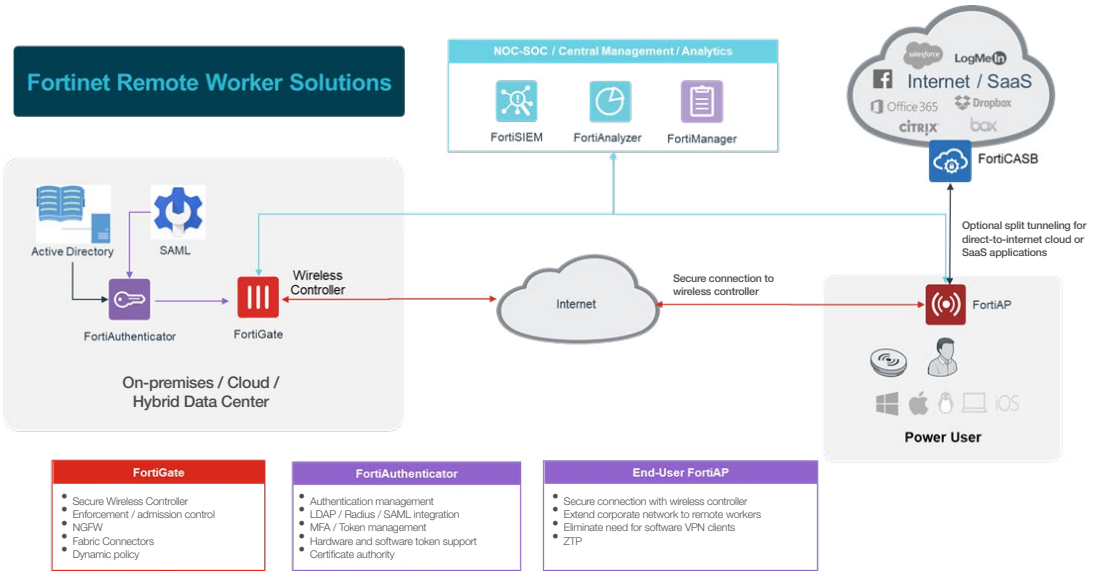

Figure 2: Notional Fortinet solution deployment for power user.

3. Súper usuario. Un súper usuario es un empleado que requiere acceso avanzado a recursos corporativos confidenciales, incluso cuando trabaja desde una oficina alternativa. Con frecuencia procesan información extremadamente sensible y confidencial. Este perfil de empleado incluye administradores con acceso privilegiado al sistema, técnicos de soporte, socios clave alineados con el plan de continuidad, personal de emergencia y gestión ejecutiva.

Para estos súper usuarios, su sitio de trabajo alternativo debe configurarse como una ubicación de oficina alternativa. Si bien requieren las mismas soluciones que los teletrabajadores básicos y los usuarios avanzados, también requieren una funcionalidad adicional. FortiAP se puede integrar con un dispositivo FortiGate NGFW o FortiWiFi para una conectividad inalámbrica segura con DLP incorporado. FortiFone proporciona versiones de hardware o soft client de VoIP de telefonía que se administra y protege a través del FortiGate NGFW in situ o una plataforma de administración centralizada FortiManager implementada en la ubicación de la sede.

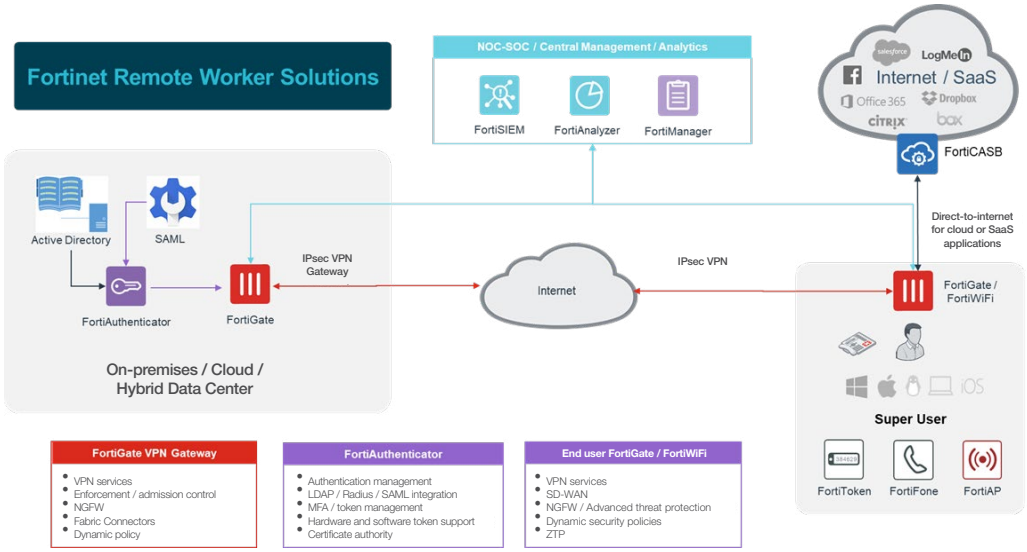

Figure 3: Notional Fortinet solution deployment for super user.

Asegurando una fuerza laboral remota

Las soluciones de Fortinet se implementan fácilmente en ubicaciones de trabajo remotas. Sin embargo, una organización también requiere recursos en sitio o en la nube para apoyar de forma segura a los teletrabajadores o fuerza laboral remota.

