Si bien la modalidad de Teletrabajo ha sido una iniciativa que llevan adoptando algunas empresas en los últimos años como parte de su forma de trabajar, hasta el momento no se ha tratado ni mucho menos de una tendencia generalizada para el grueso de compañías. En 2019 y de acuerdo con la Encuesta de Población Activa (Española), el **7'5% de empleados teletrabajaba alguna vez y sólo el 4'2% lo hacía de forma regular.**

El Problema:

Las empresas están siendo impactadas de forma inesperada por la situación macro actual "COVID-19" y deben cambiar su esquema operativo de manera urgente. Las empresas tienen que realizar estos cambios en el menor tiempo posible para asegurar la continuidad del negocio.

En un contexto en el que la superficie de exposición aumenta, **es imprescindible gestionar el nivel de ciber riesgo de las compañías sin que la implementación del teletrabajo impacte en la seguridad de las mismas.**

"En 2019 y de acuerdo con la Encuesta de Población Activa, el **7'5%** de empleados teletrabajaba alguna vez y sólo el **4'2%** lo hacía de forma regular."

Fuente: Encuesta de población activa 2019, Instituto Nacional de Estadística (INE)

+70% *

Ataques dirigidos en el contexto Covid-19

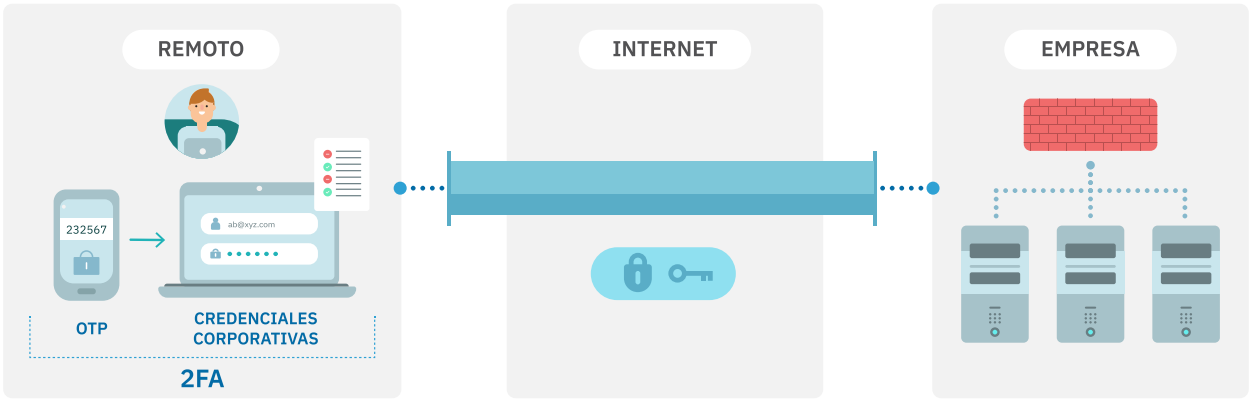
COVIDLOCK **

Ransomware dirigido

*El Centro Criptológico Nacional ha detectado este mes un incremento de un 70% en el llamado phishing

**CNIP...COVIDLOCK es un software malicioso que es considerado especialmente peligroso para las infraestructuras críticas

