FACULTAD DE INGENIERÍA

Carrera de Ingeniería de Sistemas Computacionales

"IMPLEMENTACIÓN DE OPNSENSE COMO PLATAFORMA DE ACCESO REMOTO SEGURO EN EL CONGRESO DE LA REPÚBLICA, LIMA 2020"

Trabajo de suficiencia profesional para optar el título profesional de:

Ingeniero de Sistemas Computacionales

Autor:
Emilio Alberto Cobos Benavides

Asesor:
Ing. Eduardo Martín Reyes Rodríguez

Lima - Perú

2021

DEDICATORIA

A Isaac Asimov y Eiji Tsuburaya.

AGRADECIMIENTO

A mi familia, por recordarme que nunca es tarde para cumplir metas.

Al Congreso de la República del Perú, por haber confiado en el Departamento de Tecnologías de la Información, del que formo parte, para llevar adelante este proyecto.

A la Universidad Privada del Norte, que me brindó la oportunidad de exigirme académicamente una vez más.

Al Ing. Eduardo Martín Reyes Rodríguez, sin cuya asesoría y valiosos aportes no hubiera sido posible la consecución del presente trabajo.

TABLA DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN EJECUTIVO

A inicios del año 2020 se detectaron a nivel mundial múltiples casos del Síndrome Respiratorio Severo Agudo Coronavirus 2 (SARS-CoV-2), el que fue catalogado como pandemia denominada COVID-19 por la OMS, generando la declaración de Estado de Emergencia Sanitaria por parte del Estado Peruano.

En este escenario, con el propósito de minimizar la exposición del recurso humano al virus SARS-CoV-2, el Congreso de la República dispuso la implementación del trabajo remoto como una de las medidas para permitir el desarrollo de las labores institucionales. Uno de los retos tecnológicos que se debieron enfrentar fue habilitar el acceso remoto seguro, cuya implementación y optimización se detalla en este trabajo.

La solución de acceso remoto seguro implementada en el Congreso se basó en la plataforma de código abierto OPNsense, la que se integró a la arquitectura de conectividad y seguridad existentes en la institución. Desde su despliegue, esta solución permitió mejorar la continuidad de funciones del Congreso, al brindar acceso remoto seguro a PCs y recursos web por parte del personal del Servicio Parlamentario, así como brindar el acceso de comunicaciones para la nueva aplicación de Asistencia y Votación Remota basada en dispositivos móviles, utilizada por los Congresistas para confirmar asistencia y emitir su voto durante las sesiones remotas del Pleno del Congreso.

PALABRAS CLAVE: OPNsense, OpenVPN, acceso remoto seguro, firewall, VPN, 2FA, doble factor de autenticación, múltiple factor de autenticación, RDP.

CAPÍTULO I. INTRODUCCIÓN

1.1. CONTEXTO

El trabajo que se presenta a continuación, titulado "Implementación de OPNsense como plataforma de acceso remoto seguro en el Congreso de la República, Lima 2020", describe el proceso de implementación de un sistema que complemente a la plataforma de infraestructura tecnológica existente en la institución, y permita el acceso remoto seguro a recursos informáticos a través de Internet para diversos tipos de usuarios, en el marco de la emergencia sanitaria por la pandemia de coronavirus (COVID-19) declarada en Perú por la Presidencia de la República mediante Decreto Supremo N°008-2020-SA (Presidencia, 2020), la cual ha sido sucesivamente extendida y sigue estando en vigencia al momento de la presentación del presente documento.

Debido a las medidas tomadas por los gobiernos a nivel mundial para enfrentar la pandemia de Coronavirus (COVID-19), el modo de vida de nuestra sociedad ha sido sometido a cambios en el quehacer diario. De acuerdo a las medidas dictadas por el gobierno central para enfrentar la pandemia mundial de Coronavirus (COVID-19), se determinó necesario establecer medidas tales como la restricción de desplazamiento dentro del territorio nacional, cuarentena, distanciamiento social, uso de Equipos de Protección Personal (EPP) tales como mascarillas y protectores faciales. En el caso de los centros laborales, estos debieron adoptar medidas de prevención y control sanitario para evitar la propagación del COVID-19.

Transcurridos los primeros días de cuarentena obligatoria, el Congreso de la República, mediante el Acuerdo N° 028-2020-2021/MESA-CR de la Mesa Directiva (Congreso, Portal del Congreso de la República, 2020), oficializó el "Plan para la Vigilancia, Prevención y Control del COVID-19 en el Congreso de la República" en el que se establecieron los lineamientos para preservar la salud de los trabajadores del Servicio Parlamentario con riesgo

de exposición al Sars-Cov2 (COVID-19). En el punto 7.5 numeral 1 del plan mencionado se indicó que la primera opción a considerar para el desarrollo de reuniones de trabajo sea mediante plataformas virtuales u otras que permitan la interacción a distancia. En el numeral 2 se estableció que, de no ser posible, se debían considerar la asistencia con aforos mínimos, distanciamiento social y uso de EPP. La Alta Dirección dispuso que el Departamento de Tecnologías de la Información tome las medidas necesarias y realice las labores correspondientes para la consecución de estas disposiciones, en lo que corresponda a su competencia.

1.2. DATOS DE LA INSTITUCIÓN

El Congreso de la República fue fundado el 20 de setiembre de 1822, siendo desde ese entonces el órgano representativo de la nación peruana. Tiene como funciones principales la representación de la nación, la dación de leyes, la fiscalización y control político. Es unicameral y está integrado por ciento treinta Congresistas elegidos en forma directa, de acuerdo a ley (Congreso, Funciones del Congreso de la República).

Figura 1

Palacio Legislativo.

Fuente: Portal del Congreso del Perú.

1.2.1. FUNCIONES DEL CONGRESO

1.2.1.1. FUNCIÓN LEGISLATIVA

El Congreso tiene la tarea de aprobar las leyes en beneficio del país. También aprueba las resoluciones legislativas o normas (ejemplo: aprobar un tratado internacional o autorizar al Presidente de la República a ausentarse del país). Asimismo, puede reformar la Constitución que es fundamental para la organización del Estado (Congreso, Parlamento Escolar, 2011).

1.2.1.2. FUNCIÓN DE CONTROL POLÍTICO

El Congreso tiene la responsabilidad de fiscalizar el trabajo en la administración pública y en el gobierno, pudiendo delegar facultades legislativas al Poder Ejecutivo, además de revisar los decretos de urgencia y la disposición de bienes y recursos públicos.

Además, tiene la responsabilidad de fiscalizar o supervisar la conducta de todos los funcionarios del Estado en la labor encomendada. El Congreso tiene la facultad de suspender, destituir o inhabilitar del cargo al funcionario acusado ante las evidencias de delito (Congreso, Funciones del Congreso de la República) .

1.2.1.3. FUNCIONES DE REPRESENTACIÓN

Mediante el voto, los ciudadanos otorgan al Congreso (concretamente a los congresistas) la responsabilidad de representarlos. Por lo tanto, también tiene como una función principal la defensa de los intereses del Perú (Congreso, Funciones del Congreso de la República).

1.2.2. MISIÓN Y VISIÓN

1.2.2.1. MISIÓN

El Congreso expresa la soberanía y pluralidad política de la República, en base al desempeño eficaz, honesto, legítimo y transparente de sus funciones de representación, legislación y control político, para afirmar la estabilidad democrática y la gobernabilidad del país, ayudando así al bienestar de todos los peruanos (Congreso, Misión y Visión del Congreso) .

1.2.2.2. VISIÓN

El Congreso de la República del Perú, en representación de todos los peruanos, legisla y ejerce el control político, además de cumplir con las funciones especiales establecidas por la Constitución Política, en aras del bienestar general y la consolidación del sistema democrático (Congreso, Misión y Visión del Congreso).

1.2.3. ORGANIZACIÓN INSTITUCIONAL

1.2.3.1. ORGANIZACIÓN PARLAMENTARIA

- **Pleno**

El Pleno es la máxima asamblea deliberativa del Congreso. Lo integran todos los congresistas y funciona de acuerdo con las reglas de quórum y de procedimiento que establecen la Constitución y el presente Reglamento. Allí se debaten y se votan todos los asuntos y se realizan los actos que prevén la normas constitucionales, legales y reglamentarias (Congreso, Organización del Congreso).

Figura 2

Hemiciclo de Sesiones.

Fuente: Elaboración propia.

- **Consejo Directivo**

  El Consejo Directivo está integrado por los miembros de la Mesa Directiva y los representantes de los grupos parlamentarios, que se denominan Directivos-Portavoces, elegidos por su respectivo grupo. En la conformación del Consejo Directivo se procurará guardar similar proporcionalidad a la que exista entre los grupos parlamentarios en la distribución de escaños en el Pleno del Congreso (Congreso, Organización del Congreso).

- **Junta de Portavoces**

  La Junta de Portavoces está compuesta por la Mesa Directiva y por un portavoz por cada grupo parlamentario, quien tiene un voto proporcional al número de miembros que componen su bancada (Congreso, Organización del Congreso).

- **Mesa Directiva**

La Mesa Directiva tiene a su cargo la dirección administrativa del Congreso y de los debates que se realizan en el Pleno del mismo, de la Comisión Permanente y del Consejo Directivo, así como la representación oficial del Congreso en los actos protocolares. Está compuesta por el Presidente y tres Vicepresidentes (Congreso, Organización del Congreso).

- **Presidencia**

  El Presidente del Congreso tiene como funciones principales el representar al Congreso, así como presidir las sesiones del pleno del Congreso, de la Comisión Permanente, y de la Mesa Directiva, concediendo el uso de la palabra, haciendo guardar el orden y dirigiendo el curso de los debates y las votaciones, conforme a las normas procesales constitucionales, legales y reglamentarias (Congreso, Organización del Congreso).

- **Comisiones ordinarias**

  Son entes encargados del estudio y dictamen de los asuntos ordinarios de la agenda del Congreso, con prioridad en la función legislativa y de fiscalización (Congreso, Organización del Congreso).

- **Comisión Permanente**

  La Comisión Permanente está presidida por el Presidente del Congreso y está conformada por no menos de veinte congresistas elegidos por el Pleno, guardando la proporcionalidad de los representantes de cada grupo parlamentario (Congreso, Organización del Congreso).

- **Grupos parlamentarios**

Los Grupos Parlamentarios son conjuntos de Congresistas que comparten ideas o intereses comunes o afines (Congreso, Organización del Congreso).

1.2.3.2. SERVICIO PARLAMENTARIO

- **Oficialía Mayor**

  La Oficialía Mayor es el máximo órgano del servicio parlamentario del Congreso. Está a cargo de un funcionario denominado Oficial Mayor del Congreso, quien responde ante el Presidente por la marcha y los resultados de las dependencias y el personal del servicio parlamentario. (Congreso, Organización del Congreso).

- **Dirección General Parlamentaria**

  La Dirección General Parlamentaria es un órgano de línea del Congreso de la República, encargado de brindar asesoramiento especializado para el cumplimiento de la labor parlamentaria, que comprende el proceso de creación de la ley, el control parlamentario y el ejercicio de la función de representación (Congreso, Organización del Congreso).

- **Dirección General Administrativa**

  La Dirección General de Administración es un órgano dependiente de la Oficialía Mayor del Congreso. Tiene como responsabilidades la administración de los recursos físicos, humanos y tecnológicos, los servicios, el control patrimonial, la contabilidad y la ejecución presupuestal del Congreso, así como la organización y el desarrollo de las licitaciones y

los concursos públicos de precios y méritos (Congreso, Organización del Congreso).

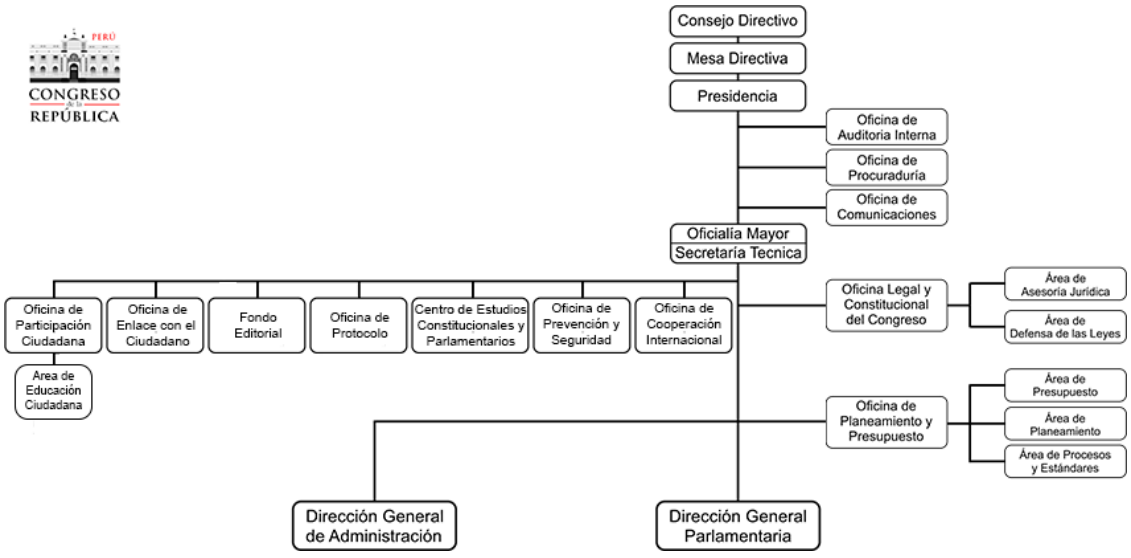
1.2.4. ORGANIGRAMA

El organigrama del Congreso de la República se muestra a continuación (Congreso, Organización del Congreso). La versión oficial firmada se encuentra en el Anexo 1.

ESTRUCTURA PRINCIPAL

Figura 3

Organigrama del Congreso - Estructura Principal.



Fuente: Portal del Congreso de la República

1.2.4.1. DIRECCIÓN GENERAL PARLAMENTARIA

Figura 4

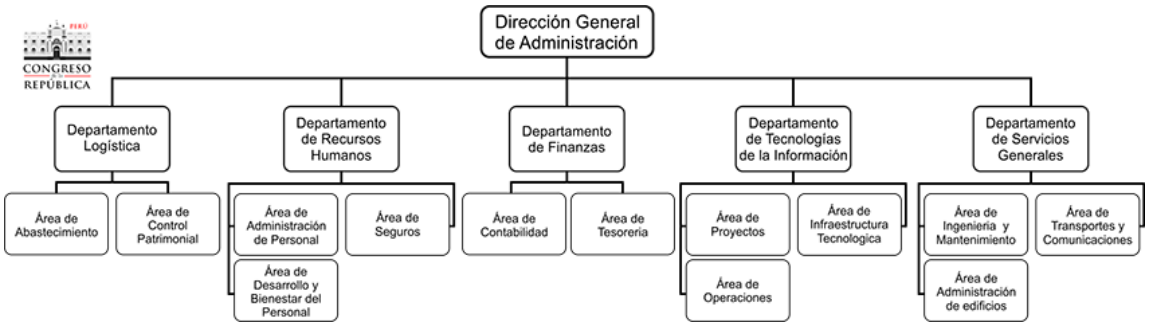
Organigrama del Congreso - Dirección General Parlamentaria.

Fuente: Portal del Congreso de la República

1.2.4.2. DIRECCIÓN GENERAL DE ADMINISTRACIÓN

Figura 5

Organigrama del Congreso - Dirección General Administrativa.



Fuente: Portal del Congreso de la República

CAPÍTULO II. MARCO TEÓRICO

2 ACCESO REMOTO SEGURO

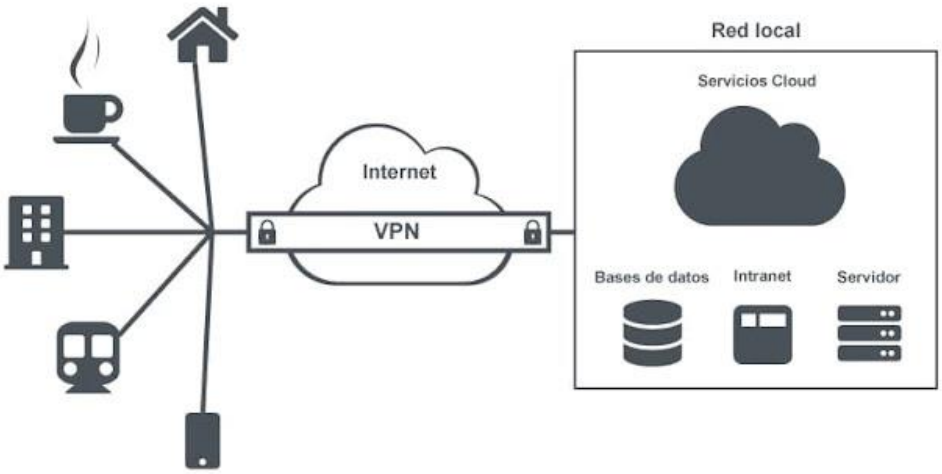
2.1 DESCRIPCIÓN DE ACCESO REMOTO SEGURO

El **Acceso Remoto Seguro** es una combinación de procesos o soluciones de **Seguridad Informática** que están diseñadas para evitar el acceso no autorizado a los activos digitales de una organización y evitar la pérdida de datos confidenciales. El acceso remoto seguro puede abarcar una serie de metodologías tales como redes privadas virtuales (Virtual Private Network – VPN), autenticación multifactor y protección de terminales (Endpoint Protection), entre otras (VMware).

Debido a la pandemia de COVID-19, se ha incrementado el número de usuarios remotos a nivel mundial, lo que hace que el acceso remoto seguro sea un elemento crítico del entorno de TI actual.

Figura 6

Esquema básico de Acceso Remoto Seguro mediante VPN.



Fuente: (Segu.Info, 2020)

Para el proyecto de Acceso Remoto Seguro en el Congreso se debieron considerar las mejores prácticas de seguridad, las que se describen a continuación.

2.2 CONCEPTOS BÁSICOS DE SEGURIDAD INFORMÁTICA

La Seguridad Informática es un conjunto de medidas de prevención, detección y corrección, orientadas a proteger la confidencialidad, integridad y disponibilidad de los activos de información de una institución (ISO/IEC 27001).

- **Confidencialidad:** prevenir el acceso no autorizado a la información crítica.
- **Integridad:** prevenir la modificación no autorizada de los sistemas y la información.
- **Disponibilidad:** prevenir la interrupción del servicio y la productividad.

El Acceso Remoto Seguro es el esquema de medidas a tomar en este proyecto para habilitar estos principios básicos de Seguridad Informática, para habilitar el trabajo remoto y la continuidad de operaciones de la institución.

2.3 CONSIDERACIONES PARA LA IMPLEMENTACIÓN DE ACCESO REMOTO SEGURO

- **Proteger los endpoints para todos los usuarios remotos y sus dispositivos:** proteger los endpoints en un centro de datos es bastante simple en comparación a proteger los endpoints para los usuarios remotos, pues estos utilizan diferentes dispositivos, ya sean proporcionados por la organización o de su propiedad. El software antivirus debe instalarse en todos los dispositivos endpoint.

  Las políticas de seguridad deben exigir que todos los empleados mantengan la protección actual si van a acceder a los recursos de la organización.

- **Evitar que el acceso remoto aumente la superficie de ataque:** la configuración del acceso remoto puede presentar riesgos para una organización. En particular, los

ataques de ransomware a menudo buscan servidores de protocolo de escritorio remoto (RDP). Es por ello que se debe evitar el abrir puertos de acceso remoto solo cuando sea necesario, y de manera controlada.

- **Adoptar la autenticación multifactor:** la autenticación de dos factores (2FA) requiere que los usuarios proporcionen "algo que saben y algo que tienen", por ejemplo, una contraseña y un token de autenticación, que puede ser generado por un dispositivo o desde una aplicación de teléfonos inteligentes. Esto puede garantizar que solo los usuarios verificados tengan acceso a los recursos corporativos.
- **Utilizar redes privadas virtuales (VPN):** los usuarios remotos pueden conectarse desde sus domicilios, desde redes Wi-Fi inseguras (ejemplo, una cafetería que ofrezca conexión a sus clientes) u otras conexiones de red que no sean de confianza. Las VPN permiten el establecimiento de un camino de comunicaciones seguro y encriptado sobre esas conexiones inseguras.
- **Educar a los usuarios:** la pandemia de COVID-19 ha visto la creación de una serie de nuevas amenazas informáticas y ataques de phishing que pretenden estar relacionados con el virus. Como parte de su capacitación en seguridad y cumplimiento, se debe recordar a todos los empleados y otras personas que acceden a los recursos corporativos que no hagan clic en ningún correo electrónico no solicitado o en los enlaces que contienen.
- **Actualizar las políticas para la fuerza de trabajo remota:** se debe asegurar que las políticas de uso aceptable incluyan los activos informáticos del hogar de un empleado, que pueden ser computadoras, laptops, tabletas y teléfonos inteligentes, validando que estos equipos disponen de las configuraciones de seguridad mínimas indispensables para accedes a los recursos institucionales (VMware).

2.4 TECNOLOGÍAS UTILIZADAS PARA BRINDAR ACCESO REMOTO SEGURO

El acceso remoto seguro no es una tecnología única, sino más bien un conjunto de tecnologías que, en su conjunto, brindan la seguridad que las organizaciones necesitan cuando los usuarios trabajan desde casa o en otras ubicaciones remotas. Estas tecnologías incluyen:

- Seguridad de Endpoint
- Red Privada Virtual (VPN)
- Control de Acceso

A continuación, se detalla cada uno de estas tres tecnologías.

2.5 SEGURIDAD DE ENDPOINT:

La protección de endpoints (endpoint protection) o seguridad de endpoints (endpoint security) es un término que se refiere a las soluciones de seguridad que abordan problemas de seguridad de endpoints, asegurando y protegiéndolos contra exploits de día cero, ataques informáticos y fugas de datos resultantes de errores humanos al prevenir no solo ataque de virus informáticos y otros software maliciosos mediante el uso de firmas (base de datos que contiene la identificación de malware conocido) y la detección heurística de ataques de día cero (Endpoint Detection and Response - EDR), así como otras características avanzadas como sandboxing (análisis del comportamiento de software sospechoso en un ambiente controlado) (Lord, 2018).

2.5.1 FUNCIONALIDADES DE SOFTWARE DE SEGURIDAD DE ENDPOINT

Básicamente, las funcionalidades ideales que debe incluir una solución de Seguridad de Endpoint son:

- **Administrar:** debe permitir la administración y monitoreo de dispositivos. Esto se logra de manera integrada en un solo software

administración/protección antimalware, o independiente como por ejemplo con software MDM (Mobile Device Management).

- **Automatizar:** por ejemplo, el despliegue de parches de sistema operativo, nuevas versiones de software. Esto se logra de manera integrada en un solo software administración/protección antimalware, o independiente como por ejemplo con software MDM (Mobile Device Management).
- **Asegurar:** debe proteger contra ataques informáticos (malware en general como virus, ransomware, intentos de phishing y hacking), mediante el uso de tecnologías como antivirus, RDR, Next Generation Firewall y sandboxing (ManageEngine).

2.5.2 TECNOLOGÍAS ASOCIADAS A SEGURIDAD DE ENDPOINT

1. ANTIVIRUS

Son la tecnología más antigua y conocida de protección de endpoints. Su funcionamiento se basa en el análisis de la "huella" digital de los programas en ejecución en un sistema. Las huellas o firmas de cada malware conocido se almacenan ya sea localmente o en la nube, y son consultadas constantemente para identificar amenazas. Si bien mantiene su utilidad, la desventaja de este sistema radica en que para una protección efectiva es necesario disponer la firma de la amenaza, y este proceso puede estar retrasado alrededor de cuatro meses con respecto a amenazas de día cero.

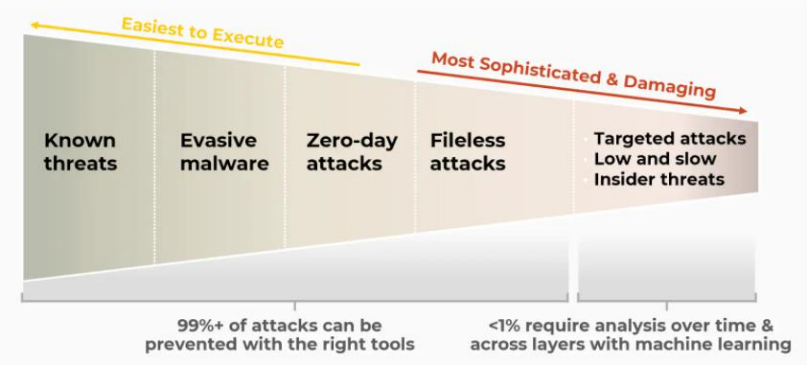
2. ENDPOINT DETECTION AND RESPONSE (EDR)

El software EDR utiliza el análisis con inteligencia artificial del comportamiento de software y eventos en endpoints y servidores para poder identificar actividad sospechosa.

En su conjunto, estas dos técnicas logran detener hasta un 99% de los ataques (con una configuración adecuada), requiriendo el porcentaje restante de ataque muy sofisticados el análisis de actividad por simulación (Sandboxing) (PaloAlto, Endpoint detection and response).

Figura 7

Niveles de amenazas detenidas por soluciones Antivirus / EDR.



Fuente: PaloAlto Networks (PaloAlto, Endpoint detection and response)

3. SANDBOXING

Las medidas de seguridad tradicionales son reactivas y se basan en la detección de firmas (los antivirus funcionan mediante la búsqueda de patrones identificados en instancias conocidas de malware), o en el caso de EDR inteligencia artificial o aprendizaje automático (detección sin firma), pero estas defensas son tan buenas como los modelos que impulsan estas soluciones. El sandboxing o pruebas de espacio aislado detectan malware

de forma proactiva mediante el uso de inteligencia artificial para la ejecución o detonación de código en un entorno seguro y aislado, para observar el comportamiento y la actividad de salida de ese código, de manera que generan un nivel adicional de protección en endpoints (Forcepoint).

2.6 RED PRIVADA VIRTUAL (VPN)

2.6.1 DEFINICIÓN DE VPN

Una VPN (Virtual Private Network), o red privada virtual, es una conexión segura y cifrada (encriptada) entre dos redes o entre un usuario determinado y una red. Las conexiones cifradas ayudan a garantizar que los datos confidenciales se transmitan de forma segura. La tecnología VPN se usa ampliamente en entornos corporativos.

FUNCIONAMIENTO

Para el establecimiento de una VPN, se requiere de los siguientes elementos (ComputerScience):

- Una LAN que está conectada a Internet.
- Una computadora fuera de la LAN que también está conectada a Internet.
- Cliente y servidor VPN que se ejecutan en la computadora (cliente) y en la LAN original (servidor).

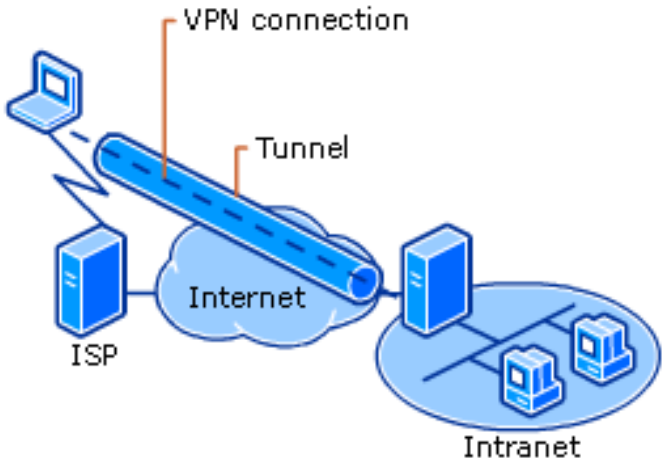
Con estos elementos, se establece una conexión que utiliza dos tecnologías:

1. **CIFRADO:** En criptografía, el cifrado es el proceso de codificar un mensaje o información de tal manera que solo las partes autorizadas pueden acceder a él y las que no están autorizadas no. El cifrado no evita en sí mismo la interferencia, pero niega el acceso legible al contenido a un posible interceptor.

2. **TUNELIZACIÓN**: En las redes informáticas, un protocolo de tunelización es un protocolo de comunicaciones que permite el movimiento de datos de una red a otra. Implica permitir que las comunicaciones de la red privada se envíen a través de una red pública (como Internet) a través de un proceso llamado encapsulación.

Figura 8

Diagrama típico de una conexión VPN.



Fuente: Computer Science Wiki (ComputerScience)

2.6.2 MÉTODOS DE SEGURIDAD VPN

Una VPN diseñada de manera adecuada utiliza varios métodos para garantizar el establecimiento seguro de la conexión.

- **CONFIDENCIALIDAD DE DATOS:** este es el servicio más importante ofrecido por cualquier implementación de VPN. Dado que los datos privados viajan a través de una red pública, la confidencialidad de estos es fundamental y puede lograrse mediante el cifrado de datos.

- **INTEGRIDAD DE DATOS:** si bien es importante que los datos se cifren a través de una red pública, es igualmente importante verificar que no se hayan modificado mientras están en tránsito.

Los métodos de confidencialidad e integridad para VPN son ofrecidos por varios protocolos que brindan las tecnologías de cifrado y tunelización. A continuación, se muestra una comparación de los más utilizados en la actualidad (IVPN).

Tabla 1

Comparación de protocolos VPN

Característica	Protocolos			
	PPTP	IPSec IKEv2	OpenVPN	WireGuard
Descripción básica **(ver "Protocolos de encriptación VPN" en el punto 2.9)**	Un protocolo VPN muy básico basado en PPP. La especificación PPTP en realidad no describe las funciones de encriptación o autenticación y se basa en el protocolo PPP que se tuneliza para implementar la funcionalidad de seguridad.	IKEv2 (intercambio de claves de Internet versión 2) es parte del conjunto de protocolos IPSec. Estandarizado en RFC 7296. IPSec se ha convertido en el protocolo estándar de facto para comunicaciones seguras de Internet, proporcionando confidencialidad, autenticación e integridad.	Protocolo VPN de código abierto desarrollado por tecnologías OpenVPN. Muy popular, sin embargo, no se basa en estándares (RFC). Utiliza un protocolo de seguridad personalizado y SSL / TLS para el intercambio de claves. Proporciona total confidencialidad, autenticación e integridad.	WireGuard es un protocolo VPN extremadamente rápido con muy poca sobrecarga y criptografía de última generación. Tiene el potencial de ofrecer una VPN más simple, más segura, más eficiente y más fácil de usar que las tecnologías existentes.
Encriptación **(ver "Algoritmos criptográficos" en el punto 2.9)**	La carga útil de PPP se cifra mediante el protocolo de cifrado punto a punto (MPPE) de Microsoft. MPPE implementa el algoritmo de cifrado RSA RC4 con un máximo de claves de sesión de 128 bits.	IKEv2 implementa una gran cantidad de algoritmos criptográficos, incluidos 3DES, AES, Blowfish, Camellia. IVPN implementa IKEv2 usando AES con claves de 256 bits.	OpenVPN utiliza la biblioteca OpenSSL para proporcionar cifrado. OpenSSL implementa una gran cantidad de algoritmos criptográficos como 3DES, AES, RC5, Blowfish. Al igual que con IKEv2, IVPN implementa	Hace uso de un protocolo de enlace basado en UDP y el intercambio de claves utiliza un secreto directo perfecto al tiempo que evita tanto la suplantación de clave comprometida

			AES con claves de 256 bits.	como los ataques de repetición.
Debilidades identificadas	La implementación de Microsoft de PPTP tiene serias vulnerabilidades de seguridad. MSCHAP-v2 es vulnerable al ataque de diccionario y el algoritmo RC4 está sujeto a un ataque de cambio de bits. Microsoft recomienda encarecidamente actualizar a IPSec cuando la confidencialidad sea una preocupación.	IPSec no tiene vulnerabilidades importantes conocidas y generalmente se considera seguro. Sin embargo, las presentaciones filtradas de la NSA indican que IKE podría explotarse de forma desconocida para descifrar el tráfico IPSec.	OpenVPN no tiene vulnerabilidades importantes conocidas y generalmente se considera seguro cuando se implementa mediante un algoritmo de cifrado seguro y certificados para la autenticación.	WireGuard no tiene vulnerabilidades importantes conocidas. Es relativamente nuevo y no ha sido objeto de una investigación exhaustiva de OpenVPN.
Velocidad	Al usar el protocolo de encriptación obsoleto e inseguro RC4 y claves de 128 bits, la sobrecarga de cifrado es menos que todos los protocolos, lo que hace que PPTP sea el más rápido.	IPSec con IKEv2 debería ser, en teoría, más rápido que OpenVPN debido al cifrado en modo de usuario en OpenVPN, sin embargo, depende de muchas variables específicas de la conexión. En la mayoría de los casos, es más rápido que OpenVPN.	Cuando se usa en su modo UDP predeterminado en una red confiable, OpenVPN funciona de manera similar a IKEv2.	WireGuard se beneficia de primitivas criptográficas de velocidad extremadamente alta y una integración profunda con el kernel del sistema operativo subyacente, por lo que las velocidades son muy altas con una sobrecarga baja en Linux.
Puertos utilizados	PPTP utiliza el puerto TCP 1723 y GRE (Protocolo 47). PPTP se puede bloquear fácilmente restringiendo el protocolo GRE.	IKEv2 utiliza UDP 500 para el intercambio de claves inicial, el protocolo 50 para los datos cifrados IPSEC (ESP) y UDP 4500 para NAT transversal. IKEv2 es más fácil de bloquear que OpenVPN debido a su dependencia de protocolos y puertos fijos.	OpenVPN se puede configurar fácilmente para que se ejecute en cualquier puerto utilizando UDP o TCP, evitando así fácilmente los cortafuegos restrictivos.	WireGuard usa el protocolo UDP y se puede configurar para usar cualquier puerto. Puede ser bloqueado más fácilmente que OpenVPN debido a la falta de soporte para TCP.
Instalación / configuración	Todas las versiones de Windows y la mayoría de los demás sistemas operativos (incluido el	Windows 7+, macOS 10.11+ y la mayoría de los sistemas operativos móviles tienen	OpenVPN no está incluido en ninguna versión del sistema operativo y requiere la	WireGuard está integrado en el árbol con Linux Kernel 5.6. Otros sistemas operativos

	móvil) tienen soporte nativo para PPTP. PPTP solo requiere un nombre de usuario, contraseña y dirección de servidor, lo que lo hace sumamente sencillo de instalar y configurar.	soporte nativo para IPSec con IKEv2.	instalación de software de cliente. La instalación del software cliente suele tardar menos de 5 minutos.	que no son Linux requieren la instalación de una aplicación cliente WireGuard. La instalación suele tardar menos de 5 minutos.
Estabilidad / compatibilidad	No es tan confiable ni recupera conectividad tan rápido como las demás alternativas.	IPSec es más complejo que OpenVPN y requiere configuraciones adicionales que puede no estén disponibles en algunas redes, tales como NAT transversal.	Muy estable y rápido sobre conexiones celulares y wifi, redes donde la pérdida de datos y la congestión es común. El modo TCP mejora la conectividad en redes muy inestables con el sacrificio de rendimiento.	Estable y robusto, manteniendo conexiones sobre líneas como WiFi y celulares. La falta de soporte TCP puede ocasionar problemas para su uso en algunos ambientes.
Plataformas soportadas	Windows macOS Linux Apple iOS Android DD-WRT	Windows macOS Linux Apple iOS Android	Windows macOS Linux Apple iOS Android DD-WRT	Windows macOS Linux Apple iOS Android

Fuente: IVPN (IVPN)

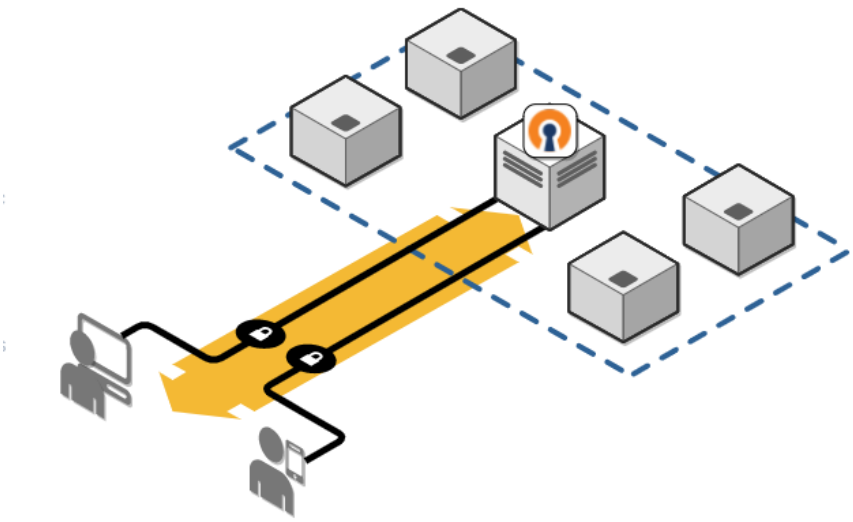
2.6.3 TIPOS DE VPN

2.6.3.1 ACCESO REMOTO

Una VPN de acceso remoto es una conexión temporal entre los usuarios y la sede, normalmente utilizada para acceder a las aplicaciones del centro de datos. Esta conexión podría usar IPsec, pero también es común usar una VPN SSL para configurar una conexión entre el punto final de un usuario y una puerta de enlace VPN (Rehan, 2020).

Figura 9

Esquema típico de una VPN de Acceso Remoto Clientes hacia un sitio remoto.



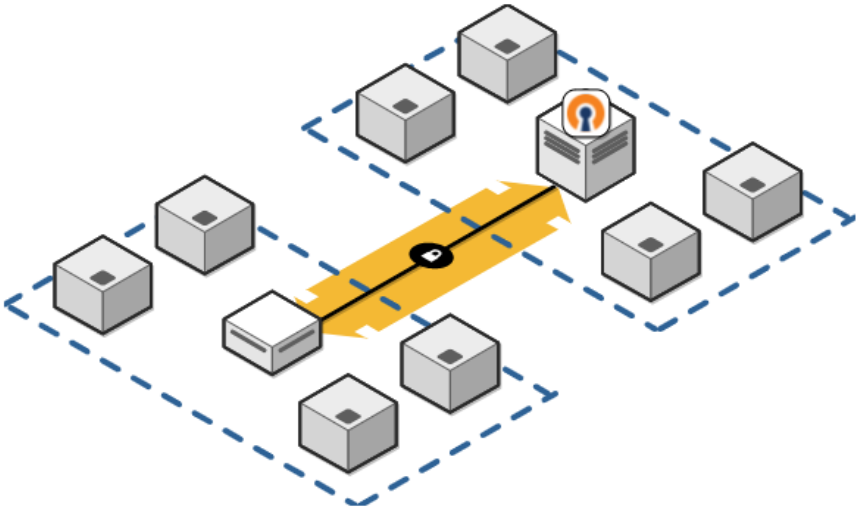
Fuente: OpenVPN (OpenVPN).

2.6.3.2 SITIO A SITIO

Una VPN de sitio a sitio es una conexión permanente diseñada para funcionar como un enlace cifrado entre oficinas (es decir, "sitios").

Figura 10

Esquema típico de VPN Site to Site - Conexión de un sitio a otro sitio remoto.



Fuente: OpenVPN (OpenVPN).

2.7 CONTROL DE ACCESO

El control de acceso es una forma de limitar el acceso a un sistema o a recursos físicos o virtuales. En informática, el control de acceso es un proceso mediante el cual los usuarios obtienen acceso y ciertos privilegios a sistemas, recursos o información. En los sistemas de control de acceso informáticos, los usuarios deben presentar credenciales antes de que se les pueda otorgar acceso. El control de acceso incluye la autorización, autenticación y auditoría de la entidad que intenta acceder (Technopedia, 2017).

2.7.1 AUTENTICACIÓN, AUTORIZACIÓN Y AUDITORÍA

La Autenticación, Autorización y Auditoría (Authentication, Authorization, Accountability o AAA) es un marco de trabajo estándar que se utiliza para controlar quién puede utilizar los recursos de la red (mediante autenticación), qué están

autorizados a hacer (mediante autorización) y capturar las acciones realizadas mientras accede a la red (mediante el registro de auditoría) (GeeksforGeeks, 2018).

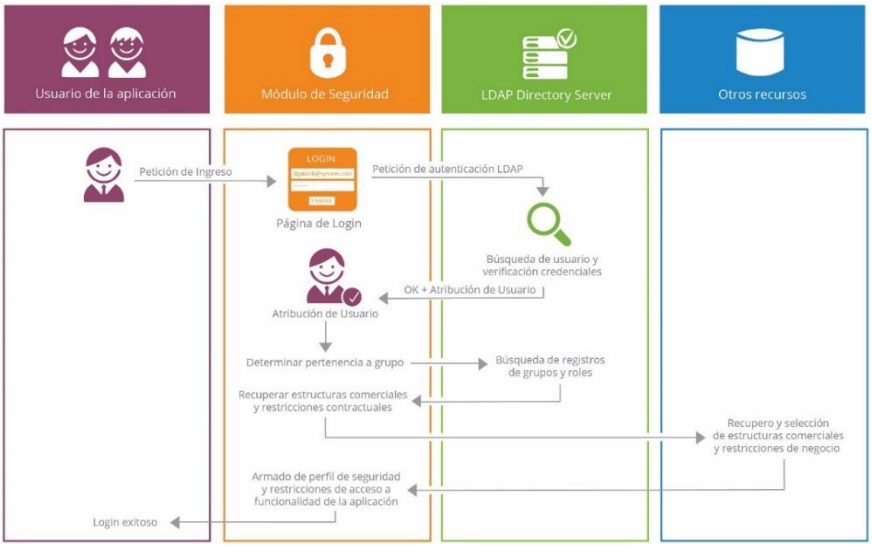
Ante una solicitud para establecer una conexión, el dispositivo VPN solicita un nombre de usuario y una contraseña. Luego, esto se puede autenticar de forma local o enviarse al servidor AAA externo, que comprueba:

- Quién es usted (**Autenticación**)
- Qué tiene permitido hacer (**Autorización**)
- Qué hace realmente (**Registro o traza de auditoría**)

La información de auditoría es especialmente útil para realizar el seguimiento de uso del cliente con fines de reportes de auditoría, solución de problemas y generación de informes de seguridad.

Figura 11

Ejemplo de proceso de Autenticación y Autorización con LDAP.



Nota: el proceso de Auditoría se puede (y debe) dar durante todo el proceso de Autenticación y Autorización. Fuente: SysOne (SysOne).

2.7.1.1 AUTENTICACIÓN

El físico Fernando Corbató fue el creador del concepto de usuario y contraseña como medida de seguridad para el uso compartido de un computador cuando trabajaba en el Massachusetts Institute of Technology (MIT) en 1960 (welivesecurity, 2017). Este método se sigue usando en la actualidad en prácticamente todos los sistemas de información conocidos; sin embargo, actualmente se considera que un solo factor de autenticación (en este caso la contraseña del usuario) es insuficiente para garantizar la privacidad de acceso. Es así como surge el concepto de Autenticación Multifactor (MFA).

AUTENTICACIÓN MULTIFACTOR: La autenticación multifactor (Multi-Factor Authentication o MFA por sus siglas en inglés) es un control de seguridad que requiere que los usuarios verifiquen sus identidades proporcionando múltiples piezas de evidencia antes de obtener acceso a un dispositivo o aplicación (HelpSystems, 2020).

El término 2FA (Two-Factor Authentication. Autenticación de Dos Factores o Doble Factor de Autenticación) es simplemente el uso de únicamente dos factores para realizar la autenticación.

Hay tres formas posibles en las que un usuario puede demostrar que es quien dice ser. Estas formas se denominan factores y son:

- **Conocimiento:** el usuario proporciona información que solo él conoce, como una contraseña o respuestas a preguntas de seguridad.
- **Posesión:** el usuario proporciona un artículo que tiene, como una tarjeta inteligente (smartcard) o una contraseña de un solo uso.

- **Inherencia:** el usuario se basa en una característica única de quién es, como una huella digital, un escaneo de retina o un reconocimiento de voz.

Figura 12

Autenticación Multifactor: algo que sabes + algo que tienes/eres.

Fuente: FEVOX (FEVOX, 2018)

2.7.1.2 AUTORIZACIÓN

La autorización es el proceso de otorgar permiso a un usuario para acceder a un recurso o función específicos. Este término a menudo se usa indistintamente con control de acceso o privilegio de cliente. Dar permiso a alguien para acceder a un computador remoto o proporcionar a usuarios individuales acceso administrativo a una aplicación son algunos ejemplos de autorización.

En entornos seguros, la autorización siempre debe seguir a la autenticación. Los usuarios deben primero demostrar que sus identidades son genuinas antes de que los administradores de una organización les otorguen acceso a los recursos solicitados (Okta).

FIREWALL: Un firewall tradicional proporciona una inspección completa del tráfico de la red. Permite o bloquea el tráfico según el estado, el puerto y el protocolo, y filtra el tráfico según las reglas definidas por el administrador. Para el caso de control de acceso, las reglas de permisos a recursos se dan sobre usuarios o grupos de usuarios, los que se definen como objetos en el firewall.

NEXT-GENERATION FIREWALL: Un firewall de próxima generación (NGFW) hace tanto las funciones de un firewall tradicional como otras funciones adicionales. Además del control de acceso, los NGFW pueden bloquear amenazas modernas como malware avanzado y ataques a la capa de aplicaciones. Según la definición de Gartner (Cisco), un firewall de próxima generación debe incluir:

- Capacidades de firewall estándar como inspección de estado y reglas de control de acceso a recursos.
- Prevención de intrusiones integrada.
- Conocimiento y control de aplicaciones para ver y bloquear aplicaciones de riesgo.
- Control de amenazas (malware).

2.7.1.3 AUDITORÍA

La auditoría se puede definir como la trazabilidad de las acciones realizadas en un sistema hasta una entidad específica del sistema (usuario, proceso, dispositivo). Por ejemplo, el uso de identificación y autenticación de usuarios únicos respalda la rendición de cuentas; el uso de identificaciones de usuario y contraseñas compartidas destruye la responsabilidad (PCMagazine).

En el caso de Acceso Remoto Seguro, se deben mantener registros de auditoría y visualizar accesos en tiempo real, para poder realizar tareas de auditoría de seguridad de información, además sirve como herramienta para identificar problemas (troubleshooting). En los sistemas de acceso se mantienen logs (archivos de texto) y/o entradas en bases de datos, las cuales almacenan la información para posterior investigación de ser necesario.

2.8 PLATAFORMA OPNSENSE

OPNsense es una plataforma de seguridad de código abierto creada y mantenida por la empresa Deciso. OPNsense está basado en tecnologías abiertas tales como HardenedBSD (sistema operativo y firewall), OpenVPN (VPN) y OpenSSL (librería para emisión de certificados digitales). OPNsense incluye la mayoría de las funciones disponibles en firewalls comerciales, y en muchos casos dispone de más características que la de estos, mediante el uso de plugins que aumentan su funcionalidad. Esta plataforma ofrece una interface gráfica de administración vía web, facilitando la configuración y uso de la misma. Otro de los beneficios que ofrece es del brindar fuentes abiertas y verificables.

OPNsense comenzó como una bifurcación de pfSense y m0n0wall (soluciones de firewall de código abierto) en 2014, con su primer lanzamiento oficial en enero de 2015. El proyecto ha evolucionado en el tiempo, conservando aspectos familiares de m0n0wall y pfSense, lo que permite facilitar la migración de estas plataformas hacia OPNsense (OPNsense).

Figura 13

Logo de OPNsense.

Fuente: Wikimedia Commons (Deciso, 2020)

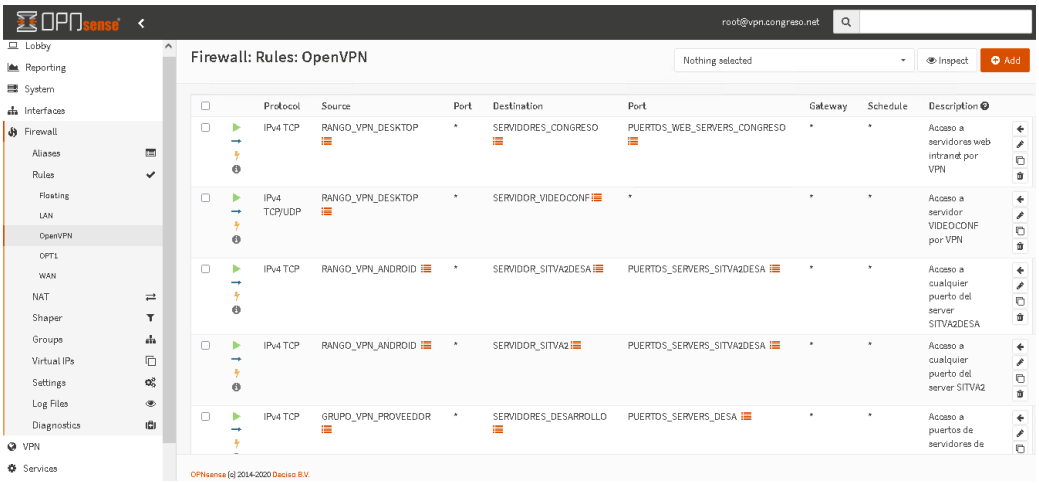
2.8.1 CARACTERÍSTICAS DE LA PLATAFORMA OPNSENSE

STATEFUL FIREWALL

Un Stateful Firewall es un firewall que realiza un seguimiento del estado de las conexiones de red que lo atraviesan (tales como transmisiones TCP, comunicación UDP). OPNsense ofrece la agrupación de reglas de firewall por categoría, una gran característica para configuraciones de red exigentes. Una de las características avanzadas que permiten facilitar la gestión es el uso de Alias, los que permiten identificar objetos o conjuntos de objetos de red (servicios, equipos, etc) y crear reglas de firewall flexibles. Este proyecto utilizó extensivamente esta característica.

Figura 14

Reglas de firewall para interface OpenVPN.



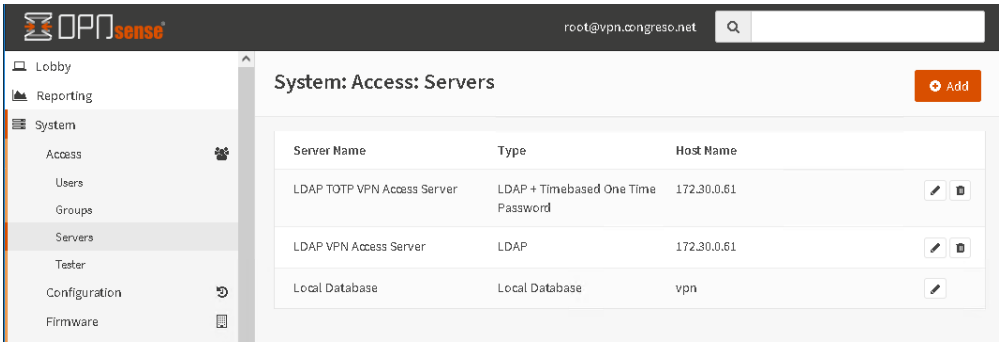
Fuente: elaboración propia.

MOTOR DE AUTENTICACIÓN INTEGRADO

Una de las características más importantes de esta plataforma es la integración de un sistema de autenticación de usuarios, ya sean estos locales o de un servicio de directorio externo (LDAP tales como Active Directory de Microsoft o Linux). Este motor de autenticación es compatible para el ingreso a la plataforma misma o para el uso de servicios tales como VPN y Proxy Caché.

Figura 15

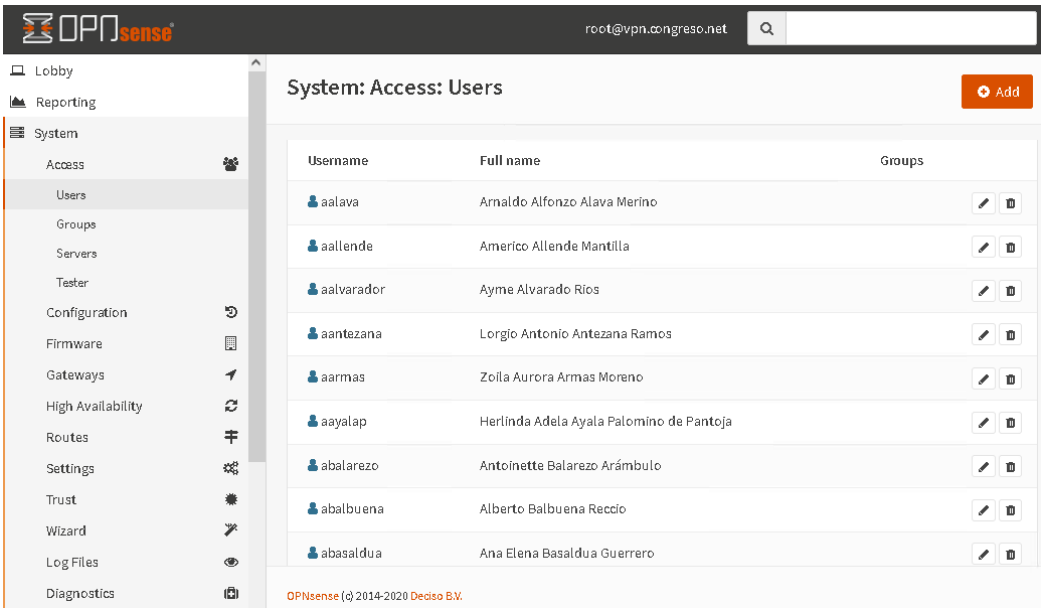
Servidores de autenticación LDAP y local.



Fuente: elaboración propia.

Figura 16

Ejemplo de lista de usuarios.



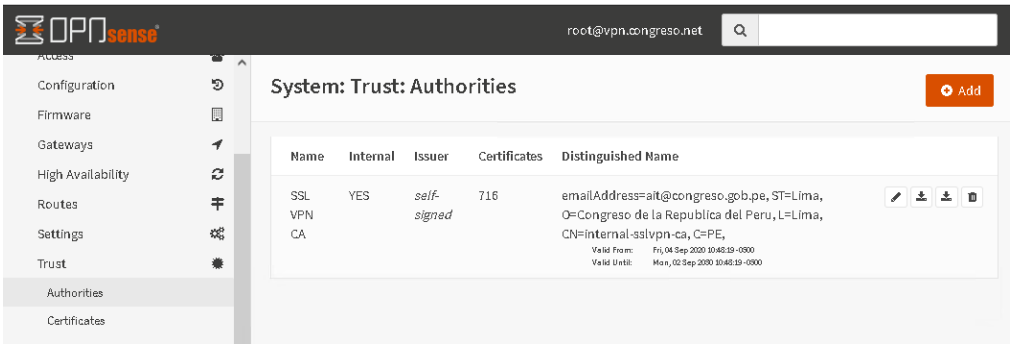
Fuente: elaboración propia.

MOTOR DE CIFRADO INTEGRADO

La plataforma soporta el uso de dos proyectos de código abierto estándares de la industria para la gestión de cifrado SSL: OpenSSL y LibreSSL. Permite la generación de certificados de servidor y usuarios, los cuales se utilizan en este proyecto como un factor de autenticación adicional.

Figura 17

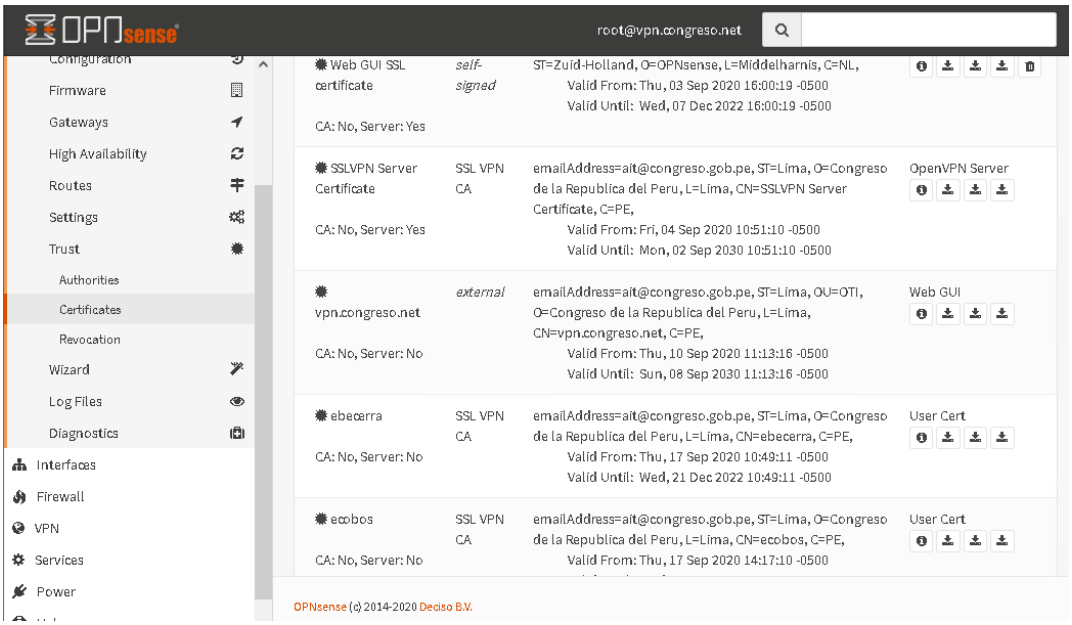
Autoridad de Certificación (CA).