Muchas organizaciones ya cuentan con estos recursos, ya que son parte de su arquitectura de seguridad existente. Un FortiGate NGFW proporciona un NGFW capaz de inspeccionar el tráfico cifrado y de texto sin formato a escala empresarial con un impacto mínimo en el rendimiento. Sin embargo, también incluye una puerta de enlace VPN integrada que actúa como un punto final para las conexiones encriptadas a los teletrabajadores.

FortiGate NGFW también incluye integración con infraestructura de TI común, incluidos servicios como Microsoft Active Directory (AD), MFA y single sing-on (SSO). FortiAuthenticator proporciona un único punto de integración centralizado para soluciones de autenticación y admite soluciones de terceros, así como FortiToken, que ofrece opciones de token de hardware, software, correo electrónico y dispositivos móviles.

Al administrar una fuerza de trabajo remota y distribuida, la visibilidad y administración de seguridad centralizada son esenciales. Todas las soluciones de Fortinet pueden integrarse a través del Fortinet Security Fabric. Esto permite que el equipo de seguridad de la organización logre visibilidad en un panel de gestión único y controle con FortiManager, realice la agregación de registros y análisis de seguridad con FortiAnalyzer, detecte y responda rápidamente a posibles amenazas usando FortiSIEM.

Logre la integración de seguridad completa con las soluciones de Fortinet

El Fortinet Security Fabric permite una integración perfecta de la fuerza de trabajo remota de una organización. Todas las soluciones de Fortinet están conectadas a través del Fortinet Security Fabric, que permite la visibilidad, configuración y monitoreo en un panel único de gestión. Una serie de conectores entrelazados, un entorno API abierto, el soporte de la comunidad DevOps y un gran ecosistema extendido de Security Fabric permiten la integración con más de 250 soluciones de terceros.

Esto es esencial cuando una organización está preparando un plan de continuidad comercial, ya que la empresa puede verse obligada a realizar una transición de la fuerza laboral a modo remoto con poco o ningún aviso. La visibilidad y gestión del panel único de gestión de la arquitectura de seguridad de una organización garantiza ese soporte para el teletrabajo y no pone en peligro la ciberseguridad de una organización.

Las siguientes soluciones son parte del Fortinet Security Fabric y admiten teletrabajo seguro:

- **FortiClient.** FortiClient fortalece la seguridad de los puntos finales a través de la visibilidad integrada, el control y la defensa proactiva, permite a las organizaciones descubrir, monitorear y evaluar los riesgos finales en tiempo real.
- **FortiGate.** FortiGate NGFW utiliza procesadores de ciberseguridad especialmente diseñados para brindar protección de primer nivel, visibilidad de extremo a extremo y control centralizado, así como inspección de alto rendimiento de clear-texted y del tráfico encriptado.
- **FortiWiFi.** Las puertas de enlace inalámbricas FortiWiFi combinan los beneficios de seguridad del FortiGate NGFW con un punto de acceso inalámbrico, proporcionando una solución integrada de red y seguridad para los teletrabajadores.
- **FortiFone.** FortiFone proporciona comunicaciones de voz unificadas con conectividad VoIP que se asegura y administra a través del FortiGate NGFWs. La interfaz de FortiFone soft client permite a los usuarios hacer o recibir llamadas, acceder al correo de voz, verificar el historial de llamadas y buscar en el directorio de la organización directamente desde un dispositivo móvil. Múltiples opciones de hardware están disponibles para esta solución.
- **FortiToken.** FortiToken confirma la identidad de los usuarios al agregar un segundo factor al proceso de autenticación a través de tokens basados en aplicaciones móviles.
- **FortiAuthenticator.** FortiAuthenticator proporciona servicios de autenticación centralizados que incluyen servicios SSO, gestión de certificados, y gestión de invitados.
- **FortiAP.** FortiAP ofrece acceso inalámbrico seguro a empresas distribuidas y trabajadores remotos y se puede administrar fácilmente desde un FortiGate NGFW o a través de la nube.
- **FortiManager.** FortiManager proporciona administración de un panel único de gestión y controles de políticas en toda la empresa extendida para obtener información en toda la red, amenazas basadas en el tráfico. Esto incluye características para contener ataques avanzados, así como escalabilidad para administrar hasta 10.000 dispositivos Fortinet.
- **FortiAnalyzer.** FortiAnalyzer proporciona seguridad cibernética basada en análisis y gestión de registros para permitir una mejor detección de amenazas y prevención de brechas.
- **FortiSandbox.** Las soluciones de sandbox de Fortinet ofrecen una poderosa combinación de detección avanzada de amenazas, mitigación automatizada, conocimiento accionable y despliegue flexible para detener ataques dirigidos y la pérdida de datos posterior. Disponible como un servicio en la nube que se incluye en la mayoría de las suscripciones FortiGuard.

Una base segura garantiza la continuidad del negocio

Prepararse para la continuidad del negocio y la recuperación ante desastres es vital para cualquier organización. Un componente importante de esto es la capacidad de apoyar una fuerza laboral mayoritaria o totalmente remota con poco o ningún aviso.

Al desarrollar planes de continuidad comercial, es esencial asegurarse de que la organización cuente con los recursos para que la fuerza laboral remota trabaje de forma segura. Las soluciones de Fortinet son fáciles de implementar, configurar y permiten a una organización mantener la seguridad, visibilidad y completo control independientemente de su entorno de implementación.

1 "The Benefits of Working From Home," Airtasker, September 9, 2019.

2 Ibid.

3 Abdullahi Muhammed, "Here's Why Remote Workers Are More Productive Than In-House Teams," Forbes, May 21, 2019.

4 Ibid.