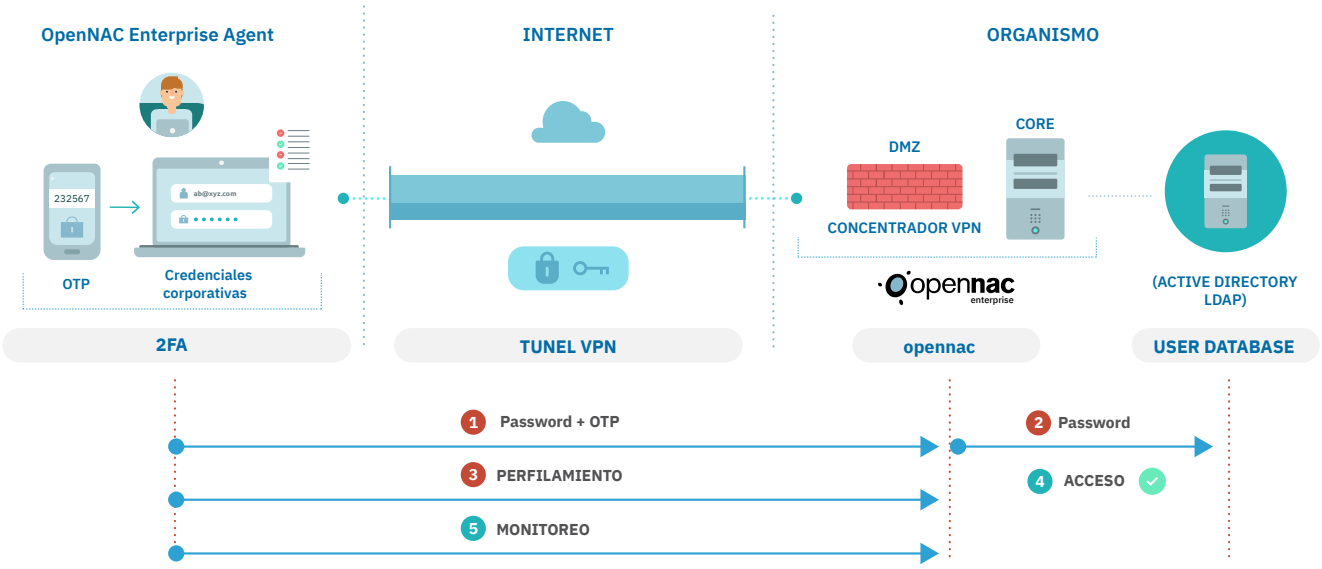
La Solución: **Acceso remoto seguro con doble factor de autenticación.**
2SRA Secure Remote Access



Para el acceso remoto seguro, el módulo de 2SRA actúa como frontend para la finalización de túneles VPN con los clientes, mediante un agente (para dispositivos corporativos y no corporativos). **OpenNAC Enterprise** realiza la autenticación, autorización y auditoría contra el gestor de identidades corporativas del Organismo (Active Directory (AD), LDAP...) y permite añadir un segundo factor de autenticación (OTP), de esta forma mitiga el riesgo de suplantación de identidad (uso de credenciales robados por parte de un atacante para acceder a la red).

Se recoge el inventario y perfilado completo del equipo. Este perfilado se podrá utilizar en las políticas de acceso a la conexión remota. Adicionalmente, permite definir y aplicar políticas de acceso en función de una postura de seguridad, además de otros factores (horario de la conexión, características del equipo, role de usuario etc.). Una conexión segura y verificada de manera robusta entre el usuario y los sistemas corporativos, monitorizando de manera continua el comportamiento de la conexión.

Arquitectura



1. El usuario envía credenciales corporativas y token (OTP) hacia OpenNAC Enterprise para validación de identidad.
2. OpenNAC Enterprise valida token y consulta credenciales corporativas al User Database.
3. El dispositivo de usuario envía su postura a OpenNAC Enterprise para que evalué cumplimiento de requerimientos mínimos de conexión.
4. El usuario obtiene los accesos corporativos asociados a su identidad.
5. Todo el tráfico intercambiado en la conexión VPN será monitorizado por el modulo de 2SRA para apoyar la identificación de anomalías en el comportamiento.

¿Cómo funciona 2SRA Secure Remote Access?

El usuario deberá instalar el agente VPN en el dispositivo que va a utilizar para realizar la conexión. A través de este llevará a cabo el proceso de validación de identidad por medio de uno o dos factores de autenticación. En caso de usar un solo factor de autenticación, utilizará sus credenciales de usuario corporativo (nombre de usuario y clave de AD / LDAP etc.) para iniciar la conexión (algo que sabe). En caso de usar dos factores de autenticación, deberá contar con Google Authenticator en un dispositivo asociado a la persona, y una semilla de token válida que permita garantizar su identidad, (OTP) (algo que tiene). El túnel VPN se establecerá entre el dispositivo de usuario y el módulo de concentración de VPNs de **OpenNAC Enterprise**. Una vez validada la identidad del usuario, el dispositivo de usuario deberá aprobar la evaluación de la postura, es decir, garantizar el cumplimiento de los requerimientos mínimo de conexión. Posteriormente se asignará un segmento de red correspondiente, el segmento asignado heredará los permisos de acceso del usuario asociados a su identidad para mantener el principio del mínimo privilegio.