Fuente: elaboración propia.

Figura 18

Ejemplo de certificados generados.



Fuente: elaboración propia.

AUTENTICACIÓN MULTIFACTOR

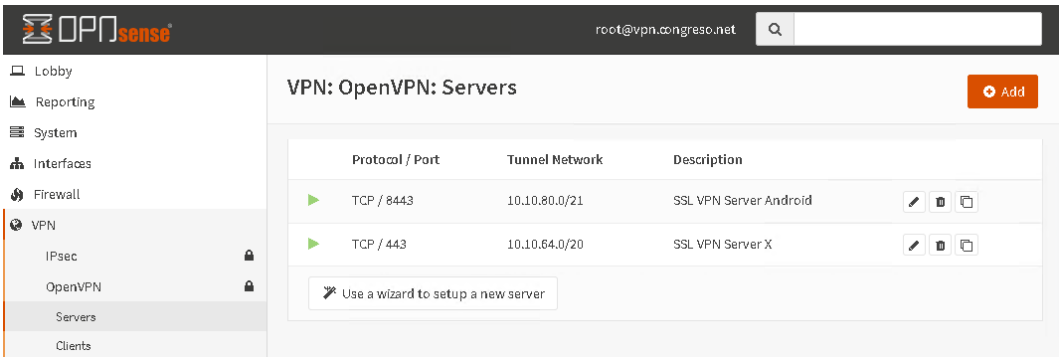
OPNsense ofrece soporte completo para la autenticación de múltiples factores en todo el sistema utilizando TOTP (Time-based One-Time Password) con aplicaciones de seguridad tales como Google Authenticator y Microsoft Authenticator. Este proyecto utiliza esta característica como un factor de autenticación adicional.

RED PRIVADA VIRTUAL (VPN)

OPNsense ofrece una amplia gama de tecnologías VPN, desde las más modernas como SSL-VPN (OpenVPN), IPsec, e incluso opciones heredadas más antiguas (ahora consideradas inseguras) como L2TP y PPTP. Se pueden configurar varios servicios VPN de manera simultánea, tanto en modo Site-to-Site como Acceso Remoto. Permite la exportación de la configuración de los clientes para facilitar la configuración de los mismos.

Figura 19

Servidores VPN OpenVPN en servicio.



Fuente: elaboración propia.

ALTA DISPONIBILIDAD

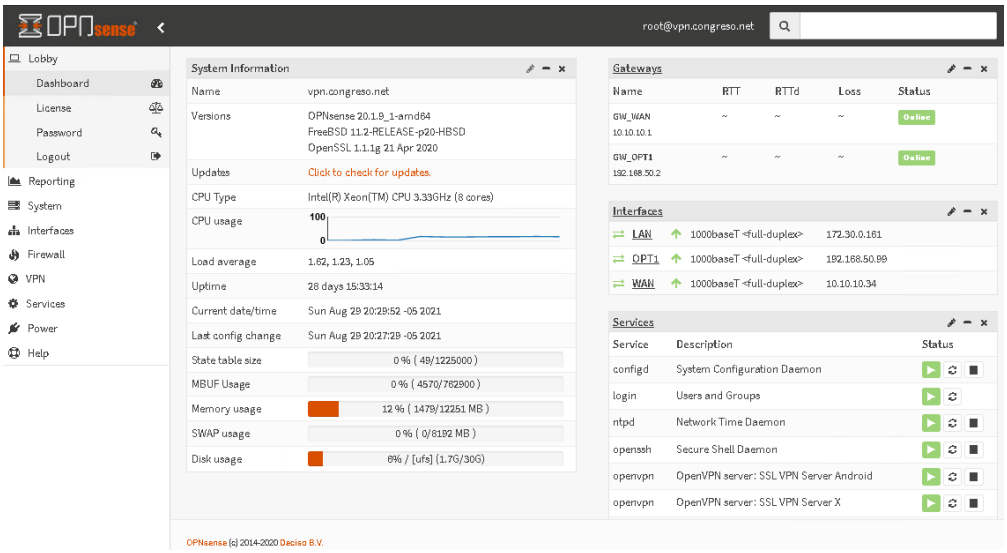
OPNsense utiliza el protocolo común de redundancia de direcciones (Common Address Redundancy Protocol o CARP) para la conmutación por falla de hardware. Se pueden configurar dos o más firewalls como grupo de conmutación por falla. Si una interfaz falla en la primaria o la primaria se desconecta por completo, la secundaria se activa. El uso de esta característica de OPNsense crea un firewall completamente redundante con conmutación automática. Mientras se cambia a la red de respaldo, las conexiones permanecen activas con una interrupción mínima para los usuarios.

CONSOLA DE VISUALIZACIÓN GRÁFICA (DASHBOARD)

OPNsense ofrece una función de panel para verificar rápidamente el estado del firewall OPNsense. Permite además tomar acciones rápidas como el reinicio de servicios.

Figura 20

Consola del sistema (Dashboard).



Fuente: elaboración propia.

Otras características

- Detección y Prevención de Intrusos (IPS).
- Portal Cautivo.
- Proxy Caché.
- Servicios de Copia de respaldo y restauración.
- Servicios de reportes y monitoreo.
- Servicios de actualización de sistema.
- Plugins o extensiones que permiten extender las características de la plataforma.

2.9 DEFINICIÓN DE TÉRMINOS BÁSICOS

- **2FA:** Two-factor authentication o doble factor de autenticación, es un proceso de seguridad en el que los usuarios proporcionan dos factores de autenticación diferentes para verificar su identidad. Estos factores deben ser de naturaleza distinta, cumpliendo el principio de "algo que sabes y algo que tienes". Ejemplo: una contraseña de ingreso acompañada de una tarjeta con chip (TechTarget).
- **AAA:** Autenticación, Autorización, Auditoría (Authentication, Authorization, Accountability) es un conjunto de herramientas, procedimientos y protocolos que garantizan un tratamiento coherente de las tareas de autenticación, autorización y registro de actividad de las entidades que tienen acceso a un sistema de información (PCI).
- **Active Directory:** Es el servicio de directorio propietario de Microsoft para su uso en redes de dominio de Windows. Cuenta con funciones de autenticación y autorización y proporciona un framework para otros servicios similares.

Consiste en una base de datos LDAP que contiene objetos en red. Active Directory utiliza el sistema operativo Windows Server (Paessler).

- **Algoritmos criptográficos:** En criptografía, un algoritmo criptográfico (encryption cipher) es un algoritmo que puede encriptar texto en lenguaje natural para hacerlo ilegible, y para que sea desencriptado con el fin de recuperar el texto original. Los algoritmos criptográficos para VPN más comunes son (Analytics Insight, 2019):
    - **Blowfish:** utiliza normalmente una llave de encriptación de 128 bits, es una alternativa válida en caso algoritmos más fuertes no estén disponibles.
    - **AES:** utiliza llaves de encriptación de 128, 192 y 256 bits. Es el algoritmo más popular para implementaciones VPN, certificado por el NIST (National Institute of Standards and Technology) y utilizado por el gobierno de los Estados Unidos. La encriptación de 256 bits es considerada indescifrable ante ataques de hacking.
    - **Camellia:** utiliza llaves de encriptación de 128, 192 y 256. Mencionada como equivalente en seguridad a AES, aún no posee certificaciones de seguridad.
    - **3DES (Triple DES):** es básicamente el algoritmo Data Encryption Standard usado tres veces. Es considerado inseguro, más lento que Blowfish y su uso estará prohibido desde el año 2023.
    - **MPPE (Microsoft Point to Point Encryption):** soporta llaves de 40, 56 y 128 bits. Considerado inseguro, no es una opción viable en la actualidad.

  - **RSA RC4 y RC5:** algoritmos propietarios, considerados inseguros y lentos. No deben ser utilizados en la actualidad.

- **Antivirus:** Es un programa o conjunto de programas diseñados para prevenir, buscar, detectar y eliminar virus de software y software malintencionado como gusanos, troyanos, adware y otros (Webroot).
- **Auditoría:** Se refiere al seguimiento del consumo de recursos de la red por parte de los usuarios. Esta información se puede utilizar para fines de gestión, planificación, facturación u otros. El monitoreo de registros en tiempo real se refiere a la información que se obtiene al mismo tiempo del consumo de los recursos. El registro por lotes se refiere a la información de registro que se guarda hasta que se entrega en un momento posterior. La información típica que se recopila en el registro es la identidad del usuario, la naturaleza del servicio prestado, cuándo comenzó el servicio y cuándo terminó.
- **Autenticación:** Es la confirmación de que un usuario que solicita servicios es un usuario válido de los servicios de red solicitados. La autenticación se logra mediante la presentación de una identidad y credenciales. Ejemplos de tipos de credenciales son contraseñas, tokens de un solo uso y certificados digitales.
- **Autorización:** Es la concesión de tipos específicos de servicio (incluido "ningún servicio") a un usuario, en función de su autenticación, los servicios que solicita y el estado actual del sistema. La autorización puede basarse en restricciones, por ejemplo, restricciones de hora del día o restricciones de ubicación física, o restricciones contra múltiples inicios de sesión por parte del mismo usuario. La autorización determina la naturaleza del servicio que se otorga a un usuario. Los ejemplos de tipos de servicio incluyen, entre otros:

filtrado de direcciones IP, asignación de direcciones, asignación de rutas, QoS / servicios diferenciales, control de ancho de banda / gestión de tráfico, tunelización obligatoria a un punto final específico y cifrado.

- **Certificado digital:** Un certificado digital es una estructura de datos firmada digitalmente, creada por un emisor, que vincula a un sujeto a otros atributos. Estos pueden ser usados para implementar control de acceso centrado en el usuario (Abdelmajid Lakbabi).
- **Cifrado:** Cifrado o encriptación es el proceso de convertir datos a una forma irreconocible o "cifrada". Se usa comúnmente para proteger información confidencial de modo que solo las partes autorizadas puedan verla. Esto incluye archivos y dispositivos de almacenamiento, así como datos transferidos a través de redes inalámbricas e Internet (TechTerms).
- **DMZ:** DeMilitarized Zone (Zona desmilitarizada) es el nombre que se le da a una red que debe estar expuesta hacia Internet, para la publicación de servidores web y otros servicios hacia usuarios externos.
- **Endpoint Detection Response (EDR):** Es la denominación de tecnologías de análisis de eventos que proporcionan monitoreo y detección en tiempo real de eventos maliciosos en endpoints (mayormente equipos de escritorio, laptops y servidores). No está basado en firmas sino en algoritmos que identifican comportamiento sospechoso y/o malicioso (Comodo, 2021).
- **Endpoint:** Un endpoint (punto final) es un dispositivo informático remoto que se comunica de ida y vuelta con una red a la que está conectado. Los ejemplos de puntos finales incluyen: PC de escritorio, laptops, smartphones, tabletas, servidores, dispositivos IoT. Los endpoints representan puntos de entrada clave

y vulnerables para los delincuentes informáticos, los que pueden aprovechar vulnerabilidades de seguridad de los sistemas operativos y software para obtener información o acceso a los mismos (PaloAlto, What is an Endpoint?).

- **Escritorio Remoto:** ver "Remote Desktop Protocol (RDP)".
- **Firewall:** Un firewall o cortafuegos s un dispositivo de seguridad de red que monitorea el tráfico de red entrante y saliente y permite o bloquea paquetes de datos según un conjunto de reglas de seguridad. Su propósito es establecer una barrera entre su red interna y el tráfico entrante de fuentes externas (como Internet) para bloquear el tráfico malicioso como virus y piratas informáticos (Forcepoint, What is a Firewall?).
- **Firma de virus:** También conocida como definición de virus, una firma de virus es la huella digital de un virus. Es un conjunto de datos únicos, o bits de código, que permiten identificarlo. El software antivirus utiliza una firma de virus para encontrar un virus en el sistema de archivos de una computadora, lo que permite detectar, poner en cuarentena y eliminar el virus. En un software antivirus, la firma del virus se denomina archivo de definición o archivo DAT (Computer Hope, 2021).
- **HardenedBSD:** HardenedBSD es una versión mejorada de FreeBSD (sistema operativo de código abierto) enfocada en seguridad, que nace el año 2014. HardenedBSD implementa muchas tecnologías de seguridad y mitigación de exploits adicionales a las que incluye FreeBSD (Vermaden, 2018).
- **IoT:** Internet de las cosas (Internet of Things) describe la red de objetos físicos ("cosas") que están integrados con sensores, software y otras tecnologías con el fin de conectar e intercambiar datos con otros dispositivos y sistemas a través

de Internet. Estos dispositivos van desde objetos domésticos ordinarios hasta sofisticadas herramientas industriales (Oracle).

- **IP:** IP o Internet Protocol es el protocolo mediante el cual se envían datos de una computadora a otra en Internet. Cada computadora en Internet tiene al menos una dirección IP que la identifica de manera única de todas las demás computadoras en Internet (Kerner).
- **ISP:** Internet Service Provide o Proveedor de Servicios de Internet, denomina a una empresa que brinda el servicio de conectividad internet a las instituciones y usuarios.
- **Llave de encriptación:** Una clave de cifrado suele ser una cadena aleatoria de bits generada específicamente para codificar y descifrar datos. Las claves de cifrado se crean con algoritmos diseñados para garantizar que cada clave sea única e impredecible. Cuanto más larga sea la clave construida de esta manera, más difícil será descifrar el código de cifrado (IBM).
- **LDAP:** LDAP (Lightweight Directory Access Protocol o Protocolo Ligero de Acceso a Directorios) es un protocolo abierto y multiplataforma que se utiliza para la autenticación de servicios de directorio. LDAP proporciona el lenguaje de comunicación que utilizan las aplicaciones para comunicarse con otros servidores de Servicios de Directorio. Los servicios de directorio almacenan los usuarios, contraseñas y cuentas de computadora, y comparten esa información con otros objetos en la red (Varonis).
- **Malware:** Abreviatura de software malicioso, el malware generalmente consiste en código desarrollado por delincuentes informáticos y diseñado para causar daños a los datos y sistemas o para obtener acceso no autorizado a los

recursos de una red. Algunos tipos de malware son los virus informáticos, gusanos, spyware, troyanos y ransonware (Forcepoint, What is Malware?).

- **MDM:** MDM es la abreviatura de Mobile Device Management, y se refiere a la administración de terminales móviles, como teléfonos inteligentes, tablets y computadoras portátiles (Miradore, 2020).
- **MFA:** La autenticación multifactor (MFA) es un control de seguridad que requiere que los usuarios verifiquen sus identidades proporcionando múltiples piezas de evidencia antes de obtener acceso a un dispositivo o aplicación (Help Systems, 2020).
- **NAT:** Network Address Translation, es una manera de mapear una (o varias) direcciones IP privadas a una dirección pública antes de transmitir información. Esta técnica se usa debido a que las direcciones IP versión 4 ruteables (números IP válidos en Internet) se agotaron hace varios años, y es necesario para permitir la conexión a internet de nuevos dispositivos, los que usan rangos de direcciones IP privadas (no ruteables en internet) tales como el rango 192.168.0.0/24, usualmente utilizado por empresas y domicilios.
- **On Premise:** "On premise" o "En las instalaciones" es un método de implementación de software en los equipos de una organización. Esto les brinda a los propietarios control físico sobre el hardware y software del servidor, sin un adicional por el acceso al mismo (Techslang).
- **Plataforma:** una plataforma es un grupo de tecnologías que son usadas como base para otras aplicaciones, procesos o servicios (Technopedia, Technopedia, 2020).

- **Protocolos de encriptación VPN:** juego de instrucciones usados cuando se establece una conexión segura entre dos dispositivos (cliente VPN y servidor VPN). Estos protocolos utilizan algún algoritmo criptográfico para realizar el cifrado de los datos transmitidos (Analytics Insight, 2019). Los más usados son:
    - **IKEv2:** es un protocolo de tunelización basado en IPSec que provee un canal de comunicación seguro y define medios de autenticación para VPNs (VPN Unlimited).
    - **IPSec:** Es un grupo de protocolos que se utilizan juntos para configurar conexiones cifradas entre dispositivos. Funciona encriptando paquetes IP, junto con la autenticación de la fuente de donde provienen los paquetes (Cloudflare).
    - **OpenVPN:** protocolo de código abierto, considerado muy seguro y configurable. Puede utilizar una amplia gama de algoritmos de cifrado, incluyendo AES.
    - **PPP / PPTP:** El protocolo punto a punto (PPP) y el protocolo de tunelización punto a punto (PPTP). Es posiblemente el más rápido de los algoritmos actuales, pero no es muy utilizado por mantener muchos problemas de seguridad conocidos (Wikipedia).
    - **Wireguard:** un protocolo reciente, considerado rápido y seguro, aunque ha entrado en su primera versión de producción en enero de 2020.
- **QR:** Un código QR (abreviatura de "quick response" o código de respuesta rápida) es un tipo de código de barras que contiene una matriz de puntos. Se

puede escanear con un escáner QR o un teléfono inteligente con cámara incorporada. Una vez escaneado, el software del dispositivo convierte los puntos dentro del código en números o una cadena de caracteres (TechTerms, QR Code).

- **Remote Desktop Protocol (RDP):** El protocolo RDP o Protocolo de Escritorio Remoto permite el acceso a un computador remoto para interactuar con el escritorio del mismo. Microsoft Windows utiliza este protocolo. Este protocolo utiliza el puerto TCP 3389 (TechTerms, Remote Desktop).
- **SaaS (Software as a Service):** Es un método de entrega de software que permite acceder a los datos desde cualquier dispositivo con conexión a Internet y un navegador web. En este modelo de servicio basado en web, los proveedores de software alojan y mantienen los servidores, las bases de datos y el código que forma una aplicación (Short, 2020).
- **Sandbox / Sandboxing:** En seguridad informática, es el proceso de ejecutar código potencialmente inseguro en un ambiente aislado (mayormente una máquina virtual) para observar su comportamiento (ProofPoint).
- **Site-to-Site VPN:** Es el método de establecer una conexión segura entre dos o más sitios físicos alejados sobre Internet.
- **TOTP:** La contraseña de un solo uso basada en tiempo (Time-based One-Time Password - TOTP) es un código de acceso de un solo uso que generalmente se usa para autenticar a los usuarios. Al usuario se le asigna un generador TOPT entregado como un llavero de hardware o una app de software. El generador implementa un algoritmo que calcula un código de acceso de una sola vez utilizando un código secreto compartido con el servidor de autenticación y la

hora actual. Por ello, es importante que tanto los clientes como el servidor de acceso se encuentren sincronizados (normalmente contra un servidor de tiempo internacional). Este algoritmo está estandarizado en la RFC 6238 (DoubleOctopus).

- **OpenSSL:** Es un conjunto de herramientas de código abierto de nivel comercial, con soporte para las funciones de los protocolos Transport Layer Security (TLS) y Secure Sockets Layer (SSL). También es una biblioteca de criptografía de uso general.
- **OPNsense:** Plataforma de firewall de código abierto, con funciones de autenticación de usuarios, administración de certificados digitales y servicios VPN.
- **UTM:** acrónimo de Unified Threat Management (Administración Unificada de Amenazas). Describe un producto que posee varias tecnologías de seguridad integradas tales como firewall, antimalware y VPN.
- **VPN:** Virtual Private Network o Red Privada Virtual, es la tecnología que permite el establecimiento de una conexión segura y privada sobre Internet, ya sea para usuarios o de sitio a sitio.

CAPÍTULO III. DESCRIPCIÓN DE LA EXPERIENCIA

Desde el año 2007 he laborado en el Departamento de Tecnologías de Información (DTI) del Congreso de la República de manera no continua, habiendo acumulado hasta el momento 12 años de experiencia en la institución. El Departamento de Tecnologías de la Información se compone de tres áreas:

- **Operaciones:** encargada del soporte a usuarios, al parque de equipos de cómputo y accesorios como escáner e impresoras, así como la custodia e instalación de licencias de software.
- **Proyectos:** esta área se encarga del desarrollo y mantenimiento de aplicaciones in-house, así como de la supervisión y apoyo a contratistas externos para proyectos de desarrollo de software.
- **Infraestructura Tecnológica:** administra la red de datos institucional, el equipamiento de redes central y de borde, wifi, cableado estructurado, así como la administración de los dos centros de datos y los servicios brindados en los mismos.

He desempeñado labores en las tres áreas que componen el departamento: Operaciones (soporte a equipos de cómputo), Proyectos (análisis de sistemas de asistencia y votación) y principalmente en el área de Infraestructura Tecnológica, donde realizo la administración de servicios (balanceadores de enlaces a internet, de aplicaciones, virtualización y correo, entre otros) así como la administración e implementación de servidores en los centros de datos de la institución. Como parte de mis funciones realizo tareas de investigación de productos, cuadros comparativos y la redacción de Especificaciones Técnicas Mínimas para procesos de adquisición de equipamiento y contratación de servicios. En el transcurso de mis labores en la institución he tenido la oportunidad de liderar y participar en varios proyectos.

3 DESCRIPCIÓN DE LA EXPERIENCIA

3.1 DESCRIPCIÓN DE LA SITUACIÓN INSTITUCIONAL

Tal como se explicó en el contexto del cap. 1, la emergencia sanitaria COVID-19 ha generado problemas tecnológicos a ser enfrentados por las empresas e instituciones a nivel mundial. En el caso del Congreso de la República, desde la declaración de emergencia sanitaria el 11 de marzo de 2020, la jefatura del DTI dispuso se evalúen productos y se implementen soluciones para cubrir las necesidades de:

- **Colaboración remota:** para poder cubrir las necesidades de comunicación básicas y colaboración entre equipos de trabajo tanto del Servicio Parlamentario como la Organización Parlamentaria, se evaluaron alternativas para ser utilizadas como plataforma oficial de videoconferencias y así garantizar el desarrollo de las actividades legislativas. De este modo, tras la evaluación de diferentes soluciones, se le brindaron a la alta dirección dos alternativas, aprobándose finalmente el uso de la plataforma colaborativa Microsoft Teams para el desarrollo de sesiones de Comisiones Ordinarias. Con el apoyo de Microsoft Perú, se estableció un sistema corporativo de gestión de usuarios, se utilizaron las capacidades de videoconferencia de Microsoft Teams, distribución de documentos mediante Sharepoint integrado a la plataforma y acceso mediante credenciales y segundo factor de autenticación basado en TOTP con la app móvil Microsoft Authenticator.

Figura 21

Sesión de Comisión de Fiscalización en Microsoft Teams.

Fuente: Elaboración propia.

- **Acceso Remoto Seguro:** tras el despliegue exitoso de la plataforma Microsoft Teams, se inició el trabajo de las Comisiones Ordinarias y el Pleno del Congreso. Desde fines del mes de abril de 2020 se inició el despliegue de clientes del producto de acceso remoto VPN "Checkpoint Enterprise Endpoint Security" según el número de licencias disponibles en el equipamiento de seguridad perimetral (firewall) de la marca Checkpoint modelo 4200, las cuales alcanzaban el número de 40. Cabe resaltar que, hasta ese momento, la incidencia de trabajo remoto en la institución era prácticamente nula. Así, este número de usuarios contaron con acceso remoto a través de internet al escritorio de cada PC de la institución asignada, las cuales se debieron mantener encendidas desde ese momento.

  Debido al número limitado de licencias disponibles del producto "Checkpoint Enterprise Endpoint Security", se dispuso el uso de clientes VPN adicionales Checkpoint configurados en la modalidad "Remote Access", los cuales no requieren

licenciamiento, pero carecen de las características adicionales de seguridad disponibles en la licencia Enterprise. Asimismo, se detallan las siguientes limitaciones al utilizar esta solución:

- **Rendimiento:** la solución de firewall Checkpoint adquirida el 2010 fue dimensionada para uso de seguridad perimetral de acceso a Internet y publicación de servidores hacia Internet. Al hacer uso del servicio de VPN, se comprobó la saturación del uso de CPU y memoria del firewall.
- **Seguridad:** el sistema de VPN disponible en el equipamiento Checkpoint no soportaba métodos de encriptación vigentes ni métodos de autenticación de múltiple factor deseados.
- **Integración:** el sistema carecía de los medios de integración con el sistema de usuarios existente en la institución (LDAP del Directorio Activo Microsoft) por lo que se debía mantener manualmente el alta y baja de usuarios y contraseñas, con la consecuente carga administrativa asociada.

Debido a estas limitaciones y teniendo al mes de junio de 2020 más de 200 usuarios realizando labores remotas mediante VPN y acceso a escritorio remoto, la Jefatura del DTI dispuso que el Área de Infraestructura Tecnológica la implementación de un Sistema de Acceso Remoto Seguro que reemplace al utilizado hasta ese momento. Así, la jefatura de Infraestructura Tecnológica me encargó la coordinación de este proyecto.

3.2 OBJETIVO

3.2.1 OBJETIVO PRINCIPAL:

Implementar OPNsense como la plataforma de Acceso Remoto Seguro en el Congreso de la República.

3.2.2 OBJETIVOS ESPECÍFICOS:

- Brindar acceso remoto a los usuarios del Servicio Parlamentario y Organización Parlamentaria, tanto a sus equipos institucionales como a los servicios web internos (Intranet, Sistema de Trámite Documentario, SIGA).
- Dar acceso remoto a los servicios web utilizados por la nueva plataforma de Asistencia y Votación Remota para los teléfonos inteligentes de los Congresistas.
- Dar acceso remoto a los servidores de desarrollo y pruebas a los equipos de Desarrollo de Software.
- Permitir el registro de un mínimo de 500 usuarios, así como permitir el acceso concurrente de al menos 100 usuarios de escritorio remoto del Servicio Parlamentario manteniendo la calidad de servicio.
- Garantizar la conexión concurrente de al menos el 90% de los dispositivos móviles asignados a los congresistas durante el desarrollo de las sesiones del Pleno del Congreso.

3.3 FACTORES Y LIMITANTES

3.3.1 PRESUPUESTO ECONÓMICO

Debido a que no se contaba con presupuesto para una solución de acceso remoto programada para el año 2020, se debió implementar una solución que no genere impacto

económico alguno a la institución. Por lo tanto, la evaluación de tecnologías se limitó a proyectos sin costo (incluidos en los sistemas operativos o de código abierto).

HARDWARE

Se dispuso que las pruebas se desarrollaran sobre un servidor IBM x3850 adquirido el año 2006 (en ese momento en desuso) que dispone de 4 tarjetas de red (1Gb Ethernet) y 2 procesadores Intel Xeon DP de 4 cores cada uno.

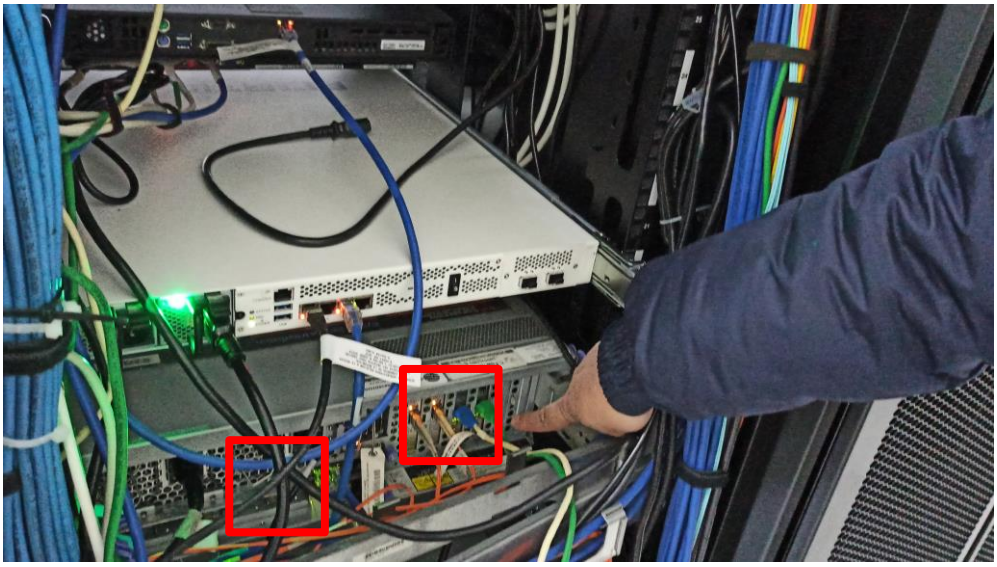
Figura 22

Vista frontal de servidor IBM x3850.

Fuente: elaboración propia

Figura 23

Conexiones LAN del servidor IBM x3850.



Fuente: elaboración propia

Figura 24

Rack de servidores y comunicaciones del Centro de Datos Edificio LAS.

Fuente: elaboración propia

3.3.2 PLAZO

El proyecto de implementación del Sistema de Acceso Remoto Seguro se debió realizar en un plazo máximo de tres meses.

3.3.3 IMPLEMENTACIÓN Y SOPORTE:

El proyecto se debió llevar a cabo en su totalidad con recursos internos del Área de Infraestructura Tecnológica.

3.4 DESARROLLO DEL PROYECTO

3.4.1 ETAPA 1: DETERMINACIÓN DE FUNCIONALIDADES REQUERIDAS

De acuerdo a lo indicado en el punto 2.3 del marco teórico, existieron tres aspectos a tener en cuenta para implementar Acceso Remoto Seguro. Con respecto a ellos, se evaluó el estado de cada uno de ellos en la institución.

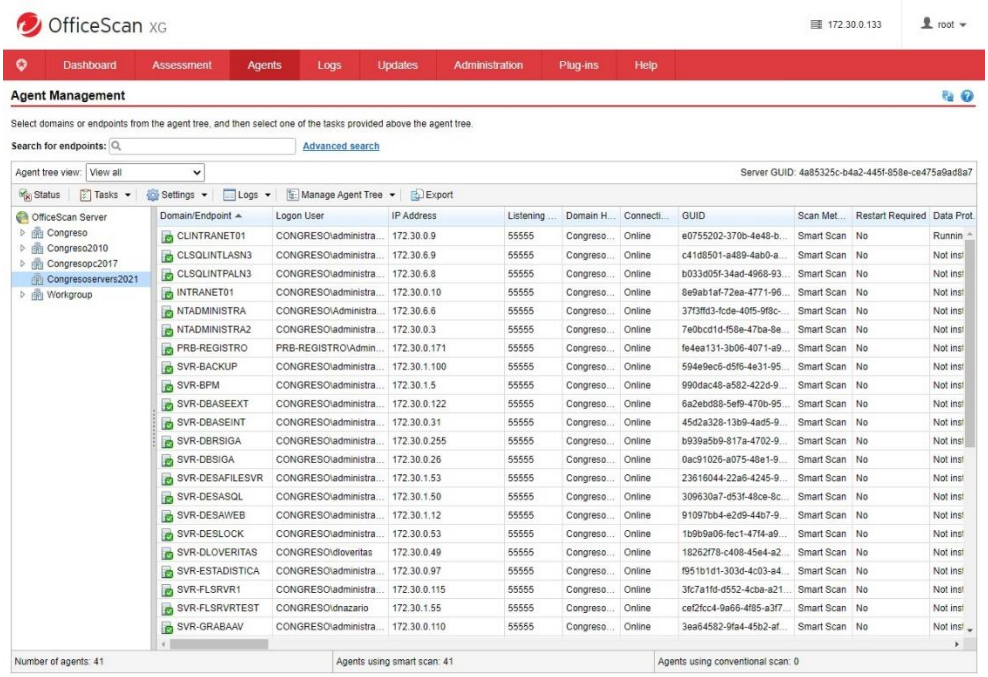
SEGURIDAD DE ENDPOINT

a. **ANTIVIRUS**

El Congreso de la República dispone de un paquete de 2000 licencias del software antivirus Trendmicro OfficeScan adquiridas para el uso en servidores Windows y Linux y que cuenta con una plataforma centralizada de gestión y alertas. Debido a que sólo se encuentraban en uso alrededor de 100 licencias, se dispuso que se instalara el cliente antivirus en los equipos remotos de los usuarios institucionales, ya sean estos equipos provistos por el Congreso o de propiedad de los usuarios.

Figura 25

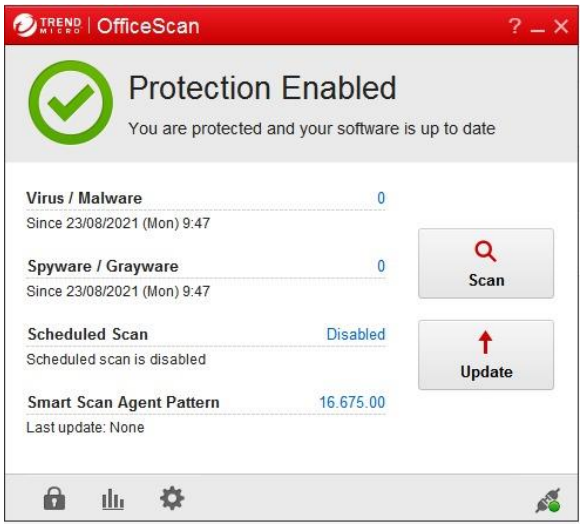
Consola de administración de Antivirus TrendMicro.



Fuente: elaboración propia.

Figura 26

Cliente antivirus TrendMicro OfficeScan.



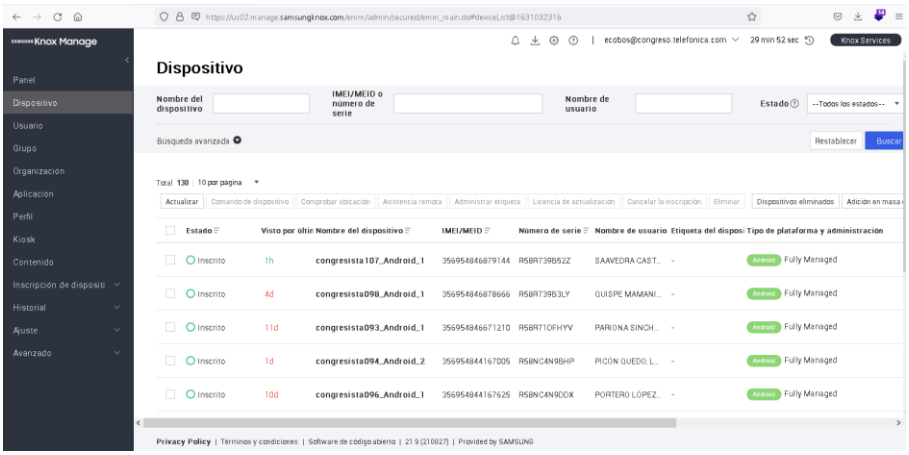
Fuente: elaboración propia.

b. **MOBILE DEVICE MANAGEMENT (MDM)**

Los dispositivos móviles Samsung modelo A21s contratados con el proveedor Telefónica del Perú cuentan con licenciamiento para el uso del MDM Samsung KnoxManage, el cual se desplegó en los teléfonos inteligentes que fueron entregados a los señores congresistas, los cuales son los únicos permitidos para acceder de manera remota, específicamente para su uso con el nuevo sistema de Asistencia y Votación Remota.

Figura 27

Pantalla de administración de MDM Samsung KnoxManage.



Fuente: elaboración propia.

Figura 28

Pantalla de cliente MDM en teléfono Android.

Fuente: elaboración propia.

RED PRIVADA VIRTUAL (VPN)

Este proyecto contempló el despliegue de una nueva solución que brinde acceso VPN a los usuarios, y que implemente los métodos de seguridad indicados en el cap. 2.

CONTROL DE ACCESO

Este proyecto consideró la necesidad de usar al menos doble factor de autenticación, la integración con el directorio de usuarios institucional, así como la necesidad de permitir acceso a los clientes solo a los recursos permitidos.

Como resultado de esta evaluación se verificó que, de los tres aspectos tecnológicos necesarios para Acceso Remoto Seguro, la institución contaba con el software necesario para cubrir el punto 1 (Seguridad de Endpoint). Por consiguiente, las funcionalidades requeridas para este proyecto se refirieron a las tecnologías de los puntos 2 (Red Privada Virtual) y 3 (Control de Acceso).

En base a las limitaciones de la solución VPN Checkpoint listadas en el punto 3.1, se procedió a redactar las funcionalidades mínimas deseadas en una nueva solución de Acceso Remoto Seguro.

3.4.1.1 FUNCIONALIDADES REQUERIDAS

1. **ACCESO**

   Brindar acceso remoto a:

   - Recursos computacionales de la institución, tales como sus PC (escritorio remoto).
   - Servicios web como la Intranet institucional, el Sistema de Trámite Documentario, SIGA y HelpDesk.
   - Servidores de desarrollo para el personal del Área de Proyectos del Departamento de Tecnologías de la Información.
   - Servicios de la nueva plataforma de Asistencia y Votación Remota para los congresistas.

2. MULTIPLATAFORMA

Soporte a las conexiones de:

- Clientes de escritorio (Microsoft Windows, Apple Mac).
- Clientes móviles (Android, iOS).

3. INTEGRACIÓN

- Debía poder integrarse con la infraestructura existente sin cambios que requieran costos adicionales ni cambios profundos en la configuración.
- Se debía integrar con el directorio institucional (Microsoft Active Directory) para autenticación de usuarios.

4. SEGURIDAD

Implementar:

- Tecnologías de seguridad VPN vigentes.
- Cifrado robusto.
- Al menos dos factores de autenticación.
- Acceso a los usuarios solamente a los recursos a los que están autorizados.

5. RENDIMIENTO

Soportar:

- Un mínimo de 500 usuarios registrados
- Al menos 100 usuarios de escritorio remoto concurrentes
- Garantizar la conexión VPN concurrente de al menos el 90% de los dispositivos móviles de los congresistas asignados para el nuevo sistema de Asistencia y Votación Remota.

6. ADMINISTRACIÓN

Debía permitir la administración mediante un entorno GUI basado en web, no siendo necesario el uso de CLI para tareas de rutina.

3.4.2 ETAPA 2: EVALUACIÓN DE PRODUCTOS

En base a las funcionalidades requeridas en el punto 3.4.1.1, se procedió a identificar las plataformas de código abierto existentes que podrían cumplir las características solicitadas. Para ello, se realizó la investigación en internet de productos de seguridad. Se listan a continuación los productos que fueron seleccionados para la evaluación.

Tabla 2

Lista de plataformas de seguridad a evaluar

Plataforma	*URL*	*Descripción*
pfsense	https://www.pfsense.org/	Plataforma basada en FreeBSD con servicios de redes tales como firewall, enrutador, servidor de balanceo de carga entre otras.https://www.techrepublic.com/a/hub/i/2017/06/16/37aff2a8-ea77-42d6-a3ab-1602f64a183b/wordtablelisti.jpg
OPNsense	https://opnsense.org/	Plataforma de firewall basada en HardenedBSD con funciones de autenticación de usuarios, administración de certificados digitales y servicios VPN.
Endian Firewall Community	https://www.endian.com/	Plataforma de código abierto que permite implementar UTM que contiene firewall, antivirus y VPN. Existe en versiones Community (libres) y de pago.
NethServer Small Business Server Community	https://www.nethserver.org/	Distribución Linux basada en RedHat sobre la que se pueden implementar servicios como firewall y VPN. Existe en versiones Community (libres) y de suscripción.

Fuente: elaboración propia

A continuación, se evaluaron las versiones sin costo de los productos de la Tabla 2 contra las funcionalidades requeridas.

3.4.2.1 METODOLOGÍA DE EVALUACIÓN

Debido a los cortos plazos para el desarrollo del proyecto, se realizó una evaluación de escritorio en base a la documentación oficial existente, evaluaciones de internet y experiencia propia con los productos, no pudiéndose realizar pruebas de instalación de los productos para compasión de rendimiento y funcionalidades.

3.4.2.2 COMPARACIÓN Y EVALUACIÓN DE PRODUCTOS

Tabla 3

Evaluación de plataformas de seguridad

Funcionalidades	Plataformas			
	pfsense	OPNsense	Endian Firewall Community	NethServer SBS Community
	Resultados			
Control de acceso				
Implementación de firewall y VPN	Si cumple	Si cumple	Si cumple	Si cumple
Multiplataforma				
Software cliente multiplataforma	Si cumple	Si cumple	Si cumple	Si cumple
Integración				
Integración con equipos de red y seguridad existentes	Si cumple	Si cumple	Si cumple	Si cumple
Integración con LDAP Active Directory para autenticación VPN	No cumple (requiere modificar archivos manualmente, bajo rendimiento)	Si cumple	No cumple (disponible sólo en versión de pago) (Endian)	No cumple
Seguridad				
VPN vigente	Si cumple (IPSec / OpenVPN)	Si cumple (IPSec / OpenVPN)	Si cumple (OpenVPN)	Si cumple (OpenVPN)
Cifrado robusto	Si cumple (OpenSSL)	Si cumple (OpenSSL / LibreSSL)	Si cumple (OpenSSL)	Si cumple (OpenSSL)
Doble factor de autenticación	Si cumple (TOTP)	Si cumple (TOTP)	No cumple	No cumple

			(disponible sólo en versión de pago) (Endian)	
Administración				
GUI basado en web	Si cumple	Si cumple	Si cumple	Si cumple
Evaluación final	**No cumple**	**Si cumple**	**No cumple**	**No cumple**

Fuente: elaboración propia

COMENTARIOS

Pfsense / OPNsense: los productos pfsense y OPNsense son similares, al compartir el mismo origen (OPNsense es una derivación de pfsense). Sin embargo, elementos como los motores de autenticación de usuarios y la interface gráfica de OPNsense han sido reescritos por completo, lo que se traduce en una mejor experiencia de usuario. Asimismo, como experiencia propia, comparé de manera práctica los productos el año 2019 en otra institución pública (para la implementación de una plataforma de proxy de acceso a internet con control de contenido) y pude determinar que OPNsense tiene un robusto motor de autenticación de usuarios con integración a Microsoft Active Directory, mientras que pfsense necesitó de una configuración a nivel de archivos de texto para alcanzar una funcionalidad similar, brindando eventualmente un rendimiento notablemente inferior.

Endian: esta plataforma posee una interface web de usuario muy avanzada y amigable comparada con los demás productos evaluados, pero algunas funcionalidades necesarias permanecen bloqueadas, solo accesibles para la versión de pago (Endian).

NethServer: es un Small Business Server (Servidor de Pequeñas Empresas) que posee muchas funcionalidades incluso en su versión gratuita, sin embargo, es un producto de propósito general que no solo ofrece tecnologías de seguridad sino servicios tales como correo electrónico, central telefónica IP, servidor de chat, nube

privada, entre otros. Es una buena opción si se tiene la necesidad de disponer de esos servicios y califica como una plataforma de seguridad, pero no dispone de algunas características especializadas (NethServer).

Rendimiento: no se pudieron realizar pruebas comparativas ni de stress de los productos, la evaluación se limitó a la documentación de dimensionamiento y rendimiento existente y la experiencia de terceros al respecto. Se determinó que, con el hardware adecuado, todas las plataformas pueden ofrecer el rendimiento solicitado.

Producto elegido para realizar la prueba de concepto: OPNsense.

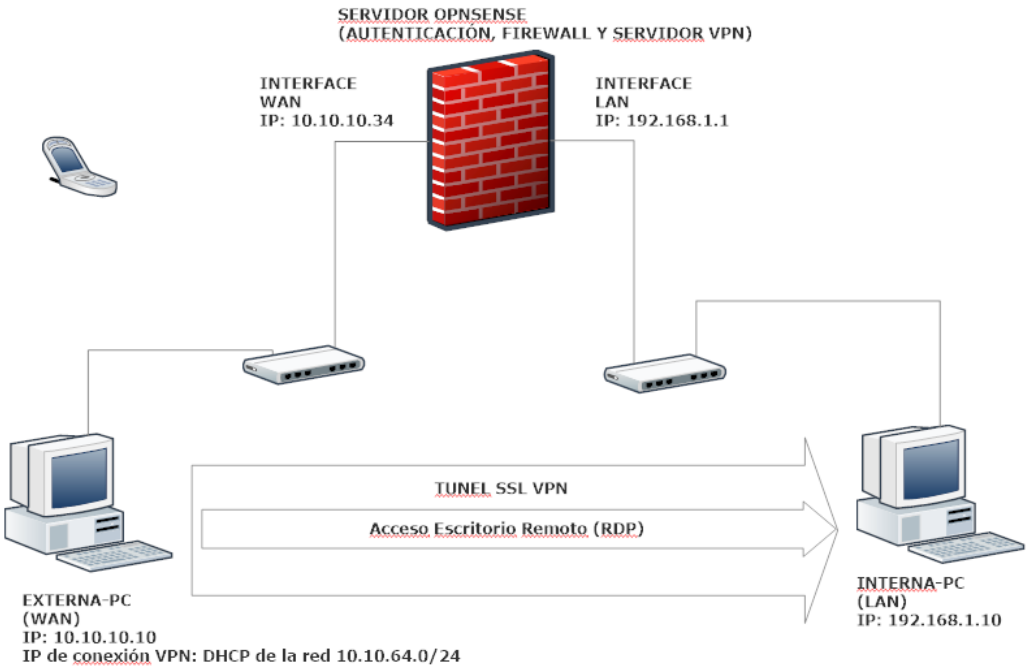
3.4.3 ETAPA 3: PRUEBA DE CONCEPTO

Para la prueba de concepto se trabajó con tres máquinas virtuales:

- 01 PC Externa para simular cliente VPN (Windows 7).
    - Una tarjeta de red en switch virtual WAN. Nro. IP: 10.10.10.10
- 01 PC Interna para simular PC de oficina a ser accedida por escritorio remoto (Windows 7).
    - Una tarjeta de red en switch virtual LAN. Nro. IP: 192.168.1.10
- 01 servidor OPNsense versión 20.1
    - Una tarjeta de red en switch virtual WAN. Nro. IP: 10.10.10.34
    - Una tarjeta de red en switch virtual LAN. Nro. IP: 192.168.1.1

Figura 29

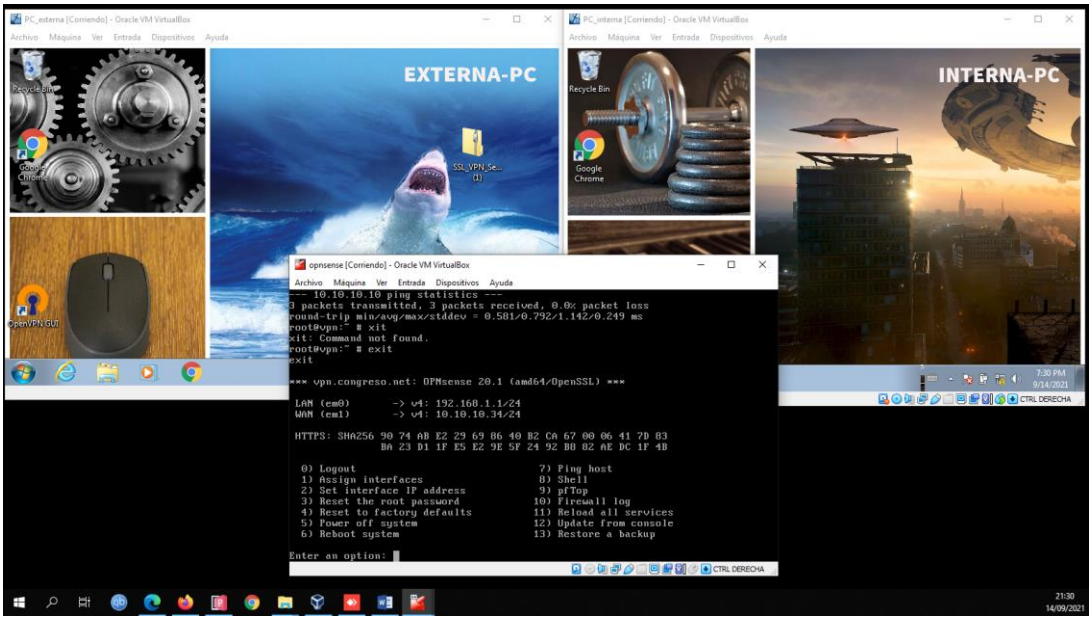
Esquema de la prueba de concepto.



Fuente: elaboración propia.

Figura 30

Pantallas de las 3 máquinas virtuales.



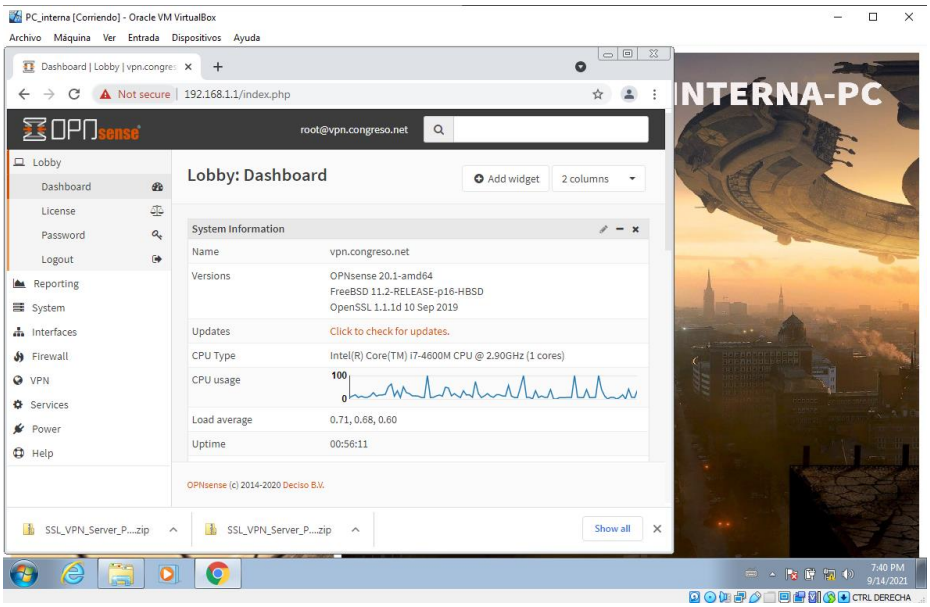
Fuente: elaboración propia.

Pasos realizados:

- En ambos computadores Windows 7 se instaló el navegador Google Chrome.
- En la PC externa se instaló el cliente de VPN OpenVPN 2.5.3.
- En la PC interna se habilitó el acceso remoto.
- Una vez instalado OPNsense, se procedió a configurarlo desde la PC interna (red LAN).

Figura 31

Configuración vía web de OPNsense.

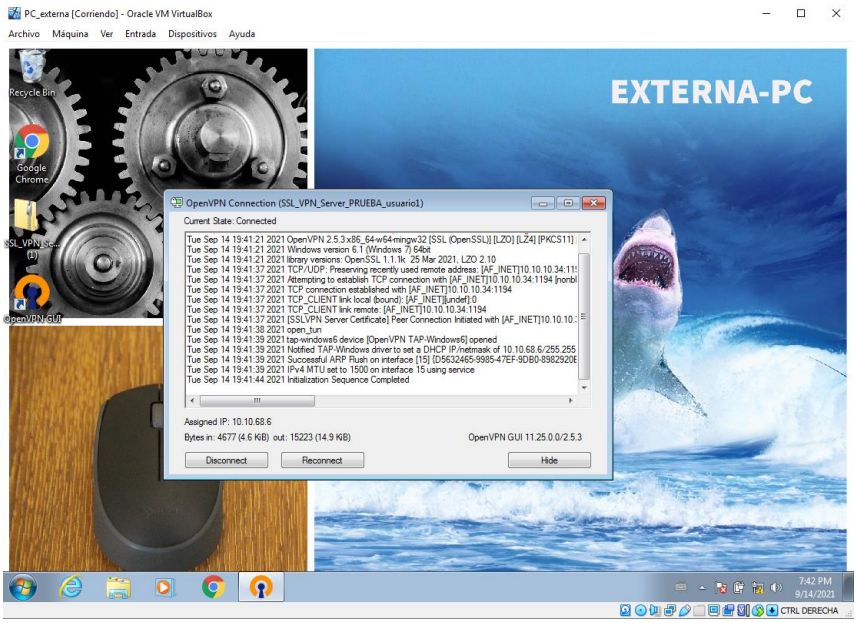


Fuente: elaboración propia.

- Se realizaron múltiples pruebas de configuración (acceso VPN, reglas de firewall, múltiple factor de autenticación, entre otras). Se identificaron todos los aspectos de la configuración que se alineaban con los requerimientos establecidos. Estas configuraciones fueron la base del producto final.
- Durante las pruebas, se exportó el archivo de configuración de cliente de la PC interna a la PC externa, donde se configuró el cliente OpenVPN (cuantas veces fue necesario).
- Se probó el acceso VPN desde la PC externa a la PC interna, y luego el acceso al escritorio remoto.

Figura 32

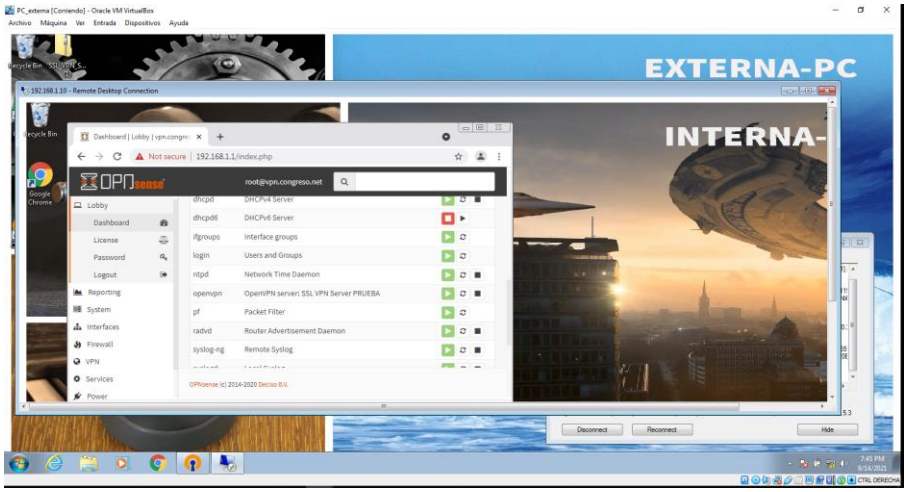
Prueba de conexión VPN en PC externa.



Fuente: elaboración propia.

Figura 33

Acceso remoto a la PC interna desde la PC externa vía VPN.



Fuente: elaboración propia.

3.4.4 ETAPA 4: PLANIFICACIÓN DE CONECTIVIDAD E INTEGRACIÓN

Una vez demostrado el funcionamiento del acceso VPN en la prueba de concepto, se procedió a planificar los requerimientos técnicos a ser configurados durante el despliegue e integración de la plataforma OPNsense con la infraestructura tecnológica del Congreso. En esta etapa, se contó con la participación del jefe y un técnico del área de Infraestructura Tecnológica. Los puntos coordinados fueron:

- **NETWORKING VPN A RED INTERNA**
    - Planificación de la conectividad de la plataforma OPNsense con respecto a la infraestructura de seguridad perimetral.
    - Definición de configuración de red: redes a ser utilizadas, gateways y rutas estáticas para el funcionamiento de la VPN.
    - Conectorización a switches de red correspondientes.
- **CONTROL DE ACCESO**
    - Determinación de factores de autenticación a implementar.
    - Determinación de los controles de acceso a red: enumeración de recursos y granularidad del control de acceso a los recursos a ser controlados por firewall.
    - Requerimientos para la integración con el Active Directory.

Figura 34

Coordinaciones con el Jefe de Infraestructura Tecnológica.

Fuente: elaboración propia.

