#ACCEDE

2.

GLOBAL PROTECT

La solución de seguridad de red para endpoints permite proteger a los trabajadores itinerantes con independencia de su ubicación. La seguridad del tráfico se garantiza gracias a la capacidad de la plataforma para entender el uso de las aplicaciones, vincular el tráfico a usuarios y dispositivos concretos, y aplicar las políticas de seguridad con ayuda de tecnologías de nueva generación.

Desde el momento que la aplicación está instalada, todos los dispositivos establecen automáticamente una conexión VPN IPsec/SSL al firewall mediante la mejor puerta de enlace disponible, otorgando a la organización de una visibilidad total del tráfico, aplicaciones, puertos y protocolos de red. Sin ángulos muertos en el tráfico de los trabajadores itinerantes, la organización disfruta de total visibilidad para conocer el uso de las aplicaciones.

Global Protect permite segmentar la red y regular el acceso a los recursos internos gracias a su capacidad de identificación de usuarios de una forma rápida y fiable, permitiendo establecer políticas personalizadas que restrinjan el acceso en función del perfil de usuario. Asimismo, recopila información sobre los hosts para determinar si los dispositivos cumplen los requisitos establecidos en las políticas de seguridad. Todos estos mecanismos permiten tomar medidas preventivas para proteger sus redes internas, adoptar controles de red Zero Trust y reducir el riesgo de ataque.

CARACTERÍSTICAS

- **Acceso remoto mediante VPN:**
  - Acceso seguro a las aplicaciones empresariales, internas o en Cloud.

- **Prevención de amenazas avanzadas:**
  - Garantiza la seguridad del tráfico de internet.
  - Impide que las amenazas alcancen el endpoint.
  - Defensa contra ataques de phishing y del robo de credenciales.

- **Filtrado de URL:**
  - Aplica las políticas de uso aceptable.
  - Filtra el acceso a dominios maliciosos y a contenido para adultos.
  - Impide el uso de herramientas de evitación y evasión.
  - Protege el acceso a aplicaciones SaaS.
  - Controla el acceso a las aplicaciones SaaS y aplica las políticas pertinentes bloqueando las App no autorizadas.

- **Dispositivos personales (BYOD):**
  - Permite implementar y utilizar redes VPN para preservar la privacidad.
  - Ofrece acceso seguro sin cliente a colaboradores, socios y contratistas.
  - Permite identificar automáticamente los dispositivos no gestionados.
  - Mecanismos de autenticación personalizados para dispositivos gestionados y no gestionados.

- **Implementación Zero Trust (confianza cero):**
  - Proporciona un sistema de identificación de usuarios fiable.
  - Información inmediata sobre los hosts para mejorar la visibilidad y aplicar las políticas.
  - Autenticación multifactor incremental para acceder a recursos confidenciales.