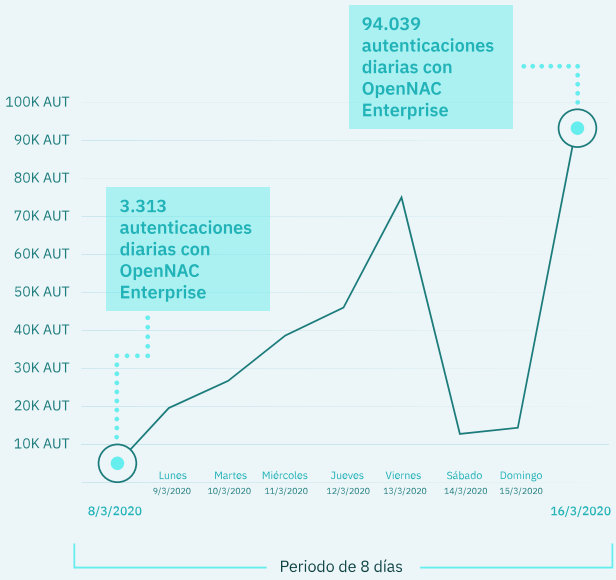
Beneficios principales de 2SRA Secure Remote Access

- **Favorece el principio del mínimo privilegio:** los usuarios sólo acceden a la información y recursos imprescindibles para el desempeño de su actividad.
- **Favorece el enfoque Zero Trust:** establece un marco de seguridad corporativa en el que sólo usuarios y dispositivos autenticados y autorizados pueden acceder a la información corporativa.
- **Ejerce controles de aseguramiento para superficie de ataque:** asegura la conexión remota mediante cifrado y los dispositivos de usuario.
- **Reduce el riesgo asociado al dispositivo de usuario:** permite la evaluación de postura de dispositivos, estableciendo el cumplimiento de los requisitos mínimos de conexión a la hora de acceder a la red.
- **Mitiga el riesgo de suplantación de identidad:** añade un nivel de seguridad extra mediante doble factor de autenticación.
- **Asistir en la identificación de comportamientos anómalos:** Permite monitorizar todo el tráfico entre el usuario (dispositivo remoto) y el sistema (protocolos usados, datos manados / recibidos, servicios utilizados, hosts contactados etc.)

El caso de éxito de uno de nuestros clientes en la situación actual: de 3.500 autenticaciones diarias a 94.000 conexiones seguras al día

"Una de las multinacionales más importantes de España, que confía en Open Cloud Factory y en su solución **OpenNAC Enterprise** desde 2018, tiene implementado desde esa fecha un módulo de **OpenNAC Enterprise** para doble factor de autenticación (2FA) de usuarios VPN, el cual ha sido de extrema utilidad y de vital importancia para ellos en un contexto de crisis internacional y necesidad de habilitación por emergencia del teletrabajo como modalidad laboral para sus empleados. Nuestro cliente ha pasado de registrar un promedio de 3.500 autenticaciones diarias por medio del 2FA de **OpenNAC Enterprise** a un pico de 94.030 autenticaciones diarias en tan sólo 8 días durante el mes de marzo de 2020. ."

Información adicional:
https://www.opencloudfactory.com/caso-exito-teletrabajo/



Reconocimientos

Gartner

Common Criteria

CCN-CERT centro criptológico nacional

Único fabricante europeo de tecnología NAC incluido en el Gartner Market Guide tres veces consecutivas.

Plataforma certificada en Common Criteria 3.1 release 5 por parte del Organismo de Certificación del Centro Criptológico Nacional OC-CCN de España.

Incluido en el catálogo de productos de Seguridad de las Tecnologías de la información y la comunicación del Centro Criptológico Nacional, Ministerio de Defensa - Gobierno de España.

Contacta con nosotros

opencloud factory

+34 91 614 53 22

www.opencloudfactory.com/contacto