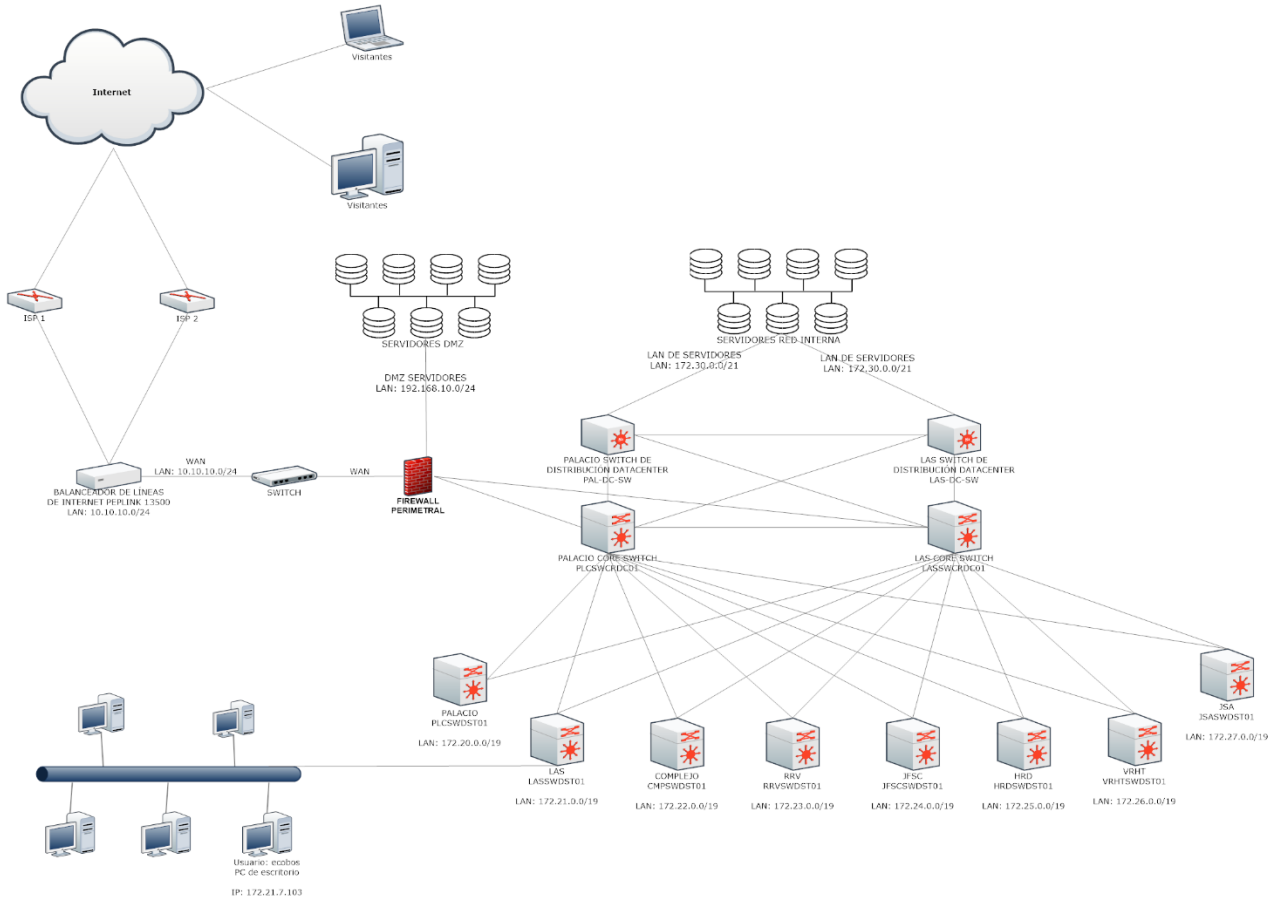
3.4.4.1 NETWORKING VPN A RED INTERNA

Las instalaciones del Congreso se encuentran distribuidas en ocho edificios en el Centro de Lima, interconectados mediante líneas de fibra óptica, y cuenta con dos centros de datos que se encuentran interconectados de manera redundante, lo que permite tener equipos (servidores, almacenamiento de datos y comunicaciones) operativos indistintamente tanto en los edificios Palacio Legislativo como Luis Alberto

Sánchez, conformando una sola red de servidores. A continuación, se muestra el esquema de la red del Congreso.

Figura 35

Esquema de red del Congreso.



Fuente: elaboración propia

En el esquema se muestran:

- El clúster de switches de Core.
- El clúster de switches de distribución de los Centros de Datos.
- Los switches de distribución de cada edificio (8 edificios)
- Los rangos de red de cada edificio.

- Un ejemplo de LAN de un edificio, con una PC de usuario (edificio Luis Alberto Sánchez).
- La conectividad hacia Internet: se cuenta con un clúster de firewalls en alta disponibilidad activo-activo (representados en el gráfico como un solo firewall), el equipo balanceador de líneas de Internet, así como los routers de los dos ISP.

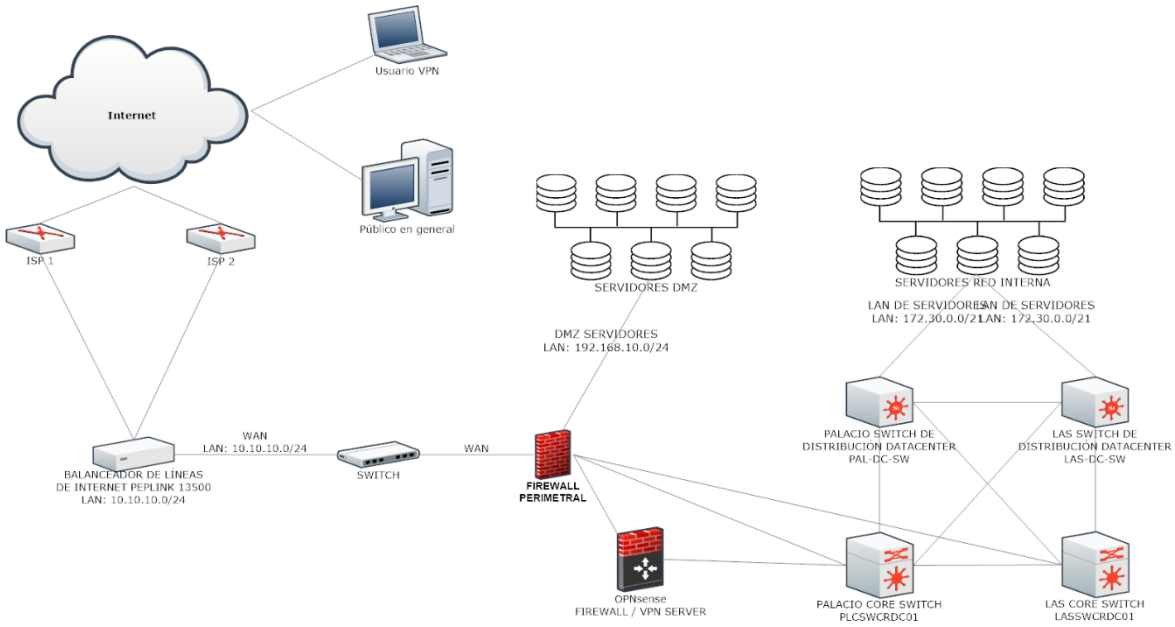
Se evaluaron tres alternativas de conectividad para la integración de la plataforma OPNsense en este esquema. A continuación, se muestran los esquemas de las tres alternativas, y se discute los pros y contras de cada una con respecto a la seguridad, mostrando finalmente la alternativa elegida.

1. ALTERNATIVA 1: DETRÁS DEL FIREWALL

En esta alternativa se propuso colocar la plataforma de Acceso Remoto Seguro detrás del firewall, de manera que las comunicaciones externas fueran recibidas primero por el firewall perimetral.

Figura 36

Alternativa 1 OPNsense detrás de firewall perimetral.



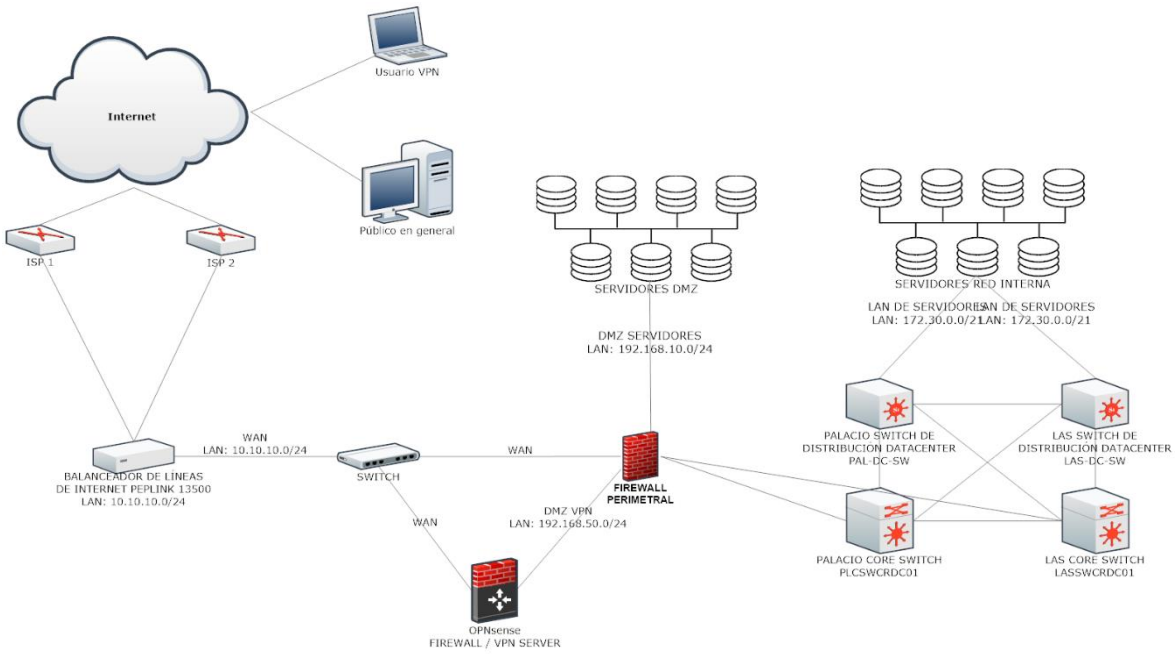
Fuente: elaboración propia

2. ALTERNATIVA 2: DELANTE DEL FIREWALL

En esta alternativa se propuso colocar la plataforma de Acceso Remoto Seguro delante del firewall, permitiendo que las conexiones de los clientes VPN se realicen directamente hacia la plataforma OPNsense, la cual se conectaría al firewall perimetral.

Figura 37

Alternativa 2 OPNsense delante de firewall perimetral.



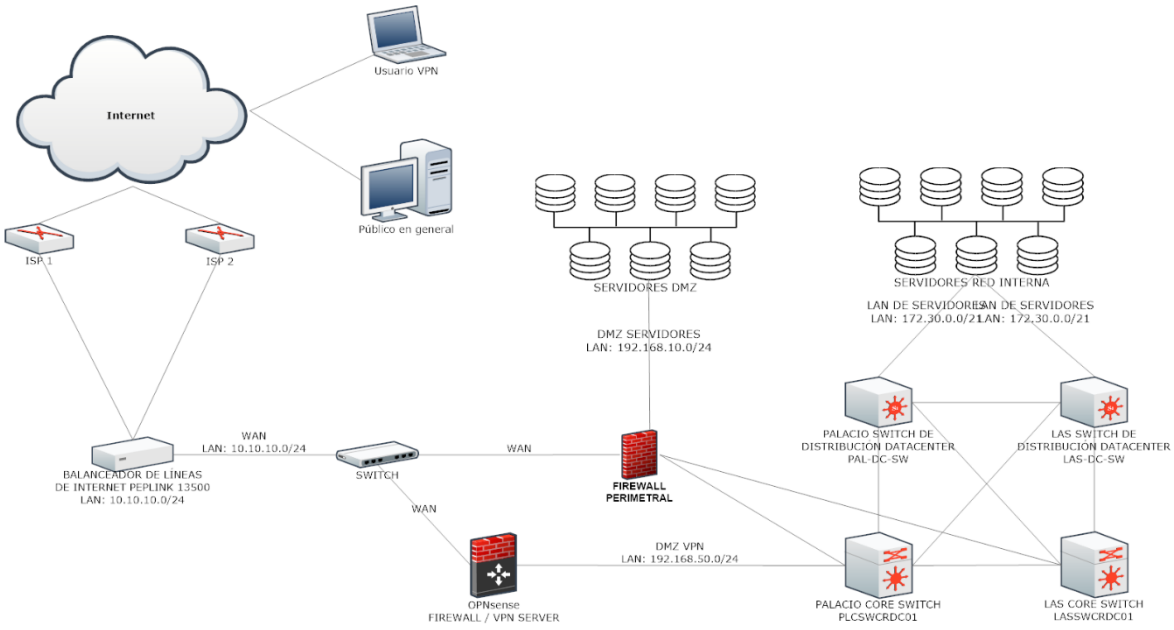
Fuente: elaboración propia

3. ALTERNATIVA 3: CONEXIÓN DIRECTA A LA LAN INTERNA

En esta alternativa se propuso colocar la plataforma de Acceso Remoto Seguro directamente a la LAN interna, evitando así el pase de comunicaciones a través del firewall perimetral.

Figura 38

Alternativa 3 conexión OPNsense directa a la LAN.



Fuente: elaboración propia

3.4.4.1.1 EVALUACIÓN DE LAS ALTERNATIVAS

En base a las tres alternativas propuestas, conjuntamente con la jefatura del área se realizó la evaluación de las mismas con respecto al pro y contra de cada una de ellas, con respecto a aspectos de seguridad e impacto en la configuración actual de la red.

Tabla 4

Evaluación de alternativas de conectividad de OPNsense

Características	Alternativas de despliegue		
	Alternativa 1 Detrás de FW	Alternativa 2 Delante de FW	Alternativa 3 Directo a LAN
Seguridad (Alta es mejor)	**Alta:** se dispondría de dos firewalls de acceso, uno especializado en VPN y el firewall perimetral	**Alta:** se dispondría de dos firewalls de acceso, uno especializado en VPN y el firewall perimetral	**Media:** sólo se contaría con un firewall entre los clientes remotos y la LAN del Congreso.
Impacto en configuración (Bajo es mejor)	**Alto:** Además de configuraciones en los firewall perimetral y OPNsense, se tendría que hacer trabajos de ruteo en el clúster de switches de core de los centros de datos.	**Bajo:** solo se configuran rutas entre los firewalls OPNsense y perimetral.	**Alto:** se tendría que hacer trabajos de ruteo en OPNsense y el cluster de switches de core de los centros de datos, lo que puede afectar el funcionamiento de la red interna.
Granularidad de control de acceso (Alta es mejor)	**Bajo:** al estar detrás del firewall perimetral, no se podrían configurar reglas de firewall	**Alto:** se pueden crear reglas de firewall granulares para control de acceso de los usuarios.	**Alto:** se pueden crear reglas de firewall granulares para control de acceso de los usuarios.

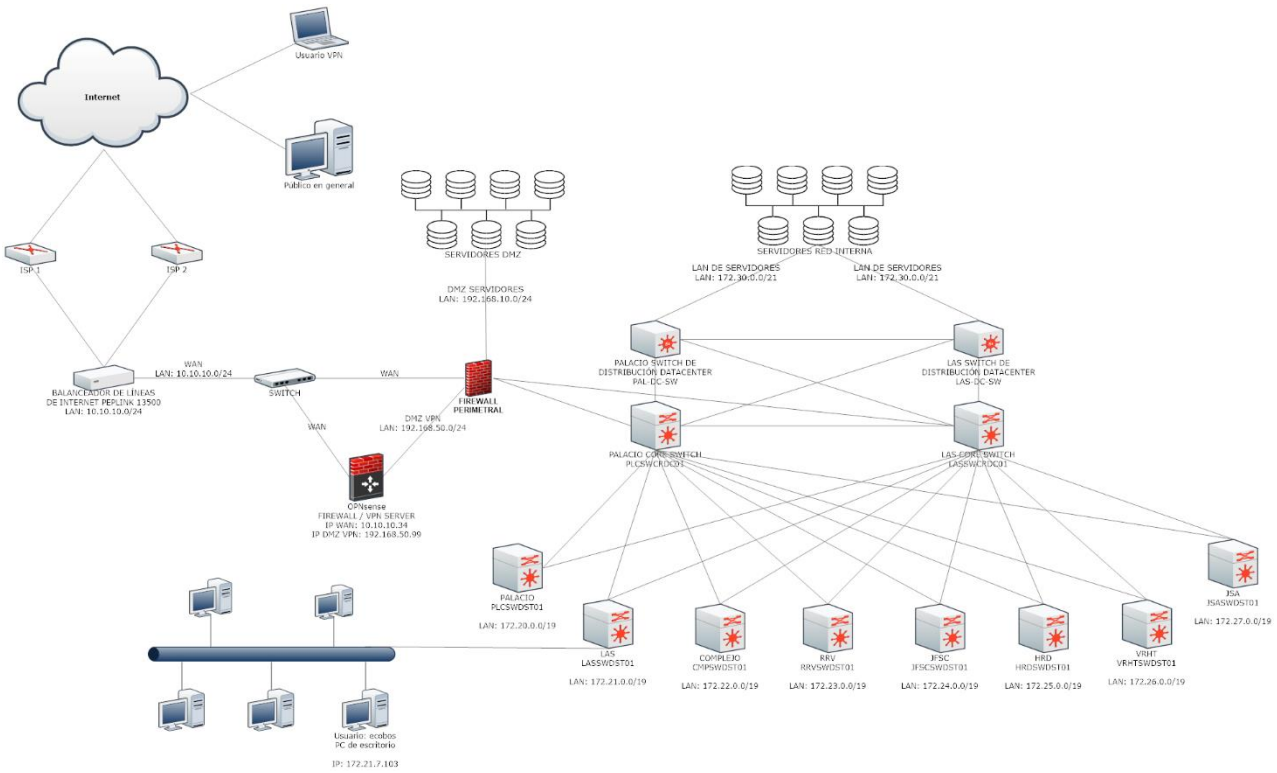
	granulares por usuario.		
Impacto en conectividad física (Bajo es mejor)	**Alto:** requiere interconectar el servidor OPNsense con interfaces ethernet de cobre hacia los switches de core de fibra óptica.	**Bajo:** sólo requiere conectividad de interfaces ethernet de cobre hacia los switches y firewall existentes.	**Alto:** requiere interconectar el servidor OPNsense con interfaces ethernet de cobre hacia los switches de core de fibra óptica.
Determinación: Mejor alternativa	**NO**	**SI**	**NO**

Fuente: elaboración propia

Definida la elección de la Alternativa 2, se muestra el esquema de red final.

Figura 39

Esquema de red final.



Fuente: elaboración propia

Como se aprecia en la figura, se creó una nueva red DMZ llamada DMZ VPN, por la cual fluye el tráfico de los clientes VPN desde internet. El flujo fue el siguiente:

- Acceso de un dispositivo remoto desde internet usando software cliente VPN OpenVPN.
- El equipo balanceador de internet deriva las comunicaciones VPN hacia OPNsense.
- La plataforma OPNsense:

- *Autentica* al usuario, estableciendo un túnel VPN entre el computador cliente y el servidor VPN.
- *Autoriza* al usuario a acceder a los recursos internos listados en el firewall de la plataforma de acuerdo a reglas granulares (acceso hacia IP y puertos de red internos específicos, tanto de PCs como servidores).
- *Registra* los accesos en los logs del sistema.

- Las comunicaciones fluyen desde la plataforma OPNsense hacia el firewall interno, el que da acceso hacia las redes internas mediante reglas de firewall generales (acceso a red de servidores y redes de edificios).

Debido a que el equipo debe ser gestionado desde la LAN del Congreso, se agregó el uso de una tarjeta de red adicional dedicada exclusivamente a gestión.

3.4.4.1.2 ESTABLECIMIENTO DE PARÁMETROS DE CONEXIÓN

Conjuntamente con el equipo de trabajo, se procedió a establecer los datos a ser utilizados durante la configuración de red del equipo.

Tabla 5

Configuración de red de la plataforma OPNsense

Parámetro	Valor
Nombre De Dominio WAN	vpn.congreso.gob.pe
IP Público	190.116.46.147
IP WAN	10.10.10.34/24
IP DMZ VPN	192.168.50.99/24
Nombre De Dominio - LAN	vpn.congreso.net
IP De Gestión	172.30.0.161/21
Rango VPN para clientes de escritorio	10.10.64.0/20
Rango VPN para clientes móviles	10.10.80.0/21
Gateway Internet	10.10.10.1
Gateway LAN Interna	192.168.50.2

Fuente: elaboración propia

La siguiente tabla muestra las rutas estáticas configuradas en los firewalls de la plataforma OPNsense y el firewall perimetral.

Tabla 6

Rutas estáticas en OPNsense

Edificio	Acrónimo	Rango de IP
Palacio Legislativo	PLC	172.20.0.0/19
Luis Alberto Sánchez	LAS	172.21.0.0/19
Complejo Legislativo	CMP	172.22.0.0/19
Roberto Ramírez del Villar	RRV	172.23.0.0/19
José Faustino Sánchez Carrión	JFSC	172.24.0.0/19
Hospicio Ruiz Dávila	HRD	172.25.0.0/19
Víctor Raúl Haya de la Torre	VRHT	172.26.0.0/19
José Santos Atahualpa	JSA	172.27.0.0/19
Servidores de aplicaciones internas		Número IP

Servidor Portal Intranet	172.30.0.9/32
Servidor de aplicaciones Java	172.30.0.239/32
Servidor SITVA2 (sistema de votación remota)	172.30.0.138/32
Sistema de videoconferencia	172.30.1.28/32
Servidor de Help Desk	172.30.0.57/32
Servidor SIGA web	172.30.6.15/32
Servidor SQL (para desarrollo)	172.30.1.50/32
Servidor de aplicaciones Sistema de Votación (para desarrollo)	172.30.1.30/32
Servidor de aplicaciones Java (para desarrollo)	172.30.2.15/32

Fuente: elaboración propia

Tabla 7

Gateways en OPNsense

Nombre de red de origen	Red de origen	IP de gateway
WAN	Internet	10.10.10.1
DMZ_VPN	172.16.0.0/19	192.168.50.2

Fuente: elaboración propia

Tabla 8

Rutas estáticas en Firewall Perimetral

Nombre de red de origen	Red de origen	IP de gateway
Red VPN clientes de escritorio	10.10.64.0/20	192.168.50.99
Red VPN clientes móviles	10.10.80.0/21	192.168.50.99

Fuente: elaboración propia

3.4.4.2 CONTROL DE ACCESO

3.4.4.2.1 FACTORES DE AUTENTICACIÓN

La plataforma OPNsense permite el uso de la autenticación de usuarios de un LDAP externo (en este caso, Microsoft Active Directory institucional), con lo que se

cuenta ya con un factor de autenticación (el combo usuario / contraseña). Para mejorar la seguridad se debía implementar al menos un factor adicional.

Requerimiento: Se debe implementar al menos un factor de autenticación adicional para la autenticación de usuarios.

Solución: OPNsense nos permitió brindar dos factores de autenticación adicionales.

- **Certificado Digital:** al disponer de un motor de Autoridad de Certificación, se pudo generar un certificado digital único para cada usuario.
- **TOTP:** permitió la creación de un código QR por usuario, el cual al ser leído por una aplicación móvil compatible con el estándar RFC 6238, tales como Autenticador de Google, Microsoft Authenticator y FreeOTP. Estas aplicaciones generan un número de 6 dígitos cada 30 segundos, el que debe ser ingresado junto con la contraseña de usuario para permitir el acceso.

Tanto el certificado digital como el código QR fueron creados desde la interface web de administración para cada usuario.

3.4.4.2.2 GRANULARIDAD DE REGLAS DE ACCESO

Como se comentó en el punto 3.4.4.1, fue necesario establecer políticas granulares de acceso para cada usuario, de manera que una vez este se conectara mediante VPN sólo disponga de acceso a los recursos a los que está autorizado.

Requerimiento: Se debe entregar a cada cliente (usuario) un número IP único cada vez que se conecte. Así, una vez conocido el número IP otorgado al usuario, se puedieron configurar reglas de firewall específicas para este usuario.

Solución:

La manera como se logró establecer este control es con dos características que brinda la plataforma OPNsense.

1. **CSO DE OPENVPN:** Se otorgó a cada cliente (usuario) un número IP único y persistente mediante el mecanismo de OpenVPN (servidor de VPN incluido en OPNsense) denominado CSO (Client Specific Override o Anulaciones Específicas del Cliente). Este mecanismo permite "anular" la configuración estándar del servidor VPN para cada cliente identificado mediante su nombre de usuario, y sobrescribirlas con una configuración personalizada específica. En este caso, se utilizó para entregarle un número IP preestablecido. Cabe señalar que la característica CSO dispone de varios parámetros adicionales que se podrían cambiar para cada cliente, lo que brindan un nivel de flexibilidad que podría ser usado para ampliar eventualmente la funcionalidad del servicio.
2. **ALIAS DE FIREWALL:** debido a que se conoce de antemano el número IP a ser otorgado a cada usuario en el momento de la conexión VPN, se le otorga un "alias" en la configuración de firewall de OPNsense, y se establecen regla(s) de firewall específicas referenciando al alias, el cual es un nombre asociado al usuario. Estos alias también se utilizaron para nombrar los IP de los servidores internos, puertos de red a utilizar, redes de edificios y los IP de las PC de cada usuario, para una fácil identificación y administración de las políticas de firewall implementadas.

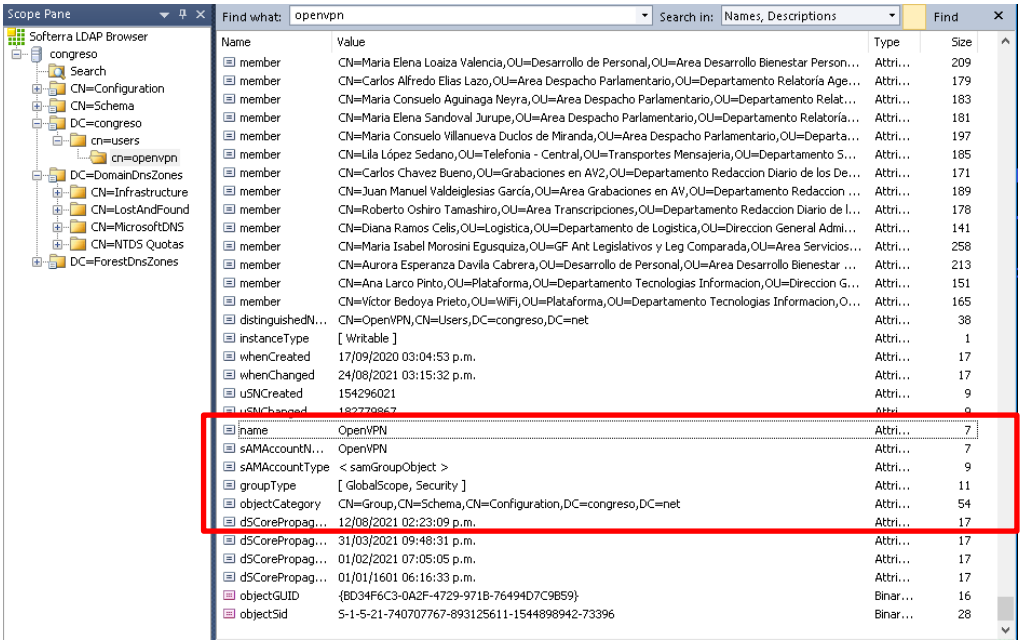
3.4.4.2.3 INTEGRACIÓN CON EL LDAP ACTIVE DIRECTORY INSTITUCIONAL

Como la plataforma permite la integración con el directorio de usuarios institucional basado en Microsoft Active Directory mediante la importación de los mismos a la base de datos de usuarios de OPNsense, se planificó que los usuarios a

importar debían pertenecer a un grupo específico del Active Directory, para evitar la importación innecesaria de los más de 3000 usuarios registrados en la actualidad. Así, se destinó el usuario de red llamado “ldaplinux” para que OPNsense lo utilice en las consultas al LDAP, y se creó el grupo “OpenVPN” en el Active Directory, como se muestra en el siguiente gráfico.

Figura 40

Grupo de Active Directory OpenVPN.



Nota. Herramienta utilizada: Softerra LDAP Browser 4.5. Fuente: elaboración propia

3.4.5 ETAPA 5: IMPLEMENTACIÓN DE LA PLATAFORMA

En este punto, se muestra como se realizó el despliegue y configuración de la plataforma OPNsense y de los equipos de infraestructura asociados (balanceador de líneas de internet Peplink y firewall perimetral).

A falta de disponibilidad de un equipo moderno para esta implementación, la jefatura de Infraestructura Tecnológica decidió que se utilice el mismo equipo de

pruebas, por lo que para la implementación de producción se utilizó el servidor de virtualización IBM x3850 indicado en el punto 3.3.2.

Tabla 9

Características técnicas de servidor

Característica	Valor
Marca	IBM
Modelo	x3850 8864-4RU
Procesador	Intel Xeon Dual DP
Memoria	20GB RAM
Almacenamiento	135 GB capacidad efectiva (3 discos de 73GB en RAID 5)
Conectividad	1Gbps Ethernet (cobre) x 4
Sistema operativo	VMware ESXi 5.1.0, 1065491

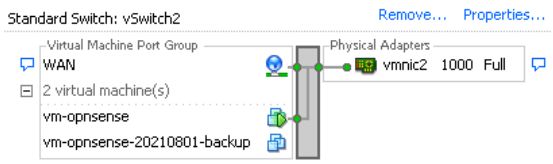
Fuente: elaboración propia

3.4.5.1 CONFIGURACIÓN DE SWITCHES VIRTUALES EN VMWARE

OPNsense se instaló como una máquina virtual en el servidor VMWare ESXi. Para poder realizar la conectividad de acuerdo a lo planificado, fue necesario configurar en VMware las tres redes a ser accedidas por la plataforma OPNsense (WAN, DMZ_VPN y LAN/ADM). Para ello, se crearon tres switches virtuales, asignando las 4 tarjetas de red físicas del servidor a las mismas de la siguiente manera:

Figura 41

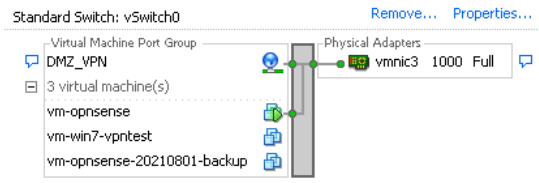
Configuración de vSwitch WAN.



Fuente: elaboración propia

Figura 42

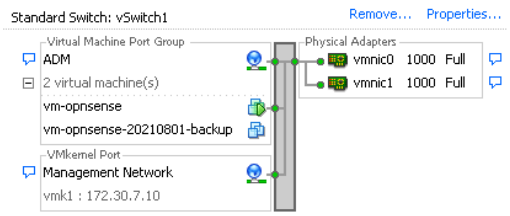
Configuración de vSwitch DMZ_VPN.



Fuente: elaboración propia

Figura 43

Configuración de vSwicth ADM.



Fuente: elaboración propia.

3.4.5.2 CONFIGURACIÓN DE BALANCEADOR DE INTERNET

En el balanceador de líneas de internet, equipo que administra los NAT de IPs públicas hacia la red denominada WAN en el esquema de red, se realizó la configuración de la asociación del IP WAN interno 10.10.10.34 al IP público 190.116.46.147.

Figura 44

Balanceador de líneas de internet Peplink Balance 13500.

Fuente: elaboración propia.

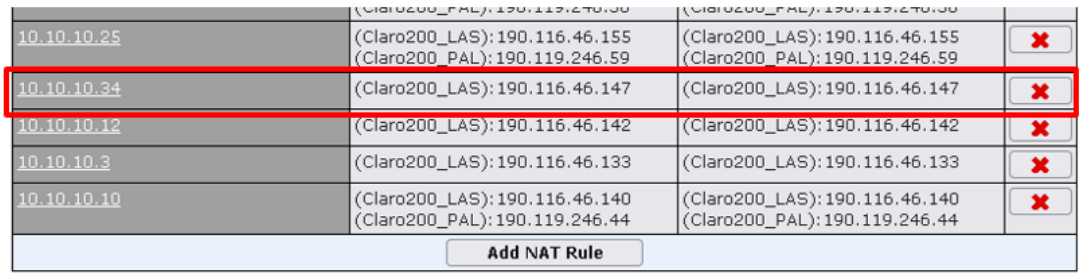
Figura 45

Configuración de NAT para IP público.

Fuente: elaboración propia

Figura 46

Asociación de IP NAT a público.



Fuente: elaboración propia

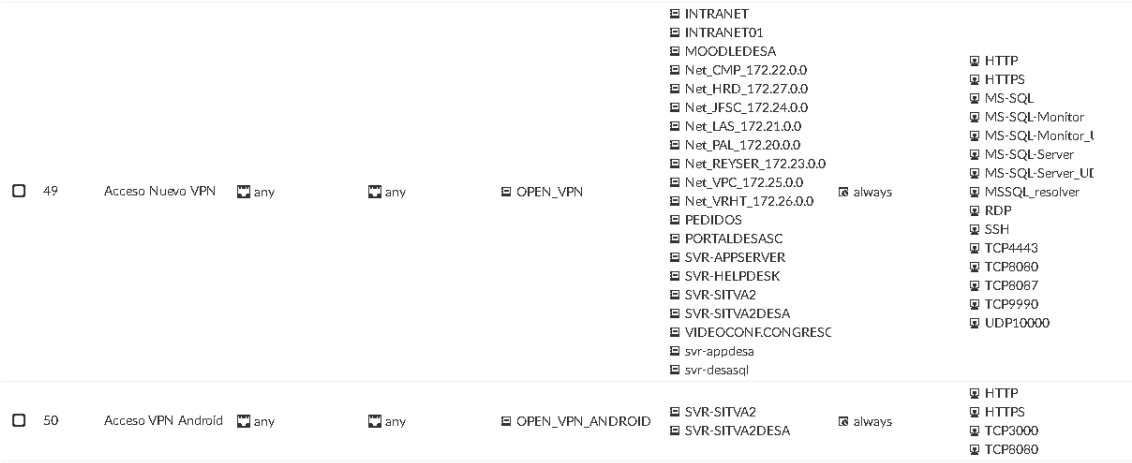
3.4.5.3 CONFIGURACIÓN DE FIREWALL PERIMETRAL

En el firewall perimetral se configuraron las reglas de firewall que permiten el pase de las comunicaciones VPN hacia la LAN institucional, así como las rutas de red

asociadas. Se muestran las capturas de pantalla de los nuevos firewall Fortinet modelo Fortigate, los que han reemplazado a los antiguos firewall de marca Checkpoint.

Figura 47

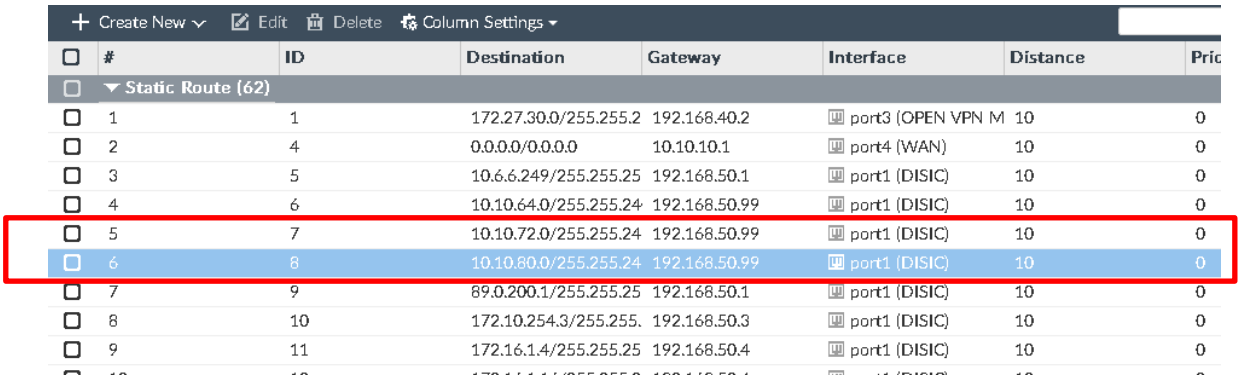
Reglas de Firewall Fortigate.



Fuente: elaboración propia.

Figura 48

Rutas estáticas en firewall Fortigate.



Fuente: elaboración propia.

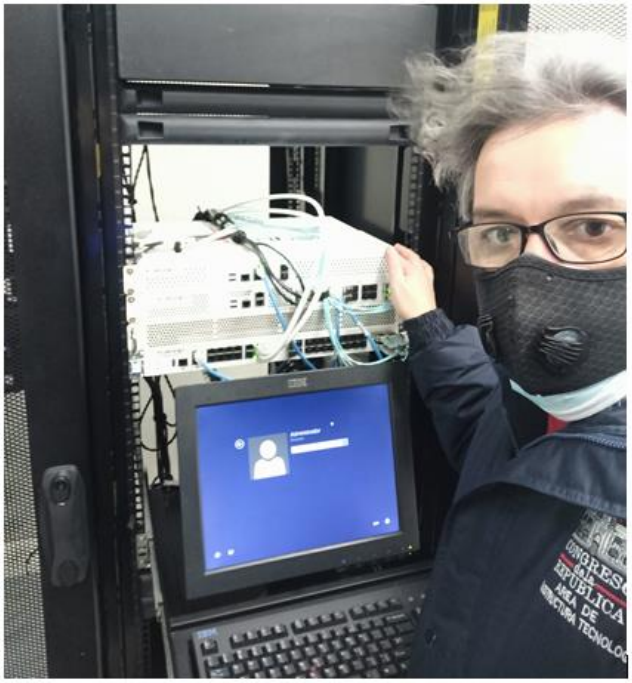
Figura 49

Firewall Checkpoint (antes de retirarlo de servicio).

Fuente: elaboración propia.

Figura 50

Firewall Fortinet Fortigate (nuevo equipamiento).



Fuente: elaboración propia.

3.4.5.4 CONFIGURACIÓN DE OPNSENSE

En este punto se procedió a la configuración de los distintos servicios necesarios para la implementación como plataforma de Acceso Remoto Seguro. Para ello se llevaron a cabo las siguientes tareas:

- **INSTALACIÓN DE OPNSENSE**

  Se instaló OPNsense como máquina virtual en el servidor VMware ESXi 5.1 indicado en el punto 3.4.5.1.

- **CONFIGURACIÓN INICIAL**

  La configuración inicial implicó la configuración de números IP de las tres tarjetas de red, nombre de dominio del servidor y configuración de servidor de tiempo, entre otros.

- **CONFIGURACIÓN DE RED**
  - Gateways.
  - Rutas de acceso de redes.

- **CONFIGURACIÓN DE SERVICIO DE AUTORIDAD DE CERTIFICACIÓN**

  Para la emisión de certificados digitales tanto para el servidor mismo como para los usuarios.

- **CONFIGURACIÓN DE SERVICIO DE AUTENTICACIÓN DE USUARIOS**

  Se necesitaron dos instancias de este servicio:

  - **Autenticación para usuarios de equipos de escritorio y laptops.**

    Esta instancia valida tres factores de autenticación: cuenta de

usuario LDAP Active Directory, certificado de usuario y token TOTP.

- **Autenticación para usuarios de equipos móviles.** Para facilitar el acceso a los congresistas y debido a que se utilizan niveles de seguridad adicionales en la aplicación de Asistencia y Votación Remota, esta instancia valida sólo dos factores de autenticación: cuenta de usuario LDAP Active Directory y certificado de usuario.

- **CONFIGURACIÓN DE SERVICIO DE VPN**

  Se necesitaron dos instancias de este servicio:

  - **VPN para usuarios de equipos de escritorio y laptops.** Este servicio utiliza el servidor de autenticación de tres factores.
  - **VPN para usuarios de equipos móviles.** Este servicio utiliza el servidor de autenticación de dos factores.

- **CONFIGURACIÓN DE REGLAS DE FIREWALL**

  - Para acceso a escritorio remoto (específicas por usuario)
  - Para acceso a servicios web varios (generales)

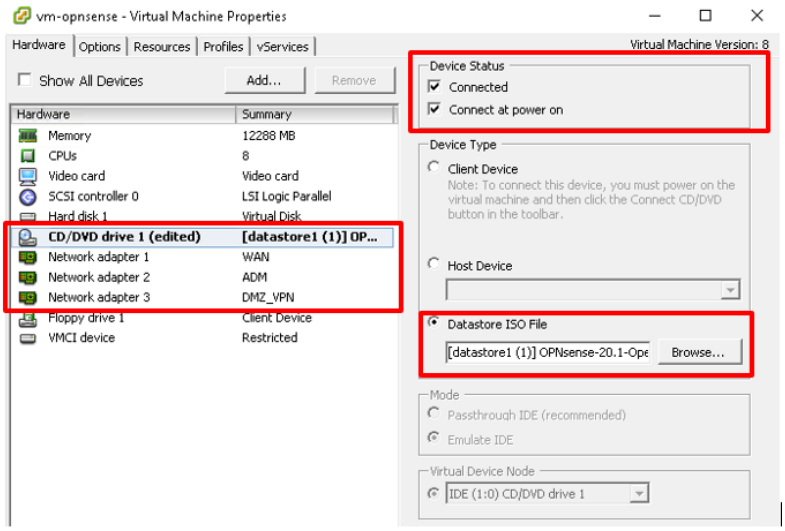
La configuración opcional de certificado SSL para la consola web de administración se muestra en el Anexo 5.

3.4.5.5 INSTALACIÓN DE OPNSENSE

- Se montó el ISO de OPNsense versión 20.1 en el CD-Drive virtual para permitir el arranque desde ese dispositivo y crear 3 NICs virtuales:
  - WAN
  - DMZ_VPN
  - ADM

Figura 51

Configuración de máquina virtual en VMware ESXi.

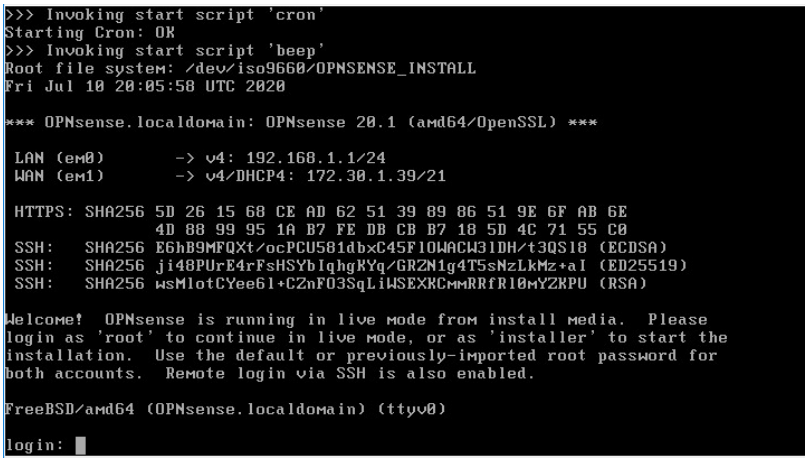


Fuente: elaboración propia.

- Encender la VM.
- La VM bootea del ISO y se llega a la siguiente ventana:

Figura 52

Pantalla inicial de OPNsense CLI.

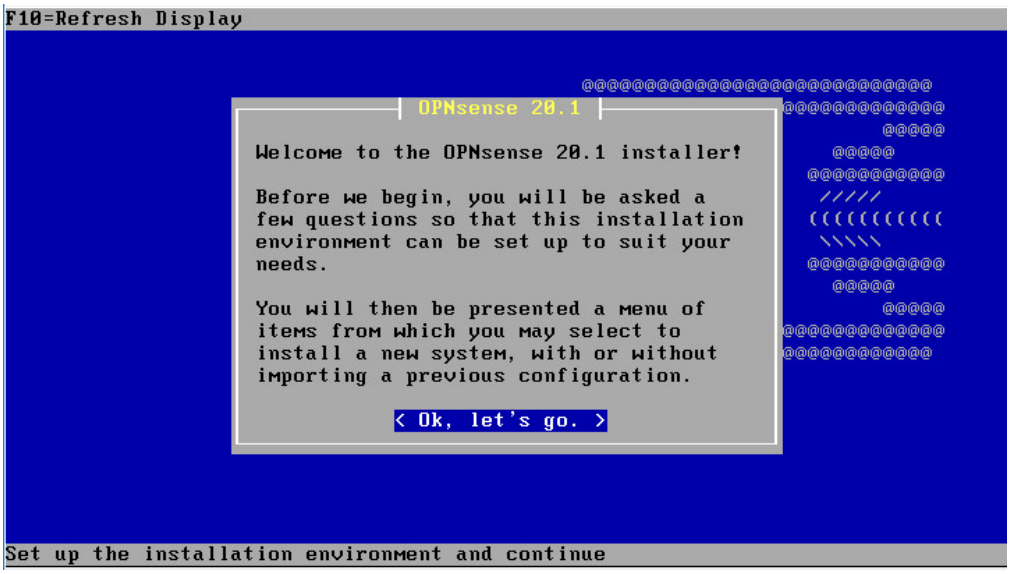


Fuente: elaboración propia.

- Colocar los valores iniciales para instalar (nótese el uso del usuario “installer” en vez de “root”. Ingresar con “root” da la opción de iniciar en modo LiveCD):
    - **Login:** installer
    - **Password:** opnsense
- Aceptar los mensajes de las siguientes pantallas:

Figura 53

Ventana de bienvenida.



Fuente: elaboración propia.

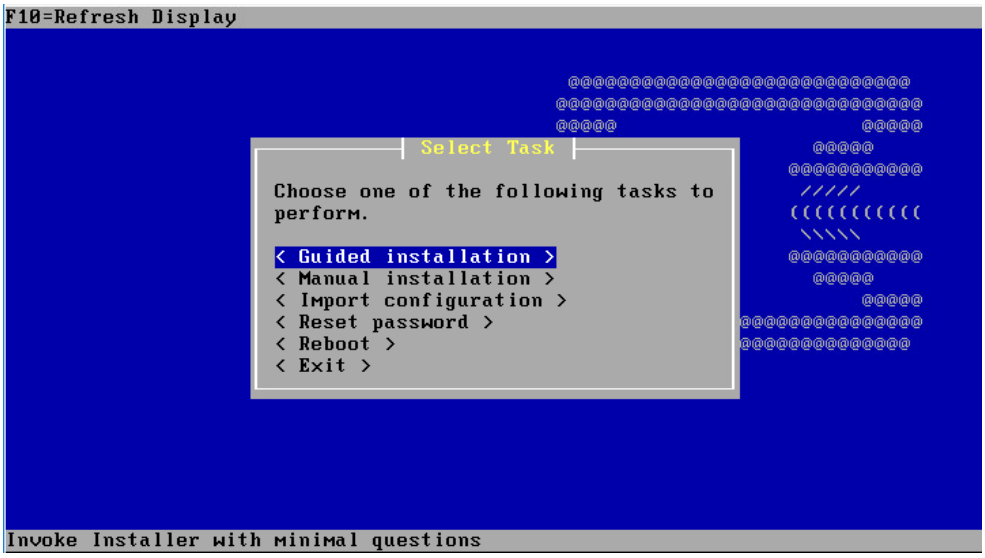
Figura 54

Configuración de teclado y fuente de texto.

Fuente: elaboración propia.

Figura 55

Selección de tipo de instalación.



Fuente: elaboración propia.

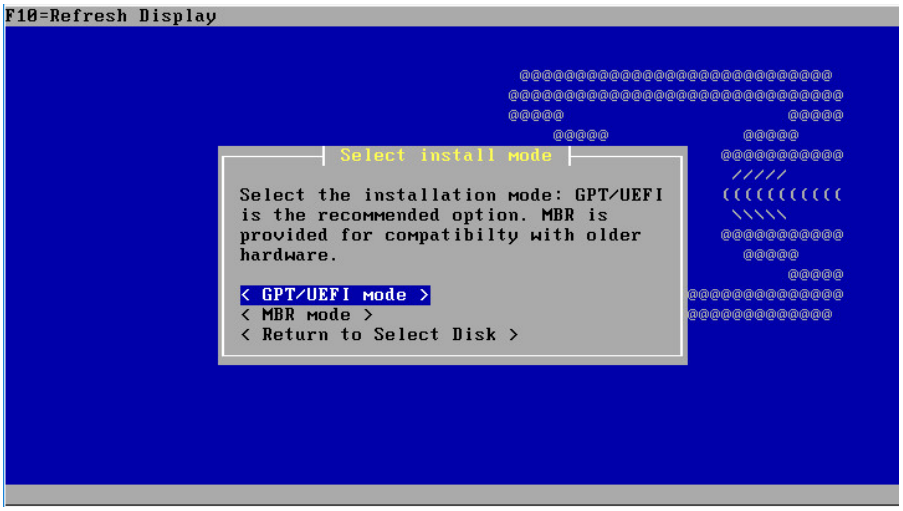
Figura 56

Selección de disco duro.

Fuente: elaboración propia

Figura 57

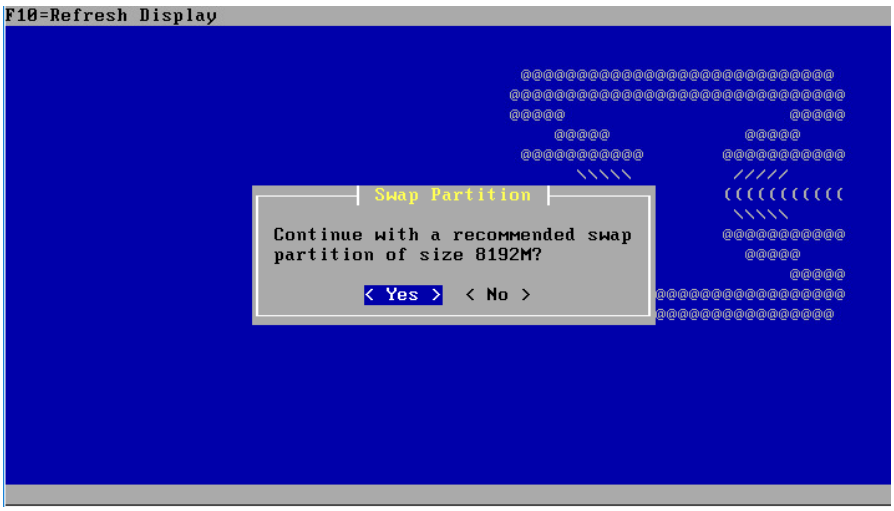
Selección de tipo de sector de arranque.



Fuente: elaboración propia.

Figura 58

Selección de tamaño de partición Swap.

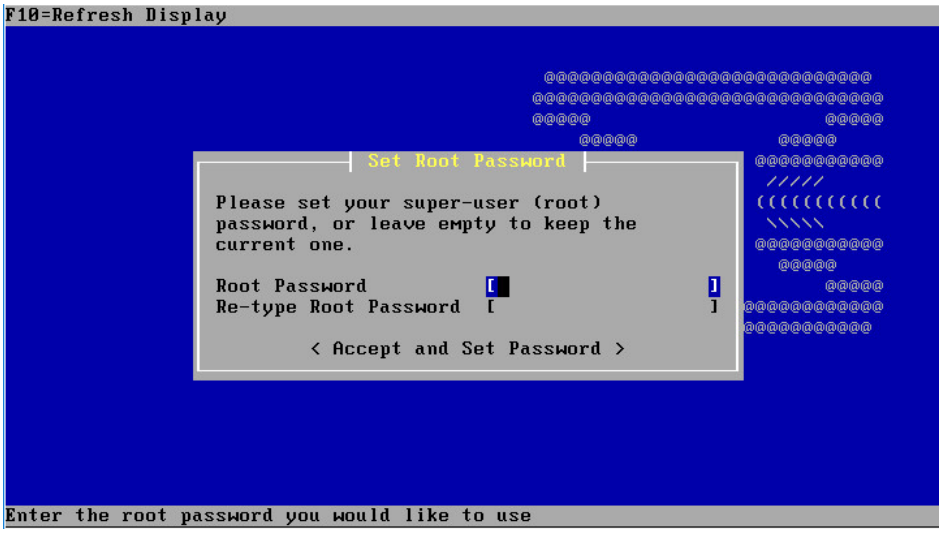


Fuente: elaboración propia.

- Colocar contraseña para usuario “root”.

Figura 59

Pantalla de ingreso de contraseña para usuario root.

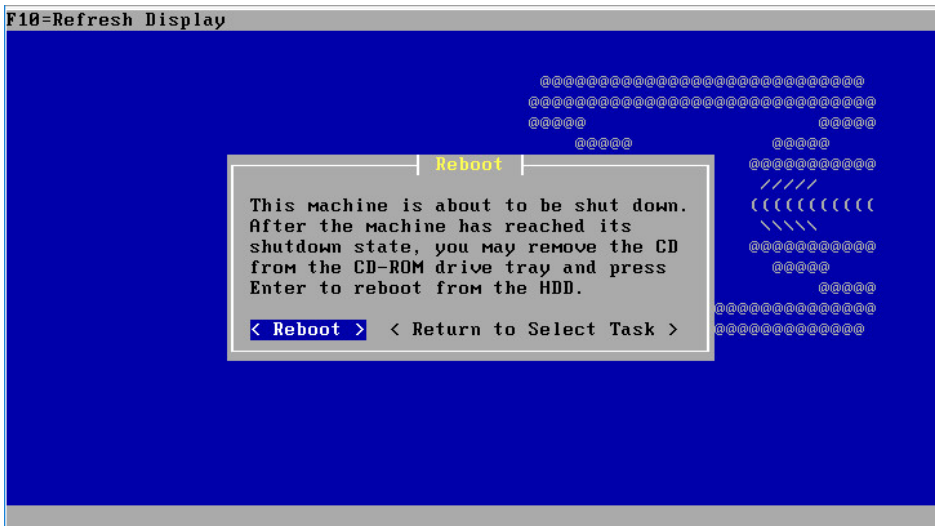


Fuente: elaboración propia.

- Reiniciar el servidor.

Figura 60

Pantalla de mensaje de reinicio.

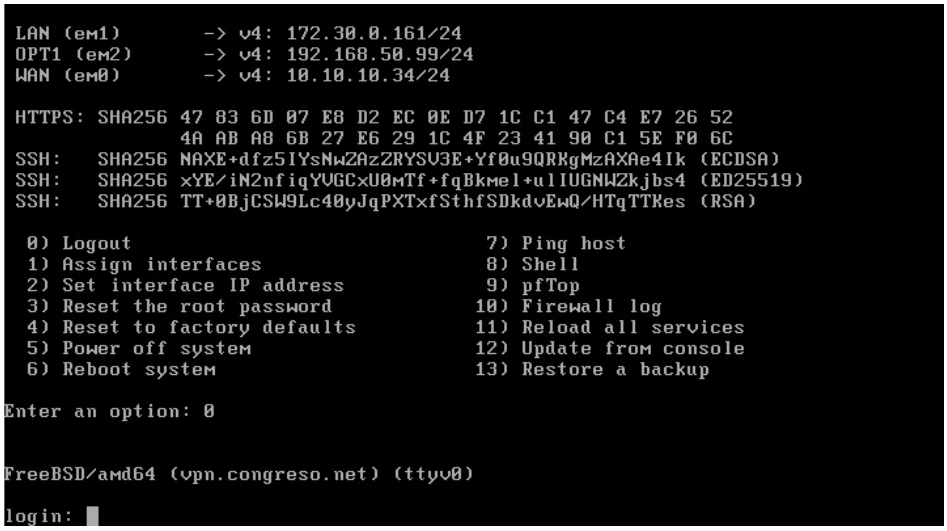


Fuente: elaboración propia.

- Tras reiniciar el servidor, aparece esta pantalla:

Figura 61

Pantalla de arranque inicial.

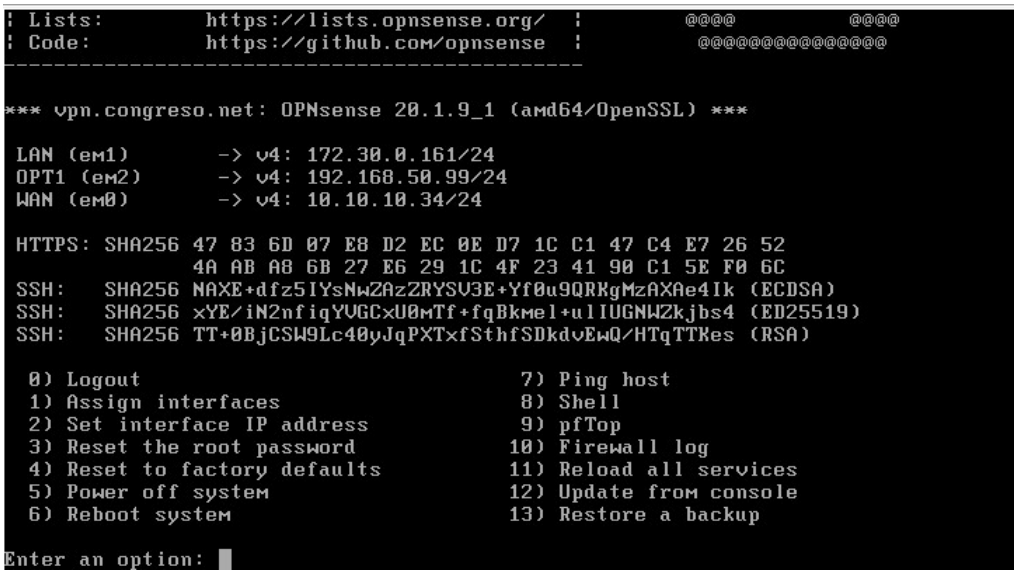


Fuente: elaboración propia.

- Ingresar las credenciales de usuario root

Figura 62

Menú principal de interface de línea de comando (CLI).



Fuente: elaboración propia.

