Red Privada Virtual (VPN-SSL)

Descripción

El servicio de Red Privada Virtual (*Virtual Private Network*) permite integrar un dispositivo externo (PC/portátil de casa, Tablet o Smartphone) en la Red Informática cableada de la Universidad de Jaén (RIUJA), posibilitando el acceso a recursos y servicios que sólo están disponibles a los equipos internos.

Esquema VPNSSL

El sistema establece una conexión segura específica (túnel virtual) entre su equipo y un servidor o sistema situado en la Universidad de Jaén. Una vez establecida la conexión VPN-SSL, todo el tráfico de red destinado a las redes internas de la UJA se encaminará a través del túnel. El resto del tráfico será encaminado a través de su conexión habitual a Internet (generalmente mediante ADSL, fibra óptica o similar).

IMPORTANTE: El servicio VPN-SSL se limita a integrar el ordenador del usuario (por ejemplo: ordenador de casa) en RIUJA y no realiza ninguna configuración para el acceso a los servicios anteriormente indicados. La configuración correcta de estos servicios es responsabilidad del usuario. Asimismo, la conexión VPN-SSL no permite directamente la conexión a su equipo de la UJA. Previamente es necesario configurar la conexión mediante Escritorio Remoto de Windows (RDP).

Conexión VPN

- Abrir conexión VPN (https://vpnssl.ujaen.es)
- Servicio de Conexión VPNSSL (Guía de usuario)
- Activación del segundo factor de autenticación (2FA) en VPN-SSL (obligatorio desde el 12 de julio de 2023)
- VPN-SSL: Preguntas frecuentes (FAQ) y resolución de problemas
- Conexión mediante Escritorio Remoto (RDP) al ordenador Windows del despacho
- Conexión mediante VNC al ordenador Mac del despacho

Solicitantes

Este servicio está destinado al PTGAS/PDI de la Universidad de Jaén.

Está activado para todo PTGAS/PDI que disponga de una cuenta TIC. No requiere solicitud de alta.

Para poder usar este servicio son necesarios los siguientes requisitos:

- Un dispositivo (PC, portátil, Tablet, Smartphone) con conexión a Internet. Están soportados equipos de sobremesa/portátiles con Windows, MacOS o Linux. También plataformas móviles (Tablets y Smartphones) con Apple iOS y Android.
- Una cuenta TIC con doble factor de autenticación activado.
- Un navegador web estándar en equipos de sobremesa/portátiles. Se han realizado pruebas satisfactorias con los siguientes navegadores: Internet Explorer, Microsoft Edge, Mozilla Firefox, Google Chrome, Safari y Opera. Para la conexión con un navegador web, necesitará instalar un complemento o plugin. El proceso de instalación del complemento suele ser bastante sencillo, pero si tiene algún problema puede

consultar las soluciones a los problemas más frecuentes.
- Un cliente específico en plataformas o dispositivos móviles (Tablets, Smartphones, etc.)
- En sistemas Microsoft Windows es necesario:
    - Tener instalado algún antivirus estándar. La plataforma de conexión VPN-SSL soporta un gran número de antivirus gratuitos y de pago que existen en el mercado.
    - Tener configurado el protector de pantalla con un tiempo menor de 15 minutos y protegido por contraseña.

IMPORTANTE: Conexión VPN-SSL desde el extranjero

Debido a las últimas tendencias en ciberataques que están usando las conexiones VPN como vía de acceso, por seguridad se ha limitado el acceso VPN-SSL únicamente a España y ciertos países puntuales solicitados a demanda por algunos de nuestros usuarios.

Si estás en el extranjero o tienes previsto viajar fuera de España y necesitas el acceso VPN-SSL de la UJA, debes comunicarlo previamente al Servicio de Informática para comprobar si tu país de destino está entre los permitidos. En caso contrario, una vez estudiado el caso y si no representa ningún potencial problema de seguridad, procederemos a añadirlo al conjunto de países de origen permitidos.

Demandas

- **Incidencia**: Mal funcionamiento del servicio VPN-SSL o de alguno de los plugins y complementos usados en la conexión.
- **Consulta**: Funcionamiento del servicio VPN-SSL. Estado de la solicitud.
- **Modificación**: Activación/desactivación de servicios especiales.

NOTA: Declinación de responsabilidad en atención de incidencias en ordenadores y dispositivos

Modos de acceso

Los solicitantes podrán comunicar sus peticiones e incidencias al Servicio de Informática por los siguientes medios:

- Plataforma de Autoservicio TIC
- **Contactando con la Oficina de Atención al Usuario**:
    - Teléfono 82000 en horario de 09:00 a 14:00
    - Dependencia D1-8009 en horario de 09:00 a14:00

- La solicitud electrónica se utilizará para comunicar exclusivamente peticiones e incidencias de conexión VPN-SSL. Por favor, no envíe incidencias relacionadas con otras aplicaciones o servicios. Antes de enviar su solicitud consulte el anexo de solicitantes. En él encontrará información sobre quién puede solicitar este servicio.

  Nota: Si la conexión VPN-SSL funciona correctamente y tiene problemas para utilizar otras aplicaciones (por ejemplo: Escritorio Remoto, cliente de correo, etc..) consulte las guías prácticas o o envíe la incidencia correspondiente a través de la Plataforma de Autoservicio TIC.

Servicios y recursos disponibles mediante VPN-SSL

La conexión VPN-SSL ofrece acceso a los siguientes servicios:

- Navegación web HTTP y HTTPS a sitios web dentro y fuera de la UJA.
- Acceso al software Panda Antivirus en la UJA.
- Acceso a determinadas páginas restringidas dentro del sitio web de la UJA (Ej: Servicio de Informática – Oficina de Atención al Usuario).
- Conexión segura a equipos de la Universidad mediante Conexión a Escritorio Remoto de Windows (RDP) y mediante SSH (Secure Shell).
- Acceso a servidores FTP internos y externos a la UJA.
- Universidad Virtual: acceso a opciones restringidas, sólo accesibles desde dentro de la UJA.
- Publicación de páginas web personales en http://www4.ujaen.es.

Este catálogo de servicios puede ser ampliado en un futuro en función de las peticiones y necesidades de los usuarios.