- Colocar hora (si es que no se dispone de un servidor NTP. Importante porque el servidor debe estar con la hora correcta para el funcionamiento de TOTP)
    - Ingresar a Shell y ejecutar el siguiente comando (año, mes, día, hora y minutos):
        - date *aammddhhmm*
- Asignar interfaces como sigue:
    - La interface **WAN** va hacia la red **WAN** (a través del balanceador de internet Peplink)
    - La interface **LAN** va a la red **ADM** (**LAN del Congreso**) para administración.
    - La interface **OPT1** va a la red **DMZ_VPN**.
        - WAN: 10.10.10.34/24
        - LAN: 172.30.0.161/21

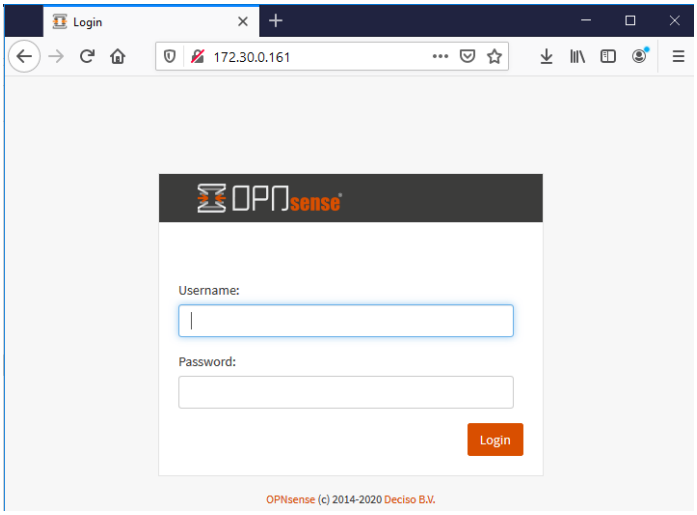
- OPT1: 192.168.50.99/24

3.4.5.6 CONFIGURACIÓN WEB INICIAL DE OPNSENSE

- Ingresar a la interface administrativa vía web utilizando el IP LAN (URL http://172.30.0.161)

Figura 63

Pantalla de ingreso de interface web.

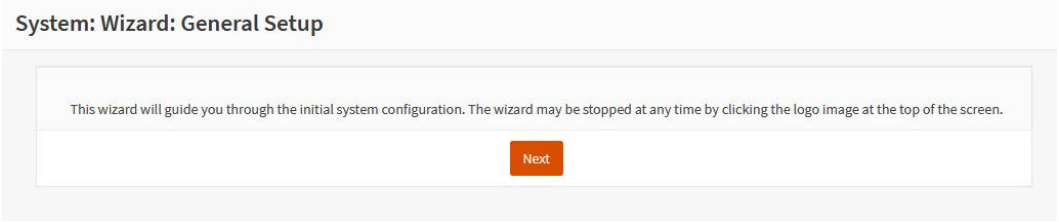


Fuente: elaboración propia

- Hacer click en “Next”

Figura 64

Asistente de configuración inicial.



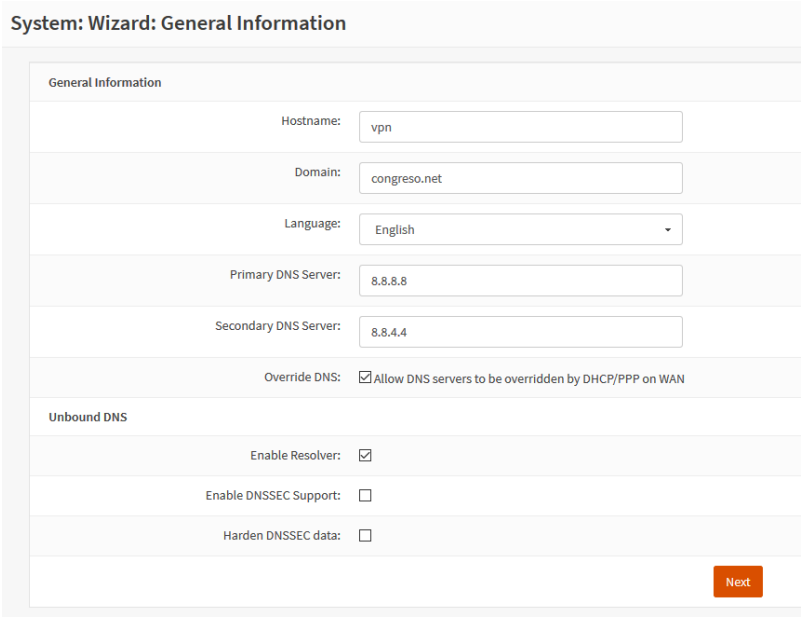
Fuente: elaboración propia.

- En esta ventana, colocar los datos solicitados:
  - **Nombre de host:** vpn

- **Dominio:** congreso.net (este es el dominio de la LAN institucional).
- **Idioma:** inglés (si bien la interface administrativa se puede configurar también en idioma español, sugiero usar el idioma inglés para la configuración inicial debido a que la mayoría de información de documentación y resolución de fallas en Internet se encuentra en este idioma).
- **DNS primario y secundario:** utilizamos los DNS de Google 8.8.8.8 y 8.8.4.4
- Dejar el resto de valores por omisión.

Figura 65

Asistente de configuración: Información general.

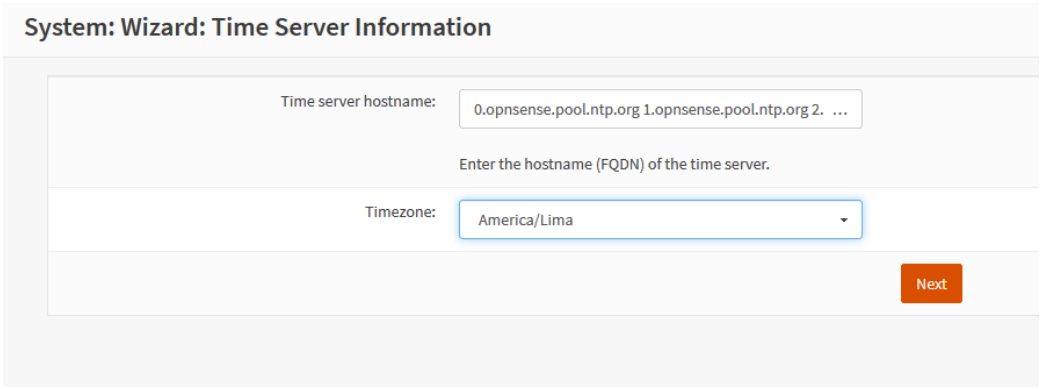


Fuente: elaboración propia.

- En esta ventana, colocar:
  - **Zona horaria:** America/ Lima
  - Dejar la lista de servidores de tiempo por omisión.

Figura 66

Asistente de configuración: servidor de tiempo.



Fuente: elaboración propia.

- **Configuración de interface WAN: e**legir configuración IP estática.

Figura 67

Selección de tipo de configuración de IP WAN.

Fuente: elaboración propia.

- Ingresar IP WAN y máscara de red previamente seleccionadas.

Figura 68

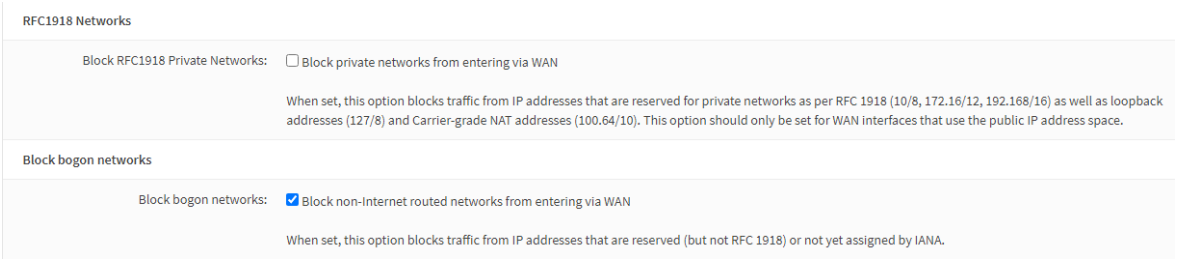
Ingreso de IP WAN.

Fuente: elaboración propia.

- Quitar la opción de bloqueo de tráfico de redes privadas via WAN.

Figura 69

Selección de bloqueo de redes.

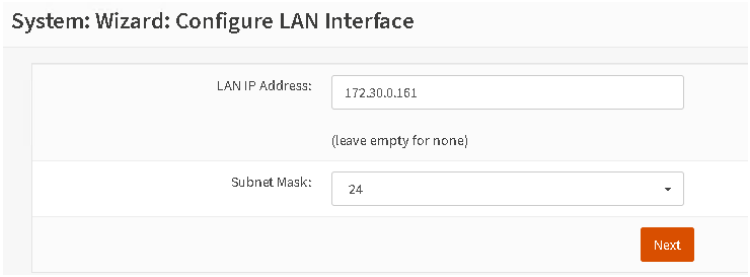


Fuente: elaboración propia

- **Configuración de interface LAN: i**ngresar IP LAN y máscara de red previamente seleccionadas.

Figura 70

Ingreso de IP LAN.

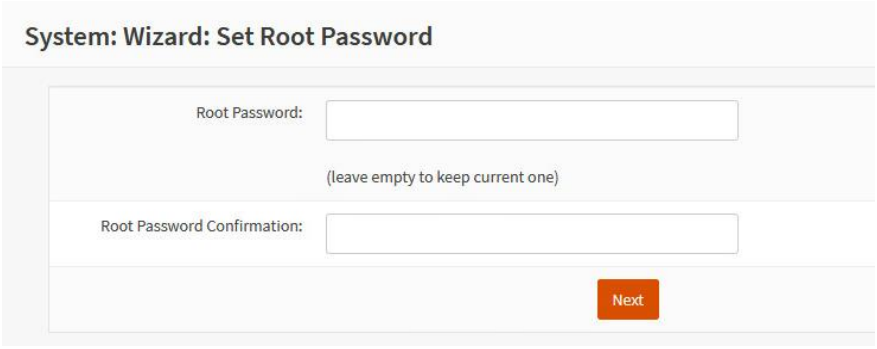


Fuente: elaboración propia.

- Cambio de contraseña de usuario “root”.

Figura 71

Cambio de contraseña inicial.

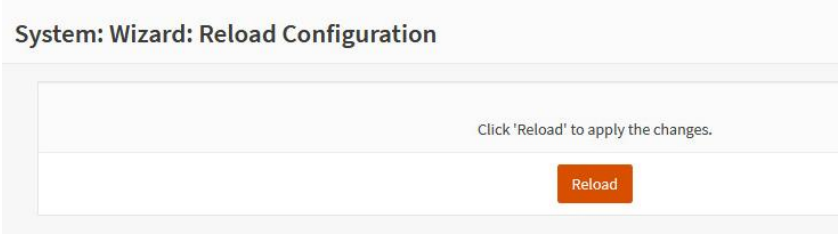


Fuente: elaboración propia.

- Seleccionar “Reload” para activar los cambios ingresados en la configuración inicial.

Figura 72

Recarga de configuración.

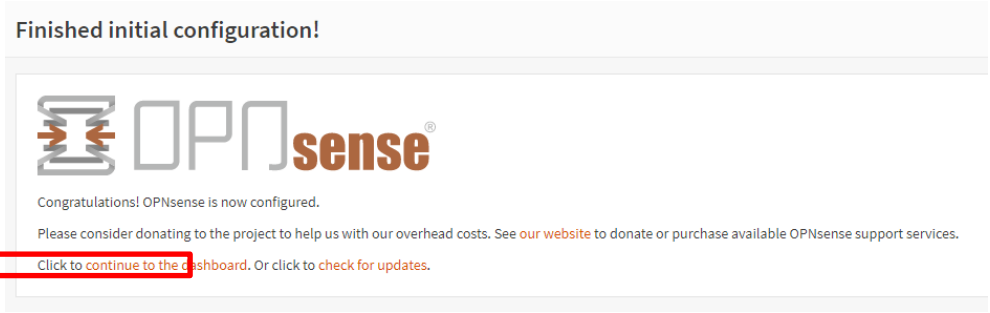


Fuente: elaboración propia.

- En la pantalla de primera carga, seleccionar la opción “continue to the dashboard” para ver la consola principal de la plataforma.

Figura 73

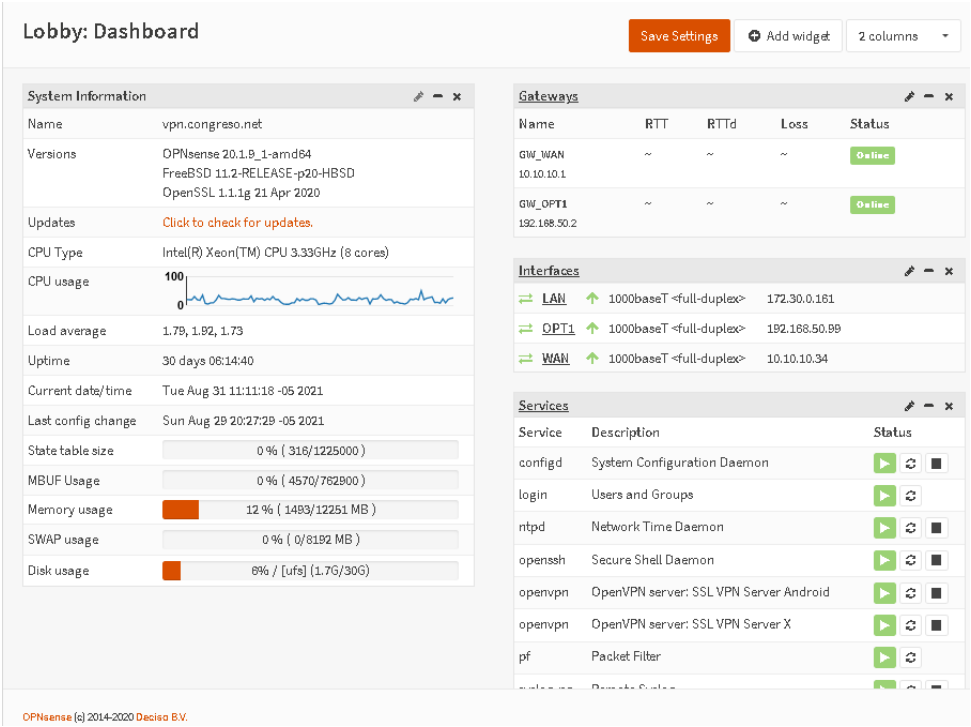
Pantalla después de recargar configuración por primera vez.



Fuente: elaboración propia.

Figura 74

Consola principal de OPNsense.



Fuente: elaboración propia.

3.4.5.7 CONFIGURACIÓN DE GATEWAYS Y RUTAS

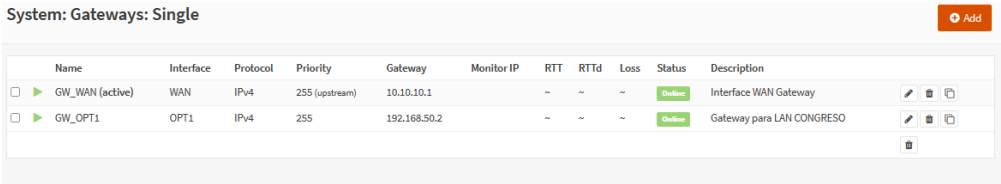
Con la configuración básica de red (IP de las interfaces) se procede a configurar en OPNsense los gateways de salida para WAN y DMZ_VPN, así como las rutas para llegar a las redes y servidores.

GATEWAYS

- Ir a System / Gateways
- Agregar los siguientes gateways:

Figura 75

Gateways.



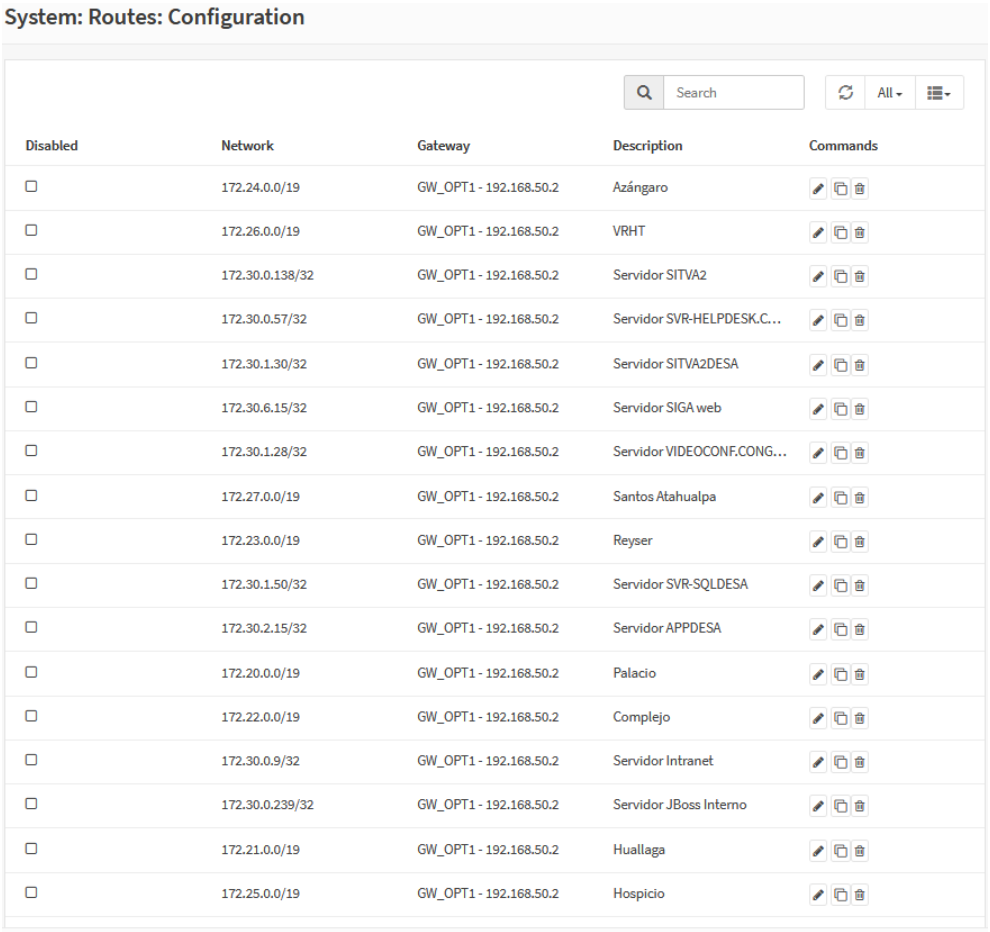
Fuente: elaboración propia.

RUTAS

- Ir a System / Routes
- Agregar las siguientes rutas:

Figura 76

Rutas a redes y servidores.



Disabled	Network	Gateway	Description	Commands
☐	172.24.0.0/19	GW_OPT1 - 192.168.50.2	Azángaro	
☐	172.26.0.0/19	GW_OPT1 - 192.168.50.2	VRHT	
☐	172.30.0.138/32	GW_OPT1 - 192.168.50.2	Servidor SITVA2	
☐	172.30.0.57/32	GW_OPT1 - 192.168.50.2	Servidor SVR-HELPDESK.C...	
☐	172.30.1.30/32	GW_OPT1 - 192.168.50.2	Servidor SITVA2DESA	
☐	172.30.6.15/32	GW_OPT1 - 192.168.50.2	Servidor SIGA web	
☐	172.30.1.28/32	GW_OPT1 - 192.168.50.2	Servidor VIDEOCONF.CONG...	
☐	172.27.0.0/19	GW_OPT1 - 192.168.50.2	Santos Atahualpa	
☐	172.23.0.0/19	GW_OPT1 - 192.168.50.2	Reyser	
☐	172.30.1.50/32	GW_OPT1 - 192.168.50.2	Servidor SVR-SQLDESA	
☐	172.30.2.15/32	GW_OPT1 - 192.168.50.2	Servidor APPDESA	
☐	172.20.0.0/19	GW_OPT1 - 192.168.50.2	Palacio	
☐	172.22.0.0/19	GW_OPT1 - 192.168.50.2	Complejo	
☐	172.30.0.9/32	GW_OPT1 - 192.168.50.2	Servidor Intranet	
☐	172.30.0.239/32	GW_OPT1 - 192.168.50.2	Servidor JBoss Interno	
☐	172.21.0.0/19	GW_OPT1 - 192.168.50.2	Huallaga	
☐	172.25.0.0/19	GW_OPT1 - 192.168.50.2	Hospicio	

Fuente: elaboración propia.

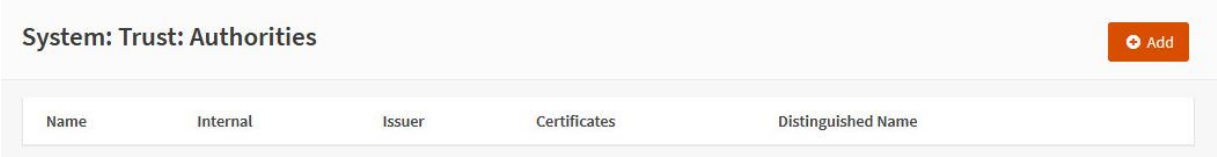
3.4.5.8 CONFIGURACIÓN DE AUTORIDAD DE CERTIFICACIÓN

Se crea una Autoridad de Certificación local que emite tanto el certificado de servidor como los certificados de cada cliente.

- Ir a System / Trust / Authorities

Figura 77

Creación de Autoridad de Certificación.



Fuente: elaboración propia.

- Hacer click en “Add”, llenar los valores indicados y hacer click en “Save”
- Valores para una entidad certificadora con 10 años de tiempo de vida

Tabla 10

Parámetros y valores para creación de Autoridad de Certificación

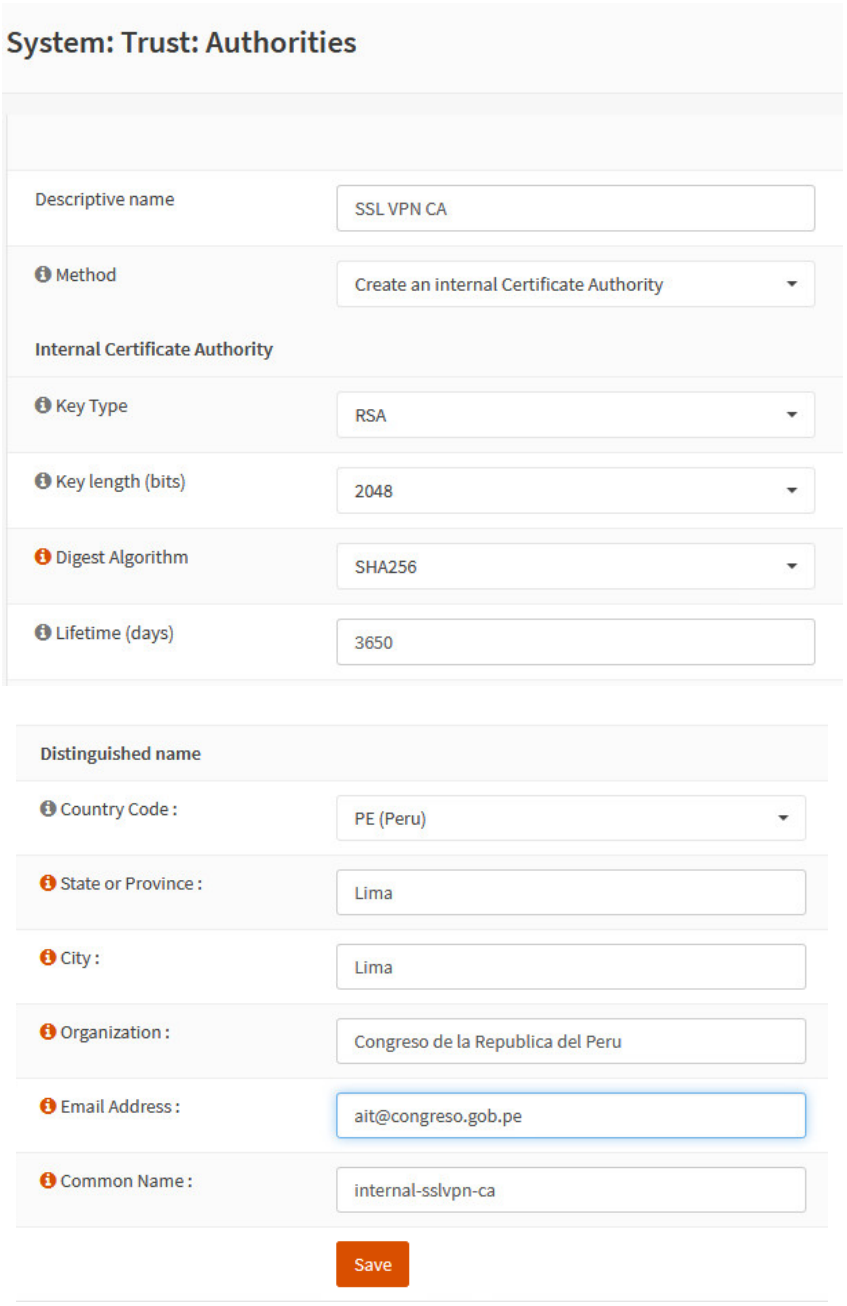
Parámetro	Valor
Descriptive name	SSL VPN CA
Method	Create an internal Certificate Authority
Key length (bits)	2048
Digest Algorithm	SHA256
Lifetime (days)	3650
Country Code	PE
State or Province	Lima
City	Lima
Organization	Congreso de la República del Perú
Email Address	ait@congreso.gob.pe
Common Name	internal-sslvpn-ca

Fuente: elaboración propia

- Pantalla:

Figura 78

Pantalla de parámetros de nueva Autoridad de Certificación.



Fuente: elaboración propia.

Figura 79

Lista de Autoridades de Certificación.

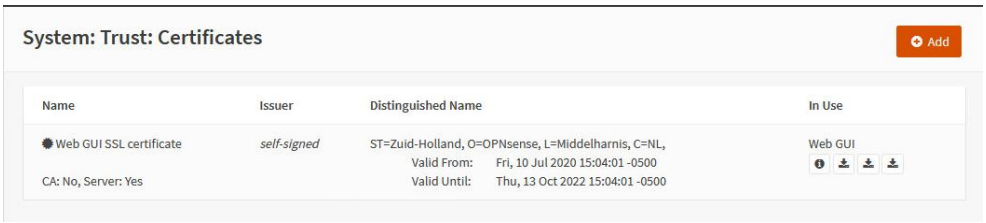
Fuente: elaboración propia.

- Creación del certificado del servidor.
  - Ir a System / Trust / Certificates y hacer click en “Add”

- Pantalla:

Figura 80

Ventana de listas de certificados con el certificado web por omisión.



Fuente: elaboración propia.

- Hacer click en “Add”, llenar los valores indicados en la siguiente tabla y hacer click en “Save”.

Tabla 11

Parámetros y valores para creación de Certificado de Servidor

Parámetro	Valor
Method	Create an internal Certificate
Descriptive name	SSLVPN Server Certificate
Certificate authority	SSL VPN CA
Type	Server Certificate
Key length (bits)	2048
Digest Algorithm	SHA256

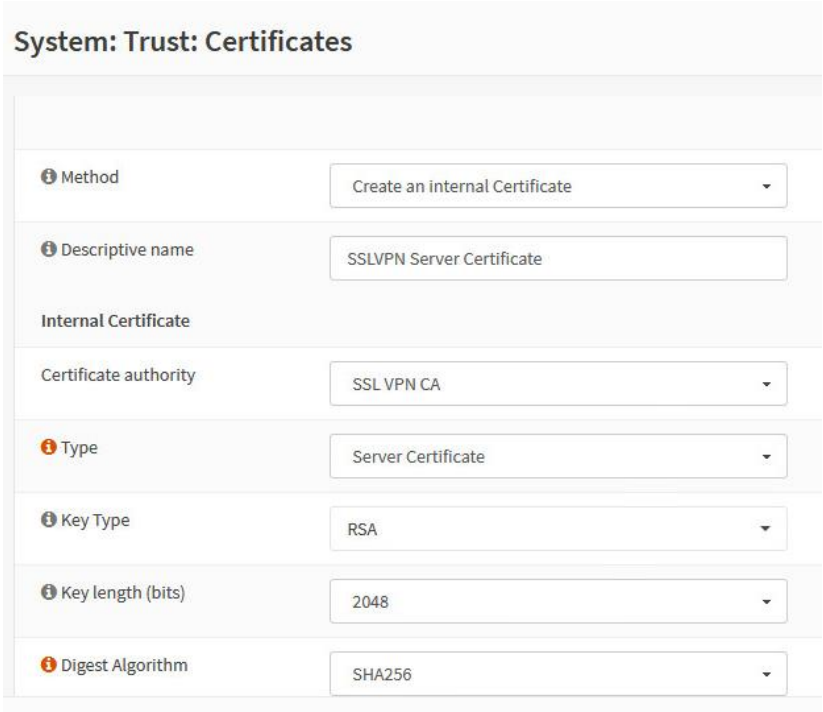
Lifetime (days)	3650
Country Code	PE
State or Province	Lima
City	Lima
Organization	Congreso de la Republica del Peru
Email Address	ait@congreso.gob.pe
Common Name	SSLVPN Server Certificate

Fuente: elaboración propia

- Pantallas:

Figura 81

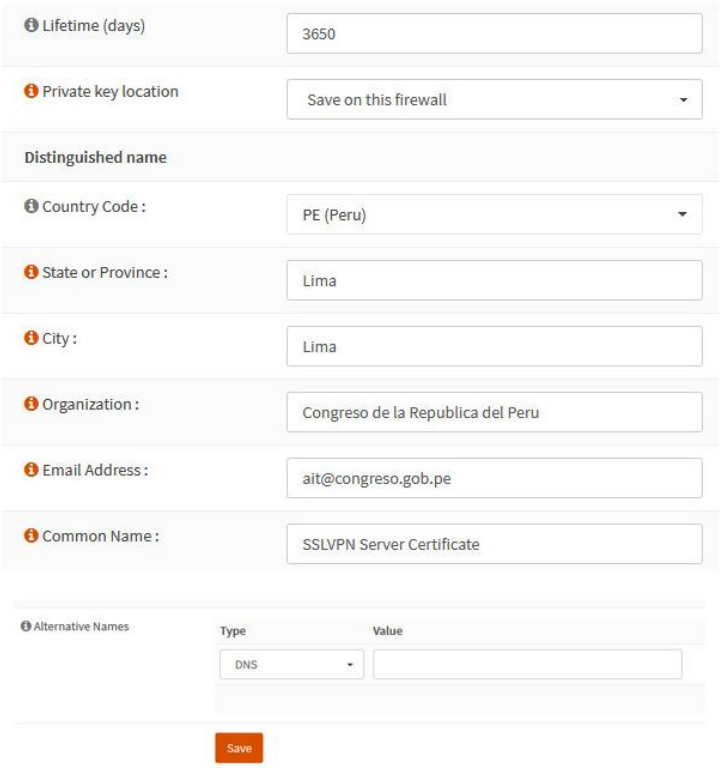
Pantalla 1 de parámetros de nuevo certificado de servidor.



Fuente: elaboración propia.

Figura 82

Pantalla 2 de parámetros de nuevo certificado de servidor.



Fuente: elaboración propia.

- Resultado:

Figura 83

Lista de certificados con nuevo certificado de servidor.

Fuente: elaboración propia.

3.4.5.9 CONFIGURACIÓN DE SERVIDORES DE AUTENTICACIÓN

Los clientes de escritorio utilizan tres factores de autenticación:

- Nombre de usuario / contraseña de dominio (LDAP)
- Certificado digital personal
- Clave TOTP

Los clientes de dispositivos móviles (congresistas con dispositivos Android) utilizan dos factores de autenticación:

- Nombre de usuario / contraseña de dominio (LDAP)
- Certificado digital personal

Para ello primero se requirió configurar un Servidor de Autenticación por cada tipo de cliente.

3.4.5.9.1 SERVIDOR DE AUTENTICACIÓN PARA CLIENTES DE ESCRITORIO

- Requiere usuario de LDAP, certificado digital de usuario y TOTP.
- Datos utilizados:
  - **IP del servidor LDAP AD del Congreso:** 172.30.0.61
  - **Puerto del servidor LDAP AD:** 389
  - **Usuario para consultas LDAP:** ldaplinux (CN=ldaplinux,OU=Plataforma,OU=Departamento Tecnologias Informacion,OU=Direccion General Administracion,OU=Politicas de Usuario,DC=congreso,DC=net)
  - **Ubicación de los usuarios del Congreso en el LDAP:** OU=Politicas de Usuario,DC=congreso,DC=net
  - **Filtro LDAP:_**los usuarios deben pertenecer al grupo OpenVPN (CN=OpenVPN,CN=Users,DC=congreso,DC=net)

- **Campo LDAP a utilizar para identificar a los usuarios:**

  sAMAccountName

- Ir a System / Access / Servers y hacer click en “Add”, ingresar estos valores, dejar el resto por omisión y grabar.

Tabla 12

Parámetros y valores para creación de Certificado de Servidor

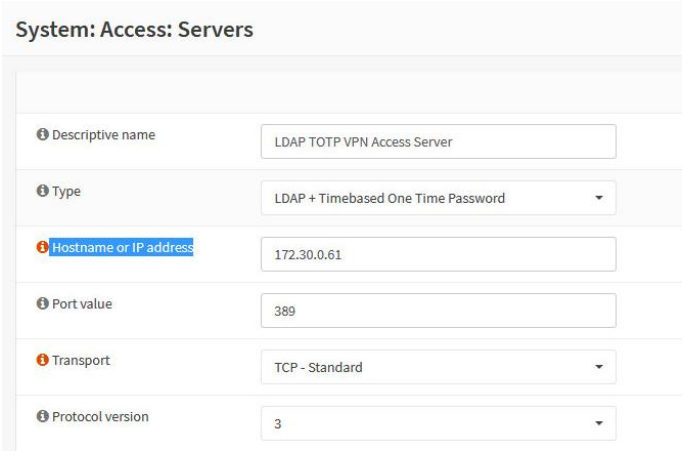
Parámetro	Valor
Descriptive name	LDAP TOTP VPN Access Server
Type	LDAP+Timebased One Time Password
Hostname or IP address|	172.30.0.61
Port value	389
Transport	TCP – Standard
Protocol version	3
Bind credentials UserDN	CN=ldaplinux,OU=Plataforma,OU=Departamento Tecnologias Informacion,OU=Direccion General Administracion,OU=Politicas de Usuario,DC=congreso,DC=net
Bind credentials Password	<Colocar contraseña de usuario “ldaplinux”>
Search scope	Entire Subtree
Base DN	OU=Politicas de Usuario,DC=congreso,DC=net
Authentication containers	OU=Politicas de Usuario,DC=congreso,DC=net
Extended query	&(objectClass=User)(memberof=CN=OpenVPN,CN=Users,DC=congreso,DC=net)
Initial Template	Microsoft AD
Using naming attribute	sAMAccountName
Reverse token order	<seleccionado>

Fuente: elaboración propia.

- Pantalla:

Figura 84

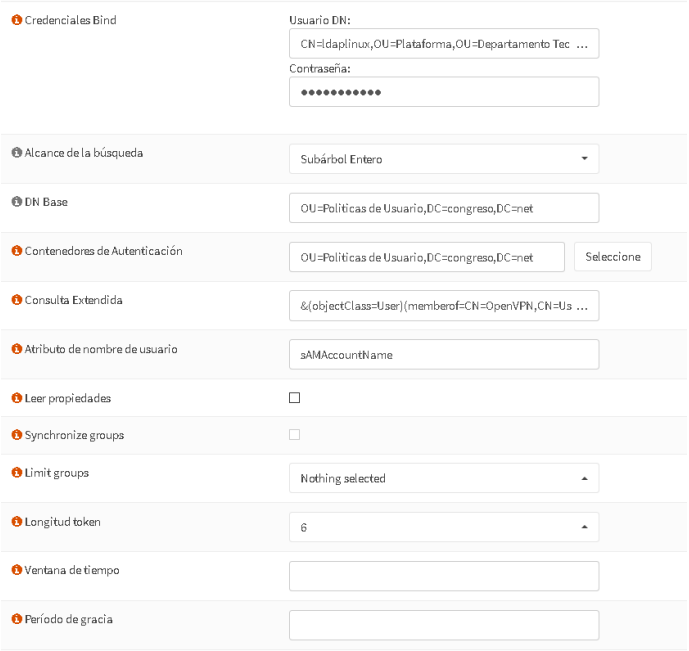
Configuración de servidor de autenticación (parte 1).



Fuente: elaboración propia.

Figura 85

Configuración de servidor de autenticación (parte 2).



Fuente: elaboración propia.

Figura 86

Configuración de servidor de autenticación (parte 3).

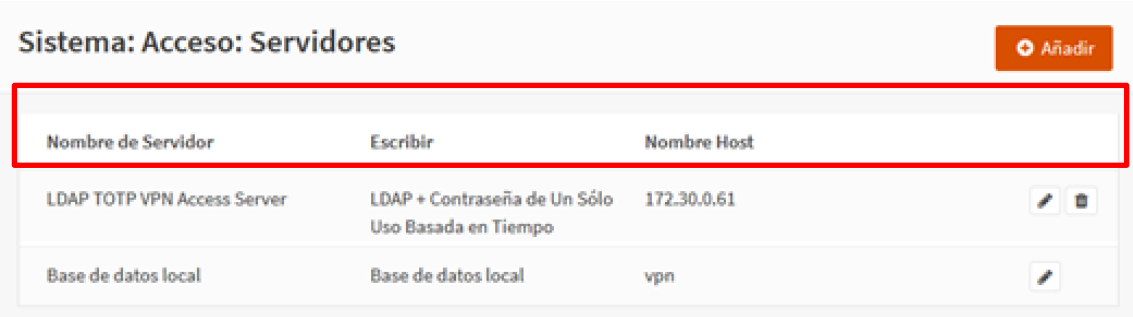
Fuente: elaboración propia.

NOTA IMPORTANTE: por omisión, el orden de ingreso en el campo contraseña es *token* + *password* (donde "token2 es el número de 6 dígitos generado por las apps Google Authenticator, Microsoft Authenticator y/o FreeOTP). Al marcar "Reverse token order", el nuevo orden de ingreso será *password* + *token*, con lo que el usuario ahora escribe primero su contraseña de dominio y luego podrá verificar y escribir el valor "token" del aplicativo TOTP.

- Resultado:

Figura 87

Lista de servidores de autenticación.



Fuente: elaboración propia.

3.4.5.9.2 SERVIDOR DE AUTENTICACIÓN PARA CLIENTES MÓVILES ANDROID

- Requiere usuario de LDAP y certificado digital de usuario.
- Datos utilizados:

- **IP del servidor LDAP AD del Congreso:** 172.30.0.61
- **Puerto del servidor LDAP AD:** 389
- **Usuario para consultas LDAP:** ldaplinux (CN=ldaplinux,OU=Plataforma,OU=Departamento Tecnologias Informacion,OU=Direccion General Administracion,OU=Politicas de Usuario,DC=congreso,DC=net)
- **Ubicación de los usuarios del Congreso en el LDAP:** OU=Politicas de Usuario,DC=congreso,DC=net
- **Filtro LDAP:_**los usuarios deben pertenecer al grupo OpenVPN (CN=OpenVPN,CN=Users,DC=congreso,DC=net)
- **Campo LDAP a utilizar para identificar a los usuarios:** sAMAccountName

- Ir a System / Access / Servers y hacer click en “Add”, ingresar estos valores, dejar el resto por omisión y grabar.

Tabla 13

Parámetros y valores para creación de Certificado de Servidor

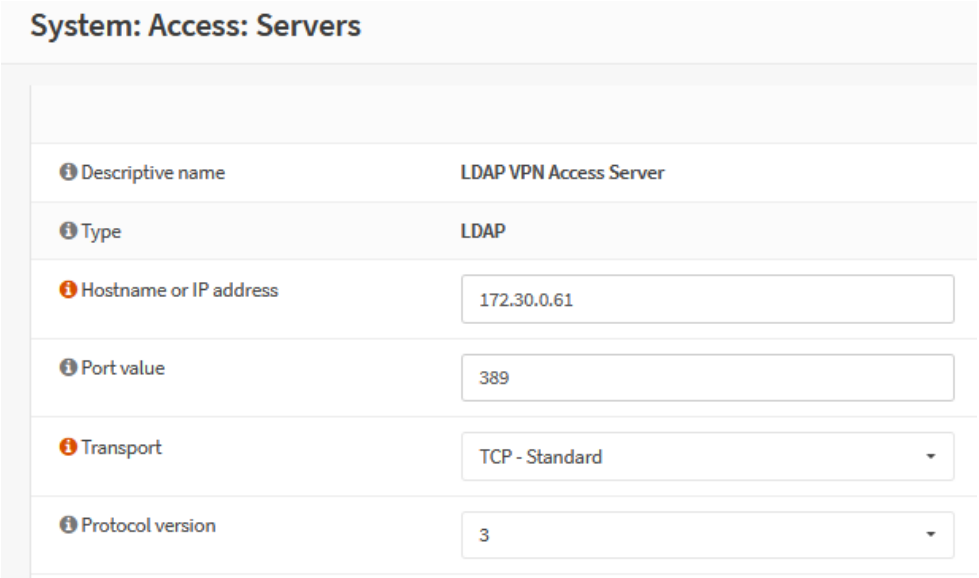
Parámetro	Valor
Descriptive name	LDAP VPN Access Server
Type	LDAP
Hostname or IP address|	172.30.0.61
Port value	389
Transport	TCP – Standard
Protocol version	3
Bind credentials UserDN	CN=ldaplinux,OU=Plataforma,OU=Departamento Tecnologias Informacion,OU=Direccion General Administracion,OU=Politicas de Usuario,DC=congreso,DC=net
Bind credentials Password	<Colocar contraseña de usuario “ldaplinux”>
Search scope	Entire Subtree
Base DN	OU=Politicas de Usuario,DC=congreso,DC=net
Authentication containers	OU=Politicas de Usuario,DC=congreso,DC=net
Extended query	&(objectClass=User)(memberof=CN=OpenVPN,CN=Users,DC=congreso,DC=net)
Initial Template	Microsoft AD
Using naming attribute	sAMAccountName

Fuente: elaboración propia.

- Pantalla:

Figura 88

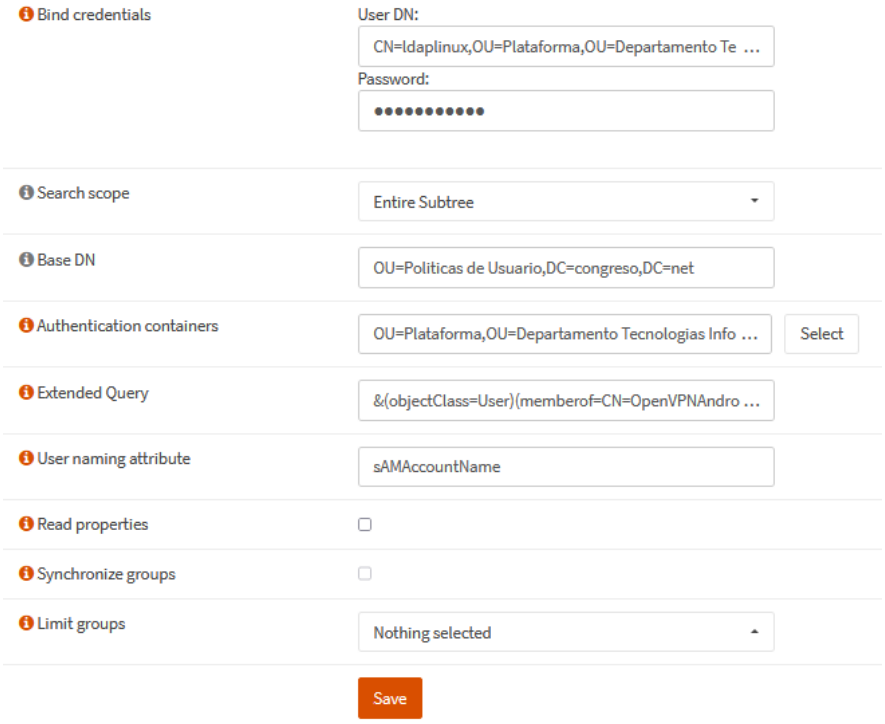
Configuración de servidor de autenticación (parte 1).



Fuente: elaboración propia.

Figura 89

Configuración de servidor de autenticación (parte 2).

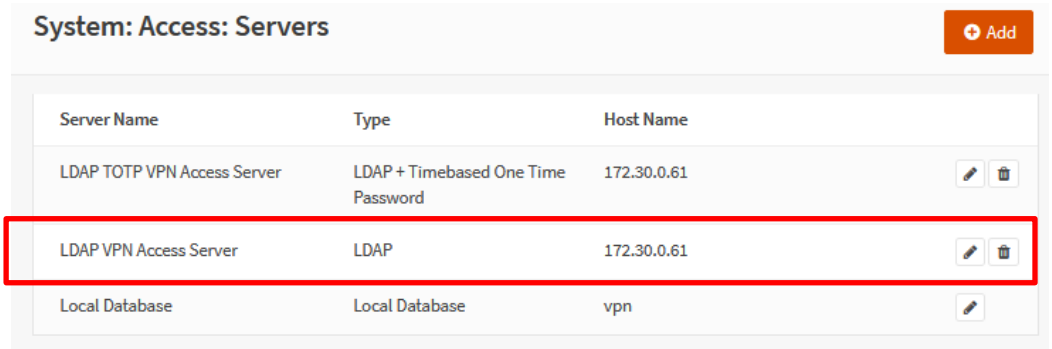


Fuente: elaboración propia.

- Resultado:

Figura 90

Lista de servidores de autenticación con tres servidores.



Fuente: elaboración propia.

3.4.5.9.3 AGREGAR USUARIOS

Una vez configurado el servidor de autenticación, se importaron los usuarios del LDAP Active Directory institucional.

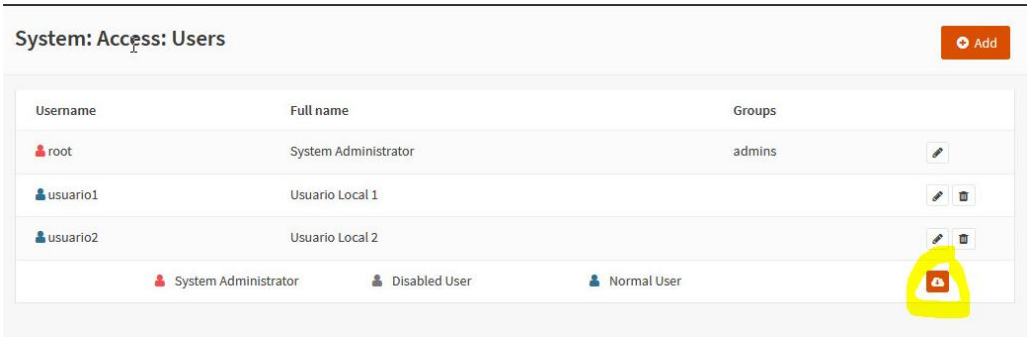
Para poder importar usuarios del LDAP, se tuvo que agregar el servidor de autenticación (creado en el punto 3.4.5.5.1) como método de autenticación de OPNsense.

NOTA: por seguridad, los usuarios importados no tienen acceso a la consola de administración de OPNsense porque no fueron incluidos en el grupo local "admins".

- Ir a System /Settings / Administration
- En Authentication > Server cambiar de "Nothing selected" a "Local database" y "LDAP TOTP VPN Access Server" y grabar con "Save".
- Ir a System / Access / Users donde apareció un nuevo botón de importación en la esquina inferior derecha:

Figura 91

Importación de usuarios.



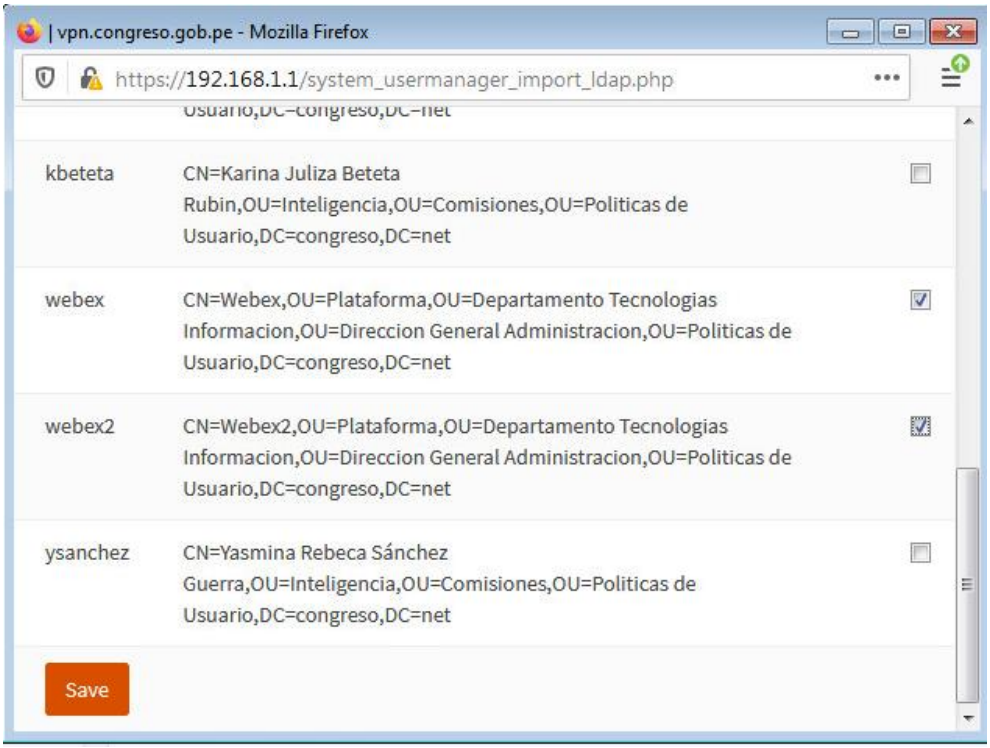
Fuente: elaboración propia.

- Hacer click en ese botón "Import" y se abre una ventana donde se listan los usuarios del dominio que cumplen los criterios del servidor de acceso LDAP.

Seleccionar los usuarios a importar (ejemplo: webex y webex2). Hacer click en "Save".

Figura 92

Selección de usuarios LDAP a importar.

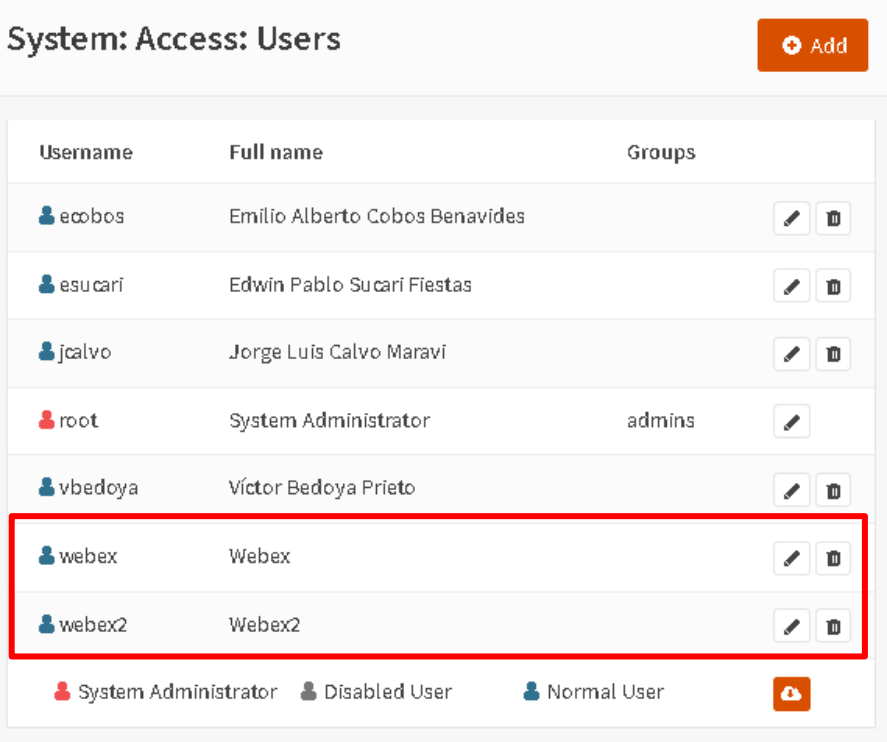


Fuente: elaboración propia.

- Resultado:

Figura 93

Usuarios importados.



Fuente: elaboración propia.

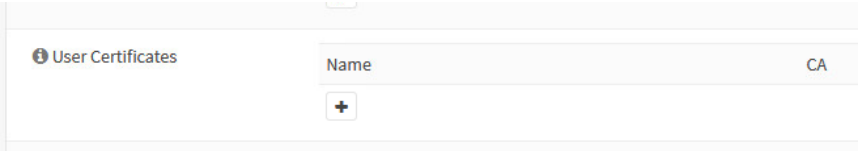
CREACIÓN DE CERTIFICADO DE USUARIO

- Editar un usuario haciendo click en la imagen de lápiz a su derecha (ejemplo: **usuario1**).

- Ir a “User certificates” y hacer click en “+”

Figura 94

Creación de certificado de usuario.

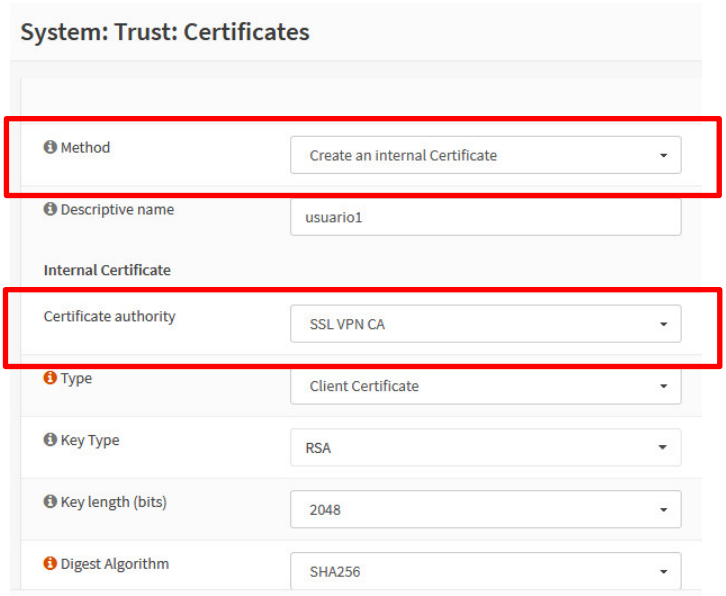


Fuente: elaboración propia.

- Seleccionar la opción “Create an internal certificate” y verificar que se usa la autoridad de certificación “SSL VPN CA” (creada en el punto 3.4.5.4).

Figura 95

Pantalla de creación de certificado de usuario (parte 1).

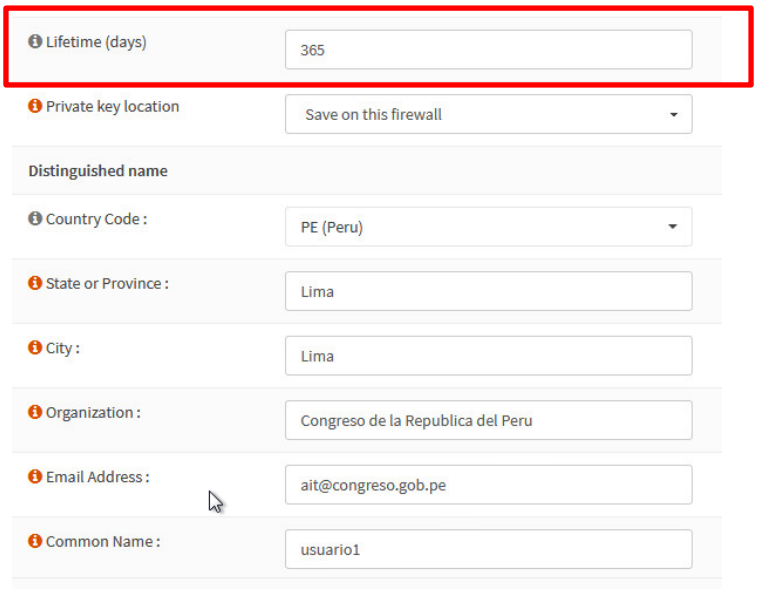


Fuente: elaboración propia.

- En esta misma ventana, elegir la duración del certificado digital, por ejemplo 365 días y grabar con “Save”.

Figura 96

Pantalla de creación de certificado de usuario (parte 2).

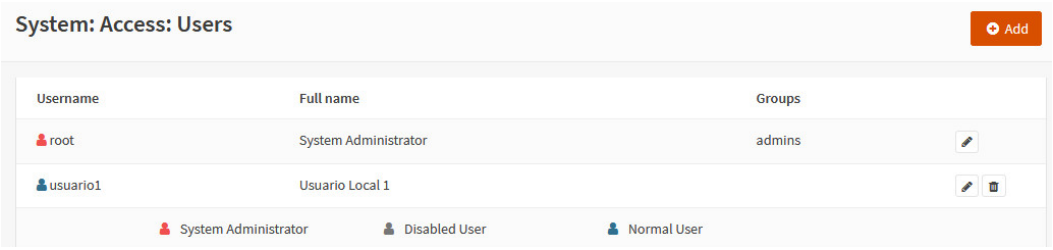


Fuente: elaboración propia.

- Resultado

Figura 97

Retorno a pantalla de lista de usuarios.



Fuente: elaboración propia.

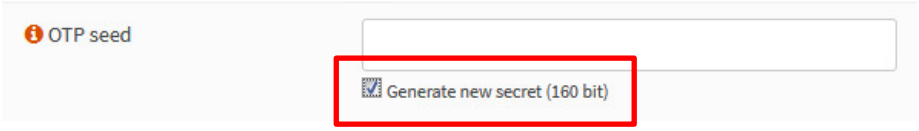
CREAR CÓDIGO QR PARA TOTP

- Editar usuario

- Ir a OTP seed y hacer click en “Generate new secret”. Grabar con “Save”.

Figura 98

Creación de código QR para TOTP.



Fuente: elaboración propia.

- Volver a OPT seed y se ve la opción “OTP QR code”. Hacer click en “Click to unhide”.

Figura 99

Mostrar código QR.

Fuente: elaboración propia.

- Copiar código QR para ser enviado a usuario.

Figura 100

Código QR para TOTP.

Fuente: elaboración propia.

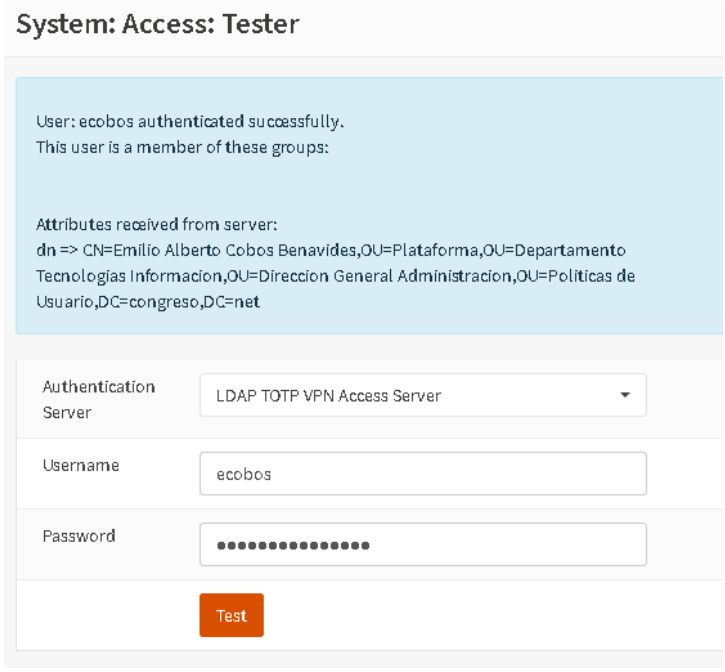
PRUEBA DE AUTENTICACIÓN DE USUARIO

- Ir a System / Access / Tester
- Para probar el acceso de un usuario, elegir el servidor de autenticación, poner las credenciales del usuario y hacer click en “Test”.

  NOTA: no olvidar colocar los 6 dígitos del token TOTP después de la contraseña de usuario.

Figura 101

Prueba de autenticación de usuario.



Fuente: elaboración propia.

3.4.5.10 CONFIGURACIÓN DEL SERVIDOR VPN PARA CLIENTES DE ESCRITORIO

Una vez que ya tenemos configurada nuestra Entidad Certificadora, Certificado de Servidor, Servidor de Autenticación LDAP y habiendo creado usuarios, se crea un nuevo servidor VPN.

- Ir a VPN / OpenVPN / Servers y hacer click en “Add”. Crearlo con los siguientes valores:

Tabla 14

Valores para configurar Servidor VPN para clientes de escritorio

Parámetro	Valor
Description	SSL VPN Server X
Server Mode	Remote Access (SSL/TLS + User Auth)
Backend for authentication	LDAP TOTP VPN Access Server

Protocol	TCP
Device Mode	tun
Interface	WAN
Local port	443
TLS Authentication	Dejar ambas habilitadas (con check)
Peer Certificate Authority	SSL VPN CA
Peer Certificate Revocation List	N/A
Server Certificate	SSLVPN Server Certificate (CA: SSL VPN CA)
DH Parameters Length	2048 bit
Encryption algorithm	AES-256-CBC (256-bit key, 128-bit block)
Auth Digest Algorithm	SHA256 (256-bit)
Hardware Crypto	No Hardware Crypto Acceleration
Certificate Depth	One (Client+Server)
Strict User / CN Matching	Habilitado (con check)
IPv4 Tunnel Network	10.10.68.0/20
IPv6 Tunnel Network	Dejar sin marcar
Redirect Gateway	Dejar sin marcar
IPv4 Local Network/s	192.168.50.0/24,172.30.1.0/24,172.20.0.0/19,172.21.0.0/19,172.22.0.0/19 ,172.23.0.0/19, 172.24.0.0/19,172.25.0.0/19, 172.26.0.0/19,172.27.0.0/19, 172.30.0.9/32,172.30.0.239/32, 172.30.6.15/32,172.30.2.15/32, 172.30.1.28/32
IPv6 Local Network/s	Dejar sin marcar
IPv4 Remote Network/s	Dejar sin marcar
IPv6 Remote Network/s	Dejar sin marcar
Concurrent connections	Dejar sin marcar
Compression	Enabled with Adaptive Compression
Type-of-Service	Dejar sin marcar
Duplicate Connections	Dejar sin marcar
Disable IPv6	Checked
Dynamic IP	Dejar sin marcar
Address Pool	**Sin marca:** no ofrece DHCP, se debe entregar número IP a cliente VPN mediante CSO.
Topology	Dejar sin marcar
DNS Default Domain	Dejar sin marcar
DNS Servers	Dejar sin marcar
Force DNS cache update	Dejar sin marcar
NTP Servers	Dejar sin marcar
NetBIOS Options	Dejar sin marcar
Client Management Port	Dejar sin marcar
Renegotiate time	0
Force CSO Login Match	Habilitado (con check)

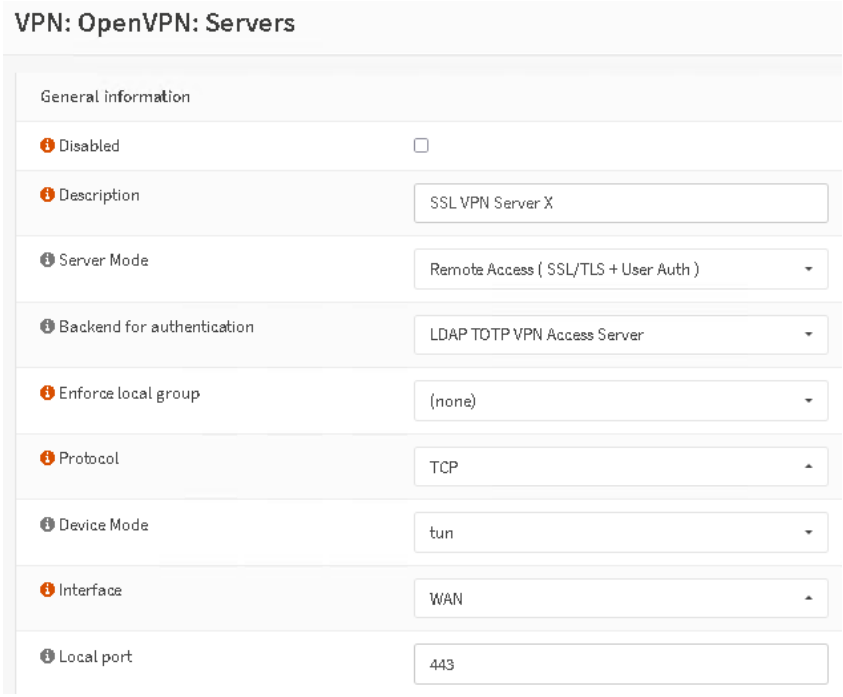
Fuente: elaboración propia.

NOTAS IMPORTANTES

- **Renegotiate time:** es necesario colocar el valor 0 (cero) para el funcionamiento de TOTP.
- **Strict User / CN matching:** se usa para evitar que un usuario use el certificado de otro usuario.
- **Force CSO Login match:** se usa para aplicar las políticas CSO.

Figura 102

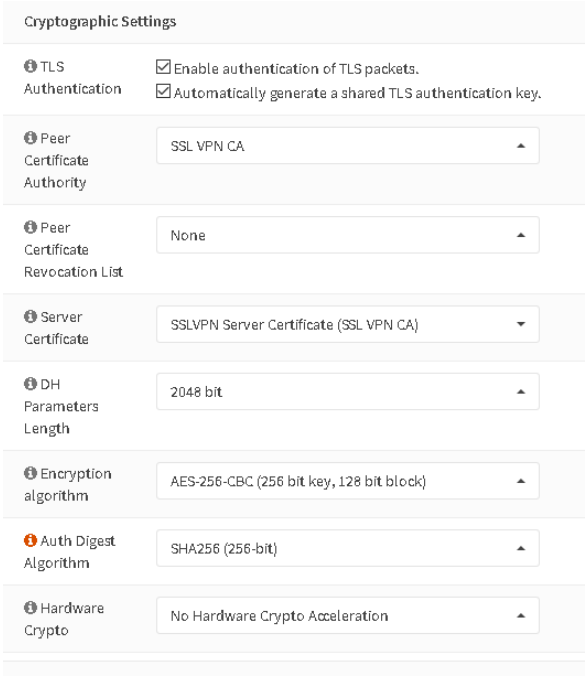
Configuración de servidor VPN para clientes de escritorio (parte 1).



Fuente: elaboración propia.

Figura 103

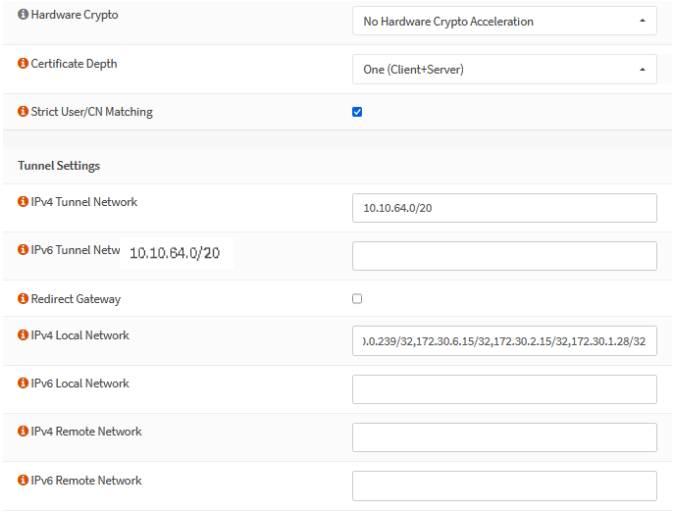
Configuración de servidor VPN para clientes de escritorio (parte 2).



Fuente: elaboración propia.

Figura 104

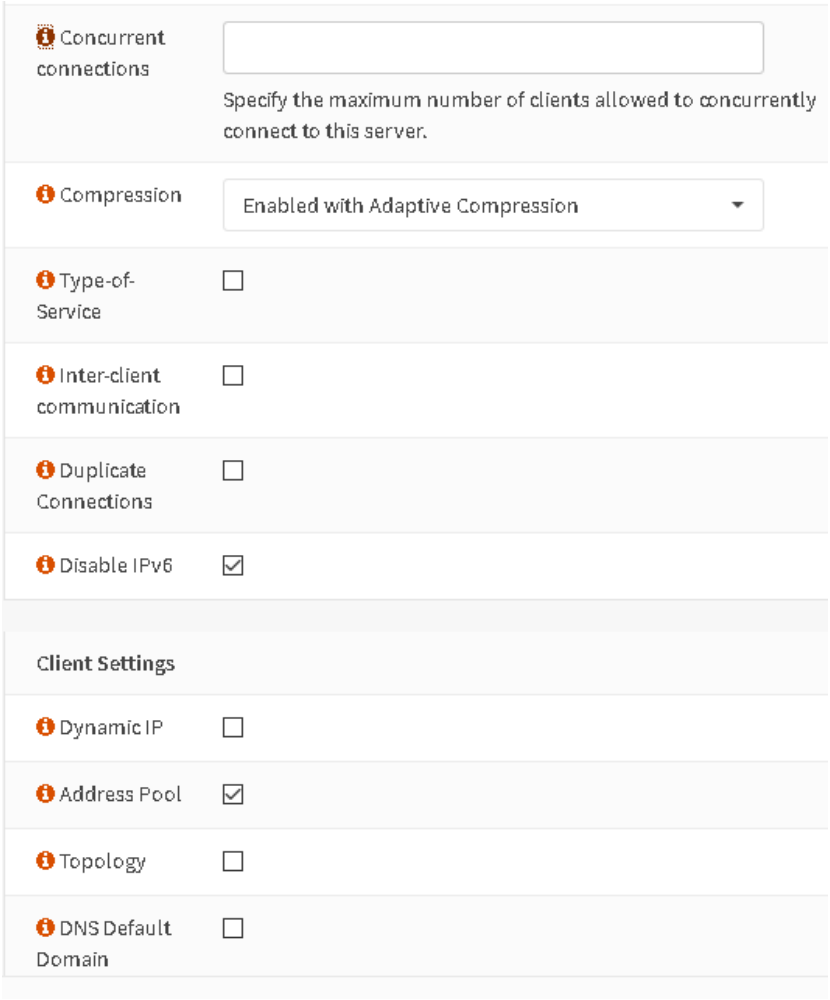
Configuración de servidor VPN para clientes de escritorio (parte 3).



Fuente: elaboración propia.

Figura 105

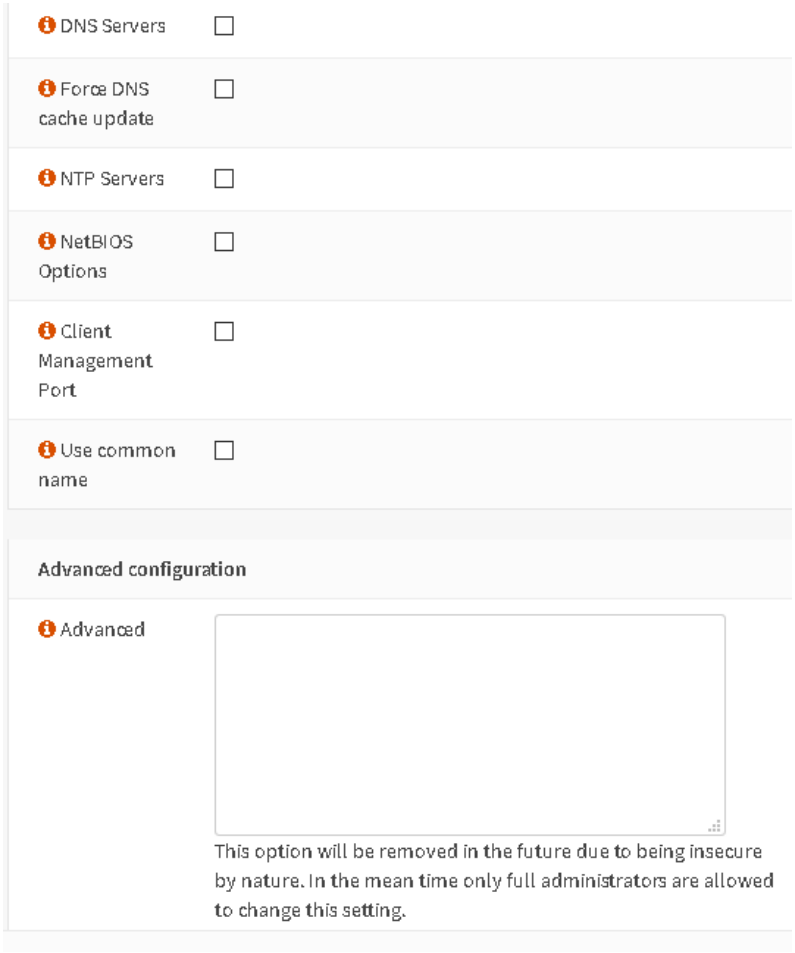
Configuración de servidor VPN para clientes de escritorio (parte 4).



Fuente: elaboración propia.

Figura 106

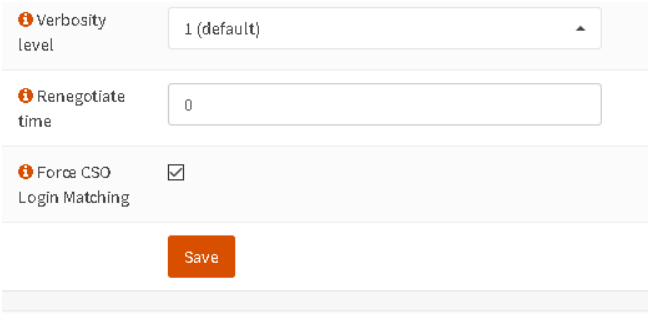
Configuración de servidor VPN para clientes de escritorio (parte 5).



Fuente: elaboración propia.

Figura 107

Configuración de servidor VPN para clientes de escritorio (parte 6).



Fuente: elaboración propia.

- Resultado:

Figura 108

Servidor VPN para clientes de escritorio creado.

Fuente: elaboración propia.

CREACIÓN DE CSO

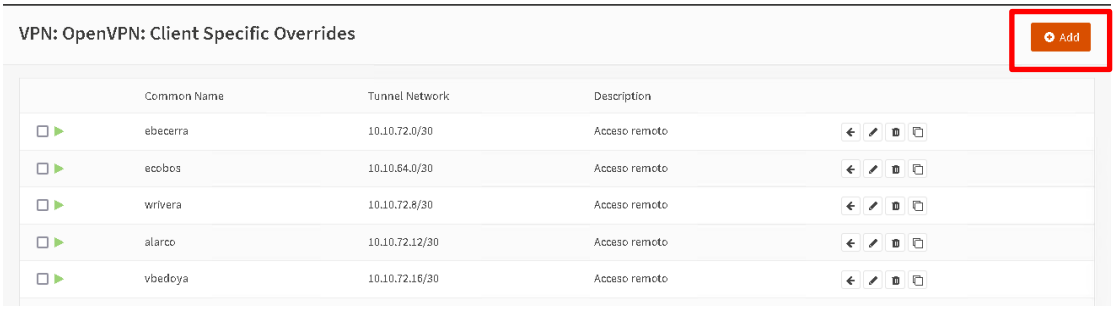
Ya configurado el servidor VPN, se procedió a realizar una configuración de gran importancia: la creación de CSOs (Client Specific Overrides). Como ya se mencionó, estas reglas permiten la asignación de configuraciones personalizadas por usuario (identificado por su nombre de usuario).

En este proyecto, se utilizó esta funcionalidad para otorgar un número IP específico a cada usuario de manera persistente, no utilizando el servicio DHCP del servidor OpenVPN. Para ello se realizaron los siguientes pasos:

- Ir a VPN / OpenVPN / Client Specific Overrides y hacer click en “Add”.

Figura 109

Agregar un CSO.



Fuente: elaboración propia.

- Crearlo con los siguientes valores:

Tabla 15

Valores para configurar un nuevo CSO

Parámetro	Valor
Servers	SSL VPN Server X
Common name	*<colocar el nombre de usuario>*
Description	Acceso remoto
IPv4 Tunnel Network	*<colocar Rango de IP para usuario (*) >*

Fuente: elaboración propia.

(*) **Rango de IP para usuario:** es una subred de 4 números IP exclusivos para el usuario correspondiente al CSO, y debe estar dentro de la subred 10.10.64.0/20 asignada en el servidor OpenVPN. Esta subred brinda un total de 4096 números IP (4094 utilizables, como se ve en la siguiente figura:

Figura 110

Cálculo de subred para los clientes VPN de escritorio.

```
Address:   10.10.64.0           00001010.00001010.0100 0000.00000000
Netmask:   255.255.240.0 = 20   11111111.11111111.1111 0000.00000000
Wildcard:  0.0.15.255           00000000.00000000.0000 1111.11111111
=>
Network:   10.10.64.0/20        00001010.00001010.0100 0000.00000000 (Class A)
Broadcast: 10.10.79.255         00001010.00001010.0100 1111.11111111
HostMin:   10.10.64.1           00001010.00001010.0100 0000.00000001
HostMax:   10.10.79.254         00001010.00001010.0100 1111.11111110
Hosts/Net: 4094                 (Private Internet)
```

Fuente: elaboración propia.

Como cada usuario necesita una subred de 4 IP, el número efectivo de usuarios de escritorio es de 4096 / 4 = 1024 usuarios. Este valor cubre las necesidades de 500 usuarios mínimos estipulados, pero puede incrementarse al modificar la configuración de subred del servidor VPN.

Es así como un primer usuario (ecobos) utiliza la primera subred de 4 IP (2 IP utilizables): 10.10.64.0/30, la que se configura en el CSO. Nótese el número IP del host máximo (10.10.64.2), el que se utiliza en el punto 3.4.5.12.2 como alias del usuario para las reglas de firewall.

Figura 111

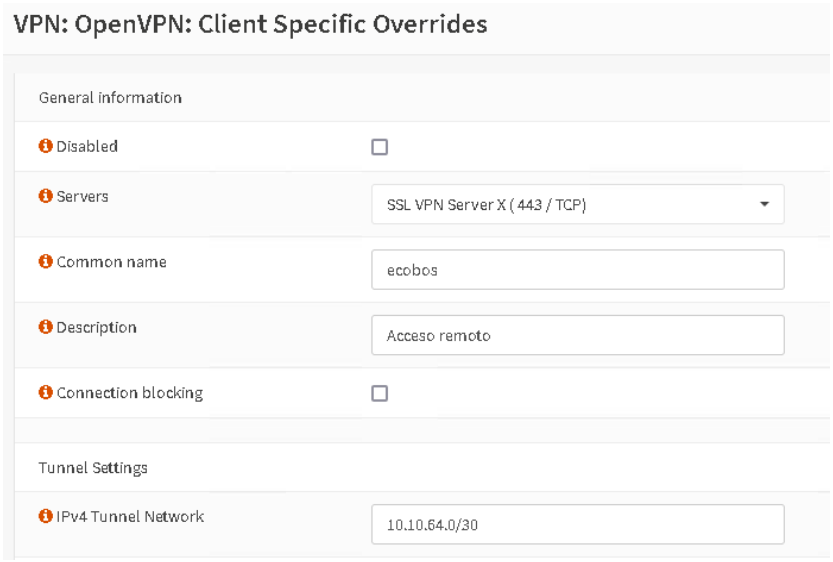
Rango de subred para CSO del primer usuario VPN de escritorio.

```
Address:   10.10.64.0           00001010.00001010.01000000.000000 00
Netmask:   255.255.255.252 = 30 11111111.11111111.11111111.111111 00
Wildcard:  0.0.0.3              00000000.00000000.00000000.000000 11
=>
Network:   10.10.64.0/30        00001010.00001010.01000000.000000 00 (Class A)
Broadcast: 10.10.64.3           00001010.00001010.01000000.000000 11
HostMin:   10.10.64.1           00001010.00001010.01000000.000000 01
HostMax:   10.10.64.2           00001010.00001010.01000000.000000 10
Hosts/Net: 2                    (Private Internet)
```

Fuente: elaboración propia.

Figura 112

Configuración de CSO para primer usuario VPN de escritorio.



Fuente: elaboración propia.

El segundo usuario (esucari) utiliza la siguiente subred de 4 IP: 10.10.64.4/30. Nótese el número IP del host máximo (10.10.64.6), el que se utiliza en el punto 3.4.5.12.2 como alias del usuario para las reglas de firewall.

Figura 113

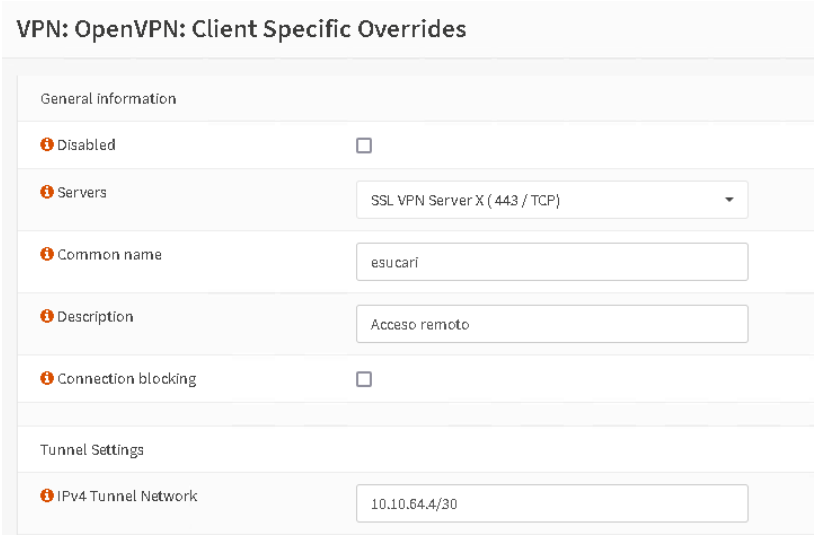
Rango de subred para CSO del segundo usuario VPN de escritorio.

```
Address:   10.10.64.4           00001010.00001010.01000000.000001 00
Netmask:   255.255.255.252 = 30 11111111.11111111.11111111.111111 00
Wildcard:  0.0.0.3              00000000.00000000.00000000.000000 11
=>
Network:   10.10.64.4/30        00001010.00001010.01000000.000001 00 (Class A)
Broadcast: 10.10.64.7           00001010.00001010.01000000.000001 11
HostMin:   10.10.64.5           00001010.00001010.01000000.000001 01
HostMax:   10.10.64.6           00001010.00001010.01000000.000001 10
Hosts/Net: 2                    (Private Internet)
```

Fuente: elaboración propia.

Figura 114

Configuración de CSO para segundo usuario VPN de escritorio.



Fuente: elaboración propia.

3.4.5.11 CONFIGURACIÓN DEL SERVIDOR VPN PARA CLIENTES MÓVILES ANDROID

- Ir a VPN / OpenVPN / Servers y hacer click en “Add”. Crearlo con los siguientes valores:

Tabla 16

Valores para configurar Servidor VPN para clientes móviles Android

Parámetro	Valor
Description	SSL VPN Server Android
Server Mode	Remote Access (SSL/TLS + User Auth)
Backend for authentication	LDAP VPN Access Server
Protocol	TCP
Device Mode	tun
Interface	WAN
Local port	8443
TLS Authentication	Dejar ambas habilitadas (con check)
Peer Certificate Authority	SSL VPN CA
Peer Certificate Revocation List	N/A
Server Certificate	SSLVPN Server Certificate (CA: SSL VPN CA)

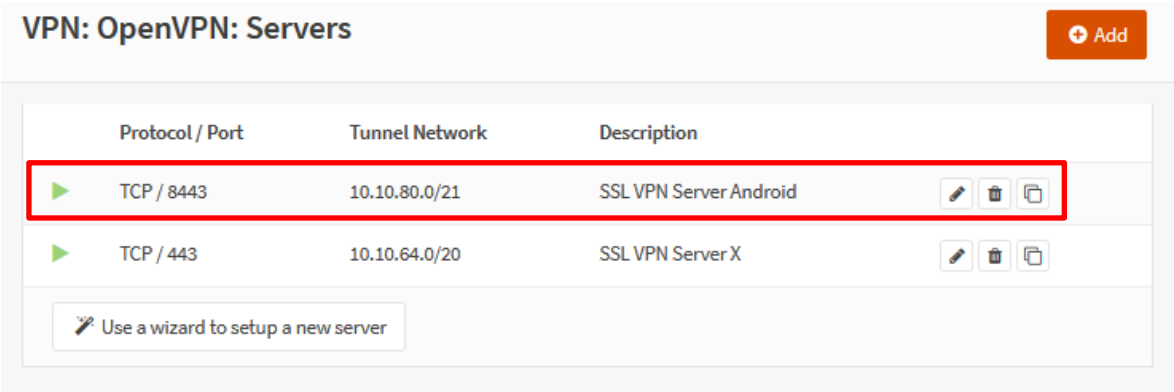
DH Parameters Length	2048 bit
Encryption algorithm	AES-256-CBC (256-bit key, 128-bit block)
Auth Digest Algorithm	SHA256 (256-bit)
Hardware Crypto	No Hardware Crypto Acceleration
Certificate Depth	One (Client+Server)
Strict User / CN Matching	Habilitado (con check)
IPv4 Tunnel Network	10.10.80.0/21
IPv6 Tunnel Network	Dejar sin marcar
Redirect Gateway	Dejar sin marcar
IPv4 Local Network/s	192.168.50.0/24,172.30.1.30/32,172.30.0.138/32
IPv6 Local Network/s	Dejar sin marcar
IPv4 Remote Network/s	Dejar sin marcar
IPv6 Remote Network/s	Dejar sin marcar
Concurrent connections	Dejar sin marcar
Compression	Enabled with Adaptive Compression
Type-of-Service	Dejar sin marcar
Duplicate Connections	Dejar sin marcar
Disable IPv6	Checked
Dynamic IP	Dejar sin marcar
Address Pool	**Con marca:** ofrece pool DHCP en rango indicado en **IPv4 Tunnel Network.**
Topology	Dejar sin marcar
DNS Default Domain	Dejar sin marcar
DNS Servers	Dejar sin marcar
Force DNS cache update	Dejar sin marcar
NTP Servers	Dejar sin marcar
NetBIOS Options	Dejar sin marcar
Client Management Port	Dejar sin marcar
Renegotiate time	0
Force CSO Login Match	Dejar sin marcar

Fuente: elaboración propia.

- Resultado:

Figura 115

Servidor SSL VPN para dispositivos Android.



Fuente: elaboración propia.

3.4.5.12 REGLAS DE FIREWALL

3.4.5.12.1 REGLAS WAN

EN INTERFACE WAN

Para permitir conexiones de cliente VPN, debimos permitir el acceso al puerto del servidor OpenVPN en la interfaz WAN. Como usamos dos servidores VPN (uno para clientes de escritorio y otro para clientes móviles), necesitamos abrir el puerto de cada uno de ellos hacia Internet.

- Server “SSL VPN Server X”: protocolo TCP puerto 443
- Server “SSL VPN Server Android”: protocolo TCP puerto 8443

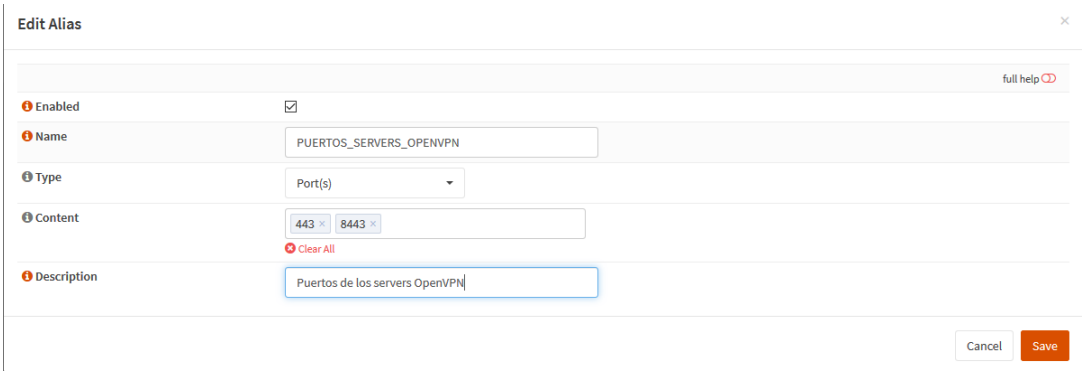
Para facilitar esto, usamos un alias de firewall denominado PUERTOS_SERVERS_OPENVPN que contenga los dos puertos.

- Ir a Firewall / Aliases y agregar un alias con el botón “+” en la esquina inferior derecha.

- Llenar los campos correspondientes y grabar.

Figura 116

Creación de Alias para puertos VPN externos.

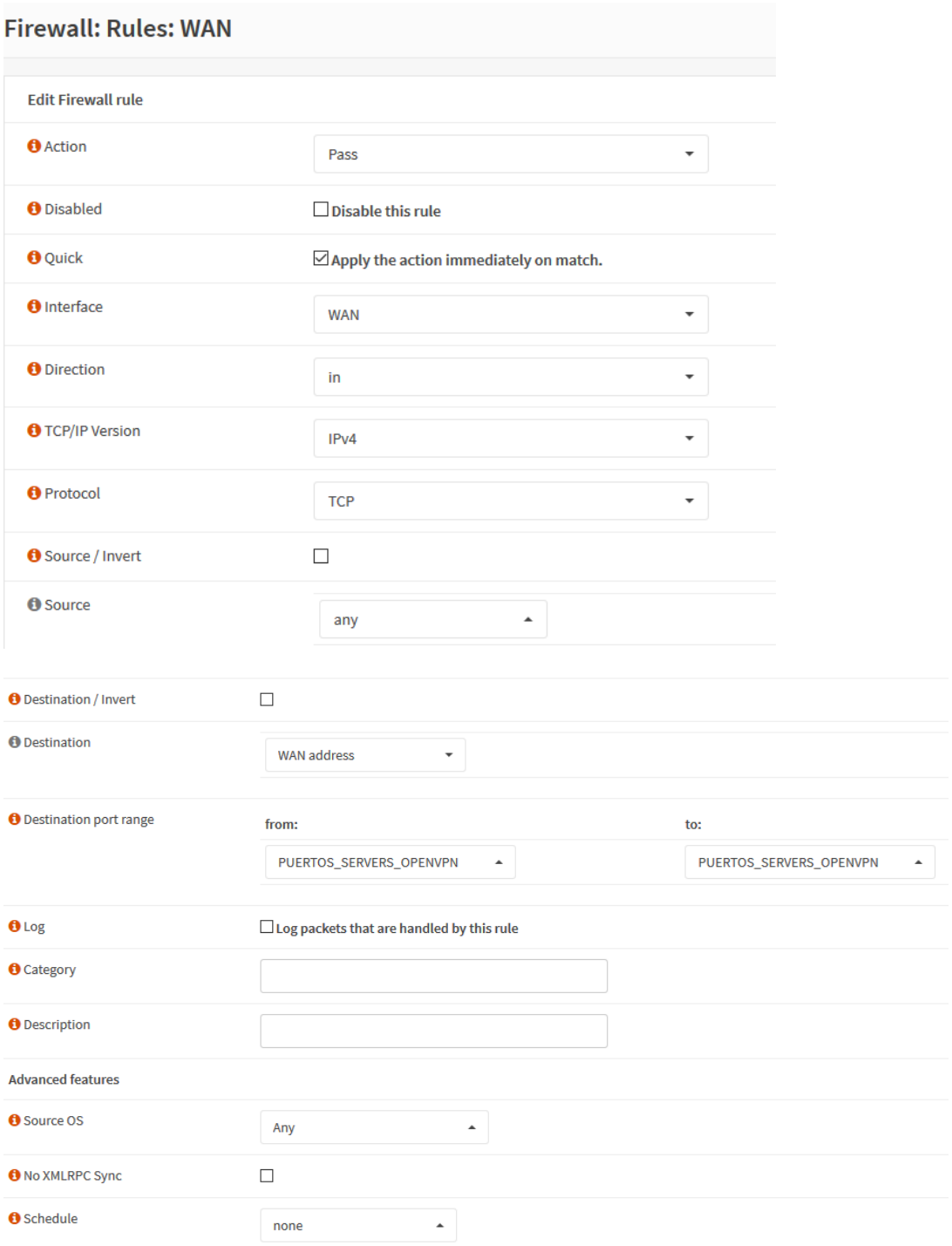


Fuente: elaboración propia.

- Ahora, crear una regla de firewall que utilice el alias PUERTOS_SERVERS_OPENVPN.
  - Crear la regla de acceso en la interface WAN:
    - **Acción:** pasar (pass)
    - **Dirección:** entrada (in)
    - **Protocolo:** TCP versión 4
    - **Destino:** dirección WAN
    - **Origen:** cualquiera
    - **Rango de puertos:** usar el alias PUERTOS_SERVERS_OPENVPN

Figura 117

Creación de regla de acceso WAN.

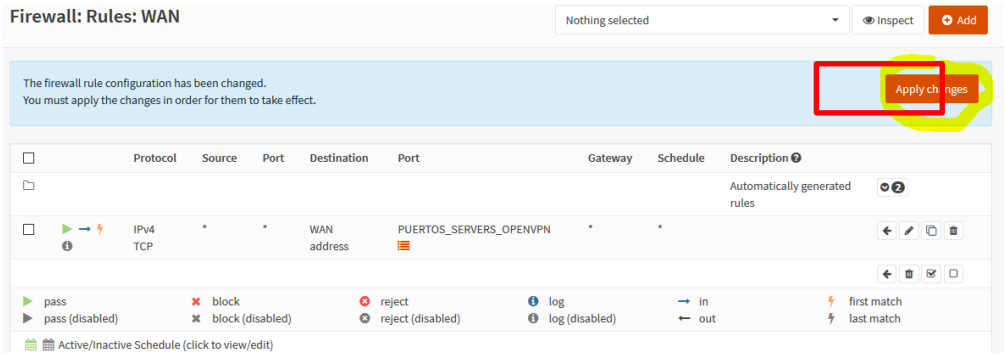


Fuente: elaboración propia.

- Aplicar los cambios:

Figura 118

Aplicar cambios en Firewall.



Fuente: elaboración propia.

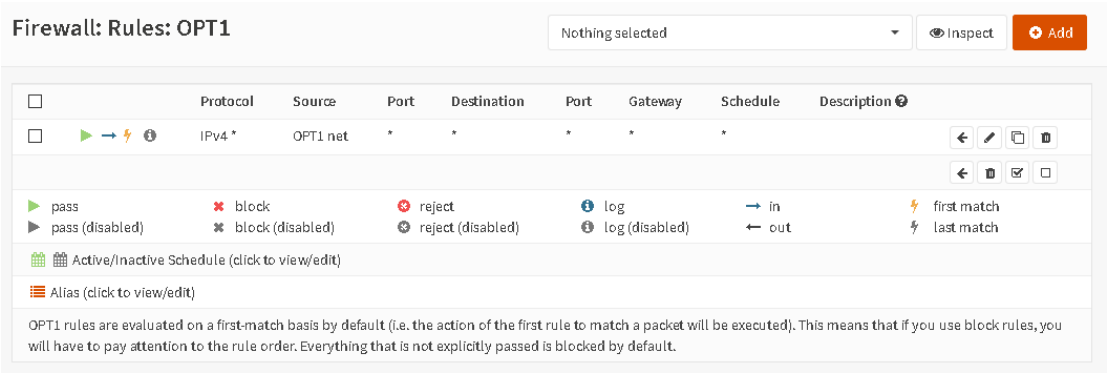
3.4.5.12.2 REGLAS DMZ_VPN

EN INTERFACE OPT1

La red intermedia entre la WAN (Internet) y la LAN (red del Congreso) se denomina DMZ_VPN. Por ello, es necesario permitir el acceso en esta red (asignada a la interface OPT1). Crear regla como se muestra en la siguiente figura:

Figura 119

Regla permisiva en interface OPT1.



Fuente: elaboración propia.

NOTA: esta regla permite el acceso de cualquier origen y puerto desde OPT1 hacia cualquier destino, porque las reglas OPENVPN son las que restringen el acceso sobre esta interface.

EN INTERFACE OPENVPN

Es en esta interface donde se configuran las reglas de acceso para los usuarios.

REGLA DE EJEMPLO 1: ACCESO A SERVIDORES (REGLA DE EJEMPLO)

Para permitir conexiones del cliente VPN hacia los servidores internos (servicios web), se deben crear reglas de firewall. Para simplificar la configuración de reglas, se utiliza la funcionalidad de "alias". En este ejemplo se permite el acceso del alias RANGO_VPN_DESKTOP hacia el alias SERVIDORES_CONGRESO y puertos con alias PUERTOS_WEB_SERVERS_CONGRESO. De esta manera se configura el acceso de todo un rango de IPs (los de los clientes VPN de escritorio) hacia un conjunto de servidores y puertos con usa sola regla de firewall.

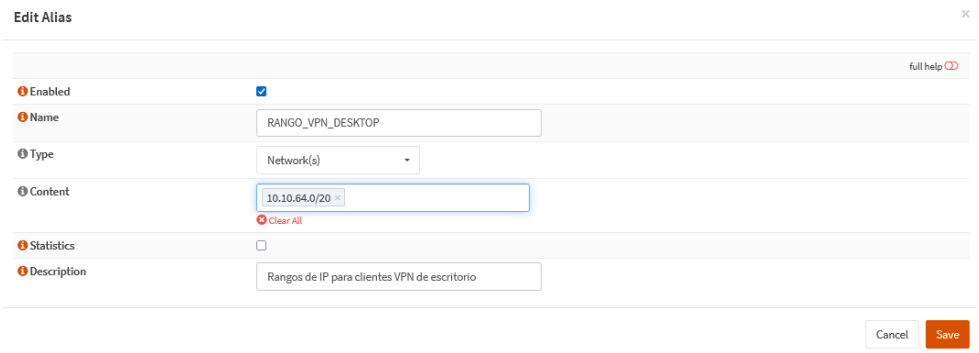
Paso 1: CREACIÓN DE ALIASES

ALIAS RANGO_VPN_DESKTOP

- Ir a Firewall / Aliases y agregar un alias con el botón "+" en la esquina inferior derecha.
- Llenar los campos correspondientes y grabar.

Figura 120

Creación de alias RANGO_VPN_DESKTOP.



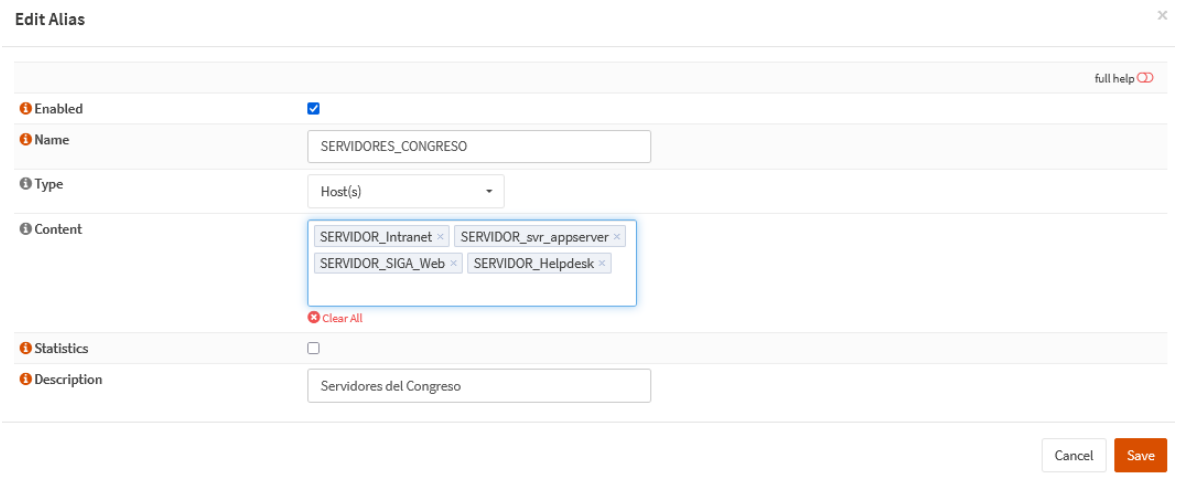
Fuente: elaboración propia.

ALIAS SERVIDORES_CONGRESO

- Ir a Firewall / Aliases y agregar un alias con el botón "+" en la esquina inferior derecha.
- Llenar los campos (en este caso se deben crear alias para los servidores de manera similar a la creación de alias RANGO_VPN_CONGRSO) y grabar.

Figura 121

Creación de alias SERVIDORES_CONGRESO.



Fuente: elaboración propia.

ALIAS PUERTOS_WEB_SERVERS_CONGRESO

- Ir a Firewall / Aliases y agregar un alias con el botón “+” en la esquina inferior derecha.
- Llenar los campos como se muestra en la siguiente figura y grabar.

Figura 122

Creación de alias PUERTOS_WEB_SERVERS_CONGRESO.

Fuente: elaboración propia.

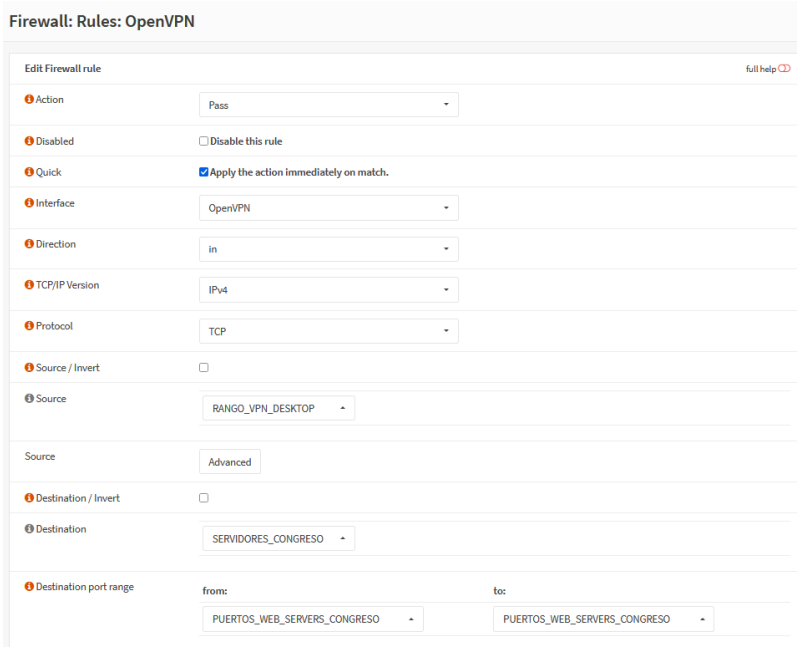
- Aplicar los cambios.

Paso 2: CREACIÓN DE REGLA DE FIREWALL PARA ACCESO A SERVIDORES

- Ir a Firewall / Rules / OpenVPN y agregar una regla con el botón “+” en la esquina superior derecha.
- Llenar los campos como se muestra en la siguiente figura y grabar.

Figura 123

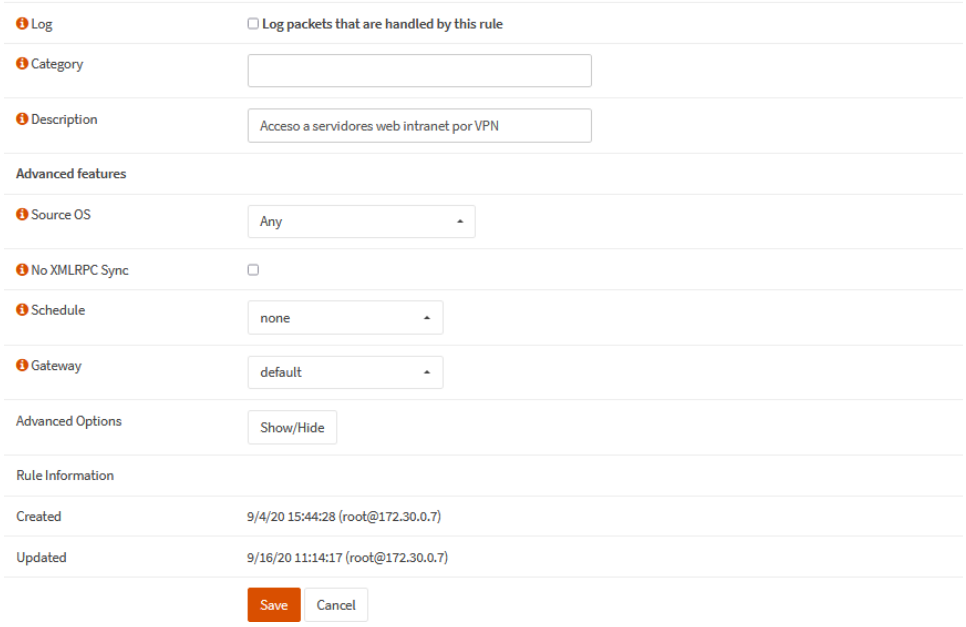
Creación de regla de firewall para acceso a servidores (parte 1).



Fuente: elaboración propia.

Figura 124

Creación de regla de firewall para acceso a servidores (parte 2).



Fuente: elaboración propia.

- Aplicar los cambios.

REGLA DE EJEMPLO 2: CREACIÓN DE REGLA DE FIREWALL PARA ACCESO DE USUARIO A ESCRITORIO REMOTO

Una vez establecida la conexión VPN, el usuario puede realizar una conexión al escritorio remoto de su PC de la oficina. Para ello, se crearon reglas que contienen:

- Alias al número IP que recibe la PC o laptop del usuario VPN (ejemplo: Alias "ecobos_vpn" para nro. IP 10.10.64.2).
- Alias al número IP de la PC en la oficina (ejemplo: Alias "ecobos_pc" para nro. IP 172.21.7.103).

Para ello, se debieron crear los alias para la PC del usuario y la PC de la oficina, y luego crear la regla de firewall que permita el acceso por el puerto 3389 (protocolo RDP de acceso remoto).

Nota: se creó una regla de acceso por usuario, en base a sus alias definidos.

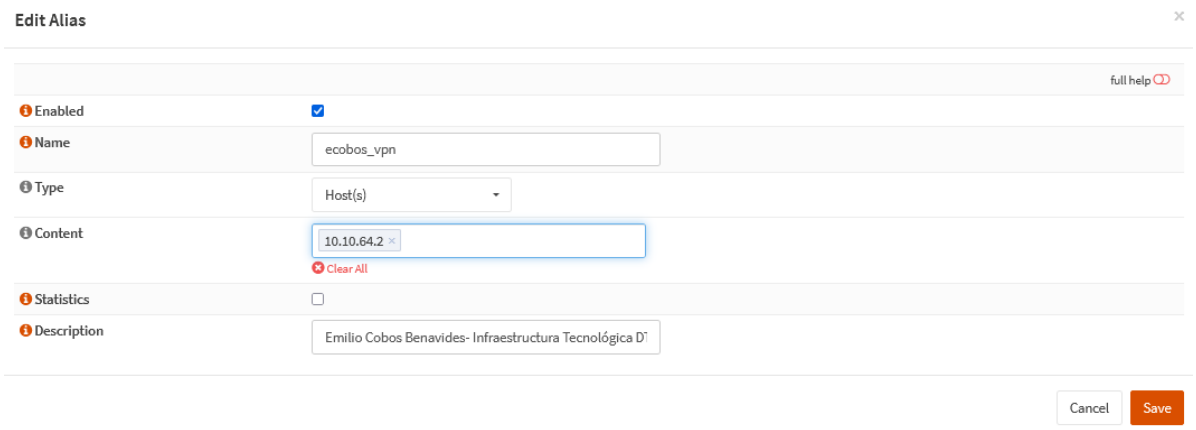
Paso 1: CREACIÓN DE ALIASES

ALIAS ecobos_vpn

- Ir a Firewall / Aliases y agregar un alias con el botón "+" en la esquina inferior derecha.
- Llenar los campos correspondientes y grabar.

Figura 125

Creación de alias ecobos_vpn.



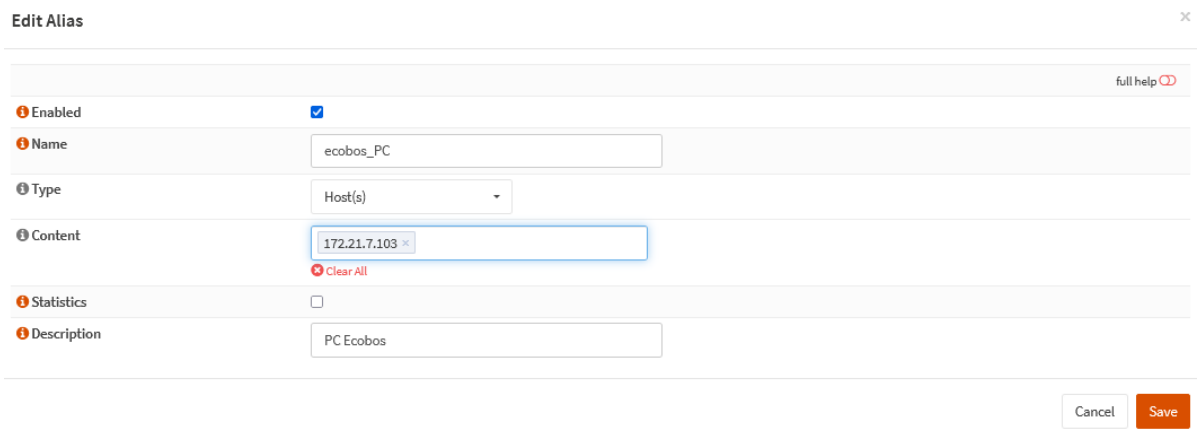
Fuente: elaboración propia.

ALIAS ecobos_pc

- Ir a Firewall / Aliases y agregar un alias con el botón "+" en la esquina inferior derecha.
- Llenar los campos correspondientes y grabar.

Figura 126

Creación de alias ecobos_pc.



Fuente: elaboración propia.

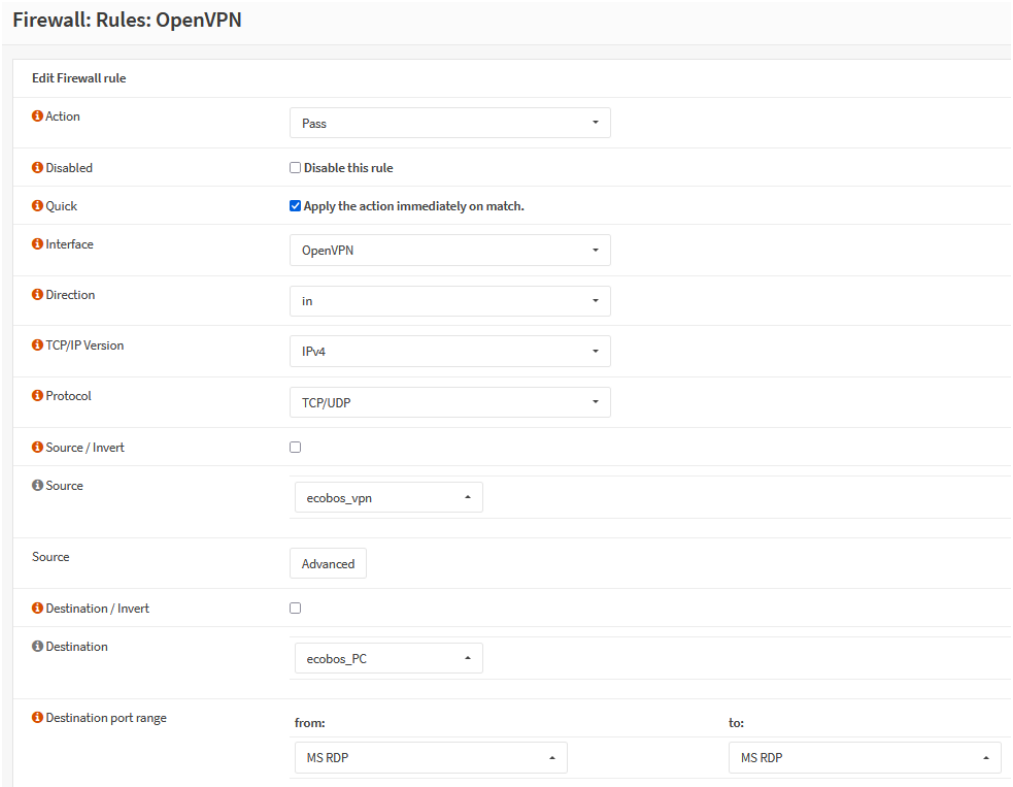
- Aplicar los cambios.

Paso 2: CREACIÓN DE REGLA DE FIREWALL PARA ACCESO A PC DE ESCRITORIO EN EL CONGRESO

- Ir a Firewall / Rules / OpenVPN y agregar una regla con el botón "+" en la esquina superior derecha.
- Llenar los campos como se muestra en la siguiente figura y grabar.

Figura 127

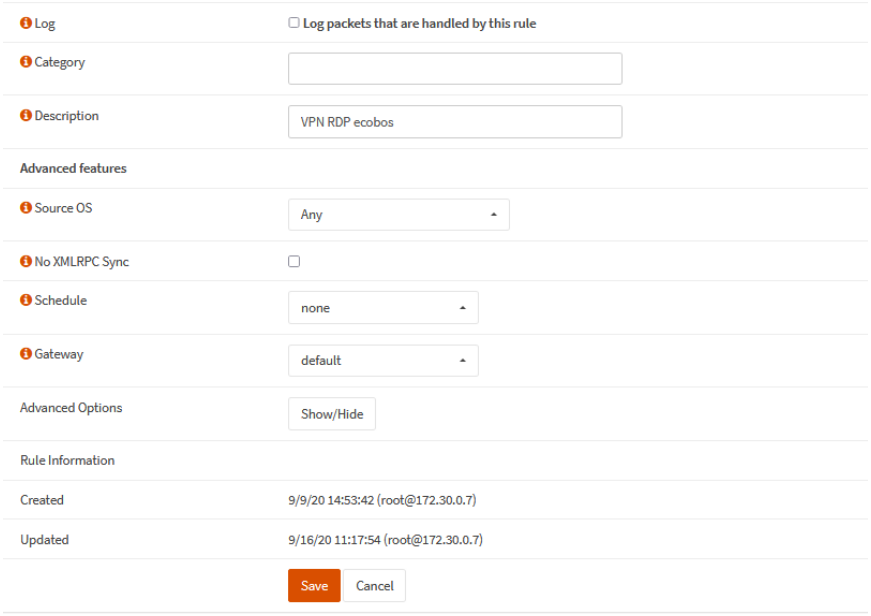
Creación de regla de firewall para acceso a escritorio remoto (parte 1).



Fuente: elaboración propia.

Figura 128

Creación de regla de firewall para acceso a escritorio remoto (parte 2).



Fuente: elaboración propia.

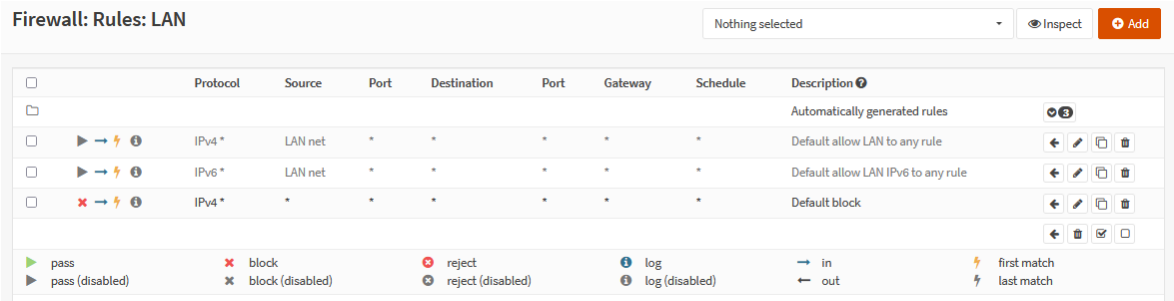
- Aplicar los cambios.

3.4.5.12.3 REGLAS DE ADMINISTRACIÓN EN INTERFACE LAN

La interface LAN recibe reglas automáticas para el acceso vía web al equipo desde la interface LAN solamente, por lo que no se hace ningún trabajo adicional.

Figura 129

Reglas de acceso a consola web por omisión.



Fuente: elaboración propia.

3.4.5.13 EXPORTAR CONFIGURACIÓN DE CLIENTE

Ya teniendo listo el servicio VPN, se exportó la configuración para cada cliente. Esta configuración se guarda en un archivo empaquetado (extensión .zip)

- Ir a VPN / OpenVPN / Client Export y seleccionar las opciones como se ve en la siguiente tabla.

Tabla 17

Parámetros para exportar cliente

Parámetro	Valor
Remote Access Server	SSL VPN Server X TCP:443
Export type	Archive
Hostname	vpn.congreso.gob.pe
P12 Password/confirm	<en blanco>
Disable password save	<seleccionado> (con check)

Fuente: elaboración propia.

- Descargar el archivo correspondiente al usuario. Ejemplo: webex (que es un usuario de dominio)

Figura 130

Pantalla de exportación de archivo de configuración de usuario.

Fuente: elaboración propia.

Este archivo y el código QR asociado fueron enviados a los usuarios.

3.4.5.14 CONFIGURAR CLIENTE

Por último, se configura el cliente en el equipo del usuario (PC o laptop).

CONFIGURAR GENERADOR TOTP

- Utilizar la aplicación Google Authenticator en su smartphone Android (descargarla de Google Play Store de ser necesario).
- En la aplicación haga click en el botón "+" en la esquina inferior derecha, elegir "Escanear un código QR" y escanear el código QR recibido.
- Así, se agrega una entrada en su lista de códigos generados con el nombre <nombre de usuario>@vpn

NOTA: también se pueden utilizar aplicaciones Microsoft Authenticator y FreeOTP.

CONFIGURAR CLIENTE VPN

- Descargar cliente de VPN OpenVPN desde https://openvpn.net/community-downloads/ (versión vigente durante la ejecución del proyecto: OpenVPN 2.4.9). Seleccionar la versión adecuada (Windows 7/8 o Windows 10):

Figura 131

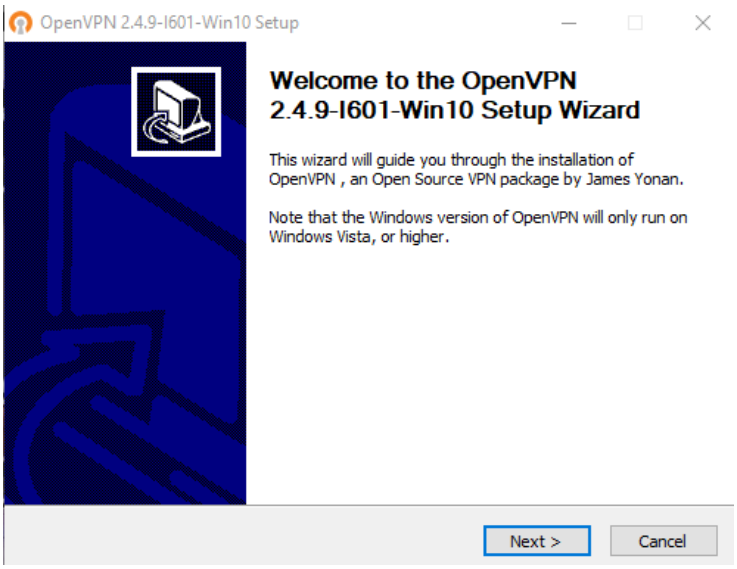
Descarga de cliente OpenVPN.

Fuente: elaboración propia.

- Instalar el cliente con las siguientes opciones:

Figura 132

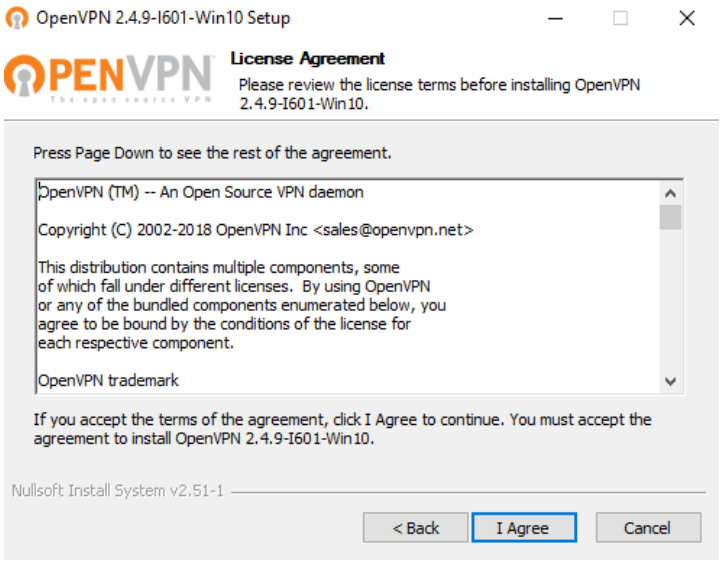
Instalación de cliente OpenVPN (paso 1).



Fuente: elaboración propia.

Figura 133

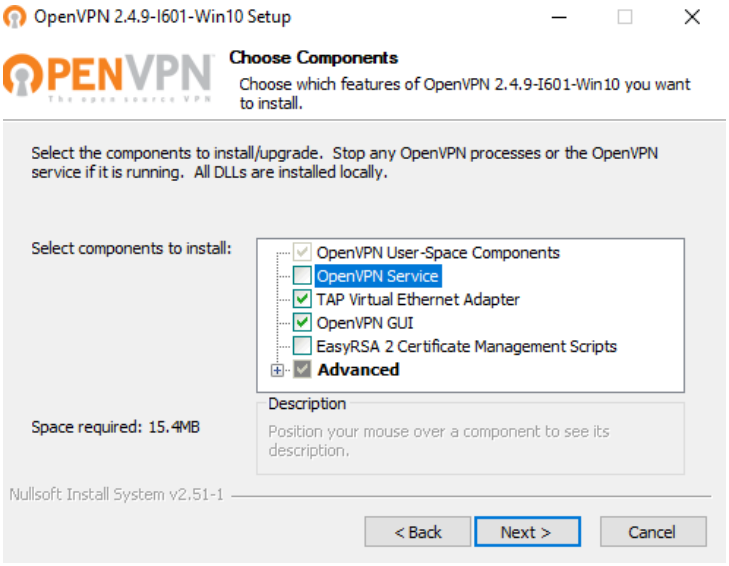
Instalación de cliente OpenVPN (paso 2).



Fuente: elaboración propia.

Figura 134

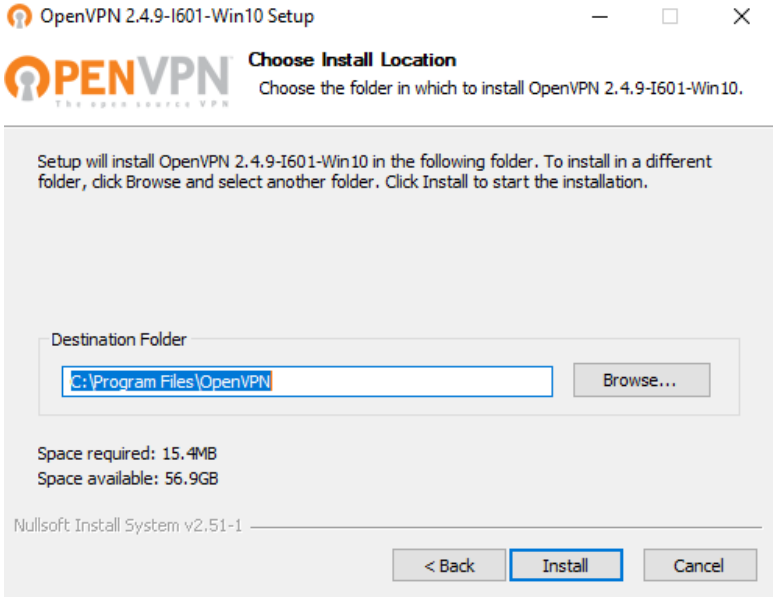
Instalación de cliente OpenVPN (paso 3).



Fuente: elaboración propia.

Figura 135

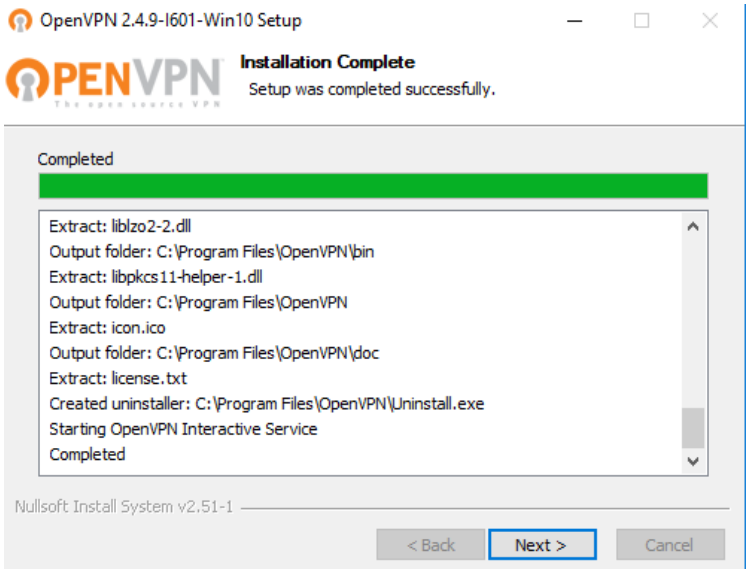
Instalación de cliente OpenVPN (paso 4).



Fuente: elaboración propia.

Figura 136

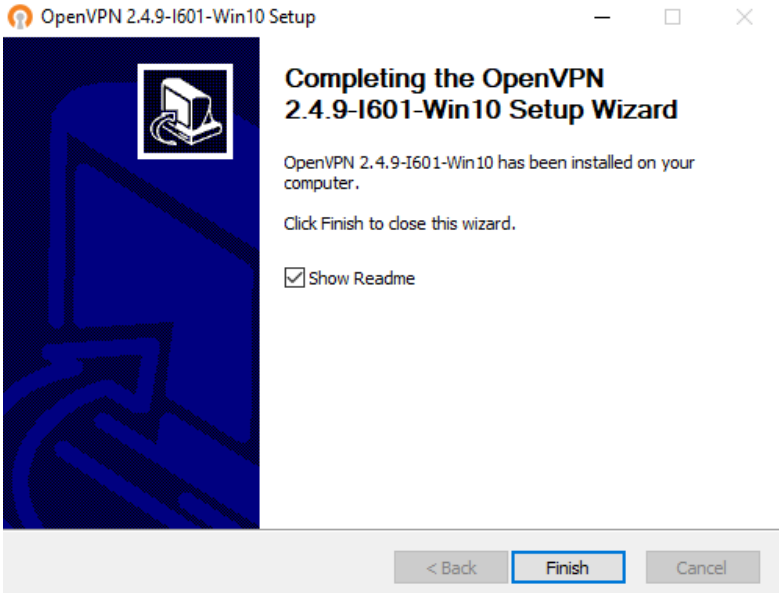
Instalación de cliente OpenVPN (paso 5).



Fuente: elaboración propia.

Figura 137

Instalación de cliente OpenVPN (paso 6).



Fuente: elaboración propia.

- Ejecutar el acceso directo de OpenVPN que se encuentra en el escritorio de Windows.

Figura 138

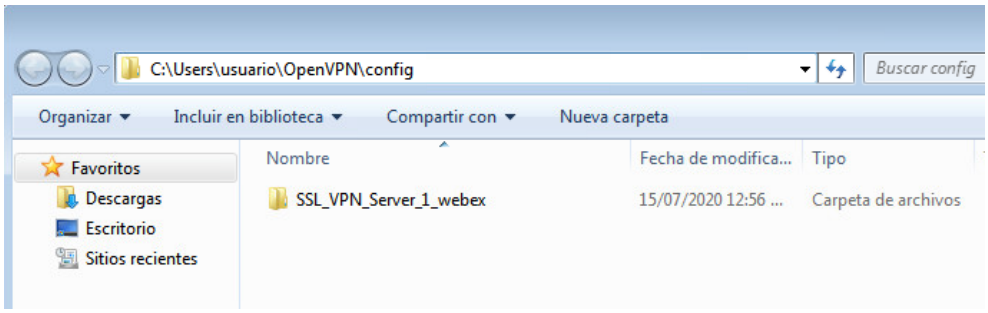
Acceso directo de OpenVPN.

Fuente: elaboración propia.

- Desempaquetar el archivo de configuración de usuario descargado del sistema VPN (ejemplo: "SSL_VPN_Server_1_webex.zip") en el directorio c:\users\<*NOMBRE DE USUARIO*>\OpenVPN\config:

Figura 139

Instalación de archivo de configuración de usuario.

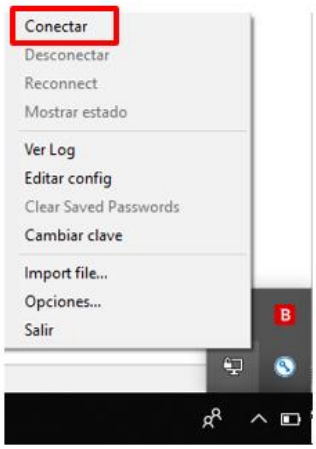


Fuente: elaboración propia.

- Acceder haciendo click derecho sobre el ícono de OpenVPN GUI en la esquina inferior derecha de la pantalla y seleccionar la opción “Conectar”

Figura 140

Conectar a VPN (paso 1).

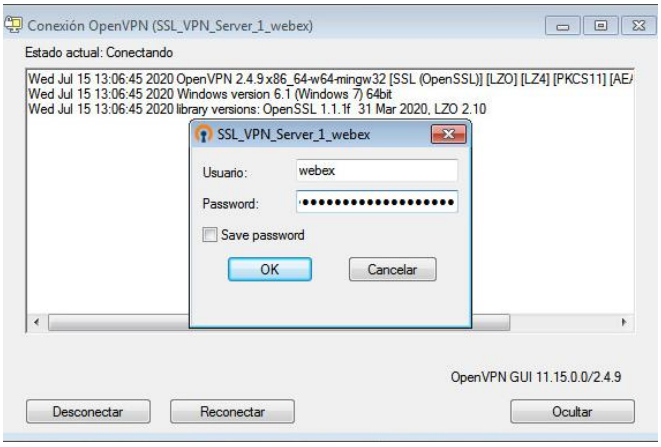


Fuente: elaboración propia.

- En esta ventana, ingresar la contraseña de dominio seguida del código de seis dígitos indicados en la app de autenticación (Google Authenticator, Microsoft Authenticator y/o FreeOTP), y haciendo click en “OK”

Figura 141

Conectar a VPN (paso 2).



Fuente: elaboración propia.

- Validar el acceso a la VPN poniendo el cursor sobre el ícono de OpenVPN GUI.

3.4.6 ETAPA 6: DOCUMENTACIÓN Y CAPACITACIÓN

Luego de la implementación de la plataforma se procedió a crear tres guías:

- Guía de implementación de la plataforma OPNsense (base material para el punto 3.4.5).
- Guía de administración, para la gestión de usuarios y exportación de paquete para clientes VPN, la cual se muestra en el Anexo 2.
- Guía de instalación de cliente OpenVPN de escritorio, la que se muestra en el Anexo 3.
- Guía de configuración de Cliente OpenVPN para dispositivos móviles de congresistas, se encuentra en el Anexo 4.

Se capacitó a dos técnicos del área de Infraestructura Tecnológica para la configuración de los clientes OpenVPN en las PC de usuarios y dispositivos móviles, y se capacitó a uno de ellos para que realice también la administración de la plataforma en lo que corresponde a gestión de usuarios y realización de copias de seguridad de la configuración.

CAPÍTULO IV. RESULTADOS

4 RESULTADOS

Luego de la implementación y puesta en producción de la plataforma OPNsense, realizamos la verificación de la consecución de los objetivos planteados en el punto 3.2.2. Para ello, se procedió a recabar evidencia que comprende los siguientes puntos:

- Número de cuentas de usuario creadas.
- Acceso a recursos institucionales.
    - Conexión a VPN - cliente de escritorio.
    - Escritorio remoto.
    - Servicios web.
- Acceso a los servicios web de sistema de asistencia y votación remotos.
    - Conexión a VPN – cliente móvil.
    - Acceso a sistema de asistencia y votación remota.
- Acceso a servidores de desarrollo.
- Funcionamiento de la plataforma.
    - Concurrencia de usuarios de escritorio.
    - Concurrencia de usuarios móviles.
- Uso de recursos.
    - Tráficos de datos.
    - Uso de CPU, memoria y almacenamiento.

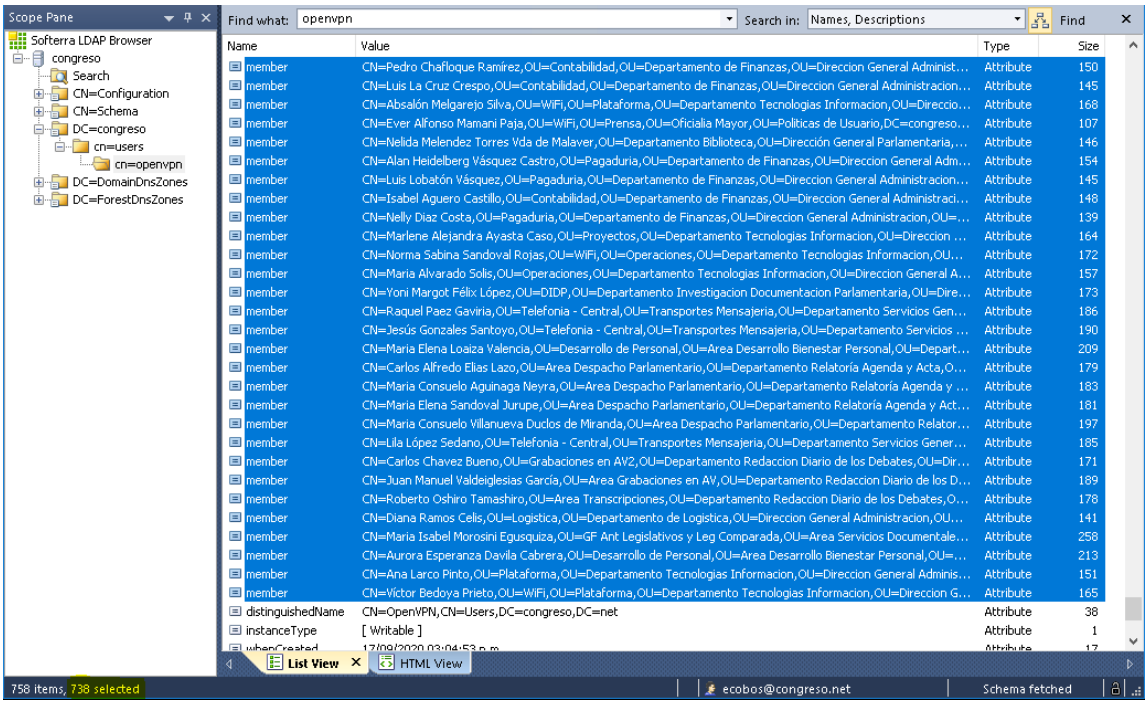
Para finalmente analizar estos resultados obtenidos con respecto a los objetivos, permitiendo así determinar la consecución de los mismos.

4.1 NÚMERO DE CUENTAS DE USUARIO CREADAS

En la siguiente figura se muestra la cantidad de usuarios en el grupo VPN del Active Directory (738 en la actualidad, mostrados en la esquina inferior izquierda de la imágen), los que son importados a la lista de usuarios de OPNsense.

Figura 142

Evidencia de número de usuarios en grupo OpenVPN del Active Directory.



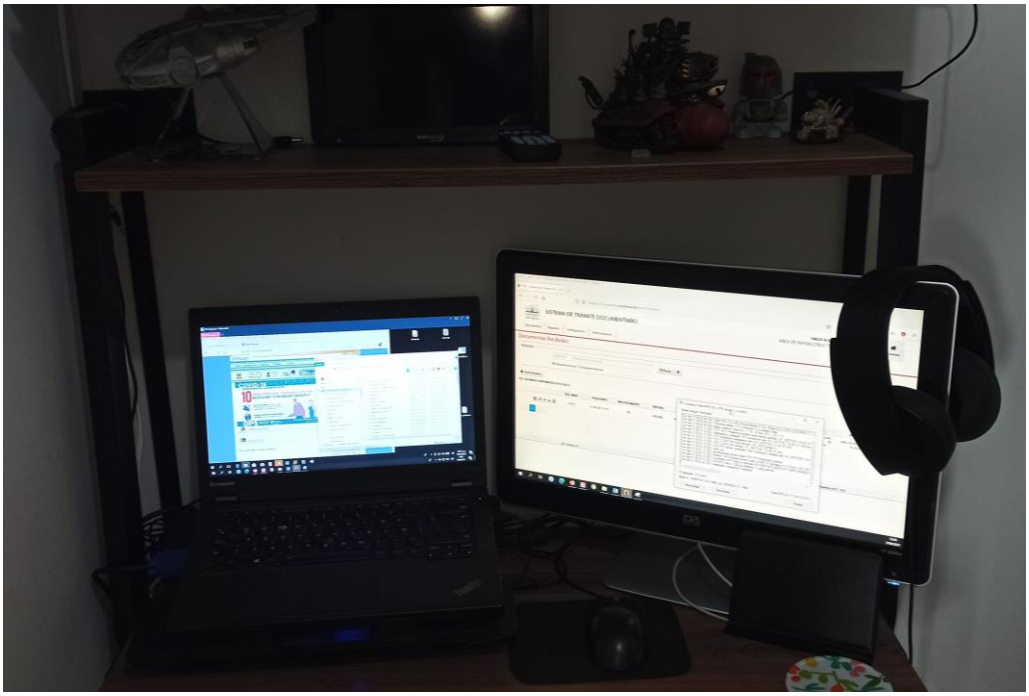
Nota: Herramienta utilizada: SoftTerra LDAP Browser. Fuente: elaboración propia.

4.2 ACCESO A RECURSOS INSTITUCIONALES

En este punto se muestra la evidencia del funcionamiento de la plataforma de acceso seguro, mediante capturas de pantalla y fotografías.

Figura 143

Caso típico de acceso a recursos de la institución desde un domicilio.



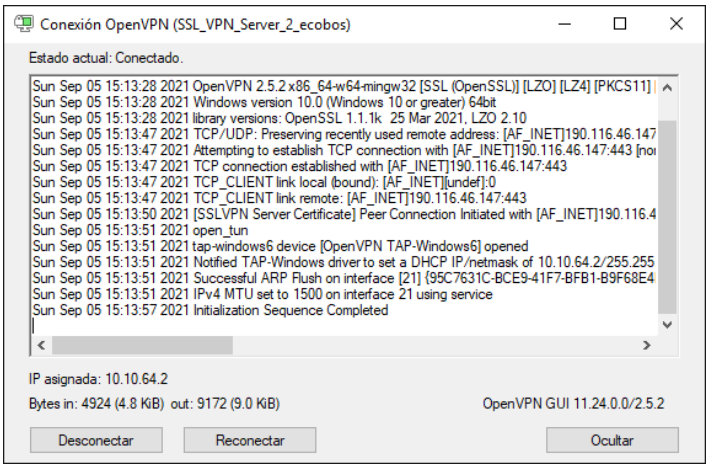
Fuente: elaboración propia.

4.2.1 CONEXIÓN A VPN - CLIENTE DE ESCRITORIO

En las siguientes figuras se ve el cliente OpenVPN conectado y el mensaje que muestra Windows 10.

Figura 144

Conexión exitosa de cliente OpenVPN.



Fuente: elaboración propia.

Figura 145

Mensaje de conexión a VPN en Windows 10.

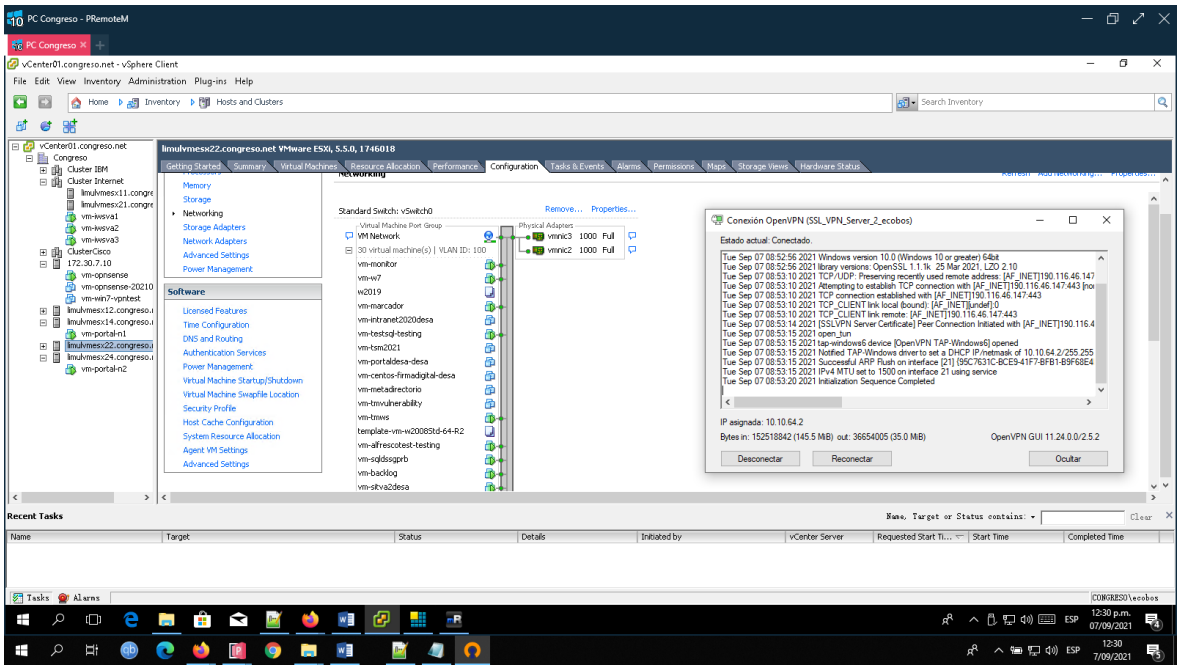
Fuente: elaboración propia.

4.2.2 ESCRITORIO REMOTO

Se muestra un ejemplo de acceso al escritorio remoto de una PC del Congreso, en la cual se está ejecutando el administrador de virtualización VMware vSphere Client.

Figura 146

Acceso a escritorio remoto (PC en el Congreso) desde domicilio vía VPN.



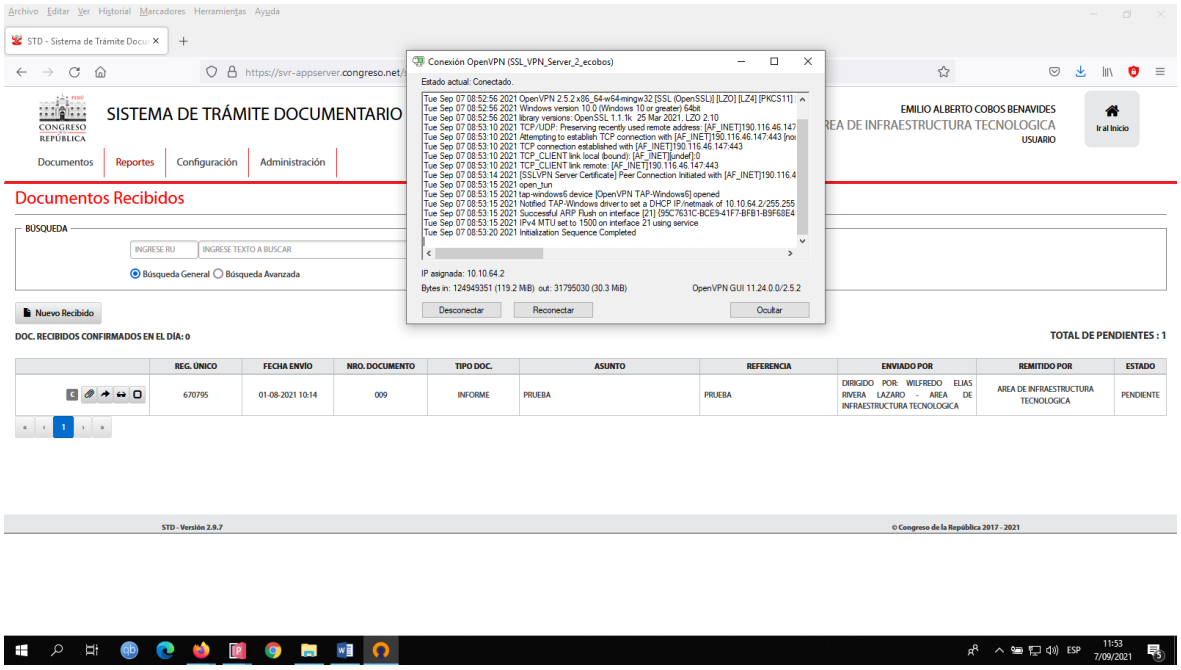
Fuente: elaboración propia.

4.2.3 SERVICIOS WEB

En la siguiente figura se muestra el acceso al servicio de Sistema de Trámite Documentario directamente desee el navegador web de un usuario que ha establecido comunicación mediante el Sistema de Acceso Remoto Seguro, sin necesidad de establecer un acceso a su escritorio remoto.

Figura 147

Acceso a recurso web interno del Congreso (Sistema de Trámite Documentario) desde domicilio vía VPN.



Fuente: elaboración propia.

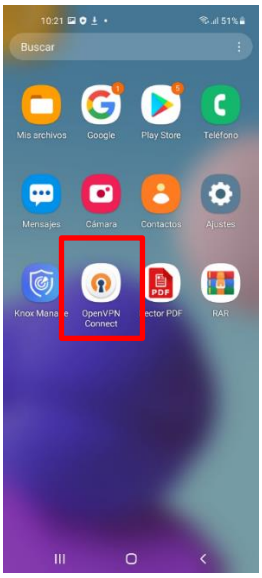
4.3 ACCESO A LOS SERVICIOS WEB DE SISTEMA DE ASISTENCIA Y VOTACIÓN REMOTOS

Las siguientes figuras muestran el acceso seguro mediante teléfonos inteligentes al sistema de Asistencia y Votación Remota del Pleno del Congreso.

4.3.1 CONEXIÓN A VPN – CLIENTE MÓVIL

Figura 148

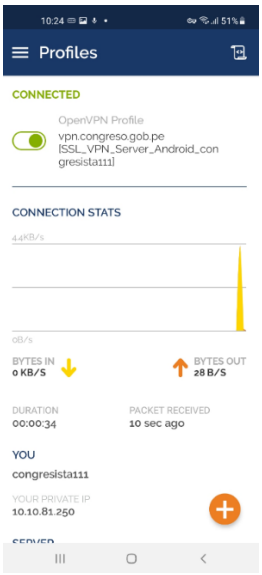
Cliente OpenVPN en Android.



Fuente: Elaboración propia.

Figura 149

Conexión OpenVPN en Android.

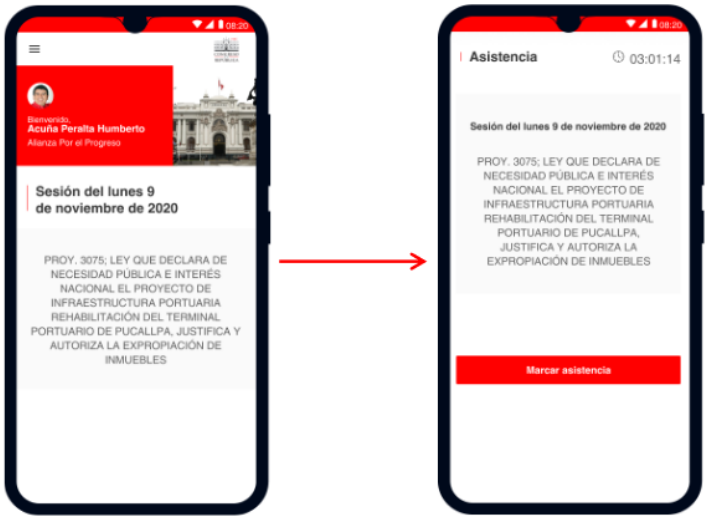


Fuente: Elaboración propia.

4.3.2 ACCESO A SISTEMA DE ASISTENCIA Y VOTACIÓN REMOTA

Figura 150

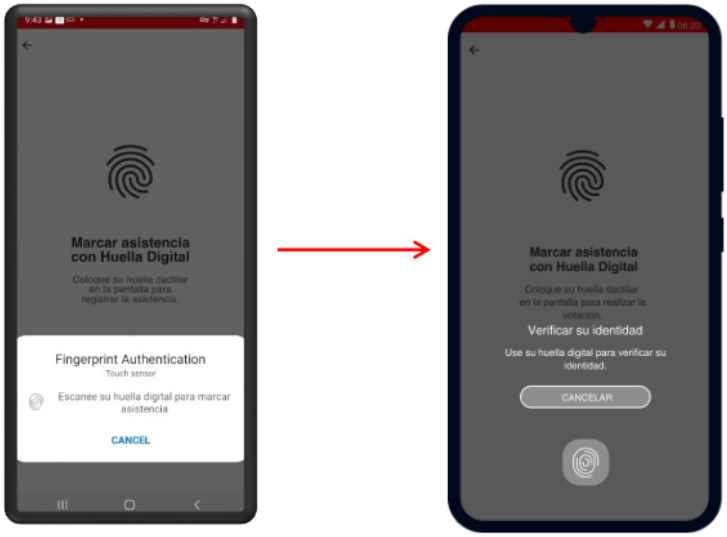
Sistema de Asistencia y Votación Remota.



Fuente: Manual del Sistema de Asistencia y Votación Remota.

Figura 151

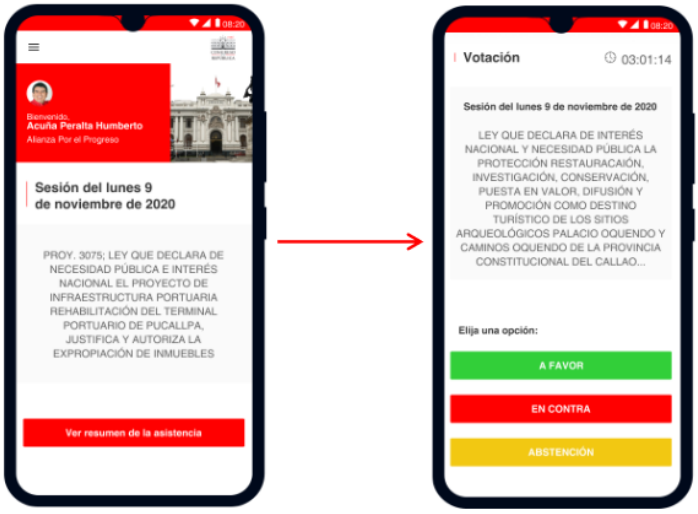
Marcado de asistencia.



Fuente: Manual del Sistema de Asistencia y Votación Remota.

Figura 152

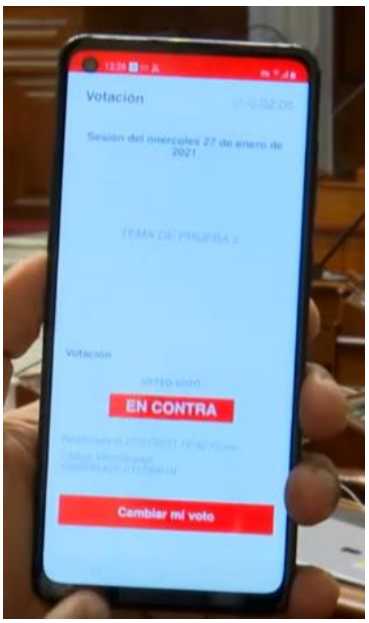
Marcado de votación.



Fuente: Manual del Sistema de Asistencia y Votación Remota.

Figura 153

Ejemplo de marcado de votación.



Fuente: Manual del Sistema de Asistencia y Votación Remota.

Figura 154

Pruebas del sistema de Asistencia y Votación remota y presencial.

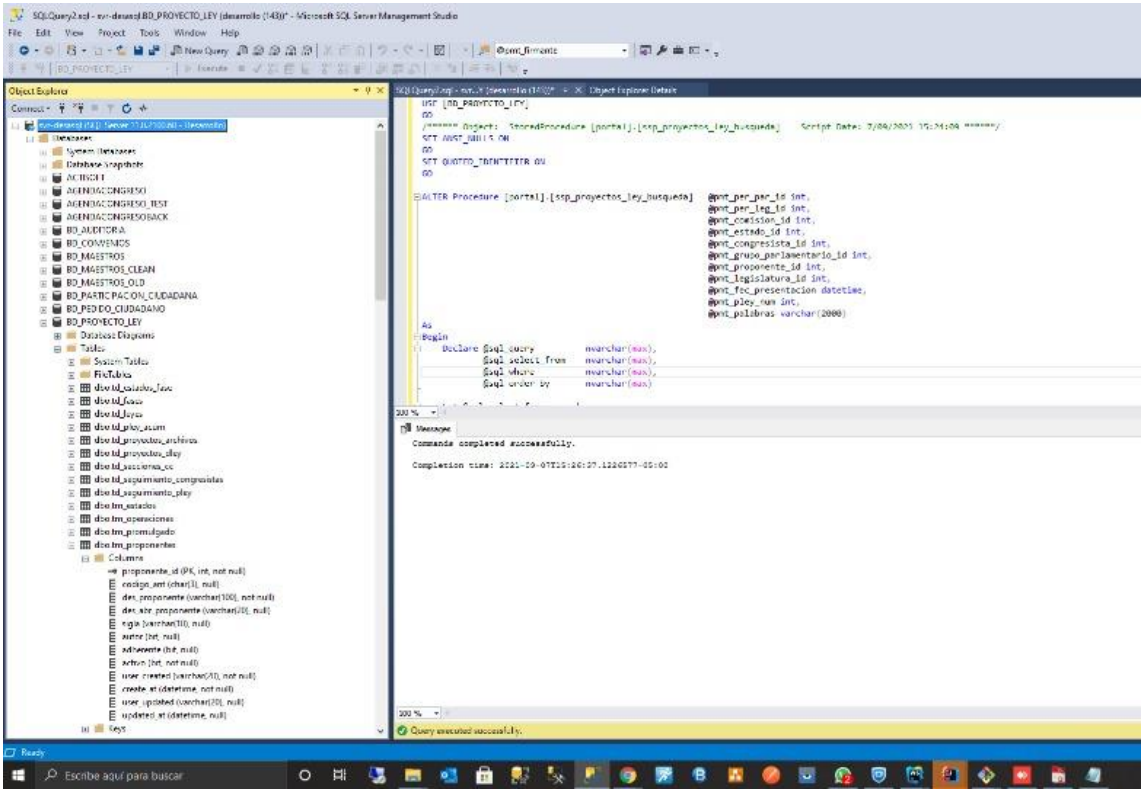
Fuente: elaboración propia.

4.4 ACCESO A SERVIDORES DE DESARROLLO

A continuación, se muestra la pantalla de acceso desde la VPN a una Base de Datos de desarrollo por parte de un programador del Congreso.

Figura 155

Acceso a servidor de Base de Datos de Desarrollo vía VPN.



Fuente: elaboración propia.

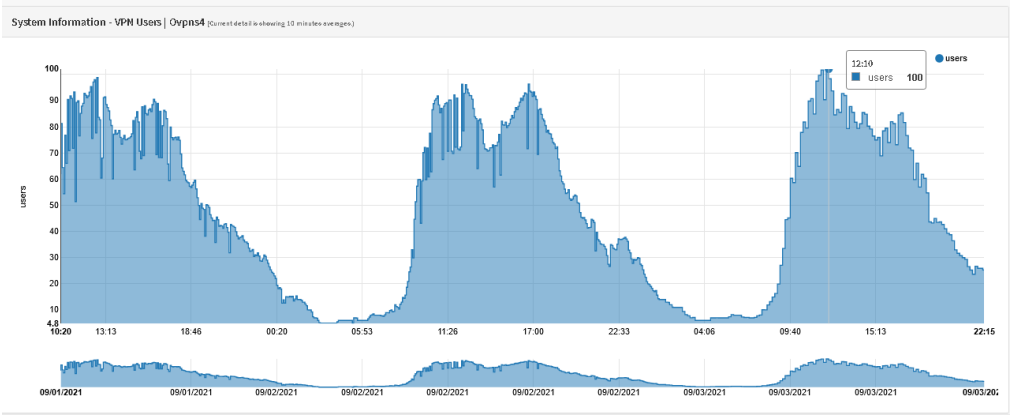
4.5 FUNCIONAMIENTO DE LA PLATAFORMA

4.5.1 CONCURRENCIA DE USUARIOS DE ESCRITORIO

En la siguiente imagen se muestra el gráfico histórico de conexiones para los días 1, 2 y 3 de setiembre de 2021. Se puede apreciar que durante las horas de oficina (9:00am a 5:00pm) se produce la mayor cantidad de conexiones concurrentes. Como ejemplo, se colocó el cursor en el punto que representa las 12:10 horas del día 3 de setiembre, pudiéndose verificar que en ese momento determinado había 100 usuarios conectados de manera simultánea.

Figura 156

Gráfico de conexiones concurrentes para usuarios VPN de escritorio.



Fuente: elaboración propia.

A continuación, se muestra a los usuarios conectados durante el pleno del día 2 de setiembre de 2021, obtenido de la plataforma OPNsense, observándose un total de 94 usuarios en ese momento.

Tabla 18

Clientes VPN de escritorio conectados a las 17:20 del día 2/9/2021.

SSL VPN Server X TCP:443 Client connections

Common Name	Real Address	Virtual Address	Connected Since	Bytes Sent	Bytes Received
ppalomino	181.65.44.142:21987	10.10.64.174	02/09/2021 14:43	81.86 MB	10.84 MB
rsanchezs	181.67.49.57:51023	10.10.79.166	02/09/2021 15:56	60.25 MB	15.00 MB
avasquez	190.237.22.135:5449	10.10.72.174	02/09/2021 09:22	345.79 MB	61.35 MB
oobregon	190.237.37.86:19845	10.10.76.66	02/09/2021 17:20	1.24 MB	107 KB
lmurrugarra	181.67.184.189:35670	10.10.77.34	02/09/2021 16:49	6.59 MB	1.02 MB
rmontero	161.132.234.47:29127	10.10.76.114	02/09/2021 15:10	67.88 MB	5.08 MB
jvicente	177.91.249.74:58961	10.10.72.86	02/09/2021 15:52	9.41 MB	2.95 MB
roshiro	187.86.167.149:6898	10.10.76.122	02/09/2021 16:42	653 KB	219 KB
jvilcaluri	190.237.46.131:3634	10.10.75.98	02/09/2021 15:56	44.58 MB	3.57 MB
ifashe	45.5.68.110:52619	10.10.75.2	02/09/2021 15:09	550 KB	241 KB
acabezas	148.102.113.63:45513	10.10.65.250	02/09/2021 16:30	603 KB	233 KB
mmunar	179.6.75.253:24447	10.10.75.254	02/09/2021 17:10	10.74 MB	1.19 MB
mlatorre	181.65.81.146:13323	10.10.72.178	02/09/2021 16:04	46.37 MB	2.48 MB
dquinones	190.239.111.235:39005	10.10.72.162	02/09/2021 13:56	11.09 MB	1.16 MB
falvaradod	181.64.68.118:49919	10.10.74.222	02/09/2021 08:02	37.61 MB	4.25 MB
evictorio	190.237.46.44:48903	10.10.74.218	02/09/2021 15:56	37.23 MB	3.07 MB
dcardenas	201.240.147.166:37923	10.10.64.238	02/09/2021 14:47	620.56 MB	35.68 MB
bcano	179.6.204.98:52674	10.10.65.46	02/09/2021 17:14	840 KB	369 KB
jsantillan	179.6.223.82:55507	10.10.75.94	02/09/2021 10:02	61.56 MB	3.47 MB
sravines	148.102.113.103:6726	10.10.76.146	02/09/2021 14:06	102.92 MB	11.40 MB
jdelgado	190.237.93.69:36974	10.10.73.150	02/09/2021 09:02	2.45 MB	452 KB
lloayza	190.236.195.79:31350	10.10.75.130	02/09/2021 15:57	34.97 MB	3.85 MB
klazarte	132.191.1.212:10178	10.10.64.202	02/09/2021 15:38	1.66 MB	237 KB
abalbuena	190.238.211.61:55366	10.10.74.110	02/09/2021 14:57	58.48 MB	8.70 MB
rvigil	179.6.170.190:55972	10.10.75.202	02/09/2021 12:57	1.85 MB	271 KB
veugenio	148.102.115.154:10161	10.10.77.226	02/09/2021 16:13	7.30 MB	919 KB
ybravo	190.236.211.2:14228	10.10.76.202	02/09/2021 15:56	53.34 MB	5.56 MB
rmorales	190.237.43.59:47445	10.10.76.118	02/09/2021 10:31	418.83 MB	29.26 MB
kmayaute	190.237.181.207:43010	10.10.72.190	02/09/2021 17:13	3.06 MB	576 KB
gyzaguirre	190.236.205.22:1315	10.10.74.246	02/09/2021 16:10	14.12 MB	1.15 MB
cpizarro	201.240.41.166:64047	10.10.73.98	02/09/2021 12:00	49.14 MB	7.82 MB
abalarezo	181.64.61.121:58365	10.10.74.106	02/09/2021 16:08	1.40 MB	188 KB
mbarriga	190.237.60.27:38653	10.10.75.10	02/09/2021 16:50	6.88 MB	1.26 MB
sperez	190.235.103.228:57938	10.10.76.142	02/09/2021 15:49	267.89 MB	11.62 MB
mmorales	181.65.126.164:54940	10.10.75.194	02/09/2021 10:45	176.71 MB	21.31 MB

lvalenzuela	190.239.77.185:37537	10.10.75.162	02/09/2021 14:08	93.45 MB	11.16 MB
mloja	181.64.122.104:38113	10.10.77.234	02/09/2021 14:22	129.35 MB	17.88 MB
mtrios	179.6.211.79:40041	10.10.75.30	02/09/2021 13:20	296.39 MB	23.21 MB
mperez	201.240.116.154:11988	10.10.77.90	02/09/2021 17:20	269 KB	56 KB
jgonzaless	190.233.131.117:63358	10.10.65.38	02/09/2021 16:19	15.54 MB	1.35 MB
dtomailla	190.238.238.126:18470	10.10.74.6	02/09/2021 16:49	3.07 MB	567 KB
mguevara	190.216.191.75:58715	10.10.79.210	02/09/2021 10:00	154.66 MB	14.46 MB
gcastro	190.238.75.127:12579	10.10.74.234	02/09/2021 14:44	2.77 MB	242 KB
ibelleza	190.233.214.150:53902	10.10.66.82	02/09/2021 15:45	686.99 MB	25.34 MB
vbarrueto	190.237.168.222:49901	10.10.76.158	06/09/2021 09:18	170.32 MB	45.68 MB
tacuna	190.236.172.98:57684	10.10.76.150	02/09/2021 14:24	88.19 MB	7.36 MB
iaguero	190.237.89.172:50198	10.10.74.254	02/09/2021 09:14	120.70 MB	9.93 MB
ebohorquez	179.6.160.129:46141	10.10.77.242	02/09/2021 15:00	83.29 MB	3.27 MB
aalvarador	200.121.1.150:8134	10.10.64.6	02/09/2021 15:56	13.96 MB	1.39 MB
jfloresg	190.237.204.155:26664	10.10.74.50	02/09/2021 15:36	900 KB	422 KB
mbaldeon	190.232.237.112:49861	10.10.75.178	02/09/2021 08:43	102.48 MB	14.59 MB
rcardenasp	181.67.112.91:59867	10.10.75.70	02/09/2021 15:33	59.78 MB	5.61 MB
jrubio	201.230.248.176:25750	10.10.75.90	02/09/2021 15:58	150.41 MB	8.47 MB
jvives	201.240.147.34:17606	10.10.75.34	02/09/2021 13:37	136.28 MB	6.34 MB
lsandoval	181.66.206.76:49906	10.10.64.14	02/09/2021 09:06	34.18 MB	1.28 MB
pchaname	190.239.232.81:31511	10.10.76.70	02/09/2021 15:56	102.46 MB	7.19 MB
aayalap	190.234.181.88:65085	10.10.74.102	02/09/2021 15:28	3.98 MB	203 KB
fsantillan	190.43.237.84:51122	10.10.66.134	02/09/2021 15:56	347 KB	65 KB
wlinares	181.65.126.55:42517	10.10.76.174	02/09/2021 16:46	8.64 MB	1.49 MB
ezapata	181.65.124.130:26481	10.10.79.246	02/09/2021 11:09	96 KB	368 KB
jfchavez	190.234.182.213:63104	10.10.72.78	02/09/2021 12:12	221.62 MB	14.93 MB
apohl	179.6.201.253:53803	10.10.78.174	02/09/2021 16:22	45.49 MB	5.56 MB
ssuarez	190.43.88.72:57018	10.10.65.14	02/09/2021 09:31	360.63 MB	52.70 MB
rchumpitaz	190.237.2.138:15025	10.10.76.98	02/09/2021 09:13	144.11 MB	12.41 MB
starrillo	190.238.105.246:64249	10.10.72.182	02/09/2021 15:34	25.38 MB	2.59 MB
jcubas	190.232.4.71:57423	10.10.75.6	02/09/2021 12:13	17.22 MB	1.85 MB
esamaniego	190.238.105.66:39456	10.10.77.246	02/09/2021 14:05	489.47 MB	26.33 MB
mpacheco	179.6.200.220:64278	10.10.76.6	02/09/2021 09:04	258.32 MB	41.37 MB
cfloresg	190.233.207.62:40757	10.10.74.174	02/09/2021 15:56	56.06 MB	9.87 MB
aalava	181.67.169.161:51596	10.10.74.98	02/09/2021 13:45	12.35 MB	3.49 MB
lsornoza	190.232.1.111:59993	10.10.75.146	02/09/2021 16:45	29.08 MB	3.30 MB
rsanchezc	201.240.194.16:63781	10.10.64.130	02/09/2021 15:07	130.79 MB	5.25 MB
rvalerio	209.45.91.42:64044	10.10.72.166	02/09/2021 14:44	38.92 MB	11.02 MB
gsandoval	190.233.218.86:49289	10.10.74.242	02/09/2021 09:33	294.37 MB	23.81 MB
emartinezt	179.6.198.143:24454	10.10.65.174	02/09/2021 16:52	1.74 MB	531 KB
hcortez	190.238.105.110:14631	10.10.74.250	02/09/2021 16:03	5.14 MB	1.92 MB
jandrade	190.236.98.220:63638	10.10.73.190	02/09/2021 14:01	331.02 MB	63.81 MB
ymaldonado	179.6.168.219:4930	10.10.76.190	02/09/2021 17:11	4.77 MB	356 KB
sesquivel	190.237.28.56:51815	10.10.78.218	02/09/2021 12:03	1.52 MB	790 KB

ryaipen	190.237.24.234:28656	10.10.76.130	02/09/2021 12:21	270.80 MB	45.87 MB
pmartinez	190.239.230.216:53897	10.10.66.86	02/09/2021 16:45	6.41 MB	293 KB
gpolo	190.233.121.65:61224	10.10.73.10	02/09/2021 14:15	375.36 MB	134.80 MB
rpaez	190.42.172.72:55409	10.10.72.214	02/09/2021 16:56	6.50 MB	851 KB
rbarrig	190.234.163.117:51892	10.10.79.230	02/09/2021 15:33	27.21 MB	8.09 MB
zochoa	179.6.152.104:44229	10.10.75.54	02/09/2021 15:46	54.67 MB	6.90 MB
ssaavedram	148.102.115.123:38797	10.10.65.34	02/09/2021 12:55	1.54 MB	181 KB
rrojas	132.251.3.121:27671	10.10.76.126	02/09/2021 16:15	90.09 MB	10.57 MB
mvillanueva	181.67.49.168:53808	10.10.65.90	02/09/2021 16:09	64.20 MB	5.90 MB
lrivero	181.67.170.1:11336	10.10.78.82	02/09/2021 15:57	2.66 MB	481 KB
rhernandezf	181.64.61.147:11198	10.10.77.62	02/09/2021 16:43	27.62 MB	3.15 MB
rcasal	190.234.8.222:49473	10.10.76.94	02/09/2021 16:11	622.48 MB	37.21 MB
lrojas	200.39.56.6:60910	10.10.72.102	02/09/2021 14:47	12.52 MB	5.06 MB
marriaran	190.236.211.47:65317	10.10.79.194	02/09/2021 17:05	7.21 MB	784 KB
mespinozam	190.237.122.157:51553	10.10.66.66	02/09/2021 17:03	20.17 MB	796 KB

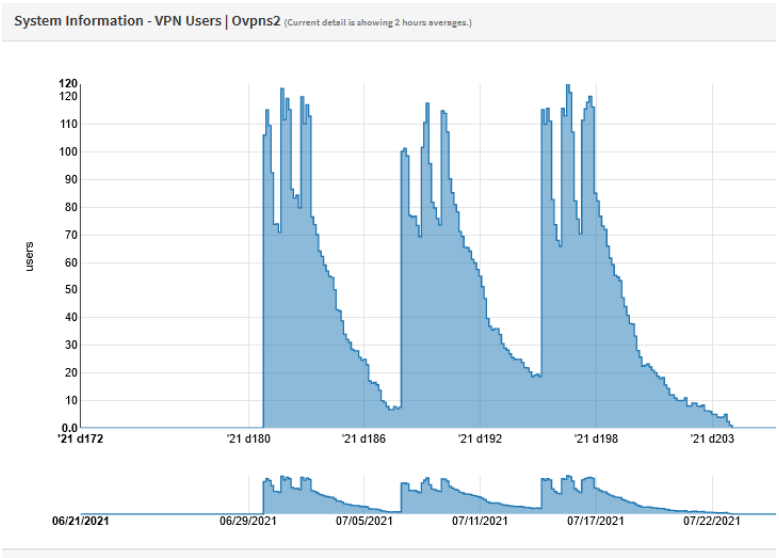
Fuente: elaboración propia.

4.5.2 CONCURRENCIA DE USUARIOS MÓVILES

Para los usuarios móviles, se muestra el gráfico de los días 30 de junio a 22 de julio, lo que representa las últimas sesiones del Congreso 2020-2021.

Figura 157

Sesiones concurrentes de congresistas con dispositivos móviles junio-julio 2021.



Fuente: elaboración propia.

A continuación, se muestra a los usuarios Android de VPN, conectados en un momento dado, obtenido de la plataforma OPNsense, observándose un total de 82 usuarios en ese momento.

Tabla 19

Clientes VPN de teléfonos móviles conectados a las 17:20 del día 2/9/2021.

SSL VPN Server Android TCP:8443 Client connections					
Common Name	Real Address	Virtual Address	Connected Since	Bytes Sent	Bytes Received
congresista050	190.239.73.7:5882	10.10.81.150	02/09/2021 16:03	76 KB	66 KB
congresista071	190.239.77.211:62718	10.10.81.98	02/09/2021 16:15	59 KB	55 KB
congresista123	190.236.3.236:22316	10.10.81.74	02/09/2021 15:36	339 KB	333 KB
congresista041	190.236.5.176:44173	10.10.80.174	02/09/2021 08:58	533 KB	539 KB
congresista070	190.239.76.88:2189	10.10.80.138	02/09/2021 12:25	422 KB	456 KB
congresista022	190.239.77.119:61515	10.10.81.118	02/09/2021 19:09	39 KB	35 KB
congresista108	190.236.8.16:12047	10.10.81.114	31/08/2021 09:37	1.17 MB	1.04 MB
congresista097	190.236.3.7:26086	10.10.81.78	02/09/2021 16:10	457 KB	487 KB
congresista061	190.236.7.215:35072	10.10.81.218	02/09/2021 16:48	303 KB	323 KB
congresista109	190.239.79.204:43542	10.10.80.54	02/09/2021 11:52	648 KB	653 KB
congresista105	179.6.88.63:7547	10.10.80.62	02/09/2021 16:00	402 KB	458 KB
congresista060	190.236.1.165:28400	10.10.81.214	02/09/2021 16:38	344 KB	383 KB
congresista011	190.236.5.66:9845	10.10.80.14	02/09/2021 15:55	93 KB	84 KB
congresista033	190.236.7.72:21105	10.10.80.170	02/09/2021 15:37	283 KB	273 KB
congresista100	190.236.7.250:37735	10.10.81.34	02/09/2021 15:22	184 KB	193 KB
congresista065	190.236.7.56:64574	10.10.81.226	02/09/2021 15:23	146 KB	157 KB
congresista009	190.236.10.149:31924	10.10.81.86	02/09/2021 15:35	83 KB	76 KB
congresista084	190.236.2.188:32688	10.10.81.230	02/09/2021 15:40	57 KB	49 KB
congresista007	190.239.73.142:39027	10.10.81.38	02/09/2021 12:19	47 KB	45 KB
congresista045	190.239.76.56:38967	10.10.81.206	02/09/2021 14:36	464 KB	526 KB
congresista075	190.239.73.252:44816	10.10.81.186	02/09/2021 09:00	607 KB	663 KB
congresista129	204.232.119.6:20129	10.10.81.42	02/09/2021 08:44	765 KB	920 KB
congresista004	190.239.79.124:61829	10.10.81.190	02/09/2021 16:16	382 KB	436 KB
congresista042	190.236.6.146:59956	10.10.80.182	02/09/2021 12:58	179 KB	194 KB
congresista127	190.239.79.98:14788	10.10.80.114	02/09/2021 15:42	241 KB	253 KB
congresista030	190.236.3.136:7248	10.10.80.110	02/09/2021 11:42	13 KB	12 KB
congresista016	190.236.15.11:56532	10.10.81.126	02/09/2021 14:23	198 KB	187 KB
congresista066	190.236.4.85:9246	10.10.80.146	02/09/2021 08:59	984 KB	1.08 MB
congresista114	190.239.75.44:47747	10.10.81.30	02/09/2021 14:20	188 KB	208 KB
congresista032	190.236.9.157:12458	10.10.81.142	02/09/2021 15:42	153 KB	150 KB

congresista026	190.236.0.12:53391	10.10.80.186	02/09/2021 16:33	352 KB	376 KB
congresista104	190.236.3.133:6021	10.10.80.162	02/09/2021 13:36	212 KB	222 KB
congresista029	190.236.8.161:38320	10.10.81.202	02/09/2021 08:21	712 KB	809 KB
congresista085	190.239.66.247:8665	10.10.82.2	02/09/2021 12:13	36 KB	29 KB
congresista043	190.239.74.223:46996	10.10.80.78	02/09/2021 11:07	35 KB	36 KB
congresista031	190.239.76.10:14445	10.10.81.134	02/09/2021 16:04	383 KB	371 KB
congresista055	190.236.2.197:56927	10.10.81.166	02/09/2021 14:24	3.34 MB	3.38 MB
congresista021	190.236.6.250:42255	10.10.81.122	02/09/2021 16:18	608 KB	599 KB
congresista098	190.236.4.139:15624	10.10.82.18	02/09/2021 09:38	165 KB	148 KB
congresista116	190.236.26.236:13531	10.10.81.22	02/09/2021 12:15	451 KB	496 KB
congresista052	190.239.75.72:47940	10.10.81.146	02/09/2021 13:39	72 KB	66 KB
congresista112	190.238.29.17:9167	10.10.80.66	02/09/2021 15:59	78 KB	79 KB
congresista083	190.236.0.140:56195	10.10.80.166	02/09/2021 15:38	120 KB	117 KB
congresista044	190.236.2.4:23734	10.10.81.158	02/09/2021 15:46	245 KB	235 KB
congresista128	190.236.10.13:32804	10.10.80.22	02/09/2021 09:22	171 KB	160 KB
congresista058	190.236.12.252:65166	10.10.80.46	02/09/2021 15:43	408 KB	488 KB
congresista077	190.236.11.94:39328	10.10.80.82	02/09/2021 15:43	438 KB	503 KB
congresista080	190.239.65.166:13167	10.10.81.54	02/09/2021 15:25	276 KB	276 KB
congresista063	190.236.15.130:20678	10.10.81.222	02/09/2021 15:35	199 KB	205 KB
congresista102	190.239.68.153:24294	10.10.80.150	02/09/2021 14:40	259 KB	276 KB
congresista118	190.239.89.145:65314	10.10.80.38	02/09/2021 16:18	19 KB	17 KB
congresista089	190.239.93.165:15462	10.10.80.230	02/09/2021 08:42	729 KB	871 KB
congresista072	190.236.15.50:64472	10.10.80.218	02/09/2021 12:06	88 KB	90 KB
congresista002	190.239.69.32:43508	10.10.81.130	02/09/2021 14:47	72 KB	56 KB
congresista111	190.236.8.212:11223	10.10.81.250	02/09/2021 11:32	252 KB	279 KB
congresista106	190.237.145.12:15467	10.10.81.10	02/09/2021 08:51	650 KB	760 KB
congresista014	190.239.74.167:9030	10.10.80.102	02/09/2021 09:39	208 KB	222 KB
congresista110	190.239.78.246:7766	10.10.80.206	02/09/2021 08:52	582 KB	635 KB
congresista125	190.236.6.24:21956	10.10.81.46	01/09/2021 17:07	377 KB	334 KB
congresista067	190.236.5.169:52204	10.10.81.178	02/09/2021 16:37	239 KB	232 KB
congresista056	190.239.64.250:11249	10.10.80.242	02/09/2021 17:14	164 KB	175 KB
congresista130	190.239.67.217:40052	10.10.81.66	02/09/2021 15:37	58 KB	50 KB
congresista053	190.236.14.206:63793	10.10.80.30	02/09/2021 14:10	34 KB	35 KB
congresista039	190.236.5.180:47475	10.10.80.118	02/09/2021 13:24	32 KB	29 KB
congresista006	190.239.65.70:2384	10.10.80.246	02/09/2021 11:16	313 KB	340 KB
congresista001	190.236.6.80:9868	10.10.81.62	01/09/2021 10:33	598 KB	533 KB
congresista068	190.236.15.229:27398	10.10.81.182	02/09/2021 15:36	757 KB	801 KB
congresista081	190.239.72.9:34435	10.10.80.34	02/09/2021 17:02	295 KB	334 KB
congresista078	190.236.8.51:30221	10.10.80.190	02/09/2021 15:29	497 KB	542 KB
congresista122	190.239.70.78:48895	10.10.81.242	02/09/2021 11:34	224 KB	244 KB
congresista015	190.236.9.184:37248	10.10.80.202	02/09/2021 14:26	134 KB	149 KB
congresista101	190.236.15.174:37627	10.10.80.134	02/09/2021 15:38	342 KB	338 KB
congresista027	190.236.3.253:60123	10.10.80.98	02/09/2021 14:22	139 KB	132 KB
congresista073	190.236.3.226:28515	10.10.80.70	02/09/2021 16:20	391 KB	452 KB

congresista090	190.239.66.117:31517	10.10.81.246	02/09/2021 16:04	467 KB	529 KB
congresista051	190.239.66.174:13576	10.10.80.94	02/09/2021 17:01	208 KB	240 KB
congresista049	190.239.74.189:53066	10.10.80.238	02/09/2021 15:45	380 KB	368 KB
congresista115	190.236.13.59:41695	10.10.80.50	02/09/2021 14:28	273 KB	294 KB
congresista019	190.239.75.107:58175	10.10.81.50	02/09/2021 16:40	330 KB	382 KB
congresista069	190.234.105.170:31498	10.10.80.90	02/09/2021 16:23	384 KB	445 KB

Fuente: elaboración propia.

4.6 USO DE RECURSOS

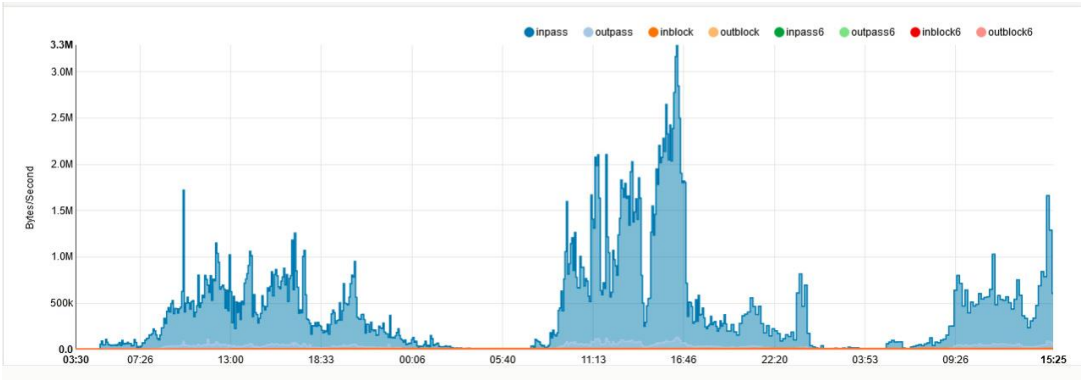
En esta sección se muestran los parámetros de funcionamiento del equipo: tráfico de datos y consumo de recursos computacionales.

4.6.1 TRÁFICO DE DATOS

En los siguientes gráficos se mostrará el tráfico de datos de VPN durante un pleno del Congreso: total, VPN para equipos de escritorio y VPN para equipos móviles de los días 1, 2 y 3 de setiembre de 2021.

Figura 158

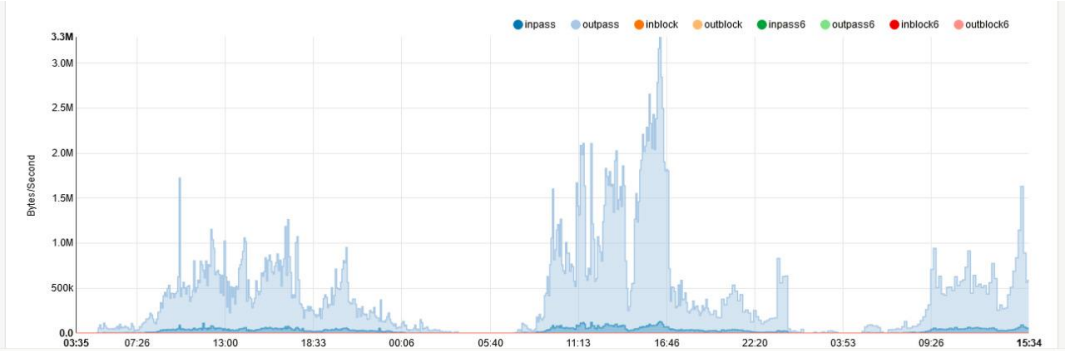
Tráfico total de datos VPN.



Fuente: elaboración propia.

Figura 159

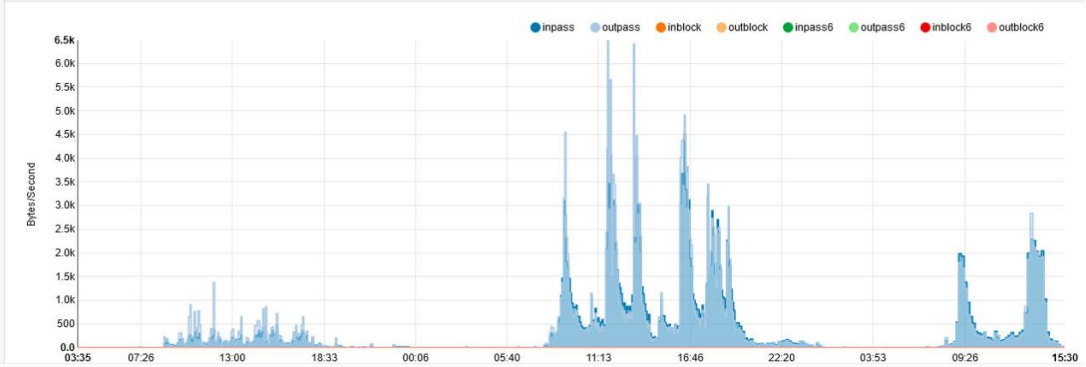
Tráfico de datos VPN de equipos de escritorio.



Fuente: elaboración propia.

Figura 160

Tráfico de datos VPN de equipos móviles.



Fuente: elaboración propia.

Como se puede ver, el consumo pico de transferencia de datos es de 3.3 MBps (26Mbps), el de VPN PC es similar (3.3 MBps o 26 Mbps) mientras que el uso máximo de datos transmitidos por la VPN para equipos móviles es de 6.5 KBps (52Kbps).

Así, se calcula que el uso pico de datos para un total de alrededor de 100 usuarios de escritorio y 90 usuarios de equipos móviles concurrentes (como se pudo apreciar en los puntos anteriores), representa un máximo de 26Mbps de manera típica. En la actualidad, el Congreso dispone de dos líneas de internet principales de 200Mbps cada una, balanceadas por el equipo Peplink Balance 13500 para un total de 400 Mbps

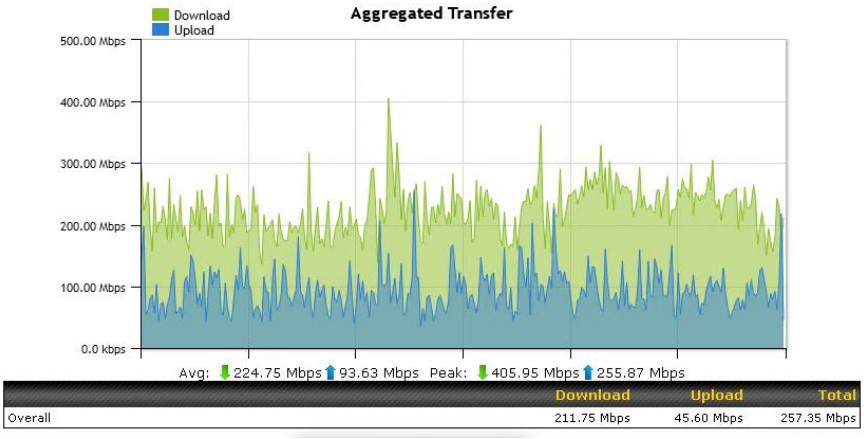
efectivos, por lo que se puede afirmar que se dispone de ancho de banda suficiente para soportar los servicios institucionales (navegación interna, publicación de servicio web y servicio VPN) sin saturar el uso de las líneas de internet.

El uso de datos por parte de los equipos móviles no tiene mayor impacto en el uso total de ancho de banda del Congreso debido a que la única aplicación utilizada para transferencia de datos es la aplicación de Asistencia y Votación Remota (la configuración del software MDM de control de equipos móviles impide la instalación de programas de terceros como WhatsApp, Facebook y otros).

Tal como se aprecia en el gráfico siguiente, el ancho de banda de internet consumido en un día típico tiene un promedio de 210 Mbps de descarga y 50Mbps de subida de datos, por lo que los 26Mbps consumidos por el Sistema de Acceso Remoto pueden ser soportados por los servicios actuales de internet, los que brindan a la institución un valor combinado de 450Mbps simétrico.

Figura 161

Tráfico total de internet en la institución.

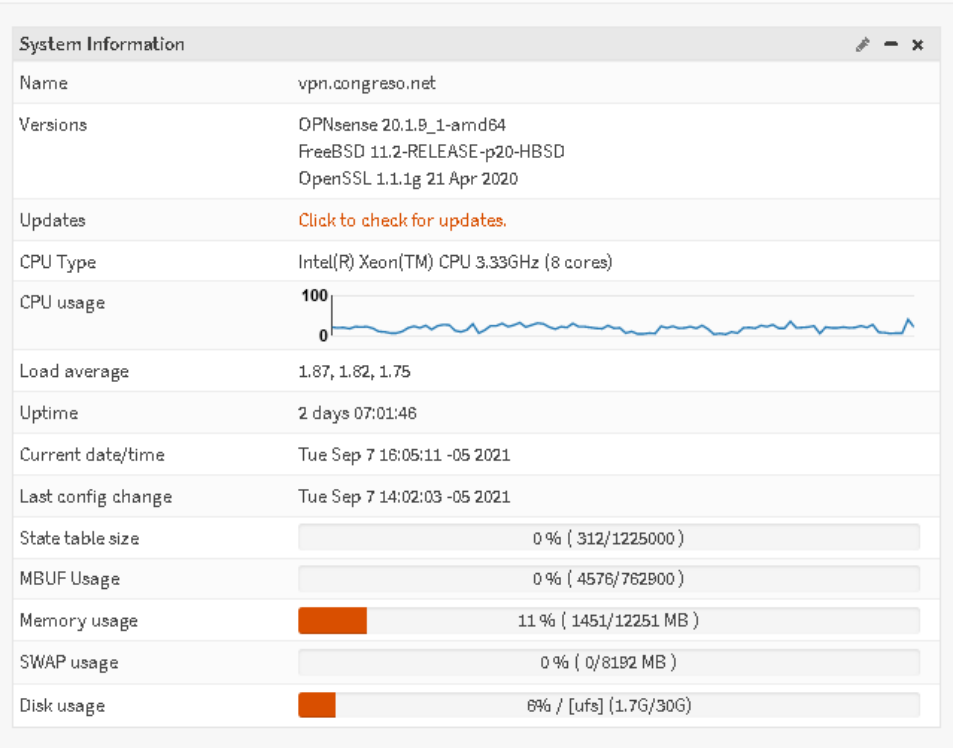


Fuente: elaboración propia.

4.6.2 CPU, MEMORIA Y ALMACENAMIENTO

Figura 162

Uso de recursos computacionales.



Fuente: elaboración propia.

4.6.3 ANÁLISIS DE RESULTADOS

De acuerdo a los resultados obtenidos, se realiza el análisis de los mismos para verificar si estos pueden demostrar el cumplimiento de los objetivos específicos establecidos en el punto 3.2.2.

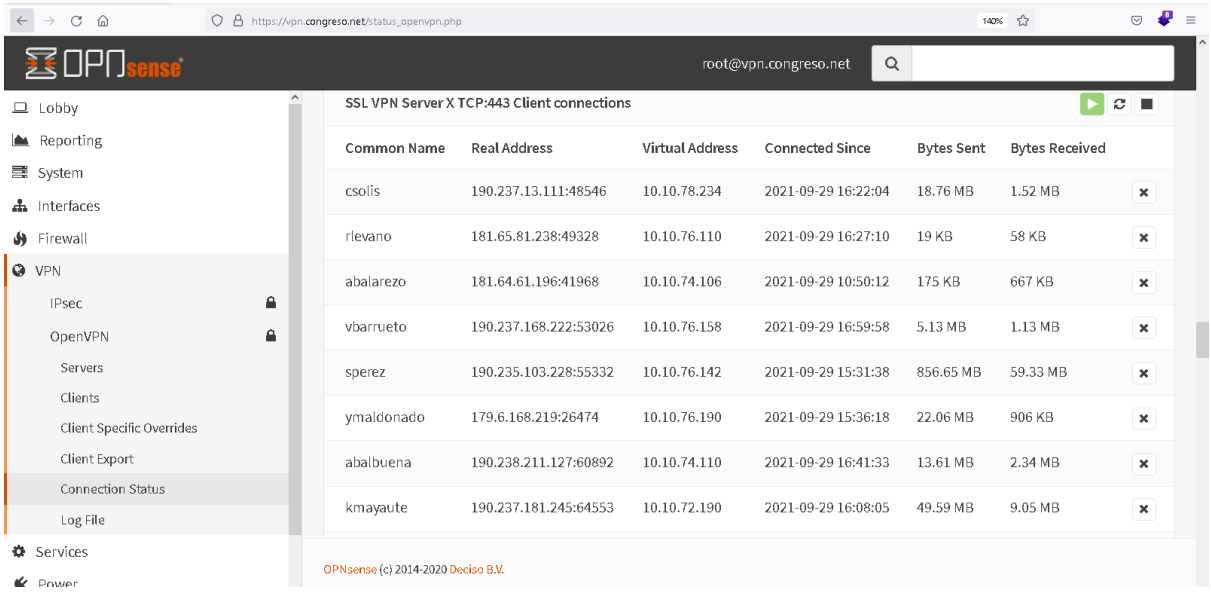
Objetivo 1: Brindar acceso remoto a los usuarios del Servicio Parlamentario y Organización Parlamentaria, tanto a sus equipos institucionales como a los servicios web internos (Intranet, Sistema de Trámite Documentario, SIGA).

Resultados: Se demuestra que se logró brindar acceso remoto a los usuarios del Servicio Parlamentario y Organización Parlamentaria, tanto a los servicios de escritorio

remoto como servicios web internos, lo cual se puede verificar en los resultados mostrados en el punto 4.2, figuras 143 a 147, así como en la siguiente figura que muestra el estado de conexiones de VPN de clientes de escritorio el día 29 de setiembre de 2021.

Figura 163

Detalle parcial de clientes VPN de escritorio activos en consola web OPNsense.



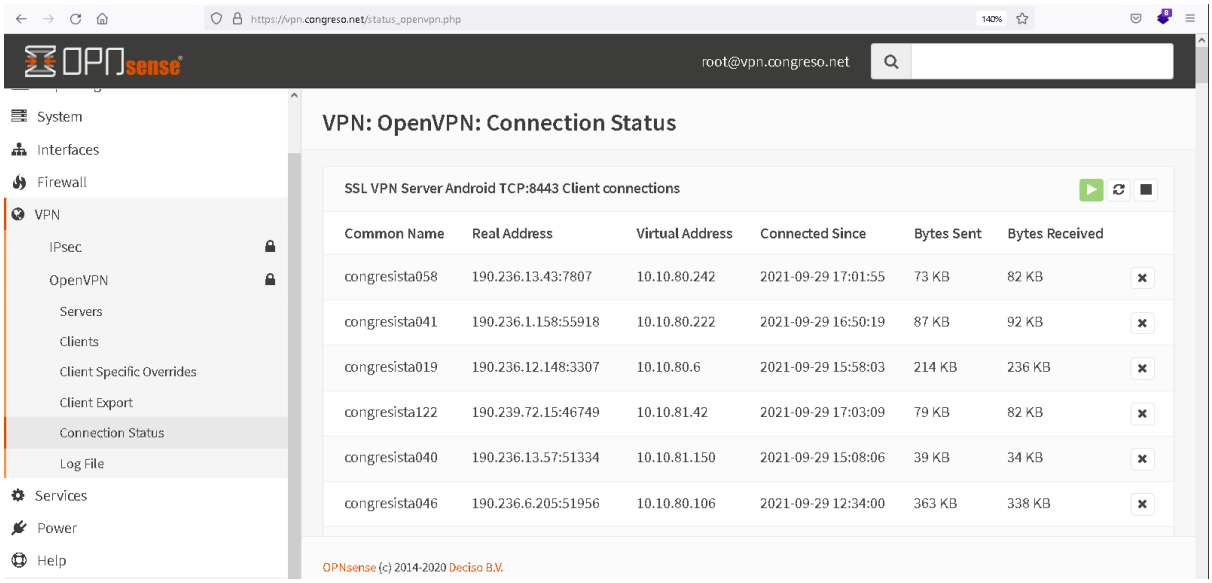
Fuente: elaboración propia.

Objetivo 2: Dar acceso remoto a los servicios web utilizados por la nueva plataforma de Asistencia y Votación Remota para los teléfonos inteligentes de los Congresistas.

Resultados: Se muestra el acceso de los teléfonos inteligentes de los señores congresistas y el funcionamiento del sistema de Asistencia y Votación remota en el Congreso, como se puede confirmar en el punto 4.3 (figuras 148 a 154) así como en la siguiente figura que muestra el estado de conexiones de VPN de clientes Android el día 29 de setiembre de 2021.

Figura 164

Detalle parcial de clientes VPN Android activos en consola web OPNsense.



Fuente: elaboración propia.

Objetivo 3: Dar acceso remoto a los servidores de desarrollo y pruebas a los equipos de Desarrollo de Software.

Resultados: El personal del Área de Proyectos utiliza el sistema de VPN para acceder a los servicios internos tales como servidores de bases de datos y servidores de aplicaciones java JBoss 7.1 y 7.3., tal como se aprecia en el punto 4.4.

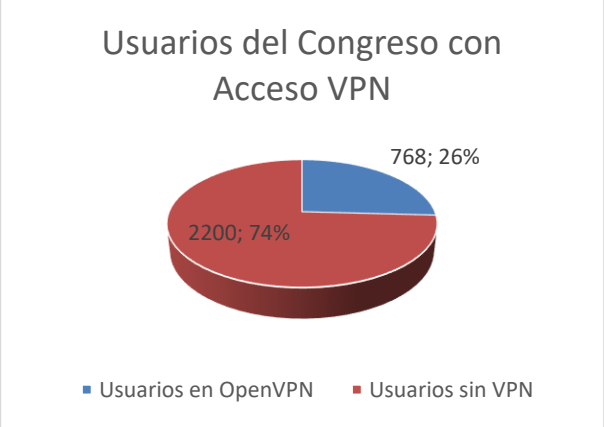
Objetivo 4: Permitir el registro de un mínimo de 500 usuarios, así como permitir el acceso concurrente de al menos 100 usuarios de escritorio remoto del Servicio Parlamentario manteniendo la calidad de servicio.

Resultados: Se puede verificar que el sistema registra más de 500 usuarios solicitados, así como el acceso concurrente a usuarios de escritorio y de dispositivos móviles de al menos 100 usuarios.

Usuarios registrados en el sistema: al 2 de setiembre de 2021 se dispone de 768 usuarios registrados en el sistema VPN como se verifica en la figura 142, contra un total de 2968 usuarios institucionales registrados en el Directorio Activo. Así, el 26% de los usuarios institucionales tiene acceso a trabajo remoto. Se está evaluando alternativas como VDI para ampliar la cobertura para trabajo remoto.

Figura 165

Usuarios del Congreso con Acceso VPN configurado.

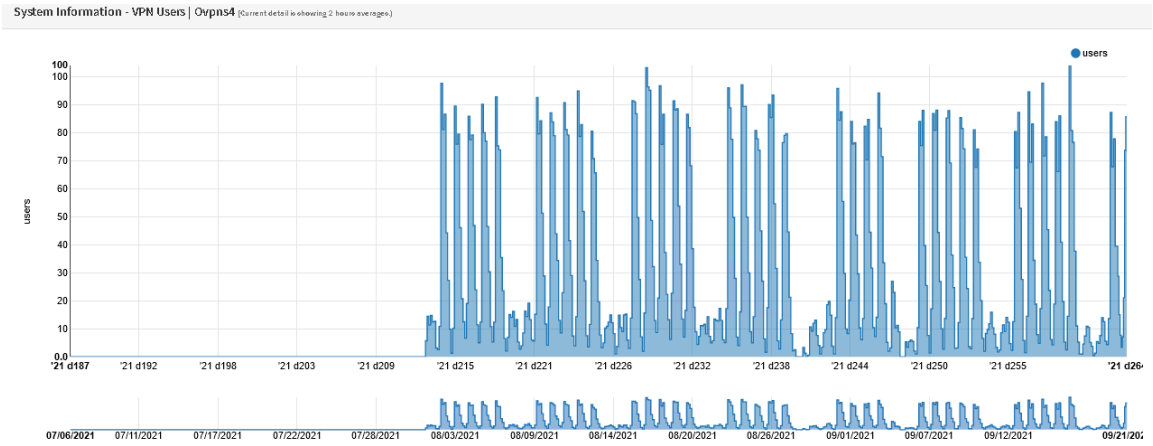


Fuente: elaboración propia.

Concurrencia de usuarios: En el siguiente gráfico se muestra la actividad de accesos VPN de los últimos dos meses, donde se aprecia que se alcanza y superan los 100 usuarios concurrentes con regularidad, disminuyendo la cantidad de usuarios los fines de semana.

Figura 166

Usuarios concurrentes de los últimos dos meses.



Fuente: elaboración propia.

En base a los datos del gráfico 156, se procedió a tomar el número de usuarios concurrentes en diferentes puntos de tiempo de tres días consecutivos, obteniendo los resultados que se muestran en la siguiente tabla.

Tabla 20

Muestreo de conexiones de usuarios de escritorio VPN concurrentes.

Día	Hora	Usuarios en VPN Desktop
01/09/2021	10:30	64
	12:45	99
	14:30	77
	17:00	80
	18:00	76
	19:05	60
	23:30	30
02/09/2021	00:00	25
	03:10	5
	08:00	9

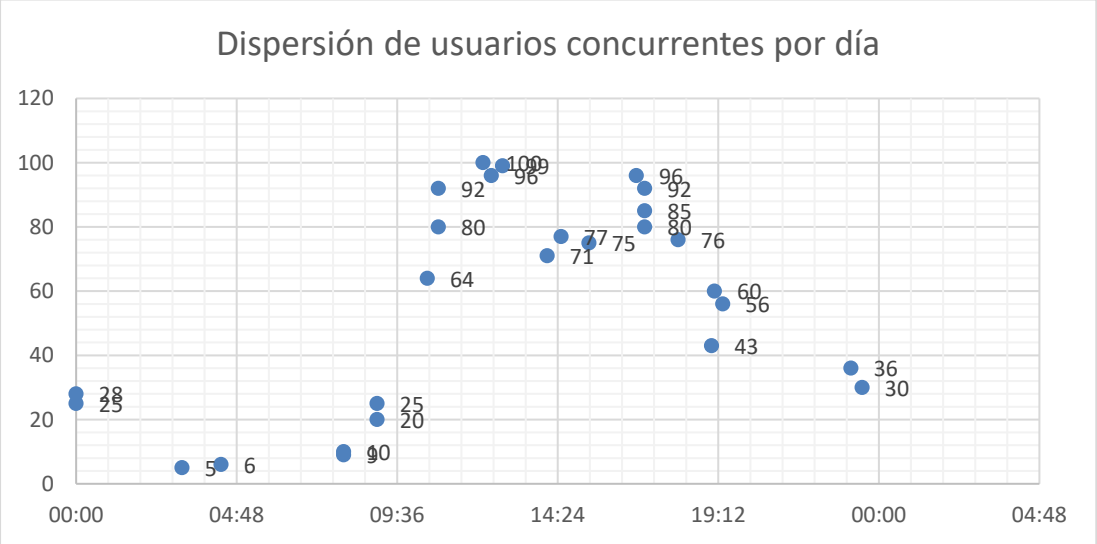
	09:00	25
	10:50	92
	12:25	96
	14:05	71
	16:45	96
	17:00	92
	19:20	56
	23:10	36
03/09/2021	00:00	28
	04:20	6
	08:00	10
	09:00	20
	10:50	80
	12:10	100
	15:20	75
	17:00	85
	19:00	43

Fuente: elaboración propia.

Con los datos de conexiones concurrentes de la Tabla 20 (datos de tres días consecutivos), se genera un gráfico de dispersión que muestra la concurrencia por horas del día, observándose el comportamiento de los usuarios: las horas pico de concurrencia para usuarios VPN de escritorio son alrededor de la 1:00pm y las 5:00pm.

Figura 167

Gráfico de dispersión de usuarios concurrentes para VPN de escritorio.



Fuente: elaboración propia.

Rendimiento: Según se aprecia en la figura 162 (detalle de la consola principal) de la plataforma OPNsense, se puede apreciar lo siguiente:

- **CPU:** la plataforma permanece en alrededor de 20% de uso en lo que corresponde a uso de CPU (unidad central de procesamiento). Se advierte que el procesador es de 8 núcleos y corre a 3.33 GHz.
- **Memoria:** desde su implementación hace un año, el uso de memoria permanece bajo el 15%. La máquina virtual cuenta con 12GB de memoria RAM.
- **Almacenamiento:** la máquina virtual se configuró con un disco duro de 30GB, de los cuales se usa un 6% (1,7 GB).

Objetivo 5: Garantizar la conexión concurrente de al menos el 90% de los dispositivos móviles asignados a los congresistas durante el desarrollo de las sesiones del Pleno del Congreso.

Resultados: Se verifica que se logró mantener el acceso concurrente de un mínimo del 90% de congresistas (al menos 117 de 130 congresistas).

En la siguiente tabla se muestra la tabulación de los datos obtenidos del gráfico 157 (Muestra de conexiones de los meses de junio-julio 2021), anotando el máximo número de usuarios concurrentes para cada sesión.

Tabla 21

Muestreo de conexiones de usuarios VPN Android concurrentes

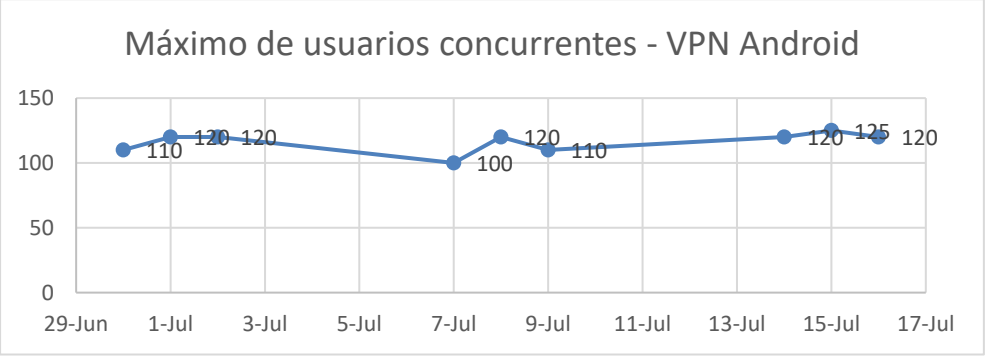
Mes	Día	Máximo de usuarios conectados
junio	30	110
julio	1	120
	2	120
	7	100
	8	120
	9	110
	14	120
	15	125
	16	120

Fuente: elaboración propia.

Con estos datos, se genera el siguiente cuadro, donde se muestra el numeró máximo de usuarios VPN Android durante los plenos del Congreso de junio-julio 2021.

Figura 168

Máximo de usuarios concurrentes de VPN Android.



Fuente: elaboración propia.

CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

- El objetivo principal del proyecto fue implementar OPNsense como la plataforma de Acceso Remoto Seguro en el Congreso de la República. Se puede verificar que efectivamente se logró la instalación, configuración e integración de la misma a la infraestructura de comunicaciones del Congreso de la República, utilizándose el sistema desde setiembre de 2020 a la actualidad. Asimismo, tal como se muestra en el análisis de resultados del cap. 4, el proyecto ejecutado pudo cumplir los objetivos específicos estipulados.
- El uso de la plataforma de Acceso Remoto Seguro ha servido como una herramienta base para facilitar la continuidad de operaciones del Congreso, permitiendo que al menos el 25% de los trabajadores de la institución realicen sus labores de manera remota durante el periodo de emergencia sanitaria declarado en el país.
- Con la ejecución y puesta en producción de este proyecto, se ha demostrado que es posible establecer una plataforma de acceso remoto seguro en base a una solución de software libre, sin que ello afecte negativamente el cumplimiento de los requerimientos de funcionalidad, integración, seguridad y rendimiento requeridos.
- Se prueba que el teletrabajo es un método viable de trabajo en nuestro medio. Se debe puntualizar que para ello es necesario disponer de medios físicos de acceso remoto a los servicios informáticos de una institución tales como computadores y línea de internet por parte de los usuarios, así como medios de software como son el establecimiento de una conexión segura mediante VPN, servicios web y de escritorio remoto habilitados, y el uso adecuado de herramientas de colaboración.

- El rendimiento de la plataforma es adecuado para los requerimientos solicitados. Sin embargo, se notó un deterioro en el rendimiento cuando se alcanzaron hasta 200 usuarios VPN de escritorio concurrentes (conjuntamente con las 130 conexiones VPN Android) entre los meses de marzo y abril de 2021. Cabe resaltar que es un escenario que no se ha repetido a la fecha.

RECOMENDACIONES

- **Adquisición de nuevo hardware para la plataforma de acceso remoto seguro.**

  Tal como se indicó en las conclusiones, en algunos momentos se llegó a observar más de 200 conexiones concurrentes de escritorio, lo cual excede en 100% las expectativas de uso del dimensionamiento original. En estos casos se notó un deterioro del rendimiento de la plataforma representado como lentitud esporádica en el funcionamiento de los escritorios remotos (alrededor de un segundo de demora en la respuesta del mouse y/o teclado cada 30 segundos aproximadamente).

  Debido a que este proyecto implementó sobre un equipo de hardware que cuenta con 15 años de antigüedad y sin soporte técnico vigente, se debe realizar la adquisición de una nueva plataforma de hardware (servidores) para el redespliegue del mismo sin afectar el funcionamiento ni configuración actuales, con lo que pretende mejorar dos aspectos claves:

  - **Alta Disponibilidad:** la plataforma OPNsense ofrece la capacidad de despliegue en alta disponibilidad, lo que brindaría un nivel de tolerancia a fallas para mantener la continuidad de operación de la que no se dispone actualmente. Por lo tanto, se deber adquirir dos (02) servidores para tal efecto.
  - **Rendimiento:** el procesador del servidor actual (Intel Xeon Dual DP del año 2006) no dispone de las instrucciones de encriptación basadas en hardware AES-NI, lo cual afecta negativamente en el rendimiento de la plataforma cuando las conexiones concurrentes exceden los 200 usuarios de escritorio, evento que ha sucedido en algunas ocasiones.

Una vez realizada la adquisición de la nueva plataforma de hardware según la recomendación arriba indicada, se podrán implementar mejoras a la configuración de la plataforma, tales como:

- **Revisión de las configuraciones de buffers de conexión OpenVPN**

  Existe la posibilidad de mejorar el rendimiento del sistema ajustando los parámetros de buffers de comunicación tanto en el servidor como en la configuración de los clientes VPN.

- **Uso de protocolo UDP en lugar de TCP**

  Para la ejecución de este proyecto se eligió usar el protocolo TCP para evitar bloqueos en firewalls externos que se conecten hacia el servicio VPN del Congreso, pero en la práctica el caso de uso de conexiones VPN ha sido eminentemente desde conexiones domiciliarias, por lo que evitar la sobrecarga de transmitir paquetes TCP de VPN sobre una conexión TCP de Internet se puede evitar al transmitir paquetes UDP VPN sobre protocolo TCP de conexiones Internet.

- **Actualización de la plataforma OPNsense**

  El Sistema de Acceso Remoto Seguro actualmente en producción se encuentra en la versión 20.1, que era la última vigente en el momento del inicio de este proyecto. Habiendo transcurrido un año de su puesta en servicio, no se han realizado actualizaciones debido a que no se dispone de hardware para realizar las pruebas de impacto y rendimiento que implicaría la actualización a la versión actual (21.7), por lo que la ejecución de esta actualización depende de la implementación de la primera recomendación (adquisiu.

- **Evaluar la posibilidad de implementación de tecnologías de escritorios virtuales (VDI – Virtual Desktop Infraestructure) en la institución, como alternativa y/o complemento al uso de VPN**

  En la actualidad las PC de los usuarios deben permanecer encendidas las 24 horas del día, los siete días de la semana para permitir el acceso remoto a las mismas, con el consecuente consumo eléctrico elevado, costos operativos, desgaste prematuro del equipamiento y riesgos eléctricos debido al sobrecalentamiento de los equipos y la antigüedad de las instalaciones.

  Una solución VDI centralizaría los computadores utilizados remotamente en servidores de virtualización hospedados en los centros de datos, mejorando el consumo eléctrico, permitiendo garantizar el funcionamiento continuo de los mismos, facilitando la realización de copias de seguridad, recuperaciones de emergencia y soporte remoto, así como mejorar la seguridad y simplificar el acceso a los recursos. En el mes de setiembre de 2021, la empresa VMware, fabricante de soluciones de virtualización de servidores y sistemas de escritorio, conjuntamente con un equipo del Área de Infraestructura Tecnológica, nos encontramos en la etapa de implementación de una Prueba de Concepto de la solución VMware Horizon, la que permitiría el acceso remoto seguro a escritorios físicos y virtuales directamente desde un navegador web.

REFERENCIAS

Abdelmajid Lakbabi, G. O. (s.f.). *Network Access Control Technology.* Obtenido de https://arxiv.org/ftp/arxiv/papers/1304/1304.0807.pdf

Cisco. (s.f.). *What Is a Next-Generation Firewall?* Obtenido de https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-next-generation-firewall.html

Comodo. (2 de agosto de 2021). *Endpoint Detection and Response (EDR).* Obtenido de https://enterprise.comodo.com/blog/what-is-endpoint-detection-response/

ComputerScience. (s.f.). *ComputerScience Wiki.* Obtenido de https://computersciencewiki.org/index.php/VPN

Congreso. (jumio de 2011). *Parlamento Escolar.* Obtenido de https://www.congreso.gob.pe/Docs/participacion/parlamento-escolar/files/separata_uso_video.pdf

Congreso. (26 de mayo de 2020). *Portal del Congreso de la República*. Obtenido de https://www.congreso.gob.pe/Docs/medidas-covid19/files/acuerdo_n_028-2020-2021mesa-cr.pdf

Congreso. (s.f.). *Funciones del Congreso de la República.* Obtenido de https://www.congreso.gob.pe/funciones/

Congreso. (s.f.). *Misión y Visión del Congreso.* Obtenido de https://www.congreso.gob.pe/VisionMision/

Congreso. (s.f.). *Organización del Congreso.* Obtenido de https://www.congreso.gob.pe/home?K=17

DoubleOctopus. (s.f.). *The Secret Security Wiki.* Obtenido de https://doubleoctopus.com/security-wiki/authentication/time-based-one-time-password/

Forcepoint. (s.f.). *What is a Firewall?* Obtenido de https://www.forcepoint.com/es/cyber-edu/firewall

Forcepoint. (s.f.). *What is Malware?* Obtenido de https://www.forcepoint.com/cyber-edu/malware

Forcepoint. (s.f.). *What is Sandbox Security?* Obtenido de https://www.forcepoint.com/es/cyber-edu/sandbox-security

GeeksforGeeks. (26 de junio de 2018). *GeeksforGeeks*. Obtenido de https://www.geeksforgeeks.org/computer-network-aaa-authentication-authorization-and-accounting/

HelpSystems. (29 de diciembre de 2020). *What's the Difference Between Two-Factor Authentication and Multi-Factor Authentication?* Obtenido de https://www.helpsystems.com/resources/articles/whats-difference-between-two-factor-authentication-and-multi-factor

HelpSystems. (29 de diciembre de 2020). *What's the Difference Between Two-Factor Authentication and Multi-Factor Authentication?* Obtenido de https://www.helpsystems.com/resources/articles/whats-difference-between-two-factor-authentication-and-multi-factor

Hope, C. (6 de julio de 2021). *Virus signature.* Obtenido de https://www.computerhope.com/jargon/v/virus-signature.htm

IVPN. (s.f.). *Comparison of VPN protocols.* Obtenido de https://www.ivpn.net/pptp-vs-ipsec-ikev2-vs-openvpn-vs-wireguard/

Lord, N. (10 de setiembre de 2018). *Digital Guardian*. Obtenido de https://digitalguardian.com/blog/what-endpoint-protection-data-protection-101

ManageEngine. (s.f.). *Manage Engine Desktop Central.* Obtenido de https://www.manageengine.com/products/desktop-central/endpoint-management.html

Miradore. (8 de setiembre de 2020). *A Complete Guide to Mobile Device Management (MDM).* Obtenido de https://www.miradore.com/blog/mdm-mobile-device-management/

Okta. (s.f.). *Authentication vs. Authorization.* Obtenido de https://www.okta.com/identity-101/authentication-vs-authorization

OPNsense. (s.f.). *OPNsense.* Obtenido de https://opnsense.org/about/about-opnsense/

Oracle. (s.f.). *What is IoT?* Obtenido de https://www.oracle.com/internet-of-things/what-is-iot/

Paessler. (s.f.). *IT Explained: Active Directory.* Obtenido de https://www.paessler.com/es/it-explained/active-directory

PaloAlto. (s.f.). *Endpoint detection and response.* Obtenido de https://www.paloaltonetworks.com/cyberpedia/what-is-endpoint-detection-and-response-edr

PaloAlto. (s.f.). *What Is a Site-to-Site VPN?* Obtenido de https://www.paloaltonetworks.com/cyberpedia/what-is-a-site-to-site-vpn

PaloAlto. (s.f.). *What is an Endpoint?* Obtenido de https://www.paloaltonetworks.com/cyberpedia/what-is-an-endpoint

PCI. (s.f.). *PCI Security Standards Council.* Obtenido de https://es.pcisecuritystandards.org/minisite/env2/

PCMagazine. (s.f.). *PC Magazine.* Obtenido de https://www.pcmag.com/encyclopedia/term/accountability

Presidencia. (11 de marzo de 2020). *Diario Oficial El Peruano*. Obtenido de https://busquedas.elperuano.pe/normaslegales/decreto-supremo-que-declara-en-emergencia-sanitaria-a-nivel-decreto-supremo-n-008-2020-sa-1863981-2/

ProofPoint. (s.f.). *What is a Sandbox?* Obtenido de https://www.proofpoint.com/us/threat-reference/sandbox

Rehan, S. A. (6 de diciembre de 2020). *Remote Access VPN To Work From Home Using OpenVPN Access Server*. Obtenido de https://nprog.medium.com/remote-access-vpn-to-work-from-home-283402bbc83

Samsung. (s.f.). *Knox Manage.* Obtenido de https://www.samsungknox.com/es-419/solutions/it-solutions/knox-manage

Short, T. (13 de febrerpo de 2020). *Software Advice.* Obtenido de https://www.softwareadvice.com/resources/saas-10-faqs-software-service/

Technopedia. (29 de noviembre de 2017). *Access Control*. Obtenido de https://www.techopedia.com/definition/5831/access-control

Techslang. (s.f.). *What is On Premises?* Obtenido de https://www.techslang.com/definition/what-is-on-premises/

TechTarget. (s.f.). *TechTarget.* Obtenido de https://searchsecurity.techtarget.com/definition/two-factor-authentication

TechTerms. (s.f.). *Encryption.* Obtenido de https://techterms.com/definition/encryption

TechTerms. (s.f.). *QR Code.* Obtenido de https://techterms.com/definition/qr_code

TechTerms. (s.f.). *Remote Desktop.* Obtenido de https://techterms.com/definition/remotedesktop

TrendMicro. (s.f.). *Endpoint Security con Apex One.* Obtenido de https://www.trendmicro.com/es_es/business/products/user-protection/sps/endpoint.html

Varonis. (s.f.). *The Difference Between Active Directory and LDA.* Obtenido de https://www.varonis.com/blog/the-difference-between-active-directory-and-ldap/

VMware. (s.f.). Obtenido de https://www.vmware.com/topics/glossary/content/secure-remote-access

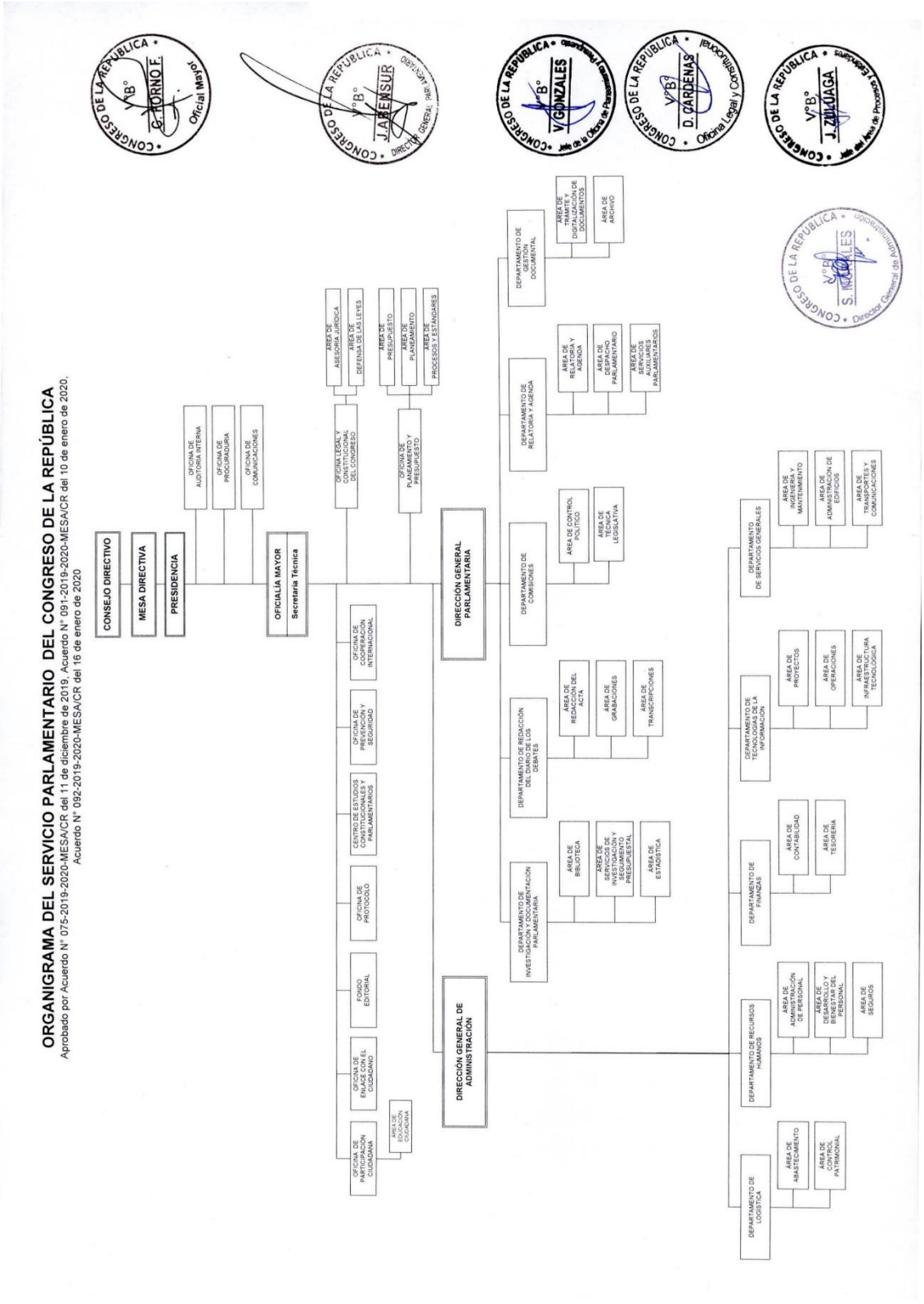
Webroot. (s.f.). *What is Antivirus Software?* Obtenido de https://www.webroot.com/us/en/resources/tips-articles/what-is-anti-virus-software

welivesecurity. (4 de mayo de 2017). *A short history of the computer password*. Obtenido de https://www.welivesecurity.com/2017/05/04/short-history-computer-password/

Wiki, C. S. (s.f.). *Computer Science Wiki*. Obtenido de https://computersciencewiki.org/index.php/VPN

ANEXOS

Anexo n.° 1. Organigrama Oficial del Congreso de la República



Anexo n.° 2. Guía De Administración De Usuarios OpenVPN

OFICINA DE TECNOLOGÍAS DE INFORMACIÓN

ÁREA DE INFRAESTRUCTURA TECNOLÓGICA

GUÍA DE ADMINISTRACIÓN DE USUARIOS OPENVPN

Versión 1.0

CONGRESO de la REPÚBLICA	GUÍA DE ADMINISTRACIÓN DE USUARIOS OPENVPN	CODIGO GUIA-ADMIN-USUARIOS-OPENVPN	
		FECHA 10/09/2020	VERSION 1.0

1. CONTROL DE CAMBIOS

VERSIÓN	FECHA	NOTA	MODIFICADO POR:
1.0	09/07/2020	Versión inicial	Emilio Cobos

2. RESUMEN

Guía para implementar un servidor de acceso VPN. Este ofrecerá el servicio de acceso a servicios internos de la institución de manera segura.

La guía muestra la configuración de dos tipos de usuario:

- Usuarios de VPN para escritorio remoto: cliente desktop.
- Usuarios de VPN por dispositivo Android: cliente móvi.

3. INDICE

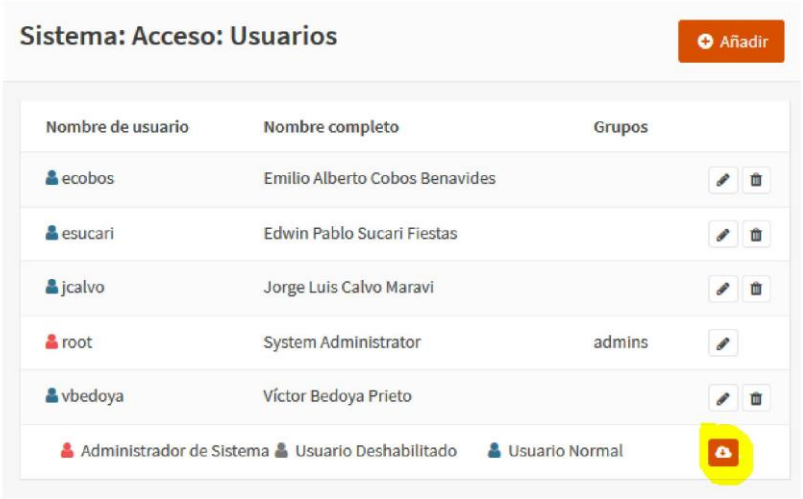
4. PROCEDIMIENTO

- Agregar al ususario de dominio al grupo “OpenVPN” del Directorio Activo (CN=OpenVPN,CN=Users,DC=congreso,DC=net).
- Ir al servidor https://vpn.congreso.net e ingresar las credenciales de administración

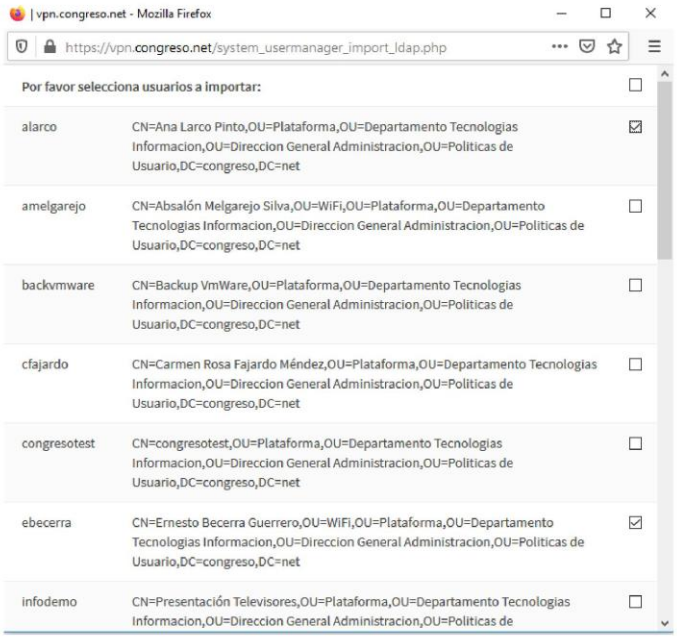
4.1. CLIENTE DESKTOP PARA ESCRITORIO REMOTO

4.1.1. IMPORTAR USUARIOS DE LDAP

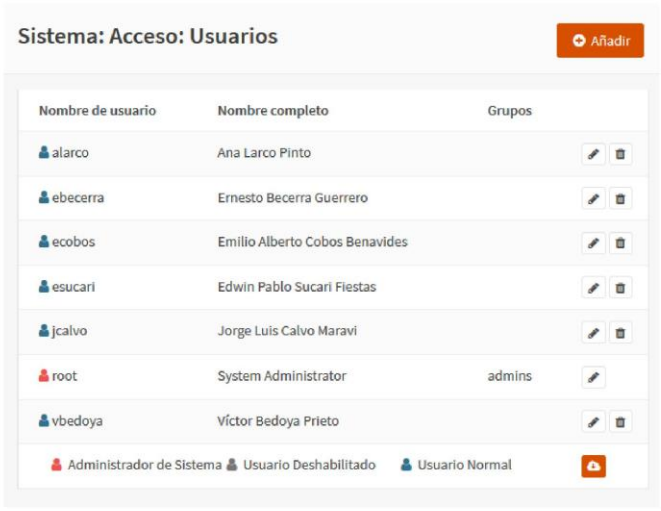
- Ir a Sistema / Acceso/ Usuarios y hacer click en el botón “Import” (esquina inferior derecha)



- Se abrirá una ventana donde se listarán los usuarios del dominio que cumplen los criterios del servidor de acceso LDAP. Seleccionar los usuarios a importar marcando la casilla a la derecha de cada usuario. Hacer click en “Guardar” al final de la ventana.


vpn.congreso.net - Mozilla Firefox
https://vpn.congreso.net/system_usermanager_import_ldap.php
Por favor selecciona usuarios a importar:
alarco CN=Ana Larco Pinto,OU=Plataforma,OU=Departamento Tecnologias Informacion,OU=Direccion General Administracion,OU=Politicas de Usuario,DC=congreso,DC=net
amelgarejo CN=Absalón Melgarejo Silva,OU=WiFi,OU=Plataforma,OU=Departamento Tecnologias Informacion,OU=Direccion General Administracion,OU=Politicas de Usuario,DC=congreso,DC=net
backvmware CN=Backup VmWare,OU=Plataforma,OU=Departamento Tecnologias Informacion,OU=Direccion General Administracion,OU=Politicas de Usuario,DC=congreso,DC=net
cfajardo CN=Carmen Rosa Fajardo Méndez,OU=Plataforma,OU=Departamento Tecnologias Informacion,OU=Direccion General Administracion,OU=Politicas de Usuario,DC=congreso,DC=net
congresotest CN=congresotest,OU=Plataforma,OU=Departamento Tecnologias Informacion,OU=Direccion General Administracion,OU=Politicas de Usuario,DC=congreso,DC=net
ebecerra CN=Ernesto Becerra Guerrero,OU=WiFi,OU=Plataforma,OU=Departamento Tecnologias Informacion,OU=Direccion General Administracion,OU=Politicas de Usuario,DC=congreso,DC=net
infodemo CN=Presentación Televisores,OU=Plataforma,OU=Departamento Tecnologias Informacion,OU=Direccion General Administracion,OU=Politicas de

- Resultado:


Sistema: Acceso: Usuarios
Añadir
Nombre de usuario
Nombre completo
Grupos
alarco Ana Larco Pinto
ebecerra Ernesto Becerra Guerrero
ecobos Emilio Alberto Cobos Benavides
esucari Edwin Pablo Sucari Fiestas
jcalvo Jorge Luis Calvo Maravi
root System Administrator admins
vbedoya Víctor Bedoya Prieto
Administrador de Sistema
Usuario Deshabilitado
Usuario Normal

4.1.2. CREAR CERTIFICADO DIGITAL DE USUARIO

- Editar usuario con el símbolo de lápiz a la derecha del nombre de usuario.
- Ir a la sección "Certificados de Usuario" y hacer click en "+"

Se mostrará la ventana Sistema / Confianza / Certificados. Elegir el método "Crear un Certificado Interno", verificar que la Autoridad de Certificación es "SSL VPN CA" y colocar el Tiempo de vida (días) del certificado. Por omisión es 825 días. **NOTA:** no cambiar el Nombre descriptivo ni el Nombre Común

-

Hacer click en "Guardar". Esto regresará a la ventana anterior donde podremos crear el código QR para TOTP.

4.1.3. CREAR QR PARA TOTP DE USUARIO

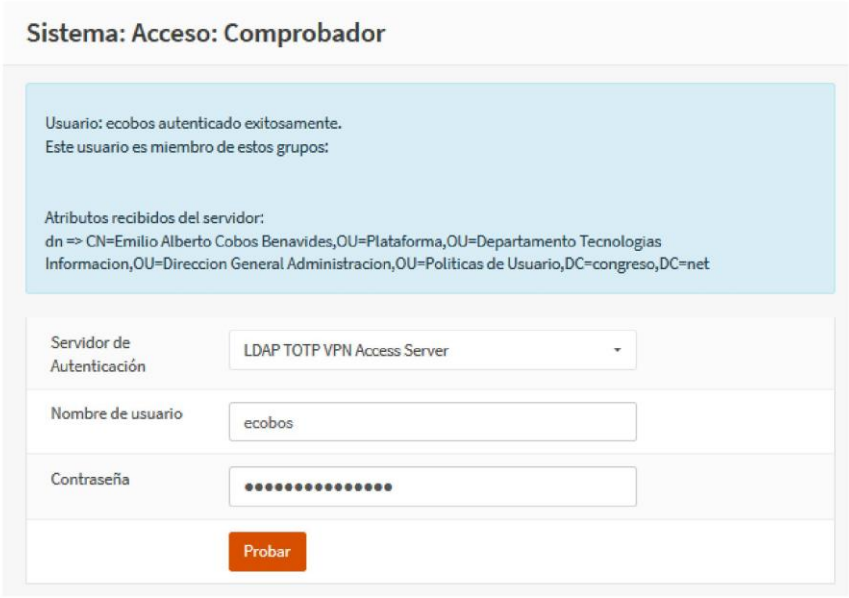
- En la ventana de edición de usuario ir a la sección "Semilla OTP" y marcar la casilla "Generar un nuevo secreto (160 bit). Hacer click en "Guardar"

- Ir a la sección "Código OTP QR" y hacer click en el botón "Clic para mostrar"
- Copiar código QR para ser enviado a usuario.

4.2. PRUEBA DE AUTENTICACIÓN DE USUARIO

- Ir a Sistema / Acceso / Comprobador

- Para probar el acceso de un usuario, elegir el servidor de autenticación, poner sus credenciales de dominio y hacer click en "Probar".
  NOTA: no olvide colocar los 6 dígitos del generador TOTP después de su contraseña de dominio



4.3. REGLAS DE FIREWALL

4.3.1. REGLAS OPENVPN

En este caso, para dar acceso MS RDP (escritorio remoto) a los usuarios, como medida de seguridad vamos a restringir que cada cliente sólo tenga acceso a su respectiva PC institucional. Para ello necesitamos:

- **1) IP fijo otorgado al cliente VPN**. Para ello, se utilizará una regla CSO (Client Specific Override o Sobreescrituras Específicas de Cliente), la cual contendrá la dirección de la subred asignada al usuario.

  Debido a que se asignará una red privada a cada usuario, se utilizará para cada usuario una red que consta de 4 números IP, y que es una subred del rango 10.10.72.0/21

  Ejemplo:

Usuario 1:	Descripción de IP
10.10.72.0/30	Nombre de red (va en la CSO)
10.10.72.1	IP del servidor
10.10.72.2	IP del cliente (va como alias para reglas de firewall)
10.10.72.3	IP de Broadcast

Usuario 2:	Descripción de IP
10.10.72.4/30	Nombre de red (va en la CSO)
10.10.72.5	IP del servidor
10.10.72.6	IP del cliente (va como alias para reglas de firewall)
10.10.72.7	IP de Broadcast

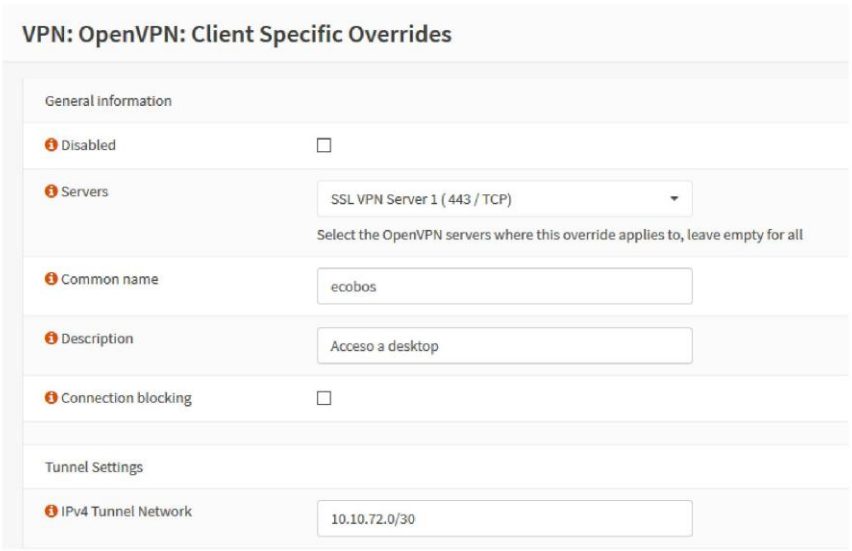
Se ha creado una hoja de Excel llamada VPN_RANGES.xlsx para llevar control de las IPs asignadas.

El nombre de la CSO debe ser el mismo del "Nombre Común" del certificado del usuario, que como vimos antes debe ser el mismo del nombre de usuario del dominio.

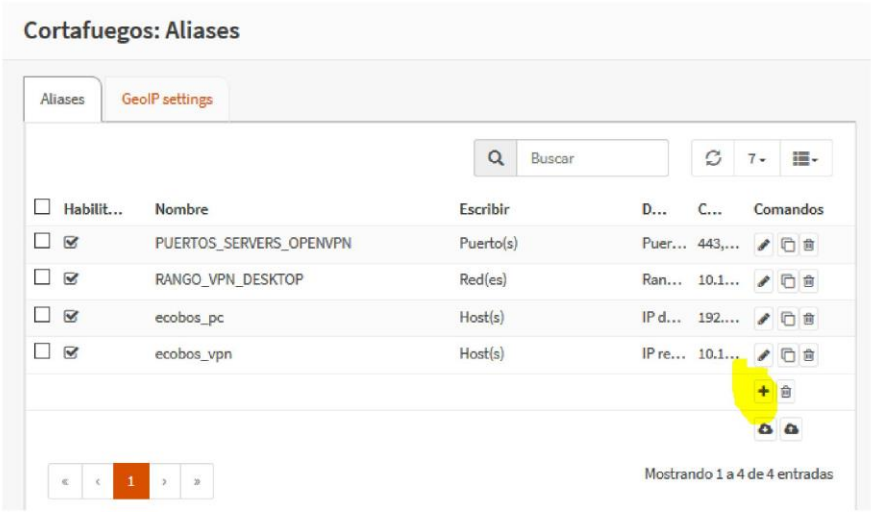
Crear CSO:

- Ir a VPN / OpenVPN / Sobreescrituras Específicas de Cliente y hacer click en "Añadir"
- Llenar según lo indicado y grabar:

Servidores	*SSL VPN Server 1 (443 / TCP)*
Nombre Común	*<nombre del usuario> Ejemplo: ecobos*
Descripción	*Acceso a desktop*
Red Tunel IPv4	*<Nombre de red> Ejemplo: 10.10.72.0/30*



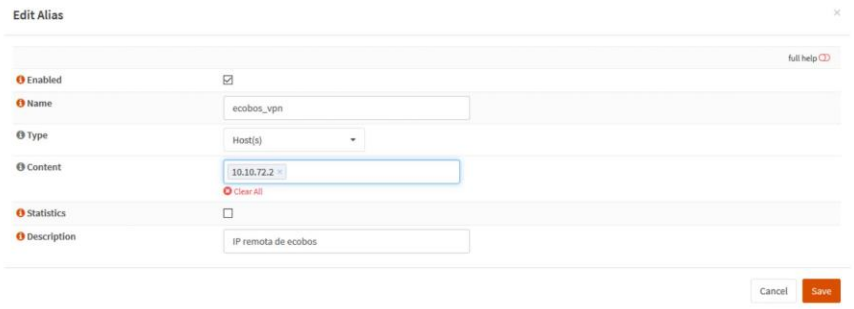
- En Cortafuegos / Aliases crear un alias al IP de cliente VPN haciendo click en "+".



- Recuerde usar el IP correspondiente según la subred elegida.
- Ejemplo:

Nombre	Contenido
ecobos_vpn	10.10.72.2

-

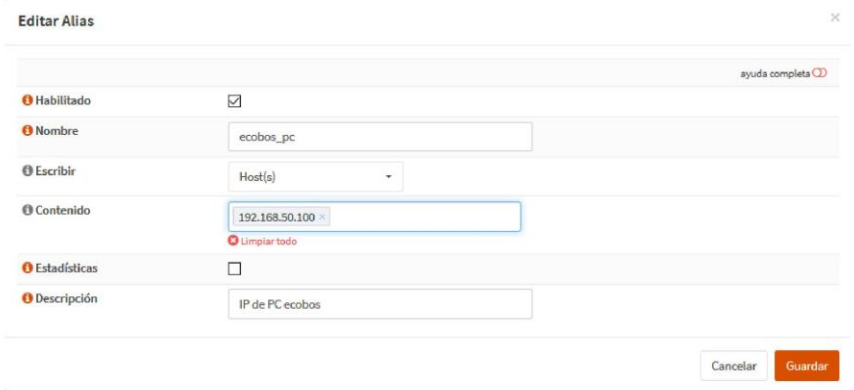


- **2) IP de la PC institucional**

Ejemplo:

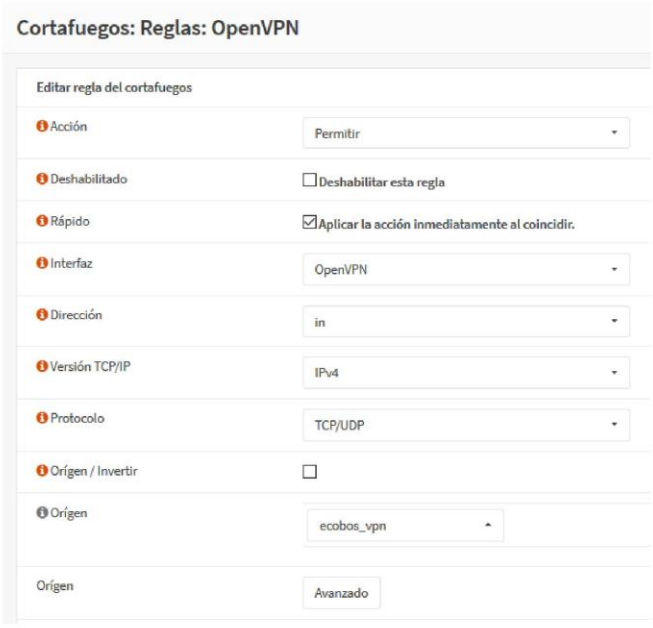
Nombre	Contenido
ecobos_pc	172.30.1.2

- En Cortafuegos / Aliases crear un alias al IP de la PC haciendo click en "+".

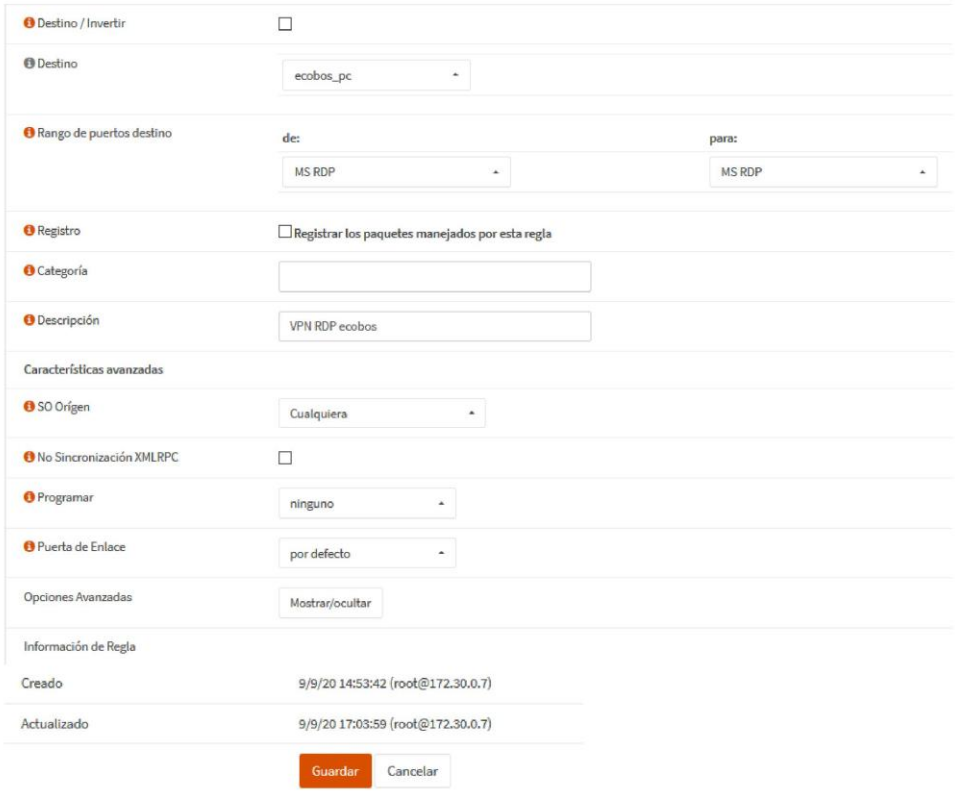


- **3) Regla de Firewall:** crear la regla de firewall específica para este usuario. Ir a Cortafuegos / Reglas /OpenVPN y agregar una regla, luego grabar y aplicar.

Interfaz	*OpenVPN*
Dirección	*In*
TCP/IP version	*IPv4*
Protocolo	*TCP/UDP*
Orígen	*<alias de IP fija de VPN de usuario>* *Ejemplo: ecobos_vpn*
Destino	*<alias de IP fija de PC local de usuario>* *Ejemplo: ecobos_pc*
Rango de puertos destino	*MS RDP a MS RDP*
Descripción	*Acceso a desktop*



CONGRESO de la REPÚBLICA	GUÍA DE ADMINISTRACIÓN DE USUARIOS OPENVPN	CODIGO GUIA-ADMIN-USUARIOS-OPENVPN	
		FECHA 10/09/2020	VERSION 1.0



5. EXPORTAR CONFIGURACIÓN DE CLIENTE

La dirección pública del servidor VPN es vpn.congreso.gob.pe (IP 190.116.46.147)

- Ir a VPN / OpenVPN / Exportar Cliente y seleccionar las siguientes opciones:

Servidor de acceso remoto	*SSL VPN Server 1 TCP:443*
Exportar tipo	*Archivo*
Nombre host	*vpn.congreso.gob.pe*
P12 Password/confirm	*<en blanco>*
Desactivar guardado de contraseña	*<seleccionado> (con check)*

- Descargar el archivo correspondiente al usuario. Ejemplo: ecobos

Este archivo y su respectivo código QR deberán ser enviados al cliente.

5.1. CONFIGURAR ACCESO VPN

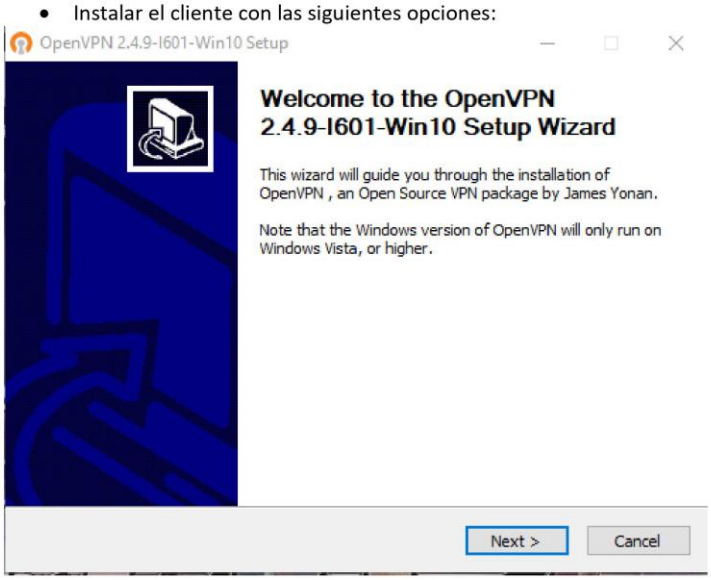
5.1.1. CONFIGURAR GENERADOR TOTP

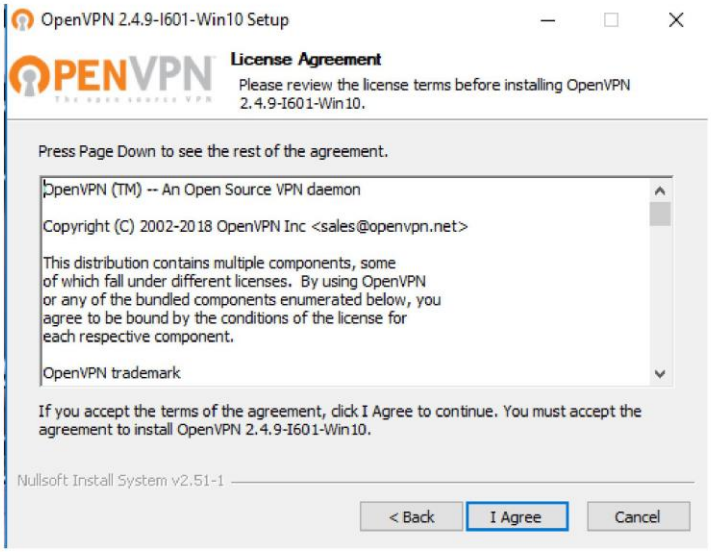
- Utilizar la aplicación Google Authenticator en su Smartphone Android (descargarla de Google Play Store de ser necesario)
- En la aplicación haga click en el botón "+" en la esquina inferior derecha, lija "Escanear un código QR" y escanée el código QR recibido.
- Se agregará una entrada en su lista de códigos generados con el nombre <nombre de usuario>@vpn

5.1.2. CONFIGURAR CLIENTE VPN

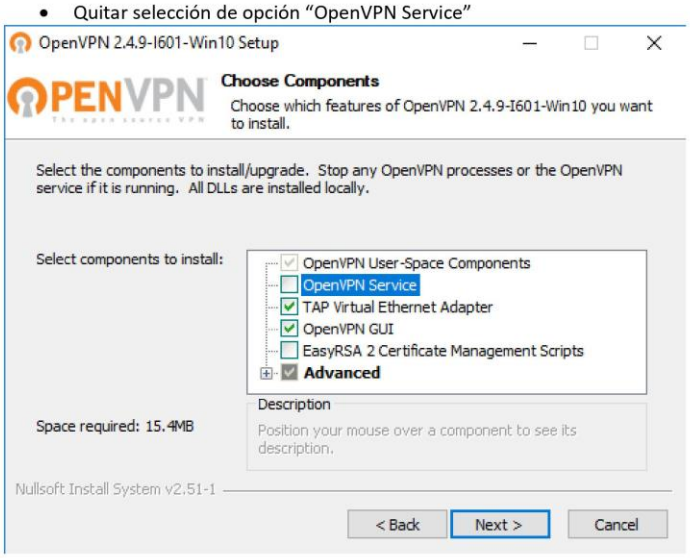
Descargar cliente desde https://openvpn.net/community-downloads/ (versión vigente a la fecha de este documento: OpenVPN 2.4.9). Seleccionar la versión adecuada para Windows 7/8 ó Windows 10:

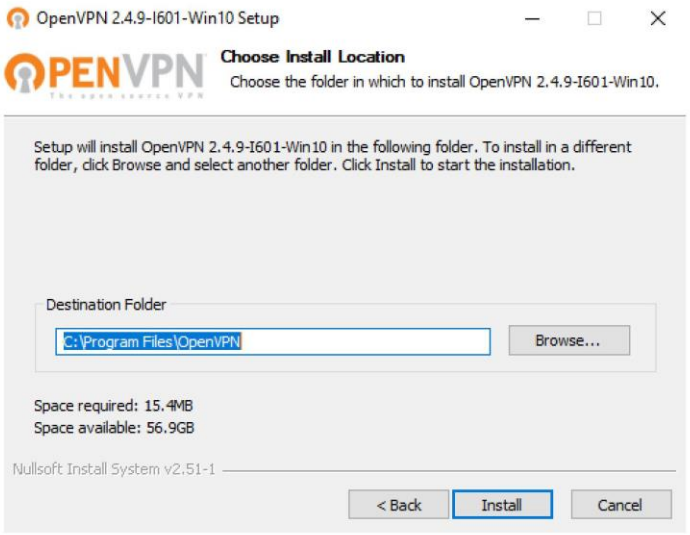
- Instalar el cliente con las siguientes opciones:

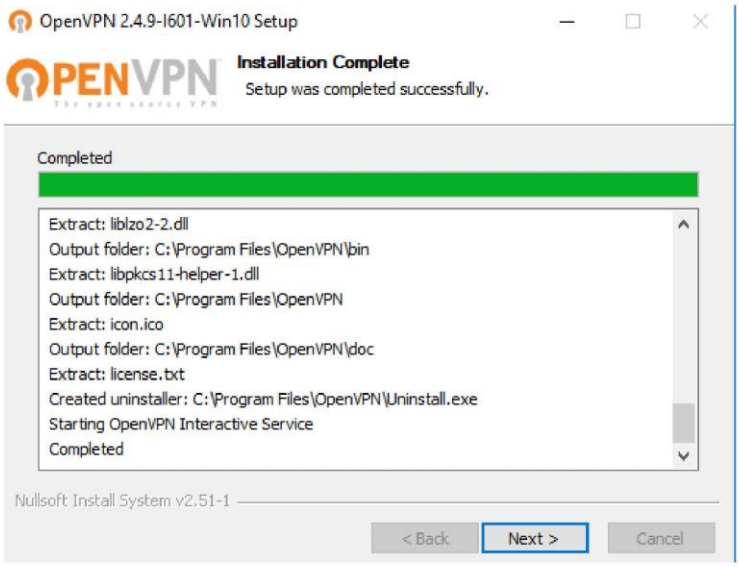


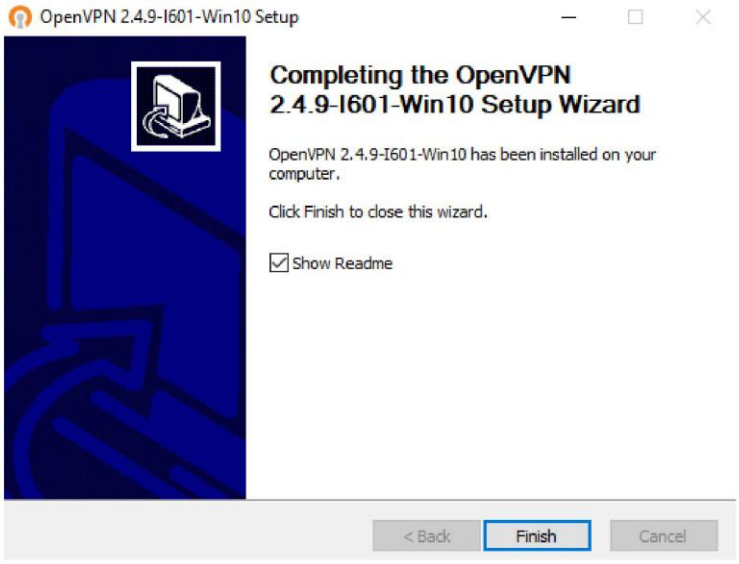


- Quitar selección de opción “OpenVPN Service”



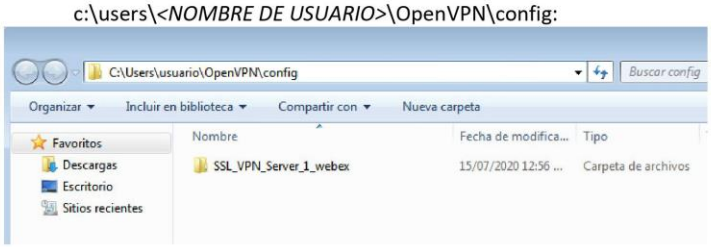

OpenVPN 2.4.9-I601-Win10 Setup
OPENVPN
Choose Install Location
Choose the folder in which to install OpenVPN 2.4.9-I601-Win10.
Setup will install OpenVPN 2.4.9-I601-Win10 in the following folder. To install in a different folder, click Browse and select another folder. Click Install to start the installation.
Destination Folder
C:\Program Files\OpenVPN
Browse...
Space required: 15.4MB
Space available: 56.9GB
Nullsoft Install System v2.51-1
< Back
Install
Cancel


OpenVPN 2.4.9-I601-Win10 Setup
OPENVPN
Installation Complete
Setup was completed successfully.
Completed
Extract: liblzo2-2.dll
Output folder: C:\Program Files\OpenVPN\bin
Extract: libpkcs11-helper-1.dll
Output folder: C:\Program Files\OpenVPN
Extract: icon.ico
Output folder: C:\Program Files\OpenVPN\doc
Extract: license.txt
Created uninstaller: C:\Program Files\OpenVPN\Uninstall.exe
Starting OpenVPN Interactive Service
Completed
Nullsoft Install System v2.51-1
< Back
Next >
Cancel



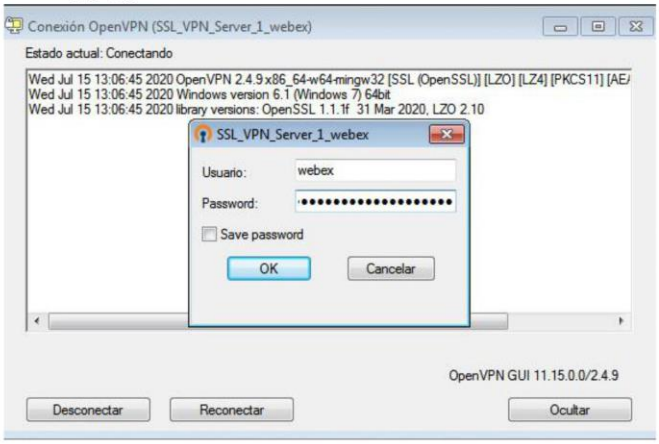
- Ejecutar el ícono:

- Desempaquetar el archivo de configuración de usuario descargado del sistema VPN (ejemplo: "SSL_VPN_Server_1_ecobos.zip") en el directorio c:\users*<NOMBRE DE USUARIO>*\OpenVPN\config:

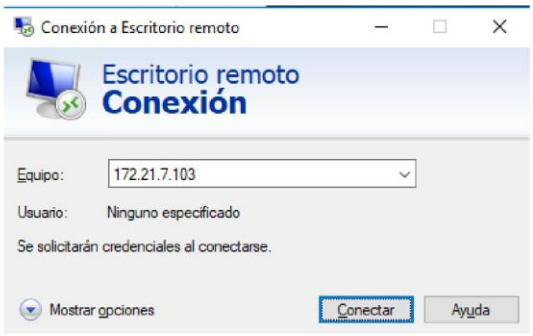


- Acceder haciendo click derecho sobre el ícono de OpenVPN GUI en la esquina inferior derecha de la pantalla y seleccionar la opción "Conectar"

- En este ventana, ingresar:
    - Usuario: nombre de usuario de acceso a PC del Congreso.
    - Password: la contraseña de acceso a PC del Congreso seguida del código de seis dígitos indicados en el app de autenticación (Google Authenticator, Microsoft Authenticator y/o FreeOTP), y haciendo click en "OK"



- Validar el acceso a la VPN póniendo el cursor sobre el ícono de OpenVPN GUI.
- Ingresar a su escritorio remoto utilizando la aplicación de Windows "Conexión a Escritorio Remoto", colocando el número IP de su PC institucional y haciendo click en "Conectar", tras lo cual se les pedirá sus credenciales de dominio.



Anexo n.° 3. Guía De Configuración De Acceso Vpn Para Usuarios

OFICINA DE TECNOLOGÍAS DE INFORMACIÓN

ÁREA DE INFRAESTRUCTURA TECNOLÓGICA

GUÍA DE CONFIGURACIÓN DE ACCESO VPN PARA USUARIOS

Versión 1.0

CONGRESO de la REPÚBLICA	GUÍA DE CONFIGURACIÓN DE ACCESO VPN PARA USUARIOS	CODIGO GUIA-CONFIGURACION-USUARIOS-OPENVPN	
		FECHA 10/09/2020	VERSION 1.0

1. CONTROL DE CAMBIOS

VERSIÓN	FECHA	NOTA	MODIFICADO POR:
1.0	09/07/2020	Versión inicial	Emilio Cobos

2. RESUMEN

Guía para configurar el acceso VPN en los equipos de los usuarios.

3. INDICE

4. PROCEDIMIENTO

4.1. CONFIGURAR GENERADOR TOTP

- Utilizar la aplicación Google Authenticator en su smartphone Android (descargarla de Google Play Store de ser necesario).
- En la aplicación haga click en el botón "+" en la esquina inferior derecha, lija "Escanear un código QR" y escanée el código QR recibido.
- Se agregará una entrada en su lista de códigos generados con el nombre <nombre de usuario>@vpn

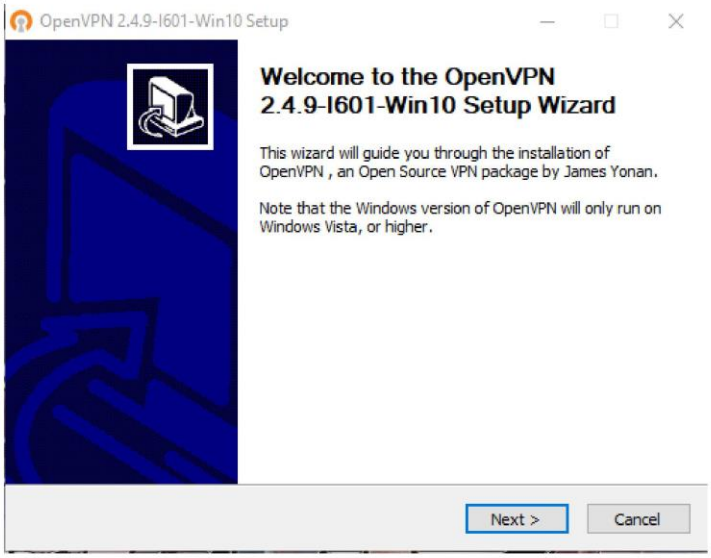
  NOTA: también se pueden utilizar aplicaciones Microsoft Authenticator y FreeOTP.

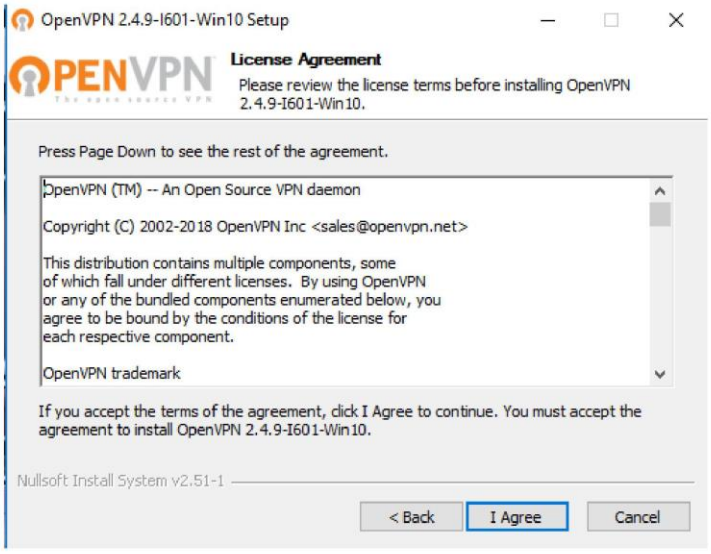
4.2. CONFIGURAR CLIENTE VPN

Descargar cliente desde https://openvpn.net/community-downloads/ (versión vigente a la fecha de este documento: OpenVPN 2.4.9). Seleccionar la versión adecuada para Windows 7/8 ó Windows 10:

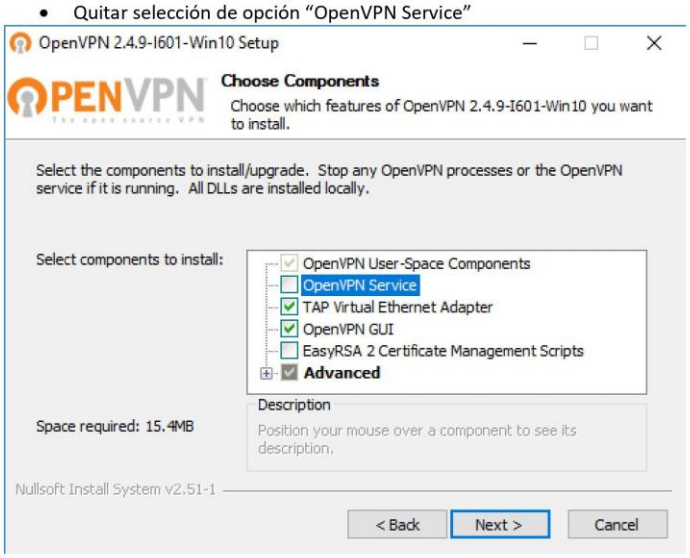
- Instalar el cliente con las siguientes opciones:

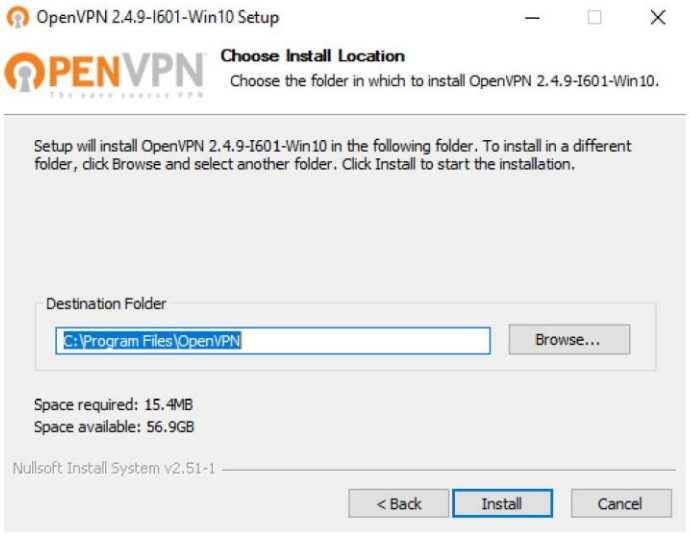
CONGRESO de la REPÚBLICA	GUÍA DE CONFIGURACIÓN DE ACCESO VPN PARA USUARIOS	CODIGO: GUIA-CONFIGURACION-USUARIOS-OPENVPN	
		FECHA: 10/09/2020	VERSION: 1.0



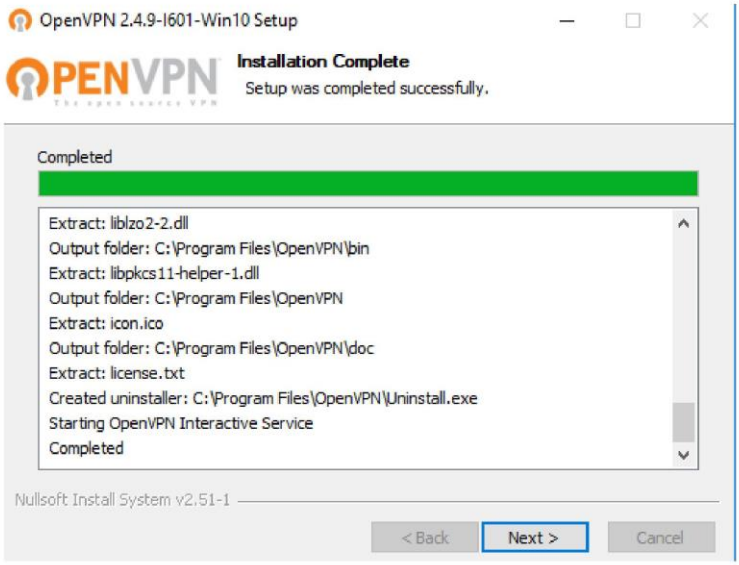


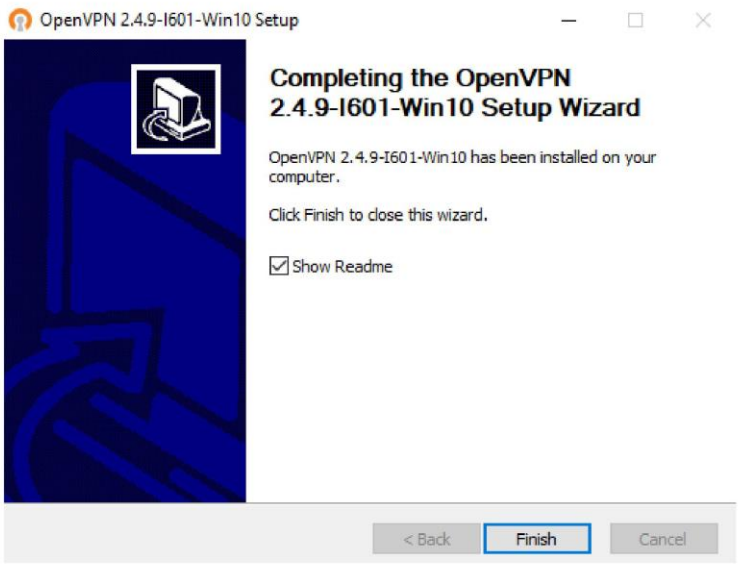
- Quitar selección de opción "OpenVPN Service"





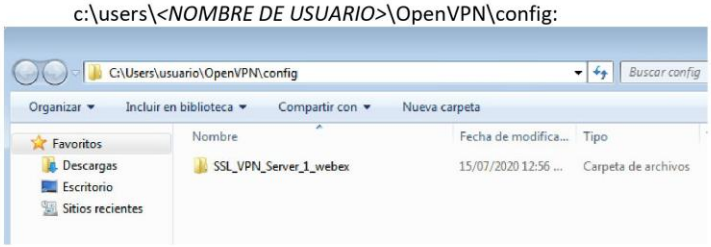
CONGRESO de la REPÚBLICA	GUÍA DE CONFIGURACIÓN DE ACCESO VPN PARA USUARIOS	CODIGO: GUIA-CONFIGURACION-USUARIOS-OPENVPN	
		FECHA: 10/09/2020	VERSION: 1.0





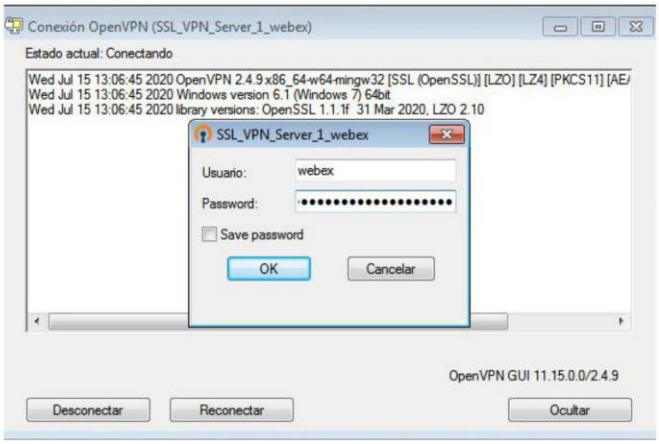
- Ejecutar el ícono:

- Desempaquetar el archivo de configuración de usuario descargado del sistema VPN (ejemplo: "SSL_VPN_Server_1_ecobos.zip") en el directorio c:\users\<*NOMBRE DE USUARIO*>\OpenVPN\config:



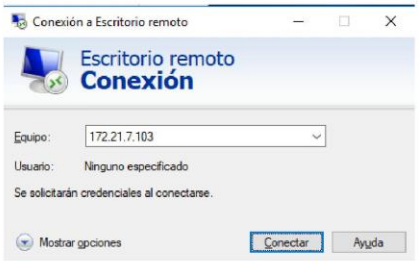
4.3. ACCEDER A LA VPN

- Acceder haciendo click derecho sobre el ícono de OpenVPN GUI en la esquina inferior derecha de la pantalla y seleccionar la opción "Conectar"
- En este ventana, ingresar:
  - Usuario: nombre de usuario de acceso a PC del Congreso.
  - Password: la contraseña de acceso a PC del Congreso seguida del código de seis dígitos indicados en el app de autenticación (Google Authenticator, Microsoft Authenticator y/o FreeOTP), y haciendo click en "OK"



- Validar el acceso a la VPN póniendo el cursor sobre el ícono de OpenVPN GUI.

- Ingresar a su escritorio remoto utilizando la aplicación de Windows "Conexión a Escritorio Remoto", colocando el número IP de su PC institucional y haciendo click en "Conectar", tras lo cual se les pedirá sus credenciales de dominio.



Anexo n.° 4. Guía de Instalación de Cliente VPN Android

OFICINA DE TECNOLOGÍAS DE INFORMACIÓN

ÁREA DE INFRAESTRUCTURA TECNOLÓGICA

GUÍA DE INSTALACIÓN DE CLIENTE VPN ANDROID

Versión 1.2

CONGRESO de la REPÚBLICA	GUÍA DE INSTALACIÓN DE CLIENTE VPN ANDROID	CÓDIGO: GUIA-INSTALACIÓN-CLIENTE-VPN-ANDROID	
		FECHA: 19/01/2021	VERSIÓN: 1.2

1. CONTROL DE CAMBIOS

VERSIÓN	FECHA	NOTA	MODIFICADO POR:
1.0	17/11/2020	Versión inicial	Pablo Sucari
1.1	12/01/2021	Actualización de configuración	Pablo Sucari
1.2	19/01/2021	Actualización de configuración	Pablo Sucari

2. RESUMEN

Procedimiento de instalación del cliente vpn Android en un dispositivo móvil.

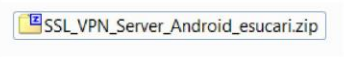
3. ÍNDICE

CONGRESO de la REPÚBLICA	GUÍA DE INSTALACIÓN DE CLIENTE VPN ANDROID	CÓDIGO: GUIA-INSTALACIÓN-CLIENTE-VPN-ANDROID	
		FECHA: 19/01/2021	VERSIÓN: 1.2

4. PROCEDIMIENTO

4.1. Descomprimir el archvio ".zip" ubicado en la ruta:

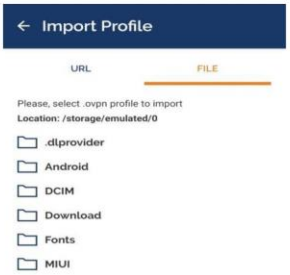
Internal Storage/Download/KnoxManage/Content



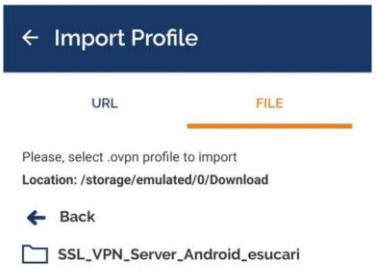
4.2. Instalar desde Play Store la aplicación OpenVpn Connect - Fast & Safe SSL VPN Client.

4.3. Al abrir la aplicación, mostrará lo siguiente:

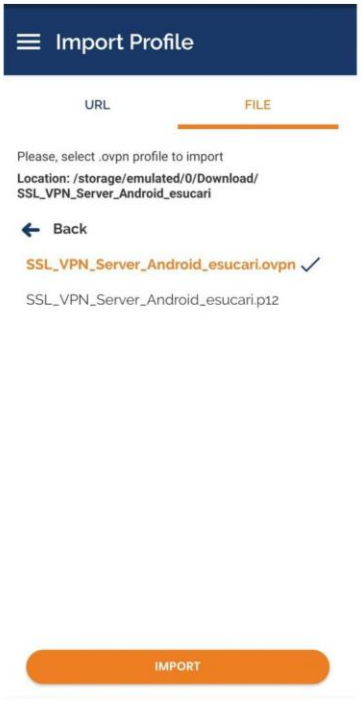
4.4. Seleccionar la opción "FILE".



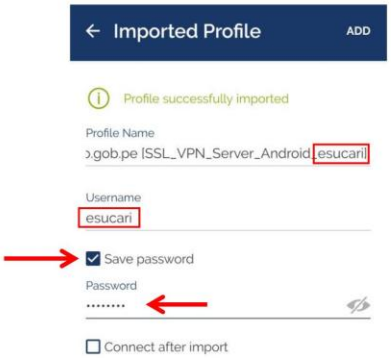
4.5. Ubicar la carpeta descomprimida del punto 4.1.



4.6. Al abrir la carpeta se visualizarán dos archivos. Primero se debe seleccionar el archivo ".ovpn" y dar click en "Importar".

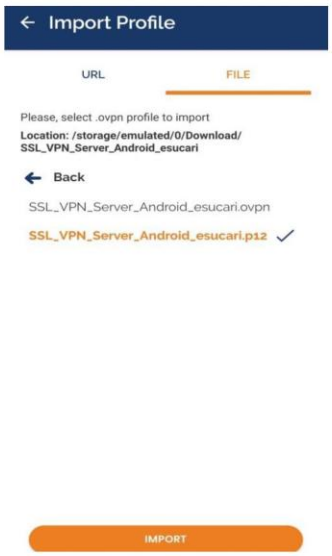


4.7. En la siguiente pantalla, ingresar el usuario, seleccionar "Save password" e ingresar vla contraseña. Luego, dar click en "ADD" para guardar el perfil.



4.8. Luego de agregar le debe mostrar la nueva conexión; en esta pantalla seleccione "+".

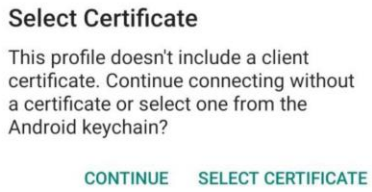
4.9. Luego, seleccionar el archivo ".p12" y dar click en "Import".



4.10. En el mensaje que muestra, dar click en "Aceptar".

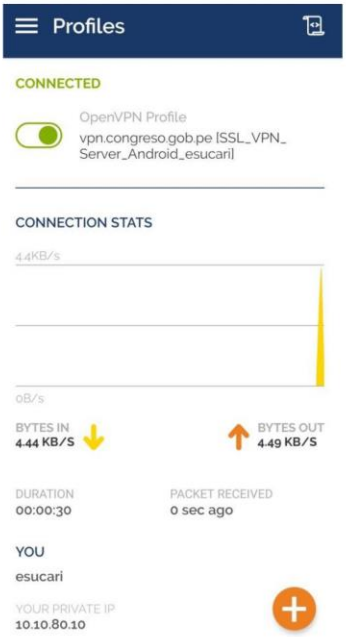
4.11. En la pantalla de conexiones, dar click en el perfil que se agregó.

4.12. En el siguiente mensaje, dar click en "Select Certificate".



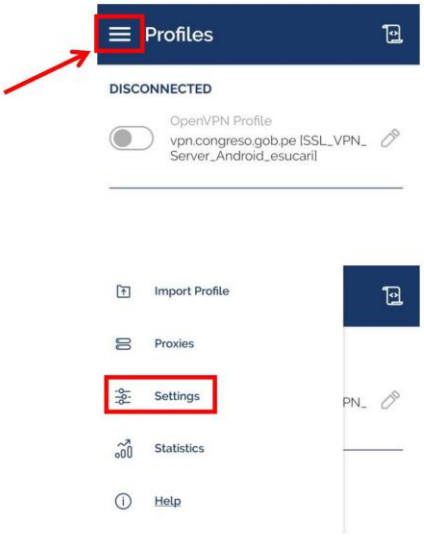
4.13. Seleccione el certificado que se instaló en el punto 4.9.

4.14. En la pantalla de conexiones, debe indicar que ya está conectado.

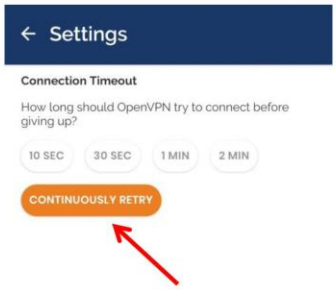


4.15. Para validar la conexión, debe ingresar a la dirección de prueba.

4.16. Finalmente, debe configurar la aplicación para reconectarse en caso haya una pérdida de datos móviles. Primero ingrese al menú y seleccione la opción "Settings".



4.17. Por último, en la sección "Connection Timeout", seleccione la opción "Continuously retry".



Anexo n.° 5. Configuración de certificado SSL para administración web OPNsense

CONFIGURACIÓN DE CERTIFICADO SSL INTERNO PARA INTERFACE GRÁFICA DE ADMINISTRACIÓN

- Se debe generar el certificado y la llave privada para el host vpn.congreso.net con el servidor de certificados SSL CA interno https://linuxca.congreso.net
- Importar el certificado en OPNsense en la opción System / Trust / Certificates > Add y llenar según se indica a continuación, colocando el contenido de los archivos de certificado y llave privada generados anteriormente desde

-----BEGIN CERTIFICATE-----

…

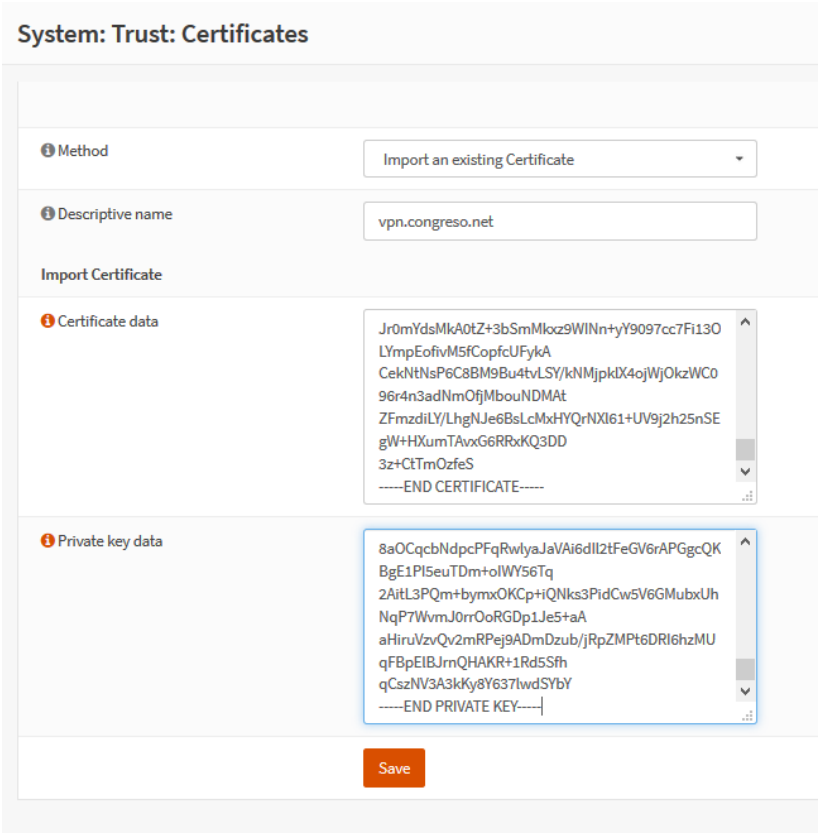
-----END CERTIFICATE-----

y

-----BEGIN PRIVATE KEY-----

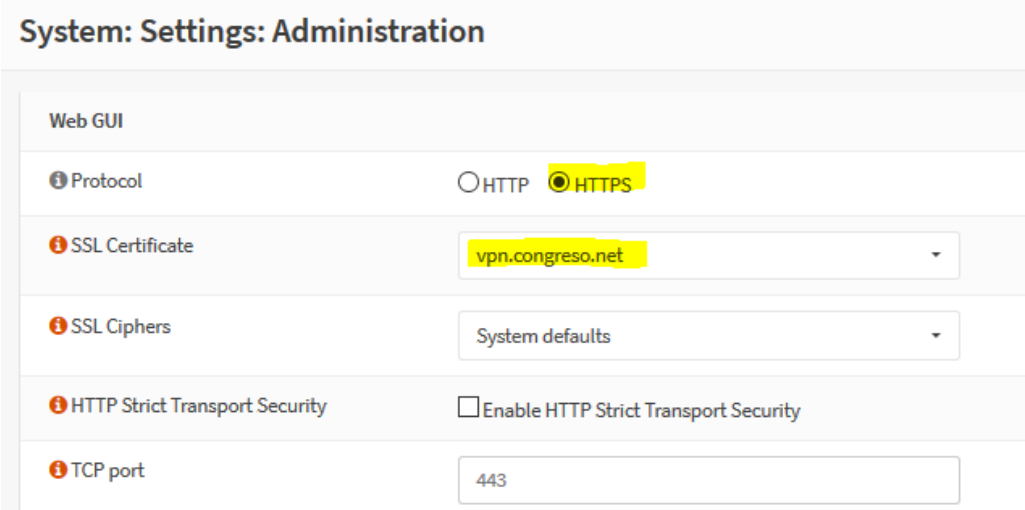
…

-----END PRIVATE KEY-----



- Se obtiene el siguiente resultado:

- Ir a System / Settings / Administration y cambiar Protocol por HTTPS, y elegir el certificado vpn.congreso.net. Grabar.



- Probar el acceso en https://vpn.congreso.net